A

Taste

of

Number Theory

K.J. Tim McDonald

Acknowledgments

For my family
Elizabeth, Lisa and Jason

Preface

The history of number theory extends over thousands of years. Some early results were found on stone tablets dating from the Babylonian era almost 4000 years ago. Humans have always been fascinated by numbers and in particular by whole numbers, their patterns and relationships.

This book attempts to be different to introductory number theory textbooks. It is a reader rather than a study book. It is written for inquisitive 16 to 19 year olds, or indeed, inquisitive minds of any age. It presents a minimum amount of the background theory of each topic before tackling some of the major results in number theory. It assumes no mathematical knowledge beyond high school algebra. It presents the theory of trigonometry and calculus in a progressive manner proving only the results that are needed for the number theory topic being studied.

Why present a number theory text that discusses simple material like the proof of the triangle inequality in an early chapter and the complicated material of the Riemann hypothesis with its background reliance on the gamma and zeta functions in its concluding chapter and the prime number theorem on the way? Maybe we can think of it as walking a chain of mountains – we start with the foothills, then some mountains are easy, others are very steep and difficult – the whole journey is a fascinating insight into the beauty of nature given us by our persistence and perspiration.

This book succeeds if it lures you into the fascinating beauty of number theory. Following Euler, we regard number theory as about all numbers, not only integers but also e and π and $\zeta(2)$. Why accept the challenge of number theory? Well, like Everest, as Hillary said, I climbed it "because it's there".

This book's inspiration is the apprenticeship system, say for becoming not just a cook, but a chef, hence the culinary references. In many countries you obtain an apprenticeship by knocking on a door and asking a master chef to take you under his wing. For the first three years of your apprenticeship you are required to attend a vocational college offering cooking trade training for one day a week. The other six days you are at the beck and call of the master.

The aim of this book is to allow the young reader to read and study and understand some of the great results in number theory, even though the reader is obviously just an apprentice. Hopefully you too will know enough from the "shopping excursions" and brief introductions to be able to "cook alongside" and appreciate the wide range of wonderful results put together by the master chefs of number theory, the greats like Pythagoras, Diophantus, Fermat, Newton, Euler, Gauss, Legendre, Lagrange, Riemann, Erdös and Selberg. Hopefully you too will be inspired to do the work needed to become a master number theorist. There's a host of unexplored areas in number theory just as there are a host of unexplored tastes in most of our mouths. Like Wiles, you may want to find that conjectured recipe, to savor the loneliness and frustrations of the long years in the cold attic in the hope that one day you will taste the adulations of your peers.

Of course, if you want to solve any of the many challenges left in number theory, to become a master number theorist, then you need to go through the corresponding "blood, sweat and tears" process to becoming a chef. As Euler said to his Tsar patron who assumed as king that he could simply have a quick course to do what Euler did, "Alas, my liege, there are no kings in mathematics".

End Signals

The end of the proof of a Theorem is signaled with a box, $\Box$
The end of an Example of more than one line is signaled with a diamond, $\diamond$.

Greek Alphabet Letters used in this Book

Letter	*Spoken as*
α	*alpha*
β	*beta*
γ	*gamma*
Δ, δ	*delta*
ϵ	*epsilon*
ζ	*zeta*
θ	*theta*
μ	*mu*
ξ	*xi*(*kigh*)
Π, π	*pi*
ρ	*rho*
Σ, σ	*sigma*
τ	*tau*
ϕ	*phi*
Ψ, ψ	*psi*(*sigh*)
Ω, ω	*omega*

Contents

I Mathematics and Number Theory 2

1 Our field of study 4

1.1 What is mathematics? 4

1.2 Mathematical operations 5

1.3 Number symbols 5

1.4 Algebra 5

1.5 Fractions and Decimals 6

1.6 Doing mathematics: Euclid's Geometry 7

1.7 Notation 8

1.7.1 Logic Notation 8

1.7.2 Sum and Product notation 8

1.7.3 Set Notation 8

1.8 Number Sets 9

1.9 Doing Mathematics - Axioms of Real Numbers 10

1.10 Further extending our Vocabulary 11

1.11 The Importance of Algebra 13

1.12 Branches of Mathematics 13

1.13 A Mathematical "no-no" 14

2 What is Number Theory? 16

2.1 What is number theory? 16

2.2 Is number theory important? 17

2.3 Is it all done? 18

2.4 Axioms of Integers 18

2.5 How is it done? Mathematical Proofs 20

2.5.1 Direct Proofs 21

2.5.2 Proofs by Contradiction 22

2.5.3 Contrapositive proofs 22

2.5.4 Mathematical Induction 23

II A Pythagorean Feast - Pythagoras to Wiles 26

3 Pythagoras: The $n = 2$ case. 28

3.1 Area 28
3.2 Pythagoras 29
3.2.1 Irrational Numbers 30
3.2.2 Pythagorean Triples 30

4 The $n = 4$ case 35
4.1 Method of Infinite Descent 35
4.2 Proof of the $n = 4$ case 36
4.3 Comments on the General Case 37

5 Euler: The $n = 3$ Case by Elementary Methods 38
5.1 Well-ordering principle 39
5.2 Divisibility and Factorization of Integers 39
5.3 Euler's Proof of the $n = 3$ case 43
5.3.1 The Lemmas 43
5.3.2 The Theorem: $n = 3$ case 50

6 Shopping Excursion I 55
6.1 The Triangle Inequality for Real Numbers 55
6.2 Complex Numbers – Notation and Definitions 56
6.3 Definitions using Polar Coordinates 57
6.4 The Theory of Complex Numbers 58
6.5 Triangle Inequality for Complex Numbers 60

7 The n = 3 Case by Complex Techniques 61
7.1 Algebraic Numbers and Algebraic Integers 62
7.2 The $k(\rho)$ Algebraic Integers 62
7.3 The Proof of the $n = 3$ Case 69

8 Postprandial Discussion: The General Case 75

III Shopping Excursion II - Calculus 77

9 Calculus and Infinite Series 79
9.1 What is Calculus? 79
9.2 Branches of Calculus 80
9.3 Differentiation 81
9.3.1 Slope or gradient of a line 81
9.3.2 Slope of Tangent Line to a Curve 81
9.3.3 The derivative of $y = f(x)$ at $x = a$ 83
9.3.4 Rules of Differentiation 84
9.4 Antiderivatives 88
9.4.1 Family of Antiderivatives 89

9.4.2 Rules for Indefinite Integration 89
9.5 Integration 91
9.5.1 Fundamental Theorems of Calculus 92
9.5.2 Properties of Definite Integrals 96
9.6 Change of Variables by Substitution 99
9.7 Infinite Series 100
9.7.1 Convergence of an infinite series 100
9.7.2 The Harmonic Series 101
9.7.3 Formal Definition of Convergence 102
9.7.4 Geometric Series 103
9.7.5 Tests for Convergence 103
9.8 Another mathematical “no-no” 106

IV Degustation – Some Classic Pearls of Number Theory108

10 Solving $ax + by = 1$, $gcd(a, b) = 1$. 110
10.1 Finding all solutions 110
10.2 Algorithm for finding the minimal solution. 111

11 The Chinese Remainder Theorem 118
11.1 Congruences 118
11.2 Chinese Remainder Theorem 119
11.3 Generalization of the Chinese Remainder Theorem 121
11.4 What Day of the Week was It? 125

12 Binomial Theorem 127
12.1 Pascal”s Triangle 128
12.2 Binomial Theorem 130

13 Fermat’s Two Squares Theorem 132
13.1 Gaussian Integers 132
13.1.1 Properties of Gaussian Integers 133
13.2 Major Theorems for Gaussian Integers 139
13.2.1 Euclidean Algorithm in Gaussian Integers 139
13.3 Fermat’s Two Squares Theorem 142
13.4 Finding a, b for a given p. 146
13.4.1 Two Finite Groups 146
13.4.2 Primitive roots or generators 147
13.4.3 Finding a, b 148

V Shopping Excursion III Exponential and Trigonometric Functions 151

14 Calculus of Exponential and Trigonometric Functions 153

14.1 The Natural Exponential Function 153

14.1.1 Graphs of exponential functions 153

14.1.2 Natural Exponential Function 154

14.1.3 Derivative of the Natural Exponential Function 154

14.2 The Trigonometric Functions 155

14.2.1 Angle 155

14.2.2 Degree 156

14.2.3 Radian 157

14.2.4 Radians and Degrees 158

14.2.5 Trigonometric Functions 158

14.2.6 Important Values of the Trigonometric Functions 160

14.3 Right Triangle Trigonometry 160

14.4 Some Important Trigonometric Identities 162

14.5 Derivatives of the Sine and Cosine Functions 164

15 Taylor Series and Roots of Unity 167

15.1 Mean Value Theorem 167

15.2 Taylor Series 168

15.3 Taylor Series of the Exponential Function 171

15.4 Taylor Series for Sine and Cosine Functions 172

15.5 Euler's Formulas 173

15.6 Roots of Unity 174

VI Exotic Tastings

Using Infinite Series 175

16 The Numbers e and π 178

16.1 e and π are irrational 178

16.1.1 e is irrational 178

16.1.2 π is irrational 180

16.2 e and π are Transcendental Numbers. 185

16.2.1 e is transcendental. 187

16.2.2 π is transcendental 190

16.3 Finding π 194

17 Bernoulli Numbers and Sum of a Finite p-series 196

17.1 Bernoulli Numbers 196

17.2 Formula for the Sums of Powers of Integers 202

VII Shopping Excursion 4

The Natural Logarithm Function **205**

18 The Natural Logarithm Function **207**
18.1 Inverse Functions 207
18.1.1 Finding inverse functions 208
18.1.2 Sketching the graphs of inverse functions 209
18.2 Logarithmic Functions 209
18.2.1 Graphs of logarithmic functions 210
18.3 The Natural Logarithmic Function 210
18.4 Derivative of the Natural Logarithmic Function 211
18.5 Alternative definition of $\log x$ 211
18.6 Laws of Logarithms 212
18.7 Exponential Laws for Base e. 214
18.8 $\log x$ and $\ln x$ 215
18.9 The derivative of $\log g(x)$. 215
18.10 Technique of logarithmic differentiation 216
18.11Taylor Series of $\log(1+x)$. 216

19 Euler's Zeta Function **219**
19.1 A Trigonometric Exploration 220
19.2 Infinite product for $\sin \pi x/\pi x$ 222
19.3 Hyperbolic Functions 224
19.4 Formula for $\zeta(2k)$ 225

VIII A Prime Banquet

The Entrée Courses **229**

20 All Primes and $4n + 3$ Primes **231**
20.1 General observations 231
20.2 Infinitude of primes 232
20.3 Primes in an arithmetic progression 232
20.4 Primes of the form $4n + 3$. 233
20.4.1 Congruences 233
20.5 Proof of the $4n + 3$ case 235

21 Primes of the form $4n + 1$: Method 1 **236**
21.1 Euler's Totient Function 236
21.2 Congruence Lemmas 237
21.3 Euler's and Fermat's Theorems 239
21.4 Method 1 Proof 240

22 Primes of the form $4n+1$: Method 2 **241**
22.1 The Key Lemma 241
22.2 Method 2: Proof 242

23 Primes of the form $4n+1$: Method 3 **243**
23.1 Quadratic Residues 243
23.2 Finding Quadratic Residues and Non-residues 244
23.3 Wilson's Theorem 245
23.4 Method 3 Proof 248

24 Primes of the form $4n+1$: Method 4 **249**
24.1 The Möbius function 249
24.2 Euler's Totient Function 254
24.3 Group Theory 257
24.4 Congruence and Finite Groups 259
24.4.1 The Additive Group $\mathbb{Z}_n$ 259
24.4.2 The Multiplicative Group $\mathbb{Z}/n\mathbb{Z}$ 261
24.4.3 Cyclic Groups 262
24.5 More on Groups 265
24.5.1 Roots of Unity 268
24.6 Conclusion 269

25 Primes of the form $4n+1$: Method 5 **271**
25.1 Zeta Function $\zeta(s)$ 271
25.2 Infinitude of Primes 274
25.3 Dirichlet's Proofs 276
25.3.1 The χ function 277
25.3.2 The $L(s)$ and $Q(s)$ Functions 277
25.4 Proof of $4n+3$ Case 279
25.5 Proof of $4n+1$ Case 280

IX Sorbet – Gamma Function **282**

26 Gamma Function **284**
26.1 Euler-Mascheroni Constant 284
26.2 Observations on Calculus on the Complex Plane 286
26.3 Weierstrasse Gamma Function 286
26.4 Euler Gamma Function 293
26.5 Duplication Formula 297

X 20th Century Banquet

Counting the Primes: Euler to Selberg 299

27 Counting the Primes 301

27.1 Algorithm for determining whether a number is prime. 302
27.2 Sieve of Erasthosthenes 302
27.3 $\pi(x)$ - the number of primes $\leq x$. 303
27.4 Cardinality of a Union of Sets 304
27.5 Legendre's Theorem 306
27.6 Approximations to $\pi(x)$. 309
27.7 The Prime Number Theorem 310
27.8 Chebyshev's Theorem 310
27.9 Big-O and Little-o Notation 317
27.10 Selberg's Proof of the PNT 318
27.10.1 Equivalences to PNT 319
27.10.2 Two Critical Theorems 323
27.10.3 Selberg's Asymptotic Formula 327
27.10.4 Proof of the Prime Number Theorem 329
27.10.5 Pathway to Lemma 9 331
27.10.6 Pathway to Lemma 12 332
27.11 Lemmas 13-15 333

28 Bertrand's Postulate 334

28.1 Preliminaries 334
28.2 Bertrand's Postulate 340

XI After-Glow

Riemann 343

29 The Riemann Hypothesis 345

29.1 First Steps with Riemann 345
29.2 The Riemann Zeta Function 346
29.3 The pole of $\zeta(s)$ 349
29.4 The Trivial Zeros of $\zeta(s)$ 349
29.5 Functional Equation of $\zeta(s)$ 351
29.6 The Non-Trivial Zeros of $\zeta(s)$ 352
29.7 Riemann Hypothesis 354

Part I

Mathematics and Number Theory

We begin with a brief review of “what is mathematics?” and “what is the branch of mathematics called number theory?”

Mathematics is a branch of philosophy which itself is the study of the nature of, and principles underlying, our universe. All disciplines of science are branches of philosophy. They all need mathematics and accordingly, mathematics is sometimes called the “Queen of the Sciences”. Many of the early philosophers, from Plato to Descartes to Bertand Russell, also made significant contributions to mathematics.

You apprentice to a branch of science or mathematics by becoming a graduate student. If your masters judge you have a broad knowledge of mathematics and have made a significant original contribution through supervised research to their branch of science or mathematics, then their university awards you a Doctorate in Philosophy.

Chapter 1

Our field of study

Course: Perusing the Menu I

1.1 What is mathematics?

Mathematics is the logical output of our minds when we look at situations and see physical commonalities at the highest level of abstraction.

For example, if Mary, Martha and Jane each have a child, then the "…" mothers altogether have "…" children. To describe what is common to the group of mothers and to the group of children, we invent a word, namely, "three".

We have used all of logic and intuition, analysis and construction, generality and individuality[1] even in this simple example. There may be other commonalities: the mothers may all be blondes, the children may all be boys, the mothers may all be wearing red lipstick, the children may all be laughing. But at the highest level of physical commonalities or abstraction, there are three of each of mother, child, blonde, red lipstick-wearer, laugher. The mother-child combinations may belong to three families, live in three separate houses, travel in three different cars. The "three" survives into these different constructions, while the blonde, boy, red-lipstick, laughing abstractions do not.

The highest level of abstraction we call numbers: one, two, three, four, etc. Each abstraction defines a group of a different size.

Our abstractions do not just apply to numbers. We see similar commonalities in geometric abstractions such as points, lines, triangles, circles, spheres, and other geometric objects. Mathematicians have extended their abstractions way beyond these!

Interestingly, psychologists distinguish the left and right sides of the human brain. The left side is best at logic, language, numbers and analytical thinking – in mathematics, at arithmetic and algebra. The right side is best at expressive and creative

[1] Words used in "What is Mathematics" by Courant and Adler

tasks – in mathematics at geometry and topology. This may explain why some students are good at arithmetic and algebra and struggle with geometry and shapes, and vice versa. It is certainly true that few mathematicians are equally adept in all branches of mathematics.

1.2 Mathematical operations

As we work with numbers, we intuitively begin to define operations. We can add two more mothers to our group of three, we can subtract one mother, we can put this group in a car and a similar group in five other cars and we know how many mothers we have altogether by multiplication. When the cars reach a destination we can divide the exiting occupants into two larger groups. We can do all these operations of $+, -, \times, \div$ in our head, but we do this in shorthand, more importantly, we internationalize the language of our calculations. I cannot talk Portuguese to a Brazilian, but we both know the answer to $2 + 2 =?$ written on a piece of paper.

1.3 Number symbols

Many civilizations developed their different symbols for numbers. What has become international is due to the Arabic-Hindu traditions. The list is short, namely, $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Why only these? Maybe because we have this many fingers or toes. More probably, because we don't need any more and any less doesn't work as efficiently for us. Of course, for computers it is different, they just need two: $0, 1$ for off/on.

Back to our operations $+, -, \times, \div$. We need only the ten symbols for an infinite number of numbers because we have accepted an international place number system. We know what 547 means. We know what "tens" are and that here we have 4 of them. We know "hundreds" are and that here we have 5 of them. And we know what "units" are and that here we have 7 of them. For us it is now easy to calculate the arithmetic problems $237 + 4378$ or 367×114 or $289 \div 17$. The poor old Romans with their number symbols may have tried to add $LMCIX + CLXIV$, pity them if it became $LMCIX \times CLXIV$.

1.4 Algebra

We also need the concept of negative numbers. If I try to remove 8 objects from a set of 6 objects, I come up short by 2. I write $6 - 8 = -2$.

We come to "how many". If we can put 17 people in each bus and we have 289 people then we know how many buses we need. We just need division $289 \div 17 = 17$.

It is an easy step to algebra. If one of our buses already has 11 people in it, how many more can it take? We define "variable", we solve the equation,

$$x + 11 = 17$$

To do this, we logically set up equality rules, that we can add or subtract the same number from both sides of the equation, or multiply or divide both sides of the equation by the same number. Then,

$$x + 11 = 17 \Rightarrow x + 11 - 11 = 17 - 11 \Rightarrow x = 6$$

where we have added a logic symbol ⇒ meaning "*if . . . then*" or "implies."

1.5 Fractions and Decimals

Division leads us to the need for fractions,

If I divide a pizza into four pieces and eat one piece,
how much is left?

I need the symbol $\frac{3}{4}$ for three-fourths,

and to decimals,

I know a dollar is 100 cents, but if I have one dollar
and divide it among my four friends,
how many dollars did each friend get?

I need the symbol 0.25 for 25 cents in terms of 1 dollar

For the latter, we therefore extend our place number system to constructions such as 37.419 and we know what this means in terms of "tenths", "hundredths", "thousandths".

For fractions, we learn that a fraction in lowest terms is the head of an infinite family, for example,

$$\frac{3}{4} = \frac{6}{8} = \frac{9}{12} = \ldots = \frac{3n}{4n}, \text{n a non-zero integer,}$$

and that we can add and subtract fractions by converting to them to the appropriate member of the respective family, for example,

$$\frac{5}{6} + \frac{3}{4} = \frac{20}{24} + \frac{18}{24} = \frac{38}{24} = \frac{19}{12} = 1\frac{7}{12}$$

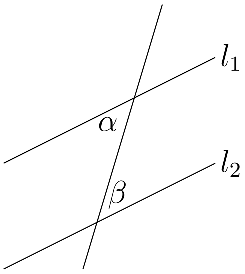
The last two equivalences required us to prove cancellation and define a notation for mixed fractions.

1.6 Doing mathematics: Euclid's Geometry

How do we "do" mathematics?
Each branch of mathematics, beginning with arithmetic, algebra and geometry, has its own set of notations and axioms from which are developed definitions, then proofs or theorems. All the axioms are based on logic and intuition, analysis and construction, generality and individuality.

A very long time ago, Euclid (circa 300 BC) stated five axioms or postulates for geometry on a plane or flat surface, the most logical environment since the earth was, after all, flat.

1. A straight line segment can be drawn joining any two points.
2. Any straight line segment can be extended indefinitely in a straight line.
3. Given any straight line segment, a circle can be drawn having one end as the center and the segment as a radius.
4. All right angles are congruent.
5. If two lines are drawn which intersect a third line in such a way that the sum of the inner angles is less than two right angles, then the two lines must invariably intersect one another on that side if extended far enough.
   (sic: parallel lines never meet),
   (sic: the alternate interior angles formed by a line intersecting two parallel lines are equal)
   Diagrammatically the last version of the fifth axiom proves theorems such as if $l_1 \parallel l_2$ then for the angles, $\alpha = \beta$.



Implied in the axioms is a set of definitions for point, line, angle, right angle and circle. If you think the definitions are obvious, try writing a definition of a point or a line or an angle.
A typical theorem is that the sum of the interior angles of a triangle is two right angles or, in our extended notation, 180^0. (To prove it, draw any triangle and a line through any vertex parallel to the opposite side and use the fifth axiom).
Before we consider the axioms for numbers, let us first extend our mathematical vocabulary.

1.7 Notation

1.7.1 Logic Notation

If P and Q are statements we have,

Symbol	*Meaning*
$P \Rightarrow Q$	If P then Q or P implies Q
$P \Leftrightarrow Q$	P and Q are equivalent statements, or P implies Q and Q implies P

1.7.2 Sum and Product notation

Symbol	*Meaning*
Sum: $\sum_{i=1}^{n} a_i$	$= a_1 + a_2 + \ldots + a_n$
Product: $\prod_{i=1}^{n} a_i$	$= a_1 a_2 \cdots a_n$

1.7.3 Set Notation

A set is a collection of objects. For our purposes, the objects are numbers, functions or polynomials. We use the following notation.

Symbol	*Meaning*
$A = \{x, y, z, ...\}$	*A is the set of objects or elements* $x, y, z, ...$
$\mid$	*such that*
$x \in A$	x *is an element of set* A
$x \notin A$	x *is not an element of set* A
$A \cup B$	*the union of two sets* A *and* B
$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$	*the union of two sets* A, B *is the set of elements* x *such that* x *is in* A *or* x *is in* B
$A \cap B$	*the intersection of two sets* A *and* B
$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$	*the intersection of two sets* A, B *is the set of elements* x *such that* x *is in* A *and* x *is in* B
$A \subset B$	A *is contained within* B *or* A *is a subset of* B *that is, every element of* A *is also in* B
$A \supset B$	A *contains* B *or* B *is a subset of* A *that is, every element of* B *is also in* A
$A = B$	*Sets are equal if* $A \subset B$ *and* $A \supset B$ *–we say equality is double containment*

1.8 Number Sets

We define,

Definition 1. *natural numbers* $\mathbb{N}$, *integers* $\mathbb{Z}$ *and rational numbers* $\mathbb{Q}$
The natural numbers, integers and rationals are defined by,

$$\begin{aligned}\mathbb{N} &= \{1, 2, 3, \ldots\}\\ \mathbb{Z} &= \{0, \pm 1, \pm 2, \pm 3, \ldots\}\\ \mathbb{Q} &= \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}\end{aligned}$$

Note 1. *We extend set notation to expressions such as,*
$\mathbb{Z}^{+}$ *are the positive integers* $\{1, 2, \ldots\}$
$\mathbb{Q} - \{0\}$ *or* $\mathbb{Q}/\{0\}$ *are the rational numbers with 0 removed.*

The Pythagorean Greeks discovered there are other numbers, for example the length of the hypotenuse of a right triangle whose other sides are both 1. They didn't have the symbol $\sqrt{2}$ for its length. We shall prove below that $\sqrt{2}$ is not a rational number. We call these numbers irrational. Both π and e are irrational as we shall prove later. There is no symbol for the set of irrational numbers but there is for the union of $\mathbb{Q}$ and the irrationals. We define,

Definition 2. *real numbers*
The real numbers are defined by $\mathbb{R} = \mathbb{Q} \cup \{x | x \textit{ is irrational}\}$

Example 1. $0, -4, 0.87, -\frac{7}{11}, \sqrt{3}, \pi \in \mathbb{R}$.

Finally, let's skip ahead and solve a quadratic equation such as $x^2 + 1 = 0$. Since x^2 is always positive (we need to prove this), then when you add it to 1 you cannot possibly obtain 0 as a result. We define imaginary or complex numbers by first saying,

$$x^2 + 1 = 0 \Rightarrow x^2 = -1 \Rightarrow x = \pm\sqrt{-1} \Rightarrow x = \pm i, \text{ where } i = \sqrt{-1}$$

then we have,

Definition 3. *complex numbers*
The complex numbers are defined by $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}, \ i = \sqrt{-1}\}$

We can write $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, meaning each left set is contained within the one on its right. While number theory is predominantly the study of the integers, we shall find its proofs require access to the other four basic sets.

1.9 Doing Mathematics - Axioms of Real Numbers

If we apply our logic and intuition, analysis and construction, generality and individuality to the real numbers under the operations of addition and multiplication, we accept, without proof, the following axioms.

1. Closure of $\mathbb{R}$ under addition and multiplication.
   For all $a, b \in \mathbb{R}$, both $a + b$ and $a \times b$ are in $\mathbb{R}$.

2. Associativity of addition and multiplication.
   For all $a, b, c \in \mathbb{R}$, the following equalities hold:
   $a + (b + c) = (a + b) + c$ and $a \times (b \times c) = (a \times b) \times c$.

3. Commutativity of addition and multiplication.
   For all $a, b \in \mathbb{R}$, the following equalities hold:
   $a + b = b + a$ and $a \times b = b \times a$.

4. Existence of additive and multiplicative identity elements.
   There exists an element of $\mathbb{R}$ called the additive identity element and denoted by 0, such that for all $a \in \mathbb{R}$, $a + 0 = a$.
   Likewise, there is an element of $\mathbb{R}$, called the multiplicative identity element and denoted by 1, such that for all $a, b \in \mathbb{R}, a \times 1 = a$.

5. Existence of additive inverses and multiplicative inverses.
   For every $a \in \mathbb{R}$, there exists an element $-a \in \mathbb{R}$, such that $a + (-a) = 0$.
   Similarly, for any $a \in \mathbb{R}$ other than 0, there exists an element $a^{-1} \in \mathbb{R}$ such that $a \times a^{-1} = 1$.
   (The expressions $a + (-b)$ and $a \times b^{-1}$ are also denoted $a - b$ and $\frac{a}{b}$ respectively.)
   In other words, subtraction and division operations exist.

6. Distributivity of multiplication over addition.
   For all $a, b, c \in \mathbb{R}$, the following equality holds,
   $a \times (b + c) = (a \times b) + (a \times c)$.

7. $\mathbb{R}$ is ordered, meaning that for all real numbers

   - If $x \geq y$ then $x + z \geq y + z$
   - If $x \geq 0$ and $y \geq 0$ then $xy \geq 0$.

In dealing with equations, we assume also the additive and multiplicative laws of equality, namely, we can add the same number to both sides of an equation and we can multiply both sides of an equation by the same number.

We will use these axioms to prove theorems. Here is a simple example.

Theorem 1. *(Additive Cancellation)*
For all real numbers x, y, x,

$$x + z = y + z \Rightarrow x = y$$

In mathematical language: $\forall x, y, z \in \mathbb{R}, x + z = y + z \Rightarrow x = y$.
(translation: for all real numbers x, y, z, if $x + z = y + z$ then $x = y$.)

Proof.

$$\begin{aligned}
&x + z = y + z \\
&\Rightarrow (x + z) + (-z) = (y + z) + (-z) \quad (Law\ of\ equality) \\
&\Rightarrow (x + (z + (-z)) = y + (z + (-z)) \quad (Associative\ axiom) \\
&\Rightarrow x + 0 = y + 0 \quad (Inverses\ axiom) \\
&\Rightarrow x = y \quad (Identity\ axiom)
\end{aligned}$$

□

1.10 Further extending our Vocabulary

Mathematics is the language of numbers and the other abstracted symbols describing the highest level of abstraction from physical objects (points, lines, angles, triangles, etc.). Its alphabet includes the symbols and notation met above. Its sentences are constructed from the symbols and notation. The axioms are the rules of its grammar. Just as we learned our native language in steps, so we learn mathematics in steps. Just as we had to learn vocabulary and how to spell before we could apply the rules of grammar to make intelligible sentences, so we have to learn the meaning of terms and notation such as:

- Divisibility in $\mathbb{Z}$: we say a divides b, written $a|b$ if $b = ac, c \in \mathbb{Z}$.
- Primes: a natural number greater than 1 is a prime if it is only divisible by itself and 1. We will use $\mathbb{P}$ for the set of all primes.
- Composites: the natural numbers other than the primes or 1.
- Natural number exponents or powers. We define $a^n,\ a, n \in \mathbb{N}$ by

  $$a^n = \overbrace{a \times a \times \cdots \times a}^{n\ times}$$

  In particular,

  - Squares: $a^2 = a \times a$
  - Cubes: $a^3 = a \times a \times a$

- Rational exponents and roots: we define $\sqrt[n]{a},\ a, n \in \mathbb{N}$ by $\sqrt[n]{a} = a^{\frac{1}{n}}$ where

$$\overbrace{a^{\frac{1}{n}} \times a^{\frac{1}{n}} \times \cdots \times a^{\frac{1}{n}}}^{n\ times} = a$$

  In particular,

  - Square roots: $\sqrt{a} \times \sqrt{a} = a$
  - Cube roots: $\sqrt[3]{a} \times \sqrt[3]{a} \times \sqrt[3]{a} = a$

- Factorization: If $b \in \mathbb{N}$ is divisible by other natural numbers greater than 1 and less than b we say b can be factored, e.g., $22 = 2 \times 11$.

- Pairs of numbers: We say the greatest common divisor of the numbers a, b is c if c is the largest number than divides both a and b and we write $gcd(a, b) = c$.

Just as we developed versatility in the use of our native language by learning simple constructions of the alphabet symbols into words, so we started mathematics with learning our times-tables.

×	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	14	16	18	20	22	24
3	3	6	9	12	15	18	21	24	27	30	33	36
4	4	8	12	16	20	24	28	32	36	40	44	48
5	5	10	15	20	25	30	35	40	45	50	55	60
6	6	12	18	24	30	36	42	48	54	60	66	72
7	7	14	21	28	35	42	49	56	63	70	77	84
8	8	16	24	32	40	48	56	64	72	80	88	96
9	9	18	27	36	45	54	63	72	81	90	99	108
10	10	20	30	40	50	60	70	80	90	100	110	120
11	11	22	33	44	55	66	77	88	99	110	121	132
12	12	24	36	48	60	72	84	96	108	120	132	144

It is also useful to have learned the squares of all the numbers from 1 to 20, the rest are:

$$13^2 = 169,\ 14^2 = 196,\ 15^2 = 225,\ 16^2 = 256$$
$$17^2 = 289,\ 18^2 = 324,\ 19^2 = 361,\ 20^2 = 400$$

We also need to recognize the lower powers of $2, 3, 4, 5$, and 6.

n	2^n	3^n	4^n	5^n	6^n
1	2	3	4	5	6
2	4	9	16	25	36
3	8	27	64	125	216
4	16	81			
5	32	243			
6	64				

1.11 The Importance of Algebra

Most college students are required to take a College Algebra course. Not only does a serious student of number theory need to be versatile with numbers, knowing multiplications and factors of numbers without (much) thought, but familiarity and ease of use of the basic topics of algebra is essential. Topics like the exponent rules, adding and multiplying polynomials and rational functions and factoring polynomials.

In number theory, we need to be crystal-clear that variables represent numbers, mostly integers. As a party trick, if you know how to factor the difference between two squares,

$$a^2 - b^2 = (a+b)(a-b),$$

then you can beat an opponent with a calculator in answering questions like 37×43, 59×61, 88×92, 996×1004 in less time![2]. Of course, you need to select the questions! Don't let her say 83×87!

1.12 Branches of Mathematics

At the simplest level, Mathematics is divided into two branches: pure and applied. Pure mathematics studies entirely abstract objects; applied mathematics uses the results of pure mathematics to model objects studied in sciences and engineering.

Pure mathematics encountered in K-12 education includes arithmetic, geometry, algebra, trigonometry and calculus. The use of concrete examples to understand pure mathematics is essentially applied mathematics.

• Arithmetic broadens into number theory and combinatorics. • Geometry broadens into topology. • Algebra broadens into abstract algebra. • Calculus broadens into analysis, both real and complex.

Mathematicians love to mix and match, they delight in a proof that crosses over and uses results from one branch to prove a result in another, none more so than number theorists! The boundaries between algebra, analysis and topology blur as we delve deeper and deeper into our abstractions.

[2] For example, $43 \times 37 = (40+3)(40-3) = 40^2 - 3^2 = 1600 - 9 = 1591$

1.13 A Mathematical “no-no”

We defined above the fractions or rational numbers $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$. We can interpret the restriction $b \neq 0$ as “division by 0” is not allowed in mathematics. Students will generally answer the question as to “Why not?” by saying “It is undefined”. But why is it undefined, why is it not allowed? Let’s do it and see why not.

We agree

$$1 \times 0 = 0 \text{ and } 2 \times 0 = 0$$

Hence,

$$1 \times 0 = 2 \times 0$$

Let’s divide by 0. We get,

$$\frac{1 \times 0}{0} = \frac{2 \times 0}{0}$$

Cancelling the zeros gives,

$$1 = 2$$

which is absolutely ridiculous or as I say to my students “It’s a stupid result.” So that is why division by zero is not allowed in mathematics. It gives stupid results. There is nothing special about starting with 1 and 2 and multiplying them by zero. We could start with any numbers at all, for example π and $\sqrt{3}$ and then “prove” they are equal. Then mathematics is reduced to “All numbers are equal!”

So, when we move into algebra and trigonometry and calculus, we always need to be careful that we are not dividing by zero. For example let’s start with,

$$a^2 - a^2 = a^2 - a^2$$

We can factor the two sides of this equation in different ways – either taking out a common factor of a on the left side or using the formula $x^2 - y^2 = (x + y)(x - y)$ on the right side to give,

$$a(a - a) = (a + a)(a - a)$$

Dividing both sides by the common factor $(a - a)$ gives,

$$\frac{a\cancel{(a-a)}}{\cancel{a-a}} = \frac{(a+a)\cancel{(a-a)}}{\cancel{a-a}} \Rightarrow a = a + a \Rightarrow a = 2a \Rightarrow 1 = 2 \ (\textit{Stupid}!)$$

In this example, without thinking enough, we divided by $a - a$, but that is 0.
This is a major reason why any function must always be defined not only by its

relationship between the variables, but also by the allowed values of the independent variables which we call the domain of the function.

For example, $y = \dfrac{1}{x-1}$ (where values of the independent variable x generate values of the dependent variable y) should always be written (but often is not!) as,

$$y = \frac{1}{x-1}, \ x \neq 1$$

so that we exclude division by zero.

Division by zero is by no means the only mathematical "no-no" as we will see. The domain of a function can be limited by other reasons. We'll deal with these as they arise.

Chapter 2

What is Number Theory?

Course: Perusing the Menu II

2.1 What is number theory?

Nowadays we say number theory is the branch of mathematics devoted entirely to the study of the integers. Its old names were arithmetic or higher arithmetic.

In general, the problems dealt with in number theory are easily explained to a lay audience. Their proofs, however, are often incomprehensible to the lay person, due to the fact that number theorists readily use results from other branches of mathematics or other findings in number theory in their proofs. Understanding their proofs therefore assumes a significant mathematical background.

The most recent example is the proof of Fermat's Last Theorem (FLT) by Andrew Wiles. We all know at least one solution $3^2+4^2=5^2$ in the integers to the Pythagorean equation $x^2+y^2=z^2$ so it is easy to understand the statement of the FLT,

There are no non-zero integer solutions to $x^3+y^3=z^3,\ x^4+y^4=z^4$ etc., or in general for $x^n+y^n=z^n,\ n\geq 3$,

yet its proof is incomprehensible to most mathematicians, let alone the lay person.

There are five major branches of number theory.

1. Elementary number theory uses proof techniques that do not include the tools of complex analysis ($i=\sqrt{-1}$, etc.). The title is misleading since elementary proofs may be considerably more difficult that those acquired through complex analysis. Complex analysis itself is barely 200 years old, so there are thousands of years of elementary proofs in number theory. One of the oldest is the Pythagorean theorem,
   In a right triangle, the square of the length of the hypotenuse is equal to the sum of the squares of the lengths of the other two sides.

2. Analytic number theory uses the tools of analysis, particularly complex analysis. One of its most famous achievements was the proof of the prime number theorem in the 1890's by Hadamard and de la Vallée-Poussin. Interestingly, Selberg and Erdös proved the same theorem in 1949 using only elementary techniques. The theorem states that the number of primes less than or equal to x gets closer and closer to $\frac{x}{log\ x}$ as x gets larger or tends to infinity, again very easy to state, yet it took over 100 years to find a proof. (Of course, we will define *log* x later!)

3. Algebraic number theory is the study of algebraic numbers using the results of abstract algebra. An algebraic number is the root of a non-zero polynomial in one variable with integer coefficients. There is the well known formula for the roots of quadratic equations,

$$ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

and there are also formulas for the roots of cubic and quartic equations, but in general the roots of polynomials of degree 5 or higher cannot be expressed in terms involving $+, -, \times, \div$, roots and powers, yet the graph of every polynomial of odd degree has at least one $x-$axis intercept, making that root a real number. We therefore need to add the algebraic numbers to the set of real numbers, indeed, they are the majority of the real numbers!

4. Diophantine number theory studies the integer solutions of polynomial equations in one or more variables. The general formulas for Pythagorean triples x, y, z that satisfy $x^2 + y^2 = z^2$ is an example.

5. Computational number theory is the study of computations with numbers, developing algorithms to calculate things such as factorizations and the numbers of points on a curve.

2.2 Is number theory important?

Beyond its intellectual challenge, number theory has important applications in the theory of cryptography. The recent invention of public-system crytosystems ensuring the confidentiality of financial and other transactions in the public domain are usually based on the difficulty of a number theory computation, often involving very large primes, has stimulated research in number theory. For example, the RSA public key encryption algorithm comes out of modular arithmetic.

In addition, research into number theory underpins many results in abstract algebra. In more recent times, number theory has become important in quantum mechanics.

2.3 Is it all done?

By no means. There are a large number of unsolved problems in number theory. The two most famous are also regarded as two of the hardest four problems in all of mathematics. Again they are easy to state.

Twin Primes Conjecture: *Prove there are an infinite number of pairs of prime numbers* (p, q) *such that* $q - p = 2$.
For example, $(3,5), (5,7), (29,31), (191,193)$

Goldbach's Conjecture: *Prove that EVERY even number greater than 4 can be expressed as the sum of two prime numbers (in at least one, maybe more, ways).*
We start with $6 = 3 + 3,\ 8 = 5 + 3,\ 10 = 3 + 7 = 5 + 5,\ 12 = 5 + 7, \ldots$

Computers are very useful in testing conjectures in number theory. Goldbach's conjecture has been shown to be true for every even number up to 4×10^{14}. (But is it true for $4 \times 10^{14} + 2$?)

Here's another unsolved problem on perfect numbers. A perfect number is the sum of its smaller factors, e.g., $6 = 1 + 2 + 3,\ 28 = 1 + 2 + 4 + 7 + 14$
Prove or disprove: There are no perfect odd numbers.

Richard Guy has authored a 436 page Springer text titled "Unsolved problems in Number Theory"

2.4 Axioms of Integers

Number theory is predominantly the study of the integers. We must begin with a set of axioms. The axioms of the integers are those of the real numbers with the exception that the integers (other than 1) do not have a multiplicative inverse. For example, there is no integer n such that $7 \times n = 1$. (Of course $7 \times \frac{1}{7} = 1$ but $\frac{1}{7} \notin \mathbb{Z}$.)
Mathematicians call the real numbers a "field" and the subset of the integers with no multiplicative inverses, a "ring". Then they generalize! In every one of their abstract fields there is a ring of abstract integers.
We extend the operations of addition and multiplication to subtraction and division, squares and square roots and so on.
We need to add the accepted laws of equality, in naive words, that we can do whatever we like to one side of an equation as long as we do exactly the same thing to the other side (and do not contravene any other laws, such as division by zero).
The main set of axioms for the integers is:

1. Closure[1] of $\mathbb{Z}$ under addition and multiplication.
   For all $a, b \in \mathbb{Z}$, both $a + b$ and $a\dot{b}$ are in $\mathbb{Z}$.

   Example 2. $2, -5 \in \mathbb{Z}$ *and* $2 + (-5) = -3 \in \mathbb{Z}$; *and* $2 \times (-5) = -10 \in \mathbb{Z}$

2. Associativity of addition and multiplication.
   For all $a, b, c \in \mathbb{Z}$, the following equalities hold:
   $$a + (b + c) = (a + b) + c \text{ and } a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

   Example 3. $(5 + 6) - 6 = 5 + (6 - 6) = 5 + 0 = 5; \quad 5 \cdot (2 \cdot 6) = (5 \cdot 2) \cdot 6 = 60$

3. Commutativity of addition and multiplication.
   For all $a, b \in \mathbb{Z}$, the following equalities hold,
   $$a + b = b + a \text{ and } a \cdot b = b \cdot a,$$

   Example 4. $5 - 3 = -3 + 5 = 2; \quad 5 \cdot 4 = 4 \cdot 5 = 20$

4. Existence of additive and multiplicative identity elements.
   There exists an element of $\mathbb{Z}$ called the additive identity element, denoted by 0, such that for all a in $\mathbb{Z}$,
   $$a + 0 = a.$$

   Example 5. *3+0=3*

   Likewise, there is an element, called the multiplicative identity element and denoted by 1, such that for all $a \in \mathbb{Z}$,
   $$a \cdot 1 = a$$

   Example 6. $5 \cdot 1 = 5$.

5. Existence of additive inverses[2]:
   For every a in $\mathbb{Z}$, there exists an element $-a$ in $\mathbb{Z}$, such that,
   $$a + (-a) = 0.$$
   The expression $a + (-b)$ is denoted $a - b$.

   Example 7. $5 + (-5) = 5 - 5 = 0$.

6. Distributivity of multiplication over addition:
   For all $a, b, c \in \mathbb{Z}$, the following equality holds,
   $$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

   Example 8. $3(4 - 2) = 3 \cdot 4 - 3 \cdot 2 = 6$

[1] A set is closed under an operation on its elements if the result is still within the set.

[2] Note the integers do not have multiplicative inverses. Thus $7 \times \frac{1}{7} = 1$ but $\frac{1}{7} \notin \mathbb{Z}$

7. Every non-empty subset S of $\mathbb{Z}$ with an upper bound in $\mathbb{Z}$ has a least upper bound in $\mathbb{Z}$.

   Example 9. *The upper bounds of* $\{3, 5, 7, 12, 4, 6\}$ *are* $\{12, 13, 14, \ldots\}$ *. The least is* 12.

8. There is an order relation $\leq$ (less than or equal to) on $\mathbb{Z}$ which totally orders $\mathbb{Z}$, namely, for all $a, b, c \in \mathbb{Z}$:

   (a) $a \leq a$

   (b) $a \leq b$ and $b \leq a \Rightarrow a = b$

   (c) $a \leq b$ and $b \leq c \Rightarrow a \leq c$
   This order relation satisfies similar laws to those of equality:

   (d) $a \leq b \Rightarrow a + c \leq b + c$

   (e) $a \times c \leq b \times c \; if \; c \leq 0$

   (f) In addition, there is the notation $0 < 1$ where "<" means "$\leq$ *but not* $=$"

2.5 How is it done? Mathematical Proofs

One of the attractions of number theory to teachers is that it provides a wealth of simple proofs that illustrate how mathematicians do mathematics. The major methods of proof in mathematics are:

1. Direct

2. Indirect

   (a) Contradiction

   (b) Contrapositive

3. Mathematical induction

Let us note:

1. A theorem sentence is always able to be put in the form "if P then Q" or $P \Rightarrow Q$ where P and Q are statements.

2. The converse of a theorem is "If Q then P" or $Q \Rightarrow P$. In logic, it is easy to show that the truth of a theorem does not mean the converse is also true. If the theorem and the converse are both true then we write $P \Leftrightarrow Q$ and say P is true or false if and only if (iff) Q is respectively true of false. We also say P and Q are equivalent statements.

3. If we are required to prove an iff statement in a theorem, then we are required to prove two statements, $P \Rightarrow Q$ and $Q \Rightarrow P$.

4. A definition is always an iff sentence. For example, " A number is a prime if it is divisible only by itself or 1" is actually "A number is a prime if and only if (iff) it is divisible only by itself or 1", but we seldom use iff instead of if in definitions. We mostly reserve iff for a theorem where the converse is also true, for example,

"If the interior angles of a polygon add up to 180^0 *then the polygon is a triangle"*
can be written
"A polygon is a triangle iff its interior angles sum to 180^0*"*
since the converse is also true, namely,
"If the interior angles of a polygon add to 180^0 *then it is a triangle".*

2.5.1 Direct Proofs

A direct proof begins with an "if" statement and proceeds to prove a "then" statement. We begin an example of such proofs with a definition.

Definition 4. *odd and even integers*
An odd integer has the form $2k+1$ *where* $k = 0, \pm 1, \pm 2, \ldots$ *or* $k \in \mathbb{Z}$.
The odd integers are $\pm 1, \pm 2 \pm 3, \ldots$ *Positive odd integers when divided by 2 always leave a (least positive) remainder of 1.*
An even integer has the form $2k$ *where* $k = 0, \pm 1, \pm 2, \ldots$ *or* $k \in \mathbb{Z}$. *The even integers are* $0, \pm 2, \pm 4, \ldots$ *Consequently, positive even integers when divided by 2 always leave a remainder of 0, that is they have 2 as a factor.*

Theorem 2.
The product of two odd integers is odd. (sic: If x, y *are odd integers, then* xy *is an odd integer)*

Proof. Let x, y be any odd integers.
Then (by definition of an odd integer), $x = 2a+1, y = 2b+1$ where $a, b \in \mathbb{Z}$.
We need to show $xy = 2c+1, c \in \mathbb{Z}$. Now,

$$\begin{aligned}
xy &= (2a+1)(2b+1) \\
&= (2a+1)\times 2b + (2a+1)\times 1 \qquad \text{(distributive law)} \\
&= 2b(2a+1) + 2a + 1 \qquad \text{(commutative and identity laws)} \\
&= 4ab + 2b + 2a + 1 \qquad \text{(distributive and commutative laws)} \\
&= 2(2ab + b + a) + 1 \qquad \text{(associative and distributive law)} \\
&= 2c + 1, c \in \mathbb{Z} \qquad \text{(closure law)}
\end{aligned}$$

making xy an odd number. □

We will always indicate the end of a proof by a box, □

2.5.2 Proofs by Contradiction

Proofs by contradiction proceed by assuming a statement is true and then proving it is false, or vice versa. These proofs are based on the laws of logic, one of which is,

$$not(notP) = P,$$

where P is a statement or proposition. For example, we prove in Theorem 3 that $\sqrt{2}$ is irrational. We begin with a definition.

Definition 5. *greatest common divisor*
The greatest common divisor, $gcd(a,b)$ of two integers a,b is the greatest positive integer that divides both a and b.

Example 10. $gcd(5,25) = 5,\ gcd(13,17) = 1$

Theorem 3.
$\sqrt{2}$ is irrational, that is $\sqrt{2} \notin \mathbb{Q}$.

Proof. By the definition of rational numbers, $\mathbb{Q} = \left\{ \frac{a}{b} | a, b \in \mathbb{Z},\ b \neq 0 \right\}$, we need to show $\sqrt{2} \neq \frac{a}{b}$ so $\sqrt{2} \notin \mathbb{Q}$. We use the rules of logic where the contradiction law says that if we assume a statement is true and that leads to an impossible result, then the statement must have been false.
Accordingly, assume $\sqrt{2} = \frac{a}{b}, a, b \in \mathbb{Z}$ where $gcd(a,b) = 1$, that is, using cancellation, no number larger than 1 divides both a and b. Squaring, and using Theorem 1,

$$2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2 \Rightarrow a^2 \text{ is even} \Rightarrow a \text{ is even.}$$

(We do need to prove that if a^2 is an even integer, then a is an even integer. We will do that in Theorem 4.)
So we let $a = 2k, k \in \mathbb{Z}$. Then,

$$a^2 = 2b^2 \Rightarrow 4k^2 = 2b^2 \Rightarrow b^2 = 2k^2 \Rightarrow b \text{ is even.}$$

Then if a, b are both even, the $gcd(a,b)$ is at least 2.
This is a contradiction to $gcd(a,b) = 1$, so the assumption is not true and $\sqrt{2}$ is not rational or $\sqrt{2}$ is irrational. □

2.5.3 Contrapositive proofs

Contrapositive proofs are based on the proof in logic that the sentences $P \Rightarrow Q$ and *not* $Q \Rightarrow$ *not* P are logically equivalent. For example, the sentence,

$$"If\ it\ is\ raining\ then\ the\ ground\ is\ wet"$$

is logically equivalent to the sentence,

$$\text{"}If\ the\ ground\ is\ NOT\ wet,\ then\ it\ is\ NOT\ raining\text{"}.$$

An example of a contrapositive proof is the following theorem.

Theorem 4.
If a^2 is an even integer, then a is an even integer.

Proof. We shall prove that if a is not an even integer, then a^2 is not an even integer. In other words, we shall prove that if a is odd, then so is a^2.
Choose any $a \in \mathbb{Z}$ that is not an even integer, so it must be an odd integer. Then, by definition of an odd integer, $a = 2k + 1, k \in \mathbb{Z}$. Therefore,

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2m + 1, m = 2k^2 + 2k \in \mathbb{Z},$$

where we have used the distributive, commutative and closure laws.
So a^2 is an odd integer. We conclude if a^2 is even then so is a. □

(We could have simply used Theorem 2 on page 21 to prove a^2 is odd if a is odd,)

2.5.4 Mathematical Induction

The Principle of Mathematical Induction is as follows.
Let $S(1), S(2), \ldots, S(n), S(n + 1)$ be a series of $n + 1$ statements, one for each of the integers $1, 2, 3, \ldots, n, n + 1$. Suppose we can prove:

1. (Basis step) $S(1)$ is a true statement.
2. (Inductive step) If $S(n)$ is true, then $S(n + 1)$ is true.

Then we can conclude that $S(k)$ is a true statement for $1 \le k < \infty$.

Proof. The reason for this is as follows:
We proved $S(1)$ is true.
But if $S(1)$ is true, then $S(2)$ is true (put $n = 1$ in the inductive step).
But if $S(2)$ is true, then $S(3)$ is true (put $n = 2$ in the inductive step).
But if $S(3)$ is true, then $S(4)$ is true.
We can continue this chain indefinitely.
So $S(k)$ is true for $k = 1, 2, 3, \ldots$ or for $1 \le k < \infty$ or $\forall k \in \mathbb{N}$. □

For example, we have the following Theorem.

Theorem 5.
The sum of the first n positive integers is given by,

$$1 + 2 + 3 + \ldots + n = \frac{n(n + 1)}{2}$$

Proof. Let $S(n)$ be the statement that $1 + 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2}$.

Basis step: $S(1)$ is the statement that $1 = \dfrac{1(1+1)}{2}$, which is true since $1 = 1$.

Inductive step: Assume $S(n)$ that $1 + 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2}$ is true.

We need to show $S(n+1)$ that $1 + 2 + 3 + \ldots + n + n + 1 = \dfrac{(n+1)(n+2)}{2}$ is true.

$$\begin{aligned}
\mathit{Left\ side} &= \overbrace{1 + 2 + 3 + \ldots + n} + n + 1 \\
&= \frac{n(n+1)}{2} + n + 1 \qquad (S(n) \text{ is assumed to be true}) \\
&= \frac{n^2 + n + 2n + 2}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \mathit{Right\ side}
\end{aligned}$$

□

Example 11.

$$1 + 2 + 3 + \ldots + 100 = \frac{100 \times 101}{2} = 5050$$

An interesting historical note is that the 10 year old Carl Gauss stunned his teacher by calculating the sum of the first 100 numbers this way.

$$\begin{aligned}
S &= 1 + 2 + 3 + 4 + \ldots + 49 + 50 + 51 + 52 + \ldots + 99 \ \mathit{plus}\ 100 \\
\mathit{Reversing}, & \\
S &= 99 + 98 + \ldots + 50 + 51 + 52 + \ldots + 3 + 2 + 1 \ \mathit{plus}\ 100 \\
\mathit{Adding}, & \\
2S &= \overbrace{100 + 100 + \ldots + 100}^{99\ \mathit{times}} + 200 \\
&\Rightarrow 2S = 99 \times 100 + 200 = 10100 \\
&\Rightarrow S = 5050
\end{aligned}$$

The study of numbers using this technique is the area of sequences, whether:

(a) Arithmetic (when each number is the previous plus some other fixed number) For example: $2, 5, 8, 11, \ldots$ (add 5 each time)

(b) Geometric (where each number is the previous multiplied by some fixed number) For example: $2, 6, 18, 54, \ldots$ (multiply by 6 each time)

Later we will use the formula

$$S_n = a + (a + d) + (a + 2d) + \ldots (a + (n - 1)d) = \frac{n}{2}(2a + (n - 1)d)$$

for the sum of n terms of the finite arithmetic progression,

$$a + (a + d) + (a + 2d) + \ldots + (a + (n - 1)d)$$

and the formula

$$a + ar + ar^2 + \ldots + ar^{n-1} = \frac{a(r^n - 1)}{r - 1}$$

for the sum of terms of the finite geometric progression,

$$a + ar + ar^2 + \ldots + ar^{n-1}$$

If your college algebra did not include this, you can prove them easily. For the first, use Gauss's method, for the second, form $rS_n - S_n$.

Part II

A Pythagorean Feast - Pythagoras to Wiles

Let us now read some major results in number theory beginning with a long trail leading directly from Pythagoras to Fermat to Wiles. Later we will follow another trail beginning with Euclid that branched out into several different fields of number theory before being put to rest by Dirichlet.

First Pythagoras to Fermat to Wiles . It is an easy step from knowing equations of the form $x^2+y^2 = z^2$ have integer solutions such as $5^2+12^2 = 13^2$ to asking whether the same applies to $x^3 + y^3 = z^3$ and so on. Taking the step, however, took thousands of years. The amateur mathematician Pierre Fermat is generally regarded as the founder of modern number theory. Number theory itself had languished for centuries after the Greeks and other ancient civilizations waned. Fermat shared only one number theory proof with his peers, however, he challenged them with results he believed to be true. In the margin of a 1621 translation of Diophantus's c. 250 A.D. book "Arithmetica", he wrote a note, discovered after his death, that would torture mathematicians for almost 400 years:

No cube can be split into two cubes, nor any biquadrate into two biquadrates, nor generally any power beyond the second into two of the same kind.
I have discovered a truly remarkable proof for this, but the margin is too narrow to contain it.

Due to Fermat's importance, this was called Fermat's Last Theorem (FLT). In today's language, it is:

The equation $x^n + y^n = z^n,\ n \geq 3$ has no non-zero integer solutions.

Although it was for centuries an unproved conjecture, it is now a theorem, proved in the 1990's by Andrew Wiles, a Princeton professor of Mathematics. The proof is so complex that nearly every one doubts Fermat actually did have a proof, but maybe he did!

Chapter 3

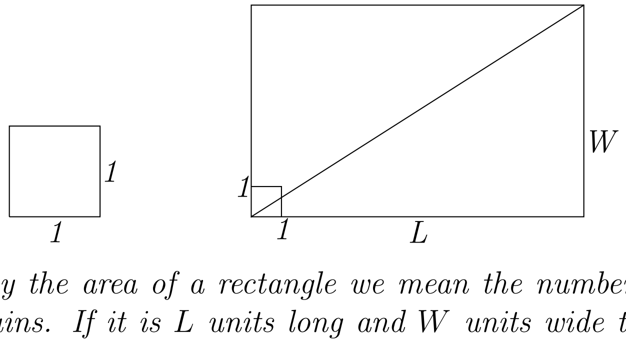
Pythagoras: The $n = 2$ case.

Let's investigate $x^2 + y^2 = z^2$.

Course: Appetizers
Ingredients
High school algebra
Area
4 congruent triangles
Greatest common divisor
Pythagorean triples
Directions
Assemble the triangles to prove the Pythagorean Theorem
Use high school algebra to find all Pythagorean triples

3.1 Area

Definition 6. - *area, area of a rectangle, area of a right triangle*
We define the area of a square of side 1 unit to be 1 square unit.



By the area of a rectangle we mean the number of squares of side 1 unit that it contains. If it is L units long and W units wide then it contains L × W squares of side 1 unit, so its area is,

$$\textit{Area of rectangle} = L \times W$$

If a diagonal is drawn from one vertex of the square to the opposite vertex, then we have a right triangle of base L and height W which is obviously half the area of the rectangle, so the area of a right triangle is.

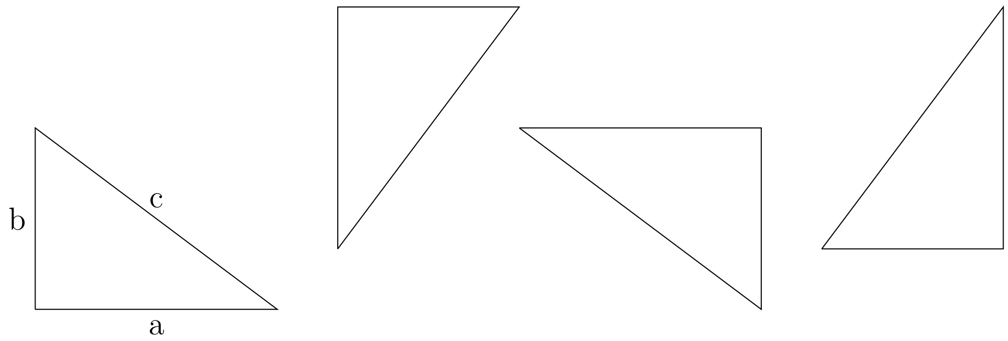
$$Area\ of\ right\ triangle = \frac{1}{2}\ L \times W$$

3.2 Pythagoras

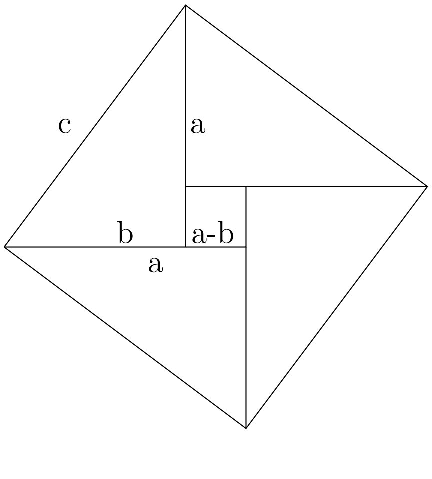
And now for the Greeks' famous theorem.

Theorem 6. *(Pythagorean Theorem)*
In a right triangle, the sum of the squares of the lengths of the two sides forming the right angle is equal to the square of the length of the side opposite the right angle (the hypotenuse).

Proof. We start with four copies of the same right triangle or four congruent triangles. We want to show $a^2 + b^2 = c^2$.



The area of each triangle is $\frac{ab}{2}$ making their combined area $2ab$. We place the four triangles together as shown.



The inner square has sides of length[1] $a - b$ making its area $(a - b)^2$.
The outer square has area c^2. It contains the four triangles and the smaller square, so,

$$(a-b)^2 + 2ab = c^2 \Rightarrow a^2 - 2ab + b^2 + 2ab = c^2 \Rightarrow a^2 + b^2 = c^2$$

□

There are 96 different proofs of the Pythagorean theorem at the web-site http://www.cut-the-knot.org/pythagoras/index.shtml. One is due to a U.S. President!

3.2.1 Irrational Numbers

Of immediate interest is that a right triangle can be drawn with the sides containing the right angle equal to 1. What then is the length of the hypotenuse? What is the number c such that $c^2 = 1^2 + 1^2 = 2$? We have already proved it is not a rational number. And, of course, it is the first of an infinite number of what we call irrational numbers. The Greeks pondered this long and hard.

3.2.2 Pythagorean Triples

We now want to find a formula that generates Pythagorean triples, that is, numbers a, b, c such that $a^2 + b^2 = c^2$.. Here are two lemmas we will use often in what follows.

Lemma 7.
Let $a, b \in \mathbb{Z}$. If $gcd(a, b) = d$ then d^n divides $a^n x + b^n y$ for all $n \in \mathbb{N}$ and for all $x, y \in \mathbb{Z}$.

Proof. $gcd(a, b) = d \Rightarrow d|a$ *and* $d|b$, in other words $a = dj, b = dk$ for some $j, k \in \mathbb{Z}$. Then,

$$a^n x + b^n y = (dj)^n + (dk)^n y = d^n j^n x + d^n k^n y = d^n(j^n x + k^n y)$$

so that $d^n | a^n x + b^n y$. □

Lemma 8.
Let $a, b, c, d \in \mathbb{Z}$. Consider the equation $a + b = c$. If $d|a$ and $d|b$ then $d|c$.

Proof. Let $a = dj$ and $b = dk$ as in the previous lemma. Then,

$$a + b = dj + dk = d(j + k) \Rightarrow d|a + b \Rightarrow d|c.$$

□

We want to generate Pythagorean Triples.

[1] It makes no difference whether $a > b$ or $a < b$ since $(a - b)^2 = (b - a)^2$.

Definition 7. *Pythagorean triples*
If the integers x, y, z satisfy $x^2 + y^2 = z^2$ we call x, y, z a Pythagorean triple.

It is trivial to observe that there are an infinite number of Pythagorean triples. Obviously, given $(3, 4, 5)$ is one, then so are $(3d, 4d, 5d)$ for all $d \in \mathbb{Z}$ since,

$$3^2 + 4^2 = 5^2 \Rightarrow d^2(3^2 + 4^2) = d^2 5^2 \Rightarrow (3d)^2 + (4d)^2 = (5d)^2$$

Example 12. *Give* $3^2 + 4^2 = 5^2$ *then* $6^2 + 8^2 = 10^2,\ 36^2 + 48^2 = 60^2$

We want to generate what are called primitive Pythagorean triples.

Definition 8. *primitive Pythagorean triples*
If x, y, z are all mutually prime or co-prime, meaning $gcd(x, y) = gcd(x, z) = gcd(y, z) = 1$, we say (x, y, z) is a primitive Pythagorean triple.

Example 13. $5^2 + 12^2 = 13^2,\ 391^2 + 120^2 = 409^2$.

The important question is whether there are an infinite number of primitive Pythagorean triples. In particular, is there a formula which generates an infinite number? Better still, is there a formula that generates every primitive Pythagorean triple?

The Pythagorean School (c. 570 B.C.) was not the first group to investigate right triangles with integer solutions. The integer solutions to $x^2 + y^2 = z^2$ are duly called Pythagorean triples, but there is a solution (4961, 6480, 8161) on a Babylonian tablet from the 2000 B.C. to 1600 B.C. period.
It is acknowledged, however, that Pythagoras was the first to find a formula for primitive Pythagorean triples. His formula was,

$$x = k, y = \frac{k^2 - 1}{2}, z = \frac{k^2 + 1}{2},\ \ k \in \mathbb{Z}$$

which follows from the algebra:

$$x^2 + y^2 = k^2 + \frac{(k^2 - 1)^2}{4} = \frac{4k^2 + k^4 - 2k^2 + 1}{4} = \frac{k^4 + 2k^2 + 1}{4} = \frac{(k^2 + 1)^2}{2^2} = z^2$$

But, this formula does not generate all Pythagorean triples (for example, (20,21,29)). Neither does that due to Plato (c. 380 B.C.), namely $(x, y, z) = (2k, k^2 - 1, k^2 + 1)$.
Let us find this elusive formula.
By requiring primitive solutions we have eliminated the possibility that both x and y are even since $gcd(x, y) = 1$. We now also eliminate the possibility that both x and y are odd.
We earlier stated all odd numbers are of the form $2k + 1, k \in \mathbb{Z}$. We can extend this to the division of odd numbers by 4. The possible remainders are 0,1,2,3 so the odd numbers will be $4k + 1$ or $4k + 3$. Since,

$$4j + 3 = 4(j + 1) - 1 = 4k - 1$$

we can also say all odd numbers are of the form $4k \pm 1$.

Theorem 9.
If $x, y, z)$ is a primitive Pythagorean triple then x and y cannot both be odd.

Proof. We use a proof by contradiction. Suppose x and y are both odd. Then, by Theorem 2, page 21, x^2 and y^2 are both odd so that their sum z^2 is even and therefore by Theorem 4, page 23, z is even.
Then, since we supposed both x and z are odd, they are of the form $4k + 1$ or $4k - 1$. Then,

$$\begin{aligned} x^2 + y^2 &= (4k \pm 1)^2 + (4j \pm 1)^2) \\ &= 16k^2 \pm 8k + 1 + 16j^2 \pm 8j + 1 \\ &= 4(4k^2 \pm 2k + 4j^2 \pm 2j) + 2 \\ &= 4m + 2, \ m = 4k^2 \pm 2k + 4j^2 \pm 2j \in \mathbb{Z} \end{aligned}$$

But if z is even, then either $z = 4k \Rightarrow z^2 = 4(4k^2)$, or $z = 4k + 2 \Rightarrow z^2 = 4(4k^2 + 4k + 1)$ and in neither case can $z^2 = 4m + 2$.
This contradiction proves x, y cannot both be odd. □

Without loss of generality we can therefore always suppose y is even.

Theorem 10. *(The $n = 2$ case)*
A Pythagorean triple (x, y, z) satisfying $x^2 + y^2 = z^2$, with y even, is primitive iff it is of the form

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$

where m, n are positive integers of opposite parity (one odd, one even) with $m > n$ and $gcd(m, n) = 1$.

Proof. We first prove,
If $x = m^2 - n^2, y = 2mn, z = m^2 + n^2$ with $gcd(m, n) = 1$, then (x, y, z) is a primitive Pythagorean triple.
It is a triple since,

$$\begin{aligned} x^2 + y^2 &= (m^2 - n^2)^2 + (2mn)^2 \\ &= m^4 - 2m^2n^2 + n^4 + 4m^2n^2 \\ &= (m^2 + n^2)^2 \\ &= z^2 \end{aligned}$$

To show it is a primitive triple, suppose not, that is $p|x, p|y$ and $p|z$ for some prime p. First we note,

$$z + x = 2m^2 \textit{ and } z - x = 2n^2$$

So, by Lemma 8, page 30, if $p|x$ and $p|z$ then $p|2m^2$ and also $p|2n^2$.
Since p is odd then $p|m^2$ and also $p|n^2$. Now[2] if a prime p divides a square such as m^2 then it must divide m. So $p|m$ and $p|n$ making $gcd(m,n) \geq p$.
This is a contradiction to $gcd(m,n) = 1$.
Then our supposition is not correct and (x,y,z) is a primitive triple.

*****

We next prove the converse that *if* (x,y,z) *is a primitive Pythagorean triple, that is, if,*

$$x^2 + y^2 = z^2, gcd(x,y) = gcd(x,z) = gcd(y,z) = 1,$$

then,

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2,\ m,n \in \mathbb{Z},\ gcd(m,n) = 1$$

Since y is even and (x,y,z) are mutually prime then x is odd and z is odd. Therefore $z+x$ and $z-x$ are both even, say $z+x = 2r$ and $z-x = 2s$. So we let,

$$r = \frac{z+x}{2},\ s = \frac{z-x}{2}$$

where we must therefore have $r,s \in \mathbb{Z}$.
Adding we get $r+s = z$ and subtracting we get $r-s = x$.
Since $z = r+s,\ x = r-s$, by Lemma 8, page 30, any common divisor of r and s must also divide x and z.
But $gcd(x,z) = 1$ and therefore $gcd(r,s) = 1$.
The reason for this is if $gcd(r,s) = q$ and $q \neq 1$, then let $r = aq,\ s = bq$ and then $x = r - s = q(a-b),\ z = r+s = q(a+b)$ so that $gcd(x,z) \geq q$ which contradicts $gcd(x,z) = 1$.
Also, since,

$$y^2 = z^2 - x^2 = (z+x)(z-x) = (2r)(2s),$$

then $\left(\frac{y}{2}\right)^2 = rs$ with y even so that $\frac{y}{2} \in \mathbb{Z}$.

But r and s have no common factors, so if their product is a perfect square then each of r and s must be a perfect square[3].

[2] Suppose $p|m^2$. Let the complete prime factorization (where the primes may not be distinct) of m be $m = p_1p_2\cdots p_n$. Then $m^2 = p_1^2p_2^2\cdots p_n^2$. So if $p|m^2$ then $p|p_i^2$ for some $i : 1 \leq i \leq n$. Since both p and p_i are primes this is only possible if $p = p_i$. Therefore $p|m$.

[3] Let us prove that if rs is a perfect square then each of r and s must be a perfect square. Suppose $rs = m^2$. We can write the prime decomposition of m as $m = p_1p_2\cdots p_n$ so that,

$$rs = (p_1p_2\cdots p_n)^2 = p_1^2p_2^2\cdots p_n^2$$

Now each p_i^2 can only be in the prime decomposition of either r or s since if, for instance, $r = p_iq$ and $s = p_it$ then $gcd(r,s) \geq p_i$ and is not 1. So the p_i^2's are distributed across the prime decompositions of r and s giving, say,

$$r = p_1^2p_2^2\cdots p_j^2 \ and\ s = p_{j+1}^2p_{j+2}^2\cdots p_n^2$$

and obviously each of r and s is a perfect square.

The reason for this is that if any prime p divides $\left(\frac{y}{2}\right)^2$ then p^2 must divide $\left(\frac{y}{2}\right)^2$ and therefore $p^2|rs$. Since $gcd(r,s) = 1$ then this p^2 must divide only one of r or s. Consequently both r and s must be products of the squares of the primes that divide $\left(\frac{y}{2}\right)^2$ making each a perfect square.
If we therefore put $r = m^2$ and $s = n^2$ then $gcd(m,n) = 1$ and

$$x = r - s = m^2 - n^2,\ y = \sqrt{4rs} = 2mn,\ z = r + s = m^2 + n^2$$

□

It is therefore easy for us to generate large Pythagorean triples. For example, if $m = 103, n = 64$ then $(6513, 13184, 14708)$ is a primitive Pythagorean triple. Maybe this is how the Babylonians found (4961, 6480, 8161) using $m = 81, n = 40$.

Chapter 4

The $n = 4$ case

We want to prove $x^4 + y^4 = z^4$ has no non-zero solutions in the integers.

Course: *Entrée*
Ingredients
Fermat's method of infinite descent
Formula for Pythagorean triples
Directions
The proof is by contradiction using infinite descent. We consider $x^4 + y^4 = z^2$ rather than $x^4 + y^4 = (z^2)^2$ since if there are no solutions to the first then there cannot be solutions to the second. If $x^4 + y^4 = z^2$ has integer solutions, then, of all the solutions, one has the smallest value of z, or z is minimal. Assume this and, using the formula for Pythagorean triples, produce another solution with a smaller value of z, providing the contradiction.
The algebra of this proof is very simple, the challenge lies in the ability to follow a logical argument. Much of mathematics is like this, some say "It's just logic!"

The only proof of a theorem the secretive Fermat shared with his peers is the following proof of the $n = 4$ case which is a special case of FLT. The proof uses his "method of infinite descent".

4.1 Method of Infinite Descent

Fermat's method of infinite descent states that the natural numbers are well-ordered and there are only a finite number of them of any given structure that are smaller than any given one.
Assuming an example with a particular property exists, one shows that another exists that is in some sense 'smaller'as measured by a natural number. Then by mathematical induction (infinitely repeating the same step), one shows there is a yet smaller example, then a yet even smaller example, and hence there must be an infinitude of ever smaller examples. Since there are only a finite number of natural numbers

smaller than the size of the initially postulated example, (for example there are only 999 natural numbers less than 1000), this is impossible – it is a contradiction, so no such initial example can exist.
A more common type of proof formulation is that we suppose a 'smallest'solution and then derive a smaller one – thereby getting a contradiction.

4.2 Proof of the $n = 4$ case

Theorem 11. *(Fermat)*
The equation $x^4 + y^4 = z^4$ has no non-zero integer solutions.

Proof. The proof is by contradiction using infinite descent. We use $x^4 + y^4 = z^2$ rather than z^4.
If $x^4 + y^4 = z^2$ has integer solutions, then, of all the solutions, one has the smallest value of z, or z is minimal. We will assume this and produce another solution with a smaller value of z, providing the contradiction.

Suppose (x, y, z) is the solution of $x^4 + y^4 = z^2$ with z minimal.
Either x, y have a common prime factor $p > 1$ or not.

*****

Case A: Suppose x, y have a common prime factor $p > 1$,
Now $p|x \Rightarrow x = pj$ and $p|y \Rightarrow y = pk$ where $j, k \in \mathbb{Z}$. Then,

$$x^4 + y^4 = p^4 j^4 + p^4 k^4 = p^4(j^4 + k^4) \Rightarrow p^4 | x^4 + y^4$$

So $p^4|z^2$ or $z^2 = mp^4, m \in \mathbb{Z}$. This is only possible in whole numbers if $m = l^2$ or m is a square[1].
Then, $z^2 = l^2 p^4 \Rightarrow z = lp^2$ means $l < z$ but also $p^2|z$.
Therefore, substituting into $x^4 + y^4 = z^2$, we obtain,

$$(jp)^4 + (kp)^4 = (lp^2)^2 \Rightarrow j^4 + k^4 = l^2$$

We have produced a smaller value l less than z satisfying an equation of the form $x^4 + y^4 = z^2$ which is a contradiction, so there are no integer solutions to $x^4 + y^4 = z^2$.

*****

[1] This is easily proved by using the fact that any integer ≥ 2 can be factored into the product of prime numbers, (specifically this is the Fundamental Theorem of Arithmetic we will prove later). Let's prove $z^2 = mp^4$ is only possible if m is a perfect sqaure. Let $z = p_1 p_2 \cdots p_n$ so that $z^2 = p_1^2 p_2^2 \cdots p_n^2$. So we have $mp^4 = p_1^2 p_2^2 \cdots p_n^2$. Then we must have something like $p^2 = p_1^2$ and $p^2 = p_2^2$ to enable cancellation. But that leaves $m = p_3^2 p_4^2 \cdots p_n^2$. So m is a perfect square.

Case B: The other possibility is that x, y have no common prime factor.
Now since we have supposed $(x^2)^2 + (y^2)^2 = z^2$ then x^2, y^2, z is a Pythagorean triple.
Then, by Theorem 9, page 32, x^2 and y^2 are of opposite parity (one odd, one even) and we may assume x^2 is odd and y^2 is even.
Then, by Theorem 10, page 32, there are integers m, n with $m > n, gcd(m, n) = 1$ such that,

$$x^2 = m^2 - n^2, y^2 = 2mn, z = m^2 + n^2$$

But, again by Theorem 10, $x^2 + n^2 = m^2$ means there are integers $r, s, gcd(r, s) = 1$ such that,

$$x^2 = r^2 - s^2, n = 2rs, m = r^2 + s^2$$

Since $y^2 = 2mn = 4mrs$ and m, r, s have no common factors, then they must all be perfect squares, making (say),

$$r = a^2, s = b^2, m = c^2, a, b, c \in \mathbb{Z}$$

Since $m = r^2 + s^2$ then, substituting into $x^2 = r^2 - s^2$, we obtain,

$$a^4 + b^4 = c^2$$

But $c^2 = m \Rightarrow c = \sqrt{m} < m$ and $z^2 = m^2 + n^2 \Rightarrow m < z$ so we have $c < z$ contradicting the minimality of z for equations of this form, and again there are no integer solutions to $x^4 + y^4 = z^2$. □

Corollary 12.
The equation $x^4 + y^4 = z^4$ has no integer solutions.

Proof. $x^4 + y^4 = z^4 \Leftrightarrow x^4 + y^4 = (z^2)^2 \Leftrightarrow x^4 + y^4 = u^2$ which has no integer solutions. □

4.3 Comments on the General Case

It is now not necessary to prove cases of $x^n + y^n = z^n,\ n \geq 3$ other than n an odd prime.
The reason for this is that for any $n \geq 3$ either $n = 4k, k \in \mathbb{N}$ or $n = kp$ where p is some odd prime. The case,

$$x^{4k} + y^{4k} = x^{4k} \Leftrightarrow (x^k)^4 + (y^k)^4 = (z^k)^4$$

has been eliminated in the previous Corollary. The cases

$$x^{kp} + y^{kp} = z^{kp} \Leftrightarrow (x^k)^p + (y^k)^p = (z^k)^p,$$

p an odd prime, are all covered by proving $x^p + y^p = z^p$ has no integer solutions for any odd prime p.

Chapter 5

Euler: The $n = 3$ Case by Elementary Methods

We prove $x^3 + y^3 = z^3$ has no non-zero integer solutions.

Course: *Main Course Choice 1*
Ingredients
Well Ordering Principle
High school algebra
Method of infinite descent
Directions
Prove a classic chain of theorems about integers, namely, Division Algorithm, Euclidean Algorithm for finding gcd(m, n)*, Solutions of Linear Diophantine Equations, Euclid's Lemma on Primes, Fundamental Theorem of Arithmetic.*
Use this chain of theorems and high school algebra to read Euler's elementary proof of the $n = 3$ *case. This proof depends upon 5 lemmas regarding the particular characteristics of* $a^2 + 3b^2$*, in particular its possible factors.*
Proceed to prove $x^3 + y^3 + (-z)^3 = 0$ *has no integer factors by supposing it does. The supposition leads to a factor of* $(-z)^3$ *of the form* $a^2 + 3b^2$*, and then, via the 5 lemmas, to an infinite number of factors of this form. By the method of infinite descent, this is not possible, so the supposition is incorrect.*

We will now prove the case $n = 3$. It is considerably more difficult to prove than the $n = 4$ case, nevertheless, the elementary proof requires no more than high school algebra. We will prove it using elementary techniques and then, in the next chapter, using complex number techniques.
For the elementary proofs we need the following results on divisibility and factorizations of integers and a principle or axiom applying to the natural numbers.

5.1 Well-ordering principle

The well-ordering principle is that every non-empty set of the positive integers contains a smallest element.

Example 14. *The set* $\{56, 31, 84, 5, 92\}$ *has a smallest element of* 5.

5.2 Divisibility and Factorization of Integers

The following theorem simply says we can divide any integer by any positive integer and obtain a remainder less than the divisor, e.g., $77 \div 8 = 9$ with a remainder of 5 which is less than 8.

Theorem 13. *(Division algorithm)*
For every $a, b \in \mathbb{Z}$ *there exist a unique pair* $q, r \in \mathbb{Z}$ *such that,*

$$a = bq + r, \;\; 0 \le r < b.$$

Proof. Let S be the set of positive integers that are greater than a/b. By the Well-Ordering principle S contains a smallest element t, that is, we can construct the inequality,

$$t - 1 \le \frac{a}{b} < t.$$

Let $q = t - 1 \Leftrightarrow t = q + 1$, multiply through by b and subtract qb from all the terms. Then,

$$q \le \frac{a}{b} < q + 1 \Rightarrow qb \le a < (q+1)b \Rightarrow 0 \le a - qb < b$$

Putting $r = a - qb$ gives us the desired result $a = qb + r$.
Then, substituting this result into $0 \le a - qb < b$ we also obtain $0 \le r < b$. □

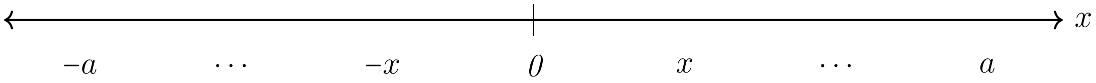
Example 15. $67, 12 \in \mathbb{Z}$ *and* $67 = 12 \cdot 5 + 7$ *where* $7 < 12$.

Definition 9. *absolute value*
By $|x|$ *we mean the absolute value of* x *defined by,*

$$|x| = \begin{cases} x & \textit{if } x \ge 0 \\ -x & \textit{if } \; x < 0 \end{cases}$$

Example 16. $|6| = 6, \;\; |-6| = 6$

Note 2. *It follows from the definition that* $|x| \le a \Leftrightarrow -a \le x \le a$. *The easiest way to see this is to realize that on the number line* $|x|$ *is simply the distance to the origin* 0 *from either* x *or* $-x$ *so if the distance is less than* a *then* x *lies between* a *and* $-a$.



Corollary 14.
Let a, b be integers with a positive. Then there exist unique integers q, r such that,

$$a = qb + r,\ |r| \leq \frac{b}{2}$$

Proof. By the theorem we have $a = qb + r,\ 0 \leq r < b$. There are two possibilities for r.
Case A: $r < \frac{b}{2}$ and we are done.
Case B: $\frac{b}{2} \leq r < b$.
Adding and subtracting b in $a = qb + r,\ 0 \leq r < b$ we have,

$$a = qb + b + r - b = b(q+1) + r - b \Rightarrow a = b(q+1) + s,\ s = r - b$$

Thus $s < 0$ since $r < b$ and $s = r - b \geq \frac{b}{2} - b \Rightarrow s \geq -\frac{b}{2}$.
Thus we have $-\frac{b}{2} \leq s < 0$ making[1] $|s| \leq \frac{b}{2}$ giving,

$$a = b(q+1) + s,\ |s| \leq \frac{b}{2}$$

□

Example 17.

$$66 = 9 \times 7 + 3,\ 3 < \frac{7}{2}$$
$$67 = 9 \times 7 + 4 = 10 \times 7 - 3,\ |-3| < \frac{7}{2} \qquad \diamond$$

Note we will always indicate the end of an example of more than one line with a ⋄
We now consider two definitions, the first of which we have already met.

Definition 10. *greatest common divisor*
Given two integers a, b the greatest common divisor, $gcd(a, b)$, is the greatest positive integer that divides both a and b.
If $gcd(a, b) = 1$ we say a, b are co-prime.

Example 18. *gcd(36,99)=9; gcd(5,7)=1*

Note 3. *If $gcd(a, b) = d$ we can write $a = jd, b = kd$ where $j, k \in \mathbb{Z}$ and $d \nmid j$ and $d \nmid k$. We will use this many times.*

[1] see Note 2 above.

Definition 11. *linear combination*
Given two integers a, b there are an infinite number of linear combinations of them of the form $ax + by$ where $x, y \in \mathbb{Z}$.

Example 19. *3a-5b is a linear combination of a, b.*

Theorem 15.

(a) Let a and b be integers and $d = gcd(a, b)$. Then d is the smallest positive integer that can be expressed as a linear combination of a and b, that is $d = ax + by$.

(b) There exist integers x, y satisfying $ax + by = c$ if and only if $d|c$ where $d = gcd(a, b)$.

Proof.
(a) Let a and b be integers and $d = gcd(a, b)$. By the Well Ordering principle[2], the set of all linear combinations of a and b contains a smallest positive element m, say $m = sa + tb$.
We want to prove $m = gcd(a, b) = d$.
By the Division Algorithm, Theorem 13 on page 39, we can write,

$$a = qm + r, \;\; 0 \le r < m. \tag{5.2.1}$$

Then, using $m = sa + tb$,

$$r = a - qm = a - q(sa + tb) = (1 - qs)a + (-tq)b,$$

so r is a linear combination of a and b.
But by (5.2.1) $0 \le r < m$ and we supposed m is the smallest positive element of the set of all possible linear combinations of a and b. This contradiction gives us $r = 0$ and $a = qm$ or $m|a$.
By a similar argument applied to $b = qm + r, \;\; 0 \le r < m$ we obtain $m|b$.
Then m is a common divisor of a and b.
Now since $d|a$ and $d|b$ then[3] $d|(sa + tb)$ so that $d|m$ making $d \le m$.
Since d is the greatest common divisor, we cannot have $d < m$ so we must have $d = m$ which proves (a), namely $d = gcd(a, b)$ is the smallest positive integer that can be expressed as a linear combination $ax + by$.

****

(b) We want to prove there exist integers x, y satisfying $ax + by = c$ iff $d|c$ where $d = gcd(a, b)$.
First assume $ax + by = c$ holds. We want to prove $d|c$.
For $d = gcd(a, b)$, let $a = ed, b = fd$. Then,

$$c = ax + by = edx + fdy = d(ex + fy) \Rightarrow d|c.$$

[2] Recall, the Well Ordering Principle states that every non-empty set of natural numbers contains a smallest element.

[3] If $a = dx, b = dy$ then $sa + tb = sdx + tdy = d(sx + ty) \Rightarrow d|(sa + tb)$.

*****

Conversely, assume $d|c$, say $kd = c$. We want to prove there exist integers x, y satisfying $ax + by = c$.
Now by Part (a), there exist x', y' such that $ax' + by' = d$. Hence, multiplying by k,

$$a(x'k) + b(y'k) = dk = c$$

In other words, $x = x'k$ and $y = y'k$ are a solution of $ax + by = c$.
This proves Part (b). □

Corollary 16.
There exist integers x, y satisfying $ax + by = 1$ iff $gcd(x, y) = 1$.

Proof. Put $c = 1$ in Theorem 15(b). □

Example 20. *For example, given $gcd(7, 11) = 1$, we can construct, as we do below,*

$$7 \times 8 - 11 \times 5 = 1. \qquad \diamond$$

Lemma 17. *(Euclid's Lemma for Integers)*
If p is a prime and $a, b \in \mathbb{Z}$, then if $p|ab$ either $p|a$ or $p|b$.

Proof. Suppose $p|ab$, p a prime and $a, b \in \mathbb{Z}$.
Now if p is a prime then either $p|a$ (and we are done) or $p\nmid a$ making $gcd(p, a) = 1$.
In this latter case, by Corollary 16, page 42 if $gcd(p, a) = 1$ then there exist integers r, s such that,

$$rp + sa = 1 \Rightarrow brp + sab = b \text{ where we multiplied through by } b.$$

Then since $p|ab$ means $ab = pk$ for some $k \in \mathbb{Z}$, we have,

$$brp + spk = b \Rightarrow b = p(br + sk) \Rightarrow p|b.$$

□

Example 21. $3|48 = 6 \times 8$ *and* $3|6$

We can go further.

Corollary 18.
In general, if $p|a_1a_2 \dots a_r$ then $p|a_i$ for at least one a_i, $1 \le i \le r$.

Proof. If $p\nmid a_1$, then $p|a_2a_3 \dots a_r$. Then if $p\nmid a_2$ then $p|a_3a_4 \dots a_r$ and so on. Thus if $p\nmid a_i$, $1 \le i \le r - 1$ then we must have $p|a_r$. □

The fundamental theorem of arithmetic is that each integer is able to be factored into the product of primes in a unique way up to order (that is, apart from the order, for example, $12 = 2^2 \times 3 = 3 \times 2^2$).

Theorem 19. *(Fundamental Theorem of Arithmetic)*
Every integer $n > 1$ is a product of a unique set of primes. That is,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

where each p_i is a prime and all $\alpha_i \in \mathbb{N}$.

Proof. To show n is a product of primes, we use a proof by contradiction.
Suppose there is an integer greater than 1 that is not the product of primes.
Then, by the Well-Ordering principle, there must be a smallest one, say m.
Either m is a prime and we are done, or m is not a prime.
In that case, m factors as say, $m = rs$. Since both r and s are smaller than m, they must be the product of primes, and therefore m is also, so we have a contradiction.
We conclude there are no integers greater than 1 that are not a product of primes.

*****

To show n is a product of a unique set of primes, we suppose there are integers greater than 1 with two different factorizations. To find a contradiction, let n be the smallest of these and let two factorizations of n be,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \dots q_s^{\beta_s} \tag{5.2.2}$$

where the p_i are distinct primes and the q_j are distinct primes and the exponents[4] $\alpha_i, \beta_j \in \mathbb{N}$.
Since p_1 divides the right side, then by Corollary 18, page 42, p_1 divides $q_j^{\beta_j}$ for some j.
Hence $p_1 = q_j$ since both are prime. Thus we may divide (5.2.2) by p_1 to get two different factorizations of $\dfrac{n}{p_1}$.
But $\dfrac{n}{p_1} < n$, so we have a contradiction since we supposed n is the smallest integer with two different factorizations.
We conclude any integer has a unique factorization into primes. □

Example 22. $720 = 2^4 3^2 5$

5.3 Euler's Proof of the $n = 3$ case

5.3.1 The Lemmas

We are now prepared to read Euler's elementary proof of the $n = 3$ case. This proof depends upon particular characteristics of $a^2 + 3b^2$, $a, b \in \mathbb{Z}$, in particular its possible factors.

[4] α=alpha, β = beta

(i) If we multiply two expressions of the form $a^2 + 3b^2$ we get another expression of the same form (a square plus three times a square)

Example 23.

$$2^2 + 3 \times 3^3 = 31$$
$$1^2 + 3 \times 2^2 = 13$$
$$13 \times 31 = 403 = 16^2 + 3 \times 7^2$$

(ii) If $2|a^2 + 3b^2$ then also $4|a^2 + 3b^2$

Example 24. $3^2 + 3 \times 1^2 = 12 = 2 \times 6 = 4 \times 3$

(iii) If a prime of the form $p^2 + 3q^2$ divides $a^2 + 3b^2$ then the quotient $\frac{a^2 + 3b^2}{p^2 + 3q^2}$ is also of this form.

Example 25. $13 = 1^2 + 3 \times 2^2$ *is a prime and* 13 *divides* $403 = 16^2 + 3 \times 7^2$, *specifically* $\frac{403}{13} = 31 = 2^2 + 3 \times 3^2$

(iv) If a^2+3b^2 has an odd factor f which is not of this form, then so does the quotient obtained by dividing $a^2 + 3b^2$ by f.

Example 26. $1452 = 33^2 + 3 \times 11^2$ *and* $\frac{1452}{11} = 132 = 11 \times 13$ *and* 11 *is not of this form.*

(v) If $gcd(a, b) = 1$, then every odd factor of $a^2 + 3b^2$ is also of this form.

Example 27. $183 = 3 \times 61$ *and* $3 = 0^2 + 3 \times 1^2$ *while* $61 = 7^2 + 3 \times 2^2$.
Actually, with a little bit of thought we realize any example for (iii) requires $gcd(a, b) \neq 1$ *and* $gcd(a, b)$ *to be not of this form.*

We proceed to prove $x^3 + y^3 + (-z)^3 = 0$ has no integer factors by supposing it does. The supposition leads to a factor of the form a^2+3b^2 and then, via the above lemmas, to an infinite number of factors of this form. By the method of infinite descent this is not possible, so our supposition is incorrect.
We first prove the lemmas stated above.

Lemma 20.
If we multiply two polynomials of the form $a^2 + 3b^2$ then we get a polynomial of the same form (a square plus three times a square).

Proof.

$$\begin{aligned}(a^2+3b^2)(c^2+3d^2) &= a^2c^2+3a^2d^2+3b^2c^2+9b^2d^2\\ &= (a^2c^2-6abcd+9b^2d^2)+(3a^2d^2+6abcd+3b^2c^2)\\ &\quad \text{(where we added and subtracted } 6abcd)\\ &= (a^2c^2-6abcd+9b^2d^2)+3(a^2d^2+2abcd+b^2c^2)\\ &= (ac-3bd)^2+3(ad+bc)^2\end{aligned}$$

□

Lemma 21.
If $2|a^2+3b^2$ then $4|a^2+3b^2$ and $\frac{a^2+3b^2}{4}=c^2+3d^2$ for some c,d.

Proof.
We can have $a=2m$ or $a=2m+1$ and $b=2n$ or $b=2n+1$.
Case 1: $a=2m, b=2n$ gives,

$$a^2+3b^2=4m^2+3\times 4n^2=4(m^2+3n^2)$$

In this case, a^2+3b^2 is even and is divisible by 4 and,

$$\frac{a^2+3b^2}{4}=c^2+3d^2, c=m, d=n,$$

Case 2: $a=2m+1, b=2n$ gives,

$$a^2+3b^2=4m^2+4m+1+3\times 4n^2=4(m^2+m+3n^2)+1$$

In this case, a^2+3b^2 is odd so the Lemma statement $2|a^2+b^2$ excludes this case.
Case 3: $a=2m, b=2n+1$ gives,

$$a^2+3b^2=4m^2+3\times(4n^2+4n+1)=4(m^2+3n^2+3n)+3$$

In this case, a^2+3b^2 is also odd so again the Lemma statement excludes this case.
Case 4: $a=2m+1, b=2n+1$ gives,

$$a^2+3b^2=4m^2+4m+1+3(4n^2+4n+1)=4(m^2+m+3n^2+3n+1)$$

In this case, a^2+3b^2 is even and is divisible by 4.
We still need to prove that in this case $\frac{a^2+3b^2}{4}=c^2+3d^2$ for some c,d. Once again, we need to go deeper into the possibilities for odd numbers, namely, $4k\pm 1$. Letting $a=4m\pm 1, b=4n\pm 1$ gives four possible cases for each of $a\pm b$:

a	b	$a+b$	$a-b$
$4m+1$	$4n+1$	$4m+4n+2$	$4m-4n=4(m-n)$
$4m+1$	$4n-1$	$4m+4n=4(m+n)$	$4m-4n+2$
$4m-1$	$4n+1$	$4m+4n=4(m+n)$	$4m-4n-2$
$4m-1$	$4n-1$	$4m+4n-2$	$4m-4n$=$4(m-n)$

So, comparing the final two columns, either $4|a+b$ or $4|a-b$.

Case 4a: $4|a+b$
Using Lemma 20, page 44, namely,

$$(c^2+3d^2)(a^2+3b^2) = (ac-3b)^2+3(ad+bc)^2$$

with $c = d = 1$ we have,

$$\begin{aligned}(1^2+3\times 1^2)(a^2+3b^2) &= (a-3b)^2+3(a+b)^2\\ \Rightarrow 4(a^2+3b^2) &= (a-3b)^2+3(a+b)^2\end{aligned}$$

Since $a-3b = (a+b)-4b$ and $4|a+b \Rightarrow a+b = 4j$ then,

$$a-3b = (a+b)-4b = 4j-4b = 4(j-b) \Rightarrow 4|a-3b$$

So let $a-3b = 4c$ and $a+b = 4d$ for some $c, d \in \mathbb{Z}$. Then,

$$\begin{aligned}c^2+3d^2 &= \left(\frac{a-3b}{4}\right)^2+3\left(\frac{a+b}{4}\right)^2\\ &= \frac{a^2-\cancel{6ab}+9b^2+3a^2+\cancel{6ab}+3b^2}{16} = \frac{a^2+3b^2}{4}\end{aligned}$$

*****

Case 4b: Similarly, using Lemma 20, page 44,

$$(c^2+3d^2)(a^2+3b^2) = (ac-3bd)^2+3(ad+bc)^2$$

with $c = 1, d = -1$ we have,

$$\begin{aligned}(1^2+3\times(-1)^2)(a^2+3b^2) &= (a+3b)^2+3(-a+b)^2\\ \Rightarrow 4(a^2+3b^2) &= (a+3b)^2+3(a-b)^2\end{aligned}$$

Since $a+3b = (a-b)+4b$ and $4|a-b$ then we must have $4|a+3b$.
So let $a+3b = 4c \Rightarrow c = \dfrac{a+3b}{4}$ and $a-b = 4d \Rightarrow d = \dfrac{a-b}{4}$. Then,

$$\begin{aligned}c^2+3d^2 &= \left(\frac{a+3b}{4}\right)^2+3\left(\frac{a-b}{4}\right)^2\\ &= \frac{a^2+\cancel{6ab}+9b^2+3a^2-\cancel{6ab}+b^2}{16} = \frac{a^2+3b^2}{4}\end{aligned}$$

□

Lemma 22.
If a prime of the form p^2+3q^2 divides a^2+3b^2 then there exist c, d such that,

$$\frac{a^2+3b^2}{p^2+3q^2} = c^2+3d^2$$

Proof. Let $p^2 + 3q^2$ be a prime[5] and,

$$\frac{a^2 + 3b^2}{p^2 + 3q^2} = f \Rightarrow a^2 + 3b^2 = f(p^2 + 3q^2) \tag{5.3.1}$$

Now, algebraically,

$$\begin{aligned}(pb - aq)(pb + aq) &= p^2b^2 - a^2q^2 \\ &= p^2b^2 + (3q^2b^2 - 3q^2b^2) - a^2q^2 \\ &= b^2(p^2 + 3q^2) - q^2(a^2 + 3b^2) \\ &= b^2(p^2 + 3q^2) - q^2f(p^2 + 3q^2) \\ &= (p^2 + 3q^2)(b^2 - q^2f)\end{aligned}$$

where we added and subtracted $3q^2b^2$ and substituted for $a^2 + 3b^2$ using (5.3.1). Since $p^2 + 3q^2$ is a prime, then by Euclid's Lemma 17, page 42, $p^2 + 3q^2$ divides either $pb - aq$ or $pb + aq$ and therefore either $d(p^2 + 3q^2) = pb + aq$ or $d(p^2 + 3q^2) = pb - aq$ for some integers d.

Rather than take this as two cases, we can treat both cases at the same time by stating,

$$d(p^2 + 3q^2) = pb \pm aq \text{ for some integer } d. \tag{5.3.2}$$

By Lemma 20, page 44,

$$(c^2 + 3d^2)(a^2 + 3b^2) = (ac - 3bd)^2 + 3(ad + bc)^2$$

With $c = p, d = \pm q$ we know,

$$(p^2 + 3(\pm q)^2)(a^2 + 3b^2) = (pa \pm 3qb)^2 + 3(pb \pm aq)^2 \tag{5.3.3}$$

$$\Rightarrow (pa \pm 3qb)^2 = (p^2 + 3q^2)(a^2 + 3b^2) - 3(pb \pm aq)^2 \tag{5.3.4}$$

Then, using (5.3.2),

$$(pa \pm 3qb)^2 = (p^2 + 3q^2)(a^2 + 3b^2) - 3d^2(p^2 + 3q^2)^2 \tag{5.3.5}$$

$$= (p^2 + 3q^2)[(a^2 + 3b^2) - 3d^2(p^2 + 3q^2)] \tag{5.3.6}$$

This implies $p^2 + 3q^2$ divides $(pa \pm 3qb)^2$ and therefore[6] the prime $p^2 + 3q^2$ divides $pa \pm 3qb$, that is,

$$pa \pm 3qb = c(p^2 + 3q^2) \text{ for some integer } c. \tag{5.3.7}$$

Together (5.3.2) and (5.3.5) mean there exist c, d such that,

$$pa \pm 3qb = c(p^2 + 3q^2) \text{ and } pb \pm qa = d(p^2 + 3q^2) \tag{5.3.8}$$

[5] For example $2^2 + 3 \times 5^2 = 79 \in \mathbb{P}$.

[6] See footnote on page 32 which shows if a prime p divides m^2 then we must have $p|m$.

Then,

$$(pa \pm 3qb)^2 + 3(pb \pm qa)^2 = [c(p^2 + 3q^2)]^2 + 3[d(p^2 + 3q^2)]^2 \tag{5.3.9}$$

From Equation (5.3.3), we have,

$$a^2 + 3b^2 = \frac{(pa \pm 3qb^2) + 3(pb \pm aq)^2}{p^2 + 3(\pm q)^2}$$

so that,

$$\begin{aligned}\frac{a^2 + 3b^2}{p^2 + 3q^2} &= \frac{(pa \pm 3qb^2) + 3(pb \pm aq)^2}{(p^2 + 3(\pm q)^2)(p^2 + 3q^2)} \\ &= \frac{[c(p^2 + 3q^2)]^2 + 3[d(p^2 + 3q^2)]^2}{(p^2 + 3q^2)^2} \text{by (5.3.9)} \\ &= c^2 + 3d^2\end{aligned}$$

□

Lemma 23.
If $a^2 + 3b^2$ has an odd factor f that is not of this form (square plus 3 times a square), then the quotient $\dfrac{a^2 + 3b^2}{f}$ has an odd factor that is not of this form.

Proof. We need to show that if an odd number f is a factor of $a^2 + 3b^2$ and $f \neq p^2 + 3q^2$ for any p, q then $\dfrac{a^2 + 3b^2}{f}$ has an odd factor f' where $f' \neq p^2 + 3q^2$ for any p, q.
Suppose $a^2 + 3b^2 = fg$ where f is odd and $f \neq p^2 + 3q^2$ for any p, q. We need to show $g = \dfrac{a^2 + 3b^2}{f}$ has a factor which is not of the form $p^2 + 3q^2$ for any p, q. We use contradiction.
Let's assume all the odd factors of g have the form $p^2 + 3q^2$. By the Fundamental Theorem of Arithmetic, Theorem 19, page 43, $g = p_1 \times p_2 \times \cdots \times p_n$, a series of primes.
So consider $f = \dfrac{a^2 + 3b^2}{g}$, $g = p_1 \times p_2 \times \cdots \times p_n$.
Now if g is even then for cancellation to be possible $a^2 + 3b^2$ must also be even, given f is odd. We cannot have a odd and b even or vice versa since we would then have $a^2 + 3b^2$ odd. So there are two cases.
Case A: a, b even. Then with $a = 2k, b = 2j$,

$$a^2 + 3b^2 = (2k)^2 + 3(2j)^2 = 4[k^2 + 3j^2]$$

Case B: a, b odd. Then with $a = 2k + 1, b = 2j + 1$,

$$a^2 + 3b^2 = (2k + 1)^2 + 3(2j + 1)^2 = 4k^2 + 4k + 1 + 12j^2 + 12j + 3 = 4[k^2 + k + 3j^2 + 3j + 1]$$

In each case $4|a^2 + 3b^2$ and by Lemma 21, page 45,

$$\frac{a^2 + 3b^2}{4} = c^2 + 3d^2, \text{ for some } c, d.$$

retaining the form when we divide $a^2 + 3b^2$ by each occurrence of 4 in the prime expansion of g.

So, eliminating all the 4 factors in g, we can say $f = \dfrac{a^2 + 3b^2}{g}$ where g is now the product of odd primes of the form $p^2 + 3q^2$ and we can divide by all the odd primes in g since we are assuming all odd factors take the form $c^2 + 3d^2$ and by Lemma 22, page 46, $\dfrac{a^2 + 3b^2}{p^2 + 3q^2} = c^2 + 3d^2$ for some p, q.

But this leaves $f = p^2 + 3q^2$ which is a contradiction. Therefore, g must have a factor which is not of the form $p^2 + 3q^2$ for some p, q. □

The following lemma is the most difficult in this series. It uses the method of infinite descent. Again, the algebra is not difficult. The difficulty lies in following the logic of the argument.

Lemma 24.
Let a, b be any integers with $gcd(a, b) = 1$. Then every odd factor x of $a^2 + 3b^2$ has the same form, that is $x = c^2 + 3d^2,\ c, d \in \mathbb{Z}$.

Proof. Let a, b be any integers with $gcd(a, b) = 1$.

Let x be a positive odd factor of $a^2 + 3b^2$. Then there exists $f \in \mathbb{Z}$ such that,

$$a^2 + 3b^2 = xf$$

Now $1 = 1^2 + 3 \times 0^2$, so the lemma is true for $x = 1$.

Assume $x > 1$. Then by the Division Algorithm, Theorem 13, page 39, there exist integers m, n, c, d such that,

$$a = mx \pm c,\ \ b = nx \pm d \text{ with } |c| < x,\ |d| < x. \tag{5.3.10}$$

As proved in Corollary 14, page 40 to the Division Algorithm, we can assume $|c| < \dfrac{x}{2}$ and $|d| < \dfrac{x}{2.}$ Then,

$$\begin{aligned} a^2 + 3b^2 &= (mx \pm c)^2 + 3(nx \pm d)^2 \\ &= x(m^2x \pm 2mc + 3n^2x \pm 6nd) + c^2 + 3d^2 \end{aligned}$$

But $x|a^2 + 3b^2$, hence $x|c^2 + 3d^2$, say $c^2 + 3d^2 = xy$.

Then using $|c|, |d| < \dfrac{x}{2}$,

$$\begin{aligned} xy = c^2 + 3d^2 < \left(\frac{x}{2}\right)^2 + 3\left(\frac{x}{2}\right)^2 = x^2 \\ \Rightarrow y < x \end{aligned} \tag{5.3.11}$$

Now $c^2 + 3d^2 \neq 0$, else both $c, d = 0$ and then by (5.3.10) $a = mx, b = nx \Rightarrow gcd(a, b) \geq x$, contradicting $gcd(a, b) = 1$.
Let $g = gcd(c, d)$ so that $c = gC, d = gD, gcd(C, D) = 1$. Then,

$$xy = c^2 + 3d^2 = g^2(C^2 + 3D^2) \Rightarrow g^2|xy. \tag{5.3.12}$$

We claim $g^2|y$. We use contradiction. Assume there is any prime p that divides g and x. Then there exist X, G such that $g = pG, x = pX$, and, again referring to (5.3.10),

$$a = mx \pm c = mpX \pm GpC = p(mX \pm GC)$$
$$b = nx \pm d = npX \pm GpD = p(nX \pm GD)$$

which means $gcd(a, b) \geq p$, contradicting $gcd(a, b) = 1$.
So none of the factors of g and therefore g^2 can divide x. Then,

$$g^2|y \Rightarrow y = g^2z, \ z \in \mathbb{Z} \tag{5.3.13}$$

Then,

$$xy = g^2(C^2 + 3D^2) \Rightarrow xz = C^2 + 3D^2 \tag{5.3.14}$$

for some $z = \dfrac{y}{g^2}$ with $gcd(C, D) = 1$.
To conclude, we claim $x = p^2 + 3q^2$ for some p, q. Again we use contradiction and assume x is not of this form.
But by Lemma 23, page 48, if $C^2 + 3D^2$ has an odd factor x which is not of this form, then the quotient $z = \dfrac{p^2 + 3q^2}{x}$ has an odd factor which is not of this form.
So there is a w such that $w|z$ and w is not of the form $p^2 + 3q^2$.
Now $w \neq 1$ since $1 = 1^1 + 3(0)^2$ (the form $p^2 + 3q^2$) and $w|z \Rightarrow w < z$ and from (5.3.13) $y = g^2z \Rightarrow z < y$ and from (5.3.11) $y < x$ so $w < z < y < x$.

We have proved that the existence of a factor x of $a^2 + 3b^2$ not of the form $p^2 + 3q^2$ proves the existence of a smaller factor w which divides a smaller value z not of the form $p^2 + 3q^2$. We can use the same argument to find a smaller factor w' which divides a smaller value of the same form and then another $w'' < w' < w$ and so on, thereby generating an infinite number of different factors of the one natural number $C^2 + 3D^2$. This is a contradiction by the method of infinite descent.
Then, $x = p^2 + 3q^2$ for some p, q. □

5.3.2 The Theorem: $n = 3$ case

Having proved the lemmas regarding $a^2 + 3b^2$, we proceed to prove $x^3 + y^3 + (-z)^3 = 0$ has no integer solutions. We again use a proof by contradiction. We suppose it does. This supposition leads to a factor of $(-z)^3$ of the form $a^2 + 3b^2$ and then to an infinite number of factors of this form. By the method of infinite descent this is not possible, so our supposition is incorrect. The proof is due to Euler.

Theorem 25. *(Euler, 1770) The $n = 3$ case.*
The equation $x^3 + y^3 = z^3 \Leftrightarrow x^3 + y^3 + (-z)^3 = 0$ has no non-zero integer solutions.

Proof. We assume a smallest solution (x, y, z) to the equation $x^3 + y^3 + z^3 = 0$, where the three non-zero integers x, y, z are pair-wise co-prime and not all positive.
One of the three must be even, whereas the other two are odd. Without loss of generality, z may be assumed to be even, say $z = 2k$.
Since x and y are both odd, their sum and difference are both even numbers, say,

$$x + y = 2u, x - y = 2v \Rightarrow x = u + v, y = u - v$$

where we claim the non-zero integers u and v are co-prime (or $gcd(u, v) = 1$) and have different parity (one is even, the other odd).
The reason for being co-prime is that if $u = rd, v = sd, gcd(u, v) = d \neq 1$, then,

$$x = u + v = d(r + s) \text{ and } y = u - v = d(r - s)$$

makes $gcd(x, y) \geq d$ contradicting $gcd(x, y) = 1$. This then means u, v cannot both be even.
Also, if both are odd, say $u = 2m + 1, v = 2n + 2$ then,

$$\begin{aligned} x &= u + v = 2m + 1 + 2n + 1 = 2(m + n + 1) \\ y &= u - v = 2m + 2 - 2n - 2 = 2(m - n) \end{aligned}$$

making both x, y even, again contradicting $gcd(x, y) = 1$. Therefore they must be of opposite parity (one odd, the other even).
Now $x = u + v, y = u - v$ gives,

$$\begin{aligned} -z^3 &= x^3 + y^3 \\ &= (u + v)^3 + (u - v)^3 \\ &= u^3 + \cancel{3u^2v} + 3uv^2 + \xcancel{v^3} + u^3 - \cancel{3u^2v} + 3uv^2 - \xcancel{v^3} \\ &= 2u(u^2 + 3v^2) \end{aligned} \qquad (5.3.15)$$

Since $u = 2k, v = 2j + 1$ or $u = 2j + 1, v = 2k$, then,

$$\begin{aligned} u^2 + 3v^2 &= (2j + 1)^2 + 3(2k)^2 = 2(2j^2 + 2j + 6k^2) + 1 = 2m + 1, m \in \mathbb{Z} \\ &\quad or \\ u^2 + 3v^2 &= (2k)^2 + 3(2j + 1)^2 = 2(2k^2 + 6j + 6j^2 + 1) + 1 = 2n + 1, n \in \mathbb{Z}, \end{aligned}$$

so $u^2 + 3v^2$ is always an odd number. Therefore, if $z = 2m$ and $u^2 + 3v^2 = 2n + 1$ then, from (5.3.14),

$$-z^3 = 2u(u^2 + 3v^2) \Rightarrow -8m^3 = 2u(2n + 1) \qquad (5.3.16)$$

which is only possible if $8|2u$, so u must be even and therefore v must be odd.
Since $gcd(u, v) = 1$, then we claim the greatest common divisor of $2u$ and $u^2 + 3v^2$ is

either 1 or 3.
This is true since if $u = 3k$ then $u^2 + 3v^2 = 9k^2 + 3v^2 = 3(3k^2 + v^2)$ is divisible by 3, so $gcd(u, u^2 + 3v^2) = 3$. But no other prime $p > 3$ can be a common divisor since if $p|u$ and we substitute $2u = pj$ into $u^2 + 3v^2 = pk$, then,

$$\frac{p^2j^2}{4} + 3v^2 = pk \Rightarrow 3v^2 = p[k - \frac{p^2j^2}{4}]$$

so $p|v$ also which is a contradiction to $gcd(u, v) = 1$. Hence $gcd(u, u^2 + 3v^2) = 1$ or 3.
Let us consider these two cases for $gcd(u, v)$.
Case A: $gcd(2u, u^2 + 3v^2) = 1$
This implies $3\nmid u$ since if $u = 3k$ then,

$$2u = 6k, u^2 + 3v^2 = 9k^2 + 3v^2 = 3(3k^2 + v^2) \Rightarrow gcd(u, v) \geq 3$$

Then in (5.3.15) $-z^3 = 2u(u^2 + 3v^2)$ is only possible if both $2u$ and $u^2 + 3v^2$ are cubes of two smaller numbers r, s say

$$2u = r^3, u^2 + 3v^2 = s^3 \tag{5.3.17}$$

Since u is even and v is odd then $u^2 + 3v^2$ is odd and so is s.
Lemma 24, page 49 proved that if s is odd and satisfies an equation $s^3 = u^2 + 3v^2$ so that s is an odd factor of $u^2 + 3v^2$ then s can be written in terms of two co-prime integers e and f as $s = e^2 + 3f^2$, so that we can only have,

$$\begin{aligned} u &= e(e^2 - 9f^2) \\ v &= 3f(e^2 - f^2), \end{aligned}$$

since then[7],

$$\begin{aligned} u^2 + 3v^2 &= [e(e^2 - 9f^2)]^2 + 3[3f(e^2 - f^2)]^2 \\ &= e^2(e^4 - 18e^2f^2 + 81f^4) + 3[9f^2(e^4 - 2e^2f^2 + f^4)] \\ &= e^6 - 18e^4f^2 + 81e^2f^4 + 27e^4f^2 - 54e^2f^4 + 27f^6 \\ &= e^6 + 9e^4f^2 + 27e^2f^4 + 27f^6 \\ &= (e^2 + 3f^2)^3 \\ &= s^3 \end{aligned}$$

***

Now $gcd(e, f) = 1$ so either e is even and f odd or vice versa. But u is even so if e were odd and f even then

$$u = e(e^2 - 9f^2) = (odd)(odd - even) = (odd)(odd)$$

[7] Recall $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$

so we must have e even and f odd.
Now from (5.3.17),

$$r^3 = 2u = 2e(e-3f)(e+3f) \tag{5.3.18}$$

We claim the factors $2e, e-3f, e+3f$ are co-prime.

***

First 3 cannot divide e, else $3|u = e(e^2 - 9f^2)$ and $3|v = 3f(e^2 - f^2)$, so $3|u$ and $3|v$ making $gcd(u,v) \geq 3$ contradicting $gcd(u,v) = 1$.
And if $3\not|e$ then $3\not|e-3f$ and $3\not|e+3f$ so we can rule out 3 as a factor of any of the three factors.
Second no other prime $p > 3$ can divide more than one of $e, e-3f, e+3f$.
First suppose $2e = kp, e \pm 3f = jp$. Then multiplying $e \pm 3f = jp$ by 2 and substituting $2e = kp$ we have

$$\begin{aligned} 2e \pm 6f = 2jp \Rightarrow kp \pm 6f = 2jp \Rightarrow p|f \text{ since } p > 3, \\ \textit{and} \\ 2e = kp \Rightarrow p|e \end{aligned}$$

so that $gcd(e,f) \geq p$ which contradicts $gcd(e,f) = 1$. Hence $gcd(2e, e \pm 3f) = 1$.
Second suppose $p > 3$ and $gcd(e+3f, e-3f) = p$. Then $e - 3f = pk, e + 3f = pj$.
Adding we have $2e = p(j+k)$ and subtracting we have $6f = p(k-j)$ Hence $p|e$ and $p|f$ again contradicting $gcd(e,f) = 1$.
We conclude the factors $2e, e-3f, e+3f$ are co-prime, proving our claim.

***

Since the three factors on the right side of Equation (5.3.18) are co-prime they must individually equal cubes of smaller integers, say,

$$-2e = k^3, e - 3f = l^3, e + 3f = m^3$$

This yields a smaller solution[8],

$$k^3 + l^3 + m^3 = -2e + e - 3f + e + 3f = 0$$

Therefore, by the argument of infinite descent, the original solution (x,y,z) was impossible.

Case B: $gcd(2u, u^2 + 3v^2) = 3$
The argument is similar to Case A.

[8] Why smaller? We have $u = e(e-3f)(e+3f) = -\frac{k^3}{2} \cdot l^3 \cdot m^3$, so all of k, l, m are less than u. But $x = u + v$ so $u < x$. Hence $k, l, m < x$ and by a similar argument y and hence z.

$gcd(2u, u^2 + 3v^2) = 3$ means $3|u$ or $u = 3w, w < u$.
Since, from (5.3.15), $8|2u \Rightarrow 4|u \Rightarrow 4|3w$ then w is even. Since u, v are co-prime, then so are v, w. Then neither 3 nor 4 divide v.
Substituting $u = 3w$ in $-z^3 = 2u(u^2 + 3v^2)$ gives,

$$-z^3 = 6w(9w^2 + 3v^2) = 18w(3w^2 + v^2)$$

Because v, w are co-prime and $3\nmid v$ then $18w$ and $3w^2+v^2$ are also co-prime[9]. Therefore, since their product is a cube, they are each the cube of smaller integers r and s thus,

$$18w = r^3, \ 3w^2 + v^2 = s^3$$

By Lemma 24, page 49, since s is odd and a factor of a number of the form $3w^2 + v^2$, it can be expressed in terms of smaller co-prime numbers, e and f as $s = e^2 + 3f^2$ so that (as above),

$$\begin{aligned} v &= e(e^2 - 9f^2) \\ w &= 3f(e^2 - f^2) \end{aligned}$$

Since v is odd, then e is odd and f is even. Now,

$$\begin{aligned} r^3 &= 18w \\ &= 54f(e^2 - f^2) \\ &= 54f(e - f)(e + f) \\ &= 3^3 \times 2 \times f(e - f)(e + f) \end{aligned}$$

Since $3^3|r^3$ then $3|r$ so $\left(\frac{r}{3}\right)^3$ is an integer and $\left(\frac{r}{3}\right)^3 = 2f(e - f)(e + f)$.
Since e and f are co-prime, so are the factors $2f, e - f, e + f$. Therefore, they must individually equal cubes of smaller integers, say,

$$2f = k^3, \ e - f = l^3, (e + f) = (-m)^3$$

By the same argument as for Case A this also yields a smaller solution,

$$k^3 + l^3 + m^3 = 2f + e - f - e - f = 0$$

Therefore, by the argument of infinite descent, the original solution (x, y, z) was impossible. □

[9] This is so since for $p > 3$ if $18w = kp$ and $3w^2 + v^2 = jp$ then $\frac{3k^2p^2}{18^2} + v^2 = jp$ implies $p|w$ and $p|v$ contracdicting $gcd(w, v) = 1$.

Chapter 6

Shopping Excursion I

Complex Numbers and the Triangle Inequality

We need to know more about numbers, not only real numbers but also complex numbers. We explore them through the example of the Triangle Inequality which is widely used in proofs in number theory and other branches of mathematics – indeed we refer to it later. Its name derives from an ancient proof by Euclid that the length of any one side of a triangle is less than the sum of the lengths of the other two sides. Let's first prove it for real numbers, then develop the theory of complex numbers to a level that enables us to prove it for complex numbers.

6.1 The Triangle Inequality for Real Numbers

First, we recall the definition of absolute value, $|x| = \begin{cases} x, \ if \ x \geq 0 \\ -x, \ if \ x < 0 \end{cases}$

It therefore follows that for all real numbers that,

$$|x|^2 = x^2 \tag{6.1.1}$$

$$xy \leq |x| \cdot |y| \tag{6.1.2}$$

since for 6.1.1 both sides are positive aand for 6.2.2 the left side may be positive or negative but the right side is always positive.

Lemma 26. *(Triangle Inequality in $\mathbb{R}$)*
For all real numbers x, y, we have $|x + y| \leq |x| + |y|$

Proof.

$$\begin{aligned} |x+y|^2 &= (x+y)(x+y) \text{ by } (6.1.1 \\ &= x^2+2xy+y^2 \\ &= |x|^2+2xy+|y|^2 \text{ by } (6.1.1) \\ &\le |x|^2+2|x|\cdot|y|+|y|^2 \text{ by } (6.1.2) \\ &= (|x|+|y|)^2 \end{aligned}$$

Taking the square root of both sides, we have $|x+y| \le |x|+|y|$ □

6.2 Complex Numbers – Notation and Definitions

Notation 1. *We put* $i = \sqrt{-1}$.
We note that i *is a solution of the equation,* $x^2+1=0$ *since* $(i)^2+1=-1+1=0$
We further note that there is no real solution to the equation $x^2+1=0$ *since the square of any real number is always positive. We call* i *an imaginary or complex number.*

Definition 12. *complex numbers*
The set $\mathbb{C}$ *of complex numbers is defined as,*

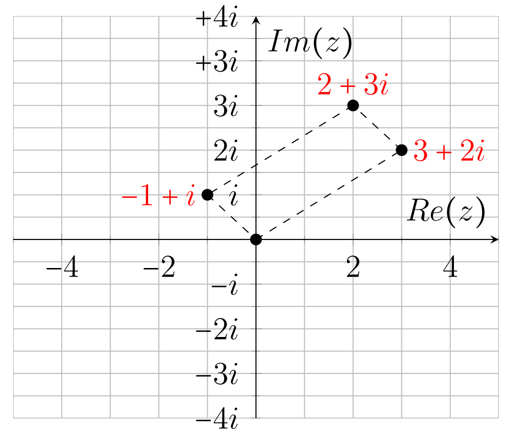
$$\mathbb{C} = \{z = x+iy \mid x, y \in \mathbb{R}, i = \sqrt{-1}\}$$

We call x the real part of z, written $x = Re(z)$, and we call y the imaginary part of z, written $y = Im(z)$.
We note that every real number is included in $\mathbb{C}$ (take $y = 0$), that is, $\mathbb{R} \subset \mathbb{C}$.

Definition 13. *complex conjugate*
The complex conjugate $\bar{z}$ *of the complex number* $z = x+iy$ *is defined by* $\bar{z} = x - iy$.

Definition 14. *magnitude of a complex number*
The magnitude $|z|$ *of the complex number* $z = x+iy$ *is defined by* $|z| = \sqrt{x^2+y^2}$.

Definition 15. *complex number plane*
Analogous to the real number plane, we define the complex number plane by retaining the $x-axis$ *for* $Re(z)$ *and assigning* $Im(z)$ *to the imaginary* $y-axis$.

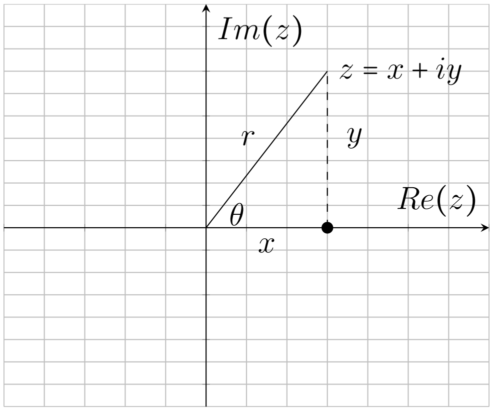


The complex numbers are placed on the complex plane as indicated by $2+3i$ corresponding to the placement of $(2,3)$ on the real number plane and so on.

The reader may choose to skip over the following section and return to it after Part III Shopping Excursion II - Calculus and Part V Shopping Excursion III: Exponential and Trigonometric Functions. If so go to section 6.4, The Theory of Complex Numbers, below.

6.3 Definitions using Polar Coordinates

Again analogous to the real number plane, each complex number may be assigned a distance r from the origin, called its magnitude, and an angle θ, called its argument, formed by the positive x-axis or $Re(z)$-axis and the line joining the number to the origin.



We have $\cos\theta = \dfrac{x}{r}$, $\sin\theta = \dfrac{y}{r}$ so we can write,

$$z = x + iy = r\cos\theta + ir\sin\theta = re^{i\theta}$$

where we used Euler's equation $e^{i\theta} = \cos\theta + i\sin\theta$. (see Theorem 119, page 173).

We define,

- Magnitude of z by $r = |z| = \sqrt{x^2+y^2}$
- Argument of z by $Arg(z) = \theta = \tan^{-1}\left(\dfrac{y}{x}\right)$
- Complex conjugate of z by $\bar{z} = x - iy$.

As an aside, let's prove a theorem using the polar coordinate form of complex numbers. We could also prove it by induction using ordinary complex numbers, but it is then a much longer proof. Polar coordinates can shorten proofs considerably!

Theorem 27. *(DeMoivre's Theorem)*
If $z = r(\cos\theta + i\sin\theta)$ *then* $z^n = r^n(\cos n\theta + i\sin n\theta)$

Proof.

$$\begin{aligned} z &= r(\cos\theta + i\sin\theta) = re^{i\theta} \\ \Rightarrow z^n &= r^n\left(e^{i\theta}\right)^n = r^n e^{in\theta} = r^n(\cos n\theta + i\sin n\theta) \end{aligned}$$

□

6.4 The Theory of Complex Numbers

We now prove a series of general lemmas for complex numbers. We will then use them in the proof of the triangle inequality for complex numbers. This procedure is excellent simple example of how theorems are built from other theorems or from lemmas.
Let $z = x + iy,\ z_1 = x_1 + iy_1,\ z_2 = x_2 + iy_2 \in \mathbb{C}$.
Note $\bar{\bar{z}} = \overline{x - iy} = x + iy = z$.

Lemma 28.

$$|z|^2 = z\bar{z}$$

Proof. $z\bar{z} = (x + iy)(x - iy) = x^2 + y^2 = |z|^2$. □

Lemma 29.

$$\bar{z}_1 z_2 = \overline{z_1\bar{z}_2}$$

Proof.

$$\begin{aligned} \overline{z_1\bar{z}_2} &= \overline{(x_1 + iy_1)(x_2 - iy_2)} \\ &= \overline{x_1x_2 + y_1y_2 + i(x_2y_1 - x_1y_2)} \\ &= x_1x_2 + y_1y_2 - i(x_2y_1 - x_1y_2) \\ &= (x_1 - iy_1)(x_2 + iy_2) \\ &= \bar{z}_1 z_2 \end{aligned}$$

□

Lemma 30.

$$\overline{z_1z_2} = \bar{z}_1\bar{z}_2$$

Proof. Replace z_2 with $\bar{z}_2$ in Lemma 29 to obtain $\bar{z}_1\bar{z}_2 = \overline{z_1\bar{\bar{z}}_2} = \overline{z_1z_2}$ □

Lemma 31.

$$|z| \geq Rez = x$$

Proof. $|z|^2 = x^2 + y^2 \geq x^2 \Rightarrow |z| \geq x = Re(z)$. □

Lemma 32.

$$z + \bar{z} = 2Re(z)$$

Proof. $z + \bar{z} = x + iy + x - iy = 2x = 2Re(z)$. □

Lemma 33.

$$|z_1 z_2| = |z_1||z_2|$$

Proof. We use $|x + iy|^2 = x^2 + y^2$.

$$\begin{aligned}
|z_1 z_2|^2 &= |(x_1 + iy_1)(x_2 + iy_2|^2 \\
&= |x_1x_2 - y_1y_2 + i(x_2y_1 + x_1y_2)|^2 \\
&= (x_1x_2 - y_1y_2)^2 + (x_2y_1 + x_1y_2)^2 \\
&= x_1^2x_2^2 - \cancel{2x_1x_2y_1y_2} + y_1^2y_2^2 + x_2^2y_1^2 + \cancel{2x_2y_1x_1y_2} + x_1^2y_2^2 \\
&= x_1^2(x_2^2 + y_2^2) + y_1^2(x_2^2 + y_2^2) \\
&= (x_1^2 + y_1^2)(x_2^2 + y_2^2) \\
&= |z_1|^2|z_2|^2
\end{aligned}$$

Take the square root to obtain the result. □

Lemma 34.

$$|z_1||\bar{z_2}| = |z_1\bar{z_2}|$$

Proof. Putting $z_2 = \bar{z_2}$ in Lemma 33 we have,

$$|z_1\bar{z_2}| = |z_1||\bar{z_2}|$$

□

Lemma 35.

$$\overline{z_1 + z_2} = \bar{z_1} + \bar{z_2}$$

Proof.

$$\begin{aligned}
\overline{z_1 + z_2} &= \overline{x_1 + iy_1 + x_2 + iy_2} \\
&= \overline{x_1 + x_2 + i(y_1 + y_2)} \\
&= x_1 + x_2 - i(y_1 + y_2) \\
&= x_1 - iy_1 + x_2 - iy_2 \\
&= \bar{z_1} + \bar{z_2}
\end{aligned}$$

□

Lemma 36.

$$|z| = |\bar{z}|$$

Proof. Put $z = \bar{z}$ in $|z|^2 = z\bar{z}$ to get $|\bar{z}|^2 = \bar{z}\bar{\bar{z}} = \bar{z}z \Rightarrow |\bar{z}|^2 = |z|^2$.
Take the square root to obtain the result. □

6.5 Triangle Inequality for Complex Numbers

Theorem 37. *(Triangle Inequality in $\mathbb{C}$)*

$$|z_1 + z_2| \leq |z_1| + |z_2|$$

Proof.

$$\begin{aligned}
|z_1 + z_2|^2 &= (z_1 + z_2)\overline{(z_1 + z_2)} \text{ by Lemma 28} \\
&= (z_1 + z_2)(\bar{z_1} + \bar{z_2}) \text{ by Lemma 35} \\
&= z_1\bar{z_1} + z_2\bar{z_2} + z_2\bar{z_1} + z_1\bar{z_2} \\
&= |z_1|^2 + |z_2|^2 + \bar{z_1}z_2 + z_1\bar{z_2} \text{ by Lemma 28} \\
&= |z_1|^2 + |z^2|^2 + \overline{z_1\bar{z_2}} + z_1\bar{z_2} \text{ by Lemma 29} \\
&= |z_1|^2 + |z^2|^2 + 2Re(z_1\bar{z_2}) \text{ by Lemma 32} \\
&\leq |z_1|^2 + |z^2|^2 + 2|z_1\bar{z_2}| \text{ by Lemma 31} \\
&\leq |z_1|^2 + |z^2|^2 + 2|z_1||\bar{z_2}| \text{ by Lemma 34} \\
&\leq |z_1|^2 + |z^2|^2 + 2|z_1||z_2| \text{ by Lemma 36} \\
&\leq (|z_1| + |z^2|)^2
\end{aligned}$$

Take the square root of both sides to obtain the result. □

Chapter 7

The n = 3 Case by Complex Techniques

We now use complex numbers to prove $x^3 + y^3 = z^3$ has no non-zero integer solutions.

Course: *Main Course Choice 2*

Ingredients

Greek alphabet

Complex number theory

Algebraic numbers and algebraic integers

$k(\rho)$, a subset of the complex numbers

Directions

Prove a bunch of lemmas relating to the numbers of $k(\rho)$.

Use the lemmas to prove the $n = 3$ case.

We will now prove there are no solutions to $x^3 + y^3 = z^3$ in the natural numbers using complex methods. The proof may be found in Hardy and Wright's "An Introduction to the Theory of Numbers." The mathematics of complex numbers usually uses Greek letters for variables. It is handy to know the English names of the Greek letters.

Name	Symbol	Name	Symbol	Name	Symbol
Alpha	α A	Beta	β B	Gamma	$\gamma\Gamma$
Delta	$\delta\Delta$	Epsilon	ϵ E	Zeta	ζ Z
Eta	η E	Theta	$\theta\Theta$	Iota	ι I
Kappa	κ K	Lambda	$\lambda\Lambda$	Mu	μ M
Nu	ν N	Xi	$\xi\Xi$	Pi	$\pi\Pi$
Rho	ρ R	Sigma	$\sigma\Sigma$	Tau	τ T
Upsilon	$\upsilon\Upsilon$	Phi	$\phi\Phi$	Chi	χ X
Psi	$\psi\Psi$	Omega	$\omega\Omega$		

7.1 Algebraic Numbers and Algebraic Integers

Definition 16. *algebraic number*
We say[1] ξ *is an algebraic number if it is the root of an equation of the form,*

$$a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0, a_n \neq 0,$$

whose coefficients a_i *are integers.*

Example 28. $\dfrac{1}{\sqrt{3}}$ *is an algebraic number since it is a root of the polynomial equation* $3x^2 - 1 = 0.$ ◇

Definition 17. *algebraic integer*
We say ξ *is an algebraic integer if it is the root of an equation of the form,*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0,$$

whose coefficients are integers and whose leading coefficient is 1.

Example 29. $\sqrt{-1}$ *is an algebraic integer since it is a root of* $x^2 + 1 = 0.$
$\rho = \dfrac{1}{2}(-1 + i\sqrt{3})$ *is an algebraic integer since it is a root of* $x^2 + x + 1 = 0.$ ◇

The three simplest cases of the algebraic integers are what we call,

1. The integers of $k(1)$: the integers or rational integers $\mathbb{Z}$.
2. The integers of $k(i)$: the complex or Gaussian integers $\{a + bi \mid a, b \in \mathbb{Z}\}$
3. The integers[2] of $k(\rho)$: $\left\{\xi = a + b\rho \mid a, b \in k(1), \rho = \dfrac{1}{2}(-1 + i\sqrt{3})\right\}$

7.2 The $k(\rho)$ Algebraic Integers

Again note we defined $k(\rho) = \left\{a + b\rho \mid a, b \in \mathbb{Z}, \rho = \dfrac{-1 + i\sqrt{3}}{2}\right\}$
Note $\rho^2 = \left(\dfrac{-1 + i\sqrt{3}}{2}\right)^2 = \dfrac{-1 - i\sqrt{3}}{2}$, so ρ and ρ^2 are complex conjugates.

We begin with a number of definitions.

[1] ξ=xi pronounced kigh
[2] ρ = rho (row as in a boat), ξ= xi (kigh rhymes with sigh)

Definition 18. *divisor and divisible*
$\xi \in k(\rho)$ *is divisible by*[3] η *if there exists a* ζ *such that* $\xi = \eta\zeta$. *We call* η *a divisor of* ξ *and write* $\eta|\xi$.

Example 30. $3+2i|13$ *or* $3+2i$ *is a divisor of* 13 *since* $13 = (3+2i)(3-2i)$.

Definition 19. *norm*
The norm of $\xi \in k(\rho)$ *is written* $N\xi$ *and for* $\xi = a + b\rho$ *is defined by,*

$$\begin{aligned} N\xi &= (a+b\rho)(a+b\rho^2) \\ &= (a+b\frac{-1+i\sqrt{3}}{2})(a+b\frac{-1-i\sqrt{3}}{2}) \\ &= a^2 - ab + b^2 \end{aligned}$$

Example 31. *The norm of* $3+2\rho$ *is* $N(3+2\rho) = 9-6+4 = 7$

Note 4.

a) *The norm of* $1 = 1 + i0$ *is* $N1 = 1^2 - 1 \times 0 + 0^2 = 1$

b) *For* $\xi \neq 0$, $N\xi = a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2$ *implies* $N\xi \geq 1$ *since both squares are necessarily positive and the smallest values of* a, b *are* $0, \pm 1$.

Lemma 38.

$$\rho + \rho^2 = -1 \tag{7.2.1}$$

$$\rho\rho^2 = 1. \tag{7.2.2}$$

Proof.

$$\begin{aligned} \rho &= \frac{-1+i\sqrt{3}}{2} \\ \Rightarrow \rho^2 &= \frac{-1+i\sqrt{3}}{2} \times \frac{-1+i\sqrt{3}}{2} = \frac{-1-i\sqrt{3}}{2} \\ \Rightarrow \rho + \rho^2 &= \frac{-1+i\sqrt{3}}{2} + \frac{-1-i\sqrt{3}}{2} = \frac{-1}{2} + \frac{-1}{2} = -1 \\ \Rightarrow \rho\rho^2 &= \frac{-1+i\sqrt{3}}{2} \times \frac{-1-i\sqrt{3}}{2} = \frac{1+3}{4} = 1. \end{aligned}$$

□

Lemma 39.
For all[4] $\alpha, \beta \in k(\rho)$ *we have* $N(\alpha\beta) = N(\alpha)N(\beta)$.

[3] η = eta, ζ = zeta

[4] α =alpha, β = beta

Proof. Let $\alpha = a + b\rho$ and $\beta = c + d\rho$.

$$\begin{aligned}
N(\alpha\beta) &= N(a + b\rho)(c + d\rho)\\
&= N(ac + bd\rho^2 + (ad + bc)\rho)\\
&= N(ac + bd(-\rho - 1) + (ad + bc)\rho) \text{ using (7.2.1)}\\
&= N(ac - bd) + (bc + ad - bd)\rho\\
&= (ac - bd)^2 - (ac - bd)(bc + ad - bd) + (bc + ad - bd)^2\\
&= a^2c^2 - \cancel{2abcd} + \cancel{b^2d^2} - abc^2 - a^2cd + abcd + b^2cd + abd^2 - \cancel{b^2d^2}\\
&\qquad + b^2c^2 + \cancel{2abcd} + a^2d^2 - 2b^2cd - 2abd^2 + b^2d^2\\
&= a^2(c^2 - cd + d^2) - ab(c^2 - cd + d^2) + b^2(c^2 - cd + d^2)\\
&= (a^2 - ab + b^2)(c^2 - cd + d^2)\\
&= N(\alpha)N(\beta)
\end{aligned}$$

□

Definition 20. *unity*
ϵ[5] is a unity of $k(\rho)$ if $\epsilon|\xi$ for all $\xi \in k(\rho)$. Equivalently, a unity is any integer which is a divisor of, or divides, 1.

In $\mathbb{Z}$ the only unities are ±1 since only ±1 divide all integers. But in $k(\rho)$ there are more than 2 unities as we will see.

Lemma 40.
The norm of a unity is 1 and any integer whose norm is 1 is a unity.

Proof. First we prove the norm of a unity is 1.
If ϵ is a unity then $\epsilon|1$ hence $\epsilon\eta = 1$ for some $\eta \in k(\rho)$.
Since $N1 = 1$ then, by Lemma 39, $N(\epsilon\eta) = N1 \Rightarrow N(\epsilon)N(\eta) = 1 \Rightarrow N(\epsilon)|1$.
But by Note 2(b), $N(\xi) \geq 1$ for all $\xi \in k(\rho)$ so $N(\epsilon) = 1$.

***

Second we prove any integer whose norm is 1 is a unity.
Let $\xi = a + b\rho \in k(\rho)$ have $N\xi = 1$.
We defined $N\xi = (a + b\rho)(a + b\rho^2)$
Hence, labelling $\bar{\xi} = a + b\rho^2$ we have $N\xi = \xi\bar{\xi}$. Then $N\xi = 1 \Rightarrow \xi\bar{\xi} = 1$.
Hence ξ is a divisor of 1 so by definition ξ is a unity. □

Note 5. *Since in Note 24 we have $N\xi \geq 1$ for all $\xi \in k(\rho)$ then if ξ is not a unity we must have $N\xi \geq 2$.*

Note 6.

[5] ϵ =epsilon, ρ = rho, ξ =xi (kigh), η = eta

Unities $\epsilon = a + b\rho$ in $k(\rho)$ are given by,

$$N\epsilon = 1 \Rightarrow a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2 = 1$$

The only solutions of this equation are $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$ or $a = 1, b = 1$ or $a = -1, b = -1$.
So the unities are:

$$\pm 1; \pm\rho; \pm(1+\rho) \Leftrightarrow \pm 1; \pm\rho; \pm\rho^2 \textit{(using (7.2.1))}$$

Note the positive unities are the roots of $x^3 - 1 = 0$ since

$$\begin{aligned} x^3 - 1 = (x-1)(x^2+x+1) = 0 \\ \Rightarrow x = 1 \text{ or } x = \frac{-1 \pm \sqrt{-3}}{2} = \rho, \rho^2. \end{aligned}$$

We may therefore factor $x^3 - 1$ as,

$$x^3 - 1 = (x-1)(x-\rho)(x-\rho^2) \tag{7.2.3}$$

Lemma 41.
The products and quotients of unities are unities.

Proof. Omitting multiplications by ±1 and using $\rho^3 = 1$ the possible combinations are:

$$\begin{aligned} 1 \times 1 &= 1 \\ \rho \times \rho &= \rho^2 \\ \rho^2 \times \rho^2 &= \rho^4 = \rho \\ \rho \times \rho^2 &= 1 \\ \frac{1}{\rho} &= \frac{1}{\rho} \times \frac{\rho^2}{\rho^2} = \frac{\rho^2}{\rho^3} = \rho^2 \\ \frac{1}{\rho^2} &= \frac{1}{\rho^2} \times \frac{\rho}{\rho} = \rho \\ \frac{\rho^2}{\rho} &= \rho \\ \frac{\rho}{\rho^2} &= \frac{1}{\rho} = \rho^2 \text{ as above} \end{aligned}$$

□

Lemma 42.
If α, β are not unities then $N(\alpha\beta) > 3$.

Proof. From Lemma 40, the norm of a unity is 1 and any integer whose norm is 1 is a unity. Suppose $\alpha, \beta \in k(\rho)$ are not unities.
Therefore,

$$N\alpha \geq 2 \text{ and } N\beta \geq 2 \Rightarrow N(\alpha\beta) = N(\alpha)N(\beta) \geq 4 \Rightarrow N(\alpha\beta) > 3.$$

□

Definition 21. *associates*
If ϵ is an unity, the number $\epsilon\xi$ is said to be an associate of ξ or associated with ξ.

In $k(1) = \mathbb{Z}$ the unities are ±1 so we could say ±7 are associated with 7.

Note 7.
The associates of ξ are therefore $\pm\xi; \pm\rho\xi; \pm\rho^2\xi$.
The associates of 1 are the unities $\pm1; \pm\rho; \pm\rho^2$.

Definition 22. *primes*
A prime π is an integer, not 0 or 1, divisible only by numbers associated with itself or 1, that is, $\pm\pi; \pm\rho\pi; \pm\rho^2\pi$. We reserve the letter[6] π for primes.

In $k(1) = \mathbb{Z}$ we could say a prime is any integer divisible only by the unities ±1 (excluding itself).

Lemma 43.
Any number whose norm is a rational prime is a prime.

Proof. Using proof by the contrapositive we need to prove if a number is not a prime then its norm is not a prime.
Let $\xi \in k(\rho)$ be an integer that is not a prime, say $\xi = \alpha\beta$. Then $N(\xi) = N(\alpha)N(\beta)$ must be a composite number and not a prime. □

Lemma 44.
$\lambda = 1 - \rho$ is a prime[7].

Proof. $N(1-\rho) = 1^2 - (1)(-1) + 1^2 = 3$, a rational prime, so by Lemma 43, λ is a prime. □

Lemma 45.
3 is associated with $\lambda^2 = (1-\rho)^2$.

Proof. We need to show λ^2 is 3 multiplied by a unity. By Lemma 38, page 63, $\rho^2 = -1 - \rho$ so $\lambda^2 = 1 - 2\rho + \rho^2 = 1 - 2\rho - 1 - \rho = -3\rho$ and $-\rho$ is a unity. □

Lemma 46.
λ does not divide 2.

[6] π = pi, ρ = rho
[7] λ = lambda

Proof. Suppose $\lambda|2$ or $2 = \lambda\delta$ for some $\delta \in k(\rho)$.
Now $N2 = N(2 + 0\rho) = 2^2 - 0 + 0 = 4$ but $N(\lambda\delta) = N(\lambda)N(\delta) = 3N(\delta)$ as shown in Lemma 44. Hence $N(\lambda\delta) \geq 6$ since, from Note 5, $N\xi \geq 2$ for all ξ not a unity.
This is a contradiction. Hence λ does not divide 2. □

We now re-introduce the notation of congruency for any of our sets of algebraic integers, $k(1), k(i)$ *or* $k(\rho)$.

Definition 23. *congruence*
Let m be an algebraic integer in $k(1), k(i)$ or $k(\rho)$. If m divides the difference $a-b$ of two integers a, b in $k(1)$, $k(i)$ or $k(\rho)$, we say "a is congruent to b modulo m" and we write,

$$a \equiv b(\text{mod } m)$$

Note 8. *Note that $m|a-b \Rightarrow a-b = mj \Rightarrow a = b + mj, j \in k(1), k(i)$ or $k(\rho)$, so that,*

$$a \equiv b(\text{mod } m) \Leftrightarrow a = b + jk, k \in k(1), k(i) \textit{ or } k(\rho).$$

Definition 24. *residue*
If $a \equiv b(\text{mod } m)$, b is called a residue of a modulo m. It is any possible remainder when a is divided by m.

Example 32.

For example in the ordinary integers, $k(1)$,

$$\begin{aligned} 23 &= 5 \times 4 + 3 &&\Leftrightarrow 23 \equiv 3(\text{mod } 5)\\ 23 &= 5 \times 3 + 8 &&\Leftrightarrow 23 \equiv 8(\text{mod } 5)\\ 23 &= 5 \times 2 + 13 &&\Leftrightarrow 23 \equiv 13(\text{mod } 5)\\ 23 &= 5 \times 1 + 18 &&\Leftrightarrow 23 \equiv 18(\text{mod } 5) \end{aligned}$$

Here the residues are $3, 8, 13$ and 18 and 3 is the preferred least non-negative residue of 23 modulo 5. Accordingly, we generally write $23 \equiv 3(\text{mod } 5)$ unless we specifically state otherwise. ◇

Definition 25. *incongruence*
b, c are said to be incongruent modulo m if $b \not\equiv c(\text{mod } m)$.

Example 33. $3, 5$ *are incongruent modulo 7 since 7 does not divide* $5 - 3$.

The next congruence lemma applies to $\mathbb{Z}$ or the $k(1)$ algebraic integers only.

Lemma 47.
The sum of two integers a, b satisfies $a + b \equiv 0, 1$ or $-1(\text{mod } 3)$.

Proof. Note $x \equiv -1(\text{mod } 3) \Rightarrow x \equiv 2(\text{mod } 3)$ so we need to show $a - b \equiv 0, 1$ *or* $2(\text{mod } 3)$.
Now the least possible non-negative residue of any integer modulo 3 is either $0, 1$ or 2 or $m \equiv 0, 1$ or $2(\text{mod } 3)$ for any $m \in \mathbb{Z}$.
In other words when any integer is divided by 3 the least non-negative remainder can only be $0, 1$ or 2.
Therefore, there are 9 possibilities for the remainder when the sum $a + b$ is divided by 3 as shown in this table.

a	b	$a+b$	$a+b(\text{mod } 3)$
$3j$	$3k$	$3l+0$	0
$3j$	$3k+1$	$3l+1$	1
$3j$	$3k+2$	$3l+2$	2
$3j+1$	$3k$	$3l+1$	1
$3j+1$	$3k+1$	$3l+2$	2
$3j+1$	$3k+2$	$3l+3$	0
$3j+2$	$3k$	$3l+2$	2
$3j+2$	$3k+1$	$3l+3$	0
$3j+2$	$3k+2$	$3k+4$	1

So the only possibilities are $a + b \equiv 0, 1$ or $2(\text{mod } 3) = -1(\text{mod } 3)$. □

Now let us consider congruences involving the $k(\rho)$ integers.

Lemma 48.
All integers[8] *of $\xi \in k(\rho)$ modulo λ fall into one of these three classes,*

$$\xi \equiv 0(\text{mod } \lambda), \xi \equiv 1(\text{mod } \lambda), \xi \equiv -1(\text{mod } \lambda),$$

where $\lambda = 1 - \rho$.

Proof. If $\xi = a + b\rho \in k(\rho)$ and $\lambda = 1 - \rho$ then $\xi = a + b - b\lambda \equiv a + b(\text{mod } \lambda)$
Since, by Lemma 38,

$$\lambda(1-\rho^2) = (1-\rho)(1-\rho^2) = 1 - (\rho + \rho^2) + \rho^3 = 1 - (-1) + 1 = 3,$$

then $\lambda | 3$ so we can say[9] $3 = \lambda\omega, \omega \in k(\rho)$
Now by Lemma 47 the sum of two integers a, b satisfies $a + b \equiv 0, 1$ or $-1(\text{mod } 3)$. Then either,

$$a + b \equiv 0(\text{mod } 3) \Rightarrow a + b = 3l \Rightarrow a + b = l\lambda\omega \Rightarrow a + b \equiv 0(\text{mod } \lambda) \text{ or},$$
$$a + b \equiv \pm 1(\text{mod } 3) \Rightarrow a + b = \pm 1 + 3l = \pm 1 + l\lambda\omega \Rightarrow a + b \equiv \pm 1(\text{mod } \lambda).$$

□

[8] $\xi = xi, \lambda = lambda, \rho = rho, \gamma = gamma$

[9] ω=omega

7.3 The Proof of the $n = 3$ Case

We are now equipped to prove the $n = 3$ case using complex numbers. This is the "hardest" proof we have met in this book and will be until we reach Chapter 16.

If we can prove we cannot have $\alpha^3 + \beta^3 + \gamma^3 = 0, \alpha \neq 0, \beta \neq 0, \gamma \neq 0$ in $k(\rho)$ then since the rational integers are also in $k(\rho)$, simply let $\alpha = x, \beta = y, \gamma = z$ to prove there are no solutions of $x^3 + y^3 + z^3 = 0$ in the integers.

Now any factor of two of α, β, γ in $\alpha^3 + \beta^3 + \gamma^3 = 0$ must by Lemma 8, page 30, be a factor of the third so we can cancel it out and we may suppose,

$$\alpha^3 + \beta^3 + \gamma^3 = 0 \text{ where } gcd(\alpha, \beta) = gcd(\beta, \gamma) = gcd(\alpha, \gamma) = 1.$$

We will precede the proof with three connected lemmas.

Lemma 49.
Let $\omega = a + b\rho$ be an algebraic integer in $k(\rho)$ and λ be the prime $1 - \rho$. If $\lambda \neq \omega$ then,

$$\omega^3 \equiv \pm 1 (\text{mod } \lambda^4) \Leftrightarrow \omega^3 = \pm 1 + \beta\lambda^4 \text{ for some } \beta \in k(\rho)$$

Proof. Since $\lambda \neq \omega$, then $\omega \neq 0 (\text{mod } \lambda)$.
By Lemma 48 page 68, ω is congruent to one of $0, 1, -1 (\text{mod } \lambda)$. Now $\lambda \neq \omega$ excludes $\omega \equiv 0 (\text{mod } \lambda)$, so $\omega \equiv \pm 1 (\text{mod } \lambda)$.
We can therefore choose $\alpha = \pm\omega$ so that $\alpha \equiv 1 (\text{ mod } \lambda) \Rightarrow \alpha = 1 + \beta\lambda$ for some $\beta \in k(\rho)$. Then,

$$\begin{aligned}
\pm(\omega^3 \mp 1) &= \alpha^3 - 1 \\
&= (\alpha - 1)(\alpha - \rho)(\alpha - \rho^2) \text{ by (7.2.3) of Note 6, page 64} \\
&= \beta\lambda(\beta\lambda + 1 - \rho)(\beta\lambda + 1 - \rho^2), \text{since } \alpha = 1 + \beta\lambda, \\
&= \beta\lambda(\beta\lambda + \lambda)(\beta\lambda + 1 - \rho^2), \text{since } \lambda = 1 - \rho, \\
&= \lambda^2\beta(\beta + 1)(\beta\lambda - \lambda\rho^2), \\
&\text{since } 1 - \rho^2 = (1 - \rho)(1 + \rho) = \lambda(1 + \rho) = -\lambda\rho^2 \text{ by Lemma 38, page 63} \\
&= \lambda^3\beta(\beta + 1)(\beta - 1 - \rho), \text{ again by Lemma 38}
\end{aligned}$$

So $\lambda^3 \mid \pm(\omega^3 \mp 1)$.
Now by Lemma 47, $\beta \equiv 0,\ 1$ or $-1 (\text{ mod } \lambda)$ so one of the three factors $\beta, \beta + 1, \beta - 1 - \rho$ is divisible by λ. This is so since the three alternatives are,

(a) $\beta \equiv 0 (\text{mod } \lambda) \Rightarrow \lambda | \beta$,

(b) $\beta \equiv -1 (\text{mod } \lambda) \Rightarrow \beta + 1 \equiv 0 (\text{mod } \lambda) \Rightarrow \lambda | \beta + 1$,

(c) $\beta \equiv 1 (\text{mod } \lambda) \Rightarrow \beta - 1 \equiv 0 (\text{mod } \lambda) \Rightarrow \lambda | \beta - 1 \Rightarrow \lambda | \beta - 1 - \lambda\rho^2$
Note we have added $-\lambda\rho^2$ since $\lambda | -\lambda\rho^2$ as well as $\lambda | \beta - 1$.

So, $\lambda^4 | \pm(\omega^3 \mp 1)$ and we have,

$$\pm(\omega^3 \mp 1) \equiv 0(\text{mod } \lambda^4) \Rightarrow \omega^3 \mp 1 \equiv 0(\text{mod } \lambda^4) \Rightarrow \omega^3 \equiv \pm 1(\text{mod } \lambda^4)$$

. □

Note 9. *In particular for any three $k(\rho)$ integers α, β, γ we have,*

$$\alpha^3 \equiv \pm 1(\text{mod } \lambda^4), \beta^3 \equiv \pm 1(\text{mod } \lambda^4), \gamma^3 \equiv \pm 1(\text{mod } \lambda^4)$$

if none of α, β, γ are divisible by λ. We use this in the next lemma.

Lemma 50.
If $\alpha^3 + \beta^3 + \gamma^3 = 0, \alpha \neq 0, \beta \neq 0, \gamma \neq 0$ then one of α, β, γ is divisible by λ.

Proof. Suppose $\alpha^3 + \beta^3 + \gamma^3 = 0$ and none of α, β, γ are divisible by λ. Then, by Lemma 48[10],

$$0 = \alpha^3 + \beta^3 + \gamma^3 \equiv \pm 1 \pm 1 \pm 1(\text{mod } \lambda^4) \equiv \pm 1(\text{mod } \lambda^4) \textit{ or } \pm 3(\text{mod } \lambda^4)$$

We cannot have $0 \equiv \pm 1(\text{mod } \lambda^4)$ since for some[11] $\delta \in k(\rho)$,

$$0 \equiv \pm 1(\text{mod } \lambda^4) \Rightarrow \delta\lambda^4 \pm 1 = 0 \Rightarrow \delta\lambda^4 = \pm 1 \Rightarrow N(\delta\lambda^4) = N(\pm 1) = 1$$

which is a contradiction, since $N\lambda = 3$, (as we saw in Lemma 44, page 66), so that $N(\delta\lambda^4) > 3^4 = 81$.
Similarly we cannot have $0 \equiv \pm 3(\text{mod } \lambda^4)$ since $\delta\lambda^4 \pm 3 = 0 \Rightarrow N(\delta\lambda^4) = N(\pm 3) = 9$ but $N(\delta\lambda^4) > 81$ as we saw above.
We conclude if $\alpha^3 + \beta^3 + \gamma^3 = 0, \alpha \neq 0, \beta \neq 0, \gamma \neq 0$ then one of α, β, γ is divisible by λ. □

What we need to prove.
We may therefore suppose $\lambda | \gamma$ and that $\gamma = \lambda^n \delta$ where $\lambda \nmid \delta$ and $n \geq 1$.
Then $\lambda \nmid \alpha$ and $\lambda \nmid \beta$ and we have to prove the impossibility of $\alpha^3 + \beta^3 + \lambda^{3n}\delta^3 = 0$ where $gcd(\alpha, \beta) = 1, n \geq 1, \lambda \nmid \alpha, \lambda \nmid \beta, \lambda \nmid \delta$.
We will assume there is a solution to $\alpha^3 + \beta^3 + \epsilon\lambda^{3n}\delta^3 = 0$ where ϵ is any unity and prove a contradiction. Putting $\epsilon = 1$ gives our result. We prove this more generally in the next two lemmas.

Lemma 51.
If there is a solution in the algebraic integers[12] of $k(\rho)$ to

$$\alpha^3 + \beta^3 + \epsilon\lambda^{3n}\delta^3 = 0$$

where $gcd(\alpha, \beta) = 1, n \geq 1, \lambda \nmid \alpha, \lambda \nmid \beta, \lambda \nmid \delta$ and ϵ is any unity, then $n \geq 2$.

[10] Note $\pm 1 \pm 1 \pm 1$ cannot be ± 2 since if any term is of opposite sign to the other two then it cancels with one of them leaving only the third equal to ± 1.

[11] $\delta = delta$

[12] $\alpha = alpha, \beta = beta, \gamma = gamma, \xi = xi, \epsilon = epsilon, \xi = xi, \delta = delta, \lambda = lambda$

Proof. Suppose there is a solution to $\alpha^3 + \beta^3 + \epsilon\lambda^{3n}\delta^3 = 0$. By Lemma 50 page 70,

$$\begin{aligned} -\epsilon\lambda^{3n}\delta^3 &= \alpha^3 + \beta^3 \equiv \pm 1 \pm 1 (\text{mod } \lambda^4) \\ \Rightarrow \epsilon\lambda^{3n}\delta^3 &\equiv \pm 2 (\text{mod } \lambda^4) \textit{ or } \epsilon\lambda^{3n}\delta^3 \equiv 0 (\text{mod } \lambda^4) \end{aligned}$$

The first case $\epsilon\lambda^{3n}\delta^3 \equiv \pm 2(\text{mod } \lambda^4)$ is impossible since, by Lemma 46, page 66, $\lambda \not| 2$ which would be required since,

$$\begin{aligned} &\epsilon\lambda^{3n}\delta^3 \equiv \pm 2(\text{mod } \lambda^4) \\ &\Rightarrow \epsilon\lambda^{3n}\delta^3 = \pm 2 + \xi\lambda^4, \ \xi \in k(\rho) \\ &\Rightarrow \lambda(-\xi\lambda^3 + \epsilon\lambda^{3n-1}\delta^3) = \pm 2 \\ &\Rightarrow \lambda | 2. \end{aligned}$$

Hence, $\epsilon\lambda^{3n}\delta^3 \equiv 0(\text{ mod } \lambda^4) \Rightarrow \epsilon\lambda^{3n}\delta^3 = \xi\lambda^4$ for some $\xi \in k(\rho)$, and since $\lambda \not| \delta$ and $\lambda^4 | \lambda^{3n}$ then n is at least 4 and certainly $n \geq 2$. □

We have shown that a solution to $\alpha^3 + \beta^3 + \epsilon\lambda^{3n}\delta^3 = 0$ requires $n \geq 2$. We continue to focus on values of n, seeking to apply the method of infinite descent.

Lemma 52.
If there is a solution in the algebraic integers of $k(\rho)$ to

$$\alpha^3 + \beta^3 + \epsilon\lambda^{3n}\delta^3 = 0$$

for $n = m > 1$ then there is a solution for $n = m - 1$, that is,

$$\phi^3 + \psi^3 + \epsilon_1\lambda^{3m-3}\theta^3 = 0$$

for some[13] *$\phi, \psi, \theta \in k(\rho)$ and ϵ_1 a unity in $k(\rho)$.*

Proof. Suppose there is a solution in the algebraic integers of $k(\rho)$ to

$$\alpha^3 + \beta^3 + \epsilon\lambda^{3n}\delta^3 = 0.$$

where we again may suppose these three terms are co-prime and specifically $\lambda \not| \beta$. Now by Lemma 38 on page 63,

$$(\alpha + \rho\beta)(\alpha + \rho^2\beta) = \alpha^2 + (\rho + \rho^2)\alpha\beta + \rho^3\beta = \alpha^2 - \alpha\beta + \beta^2 \tag{7.3.1}$$

Then we have[14],

$$\begin{aligned} \alpha^3 + \beta^3 + \epsilon\lambda^{3n}\delta^3 &= 0 \\ \Rightarrow -\epsilon\lambda^{3n}\delta^3 &= \alpha^3 + \beta^3 \\ &= (\alpha + \beta)(\alpha^2 - \alpha\beta + \beta^2) \\ &= (\alpha + \beta)(\alpha + \rho\beta)(\alpha + \rho^2\beta) \text{ by (7.3.1)} \\ &= AB\Delta \text{ say.} \end{aligned}$$

[13] $\phi = phi, \psi = psi(sigh), \theta = theta, \lambda = lambda, \epsilon = epsilon$

[14] A, B, Δ are the upper case letters of α, β and δ.

Using Lemma 38 on page 63 and putting $\lambda = 1 - \rho$ the differences of the factors are,

$$\begin{aligned}
A - B &= \alpha + \beta - \alpha - \rho\beta = \beta(1-\rho) = \beta\lambda \\
A - \Delta &= \alpha + \beta - \alpha - \rho^2\beta = \beta(1-\rho)(1+\rho) = \beta\lambda\rho^2 \\
B - \Delta &= \alpha + \rho\beta - \alpha - \rho^2\beta = \rho\beta(1-\rho) = \beta\lambda\rho
\end{aligned}$$

Each of these differences is divisible by λ but not by λ^2 since $\lambda \nmid \beta$.
Since, by Lemma 51 on page 70 if there is a solution in the algebraic integers of $k(\rho)$ to $\alpha^3 + \beta^3 + \epsilon\lambda^{3m}\delta^3 = 0$ we have $m \geq 2$, then $3m > 3$ so since,

$$-\epsilon\lambda^{3m}\delta^3 = (\alpha+\beta)(\alpha+\rho\beta)(\alpha+\rho^2\beta) = AB\Delta, \tag{7.3.2}$$

means $AB\Delta$ is divisible by at least λ^4, the three factors,

$$A = (\alpha+\beta), B = (\alpha+\rho\beta), \Delta = (\alpha+\rho^2\beta)$$

cannot all be only divisible by just one λ. One of the factors must be divisible by λ^2. We may suppose it is $A = (\alpha+\beta)$ since if it were one of the other factors, we could replace β with one of its associates, either $\rho\beta$ or $\rho^2\beta$.

So let[15] $A = (\alpha+\beta) = \sigma\lambda^2, \sigma \in k(\rho)$. Then,

$$\begin{aligned}
&A - B = \alpha + \beta - \alpha - \rho\beta = \beta - \rho\beta = \beta(1-\rho) = \beta\lambda \\
&\Rightarrow \sigma\lambda^2 - B = \beta\lambda \\
&\Rightarrow B = \sigma\lambda^2 - \beta\lambda = \lambda(\sigma\lambda - \beta)
\end{aligned}$$

which implies B is divisible by λ but not by λ^2. The same argument applies to Δ being divisible by λ but not by λ^2.
We then have, from (7.3.1)

$$-\epsilon\lambda^{3m}\delta^3 = AB\Delta \tag{7.3.3}$$

that B and Δ cancel only one of the λ's so that A is divisible by λ^{3m-2}.
We then have[16],

$$A = (\alpha+\beta) = \lambda^{3m-2}\kappa_1 \tag{7.3.4}$$
$$B = (\alpha+\rho\beta) = \lambda\kappa_2 \tag{7.3.5}$$
$$\Delta = (\alpha+\rho^2\beta) = \lambda\kappa_3 \tag{7.3.6}$$

where none of the kappas $\kappa_1, \kappa_2, \kappa_3$ is divisible by λ.
We claim $\kappa_1, \kappa_2, \kappa_3$ are mutually prime.
First, if there is any σ such that $\sigma | \kappa_2$ and $\sigma | \kappa_3$ then σ also divides $\kappa_2 - \kappa_3$ and since,

$$\lambda\kappa_2 - \lambda\kappa_3 = \alpha + \rho\beta - \alpha - \rho^2\beta = \rho\beta(1-\rho) = \beta\rho\lambda$$

[15] *σ = sigma, α = alpha, β = beta, ρ = rho, A = Alpha, B = Beta, Δ = Delta.*

[16] *κ = kappa*

then by cancellation $\kappa_2 - \kappa_3 = \rho\beta$ which means, if $\sigma|\kappa_2 - \kappa_3$, that $\sigma|\beta$.
Also, if $\sigma|\kappa_2$ and $\sigma|\kappa_3$, this would mean σ divides $\rho\kappa_3 - \rho^2\kappa_2$. But,

$$\begin{aligned}\lambda\rho\kappa_3 - \lambda\rho^2\kappa_2 &= \Delta\rho - \rho^2 B\\ &= \rho(\alpha + \rho^2\beta) - \rho^2(\alpha + \rho\beta)\\ &= \rho\alpha + \rho^3\beta - \rho^2\alpha - \rho^3\beta\\ &= \rho\alpha(1-\rho)\\ &= \rho\alpha\lambda\end{aligned}$$

so that $\rho\kappa_3 - \rho^2\kappa_2 = \rho\alpha$ showing $\sigma|\alpha$ and therefore both α and β which is not allowed as $gcd(\alpha, \beta) = 1$. Hence σ is a unity and $gcd(\kappa_2, \kappa_3) = 1$. Similarly, $gcd(\kappa_1, \kappa_2) = 1$ and $gcd(\kappa_1, \kappa_3) = 1$.
Substituting from (7.3.3), (7.3.4) and (7.3.5) into (7.3.2) we have,

$$\begin{aligned}&-\epsilon\lambda^{3m}\delta^3 = AB\Delta = \lambda^{3m-2}\kappa_1 \times \lambda\kappa_2 \times \lambda\kappa_3\\ &\Rightarrow -\epsilon\delta^3 = \kappa_1\kappa_2\kappa_3\end{aligned}$$

Hence each of $\kappa_1, \kappa_2, \kappa_3$ is an associate of a cube, say[17] $\kappa_1 = \epsilon_1\theta^3, \kappa_2 = \epsilon_2\phi^3$ and $\kappa_3 = \epsilon_3\psi^3$,so that,

$$A = \alpha + \beta = \lambda^{3m-2}\kappa_1 = \epsilon_1\lambda^{3m-2}\theta^3 \tag{7.3.7}$$
$$B = \alpha + \rho\beta = \lambda\kappa_2 = \epsilon_2\lambda\phi^3 \tag{7.3.8}$$
$$\Delta = \alpha + \rho^2\beta = \lambda\kappa_3 = \epsilon_3\lambda\psi^3 \tag{7.3.9}$$

where θ, ϕ, ψ have no common factors and are not divisible by λ and $\epsilon_1, \epsilon_2, \epsilon_3$ are unities.
Since by Lemma 38 on page 63, $1 + \rho + \rho^2 = 0$, it follows that multiplying by $\alpha + \beta$ gives,

$$\begin{aligned}0 &= (1 + \rho + \rho^2)(\alpha + \beta)\\ &= \alpha + \beta + \rho(\alpha + \beta) + \rho^2(\alpha + \beta)\\ &= \alpha + \beta + \rho\alpha + \rho^2\beta + \rho^2\alpha + \rho^4\beta\\ &\text{(where, given } \rho^3 = 1 \text{, we substituted } \rho^4\beta \text{ for } \rho\beta.)\\ &= \alpha + \beta + \rho(\alpha + \rho\beta) + \rho^2(\alpha + \rho^2\beta)\\ &= A + \rho B + \rho^2\Delta\end{aligned}$$

Substituting (7.3.6), (7.3.7) and (7.3.8) gives,

$$\begin{aligned}&\epsilon_1\lambda^{3m-2}\theta^3 + \epsilon_2\rho\lambda\phi^3 + \epsilon_3\rho^2\lambda\psi^3 = 0\\ \Rightarrow\ &\frac{\epsilon_1}{\epsilon_2\rho\lambda}\lambda^{3m-2}\theta^3 + \phi^3 + \frac{\epsilon_3\rho^2\lambda}{\epsilon_2\rho\lambda}\psi^3 = 0 \text{ (dividing by } \epsilon_2\rho\lambda)\\ \Rightarrow\ &\frac{\epsilon_1}{\epsilon_2\rho}\lambda^{3m-3}\theta^3 + \phi^3 + \frac{\epsilon_3\rho}{\epsilon_2}\psi^3 = 0\\ \Rightarrow\ &\phi^3 + \epsilon_4\psi^3 + \epsilon_5\lambda^{3m-3}\theta^3 = 0\end{aligned}$$

[17] $\theta = theta, \psi = psi(sigh), \phi = phi$

where $\epsilon_4 = \dfrac{\epsilon_3\rho^2}{\epsilon_2\rho}$ and $\epsilon_5 = \dfrac{\epsilon_1}{\epsilon_2\rho}$ are also unities as proved in Lemma 41.
Now $m \geq 2$, so $3m - 3 \geq 3$ and

$$\begin{aligned} \phi^3 + \epsilon_4\psi^3 &= -\epsilon_5\lambda^{3m-3}\theta^3 \\ \Rightarrow \phi^3 + \epsilon_4\psi^3 &\equiv 0(\text{mod } \lambda^2) \end{aligned}$$

(in fact λ^3.)
But $\lambda\nmid\phi$ and $\lambda\nmid\psi$, so by Lemma L49 page 69,

$$\begin{aligned} \phi^3 &\equiv \pm 1(\text{mod } \lambda^2) \\ \psi^3 &\equiv \pm 1(\text{mod } \lambda^2) \end{aligned}$$

(in fact λ^4.)
Hence,

$$\phi^3 + \epsilon_4\psi^3 \equiv 0(\text{mod } \lambda^2) \Rightarrow \pm 1 \pm \epsilon_4 \equiv 0(\text{mod } \lambda^2)$$

where ϵ_4 is $\pm 1, \pm\rho$ or $\pm\rho^2$.
But neither $\pm 1 \pm \rho$ nor $\pm 1 \pm \rho^2$ is divisible by λ^2 since each is a unity and therefore an associate of 1 or λ making division by λ^2 impossible.Therefore $\epsilon_4 = \pm 1$.
If $\epsilon_4 = 1$,

$$\theta^3 + \epsilon_4\psi^3 + \epsilon_5\lambda^{3m-3}\theta^3 = 0$$

is an equation of the type required.
If $\epsilon_4 = -1$, we replace ψ with $-\psi$ and

$$\theta^3 + \epsilon_4(-\psi)^3 + \epsilon_5\lambda^{3m-3}\theta^3 = 0$$

is an equation of the type required. □

Theorem 53. *(The $n = 3$ case)*
There are no solutions of $\alpha^3 + \beta^3 + \gamma^3 = 0, \alpha \neq 0, \beta \neq 0, \gamma \neq 0$ in $k(\rho)$.

Proof. If $\alpha^3 + \beta^3 + \gamma^3 = 0, \alpha \neq 0, \beta \neq 0, \gamma \neq 0$ is possible for any n then by Lemma 52, page 71, it is possible for $n - 1$, then again by the lemma for $n - 2$ and (eventually) for $n = 1$ which contradicts Lemma 51, page 70, which was,
" If there is a solution in the algebraic integers of $k(\rho)$ to

$$\alpha^3 + \beta^3 + \epsilon\lambda^{3n}\delta^3 = 0$$

where $gcd(\alpha, \beta) = 1, n \geq 1, \lambda\nmid\alpha, \lambda\nmid\beta, \lambda\nmid\delta$ and ϵ is any unity, then $n \geq 2$."
The contradiction proves there are no solutions of $\alpha^3 + \beta^3 + \gamma^3 = 0, \alpha \neq 0, \beta \neq 0, \gamma \neq 0$ in $k(\rho)$ and hence to $x^3 + y^3 = z^3$ in the integers by putting $\alpha = x + 0\rho$, etc. □

The argument is another example of the method of infinite descent.

Chapter 8

Postprandial Discussion: The General Case

Let us now discuss the general case of FLT, Fermat's Last Theorem. The trail that began with Pythagoras ends in the second half of the 20th century with Taniyama with Shimura, Frey, Ribet, Wiles and finally Taylor with Wiles.

Theorem 54. *(FLT: Wiles)*
There are no non-zero solutions of $x^n + y^n = z^n, x, y, z \neq 0,\ n \geq 3$ *in the integers.*

Proof. The proof is incredibly difficult but we can get a sense of it.

Elliptic curves are equations of the form,

$$y^2 = x^3 + ax^2 + bx + c,\ \ a, b, c \in \mathbb{Z}^+ \cup \{0\}$$

Gordon Frey[1], in 1986, completely transformed FLT into a problem about elliptic curves. He stated that if there is a solution $a^n + b^n = c^n$ to the Fermat equation $x^n + y^n = z^n$ for some exponent $n > 2$ then use it to construct the following (Frey) elliptic curve,

$$y^2 = x(x - a^n)(x + b^n) = g(x) \tag{8.0.1}$$

Now if f is a polynomial of degree k with $r_1, r_2, \ldots, r_k$ as all of its roots, then the discriminant $\Delta(f)$ of f is defined by,

$$\Delta(f) = \prod_{1 \leq i < j \leq k} (r_i - r_j)^2$$

[1] These comments are drawn from an article by Ezra Brown in "The College Mathematics Journal, Volume 31, May 2000."

If f is a monic polynomial[2] it turns out that $\Delta(f)$ is an integer. The three roots of the polynomial $g(x)$ on the right side of the Frey curve of (8.1.1) are $0, a^n, b^n$. Using the fact that for odd n,

$$a^n - (-b^n) = a^n + b^n = c^n,$$

we find,

$$\Delta(g) = (0 - a^n)^2(0 - (-b)^n)^2(a^n - (-b^n))^2 = (abc)^{2n}$$

Frey stated that an elliptic curve with such a discriminant cannot possibly be called modular (we need not define what that means) bringing the focus to the unproved Taniyama-Shimura conjecture.
The Taniyama-Shimura conjecture was that every single modular form could be matched with an elliptic curve. Frey argued that if the Taniyama-Shimura conjecture is proved to be correct and if his Frey elliptic curve can be proved to be non-modular, then you would have a contradiction from which you could conclude there is no such curve, that is, there is no such solution to a Fermat equation, there is no counterexample to Fermat's Last Theorem, and so Fermat's Last Theorem is true.
Wiles actually proved the Taniyama-Shimura conjecture. This sufficed to prove FLT according to the following argument:

1. If the Taniyama-Shimura conjecture can be proved to be true, then every elliptic curve must be modular.
2. If the Frey elliptic curve is not modular, then there can be no solutions to FLT.
3. Therefore, Fermat's Last Theorem is true.

In 1986 Ken Ribet proved Step 2, that Frey's elliptic curve is not modular.

In 1993 Andrew Wiles gave three lectures in a Cambridge symposium that appeared to prove the Taniyama-Shimura conjecture. An error was soon found, there was a crucial missing step.

In 1994, the crucial missing step was proved in "Ring Theoretic properties of certain Hecke algebras" by Richard Taylor and Andrew Wiles. On the same day, 25th October 1994, a second manuscript was released, "Modular elliptic curves and Fermat's Last Theorem" by Andrew Wiles.

The saga of Fermat's Last Theorem was over. □

[2] A polynomial $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, a_i \in \mathbb{Z}$ is monic if $a_n = 1$.

Part III

Shopping Excursion II - Calculus

The development of the theory of Calculus may be regarded as the single most important achievement in all of mathematics. It is like the discovery of the wheel in transportation or fire in food preparation.. Prior to its development we were limited to discrete approximations to our world. We had the numbers, we could count things, but we could not describe continuous events, a major deficiency since we live in a world of continuous change.

The development of Calculus took over 400 years spanning 1600 to 1900. It was initially slowed down by the absence of mass media of communication, specifically the printing press and publications not just in Latin. Letters between individuals are primitive technology compared with textbooks for the masses. The sharing of ideas is essential for the rapid development of our understanding of our universe. But, of course, sharing can lead to plagiarizing and stealing of ideas before the originator has fully promulgated them, and in the 400 year period there were instances of these and some major fights and skull-dougeries. Imagine if the developers had had the Internet, but that of course is Catch-22 since we would not have the Internet without Calculus!

The chief developers, depending on your point of view or nationality, were: Kepler, Descartes, Fermat, Pascal, Newton, Leibnitz, L'Hópital, Bernoulli, Taylor, Maclaurin, Euler, Agnesi, Lagrange, Gauss, Cauchy, Green, Stokes, Weierstrass, Riemann, Kovalesky, Lebesgue.

They are the masters we learn from.

Chapter 9

Calculus and Infinite Series

Many results in number theory require both differential and integral Calculus, results that took over 400 years to come to fruition. We shall take the shortest path, proving only what we need, leaving aside a wealth of rich results for your further investigation. The final result we prove here is usually found about the end of the second semester of the standard three semester undergraduate course in Calculus.

9.1 What is Calculus?

Calculus may be defined as the study of limits.
Let us consider a famous ancient paradox attributed to Zeno. He argued that an arrow shot at a target will never reach that target, no matter the distance involved. Suppose the target is 2 chains away.
First the arrow must travel half the distance or 1 chain with $1 = \dfrac{1}{2^0}$ chains to go.
Second the arrow must travel half the remaining 1 chain with $\dfrac{1}{2} = \dfrac{1}{2^1}$ chains to go.
Third the arrow must travel half the remaining $\dfrac{1}{2}$ chain with $\dfrac{1}{4} = \dfrac{1}{2^2}$ chains to go.
Fourth the arrow must travel half the remaining $\dfrac{1}{4}$ chain with $\dfrac{1}{8} = \dfrac{1}{2^3}$ chains to go.
Each time, the arrow continues to travel half the remaining distance $\dfrac{1}{2^n}$ with $\dfrac{1}{2^{n+1}}$ to go.
There will always be half the remaining distance to cover, ergo, the arrow will never reach the target.

The paradox results from the attempt to use discrete mathematics to describe continuous motion. We need the concept of infinity.
Since the arrow does reach the target, that is, the arrow does actually travel 2 chains, then we must agree that, $1 + \dfrac{1}{2^1} + \dfrac{1}{2^2} + \dfrac{1}{2^3} + \ldots = 2$, where the left side contains an

infinite number of discrete terms all of the form $\dfrac{1}{2^n}, n = 0, 1, 2, 3, \ldots$. Mathematically we say, "in the limit as n approaches infinity" that ,

$$1 + \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots + \frac{1}{2^n} + \ldots = 2$$

or, in shorthand,

$$\lim_{n\to\infty} \sum_{k=0}^{n} \frac{1}{2^k} = \lim_{n\to\infty} \left(1 + \frac{1}{2^1} + \frac{1}{2^2} + \ldots + \frac{1}{2^n}\right) = 2$$

The study of limits, called Calculus, enables us to model the world of continuous motion, or continuity in general.

9.2 Branches of Calculus

The first branch is differentiation. For any function f of x, such that $y = f(x)$, this begins with finding the slope or gradient m of the tangent to its graph at any point See Figure 1.

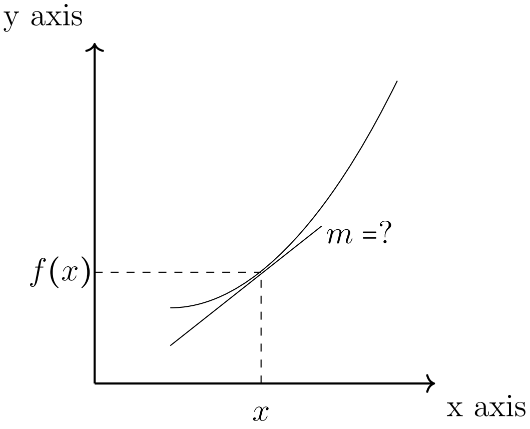


Figure 1. Differentiation

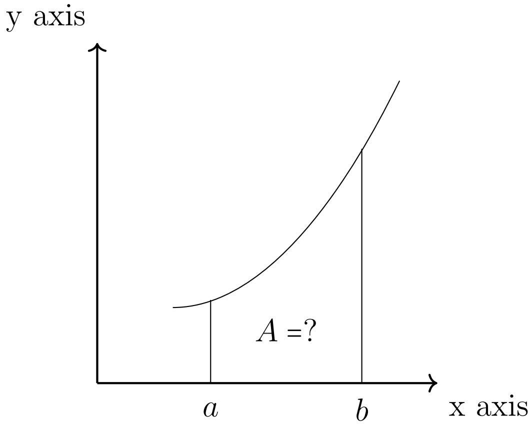


Figure 2. Integration

The second is integration. This begins with the calculation of the area A between the graph of a function (a curve) and an interval $[a, b]$ on the x−axis. See Figure 2 above.

In each case, we will find the solution requires the concept of a limit.

9.3 Differentiation

9.3.1 Slope or gradient of a line

Definition 26. *slope or gradient*
The slope or gradient m of the line joining the two points $P_1(x_1, y_1), P_2(x_2, y_2)$ on the Cartesian plane is defined as[1]*, (see Figure 3),*

$$m = \frac{\textit{change in } y}{\textit{change in } x} = \frac{\Delta y}{\Delta x} = \frac{y_2 - y_1}{x_2 - x_1}$$

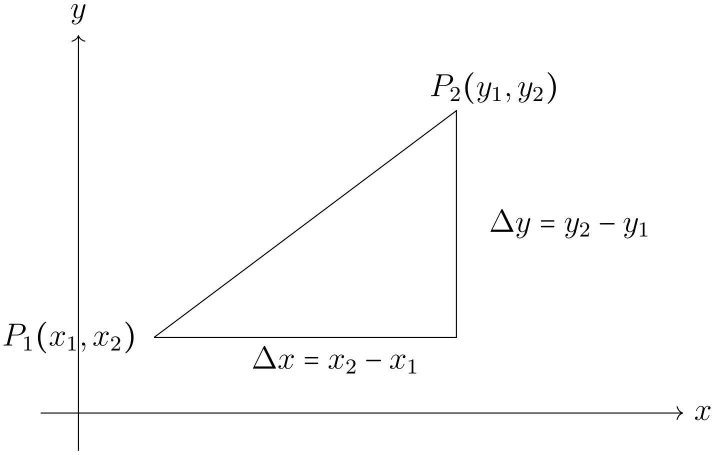


Figure 3

9.3.2 Slope of Tangent Line to a Curve

Intuitively a tangent line to a curve at a point is a line that "touches" the curve at that point. But what do we mean by "touches"? How can we draw a tangent?
We know that a line is uniquely specified if we are given two points on it. A tangent line to $y = f(x)$ at $(x, f(x))$ on the curve "touches" the curve at a point $P(x, f(x))$. What can we use for a second point Q?
We continue to use our intuition. If we choose the second point Q to be a point on the curve that is "close" to $P(x, f(x))$, say $Q(x+h, f(x+h))$ with h very small, then we can find the slope m_{sec} of the secant line PQ joining these two points on the curve. It is, (see Figure 4),

$$m_{sec} = \frac{y_2 - y_1}{x_2 - x_1} = \frac{f(x+h) - f(x)}{x + h - h} = \frac{f(x+h) - f(x)}{h}$$

[1] We use the uppercase Greek letter Delta, Δ, for "change in"

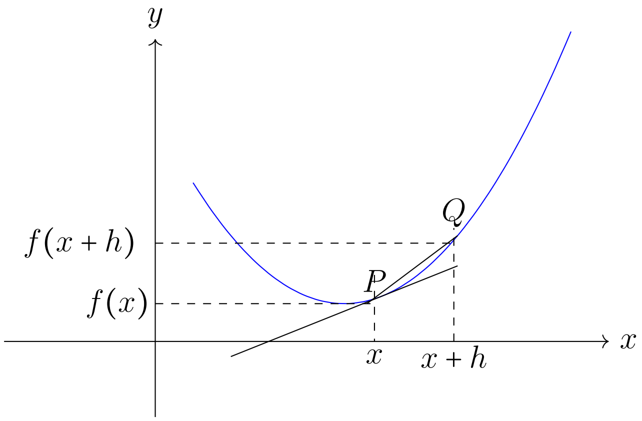


Figure 4

We easily see from Figure 4 that $m_{tan} \approx m_{sec}$ where m_{tan} is the slope or gradient of the tangent line at $(x, f(x))$ and that we can improve the approximation by taking h smaller and smaller.

Indeed, if h progressively approaches 0, just as the remaining distance for Zeno's arrow approached zero, we are intuitively sure that $m_{tan} = \lim_{h \to 0} m_{sec}$.

We use the two notations$f'(x)$ or $\dfrac{dy}{dx}$ for the slope of the tangent line to the curve $y = f(x)$ at any point $(x, f(x)) = (x, y)$ or simply the gradient of the curve at $(x, f(x))$ which we label the derivative of $f(x)$ at the point.

The two notations reflect the parallel development of Calculus in different countries, specifically in England by Newton and in Germany by Leibnitz. We then define the gradient of the tangent line at any point as follows.

Definition 27. *derivative of a function at a point*
We define the derivative $f'(x)$ or $\dfrac{dy}{dx}$ of a function $y = f(x)$ at the point $(x, f(x))$ by,

$$\begin{aligned} For\ m_{sec} &= \frac{f(x+h) - f(x)}{h} \ \ by\ \ f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \\ For\ m_{sec} &= \frac{\Delta y}{\Delta x} \qquad\qquad by \qquad \frac{dy}{dx} = \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x} \end{aligned}$$

provided the limit exists.
We call $f'(x) = \dfrac{dy}{dx}$ the **derivative** *of $y = f(x)$ with respect to x. If the limit does exist, we say $y = f(x)$ is* **differentiable** *at $(x, f(x)$. We interpret $f'(x)$ or $\dfrac{dy}{dx}$ as the gradient of the tangent to $f(x)$ at the point $(x, f(x))$.*

Example 34. *Consider $f(x) = x^2$.*

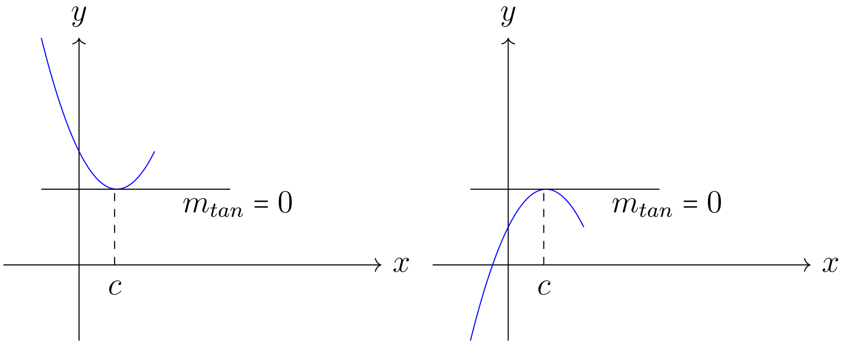
$$\begin{aligned} f'(x) &= \lim_{h\to 0} \frac{f(x+h) - f(x)}{h} \\ &= \lim_{h\to 0} \frac{(x+h)^2 - x^2}{h} \\ &= \lim_{h\to 0} \frac{\cancel{x^2} + 2xh + h^2 - \cancel{x^2}}{h} \\ &= \lim_{h\to 0}(2x+h) \\ &= 2x \qquad\qquad \diamond \end{aligned}$$

Example 35. *For example the derivative of $y = x^2$ at $x = 3$ is given by $f'(x) = 2x \Rightarrow f'(3) = 2 \times 3 = 6$.* $\diamond$

Note 10.

1. *$f'(x)$is a function. A we saw in the above example, by substituting values of x we can find the value of the derivative or the gradient of the curve at any value of x in the domain of $f(x)$.*

2. *The value/s of x for which $f'(x) = 0$ give us the point/s on the curve where the tangent is flat or $m_{tan} = 0$. For a parabola this point is the vertex and is either a maximum point of the graph or a minimum point. See Figure 5.*



Minimum at $x = c$ *Maximum at $x = c$*

Figure 5

9.3.3 The derivative of $y = f(x)$ at $x = a$

We can find the derivative of $y = f(x)$ at $x = a$ by first finding the function $f'(x)$ and then substituting $x = a$. We can also proceed more directly by using Figure 6.

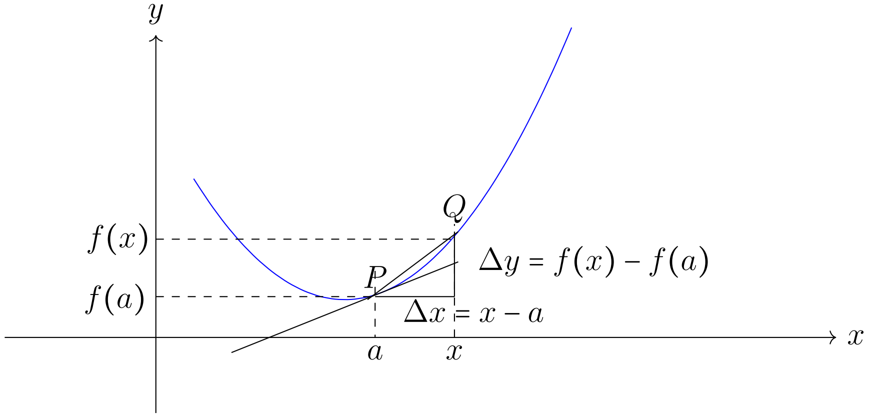


Figure 6

To find the gradient of the curve $y = f(x)$ at $P(a, f(a)$ we pick any other point x on the x−axis that is close to a for the other end $Q(x, f(x))$ of the secant and then we need x to approach a so the secant approaches the tangent line at P. Then, from the diagram,

$$f'(a) = \lim_{x \to a} \frac{f(x) - f(a)}{x - a}$$

Example 36. *The gradient of the curve $y = x^3$ at $x = 2$ is given by,*

$$\begin{aligned} f'(2) &= \lim_{x \to 2} \frac{f(x) - f(2)}{x - 2} \\ &= \lim_{x \to 2} \frac{x^3 - 2^3}{x - 2} \\ &= \lim_{x \to 2} \frac{\cancel{(x-2)}(x^2 + 2x + 4)}{\cancel{x - 2}} \\ &= 12 \end{aligned}$$

9.3.4 Rules of Differentiation

Theorem 55. *Constant Rule.*

$$\frac{d}{dx}(c) = 0 \textit{ where } c \in \mathbb{R} \textit{ or } c \textit{ is a constant.}$$

Proof. Let $f(x) = c$. Then,

$$\begin{aligned} f'(x) &= \lim_{h \to 0} \frac{f(x + h) - f(x)}{h} \\ &= \lim_{h \to 0} \frac{c - c}{h} \\ &= 0 \end{aligned}$$

□

Example 37. $\dfrac{d}{dx}(6) = 0$

Theorem 56. *Power Rule.*

$$\frac{d}{dx}(x^n) = nx^{n-1}, n \in \mathbb{N}.$$

In particular $\dfrac{d}{dx}(x) = 1$.

Proof. Note $(x-a)(x^{n-1} + x^{n-2}a + x^{n-3}a^2 + \ldots + xa^{n-2} + a^{n-1}) = x^n - a^n$. Let $f(x) = x^n$. Then,

$$\begin{aligned} f'(a) &= \lim_{x\to a} \frac{f(x)-f(a)}{x-a} \\ &= \lim_{x\to a} \frac{x^n - a^n}{x-a} \\ &= \lim_{x\to a} \overbrace{x^{n-1} + x^{n-2}a + \ldots + a^{n-2}x + a^{n-1}}^{n\ terms} \\ &= na^{n-1} \end{aligned}$$

In general, by putting $x = a$ we have $\dfrac{d}{dx}(x^n) = nx^{n-1}$. □

Example 38. $\dfrac{d}{dx}(x^3) = 3x^2$

Theorem 57. *Sum Rule*[2].

$$\frac{d}{dx}(f(x) + g(x) + h(x) + \ldots) = f'(x) + g'(x) + h'(x) + \ldots.$$

Proof. Let $y = f(x) + g(x)$. Adding more terms such as $h(x)$ is done by the same proof.

$$\begin{aligned} \frac{dy}{dx} &= \frac{d}{dx}(f(x) + g(x)) \\ &= \lim_{h\to 0} \frac{[f(x+h) + g(x+h)] - [f(x) + g(x)]}{h} \\ &= \lim_{h\to 0} \frac{f(x+h) - f(x)}{h} + \lim_{h\to 0} \frac{g(x+h) - g(x)}{h} \\ &= f'(x) + g'(x) \end{aligned}$$

□

[2] In this proof we assume the lemma $\lim\limits_{h\to 0}(F+G) = \lim\limits_{h\to 0} F + \lim\limits_{h\to 0} G$. This lemma and others concerning the theory of limits we will not prove.

Example 39. $\dfrac{d}{dx}(x^4 + x^3) = 4x^3 + 3x^2$

Theorem 58. *Constant Multiple Rule.*

$$\frac{d}{dx}(cf(x)) = cf'(x), \ \ c \in \mathbb{R}$$

Proof. Let $y = cf(x)$. Then,

$$\begin{aligned}\frac{d}{dx}(cf(x)) &= \lim_{h\to 0} \frac{cf(x+h) - cf(x)}{h} \\ &= c\lim_{h\to 0} \frac{f(x+h) - f(x)}{h} \\ &= cf'(x)\end{aligned}$$

Note a constant c can be extracted from a limit because it is unaffected by $h \to 0$. □

Example 40. $\dfrac{d}{dx}(3x^2 + 4x + 1) = 3 \times 2x + 4 \times 1 + 0 = 6x + 4$

Theorem 59. *Product Rule.*

Provided $f(x), g(x)$ are both differentiable[3]*,*

$$\frac{d}{dx}(f(x) \cdot g(x)) = f(x)g'(x) + g(x)f'(x)$$

Proof. Let $y = f(x)g(x)$. In what follows we add and subtract the same term and then form two limits, again extracting a common term. Then,

$$\begin{aligned}\frac{d}{dx}(f(x)g(x)) &= \lim_{h\to 0} \frac{f(x+h)g(x+h) - f(x)g(x)}{h} \\ &= \lim_{h\to 0} \frac{f(x+h)g(x+h) - f(x)g(x+h) + f(x)g(x+h) - f(x)g(x)}{h} \\ &= \lim_{h\to 0} \frac{f(x+h)g(x+h) - f(x)g(x+h)}{h} + \lim_{h\to 0} \frac{f(x)g(x+h) - f(x)g(x)}{h} \\ &= \lim_{h\to \ 0} g(x+h) \lim_{h\to 0} \frac{f(x+h) - f(x)}{h} + f(x) \lim_{h\to 0} \frac{g(x+h) - g(x)}{h} \\ &= g(x)f'(x) + f(x)g'(x)\end{aligned}$$

□

Example 41. $\dfrac{d}{dx}(x^3 \cdot x^4) = x^3(4x^3) + x^4(3x^2) = 7x^6$ *as expected for* $\dfrac{d}{dx}(x^7)$.

[3] Note $f'(x)$ and $\dfrac{dy}{dx}$ both mean the derivative of $y = f(x)$ at x.

Theorem 60. *Quotient Rule.*

Provided $f(x), g(x)$ are both differentiable and $g(x) \neq 0$,

$$\frac{d}{dx}\left(\frac{f(x)}{g(x)}\right) = \frac{g(x)f'(x) - f(x)g'(x)}{[g(x)]^2}$$

Proof. Let $q(x) = \dfrac{f(x)}{g(x)} \Rightarrow f(x) = q(x)g(x)$. By the Product Rule, Theorem 59,

$$\begin{aligned} f'(x) &= g'(x)q(x) + q'(x)g(x) \\ \Rightarrow q'(x) &= \frac{f'(x) - g'(x)q(x)}{g(x)} \\ &= \frac{f'(x) - g'(x)\dfrac{f(x)}{g(x)}}{g(x)} \\ &= \frac{g(x)f'(x) - f(x)g'(x)}{[g(x)]^2} \end{aligned}$$

□

Example 42.

$$\begin{aligned} \frac{d}{dx}\left(\frac{x^2}{x-1}\right) &= \frac{(x-1)\cdot 2x - x^2(1-0)}{(x-1)^2} \\ &= \frac{2x^2 - 2x - x^2}{(x-1)^2} \\ &= \frac{x^2 - 2x}{(x-1)^2} \qquad \diamond \end{aligned}$$

Theorem 61. *Extended Power Rule.*

$$f(x) = x^{-n} \Rightarrow f'(x) = -nx^{-n-1} = \frac{-n}{x^{n+1}}$$

Proof. Let $f(x) = x^{-n}$. Then, using the Quotient Rule, Theorem 60,

$$\frac{d}{dx}(x^{-n}) = \frac{d}{dx}\left(\frac{1}{x^n}\right) = \frac{x^n \times 0 - (1)(nx^{n-1})}{x^{2n}} = -nx^{-n-1}$$

□

Example 43. $\dfrac{d}{dx}\left(\dfrac{1}{x^3}\right) = \dfrac{d}{dx}(x^{-3}) = -3x^{-4} = -\dfrac{3}{x^4}$

Note 11. *In other words for all $x \in \mathbb{Z}$ the power rule is simply "put the power down in front and lower the power by 1."*

Theorem 62. *Chain Rule*
If $y = f(u)$ and $u = g(x)$ the composite function $y = f(g(x))$ has derivative,

$$\frac{dy}{dx} = \frac{dy}{du} \cdot \frac{du}{dx} \text{ or } \frac{df(g(x))}{dg(x)} \cdot \frac{dg(x)}{dx}$$

Proof. (Outline only)
Multiplying numerator and denominator by Δu gives $\frac{\Delta y}{\Delta x} = \frac{\Delta y}{\Delta u} \cdot \frac{\Delta u}{\Delta x}$.
Now if $u = g(x)$ then as $\Delta x \to 0$ we consequently have $\Delta u \to 0$, and if $y = f(u)$ then as $\Delta u \to 0$ we consequently have $\Delta y \to 0$. So $\Delta x \to 0, \Delta u \to 0$ and $\Delta y \to 0$ all occcur together. Hence,

$$\begin{aligned} \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x} &= \lim_{\Delta u \to 0} \frac{\Delta y}{\Delta u} \cdot \lim_{\Delta x \to 0} \frac{\Delta u}{\Delta x} \\ \Rightarrow \frac{dy}{dx} &= \frac{dy}{du} \cdot \frac{du}{dx} \\ \Leftrightarrow \frac{dy}{dx} &= \frac{df(g(x))}{dg(x)} \cdot \frac{dg(x)}{dx} \end{aligned}$$

□

Example 44. *Let us differentiate $y = (x^2 + 1)^6$*
We can write $y = u^6, u = x^2 + 1$ and use,

$$\frac{dy}{dx} = \frac{dy}{du} \cdot \frac{du}{dx} = 6u^5 \cdot 2x = 12x(x^2 + 1)^5,$$

or we can say,

$$\frac{dy}{dx} = \frac{d(x^2 + 1)^6}{d(x^2 + 1)} \cdot \frac{d(x^2 + 1)}{dx} = 6(x^2 + 1)^5 \cdot (2x) = 12x(x^2 + 1)^5 \qquad \diamond$$

9.4 Antiderivatives

Definition 28. *antiderivative*
F is the antiderivative of f on the interval (a, b) if $F'(x) = f(x)$ for all x in (a, b).

Notation 2. *$\int f(x)dx$ means the antiderivative of the function with respect to the variable. It is the reverse operation of $\frac{d}{dx}(f(x))$ which means the derivative of the function $f(x)$ with respect to the variable x. We call $\int f(x)dx$ the indefinite integral of $f(x)$ with respect to the variable x.*
We call $f(x)$ the integrand.
We call x the variable of the integration.

9.4.1 Family of Antiderivatives

We know,

$$\frac{d}{dx}(F(x)+c) = \frac{d}{dx}(F(x)) + 0 = \frac{d}{dx}(F(x)).$$

Provided we can find a single antiderivative, $F(x)$, there is therefore not just one but a family of antiderivatives of any function $f(x)$ given by $F(x)+c$ where c is any constant, that is $c \in \mathbb{R}$.
Thus for any function $f(x)$, given we know a function $F(x)$ such that $F'(x) = f(x)$, then $\int f(x)\ dx = F(x) + c, c \in \mathbb{R}$ so the antiderivative is indefinite and we call it an indefinite integral.

Definition 29. *indefinite integral*
If $\frac{d}{dx}F(x) = f(x)$, *we have* $\int f(x)\ dx = F(x) + c, c \in \mathbb{R}$ *and we call* $F(x)+c$ *the indefinite integral of* $f(x)$ *with respect to* x.

Example 45. *Let's find the antiderivative of* $2x$ *with respect to* x.
We know $\frac{d}{dx}(x^2) = 2x$. *Then* $\int 2x\ dx = x^2 + c, c \in \mathbb{R}$.

Word of Warning
In problems such as that of the previous example, we almost always get a little sloppy with our notation and mathematical language and simply say "find the integral of $2x$" or "integrate $2x$" when we really mean "find the indefinite integral of $2x$ with respect to x." As we will soon see, integration is actually a very different concept.

9.4.2 Rules for Indefinite Integration

The rules for indefinite integration are simply the reverse of the rules for differentiation. The first theorem illustrates this clearly.

Theorem 63. *Power Rule*

$$\int x^n\ dx = \frac{1}{n+1}x^{n+1} + c, n \neq -1$$

Proof. By Theorem 56 on page 85,

$$\frac{d}{dx}\left(\frac{1}{n+1}x^{n+1} + c\right) = \left(\frac{1}{n+1}\right) \cdot (n+1) \cdot x^{n+1-1} + 0 = x^n$$

□

Note 12. *In words the power rule is "increase the power of* x *by 1 and divide by this new power."*
Of course $n = -1$ *must be excluded but we will deal with this later.*

Example 46. $\int x^3 \; dx = \frac{x^4}{4} + c.$

Example 47. $\int \frac{1}{x^3} \; dx = \int x^{-3} \; dx = \frac{x^{-2}}{-2} + c = -\frac{1}{2x^2} + c.$

In a similar fashion we have the theorems,

a $\int (f(x) + g(x)) \; dx = \int f(x) \; dx + \int \; g(x) \; dx$

b $\int cf(x) \; dx = c\int f(x) \; dx$

We reverse the product rule as follows. We can use this formula or rule called integration by parts to integrate the product of two unlike functions. We will use this theorem many times in what follows.

Theorem 64. *Integration by Parts*

$$\int u\frac{dv}{dx} \; dx = uv - \int v\frac{du}{dx} \; dx$$

Proof. Let $u = u(x)$ and $v = v(x)$ be two functions of x. If we integrate the product rule, Theorem 59, page 86, for differentiation namely,

$$\begin{aligned} \frac{d(uv)}{dx} \; dx &= u\frac{dv}{dx} + v\frac{du}{dx} \\ \Leftrightarrow u\frac{dv}{dx} &= \frac{d(uv)}{dx} - v\frac{du}{dx} \end{aligned}$$

we have,

$$\begin{aligned} \int u\frac{dv}{dx\;dx} &= \int \frac{d(uv)}{dx} \; dx - \int v\frac{du}{dx} \; dx \\ \Rightarrow \int u\frac{dv}{dx} \; dx &= uv - \int v\frac{du}{dx} \; dx \end{aligned}$$

□

Example 48. *Suppose we want to integrate* $\int x \cdot x^3 \; dx.$

Obviously the answer is given by $\int x \cdot x^3 \; dx = \int x^4 dx = \frac{x^5}{5} + c.$

But let's verify the integration by parts rule.

It says if we put $u = x \Rightarrow \frac{du}{dx} = 1$ *and also put* $\frac{dv}{dx} = x^3 \Rightarrow v = \frac{x^4}{4}$ *in*

$\int u\frac{dv}{dx}\ dx = uv - \int v\frac{du}{dx}\ dx$, *we obtain,*

$$\begin{aligned}\int x\cdot x^3\ dx &= x\cdot\frac{x^4}{4} - \int 1\cdot\frac{x^4}{4}\ dx\\ &= \frac{x^5}{4} - \frac{x^5}{20}\\ &= \frac{x^5}{5} + c. \qquad \diamond\end{aligned}$$

Note we are dealing with an indefinite integral so we add on a constant c *at the end.*

Finally, we can reverse the chain rule $\frac{dy}{dx} = \frac{dy}{du}\cdot\frac{du}{dx}$ by identifying the u function and using,

$$\int\frac{dy}{dx}\ dx = \int\frac{dy}{du}\cdot\frac{du}{dx}\ dx \Rightarrow \int\frac{dy}{du}\cdot\frac{du}{dx}\ dx = y$$

Example 49. *To find* $\int(x^4+3x)^6(4x^3+3)\ dx$ *we let* $u = x^4+3x$ *so that* $\frac{du}{dx} = 4x^3+3 \Rightarrow du = (4x^3+3)\ dx$, *and substitute these values*[4] *to obtain,*

$$\int(x^4+3x)^6(4x^3+3)\ dx = \int u^6\ du = \frac{u^7}{7} + c = \frac{(x^4+3x)^7}{7} + c \qquad \diamond$$

Example 50. *To find* $\int(3x+1)^4\ dx$ *we let* $u = 3x+1$ *so that* $\frac{du}{dx} = 3 \Rightarrow \frac{du}{3} = dx$, *and substitute these values to obtain,*

$$\int(3x+1)^4\ dx = \int u^4\ \frac{du}{3} = \frac{1}{3}\int u^4\ du = \frac{1}{3}\cdot\frac{u^5}{5} + c = \frac{(3x+1)^5}{15} + c \qquad \diamond$$

9.5 Integration

Integration begins with the challenge of finding the area under a curve or graph of a function $f(x)$ which lies above an interval $[a,b]$ on the $x-$ axis. We initially suppose the curve is such that $f(x) > 0$ for $x \in [a,b]$, or the graph is always "above" the $x-$axis. (see Figure 7)

[4] We are assuming $\frac{du}{dx} = h(x)$ can be separated into $du = h(x)\ dx$. We do not discuss that here.

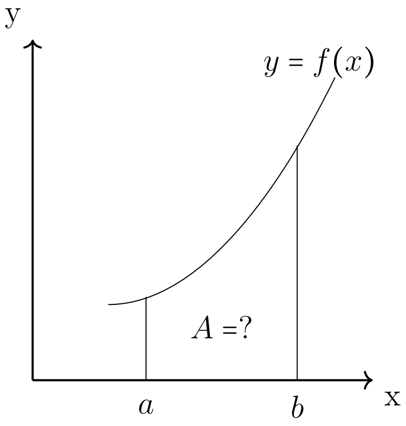


Figure 7

Definition 30. *definite integral, limits of integration, integrand*
The area under a curve $y = f(x)$ where $f(x)$ is always positive, and above an interval $[a,b]$ on the $x-$axis is called the definite integral of $f(x)$ on the interval $[a,b]$ of the $x-$axis.
It is written $\int_a^b f(x)\ dx$, read as "the integral from a to b of $f(x)$ with respect to x."
We call a and b the limits of integration and $f(x)$ the integrand.
The "dx" indicates the integration is with respect to the variable x.

9.5.1 Fundamental Theorems of Calculus

Definition 31. *area function*
Consider a function $f(t)$ defined on an interval $[a,x]$ on the $t-$axis. We define the Area Function $A(x)$ by,

$$A(x) = \int_a^x f(t)\ dt$$

As Figure 8 shows, the area function is the area under the curve $y = f(t)$ and above the interval $[a,x]$. Note it is a function of x, the area increasing as x increases and decreasing as x decreases.

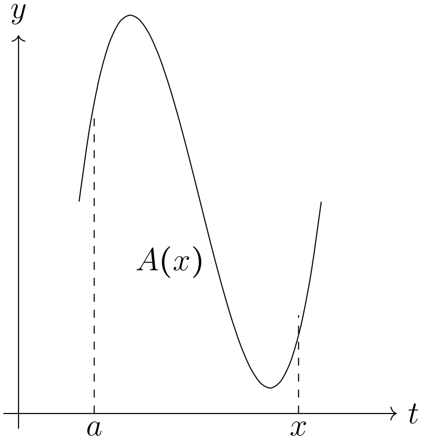


Figure 8

Now, we need a theorem we will use several times.

Theorem 65. *Squeeze Theorem*
Let f, g, h be functions satisfying $f(x) < g(x) < h(x)$ for all x near $x = c$ except possibly at $x = c$.
If $\lim_{x \to c} f(x) = \lim_{x \to c} h(x) = L$ then $\lim_{x \to c} g(x) = L$.

Proof. The informal proof follows from Figure 9. As we approach $x = c$ from either the left (below) or the right (above) along any one of these three curves we find a common value of $y = L$ at $x = c$.

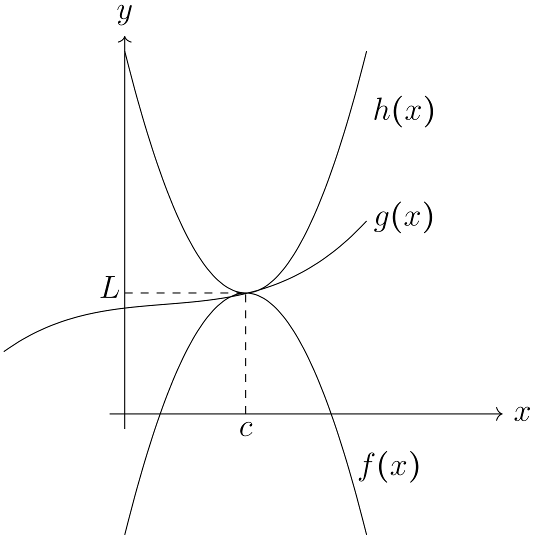


Figure 9

□

Theorem 66. *First Fundamental Theorem of Calculus*
The derivative of the area function $A(x) = \int\limits_a^x f(t)\ dt$ *with respect to* x *is* $f(x)$*, that is,*

$$\begin{aligned} A'(x) &= f(x) \\ \Leftrightarrow f(x) &= \frac{d}{dx}\int_a^x f(t)\ dt \end{aligned}$$

Proof. Consider Figure 10.

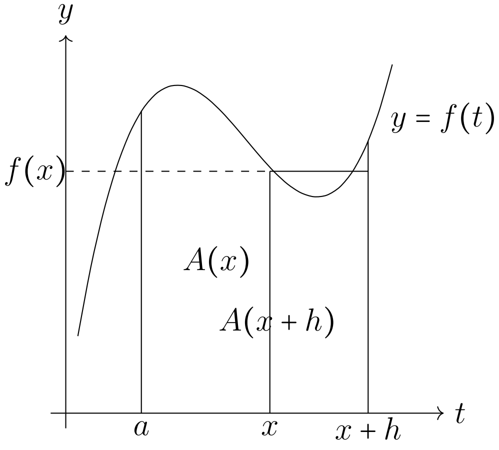


Figure 10

The area under the curve $y = f(t)$ and above the interval $[a, x]$ is $A(x)$ and the area above the interval $[a, x + h]$ is $A(x + h)$.
Thus the area above the interval $[x, x+h]$ is $A(x+h)-A(x)$ but it is also approximately a rectangle of height $f(x)$ and width h so,

$$A(x + h) - A(x) \approx h\ f(x)$$

In terms of integrals,

$$A(x + h) - A(x) = \int_a^{x+h} f(t)\ dt - \int_a^x f(t)\ dt = \int_x^{x+h} f(t)\ dt \approx hf(x)$$

Let m, M be the respective minimum and maximum values of $f(x)$ on $[x, x + h]$. Clearly, from Figure 11, the areas of the two rectangles and the area under the curve relate as,

$$\begin{aligned} mh \le A(x + h) - A(x) \le Mh, \\ \Rightarrow m \le \frac{A(x + h) - A(x)}{h} \le M \end{aligned}$$

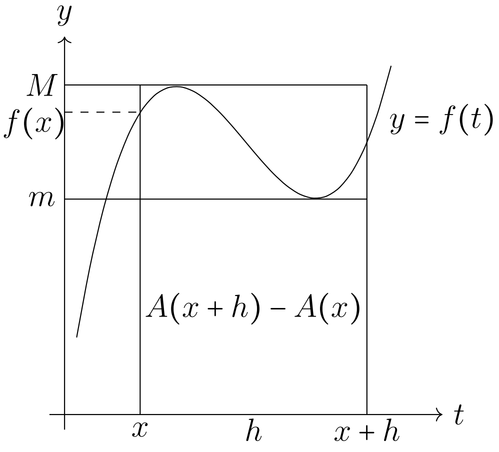


Figure 11

Now as $h \to 0$, m, M and $f(x)$ all come together or,

$$\lim_{h\to 0} m = \lim_{h\to 0} M = \lim_{h\to 0} f(x). \tag{9.5.1}$$

But by the Squeeze Theorem 65 on page 93, since,

$$m \le \frac{A(x+h) - A(x)}{h} \le M \text{ and } \lim_{h\to 0} m = \lim_{h\to 0} M = f(x)$$

we have, using (9.5.1),

$$\lim_{h\to 0} \frac{A(x+h) - A(x)}{h} = f(x) \Leftrightarrow \frac{d}{dx} A(x) = f(x)$$

Substituting for $A(x)$,

$$\frac{d}{dx} \int_a^x f(t)\ dt = f(x)$$

□

Theorem 67. *Second Fundamental Theorem of Calculus*
Suppose $f(x)$ can be integrated and $F(x)$ is an antiderivative of $f(x)$, that is $F' = f$. Then,

$$\int_a^b f(x)\ dx = F(b) - F(a)$$

Proof. Let $F(x)$ be any of the family of antiderivatives of $f(x)$ with respect to x so that $F'(x) = f(x)$. Since by the First Fundamental Theorem of Calculus, the area function obeys $A'(x) = f(x)$, we have,

$$F(x) = A(x) + c$$

Then $F(b) - F(a) = [A(b) + c] - [A(a) + c] = A(b) - A(a)$
But $A(a) = \int_a^a f(x)\ dx = 0$ since the area under any curve above the interval $[a, a]$ is clearly 0.
Hence, $F(b) - F(a) = A(b)$. Then,

$$A(b) = \int_a^b f(x)\ dx = F(b) - F(a)$$

□

Notation 3. *When finding a definite integral we find the indefinite integral first and then substitute a, b which are called the limits of the integration. Accordingly, for $F' = f$ we write,*

$$\int_a^b f(x)\ dx = [F(x)]_a^b = F(b) - F(a)$$

Note 13. *The integration by parts formula in Theorem 64, page 90 becomes for definite integrals,*

$$\int_a^b u\frac{dv}{dx}dx = [uv]_a^b - \int_a^b v\frac{du}{dx}\ dx$$

Example 51. *Let's evaluate $\int_0^{10} x^2\ dx$ which is also the area under the curve $y = x^2$ that lies above the interval $[0, 10]$.*

$$\int_0^{10} x^2\ dx = \left[\frac{x^3}{3}\right]_0^{10} = \frac{10^3}{3} - \frac{0}{3} = \frac{1000}{3} \qquad \diamond$$

Example 52. *Let's evaluate $\int_1^{10} x^{-2}\ dx$ which is also the area under the curve $y = x^{-2}$ that lies above the interval $[1, 10]$.*

$$\int_1^{10} x^{-2}\ dx = \left[\frac{x^{-1}}{-1}\right]_1^{10} = -10^{-1} + 1 = \frac{9}{10} \qquad \diamond$$

9.5.2 Properties of Definite Integrals

Theorem 68.
When you reverse the limits of integration, you must change the sign of the integral. That is,

$$\int_b^a f(x)\ dx = -\int_a^b f(x)\ dx$$

Proof. By the Second Fundamental Theorem of Calculus, if $F' = f$,

$$\int_b^a f(x)\ dx = F(a) - F(b) = -(F(b) - F(a)) = -\int_a^b f(x)\ dx$$

□

Example 53.

$$\int_2^1 x^2\ dx = \left[\frac{x^3}{3}\right]_2^1 = \frac{1}{3} - \frac{8}{3} = -\frac{7}{3},\ \textit{whereas}$$
$$\int_1^2 x^2\ dx = \left[\frac{x^3}{3}\right]_1^2 = \frac{8}{3} - \frac{1}{3} = \frac{7}{3} \qquad \diamond$$

Theorem 69.

$$\int_a^a f(x)\ dx = 0$$

Proof. This is true since the area to be calculated is zero. □

Note we cannot use the Second Fundamental Theorem of Calculus to prove this, saying $\int_a^a f(x)\ dx = F(a) - F(a) = 0$, since we used this result to prove the Fundamental Theorem - that would be what logicians call a “circular argument.”

Theorem 70.

$$\int_a^b (f(x) + g(x))\ dx = \int_a^b f(x)\ dx + \int_a^b g(x)\ dx$$

Proof. By the Second Fundamental Theorem, Theorem 67 on page 95,

$$\begin{aligned}\int_a^b (f(x) + g(x))\ dx &= (F(b) + G(b)) - (F(a) + G(a)) \text{ where } F' = f, G' = g\\ &= F(b) - F(a) + G(b) - G(a)\\ &= \int_a^b f(x)\ dx + \int_a^b g(x)\ dx\end{aligned}$$

The theorem is also illustrated from Figure 12 below. The whole area is the sum of the two smaller areas.

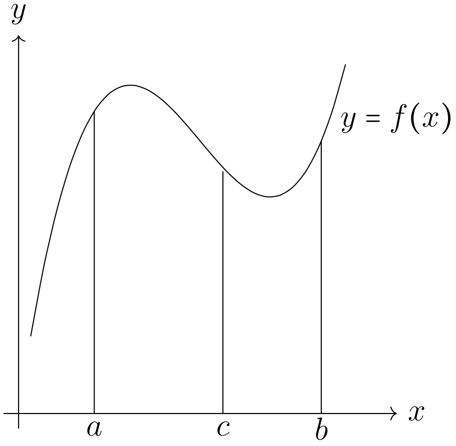


Figure 12

□

Theorem 71.

$$\int_a^b f(x)\ dx = \int_a^c f(x)\ dx + \int_c^b f(x)\ dx$$

Proof. This is obvious from Figure 12.
Where $\frac{d}{dx}F(x) = f(x)$, using the Second Fundamental Theorem, Theorem 67 on page 95,

$$\begin{aligned}\int_a^c f(x)\ dx + \int_c^b f(x)\ dx &= F(c) - F(a) + F(b) - F(c)\\ &= F(b) - F(a) = \int_a^b f(x)\ dx\end{aligned}$$

□

Example 54.

$$\begin{aligned}\int_{-2}^2 (3x^2 + 4x)\ dx &= 3\int_{-2}^2 x^2\ dx + 4\int_{-2}^2 x\ dx\\ &= 3\cdot\left[\frac{x^3}{3}\right]_{-2}^2 + 4\cdot\left[\frac{x^2}{2}\right]_{-2}^2\\ &= 3\left(\frac{8}{3} - \frac{-8}{3}\right) + 4\left(\frac{2^2}{2} - \frac{(-2)^2}{2}\right)\\ &= 16 + 0 = 16\ \textit{whereas}\end{aligned}$$

$$\int_0^2 (3x^2 + 4x)\ dx = 3\cdot\left[\frac{x^3}{3}\right]_0^2 + 4\cdot\left[\frac{x^2}{2}\right]_0^2 = 8 + 8 = 16\ \textit{and}$$

$$\int_{-2}^0 (3x^2 + 4x)\ dx = 3\cdot\left[\frac{x^3}{3}\right]_{-2}^0 + 4\cdot\left[\frac{x^2}{2}\right]_{-2}^0 = 8 - 8 = 0$$

$$\textit{Hence, } \int_{-2}^{2}(3x^2+4x)\ dx = \int_{-2}^{0}(3x^2+4x)\ dx + \int_{0}^{2}(3x^2+4x)\ dx \qquad \diamond$$

Note 14. *The reason why* $\int_{-2}^{0}(3x^2+4x)\ dx = 0$ *is clarified by Figure 13 below. Integrals relating to areas above the* $x-$ *axis are positive whilst integrals relating to areas below the* $x-$*axis are negative. This is so since if* $f(x) < 0$ *for any interval* $[a,b]$ *we can write*

$$\int_a^b f(x)\ dx \textit{ as } -\int_a^b |f(x)|\ dx$$

and then $|f(x)|$ *is "above" the* $x-$*axis giving* $\int_a^b |f(x)|\ dx > 0$ *but the value of the integral* $-\int_a^b |f(x)|\ dx$ *will be negative.*

So the integrals happen to cancel each other in this case. Of course the area from -2 *to* 0 *is not zero. We need to draw the graph to understand what is happening and then evaluate the two integrals separately to find,*

$\int_{-2}^{-\frac{4}{3}}(3x^2+4x)\ dx = +\frac{32}{27}$ *and* $\int_{-\frac{4}{3}}^{0}(3x^2+4x)\ dx = -\frac{32}{27}$.

While the integrals cancel, the area is $2 \times \frac{32}{27} = \frac{64}{27}$.

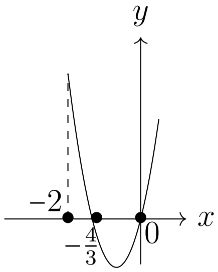


Figure 13

9.6 Change of Variables by Substitution

We can evaluate integrals of the type $\int_a^b f(u(x))u'(x)\ dx$ by changing the variable of integration from x to u, where u is the function of x we can recognize from the composition of functions $f(u(x))$. We are actually reversing the change rule. Diagrammatically we change from an area under $f(u(x))$ for the interval $a \leq x \leq b$ to an area under $u(x)$ for the interval $u(a) \leq u \leq u(b)$.

Example 55. *To evaluate* $\int_0^4 \sqrt{x^2+x}\ (2x+1)\ dx$ *we let* $u(x) = x^2 + x$ *which is the inner function of the composition* $\sqrt{x^2+x}$ *so that* $\frac{du}{dx} = 2x + 1$ *which is the other* *function and write $du = (2x+1)dx$. We also need to change the limits of integration from $0 \leq x \leq 4$ to $u(0) \leq u \leq u(4)$ or $0 \leq u \leq 20$. Then we are evaluating the simple integral,*

$$\int_0^{20} u^{\frac{1}{2}}\ du = \frac{2}{3}\left[u^{\frac{3}{2}}\right]_0^{20} = \frac{2}{3}20^{\frac{3}{2}}$$

Example 56. *(If we assume some trigonometry and calculus knowledge (as given in Chapter 14) another example is this.)*

To evaluate $\int\limits_0^{\frac{\pi}{2}} sin^2 x \cos x\ dx$ we let $u(x) = \sin x$ which is the inner function of $\sin^2 x = (\sin x)^2$ so that $\dfrac{du}{dx} = \cos x$ which is the other term and write $du = \cos x\ dx$. We change the limits from $[0, \frac{\pi}{2}]$ to $[u(0) = \sin 0 = 0, u(\frac{\pi}{2}) = \sin\frac{\pi}{2} = 1]$ or $[0,1]$ and evaluate the integral, $\int\limits_0^1 u^2\ du = \left[\dfrac{u^3}{3}\right]_0^1 = \dfrac{1}{3}$ ⋄

9.7 Infinite Series

The expression of infinitely differentiable functions as infinite series, due to Taylor and Maclaurin, is of such significance that it might justifiably be called a third branch of Calculus alongside differentiation and integration. Let us prove some results for infinite series ahead of several transcendental functions we will introduce in the next Interlude, namely, the natural exponential function and two of the trigonometric functions, sine and cosine.

Definition 32. *infinite series*
A series or infinite series has the form,

$$\sum_{k=1}^{\infty} a_k = a_1 + a_2 + \ldots,\ \ a_k \in \mathbb{R}$$

We usually evaluate $\sum\limits_{k=1}^{\infty}$ by taking the limit $\lim\limits_{n\to\infty}\sum\limits_{0}^{n}$.

We are primarily concerned with infinite series that converge, that is their sum is an unambiguous finite number.

9.7.1 Convergence of an infinite series

We earlier considered Zeno's paradox and noted that,

$$\lim_{n\to\infty}\left(1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n}\right) = 2$$

. We say the infinite series $1 + \frac{1}{2} + \frac{1}{4} + \ldots$ converges to 2.

Definition 33. *informal definition of convergence*
An infinite series converges if it sums to a unique real number, that is, does not sum to infinity or an ambiguous result.

Example 57.

Given $\sum_{n=1}^{\infty} \frac{1}{2^{n-1}} = \frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots = 2$ *we say the series converges (to 2)*

Given $\sum_{n=1}^{\infty} 2^n = 2 + 4 + 8 + \ldots \to \infty$ *we say the series diverges or goes to infinity.*

Give $\sum_{n=1}^{\infty} (-1)^{n+1} = -1 + 1 - 1 + 1 - 1 + 1 - \ldots,$ *whether the final sum is*

-1 or +1 is unclear. We say the series does not converge. ◇

9.7.2 The Harmonic Series

Theorem 72.
The harmonic series[5]

$$\sum_{n=1}^{\infty} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots$$

does not converge.

Proof. We group the terms after 1 so that each final term in a group is of the form $\frac{1}{2^n}$.

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{1}{n} &= 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) \\ &\quad + \left(\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16}\right) + \ldots \\ &\geq 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) \\ &\quad + \left(\frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16}\right) + \ldots \\ &\geq 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} \ldots \to \infty\end{aligned}$$

□

Note 15. *The alternating (in sign ±) series test for convergence is that the series*

$$a_1 - a_2 + a_3 - a_4 + \ldots = \sum_{k=1}^{\infty} (-1)^{k+1} a_k$$

[5] If you put water into a series of identical glass cylinders so they are $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots$ full and tap them with a rod the sounds they make are in harmony, hence the name.

converges if $\lim_{n\to\infty} a_n = 0$.
This is simple to apply. For example if we have the Alternating Harmoic series,

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots + \frac{1}{n} + \ldots$$

we have $\lim_{n\to\infty} a_n = \lim_{n\to\infty} \frac{1}{n} = 0$, *so this series (unlike the Harmonic series) converges. We will use this fact later but we will not prove the general theorem (but you can google it!) You will, however, notice that if we group the series as*

$$(1 - \frac{1}{2}) + (\frac{1}{3} - \frac{1}{4}) + \ldots$$

that it is a series of positive terms and therefore greater than 0 but it cannot "'go to infinity" since

$$1 - (\frac{1}{2} - \frac{1}{3}) - (\frac{1}{4} - \frac{1}{5}) - \ldots$$

shows we are continually subtracting from 1. Hence a limit near 0 seems a likely possibility! (It's actually $\log 2 = 0.693...$)
In any case the alternating harmonic series is bounded by 1 so it converges.

9.7.3 Formal Definition of Convergence

Definition 34. *partial sum*
With respect to the infinite series,

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \ldots, a_k \in \mathbb{R}$$

we use the term partial sums for the sum of the first term, the first two terms, the first three terms and so on and label them thus,

$$\begin{aligned}
&S_1 = a_1 \\
&S_2 = a_1 + a_2 \\
&S_3 = a_1 + a_2 + a_3 \\
&\ldots \\
&S_n = a_1 + a_2 + a_3 + \ldots + a_n
\end{aligned}$$

Definition 35. *convergence of an infinite series*
We say an infinite series converges if the sequence of partial sums described in Definition 34 is approaching some finite number or is bounded.

Example 58. *The partial sums of,*

$$\sum_{n=1}^{\infty} \frac{1}{2^{n-1}} = \frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots$$

are $S_1 = 1, S_2 = 1\frac{1}{2}, S_3 = 1\frac{3}{4}, S_4 = 1\frac{7}{8}$.
The sequence is bounded by 2, so we say it is a convergent series. ◇

9.7.4 Geometric Series

An often-met series is the geometric series $a + ar + ar^2 + ar^3 + \ldots$ in which a first term a is multiplied by r to give the second term and that by r to give the third term and so on. We first need a lemma.

Lemma 73.

$$\lim_{n\to\infty} r^n = \begin{cases} 0 \ if \ |r| < 1 \\ 1 \ if \ r = 1 \\ \infty \ if \ |r| > 1 \end{cases}$$

Proof. Left to the reader to explore with a calculator. Take say 0.1 and keep multiplying it by itself until your calculator cries "uncle!" □

Theorem 74. *Geometric Series Convergence*
The geometric series

$$S = \sum_{n=1}^{\infty} ar^n = a + ar + ar^2 + ar^3 + \ldots$$

converges to $\dfrac{a}{1-r}$ *if* $|r| < 1$, *else it diverges.*

Proof. Consider the partial sum of the first n terms and multiply through by r,

$$\begin{aligned} S_n &= a + ar + ar^2 + ar^3 + \ldots + ar^{n-1} \\ \Rightarrow rS_n &= \qquad ar + ar^2 + ar^3 + \ldots + ar^{n-1} + ar^n \end{aligned}$$

Subtracting,

$$S_n(1-r) = a - ar^n \Rightarrow S_n = \frac{a}{1-r} - \frac{a}{1-r} \cdot r^n$$

Taking the limit as $n \to \infty$, and using Lemma 73 above,

$$S = \lim_{n\to\infty} S_n = \lim_{n\to\infty} \frac{a}{1-r} - \lim_{n\to\infty} \frac{a}{1-r} \cdot r^n = \frac{a}{1-r} \ if \ |r| < 1.$$

□

Example 59. $1 + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \ldots = \dfrac{1}{1 - \frac{1}{3}} = \frac{3}{2}$, *where* $r = \frac{1}{3} < 1$

9.7.5 Tests for Convergence

We can use the result from Theorem 74 to find other tests for convergence of an infinite series.

Theorem 75. *Ratio Test for Convergence*
Let,

$$\sum_{k=1}^{\infty} a_k = a_1 + a_2 + a_3 + \dots$$

be a series of positive terms and let $r = \lim\limits_{k\to\infty} \dfrac{a_{k+1}}{a_k}$. *The series converges if* $r < 1$.

Proof. Suppose $r = \lim\limits_{k\to\infty} \dfrac{a_{k+1}}{a_k}$ exists. Then for all large k,

$$a_{k+1} \approx a_k r \text{ and } a_{k+2} \approx a_{k+1} r \text{ and } a_{k+3} \approx a_{k+2} r, \text{ etc.},$$

giving,

$$a_{k+1} \approx a_k r \text{ and } a_{k+2} \approx a_{k+1} r = a_k r^2 \text{ and } a_{k+3} \approx a_{k+2} = a_k r^3, \text{ etc.}$$

Thus, as k gets larger, the series from a_k onwards is,

$$a_k + a_{k+1} + a_{k+2} + a_{k+3} + \dots \approx a_k + a_k r + a_k r^2 + a_k r^3 + \dots$$

which is a convergent geometric series for $r < 1$. □

Theorem 76. *Integral Test*
Let f be a continuous, positive, non-increasing function on an interval $(1, \infty)$.
Suppose the k^{th} term of an infinite series is $a_k = f(k)$ for all $k \in \mathbb{N}$.
Then the infinite series $\sum\limits_{k=1}^{\infty} a_k$ *converges if and only if the integral* $\int\limits_1^{\infty} f(x)\ dx$ *converges.*

Proof. We use Figure 16.

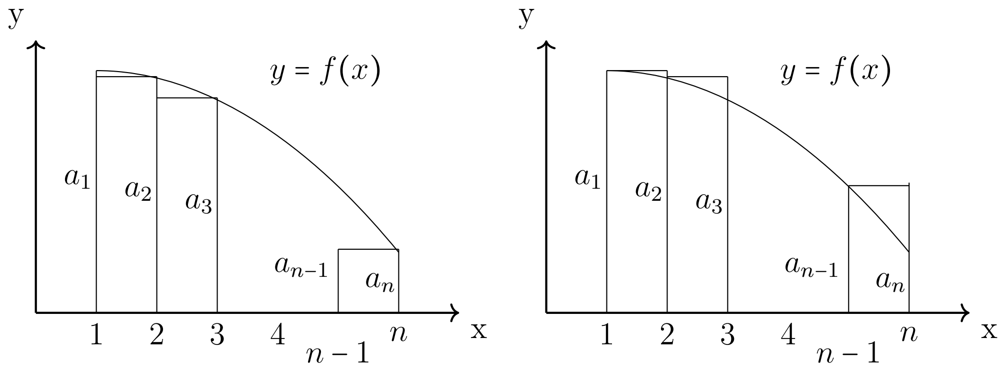


Figure 14

If we sum the areas of the rectangles of width 1 in the two diagrams and compare these with the integral area under the curve we see that,

$$\sum_{k=2}^{n} a_k \le \int_1^n f(x)\ dx \le \sum_{k=1}^{n-1} a_k$$

Suppose that $\int_1^\infty f(x)\ dx$ converges to B. Then, since,

$$S_n = a_1 + \sum_{k=2}^{n} a_k \le a_1 + \int_1^n f(x)\ dx \le a_1 + \int_1^\infty f(x)\ dx \le a_1 + B,$$

by the definition of convergence of an infinite series, since the sequence of partial sums is bounded, $\sum\limits_{k=1}^{\infty} a_k$ converges,

*****

On the other hand, suppose $\sum\limits_{k=1}^{\infty} a_k$ converges to D.
Then again using,

$$\sum_{k=2}^{n} a_k \le \int_1^n f(x)\ dx \le \sum_{k=1}^{n-1} a_k,$$

taking the limit as $n \to \infty$, we have,

$$\lim_{n\to\infty} \int_1^n f(x)\ dx = \int_1^\infty f(x)\ dx \le \lim_{n\to\infty} \sum_{k=1}^{n-1} a_k = \sum_{k=1}^{\infty} a_k = D$$

so that the integral converges. □

Theorem 77. *p–series test*
The series

$$\sum_{k=1}^{\infty} \frac{1}{k^p} = \frac{1}{k} + \frac{1}{k^2} + \frac{1}{k^2} + \ldots$$

converges if $p > 1$ *and diverges if* $p \le 1$.

Proof. If $p \ge 0$, the function $f(x) = \dfrac{1}{x^p}$ is continuous, positive and non-increasing on the interval $[1, \infty]$ and $f(k) = \dfrac{1}{k^p}$.
Thus, by the integral test, Theorem 76, $\sum\limits_{k=1}^{\infty} \dfrac{1}{k^p}$ converges if and only if $\int\limits_1^\infty f(x)\ dx$ converges to a finite number.
If $p > 1$,

$$\int_1^\infty \frac{1}{x^p}\ dx = \int_1^\infty x^{-p}\ dx = \left[\frac{x^{-p+1}}{1-p}\right]_1^\infty = \frac{1}{\infty^{p-1}} \cdot \frac{1}{1-p} - \frac{1}{1-p} = \frac{1}{p-1}$$

so the integral and therefore the series converges.
If $p = 1$ the series becomes the harmonic series which, by Theorem 72, page 101, does not converge.
If $p < 1$,

$$\int_1^\infty \frac{1}{x^p}\ dx = \int_1^\infty x^{-p}\ dx = \left[\frac{x^{1-p}}{1-p}\right]_1^\infty = \frac{1}{\infty^{1-p}} \cdot \frac{1}{1-p} - \frac{1}{1-p} = \infty,$$

so neither the integral nor the series converges.
Here in saying $\frac{1}{\infty^{p-1}} = \frac{1}{\infty}$, we have been a little loose in our treatment of infinity as a number and of integrals with an infinite limit, nevertheless the result stands. □

Note 16. *Of course, you have probably noticed that if* $p = 1$ *then the power rule for integrating* x^{-p} *cannot be used, since* $\int_1^M \frac{1}{x}\, dx$ *makes sense as an integral or area but cannot be* $\frac{x^0}{0}$*. We need to defer this to our further study of Calculus and an introduction to the natural logarithm function.*

9.8 Another mathematical "no-no"

We insist that the infinite series we are dealing with all converge – why do we do this? Let's consider the infinite series

$$x = 4 + 4 \times 5 + 4 \times 5^2 + 4 \times 5^3 + \dots.$$

What is its sum? We claim the (ridiculous) answer that $x = -1$. It's ridiculous since all the terms in the series are positive numbers.
But let's "prove" the claim. To prove $x = -1$ we simply need to prove $x + 1 = 0$. Let's add 1 to both side,

$$\begin{aligned} x + 1 &= 1 + 4 + (4 \times 5) + (4 \times 5^2) + (4 \times 5^3) + \dots. \\ &= 5 + (4 \times 5) + (4 \times 5^2) + (4 \times 5^3) + \dots. \\ &= 0 + (5 \times 5) + (4 \times 5^2) + (4 \times 5^3) + \dots. \\ &= 0 + 0 + (5 \times 5^2) + (4 \times 5^3) + (4 \times 5^4) + \dots. \\ &= 0 + 0 + 0 + (5 \times 5^3) + (4 \times 5^4) + \dots. \\ &= 0 + 0 + 0 + 0 + (5 \times 5^4) + \dots. \\ &= 0 \end{aligned}$$

The problem is that this series does not converge, its partial sums $4, 24, 124, \dots$ simply keep on increasing. This example demonstrates that we cannot work with infinite series that do not converge. This is another mathematical "no-no" and the reason why we must first show any infinite series converges (often on some interval only) before we can work with it to prove another mathematical fact.
For example, the only infinite geometric series we can work with are,

$$\sum_{k=0}^{\infty} ar^n, \ |r| < 1.$$

Later we will work with the Euler zeta function, defined by,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \ s > 1.$$

Of course, eventually someone was going to say "what if

$$x = 4 + 4 \times 5 + 4 \times 5^2 + 4 \times 5^3 + \ldots.$$

can be made to converge?"
Well we have then left real number theory and entered the strange and exotic field of $p-$ adic number theory. One day you may choose to go there.

Part IV

Degustation – Some Classic Pearls of Number Theory

A degustation is a sampling of the chef's signature creations. It may involve as many as 12 courses, all to be sampled in moderation! We will sample only four.

The first is the conclusion of the classic theorems of divisibility studied earlier, that were concluded with the corollary,

If $gcd(a, b) = 1$ then there exist x, y such that $ax + by = 1$.

The problem is how to find x, y when we are dealing with large integers. We use Calculus to find the smallest such x, y.

The second has its roots in Chinese antiquity and is therefore titled the Chinese Remainder Theorem. It is about congruences, a topic developed by Gauss.

e.g., What number has a remainder of 6 when divided by 11, 7 when divided by 8 and 8 when divided by 13?

The third is the Binomial Theorem that can be used to easily expand binomial expressions raised to a positive integer power, such as,

$$(x + y)^5 = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1$$

The fourth is Fermat's Two Squares theorem that primes p of the form $p = 4n + 1$ can be expressed uniquely as the sum of two squares a, b, that is $p = a^2 + b^2$ for some a, b.

$$e.g., 61 = 4 \times 15 + 1 = 5^2 + 6^2$$

We prove the theorem and discover an algorithm to find a,b for any given prime.

Chapter 10

Solving $ax + by = 1,\ gcd(a, b) = 1.$

In Chapter 5 we proved that for any two positive integers $a, b,\ gcd(a, b) = 1$, there are integers x, y satisfying the equation $ax + by = 1$. But how do you find x, y for any given a, b with $gcd(a, b) = 1$?

Course: Degustation Plate I
Ingredients
Solutions of the linear Diophantine equation $ax + by = 1$.
Euclid's algorithm for finding x, y in $ax + by = 1$.
Directions
Prove the x,y of $ax + by = 1$ are not unique.
Use calculus to find an algorithm for the minimal values of x, y.
Mimic the technique of Euclid's algorithm to develop an algorithm for finding any one pair x, y.

10.1 Finding all solutions

Theorem 78.
If x_0, y_0 satisfy $ax + by = 1, a, b \in \mathbb{Z}$, where the $gcd(a, b) = 1$, then all other solutions are of the form

$$x_0 \mp bk, y_0 \pm ak,\ \ k \in \mathbb{Z}$$

Proof. Suppose $ax_0 + by_0 = 1$ and $ax + by = 1$. Then, subtracting,

$$\begin{aligned}&(x - x_0)a + (y - y_0)b = 0\\ &\Rightarrow (x - x_0)a = -(y - y_0)b\\ &\Rightarrow b|x - x_0 \ and\ a|y - y_0\\ &\Rightarrow x - x_0 = bj,\ y - y_0 = ak,\ for\ some\ j, k \in \mathbb{Z}\end{aligned}$$

Hence,

$$x = x_0 + aj,\ \ y = y_0 + bk \tag{10.1.1}$$

Substituting into $ax + by = 1$ gives,

$$\begin{aligned} &ax_0 + abj + by_0 + abk = 1 \\ &\Rightarrow abj = -abk \ since \ ax_0 + by_0 = 1, \\ &\Rightarrow j = -k \\ &\Rightarrow y = y_0 + ak, \ x = x_0 - bk \ (from(10.1.1)) \end{aligned}$$

where k can be positive or negative or zero. Also,

$$\begin{aligned} &ax_0 + by_0 = 1 \\ &\Rightarrow ax_0 \mp abk \pm abk + by_0 = 1 \\ &\Rightarrow a(x_0 \mp bk) + b(y_0 \pm ak) = 1 \end{aligned}$$

Then all solutions of $ax + by = 1$ are of the form $x_0 \mp bk, \ y_0 \pm ak$. □

Example 60. *For $7x + 5y = 1$ we can find $x_0 = -7, y_0 = 10$ by "trial and error". Then all solutions are of the form,*

$$x = -7 \mp 5k, \ y = 10 \pm 7k, k = 0, 1, 2, \ldots$$

If $k = 1$ a solution is $x = -7 - 5 = -12, y = 10 + 7 = 17$ giving $7(-12) + 5(17) = 1$.
Also if $k = 1$ then $x = -2, y = 3$ giving $7(-2) + 5(3) = 1$.
If $k = 2$ a solution is $x = -17, y = 24$ giving $7(-17) + 5(24) = 1$.
Also if $k = 2$, we have $x = -7 + 10 = 3, y = 10 - 14 = -4$ giving $7(3) + 5(-4) = 1$. ⋄

10.2 Algorithm for finding the minimal solution.

Definition 36. *The minimal solution of $ax + by = 1$ is the solution for which $x^2 + y^2$ is a minimum.*

The reasoning behind this definition is that x, y lie on the line $ax + by = 1$. This line does not pass through the origin but it "almost does," intercepting the x−axis at $\left(\frac{1}{a}, 0\right)$ and the y−axis at $\left(0, \frac{1}{b}\right)$ as shown in Figure 15.

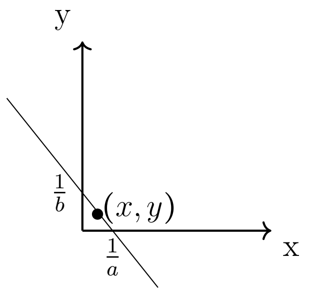


Figure 15

The smallest combined values of x, y are given by the point (x, y) on the line $ax+by = 1$ closest to the origin. The distance from (x, y) on the line $ax+by = 1$ to the origin is given by the Pythagorean Theorem. Its square is $x^2 + y^2$. So if we want the distance to be a minimum, then we want its square to be a minimum. Accordingly we have the following theorem.

Theorem 79.
Given x_0, y_0 satisfy $ax + by = 1, gcd(a, b) = 1$, let $y = y_0 + ak$ and $x = x_0 - bk$. Then the minimal solution has $k = min(n, n + 1)$ where,

$$n \le \frac{ay_0 - bx_0}{a^2 + b^2} \le n + 1,\ \ n, n + 1 \in \mathbb{Z}.$$

Proof. Given x_0, y_0 satisfy $ax + by = 1, gcd(a, b) = 1$, let $y = y_0 + ak$ and $x = x_0 - bk$. We want to minimize $x^2 + y^2$ where $x = x_0 - bk, y = y_0 + ak$ and where k varies as a discrete variable. In order to use Calculus, we put $u = k$ and consider the continuous function,

$$f(u) = (x_0 - bu)^2 + (y_0 + au)^2 = (a^2 + b^2)u^2 - (2bx_0 - 2ay_0)u + x_0^2 + y_0^2$$

This is a quadratic function in u, its graph is an upward opening parabola, so it has a minimum or lowest point. At that point, called the vertex, the tangent is flat or has gradient 0 so at this point $f'(u) = 0$. We proceed accordingly.

$$\begin{aligned} f(u) &= (a^2 + b^2)u^2 - (2bx_0 - 2ay_0) + x_0^2 + y_0^2 \\ \Rightarrow f'(u) &= 2(a^2 + b^2)u - 2(bx_0 - ay_0) = 0 \\ \Rightarrow u &= \frac{bx_0 - ay_0}{a^2 + b^2} \end{aligned}$$

Now this value of u is unlikely to be a whole number since in order to use calculus we needed k to be a continuous variable.
In order to find a minimal value for $y = y_0 \pm ak, x = x_0 \mp bk$ we need to take the nearest integer value k to $u = \dfrac{bx_0 - ay_0}{a^2 + b^2}$. Then by trying each value of $y = y_0 \pm ak, x = x_0 \mp bk$ we can easily choose the minimum combination.
Note we can also have $y = y_0 - ak, x = x_0 + bk$ which gives $u = -\dfrac{bx_0 - ay_0}{a^2 + b^2}$. □

Example 61. *Suppose we somehow found the solution $x_0 = -995, y_0 = 746$ satisfying $743x + 991y = 1$. Then,*

$$\pm u = \pm\frac{bx_0 - ay_0}{a^2 + b^2} = \pm\frac{991(-995) + 743(746)}{743^2 + 991^2} = \pm\frac{1540323}{1534130} = \pm 1^-$$

or a number very close to ±1. So we take $k = \pm 1$ in $y = y_0 + ak, x = x_0 - bk$. Then, with $k = \pm 1$, the minimal solution is given by either,

$$\begin{aligned} k = 1: &\quad x_0 - b = -995 - 991 = -1986 \textit{ and } y_0 + a = 746 + 743 = 1489 \textit{ or,} \\ k = -1: &\quad x_0 + b = -995 + 991 = -4 \textit{ and } \ y_0 - a = 746 - 743 = 3 \end{aligned}$$

So we take $k = -1$, giving

$$-4 \times 743 + 3 \times 991 = 1$$

which is much "nicer" than,

$$-995 \times 743 + 746 \times 991 = 1$$

We still need a method of finding one value of the pair x_0, y_0. The usual method is to use the Euclidean Algorithm and then reverse its steps.

Theorem 80. *Euclidean Algorithm*
Let $a, b \in \mathbb{Z}$. If we apply the Division Algorithm Theorem 13, page 39, repeatedly,

$$\begin{aligned} a &= q_1 b + r_1 && (10.2.1)\\ b &= q_2 r_1 + r_2 && (10.2.2)\\ r_1 &= q_3 r_2 + r_3 && (10.2.3)\\ &\dots && (10.2.4) \end{aligned}$$

we must come to a finite end since the degree of the remainders is becoming smaller and smaller, so we end with,

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} && (n-1)\\ r_{n-2} &= q_n r_{n-1} + r_n && (n)\\ r_{n-1} &= q_{n+1} r_n + r_{n+1} && (n+1) \end{aligned}$$

and $r_{n+1} = 0$.
Then the last non-zero remainder $r_n = gcd(a, b)$.

Proof. From equation $(n+1)$, we have

$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

Since $r_{n+1} = 0$ we see $r_n \mid r_{n-1}$, say, $r_{n-1} = c\ r_n$. Substituting into equation (n) gives,

$$r_{n-2} = c q_n r_n + r_n = r_n [c q_n + 1]$$

so that $r_n \mid r_{n-2}$, say $r_{n-2} = d r_n$.
But then from equation $(n-1)$ we see $r_n \mid r_{n-3}$ since

$$r_{n-3} = d q_{n-1} r_n + c r_n = r_n [d q_{n-1} - c],$$

and so on all the way back to equations $(10.2.1), (10.2.2)$ which show $r_n \mid b$ and finally, $r_n \mid a$ so that r_n is a common divisor of a and b.

*****

To show it is the greatest common divisor, suppose h is any other common divisor of a and b. Then by equation (10.2.1) , $h \mid r_1$, by equation (10.2.2) $h \mid r_2$ and so on all the way down the chain of equations till we reach $h \mid r_n$ making r_n the greatest common divisor, that is, $gcd(a,b) = r_n$. □

Let's consider how to use the Euclidean Algorithm to find a solution to $ax+by = 1$ when $gcd(a,b) = 1$. Clearly if we choose $a, b \in \mathbb{Z}$ so that $gcd(a,b) = 1$ then we don't need the Euclidean Algorithm to find their *gcd*. But we do need its steps to solve $ax + by = 1$. Let's see how this works.

Example 62. *We choose* $a = 9551, b = 1087$, *and apply the Division Algorithm repeatedly.*

$$9551 = 1087 \cdot 8 + 855 \tag{10.2.5}$$
$$1087 = 855 \cdot 1 + 232 \tag{10.2.6}$$
$$855 = 232 \cdot 3 + 159 \tag{10.2.7}$$
$$232 = 159 \cdot 1 + 73 \tag{10.2.8}$$
$$159 = 73 \cdot 2 + 13 \tag{10.2.9}$$
$$73 = 13 \cdot 5 + 8 \tag{10.2.10}$$
$$13 = 8 \cdot 1 + 5 \tag{10.2.11}$$
$$8 = 5 \cdot 1 + 3 \tag{10.2.12}$$
$$5 = 3 \cdot 1 + 2 \tag{10.2.13}$$
$$3 = 2 \cdot 1 + 1 \tag{10.2.14}$$
$$2 = 1 \cdot 1 + 1 \tag{10.2.15}$$
$$1 = 1 + 0 \tag{10.2.16}$$

Since the last non-zero remainder is 1, then we have verified $gcd(9551, 1087) = 1$. *But now let's solve* $9551x + 1087y = 1$. *We simply reverse the above steps like this, each time substituting for the remainder,*

$$\begin{aligned}
1 &= 3 - 2(1) from\ (10.2.14)\\
&= 3 - (5 - 3) = 2(3) - 5\ from\ (10.2.13)\\
&= 2(8 - 5) - 5 = 2(8) - 3(5)\ from\ (10.2.12)\\
&= 2(8) - 3(13 - 8) = 5(8) - 3(13)\ from\ (10.2.11)\\
&= 5(73 - 13(5)) - 3(13) = 5(73) - 28(13)\ from\ (10.2.10)\\
&= 5(73) - 28(159 - 73(2)) = 61(73) - 28(159)\ from\ (10.2.9)\\
&= 61(232 - 159) - 28(159) = 61(232) - 89(159)\ from\ (10.2.8)\\
&= 61(232) - 89(855 - 232(2)) = 328(232) - 89(855)\ from\ (10.2.7)\\
&= 328(1087 - 855) - 89(855) = 328(1087) - 417(855)\ from\ (10.2.6)\\
&= 328(1087) - 417(9551 - 8(1087)) = 3664(1087) - 417(9551)\ from\ (10.2.5)
\end{aligned}$$

giving the solution,

$$3664 \times 1087 - 417 \times 9551 = 1 \qquad \diamond$$

Note 17. *We can express the above 2-step process in one step as follows. Consider $ax + by = 1, gcd(a, b) = 1$. Assume $a > b$, and by the Division Algorithm write,*

$$a = bk_1 + c_1, k_1 > 0, c_1 < b. \tag{10.2.17}$$

Subsituting into $ax + by = 1$ gives,

$$(bk_1 + c_1)x + by = 1 \Rightarrow c_1x + b(k_1x + y) = 1 \tag{10.2.18}$$

Since $c_1 < b$, again by the Division Algorithm, we can write,

$$b = k_2c_1 + c_2, \ \ k_2 > 0, c_2 < c_1 \tag{10.2.19}$$

Substituting (10.2.19) into (10.2.18) gives,

$$c_1x + (k_2c_1 + c_2)(k_1x + y) = 1 \tag{10.2.20}$$
$$c_1(x + k_1k_2x + k_2y) + c_2(k_1x + y) = 1 \tag{10.2.21}$$

Since $c_2 < c_1$,

$$c_1 = k_3c_2 + c_3, \ \ k_3 > 0, c_3 < c_2 \tag{10.2.22}$$

Substituting (10.2.22) into (10.2.21) gives,

$$(k_3c_2 + c_3)(x + k_1k_2x + k_2y) + c_2(k_1x + y) = 1$$
$$c_2(k_3x + k_1k_2k_3x + k_2k_3y + k_1x + y) + c_3(x + k_1k_2x + k_2y) = 1$$

Since the values of c_i are getting smaller and smaller, we can continue in this way until some $c_i = 1$. We would then have,

$$c_i(cx + dy) + C(ex + fy) = 1, \ \ c_i = 1$$

We would then solve the equations,

$$cx + dy = C + 1$$
$$ex + fy = -1$$

to obtain values of x_0, y_0 such that $ax_0 + by_0 = 1$.
Finally we can find the minimal solution by using Theorem 79, page 112.

Example 63. *Let's solve the linear equation* $81x+73y=1$ *for* x,y. *We proceed as follows,*

$$\begin{aligned} 81x+73y&=1\\ (73+8)x+73y&=1\\ 8x+73(x+y)&=1\\ 8x+(9\times 8+1)(x+y)&=1\\ 8(10x+9y)+(x+y)&=1 \end{aligned}$$

We solve,

$$x+y=9 \tag{10.2.23}$$
$$10x+9y=-1 \tag{10.2.24}$$

as follows,

$$(10.2.24)-(10.2.23)\times 9 \textit{ gives } x=-82$$

and by substituting into (10.2.24) we have $y=91$. *Hence*

$$73\times 91-81\times 82=1.$$

The minimal solution is,

$$x_0\mp bk, y_0\pm ak, k\in\mathbb{Z}$$

where k *is the closest integer to one of,*

$$\pm\left|\frac{bx_0-ay_0}{a^2+b^2}\right|=\pm\left|\frac{(73)(-82)-(81)(91)}{81^2+73^2}\right|=\pm\frac{13357}{11891}=\pm 1.12$$

We take $k=-1$ *and we have,*

$$x_0-bk=-82+73=-9,\ y_0+ak=91-81=10$$

to give the minimal solution,

$$10\times 73-9\times 81=1 \qquad \diamond$$

Example 64. *Let's make a start on the example for solving* $9551x+1087y=1$.

$$\begin{aligned} 1&=9551x+1087y\\ &=(8\times 1087+855)x+1087y\\ &=855x+1087(8x+y)\\ &=855x+(855+232)(8x+y)\\ &=855(9x+y)+232(8x+y)\\ &=(3\times 232+159)(9x+y)+232(8x+y)\\ &=159(9x+y)+232(35x+y)\\ &=\ldots \textit{ for you to continue}\\ &=(2223x+253y)+2(3664+417y) \end{aligned}$$

We solve,

$$\begin{aligned} 3664x + 417y &= -1 \\ 2223x + 253y &= 3 \end{aligned}$$

to find $x = -1504, y = 13215,$ *concluding,*

$$1087 \times 13215 - 9551 \times 1504 = 1$$

which is different to the prior solution of,

$$1087 \times 3664 - 9551 \times 417 = 1$$

But let's go to the minimal solution via,

$$\pm \left| \frac{bx_0 - ay_0}{a^2 + b^2} \right| = \pm \left| \frac{-(1087)(-1504) + (13215)(9551)}{9551^2 + 1087^2} \right| \pm = \frac{127,851,313}{92,403,170} = \pm 1.4$$

Taking $k = -1$ *and giving* $x_0 = -1504 + 1087 = -417,\ \ y + 0 = 13215 - 9551 = 3664$ *we find,*

$$1087 \times 3664 - 9551 \times 417 = 1 \qquad \diamond$$

Chapter 11

The Chinese Remainder Theorem

We now consider a classic pearl of number theory, the Chinese Remainder Theorem (CRT) that has its roots in antiquity. It was the method, recorded by the Chinese mathematician Sun-Tzu, reputably used by Chinese generals to count their huge armies – "Line up in lines of 11 (count the leftovers), line up in lines of 10 (count the leftovers), and finally, line up in lines of 9 (count the leftovers)," then, "Sun-Tzu, do your thing!".

Course: Degustation Plate II
Ingredients
Congruences
Solution of linear congruences
Directions
Use the solution of linear congruences to prove the CRT.
Generalize the CRT.
For fun, find what day of the week you were born on.

11.1 Congruences

Let us recall the previous definition of congruences and let's just deal with the positive integers.

Definition 37. *congruence*
Let m be a positive integer. If m divides the difference $a - b$ of two integers, we say "a is congruent to b modulo m" and we write $a \equiv b(\text{mod } m)$.

Note that $m|a - b \Rightarrow a - b = mk$ for some $k \in \mathbb{Z}$ so that,

$$a \equiv b(\text{mod } m) \Leftrightarrow a = b + mk, k \in \mathbb{Z}.$$

Definition 38. *residue*
If $a \equiv b(\text{mod } m)$, b is called a residue of a modulo m. It is any possible remainder when a is divided by m.

Example 65.

$$\begin{aligned}23 = 5 \times 4 + 3 &\Leftrightarrow 23 \equiv 3(\text{mod } 5)\\ 23 = 5 \times 3 + 8 &\Leftrightarrow 23 \equiv 8(\text{mod } 5)\\ 23 = 5 \times 2 + 13 &\Leftrightarrow 23 \equiv 13(\text{mod } 5)\\ 23 = 5 \times 1 + 18 &\Leftrightarrow 23 \equiv 18(\text{mod } 5)\end{aligned}$$

In this example, $3, 8, 13, 18$ are residues and 3 is the least non-negative residue of $23(\text{mod } 5)$. ◇

The Chinese Remainder Theorem deals with finding a least non-negative solution to a system of congruences such as,

$$x \equiv 3(\text{mod } 5) \textit{ and } x \equiv 4(\text{mod } 7)$$

The least non-negative solution will be less than $5 \times 7 = 35$.
By trial and error on the numbers 1 to 35, the solution of these two congruences is easily found as $x = 18$. But what if we had several equations in the system, such as,

$$x \equiv 3(\text{mod } 5),\ x \equiv 4(\text{mod } 7),\ x \equiv 11(\text{mod } 19),\ x \equiv 61(\text{mod } 77)$$

We would need Sun-Tzu's theorem.

11.2 Chinese Remainder Theorem

Theorem 81. *Chinese Remainder Theorem*
Let $m_1, m_2, \ldots, m_r$ be positive integers that are relatively prime in pairs, that is $gcd(m_i, m_j) = 1$ if $m_i \neq m_j$ for all $m_i, m_j \in \{m_1, m_2, \ldots, m_r\}$.
Then for any integers $a_1, a_2, \ldots, a_r$ the r simultaneous congruences,

$$x \equiv a_i(\text{mod } m_i),\ i = 1, 2, \ldots, r$$

have a common solution and any two solutions are congruent modulo the product,

$$m = \prod_{i=1}^{r} m_i = m_1 m_2 \cdots m_r$$

The solution is

$$x_0 = \left(\frac{m}{m_1}\right) b_1 a_1 + \left(\frac{m}{m_2}\right) b_2 a_2 + \ldots + \left(\frac{m}{m_r}\right) b_r a_r$$

where each b_i is the solution of the linear congruence

$$\left(\frac{m}{m_i}\right) b_i \equiv 1(\text{mod} m_i)$$

Proof. Let $m_1, m_2, \ldots, m_r$ be positive integers that are relatively prime in pairs, that is $gcd(m_i, m_j) = 1$ if $m_i \neq m_j$ for all $m_i, m_j \in \{m_1, m_2, \ldots, m_r\}$.
Let $m = \prod_{i=1}^{r} m_i = m_1 m_2 \cdots m_r$. Then $gcd\left(\frac{m}{m_i}, m_i\right) = 1$ for all i.
By the Theorem 153, page 237, Solution of Linear Congruences, there exist integers b_i such that,

$$\left(\frac{m}{m_i}\right) b_i \equiv 1 (\text{mod} m_i)$$

We define,

$$x_0 = \left(\frac{m}{m_1}\right) b_1 a_1 + \left(\frac{m}{m_2}\right) b_2 a_2 + \ldots + \left(\frac{m}{m_r}\right) b_r a_r$$

Then since $m = m_1 m_2 \cdots m_i \cdots m_j \cdots m_r$ we have $m_i | \frac{m}{m_j}$ for all $i \neq j$.
Thus,

$$x_0 = \frac{m}{m_i} b_i a_i + m_i \sum_{k=1, k \neq i}^{r} \frac{m/m_i}{m_k} b_k a_k \Rightarrow x_0 \equiv \frac{m}{m_i} b_i a_i (\text{mod } m_i) \text{ for all } i.$$

But $\left(\frac{m}{m_i}\right) b_i \equiv 1 (\text{mod } m_i)$ or $\frac{m}{m_i} b_i = 1 + k m_i,\ k \in \mathbb{Z}$ Thus,

$$\begin{aligned} x_0 &\equiv \left(\frac{m}{m_i}\right) b_i a_i (\text{mod } m_i) \\ \Rightarrow x_0 &= \frac{m}{m_i} b_i a_i + j m_i,\ j \in \mathbb{Z} \\ &= (1 + k m_i) a_i + j m_i \\ &= a_i + m_i (k a_i + j) \\ &\equiv a_i (\text{mod } m_i) \text{ for all } i : 1 \leq i \leq r \end{aligned}$$

Thus,

$$x_0 = \left(\frac{m}{m_1}\right) b_1 a_1 + \left(\frac{m}{m_2}\right) b_2 a_2 + \ldots + \left(\frac{m}{m_r}\right) b_r a_r$$

is a common solution of all the congruences.

*****

Now we show any two solutions are congruent modulo m.
If both x_0 and y_0 are common solutions of all the congruences, then,

$$x_0 \equiv a_i (\text{mod } m_i) \Leftrightarrow x_0 = a_i + k m_i \ for \ some \ k \in \mathbb{Z}.$$
$$y_0 \equiv a_i (\text{mod } m_i) \Leftrightarrow y_0 = a_i + j m_i \ for \ some \ j \in \mathbb{Z}.$$

implies by subtraction, and using $l = k - j$,

$$x_0 - y_0 = l m_i \Leftrightarrow x_0 \equiv y_0 (\text{mod } m_i).$$

Since no two of the m_i have a common factor, all of m_i must divide $x_0 - y_0$ which means their product,

$$m|x_0 - y_0 \Leftrightarrow x_0 \equiv y_0 (\text{mod } m).$$

That is, any two solutions are congruent modulo m. □

Example 66. *Let's solve the system of linear congruences,*

$$\begin{aligned} x &\equiv 2(\text{mod } 9) \\ x &\equiv 4(\text{mod } 10) \\ x &\equiv 8(\text{mod } 11) \end{aligned}$$

To form

$$x_0 = \left(\frac{m}{m_1}\right) b_1 a_1 + \left(\frac{m}{m_2}\right) b_2 a_2 + \ldots + \left(\frac{m}{m_r}\right) b_r a_r$$

we note,

$$\begin{aligned} &m_1 = 9, m_2 = 10, m_3 = 11, a_1 = 2, a_2 = 4, a_3 = 8 \\ &m = 9 \times 10 \times 11 = 990 \\ &\frac{m}{m_1} = \frac{990}{9} = 110, \ \frac{m}{m_2} = \frac{990}{10} = 99, \ \frac{m}{m_3} = \frac{990}{11} = 90 \end{aligned}$$

Also by trial and error we have the solutions,

$$\begin{aligned} 110b_1 \equiv 1(\text{mod } 9) &\Rightarrow 108b_1 + 2b_1 \equiv 1(\text{mod } 9) \Rightarrow 2b_1 \equiv 1(\text{mod } 9) \Rightarrow b_1 = 5, \\ 99b_2 \equiv 1(\text{mod } 10) &\Rightarrow 90b_2 + 9b_2 \equiv 1(\text{mod } 10) \Rightarrow 9b_2 \equiv 1(\text{mod } 10) \Rightarrow b_2 = 9, \\ 90b_3 \equiv 1(\text{mod } 11) &\Rightarrow 88b_3 + 2b_3 \equiv 1(\text{mod} 11) \Rightarrow 2b_3 \equiv 1(\text{mod } 11) \Rightarrow b_3 = 6. \end{aligned}$$

Then,

$$\begin{aligned} x_0 &= \left(\frac{m}{m_1}\right) b_1 a_1 + \left(\frac{m}{m_2}\right) b_2 a_2 + \ldots + \left(\frac{m}{m_r}\right) b_r a_r \\ &= 110 \times 5 \times 2 + 99 \times 4 \times 9 + 90 \times 4 \times 6 \\ &= 8974 \end{aligned}$$

is a solution of the system. The smallest positive solution is

$$y_0 \equiv x_0 (\text{mod } m) \equiv 8984(\text{mod } 990) = 74$$

It is easy to check that $74(\text{mod } 9) \equiv 2, \ 74(\text{mod } 10) \equiv 4, \ 74(\text{mod } 11) \equiv 8.$

11.3 Generalization of the Chinese Remainder Theorem

We can sometimes remove the restriction that the m_i are relatively prime in pairs, that is, $gcd(m_i, m_j) = 1$ if $m_i \neq m_j$.

Theorem 82. *Generalized CRT*
The simultaneous congruences,

$$x \equiv a_i (\text{mod } m_i), i = 1, 2, \dots, r$$

have a common solution if and only if,

$$a_i - a_j \equiv 0(\text{mod } gcd(m_i, m_j)), for\ all\ i, j = 1, 2, \dots, r,$$

in which case the solution is unique congruent modulo the product,

$$\prod_{i=1}^{r} m_i = m_1 m_2 \cdots m_r.$$

Proof. Suppose the system

$$x \equiv a_i (\text{mod } m_i), i = 1, 2, \dots, r$$

has a solution.
First, if $m_i | x - a_i$ then each factor of m_i divides $x - a_i$. In particular $gcd(m_i, m_j) | x - a_i$. Then for all pairs i, j since,

$$x \equiv a_i (\text{mod } gcd(m_i, m_j))\ and\ x \equiv a_j (\text{mod } gcd(m_i, m_j))$$

by subtraction we have,

$$a_i - a_j \equiv 0(\text{mod } gcd(m_i, m_j))$$

*****

Conversely, suppose

$$a_i - a_j \equiv 0(\text{mod } gcd(m_i, m_j))\ for\ all\ i, j \in \{1.2, \dots, r\}.$$

Now if m has the prime factorization $m = p_i^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where $p_1, p_2, \dots, p_k$ are distinct primes and the $e_i \in \mathbb{N}$, then for all integers a, b if $a \equiv b(\text{mod } m)$ then
$a \equiv b(\text{mod } p_i^{e_i})\ for\ all\ i = 1, 2, \dots, k$. This is true since,

$$\begin{aligned} a \equiv b(\text{mod } m) &\Rightarrow m | a - b \\ &\Rightarrow p_i^{e_1} p_2^{e_2} \cdots p_k^{e_k} | a - b \\ &\Rightarrow p_i^{e_i} | a - b\ for\ all\ i = 1, 2, \dots, k \end{aligned}$$

Using this result we can replace each congruence $x \equiv a_i (\text{mod } m_i)$ with a finite set of congruences of the form $x \equiv a_i (\text{mod } p^e)$ where p^e ranges over all the prime factorizations of m_i.
Our intent is to apply the Chinese Remainder Theorem to this new set of congruences, but these moduli are not necessarily co-prime since some primes may divide

several m_i. We can use the hypothesis to solve this possibility.
For a given prime p let us choose i such that this m_i is the one divisible by the highest power of p, say p^e. Then if $p^f|m_j$ we have $f \leq e$ and $p^f|gcd(m_i, m_j)$ and hence by our hypothesis $p^f|a_i - a_j$.
Thus $a_i \equiv a_j(\text{mod } p^f)$ so the congruence $x \equiv a_i(\text{mod } p^e)$, if true, will imply
$x \equiv a_i(\text{mod } p^f)$ and hence $x \equiv a_j(\text{mod } p^f)$.
So we can discard all the congruences $x \equiv a_j(\text{mod } p^f)$ for this prime p from our set of congruences with the single exception of the congruence $x \equiv a_j(\text{mod } p^e)$ involving the highest power of p since this congruence implies the others.
If we do this for each prime p we are left with a finite set of congruences of the form $x \equiv a_j(\text{mod } p^e)$ involving distinct and therefore co-prime primes p so that we can apply the Chinese Remainder Theorem and claim these congruencers have a common solution which is obviously the solution of the original set of congruences.
The proof of uniqueness is similar to that for the Chinese Remainder Theorem. □

Example 67. *Let's consider finding a solution for this system,*

$$\begin{aligned} x &\equiv a_1(\text{mod } 2^3 \times 3) \\ x &\equiv a_2(\text{mod } 3^2 \times 5) \\ x &\equiv a_3(\text{mod } 2 \times 5^2) \end{aligned}$$

where

$$m_1 = 24,\ m_2 = 45,\ m_3 = 50$$

and

$$gcd(m_1, m_2) = 3 \neq 1,\ gcd(m_2, m_3) = 5 \neq 1,\ gcd(m_1, m_3) = 2 \neq 1.$$

Under what conditions can we expect to find a solution of this system of linear congruences?
Now,

$$\begin{aligned} x \equiv a_1(\text{mod } 2^3 \times 3) &\Rightarrow x = a_1 + 2^3 \times 3k \Rightarrow x \equiv a_1(\text{mod } 2^3) \textit{ and } x \equiv a_1(\text{mod } 3) \\ x \equiv a_2(\text{mod } 3^2 \times 5) &\Rightarrow x = a_2 + 3^2 \times 5k \Rightarrow x \equiv a_2(\text{mod } 3^2) \textit{ and } x \equiv a_2(\text{mod } 5) \\ x \equiv a_3(\text{mod } 2 \times 5^2) &\Rightarrow x = a_3 + 2 \times 5^2k \Rightarrow x \equiv a_3(\text{mod } 2) \textit{ and } x \equiv a_3(\text{mod } 5^2) \end{aligned}$$

Now $x \equiv a_1(\text{mod } 2^3) \Rightarrow x \equiv a_1(\text{mod } 2)$. *But we also have* $x \equiv a_3(\text{mod } 2)$. *By subtraction we must have* $a_1 - a_3 \equiv 0(\text{mod } 2)$. *The same applies to the other pairs mod the same number, so altogether we have,*

$$\begin{aligned} a_1 - a_3 &\equiv 0(\text{mod } 2) \\ a_1 - a_2 &\equiv 0(\text{mod } 3) \\ a_3 - a_2 &\equiv 0(\text{mod } 5) \end{aligned}$$

Hence there can only be a solution of our system if a_1, a_2 *and* a_3 *are (carefully) chosen so that,*

$$\begin{aligned} a_1 &= a_2 + 3i \\ a_2 &= a_3 + 5k \\ a_3 &= a_1 + 2j \end{aligned}$$

There are infinite number of choices nevertheless so let's choose

$$a_2 = 7,\ \ a_1 = 7 + 3 = 10,\ \ a_3 = 7 + 5 = 12$$

so that we also have $a_3 - a_1 = 2$. *So we solve the system,*

$$\begin{aligned} x &\equiv 10 (\bmod\ 24) \\ x &\equiv 7 (\bmod\ 45) \\ x &\equiv 9 (\bmod\ 50) \end{aligned}$$

which, following Theorem 82, we reduce to moduli of the highest power of each prime to give,

$$\begin{aligned} x &\equiv 10 (\bmod\ 2^3) \\ x &\equiv 7 (\bmod\ 3^2) \\ x &\equiv 12 (\bmod\ 5^2) \end{aligned}$$

Then, following Theorem 81 on page 119, we have

$$m_1 = 8, m_2 = 9, m_3 = 25, m = 1800, \frac{m}{m_1} = 225, \frac{m}{m_2} = 200, \frac{m}{m_3} = 72$$

Still following Theorem 81 we need to solve $\frac{m}{m_i} b_i \equiv 1 (\bmod\ m_i)$ *specifically,*

$$\begin{aligned} &3^3 5^2 b_1 \equiv 1 (\bmod\ 2^3) \Rightarrow (8 * 28 + 1) b_1 \equiv 1 (\bmod\ 8) \Rightarrow b_1 = 1 \\ &2^3 5^2 b_2 \equiv 1 (\bmod\ 9) \Rightarrow (198 + 2) b_2 \equiv 1 (\bmod\ 9) \Rightarrow 2b_2 \equiv 1 (\bmod\ 9) \Rightarrow b_2 = 5 \\ &2^3 3^2 b_3 \equiv 1 (\bmod\ 25) \Rightarrow (50 + 22) b_3 \equiv 1 (\bmod\ 25) \Rightarrow 22b_3 \equiv 1 (\bmod\ 25) \Rightarrow b_3 = 8 \end{aligned}$$

Accordingly the solution to our system is given by substituting into,

$$x_0 = \left(\frac{m}{m_1}\right) b_1 a_1 + \left(\frac{m}{m_2}\right) b_2 a_2 + \ldots + \left(\frac{m}{m_r}\right) b_r a_r \ \textit{to give}$$

$$x_0 = 3^2 \cdot 5^2 \cdot 1 \cdot 10 + 2^3 \cdot 5^2 \cdot 7 \cdot 5 + 2^3 \cdot 3^2 \cdot 12 \cdot 8 = 16162 \equiv 1762 (\bmod\ 1800) = 1762$$

which satisfies

$$1762 \equiv 7 (\bmod\ 45) \equiv 10 (\bmod 24) \equiv 12 (\bmod 50) \quad \diamond$$

11.4 What Day of the Week was It?

Suppose we want to find what day of the week was a particular day in the 20th or 21st century (maybe your birthday!).
We use congruences modulo 7. We code the days as,

Saturday	0
Sunday	1
Monday	2
Tuesday	3
Wednesday	4
Thursday	5
Friday	6

We use January 1, 1900 which fell on a Monday as our reference point.
Any other day in January, 1900 is the date plus 1 (January month code) modulo 7.
For example, January 19th is $19 + 1(\text{mod } 7) \equiv 6$ or a Friday.
Each month following January adds on a different number of days. We simply code them accordingly modulo 7. The month codes are,

January		1
February	$31 + 1(\text{mod } 7) \equiv$	4
March	$28 + 4(\text{mod } 7) \equiv$	4
April	$31 + 4(\text{mod } 7) \equiv$	0
May	$30 + 0(\text{mod } 7) \equiv$	2
June	$31 + 2(\text{mod } 7) \equiv$	5
July	$30 + 5(\text{mod } 7) \equiv$	0
August	$31 + 0(\text{mod } 7) \equiv$	3
September	$31 + 3(\text{mod } 7) \equiv$	6
October	$30 + 6(\text{mod } 7) \equiv$	1
November	$31 + 1(\text{mod } 7) \equiv$	4
December	$30 + 4(\text{mod } 7) \equiv$	6

For the ordinary years we add another 1 since $365(\text{mod } 7) \equiv 1$.
For leap years, since $366(\text{mod } 7) \equiv 2$, we need to add another 1 (to the 1 already counted).
Finally, if we go into the 21st century, we do not need a correction for the year 2000 which was a leap year. (It's 1800, 1900, 2100, etc. that are not leap years).

Example 68. *What day of the week was June* 1^{st}*, 1941?*
Remember our base is January 1^{st}*, 1900.*

Number of leap years is the nearest integer less than or equal to 41/4, written $\left[\frac{41}{4}\right] = 10 \equiv 3 \pmod 7$.	*3*
Number of ordinary years was $41 \equiv 6 \pmod 7$	*6*
Month code of June	*5*
Date	*1*
Total	*15*

Since $15 \pmod 7 \equiv 1$, *June* 1^{st}, *1941 was a Sunday.* ◇

Example 69. *What day of the week was November* 14^{th}*, 2012?*
Remember our base is January 1, 1900.

Number of leap years is the nearest integer less than or equal to 112/4, written $\left[\frac{112}{4}\right] = 28 \equiv 0 \pmod 7$.	*0*
Number of ordinary years was $112 \equiv 0 \pmod 7$	*0*
Month code of November	*4*
Date is $14 \equiv 0 \pmod 7$	*0*
Total	*4*

Since $4 \pmod 7 \equiv 4$, *November* 14^{th}, *2012 is a Wednesday. (it's actually for me, as I write this, today!)* ◇

Chapter 12

Binomial Theorem

Course: Degustation Plate III
Ingredients
Definitions of factorials, binomial coefficients
Mathematical Induction
Diirections
Prove the lemma behind Pascal's Triangle
Prove the Binomial Theorem by induction.

The Binomial Theorem is the general formula for expanding,

$$(x+y)^n, n \in \mathbb{N}$$

into a series of terms. Of course,

$$\begin{aligned}(x+y)^1 &= x+y\\(x+y)^2 &= x^2+2xy+y^2\end{aligned}$$

and, with not too much effort, we can multiply out,

$$(x+y)^3 = x^3+3x^2y+3xy^2+y^3$$

But there is too much further effort involved in this approach. We need a formula. Note first, however, that in each of the $n = 1, 2, 3$ cases, the terms begin with x^n and then each successive term has one less x and one more y until we finish with y^n. So we just need a formula for the coefficients of each term.

12.1 Pascal"s Triangle

The French mathematician Blaise Pascal discovered a simple triangle that churns out the coefficients of each term in $(x+y)^n$. Each number in a line is obtained by adding together the two numbers to its left and right on the line above it. For the ends, where there isn't a number on the left/right, just use 0.

$$\begin{array}{c} 1\ 1 \\ 1\ 2\ 1 \\ 1\ 3\ 3\ 1 \\ 1\ 4\ 6\ 4\ 1 \\ 1\ 5\ 10\ 10\ 5\ 1 \\ 1\ 6\ 15\ 20\ 15\ 6\ 1 \end{array}$$

The first number greater than 1 in each line tells you the value of n you are dealing with. For example,

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$$

It's nice and easy for small values of n but we need more! We start with definitions and a lemma.

Definition 39. *factorial*
For $n \in \mathbb{Z}^+ \cup 0$, "factorial n" or "n factorial" is written $n!$ and is defined as,

$$n! = n(n-1)(n-2)\cdots 1.$$

We could also define $n!$ recursively by,

$$n! = n(n-1)! \textit{ beginning with } 0! = 1.$$

Example 70. *Using the recursive definition it is easy to calculate successive values of $n!$*

$0! = 1;\quad 1! = 1\times 0! = 1;\quad 2! = 2\times 1! = 2;\quad 3! = 3\times 2! = 6;$
$4! = 4\times 3! = 24;\quad 5! = 5\times 4! = 120;\quad 6! = 6\times 5! = 720;\quad 7! = 7\times 6! = 5040;\ \ldots$
$20! = 2.4329020\times 10^{18}$

The factorial function increases extremely rapidly in value as n increases as this example shows. It therefore follows that $\lim_{n\to\infty}\frac{f(n)}{n!} = 0$ for almost all functions $f(n)$. We will use this fact several times. ◇

Definition 40. *binomial coefficient*
For $n,k \in \mathbb{N}\cup\{0\}$, the binomial coefficient $\binom{n}{k}$, spoken as "n choose k" is defined by,

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Example 71. $\binom{7}{4} = \frac{7!}{3! \times 4!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 35$

In a course in either combinatorics or introductory probability theory, you would find that the number of ways of choosing 4 objects from a collection of 7 objects is $\binom{7}{4} = 35$, hence the way we say the binomial coefficient – “7 choose 4”.

Lemma 83.
The number of ways of choosing k objects from n objects is clearly the same as the number of ways of choosing $n - k$ objects from n objects, since in each case we are simply separating the objects into a group of k objects and a group of $n - k$ objects. That is we claim,

$$\binom{n}{k} = \binom{n}{n-k}.$$

Proof. Note $k = n - (n - k)$,

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n!}{(n-(n-k))!(n-k)!} = \binom{n}{n-k}$$

□

The reason why Pascal’s Triangle works is due to the following lemma.

Lemma 84.

$$\binom{n}{n-k} + \binom{n}{k} = \binom{n+1}{k}$$

Proof.

$$\begin{aligned}
\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(n-k+1)!(k-1)!} + \frac{n!}{(n-k)!k!} \\
&= \frac{n!}{(n-k)!(k-1)!}\left(\frac{1}{n-k+1} + \frac{1}{k}\right) \\
&= \frac{n!}{(n-k)!(k-1)!}\left(\frac{\cancel{k} + n - \cancel{k} + 1}{k(n-k+1)}\right) \\
&= \frac{(n+1)!}{(n-k+1)!k!} \\
&= \binom{n+1}{k}
\end{aligned}$$

□

12.2 Binomial Theorem

In the following proof we manipulate finite sums. Note that the summation index in a sum is a "dummy index". That is, the symbol we use to sum it is irrelevant. For example,

$$\sum_{i=o}^{20} k^2 = \sum_{j=0}^{20} j^2 = 1^2 + 2^2 + \ldots + 20^2$$

Accordingly, for example, we can replace j in,

$$\sum_{j=1}^{9} x^{j-1} = x^0 + x^1 + \ldots + x^8$$

with $k = j - 1$ to give,

$$\sum_{k=0}^{8} x^k = x^0 + x^1 + \ldots + x^8$$

Theorem 85. *Binomial Theorem*
The expansion of the product of the n terms in $(x+y)^n$ is,

$$\begin{aligned}(x+y)^n &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\end{aligned}$$

Proof. We use the method of mathematical induction and Lemma 84.
Let $S(n)$ be the statement that,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n}y^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$$

Then the $S(1)$ statement

$$(x+y)^1 = \binom{1}{0}x^1 + \binom{1}{1}y^1 = \frac{1!}{1!0!}x + \frac{1!}{0!1!}y = x + y$$

is true.
Assume $S(n)$ is true. We want to prove $S(n+1)$ is true, that is,

$$(x+y)^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n-k+1}y^k$$

Now,

$$(x+y)^{n+1} = (x+y)(x+y)^n = x(x+y)^n + y(x+y)^n$$

$$= x\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k + y\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$$

where we used $S(n)$ is true and substituted for $(x+y)^n$.

$$= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1}$$

We put $j = k$ in the first sum and $j = k+1$ in the second sum,

$$= \sum_{j=0}^{n}\binom{n}{j}x^{n-j+1}y^j + \sum_{j=1}^{n+1}\binom{n}{j-1}x^{n-j+1}y^j$$

We separate out the first term in the first sum and the last term in the second sum

$$= \binom{n}{0}x^{n+1} + \sum_{j=1}^{n}\binom{n}{j}x^{n-j+1}y^j + \sum_{j=1}^{n}\binom{n}{j-1}x^{n-j+1}y^j + \binom{n}{n}y^{n+1}$$

We combine the sums noting $1 = \binom{n}{n} = \binom{n+1}{n+1}$ and $1 = \binom{n}{0} = \binom{n+1}{0}$ and alter j to k.

$$= \binom{n+1}{0}x^{n+1} + \sum_{k=1}^{n}\left\{\binom{n}{k} + \binom{n}{k-1}\right\}x^{n-k+1}y^k + \binom{n+1}{n+1}y^{n+1}$$

We apply Lemma 84 page 129,

$$= \binom{n+1}{0}x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^{n-k+1}y^k + \binom{n+1}{n+1}y^{n+1}$$

We put the first and last terms back into the sum and obtain,

$$(x+y)^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n-k+1}y^k$$

This concludes the proof. □

Example 72.

$$(x+y)^6$$
$$= \binom{6}{0}x^6y^0 + \binom{6}{1}x^5y^1 + \binom{6}{2}x^4y^2 + \binom{6}{3}x^3y^3 + \binom{6}{4}x^2y^4 + \binom{6}{5}x^1y^5 + \binom{6}{6}x^0y^6$$
$$= \frac{6!}{0!6!}x^6 + \frac{6!}{1!5!}x^5y + \frac{6!}{2!4!}x^4y^2 + \frac{6!}{3!3!}x^3y^3 + \frac{6!}{4!2!}x^2y^4 + \frac{6!}{5!1!}xy^5 + + \frac{6!}{6!0!}y^6$$
$$= x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6$$

Chapter 13

Fermat's Two Squares Theorem

We now prove that every prime of the form $4n + 1$ can be expressed as the sum of two squares in a unique way. We will do this by using a subset of the complex numbers called Gaussian integers. We start with the set of definitions relating to these numbers. The development is similar to that for $k(\rho)$ in Chapter 7 and $k(1) = \mathbb{Z}$ in Chapter 5. The final approach is due to Dedekind.

Course: Degustation Plate IV
Ingredients
The theory of Gaussian integers, their sum, product, norm, complex conjugates, units, primes
Directions
Prove the lemmas for the theory of Gaussian integers.
Prove the parallel chain of theorems for Gaussian integers: Division algorithm, Euclidean Algorithm for finding gcd(m,n), Solutions of Linear Diophantine equations, Euclid's lemma on primes, Fundamental Theorem of Arithmetic.
Prove Wilson's theorem.
Prove an integer prime $p \equiv 1 (\mathrm{mod}\ 4)$ is not a prime in Gaussian integers.
Prove Fermat's two squares theorem $p = a^2 + b^2$ if $p \equiv 1 (\mathrm{mod}\ 4)$.
Prove a, b are unique for any prime $p \equiv 1 (\mathrm{mod}\ 4)$.
Develop an algorithm for finding a,b and apply it to an example.

13.1 Gaussian Integers

Definition 41. *Gaussian integers*
The set of Gaussian integers, denoted $\mathbb{Z}[i]$, spoken as "$\mathbb{Z}$ append i," is the set,

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$$

Definition 42. *sum and product of Gaussian integers*
Let $a + bi, c + di \in \mathbb{Z}[i]$.

As expected, using $i^2 = -1$, we define their sum and product by,

$$(a+bi)+(c+di) = (a+c)+(b+d)i$$
$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i$$

Definition 43. *magnitude*
The magnitude $|z|$ of a Gaussian integer z is defined to be,

$$|z| = \sqrt{a^2+b^2} \Rightarrow |z|^2 = a^2+b^2$$

Definition 44. *norm*
Let $z = a = bi \in \mathbb{Z}[i]$.
We define the norm $N(z)$ of z by,

$$N(z) = a^2+b^2$$

If z is a Gaussian integer, then $|z|^2 = N(z)$.
We could interpret the norm of z as its magnitude defined as the distance from the point (a,b) in the complex number plane to the origin.

Note 18. *For $z = a+bi$, $N(z) = a^2+b^2$ with $a,b \in \mathbb{Z}$ means $N(z) \geq 1$ since the smallest values of $N(z)$ are given by $a = \pm 1, b = 0$ or vice versa.*

Definition 45. *complex conjugate*
The complex conjugate of $z = a+bi \in \mathbb{Z}[i]$ is $\bar{z} = a-bi$.

13.1.1 Properties of Gaussian Integers

We continue with a set of lemmas generating the important properties of Gaussian integers. Essentially we describe the Gaussian integers in a parallel manner to how we described the ordinary integers.

Lemma 86.
Let r,s be Gaussian integers. Then,

$$N(rs) = N(r)N(s)$$

Proof. Let $r = a+bi, s = c+di$. Then,

$$\begin{aligned} N(rs) &= N((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2+(ad+bc)^2 \\ &= a^2c^2 - \cancel{2abcd} + b^2d^2 + a^2d^2 + b^2c^2 + \cancel{2abcd} \\ &= (a^2+b^2)(c^2+d^2) \\ &= N(r)N(s). \end{aligned}$$

□

Lemma 87.
Let $r = a + bi, s = c + di$. Then,

$$\overline{rs} = \bar{r}\bar{s}$$

Proof.

$$rs = (ac - bd) + (ad + bc)i \Rightarrow \overline{rs} = (ac - bd) - (ad + bc)i$$

Whereas,

$$\bar{r}\bar{s} = (a - bi)(c - di) = (ac - bd) - (ad + bc)i = \overline{rs}$$

□

Lemma 88.
Let $z \in \mathbb{Z}[i]$. Then,

$$N(z) = z\bar{z}$$

Proof. Let $z = a + bi$. Then,

$$z\bar{z} = (a + bi)(a - bi) = a^2 - b^2i^2 = a^2 + b^2 = N(z)$$

□

Definition 46. *division of Gaussian integers*
Let $a, d \in \mathbb{Z}[i]$. We say d divides a, written $d|a$, if there exists a $q \in \mathbb{Z}[i]$ such that $a = qd$.

Example 73. $3 - i \mid 10$ *since* $10 = (3 - i)(3 + i)$.

Lemma 89. *Linear Combination Lemma*
Let $d, m, n, x, y \in \mathbb{Z}[i]$. If $d|x, d|y$ then $d|mx + ny$.

Proof.
$d|x \Rightarrow x = dd_1$ for some $d_1 \in \mathbb{Z}[i]$.
$d|y \Rightarrow y = dd_2$ for some $d_2 \in \mathbb{Z}[i]$.
Then, $mx + ny = mdd_1 + ndd_2 = d(md_1 + nd_2) \Rightarrow d \mid mx + ny$. □

In the ordinary integers there are only two numbers that have multiplicative inverses[1] that are integers, namely ±1. Each is its own multiplicative inverse since $1 \times 1 = 1$ and $(-1) \times (-1) = 1$. Note the magnitude of both 1 and -1 is 1. In the Gaussian integers there will turn out to be four units.

Definition 47. *unit*
Gaussian integers that have multiplicative inverses in the Gaussian integers are called units. That is, $u \in \mathbb{Z}[i]$ is a unit if there exists a $z \in \mathbb{Z}[i]$ such that $u \times z = 1$.

[1] a has multiplicative inverse b if $ab = 1$.

Lemma 90.
The only units in $\mathbb{Z}[i]$ are $\pm1, \pm i$ and if u is a unit then $N(u) = 1$.

Proof. Note $N(1) = N(-1) = (\pm1)^2 + 0^2 = 1$ and $N(i) = N(-i) = 0^2 + (\pm1)^2 = 1$.
First,
1 is a unit since it has the multiplicative inverse $z = 1$ making $1 \cdot z = 1$
-1 is a unit since it has the multiplicative inverse $z = -1$ making $-1 \cdot z = 1$
i is a unit since it has the multiplicative inverse $z = -i$ making $i \cdot z = 1$
$-i$ is a unit since it has the multiplicative inverse $z = i$ making $-i \cdot z = 1$

Second, suppose there is another unit $u \in \mathbb{Z}(i)$.
Let z be such that $u \cdot z = 1$.
Then, $N(uz) = N(1) = 1 \Rightarrow N(z)N(u) = 1 \Rightarrow N(u)|1$.
But $N(a + bi) = a^2 + b^2$ so apart from $a + bi = 0 + 0i$ we must have $N(a + bi) \geq 1$.
Thus if $N(u)|1$ we must have $N(u) = 1$.
So if $u = a + bi$ then $N(u) = a^2 + b^2 = 1$ which is only possible if $a = \pm1, b = 0$ or $a = 0, b = \pm1$.
Accordingly the only units in $\mathbb{Z}[i]$ are $\pm1, \pm i$ each with a norm of 1.

Third, suppose u is a unit. Then there is a v such that $uv = 1$.
Then $N(uv) = N(1) = 1 \Rightarrow N(u)N(v) = 1 \Rightarrow N(u) = 1$ since $N(z) \geq 1$ for all $z \in \mathbb{Z}[i]$ as discussed in Note 4 on page 63. □

In $\mathbb{Z}$ we could define a prime p as a positive integer that is not a positive unit (not 1) and is such that if $p = ab$ then either $a = 1$ or $b = 1$. We do the same in the Gaussian integers, except here there are 4 units.

Definition 48. *prime*
Let $p \in \mathbb{Z}[i]$. We say p is prime[2] if for all $a, b \in \mathbb{Z}$, $p = ab$ implies either a is a unit or b is a unit.

Example 74.

(a) 5 *is not prime in* $\mathbb{Z}[i]$ *since* $5 = (1 + 2i)(1 - 2i)..$

(b) $1 + 3i$ *is not prime in* $\mathbb{Z}[i]$ *since* $1 + 3i = (1 - i)(-1 + 2i)$.

(c) $5 + 4i$ *is prime in* $\mathbb{Z}[i]$ *as shown by this argument.*
First, $N(5 + 4i) = 4^2 + 5^2 = 41$.
Suppose $5 + 4i = ab, a, b \in \mathbb{Z}[i]$.
Then, $N(5 + 4i) = N(ab) = N(a)N(b) = 41$ *which is a prime number in* $\mathbb{Z}$.
Then either $N(a) = 1$ *or* $N(b) = 1$, *so one of* a, b *is a unit and by Definition 48,* $5 + 4i$ *is prime.* ◇

[2] While we say 5 is a prime in $\mathbb{Z}$ we say $5 + 4i$ is prime in $\mathbb{Z}[i]$ (as we show in the next example), omitting the "a".

The proof that $5 + 4i$ is prime in $\mathbb{Z}[i]$ relied upon that fact that 41 is a prime in $\mathbb{Z}$. This suggests a general lemma.

Lemma 91.
Let $z \in \mathbb{Z}[i]$. If $N(z)$ is a prime in the ordinary integers $\mathbb{Z}$ then z is prime in $\mathbb{Z}[i]$.

Proof. Let $z = a + bi$.
Let $N(z) = a^2 + b^2 = p$ say where p is a prime in $\mathbb{Z}$.
Suppose $z = cd, c, d \in \mathbb{Z}[i]$.
Then $N(z) = N(c)N(d) = p$ implies either $N(c) = 1$ or $N(d) = 1$.
So one of c, d is a unit making z prime in $\mathbb{Z}[i]$. □

In the ordinary integers, two numbers a, b are relatively prime if $gcd(a, b) = 1$, that is, they have no common divisors greater than 1.
In the Gaussian integers $\mathbb{Z}[i]$ the unit 1 in $\mathbb{Z}$ is replaced by any of the four units $\pm 1, \pm i$ in $\mathbb{Z}[i]$.

Definition 49. *relatively prime*
Let $a, b \in \mathbb{Z}[i]$. We say a, b are relatively prime in $\mathbb{Z}[i]$ if the only $d \in \mathbb{Z}[i]$ such that $d|a$ and $d|b$ is a unit.

In Chapter 5, we proved a chain of theorems about integers, namely,

$$\begin{tikzcd}
\text{Division Theorem} \arrow[r] & \text{Linear Diophantine Equations } ax + by = 1 \arrow[r] & \text{Euclid's Lemma} \arrow[r] & \text{Fundamental Properties of Primes} \arrow[r] & \text{Fundamental Theorem of Arithmetic} \\
 & \text{Euclidean Algorithm} \arrow[u] & & &
\end{tikzcd}$$

We will prove a similar chain of theorems for the Gaussian Integers. We start with two lemmas about distances, one for rationals and the integers, a parallel one for complex numbers and Gaussian integers.
Obviously, on the real line, every real number is within $\frac{1}{2}$ of an ordinary integer. Gaussian integers, however, lie on the complex plane, so how far apart can they be? We expect the Pythagorean theorem to appear when we calculate distances.

Lemma 92.
Let $x \in \mathbb{Q}$. Then there is an $n \in \mathbb{Z}$ such that,

$$|x - n| \leq \frac{1}{2}$$

Proof.
We use Corollary 14 page 40 of the Division Algorithm of the ordinary integers in the

form,
"If $a, b \in \mathbb{N}$, there exist integers n, r such that $a = nb + r,\ |r| \le \frac{b}{2}$."
In particular, if we divide a by b we can always have a remainder $|r| \le \frac{b}{2}$.
Let $x = \frac{a}{b}, a, b \in \mathbb{Z}, b \ne 0$. Then,

$$\begin{aligned} x &= \frac{a}{b} = \frac{nb+r}{b} = n + \frac{r}{b}, |r| \le \frac{b}{2} \\ \Rightarrow x - n &= \frac{r}{b},\ |r| \le \frac{b}{2} \\ \Rightarrow |x - n| &= \left|\frac{r}{b}\right| \le \frac{1}{2} \end{aligned}$$

□

Lemma 93.
Every complex number is within $\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$ *of a Gaussian integer, that is, for all* $z \in \mathbb{C}$ *there exists a* $q \in \mathbb{Z}[i]$ *such that* $|z - q| \le \frac{\sqrt{2}}{2}$.

Proof. Let $z = \frac{a}{b}$ where $a = s + ti, b = u + vi \in \mathbb{Z}[i], b \ne 0$. Then,

$$\begin{aligned} z &= \frac{a}{b} \\ &= \frac{s+ti}{u+vi} \cdot \frac{u-vi}{u-vi} \\ &= \frac{su+tv}{u^2+v^2} + i\frac{tu-sv}{u^2+v^2} \\ &= x + iy,\ x, y \in \mathbb{Q},\ say. \end{aligned}$$

By Lemma 92, there exist integers m, n such that,

$$\begin{aligned} |x - n| &\le \frac{1}{2} \text{ and } |y - m| \le \frac{1}{2} \\ \Rightarrow (x-n)^2 &\le \frac{1}{4} \text{ and } (y-m)^2 \le \frac{1}{4} \end{aligned}$$

Consider, using $z = x + iy$,

$$z - (n + mi) = (x - n) + i(y - m)$$

giving,

$$|z - (n + mi)|^2 = (x-n)^2 + (y-m)^2 \le \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

So there exists a q such that $|z - q| \le \frac{1}{\sqrt{2}}$ namely $q = n + mi$. □

Theorem 94. *Division Algorithm of Gaussian Integers*
Let $a, b \in \mathbb{Z}[i], b \neq 0$. Then there exist $q, r \in \mathbb{Z}[i]$ such that,

$$a = qb + r, N(r) < N(b).$$

Proof.
Let $a, b \in \mathbb{Z}[i], b \neq 0$.
Let $z = \frac{a}{b} \Rightarrow a = zb$.
Let $r = a - qb \Rightarrow a = qb + r$ where q is chosen so that $|z - q| \leq \frac{\sqrt{2}}{2}$. Then,

$$|r| = |a - qb| = |zb - qb| = |(z - q)b| = |(z - q)||b| \leq \frac{\sqrt{2}}{2}|b| < |b|$$

We conclude since[3] $N(r) = |r|^2, N(b) = |b|^2$ that $N(r) < N(b)$.

□

Example 75.
Let $a = 27 - 23i$ and $b = 8 + i$. We want to write the equation,

$$a = bq + r, N(r) < N(b).$$

for $a, b, q, r \in \mathbb{Z}[i]$.
We divide a by b in the usual manner, using the complex conjugate of b to make the denominator an integer, thus,

$$\frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} = \frac{(27 - 23i)(8 - i)}{(8 + i)(8 - i)} = \frac{193}{65} - \frac{211i}{65}$$

It is generally the case, as we find here, that the answer $\frac{193}{65} - \frac{211i}{65} \notin \mathbb{Z}[i]$ since $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.
We proceed as follows keeping in mind that we need $N(r) < N(b) = 65$.
We choose the closest integers to $\frac{195}{65} \approx 2.97$ and $\frac{-211}{65} \approx -3.25$ namely $3, -3$ and write $a = bq + r$ as,

$$27 - 23i = (8 + i)(3 - 3i) + r$$

Since $(8 + i)(3 - 3i) = 27 - 21i$ we have $r = 27 - 23i - 27 + 21i = -2i$ and we note $N(r) = N(-2i) = 4$ and $N(b) = N(8 + i) = 65$ so that $N(r) < N(b)$. We conclude that,

$$27 - 23i = (8 + i)(3 - 3i) - 2i$$

There are of course an infinite number of values of c, d, e, f satisfying

$$27 - 23i = (8 + i)(c + di) + (e + fi)$$

but this choice always has $N(r) < N(b)$. ◇

[3] If $z = a + bi$ then $N(z) = a^2 + b^2$ but also $|z| = \sqrt{a^2 + b^2}$ so $N(z) = |z|^2$

13.2 Major Theorems for Gaussian Integers

13.2.1 Euclidean Algorithm in Gaussian Integers

Theorem 95.
Suppose we want to find gcd(a,b) for two Gaussian integers a,b with $b \neq 0$. We apply the Division Theorem to divide a by b. If the remainder is not 0, then we continue dividing the previous step's divisor by its remainder. When a remainder of 0 is obtained, STOP. The gcd(a,b) is the last non-zero remainder. The algorithm results in the following system of equations,

$$a = q_1 b + r_1 \qquad N(r_1) < N(b) \tag{13.2.1}$$
$$b = q_2 r_1 + r_2 \qquad N(r_2) < N(r_1) \tag{13.2.2}$$
$$r_1 = q_3 r_2 + r_3 \qquad N(r_3) < N(r_2) \tag{13.2.3}$$
$$\dots \tag{13.2.4}$$
$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \qquad N(r_{n-1}) < N(n) \tag{13.2.5}$$
$$r_{n-2} = q_n r_{n-1} + r_n \qquad N(r_n) < N(r_{n-1}) \tag{13.2.6}$$
$$r_{n-1} = q_{n+1} r_n + 0 \tag{13.2.7}$$

The gcd(a,b) is r_n, the last non-zero remainder.

Proof. By (13.2.7), $r_n | r_{n-1}$, say $r_{n-1} = k_1 r_n$.
Substituting into (13.2.6), we have $r_{n-2} = q_n k_1 r_n + r_n$ so $r_n | r_{n-2}$, say $r_{n-2} = k_2 r_n$.
Substituting into (13.2.5), we have $r_{n-3} = q_{n-1} k_2 r_n + k_1 r_n$ so $r_n | r_{n-3}$.
Continuing in this way back up the system of equations we find $r_n | b$ and finally, in (13.2.1) that $r_n | a$.
Hence r_n is a common dividsor of a and b.
To prove it is the greatest common divisor we suppose some other common divisor d divides both a and b, say $a = j_1 d, b = j_2 d$ for some $j_1, j_2 \in \mathbb{Z}[i]$.
Substituting into (13.2.1) we have

$$j_1 d = q_1 j_2 d + r_1 \Rightarrow r_1 = j_1 d + q_1 j_2 d = d(j_1 + q_1 j_2)$$

so $d | r_1$, say $r_1 = j_3 d$. Substituting into (13.2.2),

$$j_2 d = q_2 j_3 d + r_2 \Rightarrow d | r_2.$$

Back down the system of equations we proceed in this way to reach via (13.2.7) that $d | r_n$. Hence r_n is the gratest common divisor of a, b. □

Example 76. *Let's find gcd(a,b) where $a = 11 + 3i, b = 1 + 8i$. We have, using the division process illustrated in Example 75 above,*

$$\begin{aligned} 11 + 3i &= (1 + 8i)(1 - i) + 2 - 4i \\ 1 + 8i &= (2 - 4i)(-1 + i) - 1 + 2i \\ 2 - 4i &= (-1 + 2i)(-2) + 0 \end{aligned}$$

Hence $gcd(11+3i, 1+8i) = -1+2i$. *So these two Gaussian integers are not relatively prime.*
Let's repeat the process for $32+9i$ *and* $4+11i$.

$$\begin{aligned} 32+9i &= (4+11i)(2-2i)+2-5i \\ 4+11i &= (2-5i)(-2+i)+3-i \\ 2-5i &= (3-i)(1-i)-i \\ 3-i &= (-i)(1+3i)+0 \end{aligned}$$

The last non-zero remainder is $-i$ *which is a unit, so* $gcd(11+3i, 4+11i)$ *is a unit and they are relatively prime.* ◇

Theorem 96. *Gaussian Linear Diophantine Equation*
Let $a, b \in \mathbb{Z}[i]$. *The equation* $ax+by=1$ *has a solution* $x, y \in \mathbb{Z}[i]$ *if and only if* a, b *are relatively prime, that is* $gcd(a,b) = \pm 1$ *or* $\pm i$.

Proof. Suppose there exist $x, y \in \mathbb{Z}[i]$ such that $ax+by=1$. We need to show a, b are relatively prime.
Let $d \in \mathbb{Z}[i]$ be a common factor of a and b. Since $d|a$ and $d|b$,, by Lemma 89 on page 134, $d|ax+by$. So $d|1$ and hence d is a unit. Therefore, by definition, a and b are relatively prime.

*****

Conversely, suppose a, b are relatively prime.
We need to show there exist an $x, y \in \mathbb{Z}[i]$ such that $ax+by=1$.
Consider the set S of all linear combinations of a and b,

$$S = \{ax+by \mid x, y \in \mathbb{Z}[i]\}$$

It follows from the Well-Ordering Principle[4] that there exists a nonzero element $d \in S$ of smallest norm, say $d = ad_1 + bd_2$.
By the Division Algorithm, Theorem 94, page 139, there exist Gaussian integers q, r such that,

$$a = qd + r, N(r) < N(d)$$

Since,

$$r = a - qd = a - q(ad_1 + bd_2) = a(1 - qd_1) + b(-qd_2)$$

then r is a linear combination of a and b so $r \in S$.
But d has the smallest norm of nonzero elements of S, so since $N(r) < N(d)$ then we must have $r = 0$.
Thus,

$$a = qd + r = qd \Rightarrow d|a.$$

[4] The Well-Ordering Principle applied to Gaussian integers states any finite set of Gaussian integers has a "smallest" element, defined as an element with least norm.

By a similar argument $d|b$.
Since a and b are relatively prime then d is a unit.
Since $d \in S$ there exist Gaussian integers x, y such that $ax + by = d$.
Since d is a unit, it has a multiplicative inverse $d^{-1} \in \mathbb{Z}[i]$. Multiplication by d^{-1} yields,

$$axd^{-1} + byd^{-1} = dd^{-1} = 1$$

Hence (xd^{-1}, yd^{-1}) is a solution of $ax + by = 1$. □

Lemma 97. *Gaussian Euclid's Lemma*
Let $d, m, n \in \mathbb{Z}[i]$ be such that d, m are relatively prime so $d \nmid m$. If $d|mn$ then $d|n$.

Proof. If $gcd(d, n)$ is a unit then by Theorem 96 on page 140,there exists an x, y such that

$$dx + ny = 1 \Rightarrow mdx + mny = m.$$

Now $d|mn$ means $mn = dk$ for some $k \in \mathbb{Z}[i]$. Hence substituting,

$$mdx + kdy = m \Rightarrow m = d(mx + ky) \Rightarrow d|m.$$

□

Theorem 98. *Fundamental Property of Gaussian Primes*
Let p be prime in the Gaussian integers and let $a, b \in \mathbb{Z}[i]$. If $p|ab$ then $p|a$ or $p|b$.

Proof. We use a proof by contradiction.
Assume $p \nmid a$ and $p \nmid b$.
Now, by definition, we know a, p are relatively prime in $\mathbb{Z}[i]$ if for all $d \in \mathbb{Z}[i]$

$$d|a \text{ and } d|p \Rightarrow \ d \text{ is a unit.}$$

Since p is prime, only units divide it and since $p \nmid a$ it follows that p, a are relatively prime.
Thus $p|ab$ and $p \nmid a$ so by the Lemma 97, page 141, $p|b$.
This contradicts the assumption, and we conclude $p|a$ or $p|b$. □

Theorem 99. *Fundamental Theorem of Gaussian Arithmetic*
Every non-zero Gaussian integer can be written as a unique (up to order and units) product of Gaussian primes.

Proof. Suppose a factorization into a product of primes does not always exist. Take x to be a Gaussian integer with smallest norm $N(x)$ which is not a product of primes. Then x is not a prime so let $x = ab$ where a, b must each have a smaller norm than x given $N(x) = N(a)N(b)$.
So, by the assumption on x both a, b must be a product of primes. But then $x = ab$ must also be a product of primes so we have a contradiction.

*****

To prove uniqueness, suppose x is the Gaussian integer with smallest norm that has two different expressions as a product of primes thus,

$$x = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

Using Theorem 98 above either $p_1 | q_1$ or $p_1 | q_2 q_3 \cdots q_m$. If $p_1 \nmid q_1$ then either $p_1 | q_2$ or $p_1 | q_3 \cdots q_m$. We must eventually have $p_1 | q_k$ for some k.
Because p_1 is a prime then q_k is p_1 times a unit. Then we can cancel them out and we get a new x with two different expressions and a smaller norm, which contradicts our choice of the original x. □

13.3 Fermat's Two Squares Theorem

We are ready to tackle our major theorem through a series of theorems.

Theorem 100.
Let $n \in \mathbb{N}$. If $n \equiv 3 (\mathrm{mod}\ 4)$ there do NOT exist $a, b \in \mathbb{Z}$ such that $n = a^2 + b^2$.

Proof. Either $a \equiv 0 (\mathrm{mod}\ 4)$ *or* $a \equiv 1 (\mathrm{mod}\ 4)$ *or* $a \equiv 2 (\mathrm{mod}\ 4)$ *or* $a \equiv 3 (\mathrm{mod}\ 4)$.
Then $a^2 \equiv 0 (\mathrm{mod}\ 4)$ *or* $a^2 \equiv 1 (\mathrm{mod}\ 4)$ and so is b^2.
Then $a^2 + b^2 \equiv 0 (\mathrm{mod}\ 4)$ *or* $a^2 + b^2 \equiv 1 (\mathrm{mod}\ 4)$ *or* $a^2 + b^2 \equiv 2 (\mathrm{mod}\ 4)$.
Hence there do NOT exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = n$ if $n \equiv 3 (\mathrm{mod}\ 4)$. □

We do not need the following corollary. But it is a good exercise!

Corollary 101.
Let $p \in \mathbb{N}$. If $p \equiv 3 (\mathrm{mod}\ 4)$ then p is prime as a Gaussian integer.

Proof. Exercise! □

We now prove the other possible primes $p \equiv 1 (\mathrm{mod}\ 4)$ cannot be prime as Gaussian integers. First we need a theorem and a lemma. We will later prove the famous theorem due to Wilson in Chapter 22. Here we are content to simply understand it.

Theorem 102. *(Wilson's Theorem)*
Let $p \in \mathbb{N}$. Then p is prime if and only if,

$$(p-1)! \equiv 1 (\mathrm{mod}\ p).$$

Discussion

For the prime $p = 7$ consider the numbers $1, 2, 3, 4, 5,$ and 6. We will operate on them using multiplication *mod* 7, that is when we multiply any two of them we apply *mod* 7 to the result, taking the smallest non-negative solution. For example we don't write $4 \times 5 = 20$ but $4 \times 5 (\mathrm{mod}\ 7) \equiv 6$.
The numbers $1, 2, 3, 4, 5, 6$ fall into two groups.

The numbers 1 and 6 when multiplied by themselves *mod* 7 both become 1, that is $1 \times 1 \equiv 1 (\text{mod } 7)$ and $6 \times 6 = 36 \equiv 1 (\text{mod } 7)$.
The other numbers $2, 3, 4, 5$ can be grouped so that their multiple is also $1 (\text{mod } 7)$, specifically,

$$2 \times 4 (\text{mod } 7) \equiv 1 \textit{ and } 3 \times 5 (\text{mod } 7) \equiv 1.$$

We say each of the numbers $1, 2, 3, 4, 5, 6$ has a unique inverse *mod* 7.
If you do this analysis for any odd prime (try it with 17), you find the same thing happens. The first and last numbers are their own inverses. Each of the others pairs up with a different one so that their multiple *mod* 17 is 1.
To prove Wilson's Theorem we need to prove this is true for all odd primes p, that is $1,\ p-1$ are their own inverses and $2, 3, \ldots, p-2$ have unique inverses distinct from themselves.
Given that is true, then $(p-2)! = (p-2)(p-3)\cdots 2$ can be rearranged so that the pairs of inverses a, b are together. So since each pair[5] satisfies $ab (\text{mod } p) \equiv 1$, we have,

$$\begin{aligned} (p-2)! &\equiv 1 (\text{mod } p) \\ \Rightarrow (p-1)(p-2)! &\equiv (p-1)(\text{mod } p) \\ \Rightarrow (p-1)! &\equiv -1 (\text{mod } p) \end{aligned}$$

End of Discussion.

Lemma 103.
Let a prime p be such that $p \equiv 1 (\text{mod } 4)$. Then there exists an $x \in \mathbb{Z}$ such that,

$$x^2 \equiv -1 (\text{mod } p).$$

Proof.

$$\begin{aligned} (p-1)! &= 1 \times 2 \times 3 \times \cdots \times (p-1) \\ &= \left[1 \times 2 \times 3 \times \cdots \times \frac{(p-1)}{2} \right] \times \left[\frac{(p+1)}{2} \times \cdots \times (p-2) \times (p-1) \right] \end{aligned}$$

The first bracket of terms are simply,

$$\begin{aligned} 1 &\equiv 1 (\text{mod } p) \\ 2 &\equiv 2 (\text{mod } p) \\ &\ldots \\ \frac{p-1}{2} &\equiv \frac{p-1}{2} (\text{mod } p) \end{aligned}$$

[5] If $ab \equiv 1 (\text{mod } 7)$ and $cd \equiv 1 (\text{mod } 7)$ then their product $abcd \equiv 1 (\text{mod } 7)$. This is so since $ab = 1 + 7k, cd = 1 + 7j \Rightarrow abcd = 1 + 7l, l = k + j + 7kj$.

while the second bracket of terms modulo p repeat the first terms but with negative values, thus,

$$\begin{aligned} p-1 &\equiv -1 (\text{mod } p) \\ p-2 &\equiv -2 (\text{mod } p) \\ &\cdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} (\text{mod } p) \end{aligned}$$

So multiplying all the terms together we conclude,

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 (\text{mod } p)$$

Assume $p \equiv 1(\text{mod } 4) \Rightarrow p = 1 + 4k, k \in \mathbb{Z}$. Let $x = \left(\frac{p-1}{2}\right)!$

Note $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = 1$. Then, by Wilson's Theorem 102,

$$\begin{aligned} (p-1)! &\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 (\text{mod } p) \\ \Rightarrow \left[\left(\frac{p-1}{2}\right)!\right]^2 &\equiv -1 (\text{mod } p) \end{aligned}$$

So, if $p \equiv 1(\text{mod } 4)$ there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv -1(\text{mod } p)$, namely $x = \left(\frac{p-1}{2}\right)!$ □

Example 77. *Let $p = 5$. Then $x = \left(\frac{5-1}{2}\right)! = 2$ so that $x^2 = 4 \equiv -1(\text{mod } 5)$.*

Theorem 104.
If a prime p satisfies $p \equiv 1(\text{mod } 4)$ then p is not prime as a Gaussian integer.

Proof. Since by Lemma 103, $p \equiv 1(\text{mod } 4)$ implies there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv -1(\text{mod } p)$, we have,

$$\begin{aligned} x^2 \equiv -1(\text{mod } 4) &\Rightarrow x^2 = -1 + kp,\ k \in \mathbb{Z} \\ &\Rightarrow x^2 + 1 = kp \\ &\Rightarrow (x-i)(x+i) = kp \\ &\Rightarrow p|(x-i)(x+i) \ in\ \mathbb{Z}[i]. \end{aligned}$$

Suppose p is prime as a Gaussian integer. By Theorem 99, page 141, $p|x-i$ or $p|x+i$ Thus there exists an $m+ni$ such that

$$p(m+ni) = x+i \ or\ p(m+ni) = x-i.$$

Equating the imaginary parts,

$$pn = 1 \text{ or } pn = -1$$

This implies p is a unit and that contradicts the hypothesis that p is prime in $\mathbb{Z}[i]$. So p is not prime as a Gaussian integer. □

Theorem 105. *(Fermat's Two Squares Theorem)*
Let p be an odd prime number. Then there exist $a, b \in \mathbb{N}$ such that $p = a^2 + b^2$ if and only if $p \equiv 1 (\text{mod } 4)$.

Proof. Let p be an odd prime number.
Suppose there exist $a, b \in \mathbb{N}$ such that $p = a^2 + b^2$.
Then, by Theorem 100, page 142 above $p \not\equiv 3 (\text{mod } 4)$ so we must have $p \equiv 1 (\text{mod } 4)$.

*****

Conversely, assume $p \equiv 1 (\text{mod } 4)$.
By Theorem 104 above, p is not prime in $\mathbb{Z}[i]$.
Thus there exist $y, z \in \mathbb{Z}[i]$ such that $p = yz$ with both $N(y), N(z) > 1$.
Now $N(p) = N(y)N(z)$ so $p^2 = N(y)N(z)$ which is only possible if $N(y) = p$ and $N(z) = p$.
But if $N(y) = p$ then since $y = a + bi$ for some a, b, making $N(y) = a^2 + b^2$, we have $p = a^2 + b^2$. □

Theorem 106. *Uniqueness of Fermat's Two Squares Theorem*
Let p be an odd prime such that $p \equiv 1 (\text{mod } 4)$. Then p can be expressed as a sum of two squares in a unique way, up to order ($a^2 + b^2 = b^2 + a^2$).

Proof. Let p be an odd prime such that $p \equiv 1 (\text{mod } 4)$.
Suppose there exist $a, b, c, d \in \mathbb{Z}$ such that,

$$p = a^2 + b^2 \text{ and } p = c^2 + d^2.$$

We want to show $a^2 = c^2$ *and* $b^2 = d^2$ or $a^2 = d^2$ *and* $b^2 = c^2$.
Now we can factor p in two different ways as,

$$p = (a + bi)(a - bi) \text{ and } p = (c + di)(c - di)$$

Since the norm,

$$N(a + bi) = a^2 + b^2 = p$$

then by Lemma 91 on page 136, $a + bi$ must be prime as a Gaussian integer. Similarly, the numbers $a - bi, c + di, c - di$ are all prime as Gaussian integers. Thus,

$$p = (a + bi)(a - bi) \text{ and } p = (c + di)(c - di)$$

are two ways to factor p as a product of prime Gaussian integers.
By the Fundamental Theorem of Gaussian Arithmetic, Theorem 98, page 141, these two factorizations must be the same up to order and units. In particular,

$$a + bi = c + di \text{ } or \text{ } a + bi = u(c - di)$$

for some unit u.
The possibilities are,

$$\begin{aligned} a + bi = \pm 1(c + di) &\Rightarrow a = \pm c, b = \pm d \Rightarrow a^2 = c^2, b^2 = d^2 \text{ } or \\ a + bi = \pm i(c - di) &\Rightarrow a = \pm d, b = \pm c \Rightarrow a^2 = d^2, b^2 = c^2 \end{aligned}$$

where we equated real and imaginary parts. So $a^2 + b^2$ is unique for each $4k + 1$ prime. □

13.4 Finding a, b for a given p.

We will discuss group theory in Chapter 24. For the present we will simply say a group is a set of numbers together with an operation such as addition or multiplication subject to certain conditions or axioms.

13.4.1 Two Finite Groups

Definition 50. *The additive group $\mathbb{Z}_p$*
The group $\mathbb{Z}_p$ is formed from the integers $\mathbb{Z}$ by applying mod p *to every integer $n \in \mathbb{Z}$. Accordingly,*

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p - 1\}$$

since when any n is divided by p the least positive remainders are 0,1,. . . ,p-1. Associated with the group $\mathbb{Z}_p$ is the operation of addition modulo p so that if $a, b \in \mathbb{Z}_p$ then we operate to get,

$$a + b \equiv c(\text{mod } p)$$

where $c \in \mathbb{Z}_p$.

Example 78. $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ *together with the operation of addition* mod 7. *So we have for example,*

$$4 + 5 \equiv 2(\text{mod } 7), \quad 2 \in \mathbb{Z}_7. \qquad \diamond$$

Definition 51. *The multiplicative group $\mathbb{Z}_p^*$*
We define the set $\mathbb{Z}_p^*$ by

$$\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p - 1\}$$

or $\mathbb{Z}_p$−$\{0\}$. Associated with this group is the operation "multiplication mod p" by which we mean that whenever we multiply any two positive integers we always apply mod p *to the result. The significance of the "*" is to indicate integers divisible by p have been excluded when $\mathbb{Z}_p^*$ is formed from $\mathbb{Z}$. The removal of the element 0, originating from any integer divisible by p, is due to the fact 0 does not have a multiplicative inverse and we need our group $\mathbb{Z}_p^*$ to have inverses as we shall see.*

Example 79. $\mathbb{Z}_5^* = \{1,2,3,4\}$ *and* $3 \times 4 \equiv 2 (\bmod\ 5)$. *If we are working within* $\mathbb{Z}_5^*$ *we simply say* $3 \times 4 = 2$. ⋄

13.4.2 Primitive roots or generators

Definition 52. *primitive root*
Some of the elements of $\mathbb{Z}_p^*$ are called primitive roots or generators, meaning that if we repeatedly multiply them by themselves, applying mod p each time, then we obtain all the other elements of the group.

Example 80. $\mathbb{Z}_5^* = \{1,2,3,4\}$ *is generated by 3 since under repeated multiplication we have,*

$$\begin{aligned} 3 &\equiv 3(\bmod\ 5) \\ 3 \times 3 &\equiv 9(\bmod\ 5) \equiv 4(\bmod\ 5) \\ 3 \times 3 \times 3 &\equiv 27(\bmod\ 5) \equiv 2(\bmod\ 5) \\ 3 \times 3 \times 3 \times 3 &\equiv 81(\bmod\ 5) \equiv 1(\bmod\ 5) \\ 3 \times 3 \times 3 \times 3 \times 3 &\equiv 243(\bmod\ 5) \equiv 3(\bmod\ 5) \end{aligned}$$

Thereafter we just get repetition of 1,2,3,4 such as,

$$3^{18} = (3^4)^4 3^2 \equiv 1^4 \times 9(\bmod\ 5) \equiv 4(\bmod\ 5)$$

where we used the result above of $81 = 3^4 \equiv 1(\bmod\ 5)$.

Only some of the elements are primitive roots. For example, 2 is not a generator of $\mathbb{Z}_5^*$ since

$$\begin{aligned} 2 &\equiv 2(\bmod\ 5) \\ 2 \times 2 &\equiv 4(\bmod\ 5) \\ 2 \times 2 \times 2 &\equiv 8(\bmod\ 5) \equiv 3(\bmod\ 5) \\ 2 \times 2 \times 2 \times 2 &\equiv 16(\bmod\ 5) \equiv 1(\bmod\ 5) \\ 2 \times 2 \times 2 \times 2 \times 2 &\equiv 32(\bmod\ 5) \equiv 2(\bmod\ 5) \end{aligned}$$

so the element 5 is not generated. ⋄

Definition 53. *order of a group element.*
The order of an element a of the group $\mathbb{Z}_p^*$ is the smallest power n such that $a^n \equiv 1(\bmod\ p)$. If the smallest power is all the way up to $p-1$ we say a has maximum order.

Example 81. *In $\mathbb{Z}_5^*$ since*

$$4^1 = 4(\text{mod } 5); 4^2 \equiv 1(\text{mod } 5)$$

we conclude the order of 4 is 2. But as we saw in the previous example of the powers of 3 and 2 only $3^4 \equiv 1(\text{mod } 5)$, so 3 has order 4 which is $p-1 = 5-1 = 4$ so 3 has maximum order. ◇

Note 19.
Clearly any primitive root or generator must have maximum order to be able to produce $p-1$ elements, just as 3 did in $\mathbb{Z}_5^*$. That is, if g is a generator or primitive root then,

$$g^{p-1} \equiv 1(\text{mod } p) \text{ but } g^j \not\equiv 1(\text{mod } p), \text{ if } j \neq p-1$$

Note this means,

$$g^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$$

since we cannot also have $g^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$

Example 82. *In $\mathbb{Z}_5^*$ we have $3^{\frac{5-1}{2}} = 3^2 \equiv 4(\text{mod } 5) \equiv -1(\text{mod } 5)$, so 3 is a generator of $\mathbb{Z}_5^*$.* ◇

13.4.3 Finding a, b

With that knowledge let's now proceed to find a, b for $p = a^2 + b^2, p \equiv 1(\text{mod } p)$. In the proof of the Two Squares Theorem 105, page 145, we had $p = yz$ where $y = a + bi$. So to find a, b we simply need to factor p in $\mathbb{Z}[i]$.
By Lemma 103 on page 143, we know there is an x satisfying $x^2 \equiv -1(\text{mod } p)$. Then,

$$x^2 + 1 = kp \Rightarrow (x+i)(x-i) = kp = k(a^2 + b^2) = k(a+bi)(a-bi)$$

Now in the proof of the Uniqueness Theorem 106, page 145, we showed $a + bi, a - bi$ are primes in $\mathbb{Z}[i]$.
Then $(x+i)(x-i) = k(a+bi)(a-bi)$ means one of $a \pm bi$ divides $x + i$. They cannot both divide $x + i$ since we are then left with $k = x - i$ but k is an integer.
Then that value of $a \pm bi$ is the $gcd(x + i, p)$ since both of $a \pm bi$ divide p. So to find a, b we need to find $gcd(x + i, p)$. First we must find x.

Suppose $d^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$. Let $x = d^{\frac{p-1}{4}} \Rightarrow x^2 = d^{\frac{p-1}{2}}$ so x satisfies $x^2 \equiv -1(\text{mod } p)$.
Now $d^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$ means $d^{p-1} \equiv 1(\text{mod } p)$ so d has order $p-1$ in $\mathbb{Z}_p^*$ but, more importantly, $d^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$ means d is a primitive root or has maximum possible

order in $\mathbb{Z}_p^*$. So we actually need to find a primitive root d in $\mathbb{Z}_p^*$ and set $x = d^{\frac{p-1}{4}}$.

We can do[6] that by letting $d = 2, 3, 5, 7, 11, \ldots$ or successive primes, until we find a value of d such that $d^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$.
Once we have found a primitive root we can compute x and then $gcd(x + i, p)$, by using the Gaussian Euclidean Algorithm, Theorem 95, page 139.

Example 83. *Consider the prime number* $193 \equiv 1(\text{mod } 4)$ *where* $\dfrac{p-1}{2} = 96$.
We look in $2, 3, 5, 7, 11, \ldots$ *for a value of* d *such that* $d^{96} \equiv -1(\text{mod } p)$.

$$\begin{aligned}2^{96}(\text{mod } 193) &\equiv 1\\ 3^{96}(\text{mod } 193) &\equiv 1\\ 5^{96}(\text{mod } 193) &\equiv 192 \textit{ or } -1\end{aligned}$$

So 5 *is a primitive root of* $\mathbb{Z}_{193}^*$.
Then x *is given by*

$$5^{\frac{192}{4}}(\text{mod } 193) \equiv 112.$$

We now find $gcd(112 + i, 193)$ *using the construct from the Gaussian Euclidean Algorithm,*

$$\begin{aligned}
a &= q_1 b + r_1 & N(r_1) &< N(b) && (13.4.1)\\
b &= q_2 r_1 + r_2 & N(r_2) &< N(r_1) && (13.4.2)\\
r_1 &= q_3 r_2 + r_3 & N(r_3) &< N(r_2) && (13.4.3)\\
&\ldots & & && (13.4.4)\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} & N(r_{n-1}) &< N(n) && (13.4.5)\\
r_{n-2} &= q_n r_{n-1} + r_n & N(r_n) &< N(r_{n-1}) && (13.4.6)\\
r_{n-1} &= q_{n+1} r_n + 0 & & && (13.4.7)
\end{aligned}$$

With $a = 193$ *and* $b = 112 + i$ *we have,*

$$193 = (112 + i)q_1 + r_1$$

So we divide[7] *to find,*

$$\frac{193}{112 + i} = \frac{112}{65} - \frac{1}{65}i$$

[6] There is a very powerful computational program called "gp Pari" available free on the internet. It takes a few minutes to download but is well worth the trouble for a number theorist. Once you have downloaded it then run it to get the gp prompt. Type, for example, Mod(2 uparrow 96,193), to find $2^{96}(\text{mod } 193)$. Of course it has an accompanying user manual!

[7] To find $\dfrac{193}{112 + i}$ in gp Pari, type $(193{+}0{*}I)/(112{+}1{*}I)$ to get the immediate response $\dfrac{112}{65} - \dfrac{1}{65} * I$.

For the right side we take the nearest complex number with whole integers, namely $2 - 0i = 2$*, put* $q_1 = 2$ *and construct,*

$$193 = (112 + i) \times 2 - 31 - 2i$$

which is (13.4.1) above. Similarly, to find $112 + i = q_2(-31 - 2i) + r_2$ *we calculate,*

$$\frac{112 + i}{-31 - 2i} = -\frac{18}{5} + \frac{1}{5}i$$

and choose $q_2 = -4 + 0i$ *so we construct (13.4.2) above as,*

$$112 + i = (-31 - 2i)(-4) - 12 - 7i$$

Finally $\dfrac{-31 - 2i}{-12 - 7i} = 2 - i$ *with a remainder of 0, so for (13.4.7) we find,*

$$-31 - 2i = (-12 - 7i)(2 - i) + 0$$

so the $gcd(112 + i, 193) = -12 - 7i$ *giving by* $gcd(x + i, p) = a + bi$*, the result,*

$$193 = 12^2 + 7^2.$$

Finally we note we have also found the factors of 193 *in* $k(i)$ *since,*

$$(12 + 7i)(12 - 7i) = 193$$

Part V

Shopping Excursion III Exponential and Trigonometric Functions

In Chapter 14 we introduce the natural exponential function and two of the trigonometric functions, sine and cosine. We find their derivatives.

In Chapter 15 we are introduced to a major breakthrough theorem in mathematics, the proof that many functions can be expressed as an infinite series. We find those series for our new functions.

Chapter 14

Calculus of Exponential and Trigonometric Functions

Ingredients
Definition of exponential functions in general.
Definition of natural exponential function in particular.
Definitions of angles, degrees, radians, unit circle.
Definitions of the trigonometric functions sine and cosine.
Directions
Find the derivative of e^x.
Prove the addition identities for sine and cosine functions.
Find the derivatives of the sine and cosine functions.

14.1 The Natural Exponential Function

Definition 54. *exponential function*
An exponential function is of the form $f(x) = b^x, b > 1, x \in \mathbb{R}$.

Example 84. *Some exponential functions are $f(x) = 2^x, f(x) = 3^{-x}, f(x) = \pi^x$.*

14.1.1 Graphs of exponential functions

The graphs of all exponential functions b^x with $x > 0$ pass through $(0, 1)$ and they all have the same basic shape, climbing exponentially for $x > 0$ and having the negative $x-$axis as an asymptote. See Figure 16.

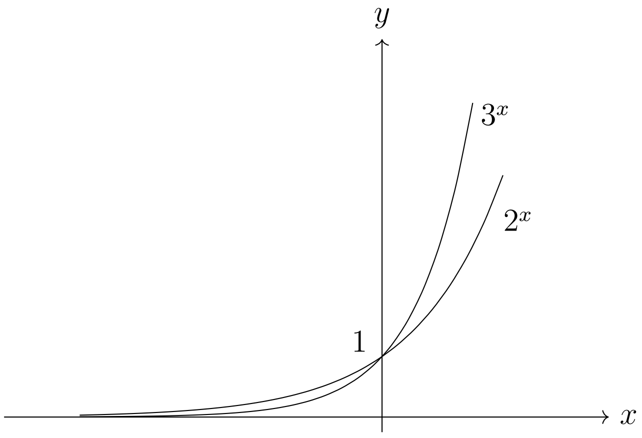


Figure 16

14.1.2 Natural Exponential Function

Definition 55. *natural exponential function*
The natural exponential function $f(x) = e^x$ is the exponential function whose gradient at $(0,1)$ is exactly 1.

Note 20. *The slopes of the secant lines of $2^x, 3^x$ between $x = 0$ and $x = 0.1$ are approximately the same as the slope of the tangent lines to these two functions at $(0,1)$. (See Figure 17 below for an example) By using $m = \dfrac{y_2 - y_1}{x_2 - x_1}$ and a calculator, these two tangent line slopes are approximately 0.7 and 1.1 respectively. Accordingly, since e^x has slope 1, we estimate e is between 2 and 3. It is actually $2.71828\ldots$ as we shall prove in a later chapter.*

14.1.3 Derivative of the Natural Exponential Function

Theorem 107.
The derivative of $f(x) = e^x$ is $f'(x) = e^x$.

Proof. Consider a point (h, e^h) near the origin on the graph of $f(x) = e^x$. See Figure 17.

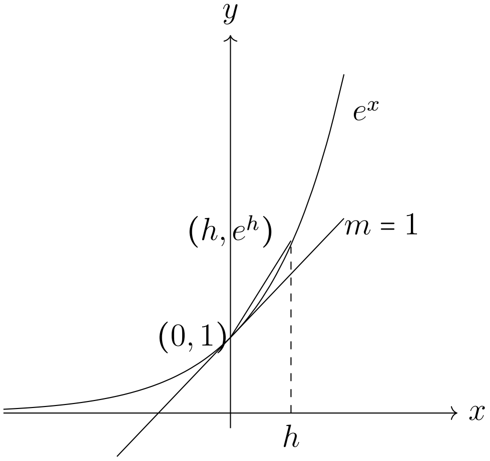


Figure 17

From the diagram, for the tangent at $(0, 1)$ we have,

$$m_{tan} = \lim_{h \to 0} m_{sec} = \lim_{h \to 0} \frac{e^h - 1}{h - 0}$$

By our definition of $f(x) = e^x$, $m_{tan} = 1$ so that,

$$\lim_{h \to 0} \frac{e^h - 1}{h} = 1$$

Then,

$$\begin{aligned} \frac{d}{dx}(e^x) &= \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \\ &= \lim_{h \to 0} \frac{e^{x+h} - e^x}{h} \\ &= e^x \left(\lim_{h \to 0} \frac{e^h - 1}{h} \right) \\ &= e^x \end{aligned}$$

□

Note 21.
e^x may be defined as the unique function whose derivative is itself.

14.2 The Trigonometric Functions

14.2.1 Angle

The standard way to draw an angle on the Cartesian plane is to draw two rays or half-lines out from the origin.

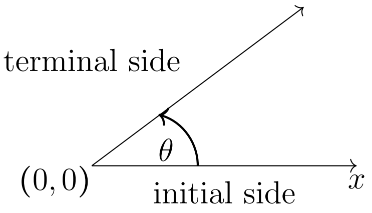


Figure 18A: Positive Angles

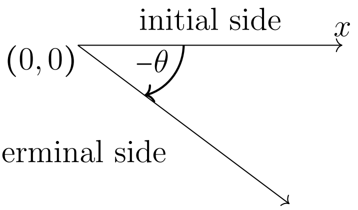


Figure 18B: Negative Angles

One of the rays is the positive $x-$axis. We call this the initial side of the angle. The other is called the terminal side. The terminal side starts also on the positive $x-$axis and rotates counterclockwise to form positive angles (Figure 18A) and clockwise to form negative angles (Figure 18B).

14.2.2 Degree

Definition 56. *degree*
If the terminal side rotates counterclockwise to finish on the positive $y-$axis we measure the angle as 90 degrees or 90^0. See the first diagram below. All other angles are some multiple, positive or negative, of 90^0.

Example 85. *This leads to the following examples of angles measured in degrees.*

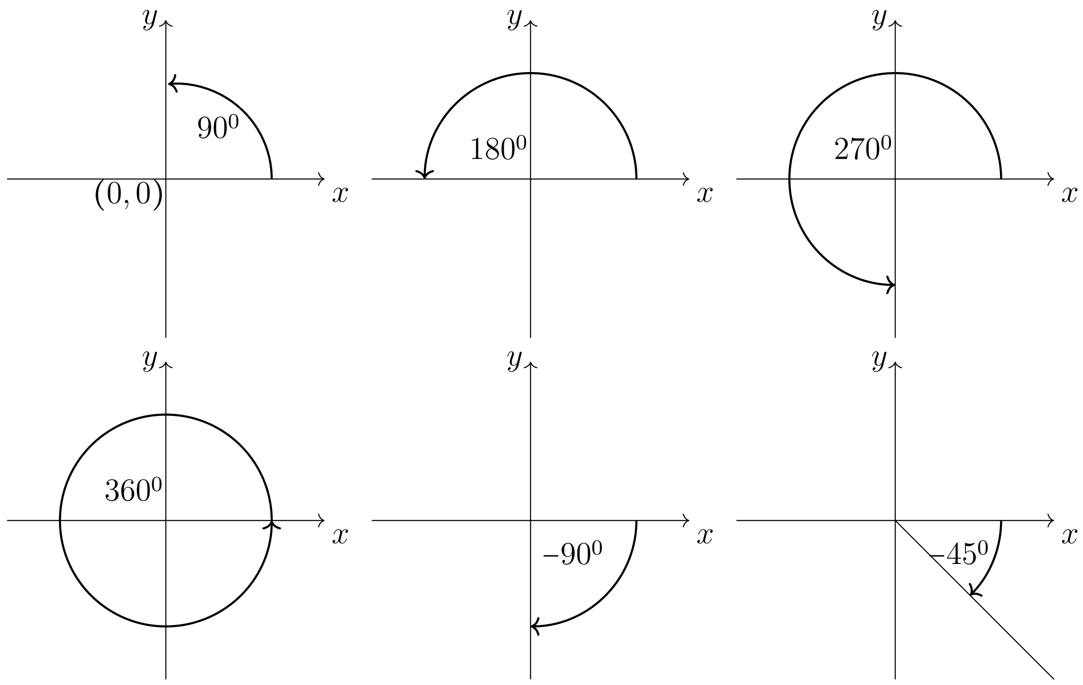


Figure 19

Angles can be formed by more than one rotation. Hence we have:

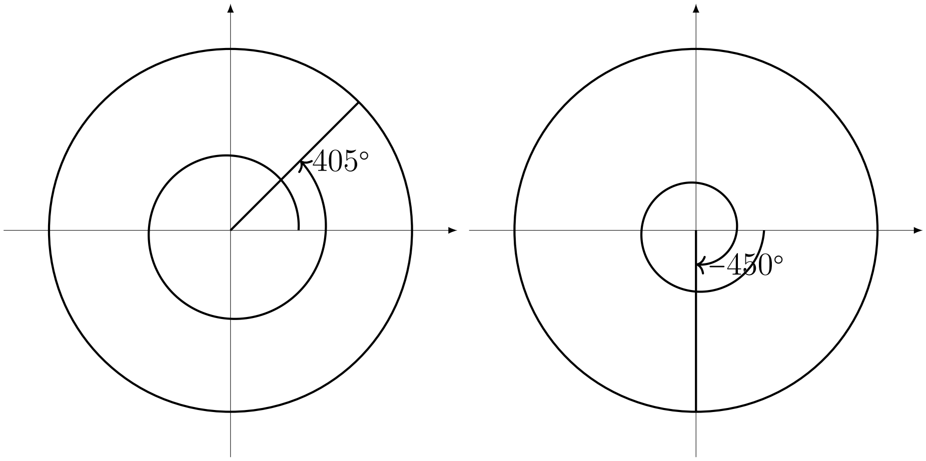
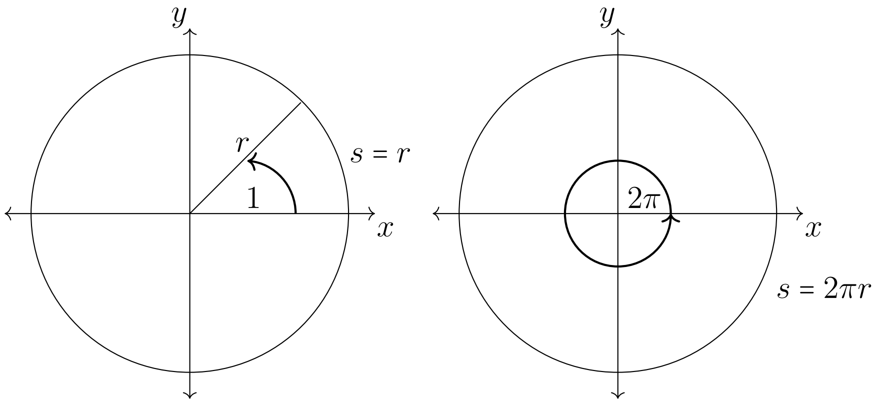


Figure 20

14.2.3 Radian

If we draw a circle of radius r centered at the origin, its circumference is $2\pi r$. We use the symbol s for the length of an arc of the circle.

Definition 57. *radian*
An angle of measure one radian is the angle subtended[1] *at the origin of a circle of radius r by an arc of the circle of length r. See Figure 21.*



Angle of 1 radian Angle of 2π radians

Figure 21

Algebraically, this means the arc length s, radius r and angle θ in radians are related by,

$$s = r\theta \Rightarrow \theta = \frac{s}{r},$$

[1] "Subtended" means formed by the rays drawn from the ends of the arc to the center

since if $s = 2r, \theta = 2$ radians, if $s = 3r, \theta = 3$ radians, and so on.

If we take one complete revolution, then the arc length is simply the circumference of the circle, that is, $s = 2\pi r$. Then $\theta = \frac{s}{r} = \frac{2\pi r}{r} = 2\pi$ radians or the angle subtended by the whole circle at the center is 2π radians. See Figure 21.

Similarly, given the area πr^2 of a whole circle subtended by an angle of 2π radians at the center may be written as $\frac{1}{2}r^2(2\pi)$ it is easy to see the area of the sector of a circle subtended by an angle θ at the center is given by

$$A = \frac{1}{2}r^2\theta$$

14.2.4 Radians and Degrees

Since the angle subtended by the whole circle at the center is also 360^0 it follows that,

$$\begin{aligned} 2\pi \ radians &= 360^0 \\ \Rightarrow 1 \ radian &= \frac{180^0}{\pi} \\ \Rightarrow 1^0 &= \frac{\pi}{180} \ radians. \end{aligned}$$

The common angles are related as follows. Note, when we write an angle in radians, we normally omit the word "radians", that is $\pi = \pi$ radians.

Degrees	0^0	30^0	45^0	60^0	90^0	180^0	270^0	360^0
Radians	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π

14.2.5 Trigonometric Functions

We define the trigonometric functions on a unit circle.

Definition 58. *unit circle*
A unit circle on the Cartesian plane is a circle of radius 1 centered at the origin $(0, 0)$.

Definition 59. *sine, cosine and tangent functions*
To define the trigonometric functions, we take a number line $(-\infty, +\infty)$, *place its 0 point on the unit circle's* $(1, 0)$ *point and wrap its positive half around the unit circle in a counter-clockwise sense and its negative half in a clockwise sense. Then every*

real number may be found somewhere on this "wrapped" unit circle.

Let θ be any real number and $P(x,y)$ be the point on the wrapped unit circle corresponding to an angle θ subtended at the origin by the arc AP where $A = (1,0)$. See Figure 22.

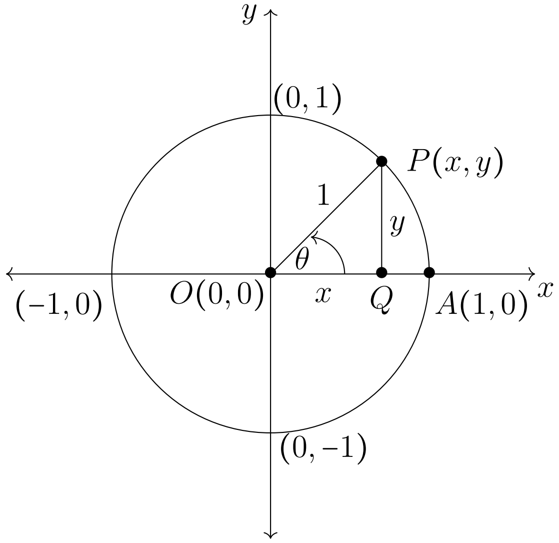


Figure 22

We define the trigonometric functions sine, cosine and tangent[2] *by,*

$$\sin\theta = y,\ \cos\theta = x,\ \tan\theta = \frac{\sin\theta}{\cos\theta} = \frac{y}{x},\ (x \neq 0.)$$

Accordingly we can label the point $P(x,y)$ as $P(\cos\theta, \sin\theta)$ as in Figure 23.

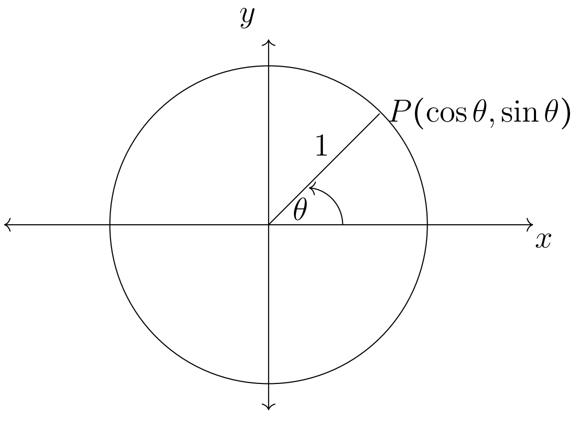


Figure 23

[2] We do not use the tangent function in this book.

Theorem 108. *(Pythagorean Identity)*

$$\sin^2\theta + \cos^2\theta = 1$$

Proof. Apply the Pythagorean theorem to the triangle POQ in Figure 22 to obtain,

$$x^2 + y^2 = 1 \Rightarrow \sin^2\theta + \cos^2\theta = 1.$$

□

14.2.6 Important Values of the Trigonometric Functions

We note from Figure 22 that the terminal rays for $\theta = 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi$ finish at $(0,0), (0,1), (-1,0), (0,-1)$ *and* $(0,0)$ respectively. So we have,

θ	0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π
$\sin\theta$	0	1	0	-1	0
$\cos\theta$	1	0	-1	0	1

Note 22. *We note values of* $\sin\theta$ *and* $\cos\theta$ *are not limited to* $0 \le \theta \le 2\pi$. *In particular as we increase the angles on the unit circle in either a clockwise or anti-clockwise sense, we find* $\sin k\pi = 0$ *for all* $k \in \mathbb{Z}$ *and* $\cos k\pi = \pm 1$ *depending on whether* k *is even or odd.*

14.3 Right Triangle Trigonometry

A major application of trigonometry is in the solution of right-angle triangles. This means, given some of the sides and angles, find the others. We can label any right-angle triangle as shown in Figure 24, the labels opposite and adjacent being with reference to the acute angle θ.

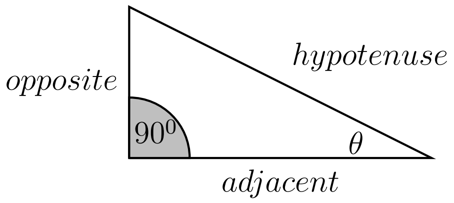


Figure 24

We can then superimpose this triangle on the unit circle as shown in Figure 25.

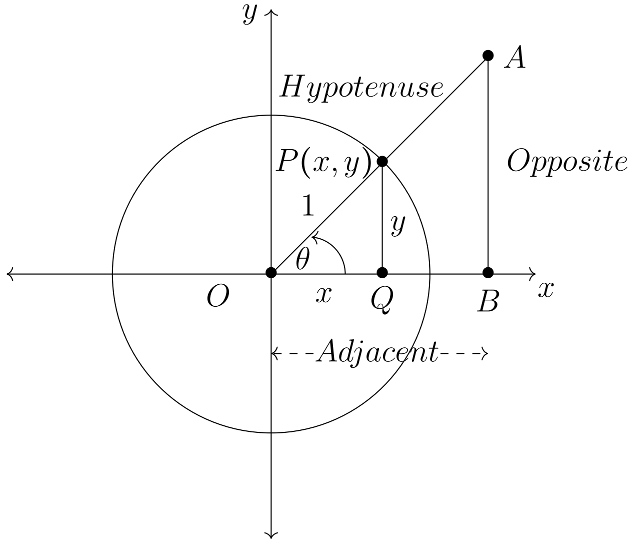


Figure 25

The triangles OPQ and OAB are similar triangles. They have the same angles $\theta, 90^0 - \theta, 90^0$ and therefore their corresponding sides are in the same ratio. Then,

$$\frac{y}{1} = \frac{opposite\ AB}{hypotenuse\ OA} \Rightarrow \sin\theta = \frac{opposite}{hypotenuse}$$
$$\frac{x}{1} = \frac{adjacent\ OB}{hypotenuse\ OA} \Rightarrow \cos\theta = \frac{adjacent}{hypotenuse}$$
$$\frac{y}{x} = \frac{opposite\ AB}{adjacent\ OA} \Rightarrow \tan\theta = \frac{opposite}{adjacent}$$

-

Example 86. *Let's find the trigonometric values of the angle θ in the triangle shown in Figure 26.*

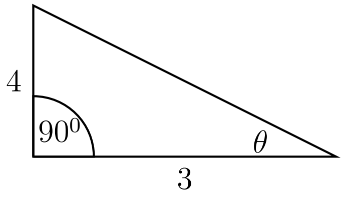


Figure 26

By the Pythagorean Theorem, the hypotenuse $= \sqrt{3^2 + 4^2} = 5$.
We also have Adjacent $= 3$ *and Opposite* $= 4$. *The values are,*

$$\sin\theta = \frac{4}{5},\ \cos\theta = \frac{3}{5},\ \tan\theta = \frac{4}{3}$$

14.4 Some Important Trigonometric Identities

Theorem 109.

$$\sin\theta = \cos(\frac{\pi}{2} - \theta) \tag{14.4.1}$$

$$\cos\theta = \sin(\frac{\pi}{2} - \theta) \tag{14.4.2}$$

Proof. From the triangle in Figure 27,

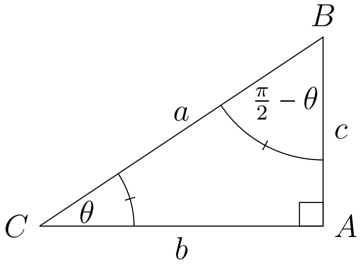


Figure 27

we have:

$$\sin\theta = \cos(\frac{\pi}{2} - \theta) \textit{ since both equal } \frac{c}{a}$$
$$\cos\theta = \sin(\frac{\pi}{2} - \theta) \textit{ since both equal } \frac{b}{a}$$

□

We can prove these identities for general $\theta \in \mathbb{R}$ by positioning the angles θ and $\frac{\pi}{2} - \theta$ in the unit circle.

Theorem 110.

$$\sin(-\theta) = -\sin\theta \tag{14.4.3}$$

$$\cos(-\theta) = \cos\theta \tag{14.4.4}$$

Proof. Since $\sin\theta$ and $\cos\theta$ are the y and x coordinates respectively of the angle θ's terminal ray's intersection with the unit circle it is obvious from Figure 28 that by comparing the x and y coordinates of A and B,

$$\sin(-\theta) = -\sin\theta$$
$$\cos(-\theta) = \cos\theta$$

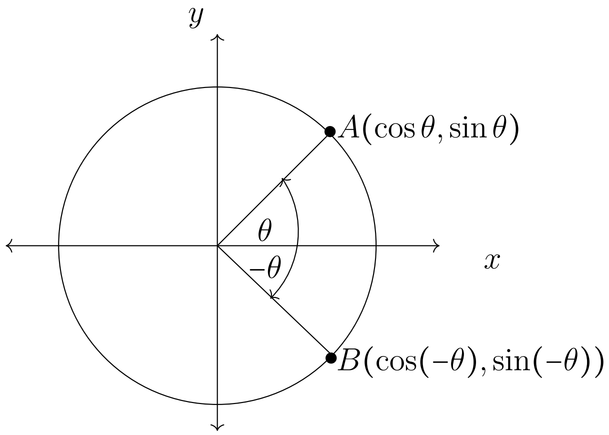

y
x
$A(\cos\theta, \sin\theta)$
θ
$-\theta$
$B(\cos(-\theta), \sin(-\theta))$

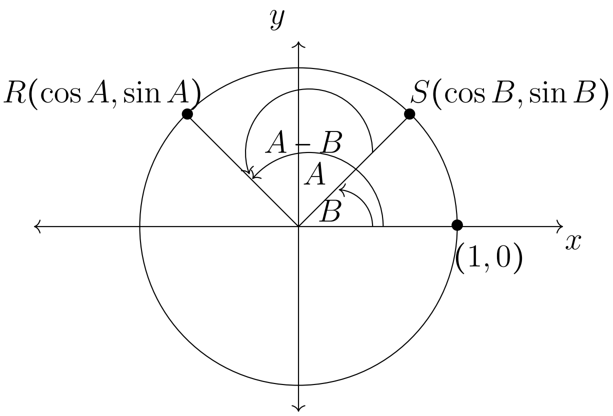
Figure 28

□

Theorem 111. *(Addition Formulas)*
If A, B are any two angles, we prove the Addition formulas,

$$\sin(A+B) = \sin A\cos B + \cos A\sin B \tag{14.4.5}$$
$$\sin(A-B) = \sin A\cos B - \cos A\sin B \tag{14.4.6}$$
$$\cos(A+B) = \cos A\cos B - \sin A\sin B \tag{14.4.7}$$
$$\cos(A-B) = \cos A\cos B + \sin A\sin B \tag{14.4.8}$$

Proof. We obtain Figure 30 from Figure 29 by repositioning the arc RS so that S is at $(1,0)$.



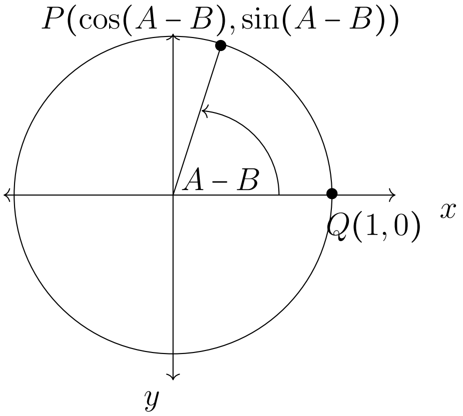


Figure 29 Figure 30

Clearly $PQ = RS \Rightarrow PQ^2 = RS^2$.
Using the distance formula, $P_1P_2^2 = (x_2-x_1)^2+(y_2-y_1)^2$ and the Pythagorean Identity

$\sin^2\theta + \cos^2\theta = 1$ we have,

$$\begin{aligned}
&PQ^2 = RS^2\\
&\Rightarrow [\cos(A-B)-1]^2 + \sin^2(A-B) = [\cos A - \cos B]^2 - [\sin A - \sin B]^2\\
&\Rightarrow \cos^2(A-B) - 2\cos(A-B) + 1 + \sin^2(A-B)\\
&\qquad\qquad = \cos^2 A - 2\cos A\cos B + \cos^2 B + \sin^2 A - 2\sin A\sin B + \sin^2 B\\
&\Rightarrow -2\cos(A-B) + \cancel{2} = -2\cos A\cos B - 2\sin A\sin B + \cancel{2}\\
&\Rightarrow \cos(A-B) = \cos A\cos B + \sin A\sin B
\end{aligned}$$

Putting $B = -B$ and using Theorem 110, page 162, that $\sin(-x) = -\sin x$ and $\cos(-x) = \cos x$ we have,

$$\cos(A+B) = \cos A\cos B - \sin A\sin B$$

Using (14.4.1) and (14.4.2) we have,

$$\begin{aligned}
\sin(A+B) &= \cos\left(\frac{\pi}{2} - (A+B)\right)\\
&= \cos\left((\frac{\pi}{2} - A) + B\right)\\
&= \cos\left(\frac{\pi}{2} - A\right)\cos B + \sin\left(\frac{\pi}{2} - A\right)\sin B\\
&= \sin A\cos B + \cos A\sin B
\end{aligned}$$

Replace B with $-B$ to obtain the final result,

$$\sin(A-B) = \sin A\cos B - \cos A\sin B$$

□

14.5 Derivatives of the Sine and Cosine Functions

We first prove the following limits.

Theorem 112.

(a) $\displaystyle\lim_{x\to 0}\frac{\sin x}{x} = 1$

(b) $\displaystyle\lim_{x\to 0}\frac{\cos x - 1}{x} = 0$

Proof. (a) Consider the unit circle in Figure 31.

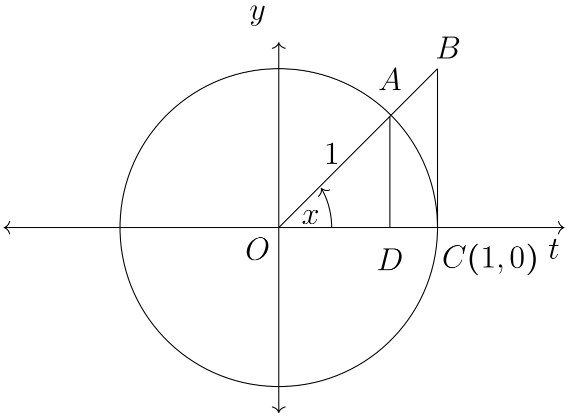


Figure 31

By definition $\sin x = AD,\ \cos x = OD$. By the similar triangles OAD and OBC,

$$\frac{BC}{1} = \frac{AD}{OD} = \frac{\sin x}{\cos x}$$

Now for the triangles OAD, OBC and the sector OAC,

$$\begin{aligned}
&Area \triangle OAD < Area \ \lhd OAC < Area \triangle OBC \\
&\Rightarrow \frac{1}{2}\cdot \sin x \cdot \cos x < \frac{1}{2}\cdot 1^2 \cdot x < \frac{1}{2}\cdot 1 \ \cdot \frac{\sin x}{\cos x} \\
&\Rightarrow \cos x < \frac{x}{\sin x} < \frac{1}{\cos x}
\end{aligned}$$

Now $\lim\limits_{x\to 0}\cos x = \lim\limits_{x\to 0}\dfrac{1}{\cos x} = 1$ so by the Squeeze Theorem 65, page 93, we have,

$$\lim_{x\to 0}\frac{x}{\sin x} = 1$$

(b) We have,

$$\begin{aligned}
\lim_{x\to 0}\frac{1-\cos x}{x} &= \lim_{x\to 0}\frac{1-\cos x}{x}\cdot\frac{1+\cos x}{1+\cos x} \\
&= \lim_{x\to 0}\frac{1-\cos^2 x}{x(1+\cos x)} \\
&= \lim_{x\to 0}\frac{\sin^2 x}{x(1+\cos x)} \\
&= \lim_{x\to 0}\frac{\sin x}{x}\cdot\lim_{x\to 0}\frac{\sin x}{1+\cos x} \\
&= 1\cdot\frac{0}{1+1} \\
&= 0
\end{aligned}$$

□

Theorem 113. *(Derivatives of sine and cosine functions)*

$$\begin{aligned} \frac{d}{dx}(\sin x) &= \cos x \\ \frac{d}{dx}(\cos x) &= -\sin x \end{aligned}$$

Proof. We use the definition of the derivative and Theorems 111 and 112.

$$\begin{aligned} &\frac{d}{dx}(\sin x) \\ &= \lim_{h\to 0} \frac{\sin(x+h) - \sin x}{h} \\ &= \lim_{h\to 0} \frac{\sin x \cos h + \cos x \sin h - \sin x}{h} \\ &= \lim_{h\to 0} \frac{\sin x(\cos h - 1)}{h} + \lim_{h\to 0} \frac{\cos x \sin h}{h} \\ &= -\sin x \lim_{h\to 0} \frac{1 - \cos h}{h} + \cos x \lim_{h\to 0} \frac{\sin h}{h} \\ &= -\sin x \cdot 0 + \cos x \cdot 1 \\ &= \cos x \end{aligned}$$

$$\begin{aligned} &\frac{d}{dx}(\cos x) \\ &= \lim_{h\to 0} \frac{\cos(x+h) - \cos x}{h} \\ &= \lim_{h\to 0} \frac{\cos x \cos h - \sin x \sin h - \cos x}{h} \\ &= \lim_{h\to 0} \frac{\cos x(\cos h - 1) - \sin x \sin h}{h} \\ &= \lim_{h\to 0} \cos x \frac{\cos h - 1}{h} - \lim_{h\to 0} \sin x \frac{\sin h}{h} \\ &= \cos x \cdot 0 - \sin x \cdot 1 \\ &= -\sin x \end{aligned}$$

□

Chapter 15

Taylor Series and Roots of Unity

15.1 Mean Value Theorem

The mean value theorem of Calculus states that if a line segment is drawn joining the end points of a smooth curve then there is at least one point $(c, f(c))$ on the curve where the tangent at that point and the line segment are parallel or have the same slope. The diagram below illustrates the theorem. If the line segment has a slope of zero then there are an infinite number of such points with $x-$coordinate c. Otherwise, the number of c points depends upon the number of maximum and minimum points between the two end points.

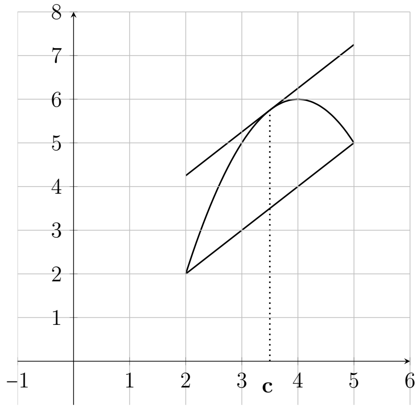


Figure 32

Let us now consider a general theorem that can be used to express "nice" or smooth functions as a polynomial-type infinite series called, after their discoverer, Taylor Series.

15.2 Taylor Series

Definition 60. *smooth function*
A smooth function at a point is a function that can be differentiated an infinite number of times at that point. That is we can differentiate the function as many times as we like and all the derivatives exist.

Example 87.
$f(x) = e^x$ is smooth for all x since $f'(x) = f''(x) = f'''(x) = \ldots = e^x$.

$f(x) = \sin x$ is smooth for all x since $f'(x) = \cos x, f''(x) = -\sin x, f'''(x) = -\cos x$, $f^4(x) = \sin x$ and these four just keep on repeating in the same order.

$f(x) = \sqrt{x}$ exists at $x = 0$ but is not smooth there since all the derivatives have a power of x in the denominator, thus $f'(x) = \dfrac{1}{2\sqrt{x}}$, etc., which do not exist at $x = 0$. ◇

Theorem 114.
Suppose a smooth function has the representation $f(x) = c_0 + c_1x + c_2x^2 + \ldots$ for all values of x near 0. Then,

$$c_n = \frac{f^{(n)}(0)}{n!} \ for\ all\ n \in \mathbb{Z}^+ \cup \{0\}$$

Proof.

$$\begin{aligned}
f(x) &= c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + \ldots + c_nx^n + \ldots \\
f'(x) &= 1!c_1 + 2c_2x + 3c_3x^2 + 4c_4x^3 + \ldots + nc_nx^{n-1} + \ldots \\
f''(x) &= 2!c_2 + 3\cdot 2c_3x + 4\cdot 3c_4x^2 + \ldots + n(n-1)c_nx^{n-2} + \ldots \\
f'''(x) &= 3!c_3 + 4\cdot 3\cdot 2c_4x + \ldots + n(n-1)(n-2)c_nx^{n-3} + \ldots \\
&\vdots
\end{aligned}$$

Substituting $x = 0$ into these equations yields,

$$c_0 = f(0),\ c_1 = \frac{f'(0)}{1!},\ c_2 = \frac{f''(0)}{2!},\ c_3 = \frac{f'''(0)}{3!},\ c_4 = \frac{f^{(4)}(0)}{4!}, \ldots \Rightarrow c_n = \frac{f^{(n)}(0)}{n!}$$

□

Theorem 115.
Suppose a function is smooth for all points in an interval about $x = 0$. Then for all x in that interval, we can write,

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + R_n(x),$$

where the remainder $R_n(x) = \dfrac{f^{(n+1)}(c)}{(n+1)!}x^{n+1}$ and c is some point between x and 0.

Proof. Define,

$$R_n(x) = f(x) - f(0) - \frac{f'(0)}{1!}x - \frac{f''(0)}{2!}x^2 - \frac{f'''(0)}{3!}x^3 - \ldots - \frac{f^{(n)}(0)}{n!}x^n \tag{15.2.1}$$

Define,

$$\begin{aligned} g(t) &= f(x) - f(t) - \frac{f'(t)}{1!}(x-t) - \frac{f''(t)}{2!}(x-t)^2 - \frac{f'''(t)}{3!}(x-t)^3 \\ &- \ldots - \frac{f^{(n)}(t)}{n!}(x-t)^n - R_n(x)\frac{(x-t)^{n+1}}{x^{n+1}} \end{aligned}$$

where we regard x as a constant and t as the variable. Then substituting $t = x$ we have,

$$\begin{aligned} g(x) &= f(x) - f(x) - \frac{f'(x)}{1!}(x-x) - \frac{f''(x)}{2!}(x-x)^2 - \frac{f'''(x)}{3!}(x-x)^3 \\ &- \ldots - \frac{f^{(n)}(x)}{n!}(x-x)^n - R_n(x)\frac{(x-x)^{n+1}}{x^{n+1}} \\ &= 0 \end{aligned}$$

and,

$$\begin{aligned} g(0) &= f(x) - f(0) - \frac{f'(0)}{1!}x - \frac{f''()x)}{2!}x^2 - \frac{f'''(0)}{3!}x^3 \\ &- \ldots - \frac{f^{(n)}(0)}{n!}x^n - R_n(x)\frac{x^{n+1}}{x^{n+1}} \\ &= R_n(x) - R_n(x) \text{ by (15.2.1)} \\ &= 0 \end{aligned}$$

Since $g(x) = g(0) = 0$, making the slope of the line segment joining them equal to 0, by the Mean Value Theorem[1] there is a point on the curve with x–coordinate $c \in [0, x]$ such that $g'(c) = 0$. Now, using the product and chain rules,

$$\begin{aligned} g'(t) &= 0 - \cancel{f'(t)} - \cancel{\frac{f''(t)}{1!}(x-t)} + \cancel{\frac{f'(t)}{1!}} - \xcancel{\frac{f'''(t)}{2!}(x-t)^2} + \cancel{\frac{f''(t)}{1!}(x-t)} - \ldots \\ &- \frac{f^{n+1}(t)}{n!}(x-t)^n + \xcancel{\frac{f^{n+1}(t)}{(n-1)!}(x-t)^{n-1}} + R_n(x)\frac{(n+1)(x-t)^n}{x^{n+1}} \\ &= -\frac{f^{n+1}(t)}{n!}(x-t)^n + R_n(x)\frac{(n+1)(x-t)^n}{x^{n+1}} \end{aligned}$$

[1] The mean value theorem states that for any continous curve $g(x)$ joining two points A, B with x–coordinates $x = a, x = b$ there is a point $(c, g(c))$ on the curve such that $a \le c \le b$ and the slope of the curve at this point, $(c, g(c))$, is the same as the slope of the line segment joining A and B, that is, $g'(c) = \dfrac{g(b) - g(a)}{b - a}$. – see Figure 32.

Then, substituting $t = c$ and using $g'(c) = 0$ we have,

$$\begin{aligned} g'(c) &= -\frac{f^{(n+1)}(c)}{n!}(x-c)^n + R_n(x)\frac{(n+1)(x-c)^n}{x^{n+1}} = 0 \\ \Rightarrow R_n(x)\frac{(n+1)(x-c)^n}{x^{n+1}} &= \frac{f^{(n+1)}(c)}{n!}(x-c)^n \\ \Rightarrow R_n(x) &= \frac{f^{(n+1)}(c)}{(n+1)n!}x^{n+1} \\ \Rightarrow R_n(x) &= \frac{f^{(n+1)}(c)}{(n+1)!}x^{n+1} \end{aligned}$$

□

Theorem 116. *(Taylor's Theorem)*
Let $f(x)$ be a smooth function for all points in an interval $(-r, r)$ about 0. The Taylor series defined by

$$f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

converges to $f(x)$ on the interval $(-r, r)$ as $n \to \infty$ if and only if,

$$\lim_{n\to\infty} R_n(x) = 0 \text{ where } R_n(x) = \frac{f^{(n+1)}(c)}{(n+1)!}x^{n+1}$$

and c is some point between x and 0.
That is, we have

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

for any point x in $(-r, r)$ if and only if,

$$\lim_{n\to\infty} \frac{f^{(n+1)}(c)}{(n+1)!}x^{n+1} = 0$$

for some point c between x and 0.

Proof. Assume

$$\lim_{n\to\infty} R_n(x) = \lim_{x\to\infty} \frac{f^{(n+1)}(c)}{(n+1)!}x^{n+1} = 0$$

We want to show that

$$f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

converges to $f(x)$ as $n \to \infty$. Let,

$$p_n(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n$$

Note the Taylor series is $\lim\limits_{n\to\infty} p_n(x)$. Then since by Theorem 115 above,

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + R_n(x),$$

we have here,

$$\begin{aligned} & p_n(x) = f(x) - R_n(x) \\ & \Rightarrow \lim_{n\to\infty} p_n(x) = \lim_{n\to\infty} f(x) - \lim_{n\to\infty} R_n(x) = f(x) - 0 \\ & \Rightarrow f(x) = \lim_{n\to\infty} p_n(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots \end{aligned}$$

***

Conversely, assume the Taylor series converges to $f(x)$ on $(-r, r)$, that is,

$$f(x) = \lim_{x\to\infty} p_n(x).$$

Then again with $p_n(x) = f(x) - R_n(x)$,

$$0 = f(x) - \lim_{n\to\infty} p_n(x) = \lim_{n\to\infty} (f(x) - p_n(x)) = \lim_{n\to\infty} R_n(x)$$

□

15.3 Taylor Series of the Exponential Function

Theorem 117.
The Taylor series for the natural exponential function is,

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Proof. Let $f(x) = e^x$. Then the n^{th} derivative $f^{(n)}(x) = e^x$ for all n and $f^{(n)}(0) = e^0 = 1$ for all n. Then the general Taylor series,

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

gives,

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

since,

$$\lim_{n\to\infty} R_n(x) = \lim_{n\to\infty} \frac{f^{n+1}(c)}{(n+1)!}x^{n+1} = \lim_{n\to\infty} \frac{e^c}{(n+1)!}x^{n+1} = 0$$

since the factorial in the denominator is approaching infinity much more rapidly that the numerator. □

15.4 Taylor Series for Sine and Cosine Functions

Theorem 118.
For all values of x,

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^{2n-1}}{(2n-1)!}$$
$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots = \sum_{n=0}^{\infty}(-1)^{n}\frac{x^{2n}}{(2n)!}$$

Proof. Let,

$$\begin{aligned} & f(x) = \sin x \\ & \Rightarrow f'(x) = \cos x \\ & \Rightarrow f''(x) = -\sin x \\ & \Rightarrow f'''(x) = -\cos x \\ & \Rightarrow f^{(4)}(x) = \sin x \end{aligned}$$

Clearly this pattern repeats every four derivatives. Then we have these four terms repeated,

$$f(0) = 0,\ f'(0) = 1,\ f''(0) = 0,\ f'''(0) = -1.$$

Thus,

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots,$$

gives

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^{2n-1}}{(2n-1)!}$$

provided $\lim_{n\to\infty} R_n = \lim_{n\to\infty}\frac{f^{(n+1)}(c)}{(n+1)!} = 0$. But $f^{(n+1)}(c)$ is one of $\pm\sin c, \pm\cos c$ which take values between -1 and $+1$. So we have,

$$-1 \le f^{(n)}(c) \le +1 \Rightarrow -\frac{x^{n+1}}{(n+1)!} \le f^{(n)}(c)\frac{x^{n+1}}{(n+1)!} \le \frac{x^{n+1}}{(n+1)!}$$

Now both of $\lim_{n\to\infty} \pm\frac{x^{n+1}}{(n+1)!} = 0$ since[2] $(n+1)! \to \infty$ much much more rapidly than does the numerator x^{n+1}.
Hence,

$$\lim_{n\to\infty} R_n = \lim_{n\to\infty}\frac{f^{(n+1)}(c)}{(n+1)!} = 0.$$

[2] Strictly speaking we should invoke the Squeeze Theorem, which says if at a given point a function is squeezed between two other functions both approaching the same limit at that point then it must also be approaching that same limit at that point.

We could repeat this argument for $\cos x$ but it is easier to use $\dfrac{d\sin x}{dx} = \cos x$. So, if we differentiate $\sin x = x - \dfrac{x^3}{3!} + \dfrac{x^5}{5!} - \dfrac{x^7}{7!} + \ldots$ with respect to x, we obtain,

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots = \sum_{n=0}^{\infty}(-1)^n \frac{x^{2n}}{(2n)!}$$

□

15.5 Euler's Formulas

We reach two of the most famous and most useful equations in the whole of mathematics. The second one is wonderful, combining two transcendental numbers with a complex number to produce an integer!

Theorem 119. *(Euler)*

$$\begin{aligned}
&e^{ix} = \cos x + i\sin x, \ \textit{where}\ i = \sqrt{-1}\\
&e^{\pi i} = -1
\end{aligned}$$

Proof.

$$\begin{aligned}
e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots\\
\Rightarrow e^{ix} &= 1 + ix + \frac{(ix)^2}{2!} + \frac{(ix)^3}{3!} + \frac{(ix)^4}{4!} + \frac{(ix)^5}{5!} + \frac{(ix)^6}{6!} + \frac{(ix)^7}{7!} + \frac{(ix)^8}{8!} + \ldots\\
&= 1 + ix - \frac{x^2}{2!} - i\frac{x^3}{3!} + \frac{x^4}{4!} + i\frac{x^5}{5!} - \frac{x^6}{6!} - i\frac{x^7}{7!} + \frac{x^8}{8!} + \ldots\\
&= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} + \ldots + i(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots)\\
&= \cos x + i\sin x
\end{aligned}$$

Put $x = \pi$, then,

$$e^{\pi i} = \cos\pi + i\sin\pi = -1 + i\cdot 0 = -1$$

□

Here are two examples of the usefulness of these results.

Corollary 120. *(De Moivre's Formula)*

$$(\cos x + i\sin x)^n = \cos nx + i\sin nx$$

Proof.

$$(\cos x + i\sin x)^n = (e^{ix})^n = e^{i(nx)} = \cos nx + i\sin nx$$

□

Corollary 121. *Complex Formulas for* $\sin x$ *and* $\cos x$.

$$\begin{aligned}\sin x &= \frac{e^{ix} - e^{-ix}}{2i}\\ \cos x &= \frac{e^{ix} + e^{-ix}}{2}\end{aligned}$$

Proof.

$$\begin{aligned}&e^{ix} = \cos x + i\sin x\\ \Rightarrow\ &e^{-ix} = e^{i(-x)} = \cos(-x) + i\sin(-x) = \cos x - i\sin x\end{aligned}$$

Add and subtract the two equations to obtain,

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i} \tag{15.5.1}$$

$$\cos x = \frac{e^{ix} + e^{-ix}}{2} \tag{15.5.2}$$

□

15.6 Roots of Unity

Complex numbers are defined by $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$.
Now the solution of $x^2 - 1 = 0 \Rightarrow x^2 = 1$ is $x = \pm 1$. We say ± 1 are the second roots of unity.
We can also solve, say, $x^4 - 1 = 0 \Rightarrow x^4 = 1$ by noting $(e^{\pi i})^4 = (-1)^4 = 1$ so that one solution is clearly $x = e^{\pi i}$.
However, since this is an equation of degree 4, we expect 4 solutions. They are,

$$x = e^{\frac{2k\pi i}{4}},\ k = 1, 2, 3, 4 \textit{ or } x = e^{\frac{2\pi i}{4}},\ x = e^{\frac{4\pi i}{4}},\ x = e^{\frac{6\pi i}{4}},\ x = e^{\frac{8\pi i}{4}},$$

since,

$$x^4 = \left(e^{\frac{2k\pi i}{4}}\right)^4 = (e^{2k\pi i}) = (e^{\pi i})^{2k} = (-1)^{2k} = 1$$

The numbers $x = e^{\frac{2\pi i}{4}}$, $x = e^{\frac{4\pi i}{4}}$, $x = e^{\frac{6\pi i}{4}}$, $x = e^{\frac{8\pi i}{4}}$, are called the 4th roots of unity.

Definition 61. *roots of unity*
The n^{th} *roots of unity are the solutions of the equation* $x^n = 1$. *They are*

$$e^{\frac{2k\pi i}{n}},\ 0 \le k \le (n-1).$$

Part VI

Exotic Tastings

Using Infinite Series

A Tasting Plate is an assembly of the chef's signature appetizers to be taken prior to the main course. We will consider three such.

The first concerns the numbers e and π that occur so frequently in mathematics. They are not "normal" numbers, but how strange are they?

The second concerns summing finite series. Way back in Chapter 2 we proved

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

We want to extend this to find formulas for,

$$1^2 + 2^2 + 3^2 + \ldots + n^2$$

and further sums of sequences of the higher powers of the natural numbers. On the way we meet the interesting Bernoulli numbers which crop up in many places in mathematics just as do e and π.

The third concerns the zeta function $\zeta(s)$ which also crops up quite frequently and is the subject of a great deal of mathematical research. In our introduction to it we will find how to sum sequences of higher powers of the inverses of the natural numbers, namely the values of,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for $s = 2k$ where k is a natural number.

First e and π.

The numbers e and π occur often in all of mathematics. Each of them is irrational and each is also transcendental. We will need trigonometry and calculus to prove this statement.

A rational number is of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and b is not zero. Irrational numbers are not able to be expressed as $\frac{a}{b}$. We have already proved by contradiction that $\sqrt{2}$ is not a rational number. The proofs that e and π are irrational are also proved by contradiction. We can approach e directly through the Taylor/Maclaurin series of e^x. The proof for π is more circuitous – we use a polynomial in $x - \pi$ and then an integral that uses the sine and cosine functions where we know $\sin\pi = 0, \cos\pi = -1$.

A transcendental number is a real number that is not algebraic. A real number is algebraic if it is the root of a polynomial with integer coefficients, that is a root of,

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, a_0 \neq 0, a_i \in \mathbb{Z}$$

for some $n \in \mathbb{N}$. Specifically, if α is an algebraic number then, for some n and some $a_i's$,

$$f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0$$

So a transcendental number is not the root of a polynomial with integer coefficients.

While the integers are obviously algebraic since if $\alpha \in \mathbb{Z}$, then α is a root of $f(x) = x - \alpha$, and the rationals are also obviously algebraic since if $\alpha = \frac{a}{b} \in \mathbb{Q}$ then α is a root of $f(x) = bx - a$, the picture gets a little cloudier as we deal with the irrationals. Clearly $\sqrt{2}$ is algebraic since it is a root of $f(x) = x^2 - 2$ but $\frac{\sqrt{6} - \sqrt{2}}{3}$ is not obviously the root of a polynomial equation.

One question is whether exact values of all algebraic numbers can be found. For example, $f(x) = x^5 - 4x^4 + x^3 - 2x^2 + x - 7$ must equal zero for some value of x since its graph crosses the x−axis. But finding that algebraic number exactly is almost impossible. Since it is a fact that the graph of any polynomial with integer coefficients that is of odd degree must cross the x−axis, there are an infinite number of algebraic numbers, the vast majority of which cannot be determined. This means the real number line on which we can put all the integers and fractions is crowded with algebraic numbers, they are actually the majority.

What we are interested in for this chapter is other numbers on the real number line that are not algebraic. The first two are e and π. Proving they are transcendental and not algebraic means proving we can never construct for any n, the equations,

$$a_0e^n + a_1e^{n-1} + \ldots + a_{n-1}e + a_n = 0, a_0 \neq 0, a_i \in \mathbb{Z}$$
$$a_0\pi^n + a_1\pi^{n-1} + \ldots + a_{n-1}\pi + a_n = 0, a_0 \neq 0, a_i \in \mathbb{Z}$$

This is obviously more difficult that proving they are not of the form $\frac{a}{b}$. This is difficult chapter, particularly the proof that π is transcendental.

Chapter 16

The Numbers e and π

Course: Tasting Plate I
Ingredients
Definitions of irrational, algebraic and transcendental numbers
Calculus
Calculus of Exponential and Trigonometric Functions
Directions
Prove e, π are irrational numbers.
Prove e, π are transcendental numbers.

16.1 e and π are irrational

16.1.1 e is irrational

Theorem 122. *(Joseph Fourier)*
The exponential number e is irrational where we define e^x as the exponential function whose gradient at $(0,1)$ is 1.

Proof.
Using the Taylor/Maclaurin series of e^x, Theorem 114, page 168, namely $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ with $x = 1$ we have,

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} \ldots = 2.71828\ldots$$

We use contradiction, so suppose $e = \frac{a}{b},\ a, b \in \mathbb{Z}^+,\ gcd(a,b) = 1$.
Since $e = 2.71828\ldots$ is not an integer, then $b > 1$. Define,

$$x = b!\left(e - \sum_{n=0}^{b} \frac{1}{n!}\right) \tag{16.1.1}$$

Substitute $e = \dfrac{a}{b}$ to give,

$$x = b!\left(\frac{a}{b} - \sum_{n=0}^{b}\frac{1}{n!}\right) = a(b-1)! - \sum_{n=0}^{b}\frac{b!}{n!}$$

Now, $a(b-1)!$ is an integer. Since $n \le b$ then

$$\frac{b!}{n!} = \frac{b(b-1)\cdots(n)(n-1)\cdots 1}{n(n-1)(n-2)\cdots 1}$$

is also an integer for all possible values of n. Therefore x is an integer.
We now prove $0 < x < 1$ so x cannot be an integer, which is a contradiction to the finding that x is an integer based on supposing $e = \dfrac{a}{b}$, so e is irrational.

First we prove $x > 0$.
Substitute $e = \sum_{n=0}^{\infty}\dfrac{1}{n!}$ into the definition of x in (16.1.1) to give,

$$\begin{aligned} x &= b!\left(\sum_{n=0}^{\infty}\frac{1}{n!} - \sum_{n=0}^{b}\frac{1}{n!}\right) \\ &= b!\left(\frac{1}{0!} + \frac{1}{1!} + \ldots + \frac{1}{b!} + \frac{1}{(b+1)!} + \frac{1}{(b+2)!} + \ldots\right) - \left(\frac{1}{0!} + \frac{1}{1!} + \ldots + \frac{1}{b!}\right) \\ &= b!\left(\frac{1}{(b+1)!} + \frac{1}{(b+2)!} + \ldots\right) \\ &= b!\sum_{n=b+1}^{\infty}\frac{1}{n!} \qquad (16.1.2) \end{aligned}$$

which is always positive, hence $x > 0$.

Second we prove $x < 1$.
Noting in our derivation in (16.1.2) of $x = b!\sum_{n=b+1}^{\infty}\dfrac{1}{n!}$ that we now have $n \ge b+1$ and writing $n = b + (n-b)$ we have,

$$\begin{aligned} \frac{b!}{n!} &= \frac{b(b-1)(b-2)\cdots 1}{1\cdot 2\cdots\cdot(b-1)(b)(b+1)(b+2)\cdot\cdots n} \\ &= \frac{1}{(b+1)(b+2)\cdots(b+(n-b))} \end{aligned}$$

where the denominator has $(n-b)$ factors each of the form $\dfrac{1}{b+r}$.
Now $\dfrac{1}{b+r} < \dfrac{1}{b+1}$ for all r such that $1 < r \le n-b$ so that,

$$\frac{b!}{n!} < \frac{1}{(b+1)^{n-b}}$$

Then,

$$x = \sum_{n=b+1}^{\infty} \frac{b!}{n!} < \sum_{n=b+1}^{\infty} \frac{1}{(b+1)^{n-b}}$$

Changing the index of summation to $k = n - b \Rightarrow k = 1$ *when* $n = b + 1$, gives,

$$x < \sum_{k=1}^{\infty} \frac{1}{(b+1)^k}$$

This is a geometric series with first term $a = \dfrac{1}{b+1}$ and common ratio $r = \dfrac{1}{b+1} < 1$, hence its sum is $\dfrac{a}{1-r}$ giving,

$$x < \frac{\frac{1}{b+1}}{1 - \frac{1}{b+1}} = \frac{1}{b} < 1 \Rightarrow x < 1.$$

Together, these two results show $0 < x < 1$ so x cannot be an integer and the supposition that $e = \dfrac{a}{b}$ is false.
e is therefore an irrational number. □

16.1.2 π is irrational

Theorem 123. *(Niven)*
The number π is irrational where π is the ratio of the circumference of a circle to its diameter. Equivalently, π is the angle (in radians) in the unit circle whose terminal ray ends at $(-1,0)$.

Proof. We again proceed to prove a contradiction.
We assume $\pi = \dfrac{p}{q}, p, q \in \mathbb{Z}^+,\ gcd(p,q) = 1.$
Consider the n functions,

$$\begin{aligned} f_n(x) &= \frac{1}{n!} q^n x^n (\pi - x)^n,\ n \in \mathbb{N} && (16.1.3)\\ &= \frac{1}{n!} q^n x^n \left(\frac{p}{q} - x\right)^n && (16.1.4)\\ &= \frac{1}{n!} x^n (p - qx)^n && (16.1.5)\end{aligned}$$

Note:

(i) f_n is a polynomial of degree $2n$ and, by the Binomial Theorem 85, page 130, all its coefficients are fractions of integers divided by $n!$

(ii) $f_n(x) > 0$ if $0 < x < \pi$ since, (see (16.1.4)), $x < \dfrac{p}{q} \Rightarrow p - qx > 0$.

(iii) $f_n(0) = f_n(\pi) = 0$.

(iv) The maximum value M_n of $f_n(x)$ on the interval $[0, \pi]$ is,

$$M_n = f_n\left(\frac{\pi}{2}\right) = \frac{1}{n!}q^n\left(\frac{\pi}{2}\right)^{2n} \tag{16.1.6}$$

which we now prove by Calculus. We need to find the maximum and minimum values where the slope is zero or $f_n'(x) = 0$ and to do this we apply the product and chain rules to (16.1.5).

$$\begin{aligned} f_n'(x) &= \frac{1}{n!}\left[nx^{n-1}(p-qx)^n + x^n \cdot n(p-qx)^{n-1}(-q)\right] \\ &= \frac{nx^{n-1}(p-qx)^{n-1}}{n!}(p-qx-qx) \\ &= \frac{nx^{n-1}(p-qx)^{n-1}}{n!}(p-2qx) \end{aligned}$$

Then $f'(n) = 0$ if $x = 0$ or $x = \dfrac{p}{q} = \pi$ or $x = \dfrac{p}{2q} = \dfrac{\pi}{2}$.
Since $f_n(0) = f_n(\pi) = 0$ and $f_n(x) > 0$ if $0 < x < \pi$ then $x = 0, \pi$ are minimum points and $x = \dfrac{\pi}{2}$ is a maximum on the interval $[0, \pi]$ as shown in Figure 33.

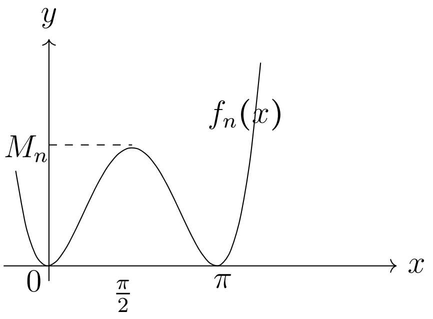


Figure 33

Substituting, $x = \dfrac{\pi}{2}$ into (16.1.2) we have the maximum value,

$$\begin{aligned} M_n &= f_n\left(\frac{\pi}{2}\right) \\ &= \frac{1}{n!}\left(\frac{\pi}{2}\right)^n\left(p - q\frac{\pi}{2}\right)^n \\ &= \frac{1}{n!}\left(\frac{\pi}{2}\right)^n\left(\frac{\pi q}{2}\right)^n, \text{ since } p = \pi q \\ &= \frac{1}{n!}q^n\left(\frac{\pi}{2}\right)^{2n} \end{aligned}$$

(v) We note,

$$\lim_{n\to\infty} M_n = \lim_{n\to\infty} f_n\left(\frac{\pi}{2}\right) = \frac{1}{n!}q^n\left(\frac{\pi}{2}\right)^{2n} = 0$$

since $n!$ grows much more rapidly than $q^n\left(\frac{\pi}{2}\right)^{2n}$.

Let us proceed with the proof that π is irrational.
Since $\lim\limits_{n\to\infty} M_n = 0$, as n gets larger M_n gets smaller and is eventually zero. Hence, there must be some large value of n for which $M_n < \frac{1}{2}$.
Define I_n by,

$$I_n = \int_0^\pi f_n(x)\sin x\ dx$$

Since both $f_n(x)$ and $\sin x$ are positive on $[0,\pi]$, the graph of $f_n(x)\sin x$ is above the $x-$ axis and their integral is positive, thus $I_n > 0$. See Figure 34.

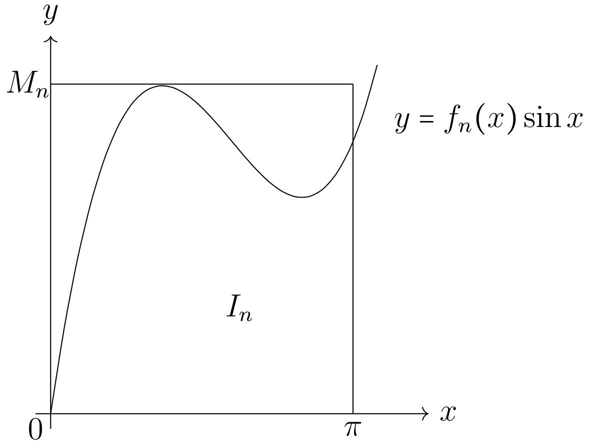


Figure 34

On the other hand, if the maximum of a function on an interval is M_n then the rectangle of height M_n on the base $[0,\pi]$ is obviously greater than the area under the graph of the function $f_n(x)\sin x$ on $[0,\pi]$ (see Figure 34) then,

$$\begin{aligned} I_n &= \int_0^\pi f_n(x)\sin x\ dx \\ &< \int_0^\pi M_n \sin x\ dx = M_n[-cosx]_0^\pi = M_n(-(-1)-(-1)) = 2M_n \end{aligned}$$

Thus if we take n large enough so that $M_n < \frac{1}{2}$ then $0 < I_n < 1$.
Similar to the proof of the irrationality of e we proceed to prove the contradiction to $\pi = \frac{p}{q}$ by proving that I_n is an integer.

In what follows we will repeatedly differentiate one function using the product and chain rules and after that repeatedly integrate another function using integration by parts. So to fully understand this you need to be skilled in these procedures – the standard Calc II course.

Let us assume x is large and repeatedly differentiate $f_n(x)$ by using the product and chain rules, Theorem 60, page 87 and Theorem 62, page 88 respectively.

$$\begin{aligned}
f_n(x) &= \frac{q^n}{n!}x^n(\pi - x)^n \\
f_n'(x) &= \frac{q^n}{n!}\left[nx^{n-1}(\pi - x)^n - nx^n(\pi - x)^{n-1}\right] \\
f_n''(x) &= \frac{q^n}{n!}[n(n-1)x^{n-2}(\pi - x)^n - n^2x^{n-1}(\pi - x)^{n-1} \\
&\qquad - n^2x^{n-1}(\pi - x)^{n-1} + n(n-1)x^n(\pi - x)^{n-2}] \\
f_n'''(x) &= \frac{q^n}{n!}[n(n-1)(n-2)x^{n-3}(\pi - x)^n + \text{ terms in } x^r(\pi - x)^s \\
&\qquad (-1)^3n(n-1)(n-2)x^n(\pi - x)^{n-3}]
\end{aligned}$$

Note in all these derivatives, as in $f_n(x)$ itself, each term contains an x and a $\pi - x$ and therefore they are all zero at $x = 0$ or $x = \pi$.
Note also that each differentiation causes the power of the x in the first term and the power of the $\pi - x$ in the last terms to go down by 1. So eventually, as we continue to differentiate, we reach a value of $m = n$ and have,

$$f_n^{(m)}(x) = \frac{q^n}{n!}[n!(\pi - x)^n + \textit{ terms in } x^r(\pi - x)^s + (-1)^n n! x^n]$$

with no x in the first, and no $\pi - x$ in the last, terms.Then,

$$\begin{aligned}
f_n^{(m)}(0) &= \frac{q^n}{n!}n!\pi^n = p^n \\
f_n^{(m)}(\pi) &= \frac{q^n}{n!}(-1)^n n!\pi^n = (-1)^n p^n
\end{aligned}$$

and both of these are integers.
For $m > n$ say $m = n + t$,

$$f_n^{(m)}(x) = q^n\frac{d^t}{dx^t}[(\pi - x)^n + \textit{ terms in } \frac{x^r(\pi - x)^s}{n!} + \frac{(-1)^n x^n}{n!}]$$

and either the repeated differentiation leads to 0 or there are remaining terms in x and/or $\pi - x$. In either case when we substitute $x = 0$ or $x = \pi$, the resulting power of $\pi = \dfrac{p}{q}$ will be less than n (the power of q^n) so the denominator cancels out and both $f_n^{(m)}(0)$ and $f_n^{(m)}(\pi)$ will be integers.

We now integrate,

$$I_n = \int_0^\pi f_n(x)\sin x \; dx$$

repeatedly by parts $2n+1$ times.[1]

First, in the integration by parts formula,

$$\int_a^b u\frac{dv}{dx}\ dx = [uv]_a^b - \int_a^b v\frac{du}{dx}\ dx$$

put $u = f_n(x) \Rightarrow \dfrac{du}{dx} = f_n'(x)$ and $\dfrac{dv}{dx} = \sin x \Rightarrow v = -\cos x$ to give,

$$\begin{aligned} I_n &= \int_0^\pi f_n(x)\sin x\ dx \\ &= [-f_n(x)\cos x]_0^\pi + \int_0^\pi f_n'(x)\cos x\ dx \\ &= \int_0^\pi f_n'(x)\cos x\ dx \end{aligned}$$

since what we call the boundary term,

$$[-f_n(x)\cos x]_0^\pi = -f_n(\pi)\cos\pi + f_n(0)\cos 0 = 0$$

given both $f_n(0)$ and $f_n(\pi)$ are 0 as shown above.

Continuing on, let $u = f_n'(x) \Rightarrow \dfrac{du}{dx} = f_n''(x)$ and $\dfrac{dv}{dx} = \cos x \Rightarrow v = \sin x$ to give,

$$\begin{aligned} I_n &= [f_n'(x)\sin x]_0^\pi - \int_0^\pi f_n''(x)\sin x\ dx \\ &= -\int_0^\pi f_n''(x)\sin\ dx \end{aligned}$$

since again, due to $\sin 0 = \sin\pi = 0$, the boundary term,

$$[-f_n(x)\sin x]_0^\pi = -f_n(\pi)\sin\pi + f_n(0)\sin 0 = 0 - 0 = 0$$

As we continue to $m \geq n$ the boundary terms are successively of the forms,

$$[f_n^{(m)}(x)\sin x]_0^\pi = 0 \text{ since } \sin 0 = \sin\pi = 0$$

or

$$[f_n^{(m)}(x)\cos x]_0^\pi$$

which is an integer since $\cos 0 = 1, \cos\pi = -1, f_n^{(m)}(0) \in \mathbb{Z}, f_n^{(m)}(\pi) \in \mathbb{Z}$ as shown above in the differentiation step.

After integrating $2n+1$ times, the remaining integral contains $f_n^{(2n+1)}(x)$ which is zero since $f_n(x)$ is a polynomial of degree $2n$ and each differentiation lowers the power by 1.

We conclude I_n is an integer, which completes the contradiction, showing π is irrational. □

[1] See Theorem 64, page 90.

16.2 e and π are Transcendental Numbers.

In both proofs we make use of the following results.

Lemma 124.
If,

$$I(t) = \int_0^t e^{t-x} f(x)\ dx = e^t \int_0^t e^{-x} f(x)\ dx$$

where $t \in \mathbb{C}$ and $f(x)$ is a polynomial of degree n with complex number coefficients, then,

$$I(t) = e^t \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(t)$$

Proof. Using repeated integration by parts, first with $u = f(x), \dfrac{dv}{dx} = e^{-x}$, we have,

$$\begin{aligned}
I(t) &= e^t \int_0^t e^{-x} f(x)\ dx \\
&= e^t \left([-e^{-x} f(x)]_0^t + \int_0^t e^{-x} f'(x)\ dx \right) \\
&= e^t \left(-e^{-t} f(t) + f(0) + \int_0^t e^{-x} f'(x)\ dx \right) \\
&\text{Put } u = f'(x), \frac{dv}{dx} = e^{-x} \text{ in the integral,} \\
&= -f(t) + e^t f(0) + e^t [-e^{-x} f'(x)]_0^t + e^t \int_0^t e^{-x} f''(x)\ dx \\
&= e^t f(0) - f(t) + e^t \left(-e^{-t} f'(t) + f'(0) \right) + e^t \int_0^t e^{-x} f''(x)\ dx \\
&= e^t f(0) - f(t) - f'(t) + e^t f'(0) + e^t \int_0^t e^{-x} f''(x)\ dx \\
&= e^t \sum_{j=0}^{1} f^{(j)}(0) - \sum_{j=0}^{1} f^{(j)}(t) + e^t \int_0^t e^{-x} f''(x)\ dx \\
&\text{Put } u = f''(x), \frac{dv}{dx} = e^{-x} \text{ in the integral,} \\
&= e^t \sum_{j=0}^{1} f^{(j)}(0) - \sum_{j=0}^{1} f^{(j)}(t) + e^t [-e^{-x} f''(x)]_0^t + e^t \int_0^t e^{-x} f'''(x)\ dx \\
&= e^t \sum_{j=0}^{1} f^{(j)}(0) - \sum_{j=0}^{1} f^{(j)}(t) - f''(t) + e^t f''(0) + e^t \int_0^t e^{-x} f'''(x)\ dx \\
&= e^t \sum_{j=0}^{2} f^{(j)}(0) - \sum_{j=0}^{2} f^{(j)}(t) + e^t \int_0^t e^{-x} f'''(x)\ dx
\end{aligned}$$

The first two sums will continue to build as will the order m for $f^{(m)}(x)$ under the integral sign. Note the order of $f^{(m)}(x)$ is one more than the upper number in the sums. If the degree of $f(x)$ is n then when this upper number reaches $n+1$ we will have $f^{(n+1)}(x) = 0$ in the integral. We conclude,

$$I(t) = e^t \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(t)$$

□

We now write $f(x)$ as a polynomial of degree n in x,

$$f(x) = \sum_{j=0}^{n} a_j x^j$$

We define,

$$\bar{f}(x) = \sum_{j=0}^{n} |a_j| x^j$$

where clearly $f(x) \leq \bar{f}(x)$ since all the coefficients of $\bar{f}(x)$ have been made positive, whereas those of $f(x)$ may be positive or negative. We proceed to prove,

Lemma 125.

$$|I(t)| \leq |t| e^{|t|} \bar{f}(t) \tag{16.2.1}$$

Proof. (general idea)
$I(t) = \int\limits_0^t e^{t-x} f(x)\ dx$ represents the area under the curve $e^{t-x}f(x)$ on the interval $[0,t]$. On some sub-intervals $e^{t-x}f(x)$ may be positive, on others negative so $I(t)$ may actually be negative if for more of the sub-intervals the graph of $e^{t-x}f(x)$ is below the x−axis than above it. If we replace $e^{t-x}f(x)$ with $|e^{t-x}f(x)|$, then we can write, (where we actually invoke the Triangle Inequality of Lemma 26 on page 55),

$$|I(t)| = \left| \int_0^t e^{t-x} f(x)\ dx \right| \leq \left| \int_0^t |e^{t-x} f(x)|\ dx \right|$$

We are now dealing on the right with an area all above the x−axis. In turn this area is contained within a box of width $|t|$ and height the maximum value of $|e^{t-x}f(x)|$ for which,

$$|e^{t-x} f(x)| = |e^{t-x}|\ |f(x)| \leq |t|\ max\{|e^{t-x}|\}\ max\{|f(x)|\} \leq |t||e^{|t|}\bar{f}(t)|$$

Accordingly,

$$|I(t)| \leq |t| e^{|t|} \bar{f}(t)$$

□

Note 23. *The Extended Product Rule*
Before we consider the proof of the theorem that e is transcendental, let us consider the product rule for differentiating the product of more than two functions. Writing $\frac{d}{dx}f(x) = f'(x)$, etc., and leaving out the variable x, we proved,

$$y = fg \Rightarrow y' = fg' + gf'$$

where y, f, g are all functions of an independent variable, whether x or t or other. Then,

$$y = fgh = f(gh) \Rightarrow y' = f(gh)' + ghf' = fgh' + fhg' + ghf'.$$

In general, the product of n functions will have n such terms in its derivative,

$$y = f_1 f_2 \cdots f_n \Rightarrow y' = (f_2 f_3 \cdots f_n) f_1' + (f_1 f_3 \cdots f_n) f_2' + \ldots + (f_1 f_2 \cdots f_{n-1}) f_n'$$

The second derivative $y'' = y^{(2)}$ is the derivative of n products of n functions. It will therefore have n^2 terms in its derivative, $y''' = y^{(3)}$ will have n^3 terms and so on. Given the rapid growth of the number of terms in the higher order derivatives, the key ingredient in the transcendence proof for e is the use of a function for which almost all of these terms are zero for selected values of the independent variable x. The function is due to Hermite.

16.2.1 e is transcendental.

Theorem 126.
The natural exponential number e is transcendental.

Proof. We again use contradiction. Assume e is a root of the polynomial,

$$g(x) = b_0 + b_1 x \ldots + b_r x^r, \ b_r \neq 0, b_i \in \mathbb{Z}, n \in \mathbb{N}.$$

That is assume,

$$g(e) = b_0 + b_1 e \ldots + b_r e^r = 0 \qquad (16.2.2)$$

Let p be a prime larger than the larger of r and $|b_0|$, that is $p > max\{r, |b_0|\}$.
Define (this is the key ingredient),

$$f(x) = x^{p-1}(x-1)^p(x-2)^p \cdots (x-r)^p$$

With

$$I(t) = e^t \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(t)$$

as derived in Lemma 124, consider,

$$J = b_0 I(0) + b_1 I(1) + \ldots + b_r I(r) = \sum_{j=0}^{r} b_j I(j)$$

Using the assumption in (16.2.2) we will prove $|J| \to \infty$ but also $|J| < \infty$ and this contradiction, which assumes $g(e) = 0$ will prove e is transcendental.
First, the contribution to J of the first sum $e^t \sum_{j=0}^{n} f^{(j)}(0)$ of $I(t)$ is,

$$\begin{aligned}
&b_0 e^0 \sum_{j=0}^{n} f^{(j)}(0) + b_1 e^1 \sum_{j=0}^{n} f^{(j)}(0) + \ldots + b_r e^r \sum_{j=0}^{n} f^{(j)}(0)\\
&= \left(b_0 e^0 + b_1 e^1 + \ldots + b_r e^r\right) \sum_{j=0}^{n} f^{(j)}(0)\\
&= 0
\end{aligned}$$

since we have in (16.2.2) assumed e is a root of $g(x)$. Thus, the contributions to J from $I(t)$ are due only to,

$$I(t) = -\sum_{j=0}^{n} f^{(j)}(t)$$

and we have,

$$\begin{aligned}
J &= b_0 I(0) + b_1 I(1) + \ldots + b_r I(r)\\
&= -b_0 \sum_{j=0}^{n} f^{(j)}(0) - b_1 \sum_{j=0}^{n} f^{(j)}(1) - \ldots - b_r \sum_{j=0}^{n} f^{(j)}(r)\\
&= -\sum_{k=0}^{r} \sum_{j=0}^{n} b_k f^{(j)}(k)
\end{aligned}$$

Let us now separate out the $k = 0$ term.

$$J = -b_0 \sum_{j=0}^{n} f^{(j)}(0) - \sum_{k=1}^{r} \sum_{j=0}^{n} b_k f^{(j)}(k)$$

The degree of $f(x) = x^{p-1}(x-1)^p(x-2)^p \cdots (x-r)^p$ is,

$$n = p - 1 + \overbrace{p + p + \ldots + p}^{r\ times} = rp + p - 1,$$

hence since each differentiation lowers the power by one, the derivatives $f^{(j)}(x) = 0$ for $j > n = rp + p - 1$.
Now by repeated differentiation of x^{p-1} and x^p we have,

$$\frac{d^{(p-1)}}{dx^{(p-1)}}(x^{p-1}) = (p-1)! \tag{16.2.3}$$

$$\frac{d^{(p)}}{dx^{(p)}}(x-s)^p = p! \text{ for } 1 \le s \le r. \tag{16.2.4}$$

Let us first consider $b_0 \sum_{j=0}^{n} f^{(j)}(0)$. We write,

$$f(x) = x^{p-1}h(x) \text{ where } h(x) = (x-1)^p(x-2)^p \cdots (x-r)^p$$

Then, differentiating twice,

$$\begin{aligned}
&f'(x) = (p-1)x^{p-2}h(x) + x^{p-1}h'(x) \\
&f''(x) = (p-1)(p-2)x^{p-3}h(x) + (p-1)x^{p-2}h'(x) + (p-1)x^{p-2}h(x) + x^{p-1}h''(x)
\end{aligned}$$

If we continue to differentiate then we arrive at,

$$f^{(p-1)}(x) = (p-1)!h(x) + \overbrace{\text{terms with } x \text{ a factor}} + x^{p-1}h^{(p-1)}(x)$$

Then,

$$\begin{aligned}
f^{(p-1)}(0) &= (p-1)!h(0) \\
&= (p-1)!(-1)^p(-2)^p \cdots (-r)^p \\
&= (p-1)!(-1)^{rp}(r!)^p
\end{aligned}$$

Since $p > r$ and $p > p-1$ then $f^{(p-1)}(0)$ is not divisible by p.
Now the terms with x a factor contain the successive derivatives of $h(x)$ from $h'(x)$ to $h^{(p-1)}(x)$ so they contain the derivatives of orders 1 to $p-1$ of each $(x-s)^p$. But the complete elimination of any factor of the form $(x-s)^p$ requires at least differentiation of order p as shown by (16.2.4). Therefore $f^{(p-1)}(s) = 0$ for $1 \le s \le r$. Hence,

$$\begin{aligned}
\sum_{j=0}^{n} b_0 f^{(j)}(0) &= b_0\left(0 + 0 + \ldots + f^{(p-1)}(0) + \sum_{j=p}^{n} b_0 f^{(j)}(0)\right) \\
&= b_0\left((p-1)!(-1)^{rp}(r!)^p + \sum_{j=p}^{n} f^{(j)}(0)\right)
\end{aligned}$$

The same argument applies to $\sum\limits_{j=p}^{n} f^{(j)}(0)$ and to the second sum of $\sum\limits_{k=1}^{r}\sum\limits_{j=0}^{n} b_k f^{(j)}(k)$ of J. Each term in $f^{(j)}(x)$ will contain all the factors $(x-s),\ 1 \le s \le r$ unless $j = p$ in which case the term then contains $p!$
Then for any given value of s, $f^{(j)}(s)$ consists of all zero terms except for the one containing the factor $p!$
Accordingly, apart from the leading term $b_0(p-1)!(-1)^{rp}(r!)^p$ every other non zero term in J is divisible by $p!$
Thus since $p > |b_0|$, we see that J is an integer divisible by $(p-1)!$ but not by $p!$ In other words,

$$|J| \ge (p-1)!$$

***

On the other hand, since,

$$f(x) = \sum_{j=0}^{n} a_j x^j \Rightarrow f(\bar{x}) = \sum_{j=0}^{n} |a_j| x^j$$

then if all the coefficients of $f(x) = x^{p-1}(x-1)^p(x-2)^p\cdots(x-r)^p$ are made positive, we must have,

$$\bar{f}(j) = j^{p-1}(j+1)^p(j+2)^p\cdots(j+r)^p \ for \ 0 \le j \le r,$$

Then since, given $j \le r$, each of the terms on the right side is less than $2r$ we have,

$$\bar{f}(j) \le (2r)^{rp+p-1} = (2r)^n \tag{16.2.5}$$

Then $J = \sum_{j=0}^{r} b_j I(j)$ gives us,

$$\begin{aligned} |J| &\le \sum_{j=0}^{r} |b_j||I(j)| \\ &\le \sum_{j=0}^{r} |b_j||je^t\bar{f}(j)| \text{ by (16.2.1) of Lemma 125} \\ &\le \sum_{j=0}^{r} |b_j||j||e^j| \times (2r)^n \text{ by (16.2.5)} \\ &\le c(2r)^n \end{aligned}$$

since the finite sum $\sum_{j=0}^{r} |b_j||j||e^j|$ is just some constant c.
But we cannot also have $|J| \ge (p-1)!$ where p is a prime as large as we like since the factorial rapidly outgrows the exponent terms in p. This gives the contradiction that establishes that e is transcendental and concludes the proof.

□

16.2.2 π is transcendental

The proof that π is a transcendental number is considerably more difficult and requires much more background. Its proof requires some advanced results from Abstract Algebra.

Definition 62. *We first distinguish between an algebraic number and an algebraic integer. Each is the root of a polynomial,*

$$g(x) = \sum_{k=0}^{n} b_k x^k = b_0x^n + b_1x^{n-1} + \ldots + b_n$$

with integer coefficients but for an algebraic integer, the leading coefficient b_0 must equal 1. We call such polynomials monic.

The proof uses the following lemmas on algebraic numbers and integers.

Lemma 127.
If α, β are algebraic numbers then so are $\alpha \pm \beta, \alpha\beta$ and α/β. Specifically, if π is an algebraic number, then since i is a root of $g(x) = x^2 + 1$ making i algebraic, then so is πi.

Lemma 128.
If α is an algebraic number with minimal (meaning least possible degree) polynomial $g(x) = \sum_{k=0}^{n} b_k x^k$ then $b_0\alpha$ is an algebraic integer.

Lemma 129.
If α is an algebraic integer and α is a rational number ($\alpha \in \mathbb{Q}$) then α must be an integer ($\alpha \in \mathbb{Z}$.)

The proof also uses the fundamental theorem of elementary symmetric polynomials in several variables. A symmetric polynomial is one left unchanged by any permutation of its variables. For example if,

$$f(x,y,z) = x^2 + y^2 + z^2 + 3xyz$$

then if we interchange x and y, then $f(x,y,z)$ is unchanged, making it a symmetric polynomial. An understanding and proof of the fundamental theorem of symmetric functions requires significant abstract algebra. We will invoke the fundamental theorem twice without saying what it is or proving it.
First Lemma 127, renamed as,

Lemma 130.
If π is algebraic then so is πi, $i = \sqrt{-1}$.

Proof. If π is algebraic then $f(\pi) = 0$ for some polynomial

$$f(x) = \sum_{k=0}^{n} a_k x^{n-k}, \ a_k \in \mathbb{Z}$$

We claim $g(x) = f(ix)f(-ix)$ is also a polynomial with integer coefficients. The proof of this is by induction on n where we put $f_n(x) = \sum_{k=0}^{n} a_k x^{n-k}$.

Basic Step: Let $n = 1$. Then,

$$\begin{aligned} f_1(x) &= a_0 x + a_1 \\ \Rightarrow g_1(x) &= f_1(ix)f_1(-ix) \\ &= (a_0 ix + a_1)(-a_0 ix + a_1) \\ &= a_0 x^2 + a_1 x^2 \end{aligned}$$

which is a polynomial with integer coefficients.

Supposition Step: Suppose,

$$\begin{aligned} g_n(x) &= f_n(ix)f_n(-ix) \\ &= \left(\sum_{k=0}^{n} a_k (ix)^{n-k}\right)\left(\sum_{k=0}^{n} a_k (-ix)^{n-k}\right) \end{aligned}$$

is a polynomial with integer coefficients.

Induction Step: We want to show

$$\begin{aligned} g_{n+1}(x) &= f_{n+1}(ix)f_{n+1}(-ix) \\ &= \left(\sum_{k=0}^{n+1} a_k(ix)^{n+1-k}\right)\left(\sum_{k=0}^{n+1} a_k(-ix)^{n+1-k}\right) \end{aligned}$$

is a polynomial with integer coefficients. But this is true since,

$$\begin{aligned} &\left(\sum_{k=0}^{n+1} a_k(ix)^{n+1-k}\right)\left(\sum_{k=0}^{n+1} a_k(-ix)^{n+1-k}\right) \\ &= \left(\sum_{k=0}^{n} a_k(ix)^{n-k} + a_{n+1}\right)\left(\sum_{k=0}^{n} a_k(-ix)^{n-k} + a_{n+1}\right) \\ &= f_n(ix)f_n(-ix) + a_{n+1}^2 + \sum_{k=0}^{n} a_{n+1}a_k\left((ix)^{n-k} + (-ix)^{n-k}\right) \\ &= f_n(ix)f_n(-ix) + a_{n+1}^2 + \sum_{k=0}^{n} a_{n+1}a_k x^{n-k} i^{n-k}\left(1 + (-1)^{n-k}\right) \end{aligned}$$

and terms having a factor i^{n-k} are either free of i when $n-k$ is even or
$1 + (-1)^{n-k} = 1 - 1 = 0$ when $n-k$ is odd.
Finally we note that,

$$g(i\pi) = f(-\pi)f(\pi) = f(-\pi)\cdot 0 = 0$$

and therefore $i\pi$ is algebraic. □

Theorem 131.
The number π is transcendental.

Proof. We again use a proof by contradiction.
Suppose $\theta = i\pi$ is algebraic with r the degree of its minimal polynomial $g(x)$.
Since $g(\theta) = 0$ then one factor of $g(x)$ is $x - \theta$.
The r factors are $x - \theta_j$ where $\theta_1, \theta_2, \ldots, \theta_r$ are the complex conjugates of θ and one of which is θ.
Let b be the leading coefficient of $g(x)$.
Since $e^{\theta} = e^{\pi i} = -1$ then $1 + e^{\theta_j} = 0$ for some j and therefore,

$$(1 + e^{\theta_1})(1 + e^{\theta_2})\cdots(1 + e^{\theta_r}) = 0 \tag{16.2.6}$$

$$\Rightarrow 1 + (e^{\theta_1} + e^{\theta_2} + \ldots + e^{\theta_r}) + (e^{\theta_1}e^{\theta_2} + e^{\theta_1}e^{\theta_3} + \ldots + e^{\theta_1}e^{\theta_r}) + \ldots = 0 \tag{16.2.7}$$

$$\Rightarrow 1 + \sum_{j=1}^{r} e^{\theta_j} + \sum_{\substack{j,k=1 \\ j\neq k}}^{r} e^{\theta_j+\theta_k} + \sum_{\substack{i,j,k=1 \\ 1\neq j\neq k}}^{r} e^{\theta_i+\theta_j+\theta_k} + \ldots + e^{\sum_{j=1}^{r}\theta_j} = 0 \tag{16.2.8}$$

The left side of (16.2.6)contains 2^r terms so the left side of (16.2.8) contains 2^r terms all of the form e^{ϕ} where

$$\phi = \epsilon_1\theta_1 + \epsilon_2\theta_2 + \ldots + \epsilon_r\theta_r \text{ in which } \epsilon_j = 0\ or 1,$$

many of which are zero.
Let $\phi_1, \phi_2, \ldots, \phi_n$ be the n non-zero terms so that there are $2^r - n$ zero terms. Then with $q = 2^r - n$,

$$q + e^{\theta_1} + e^{\theta_2} + \ldots + e^{\theta_r} = 0 \tag{16.2.9}$$

We now introduce the Hermite-like polynomial. The remainder of the proof is very similar to that of the proof that e is transcendental and will be dealt with more concisely when it uses results already proved in that proof.
Let p be a large prime and let,

$$f(x) = b^{np}x^{p-1}(x-\phi_1)^p(x-\phi_2)^p \cdots (x-\phi_n)^p$$

By the fundamental theorem of elementary symmetric functions and Lemmas 128 and 129, $f(x)$ is a polynomial in x with integer coefficients. (This is the unproven step)
With the function $I(t)$ as in Lemma 124, page 185, define,

$$J = I(\phi_1) + I(\phi_2) + \ldots + I(\phi_n)$$

From Lemma 124,

$$I(t) = e^t \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(t)$$

We deduce that with q as in (16.2.9),

$$J = -q\sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m}\sum_{k=1}^{n} f^{(j)}(\phi_k), \; m = (n+1)p - 1. \tag{16.2.10}$$

Now the sum over k is a symmetric polynomial in $b\phi_1, b\phi_2, \ldots, b\phi_n$ with integer coefficients and is therefore a symmetric polynomial with integer coefficients in the 2^r numbers

$$b\phi = b(\epsilon_1\theta_1 + \epsilon_2\theta_2 + \ldots + \epsilon_r\theta_r).$$

Hence, by the fundamental theorem of elementary symmetric functions, this sum is an (ordinary) rational number. Also, Lemmas 128 and 129 imply that the sum is further an (ordinary) integer, that is, $J \in \mathbb{Z}$.
(The remainder of the proof, giving the contradiction, is very similar to that for the corresponding J in the proof for e and the details are therefore omitted.)
Since $f^{(j)}(\phi_k) = 0$ for $j < p$ we deduce that the double sum in the above expression (16.2.5) for J is an ordinary integer divisible by $(p-1)!$.

Further, if p is sufficiently large, then $f^{(p-1)}(0)$ is not divisible by p. If also $p > q$, then,

$$|J| \geq (p-1)!$$

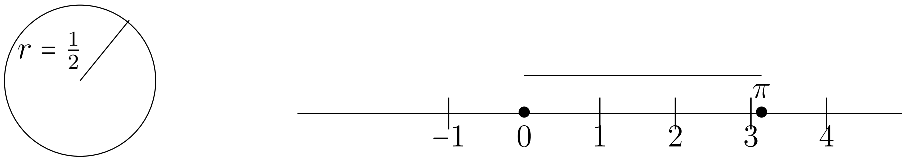
On the other hand, using the upper bound we obtained for $|I(t)|$, we have,

$$|J| \leq \sum_{k=1}^{n} |\phi_k| e^{|\phi_k|} \bar{f}(|\phi_k|) \leq c_1 c_2^p$$

for some constants c_1, c_2. This contradiction completes the proof. □

16.3 Finding π

Let's pause after that for some light relief. How can we find the actual value of π? It's is easy to see that π is about 3.14. By definition π is the ratio of the circumference C of a circle to its diameter d or $\pi = \dfrac{C}{d}$. So if we take a circle (say made of string) of diameter 1 or radius $\dfrac{1}{2}$ then its circumference is π. To find π we simply need to cut the circle and spread it out on a number line with its left end on 0 and read off the value under its right end.



But how can we find a much better value of π, something like 3.14159265359? Well, one way is we put $x = \dfrac{1}{2}$ and $\sin\dfrac{\pi}{2} = 1$ in Equation (19.2.6) which we derive in Chapter 19, namely,

$$\frac{\sin \pi x}{\pi x} = \prod_{r=1}^{\infty}\left(1 - \frac{x^2}{r^2}\right)$$

to give,

$$\frac{\sin\dfrac{\pi}{2}}{\dfrac{\pi}{2}} = \frac{2}{\pi} = \prod_{r=1}^{\infty}\left(1 - \frac{1}{(2r)^2}\right)$$

$$\Rightarrow \pi = \frac{2}{\displaystyle\prod_{r=1}^{\infty}\left(1 - \frac{1}{(2r)^2}\right)}$$

$$\Rightarrow \pi = \frac{2}{\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{16}\right)\left(1 - \frac{1}{36}\right)\dots}$$

Keeping things simple, you can set this up on an Excel spreadsheet putting say 1 to 20,000 in the first column, start the second column with $\dfrac{2}{1-\dfrac{1}{4}}$ and add in the successive $1-\dfrac{1}{(2r)^2}$ terms in the denominator as you progress down the second. You will see the value of π builds extremely slowly like this.

r	π
1	2.8
19	3.1
493	3.14
1,331	3.141
8,447	3.1415
20,000	3.14155

The "cut the circle" exercise above shows π converges but its convergence is extremely slow. There are other series giving values of π. One is the Gregory Series for the infinite series of the inverse tan function, namely

$$\tan^{-1} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots$$

where with $x = 1$ we have $\tan^{-1} x = \dfrac{\pi}{4}$ so

$$\pi = 4(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots)$$

but this series converges much more slowly than the one we developed above based on $\dfrac{\sin \pi x}{\pi x}$. It needs 5 billion terms to give 10 decimal places accurately. At 40,000 terms it gives $\pi = 3.141543$ which is still not as accurate as the $\dfrac{\sin \pi x}{\pi x}$ series at 20,000 terms. You can see how math can be quite competitive!

Chapter 17

Bernoulli Numbers and Sum of a Finite p-series

Our goal in this chapter is to sum a finite series such as $1^2 + 2^2 + 3^2 + \ldots + n^2$ or in general the p-series,

$$1^p + 2^p + \ldots + n^p,\ p = 1, 2, 3, \ldots$$

We will find, for example, that,

$$1^3 + 2^3 + 3^3 + \ldots + 100^3 = \frac{100^4}{4} + \frac{100^3}{2} + \frac{100^2}{4} = 25,502,500$$

It turns out that the sum of these finite series can be expressed in what is called a "closed form" or a single formula. This formula involves a famous sequence of numbers called Bernoulli numbers, named after their discoverers, the Bernoulli brothers.

Course: Tasting Plate II
Ingredients
Calculus of the natural exponential function.
Taylor series for e^x
Definition of Bernoulli numbers
Directions
Define and develop the theory of Bernoulli numbers.
Find the formula for the sum of a finite p-series and give examples.

17.1 Bernoulli Numbers

Definition 63. *Bernoulli numbers*
The Bernoulli numbers B_n are defined as the coefficients in the expansion,

$$\frac{x}{e^x - 1} = B_0 + \frac{B_1}{1!}x + \frac{B_2}{2!}x^2 + \frac{B_3}{3!}x^3 + \ldots \qquad (17.1.1)$$

Consider,

$$\frac{x}{e^x - 1} = \frac{x}{x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots}$$

where we applied the Taylor series for e^x derived in Theorem 117, page 171. Let's (drearily) perform the long division to express the right side as,

$$B_0 + \frac{B_1}{1!}x + \frac{B_2}{2!}x^2 + \frac{B_3}{3!}x^3 + \dots$$

We begin,

$$\begin{array}{r l}
 & 1 - \frac{1}{2}x + \frac{1}{12}x^2 + \dots \\ \cline{2-2}
x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \dots) & x \\
 & x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \dots \\ \cline{2-2}
 & \quad - \frac{x^2}{2} - \frac{x^3}{6} - \frac{x^4}{24} - \frac{x^5}{120} + \dots \\
 & \quad - \frac{x^2}{2} - \frac{x^3}{4} - \frac{x^4}{12} - \frac{x^5}{48} + \dots \\ \cline{2-2}
 & \qquad\quad + \frac{x^3}{12} + \frac{x^4}{24} + \frac{x^5}{60} + \dots \\
 & \qquad\quad \dots\dots\dots\dots\dots\dots
\end{array}$$

From the above long division we have,

$$B_0 + \frac{B_1}{1!}x + \frac{B_2}{2!}x^2 + \dots = 1 - \frac{1}{2}x + \frac{1}{12}x^2 + \dots$$

hence

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{12} \cdot 2! = \frac{1}{6}$$

***

But let's stop here and try another route! A more efficient way to proceed is to equate powers of x in the adjusted equation (17.1.1)

$$x = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n \cdot (e^x - 1)$$

We have,

$$\begin{aligned}
x &= \left(B_0 + \frac{B_1}{1!}x + \frac{B_2}{2!}x^2 + \frac{B_3}{3!}x^3 + \dots\right) \cdot \left(x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \dots\right) \\
&= B_0 x + \left(\frac{B_0}{2!} + \frac{B_1}{1!}\right)x^2 + \left(\frac{B_0}{3!} + \frac{B_1}{1!} \cdot \frac{1}{2!} + \frac{B_2}{2!}\right)x^3 + \dots
\end{aligned}$$

Equating coefficients of x gives $1 = B_0$.
Equating coefficients of x^2 gives $0 = \frac{B_0}{1} + B_1 \Rightarrow B_1 = -\frac{1}{2}$
Equating coefficients of x^3 gives,

$$0 = \frac{B_0}{6} + \frac{B_1}{2} + \frac{B_3}{2} \Rightarrow B_2 = 2\left(-\frac{1}{6} + \frac{1}{4}\right) = \frac{1}{6}$$

Equating coefficients of x^4 gives,

$$0 = \frac{B_0}{24} + \frac{B_1}{6} + \frac{B_2}{4} + \frac{B_3}{6} = \frac{1}{24} - \frac{1}{12} + \frac{1}{24} + \frac{B_3}{6} \Rightarrow B_3 = 0$$

OK, it's more efficient, but it is still dreary! Let's go elsewhere.

***

Definition 64. *even and odd functions*
A function $f(x)$ is an even function if $f(-x) = f(x)$.
A function $f(x)$ is an odd function if $f(-x) = -f(x)$.

Example 88.
$f(x) = x^4 + 3x^2 + 6$ is an even function since $f(-x) = (-x)^4 + 3(-x)^2 + 6 = f(x)$.
$f(x) = x^3 - 7x$ is an odd function since $f(-x) = (-x)^3 - 7(-x) = -x^3 + 7x = -f(x)$ ◇

If $f(x)$ is a polynomial, it is obvious it can only be an even function if all terms containing odd powers of x have a coefficient of zero.

Example 89. *Since the Taylor series of $\sin x$ contains only odd powers of x then it is not an even function, but $\cos x$ obviously is an even function.*

$$\sin x = \frac{x}{1!} + \frac{x^3}{3!} + \frac{x^5}{5!} + \dots$$
$$\cos x = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \frac{x^6}{6!} + \dots$$

Invoking Theorem 110 on page 162, we actually do have $\sin(-x) = -\sin x$, $\cos(-x) = \cos x$, so $\cos x$ is an even function and $\sin x$ is not. ◇

Lemma 132.
The odd Bernoulli numbers $B_{2n+1}, n > 1$ are all zero.

Proof. By definition the Bernoulli numbers are generated by,

$$\begin{aligned}\frac{x}{e^x - 1} &= B_0 + \frac{B_1}{1!}x + \frac{B_2}{2!}x^2 + \frac{B_3}{3!}x^3 + \frac{B_4}{4!}x^4 + \frac{B_5}{5!}x^5 + \dots \\ &= 1 - \frac{x}{2} + \frac{B_2}{2!}x^2 + \frac{B_3}{3!}x^3 + \frac{B_4}{4!}x^4 + \frac{B_5}{5!}x^5 + \dots \text{ putting } B_1 = -\frac{1}{2}\end{aligned}$$

$$\Rightarrow \frac{x}{e^x - 1} + \frac{x}{2} = 1 + \frac{B_2}{2!}x^2 + \frac{B_3}{3!}x^3 + \frac{B_4}{4!}x^4 + \frac{B_5}{5!}x^5 + \dots \tag{17.1.2}$$

Now if $f(x) = \dfrac{x}{e^x - 1} + \dfrac{x}{2}$ then,

$$\begin{aligned} f(x) - f(-x) &= \frac{x}{e^x - 1} + \frac{x}{2} - \left(\frac{-x}{e^{-x} - 1} + \frac{-x}{2} \right) \\ &= \frac{x}{e^x - 1} + \frac{x}{2} + \frac{x}{e^{-x} - 1} + \frac{x}{2} \\ &= x + x\left(\frac{1}{e^x - 1} + \frac{e^x}{1 - e^x} \right) \\ &= x + x\left(\frac{1 - e^x}{e^x - 1} \right) \\ &= x - x = 0 \end{aligned}$$

Then $f(x) = f(-x)$ so $f(x)$ is an even function. But since the left side of the equation (17.1.2) is an even function, then the right side must also be an even function, that is, the coefficient of every odd power of x must be zero, implying the odd Bernoulli numbers B_{2n+1} are all zero. □

We still lack an efficient way of calculating the even Bernoulli numbers. The following theorem is an excellent example of obtaining a result by generalizing the relevant definition.

Definition 65. *generalized Bernoulli function*
For any complex number z we define the generalized functions $B_n(x)$ by the equation,

$$\frac{ze^{xz}}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n, \quad \textit{where } |z| \le 2\pi$$

The constant functions $B_n(0)$ with $x = 0$ are generated by,

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n(0)}{n!} z^n$$

Accordingly, referencing (17.1.1), they are the Bernoulli numbers and we let
$B_n(0) = B_n$.

Theorem 133.
The functions $B_n(x)$ are polynomials in x given by

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$$

Proof. We have, using the definition of B_n and the Taylor series expansion for e^x from

Theorem 117, page 171 written in reverse,

$$\begin{aligned}
&\sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n \\
&= \frac{z}{e^z - 1} \cdot e^{xz} \\
&= \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n \right) \times \left(\sum_{n=0}^{\infty} \frac{x^n}{n!} z^n \right) \\
&= \left(\frac{B_0}{0!} + \frac{B_1}{1!} z + \ldots + \frac{B_n}{n!} z^n \right) \left(\ldots \frac{x^n}{n!} z^n + \frac{x^{n-1}}{(n-1)!} z^{n-1} + \frac{x^{n-2}}{(n-2)!} z^{n-2} + \ldots + \frac{x}{1!} z + 1 \right)
\end{aligned}$$

Selecting the terms in z^n we have,

$$\begin{aligned}
\frac{B_n(x)}{n!} z^n &= \frac{B_0}{0!} \frac{x^n}{n!} z^n + \frac{B_1}{1!} \frac{x^{n-1}}{(n-1)!} z^n + \frac{B_2}{2!} \frac{x^{n-2}}{(n-2)!} z^n + \ldots + \frac{B_n}{n!} z^n \\
\Rightarrow \frac{B_n(x)}{n!} &= \sum_{k=0}^{n} \frac{B_k}{k!} \frac{x^{n-k}}{(n-k)!} \\
\Rightarrow B_n(x) &= \sum_{k=0}^{n} \frac{n!}{(n-k)!k!} B_k x^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}
\end{aligned}$$

□

Theorem 134. *The Bernoulli polynomials $B_n(x)$ satisfy the difference equation,*

$$B_n(x+1) - B_n(x) = nx^{n-1} \text{ if } n \geq 1$$

Therefore,

$$B_n(0) = B_n(1) \text{ if } n \geq 2$$

Proof. We construct the identity,

$$\sum_{n=0}^{\infty} \frac{B_n(x+1) - B_n(x)}{n!} = z\frac{e^{(x+1)z}}{e^z - 1} - z\frac{e^{xz}}{e^z - 1} = ze^{xz} \left(\frac{e^z - 1}{e^z - 1} \right) = ze^{xz}$$

From this identity, using the Taylor expansion $e^{xz} = \sum_{n=0}^{\infty} \frac{(xz)^n}{n!}$, we find,

$$\begin{aligned}
\sum_{n=0}^{\infty} \frac{B_n(x+1) - B_n(x)}{n!} z^n &= \sum_{n=0}^{\infty} z\frac{(xz)^n}{n!} \\
&= \frac{x^0}{0!} z^1 + \frac{x^1}{1!} z^2 + \ldots + \frac{x^{n-1}}{(n-1)!} z^n + \ldots
\end{aligned}$$

Equating the coefficients of $z^n, n \geq 1$ and noting $\dfrac{n!}{(n-1)!} = n$ we obtain,

$$\frac{B_n(x+1) - B_n(x)}{n!} = \frac{x^{n-1}}{(n-1)!} \text{ if } n \geq 1$$
$$\Rightarrow B_n(x+1) - B_n(x) = nx^{n-1}$$

Putting $x = 0$ and avoiding division by zero we find,

$$B_n(0) = B_n(1) \text{ if } n \geq 2$$

□

Theorem 135.
If $n \geq 2$ we have,

$$B_n = \sum_{k=0}^{n} \binom{n}{k} B_k$$

Proof. Since by Theorem 133 the functions $B_n(x)$ are polynomials in x given by,

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k},$$

putting $x = 1$ and using $B_n = B_n(0) = B_n(1)$ if $n \geq 2$ we find,

$$B_n = B_n(1) = \sum_{k=0}^{n} \binom{n}{k} B_k$$

□

We now have a recursive formula for calculating the Bernoulli numbers succeeding $B_0 = 1, B_1 = -\dfrac{1}{2}$.

$$B_2 = \sum_{k=0}^{2} \binom{2}{k} B_k = \binom{2}{0} B_0 + \binom{2}{1} B_1 + \binom{2}{2} B_2 = 1 + 2\left(-\frac{1}{2}\right) + B_2 = B_2$$

tells us nothing, but,

$$\begin{aligned} B_3 = \sum_{k=0}^{3} \binom{3}{k} B_k &= \binom{3}{0} B_0 + \binom{3}{1} B_1 + \binom{3}{2} B_2 + \binom{3}{3} B_3 \\ &= 1 + 3\left(-\frac{1}{2}\right) + 3B_2 + B_3 \\ \Rightarrow 3B_2 &= \frac{3}{2} - 1 = \frac{1}{2} \\ \Rightarrow B_2 &= \frac{1}{6} \end{aligned}$$

In a similar fashion, omitting all the odd Bernoulli numbers which are all zero,

$$B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30},\ B_{10} = \frac{5}{66}$$

17.2 Formula for the Sums of Powers of Integers

Theorem 136.
For $m \ge 1$,

$$S_m(n) = 1^m + 2^m + \ldots + (n-1)^m = \sum_{k=0}^{m} \binom{m+1}{k} \frac{B_k}{m+1} n^{m+1-k}$$

Proof. Let $S_m(n) = 1^m + 2^m + \ldots + (n-1)^m$.
From Theorem 117, page 171,

$$\begin{aligned} e^x &= 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \\ \Rightarrow e^{kt} &= 1 + \frac{kt}{1!} + \frac{(kt)^2}{2!} + \frac{(kt)^3}{3!} + \ldots \end{aligned}$$

Substituting $k = 0, 1, 2, \ldots, n-1$ gives the equations,

$$\begin{aligned} e^0 &= 1 \\ e^t &= 1 + 1 \cdot \frac{t}{1!} + 1^2 \cdot \frac{t^2}{2!} + 1^3 \cdot \frac{t^3}{3!} + 1^4 \cdot \frac{t^4}{4!} + \ldots \\ e^{2t} &= 1 + 2 \cdot \frac{t}{1!} + 2^2 \cdot \frac{t^2}{2!} + 2^3 \cdot \frac{t^3}{3!} + 2^4 \cdot \frac{t^4}{4!} + \ldots \\ e^{3t} &= 1 + 3 \cdot \frac{t}{1!} + 3^2 \cdot \frac{t^2}{2!} + 3^3 \cdot \frac{t^3}{3!} + 3^4 \cdot \frac{t^4}{4!} + \ldots \\ &\ldots \\ e^{(n-1)t} &= 1 + (n-1) \cdot \frac{t}{1!} + (n-1)^2 \cdot \frac{t^2}{2!} + (n-1)^3 \cdot \frac{t^3}{3!} + (n-1)^4 \cdot \frac{t^4}{4!} + \ldots \end{aligned}$$

Adding the columns of these equations gives[1],

$$\begin{aligned} 1 + e^t + e^{2t} + e^{3t} + e^{4t} + \ldots + e^{(n-1)t} &= n - 1 + S_1(n)\frac{t}{1!} + S_2(n)\frac{t^2}{2!} + S_3(n)\frac{t^3}{3!} + S_4(n)\frac{t^4}{4!} + \ldots \\ &= \sum_{m=0}^{\infty} S_m(n) \frac{t^m}{m!} \end{aligned}$$

Recalling the sum of the first n terms of the geometric series $a + ar + ar^2 + \ldots + ar^{n-1}$ is given by,

$$a + ar + ar^2 + \ldots + ar^{n-1} = \frac{a(r^n - 1)}{r - 1},$$

we have, with $a = 1, r = e^t$,

$$\frac{e^{nt} - 1}{e^t - 1} = \sum_{m=0}^{\infty} S_m(n) \frac{t^m}{m!} \tag{17.2.1}$$

[1] Note $S_0(n) = 1^0 + 2^0 + \ldots + (n-1)^0 = n - 1$

Now,

$$\begin{aligned}\frac{e^{nt}-1}{e^t-1} &= \frac{e^{nt}-1}{t} \bullet \frac{t}{e^t-1}\\ &= \frac{\left(\cancel{1}+nt+\frac{(nt)^2}{2!}+\frac{(nt)^3}{3!}+\ldots-\cancel{1}\right)}{t} \bullet \sum_{j=0}^{\infty} B_j\frac{t^j}{j!}\\ &= \left(n+\frac{n^2t}{2!}+\frac{n^3t^2}{3!}+\ldots\right)\bullet\sum_{j=0}^{\infty} B_j\frac{t^j}{j!}\end{aligned}$$

Then we have from (17.2.1),

$$\begin{aligned}\sum_{m=0}^{\infty} S_m(n)\frac{t^m}{m!} = &\left(n+\frac{n^2t}{2!}+\ldots+\frac{n^m t^{m-1}}{m!}+\frac{n^{m+1}t^m}{(m+1)!}+\ldots\right)\\ &\bullet\left(\ldots+\frac{B_m}{m!}t^m+\frac{B_{m-1}}{(m-1)!}t^{m-1}+\ldots+\frac{B_2}{2!}t^2+\frac{B_1}{1!}t^1+B_0\right)\end{aligned}$$

If we equate the terms in t^m on either side we have,

$$S_m(n)\frac{1}{m!} = \frac{B_m}{m!}\cdot n+\frac{B_{m-1}}{(m-1)!}\cdot\frac{n^2}{2!}+\ldots+\frac{B_1}{1!}\bullet\frac{n^m}{m!}+B_0\bullet\frac{n^{m+1}}{(m+1)!}$$

Multiplying by $(m+1)!$ gives,

$$\begin{aligned}\frac{(m+1)!}{m!}S_m(n) = \frac{B_m}{m!}(m+1)!\bullet n+\frac{B_{m-1}}{(m-1)!}(m+1)!\bullet\frac{n^2}{2!}+\frac{B_{m-2}}{(m-2)!}(m+1)!\frac{n^3}{3!}+\\ \ldots+\frac{B_1}{1!}\bullet\frac{n^m(m+1)!}{m!}+B_0\bullet\frac{n^{m+1}(m+1)!}{(m+1)!}\end{aligned}$$

So we have,

$$\begin{aligned}(m+1)S_m(n) &= \sum_{k=0}^{m}\binom{m+1}{k}B_k n^{m+1-k}\\ \Rightarrow S_m(n) &= \sum_{k=0}^{m}\binom{m+1}{k}\frac{B_k}{m+1}n^{m+1-k}\\ \Rightarrow 1^m+2^m+\ldots+(n-1)^m &= \sum_{k=0}^{m}\binom{m+1}{k}\frac{B_k}{m+1}n^{m+1-k}\end{aligned}$$

□

Example 90. *We can now apply the formula to* $\sum_{k=0}^{n} k^p$, $p = 1, 2, 3, \ldots$ *Note,* $S_m = 1^m + 2^m + \ldots + (n-1)^m$ *so that* $\sum_{k=1}^{n} k^m = S_m + n^m$.

$$\begin{aligned}
\sum_{k=1}^{n} k^1 &= \frac{n^2}{2} + \frac{n}{2} \\
\sum_{k=1}^{n} k^2 &= \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} \\
\sum_{k=1}^{n} k^3 &= \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4} \\
\sum_{k=1}^{n} k^4 &= \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30} \\
&\ldots \\
\sum_{k=1}^{n} k^{10} &= \frac{n^{11}}{11} + \frac{n^{10}}{2} + \frac{5n^9}{6} - n^7 + n^5 - \frac{n^3}{2} + \frac{5n}{66}
\end{aligned}$$

Now $\sum_{k=1}^{100} k^{10} = 1^{10} + 2^{10} + \ldots + 100^{10}$ *has 100 terms each of which soon becomes huge as we multiply it out (like* 50^{10}*) but the whole is easily computed from*

$$\frac{100^{11}}{11} + \frac{100^{10}}{2} + \frac{5 \bullet 100^9}{6} - 100^7 + 100^5 - 100^3 + \frac{5 \bullet 100}{66} \qquad \diamond$$

Part VII

Shopping Excursion 4

The Natural Logarithm Function

Just as the natural exponential function e^x arises “naturally” in many branches of mathematics and science, so does its inverse function, the natural logarithmic function $\log x$.
Like its inverse, $\log x$ has a simple derivative, filling in the integral’s power rule,

$$\int x^n \; dx = \frac{x^{n+1}}{n+1} + c, \;\; n \neq 1$$
$$\int x^{-1} \; dx = \log x + c$$

Like its inverse, $\log x$ has a Taylor series.
We will use the $\log x$ properties many times in the following chapters.

Chapter 18

The Natural Logarithm Function

Ingredients
Inverse function theory – definitions, finding and graphing inverses
The natural exponential function
Directions
Define and study the natural logarithmic function.
Find its derivative.
Study an alternative definition of the natural logarithmic function.
Derive the laws of logarithms.
Derive the exponential laws.
Study extensions of the natural logarithmic function.
Learn how to differentiate complicated functions using logarithms.
Apply Taylor series to find the series for a logarithmic function.

We define the natural logarithmic function as the inverse function of the natural exponential function.

18.1 Inverse Functions

Definition 66. *composition of functions*
The composition $f(g(x))$ of two functions $f(x), g(x)$ means that the variable x in the function f is replaced with the expression for $g(x)$. You may already know its notation as $f \circ g(x)$.

Example 91. *If $f(x) = 2x - 1$ and $g(x) = x^2 - 4$ then*

$$f(g(x)) = 2g(x) - 1 = 2(x^2 - 4) - 1 = 2x^2 - 9 \qquad \diamond$$

Definition 67. *inverse functions*
Two functions f and g are said to be inverse functions if,

- *$f(g(x)) = x$ for all x in the domain of g*

- *$g(f(x)) = x$ for all x in the domain of f.*

Example 92. *To prove $f(x) = \frac{1}{3}x - 7$ and $g(x) = 3x + 21$ are inverse functions we show,*

- $f(g(x)) = \frac{1}{3}g(x) - 7 = \frac{1}{3}(3x + 21) - 7 = x$
- $g(f(x)) = 3f(x) + 21 = 3\left(\frac{1}{3}x - 7\right) + 21 = x$

So f and g are inverse functions. ◇

Notation 4. *We write a function and its inverse as f and f^{-1} or g and g^{-1}, etc. Then our definition becomes:*
Two functions f and f^{-1} are said to be inverse functions if and only if,

- $f(f^{-1}(x)) = x$ for all x in the domain of f^{-1}
- $f^{-1}(f(x)) = x$ for all x in the domain of f.

18.1.1 Finding inverse functions

Assuming the inverse function of $y = f(x)$ exists, we can find it as follows:

1. Interchange x and y in the equation $y = f(x)$ to get $x = f(y)$.
2. Solve the new equation for y in terms of x. This new equation is the inverse function $f^{-1}(x)$.

Note, since we have interchanged x and y, it follows that the domain of the inverse function is the range of the original function and the range of the inverse function is the domain of the original function.

Example 93.
To find the inverse function of $f(x) = 4x - 3$, we write $y = 4x - 3$ and,

1. *Interchange x and y in the equation $y = 4x - 3$ to get $x = 4y - 3$.*
2. *Solve the new equation for y in terms of x, giving $y = \frac{x+3}{4} = f^{-1}(x)$.*

To show this is correct we return to the definition to show,

$$f(f^{-1})(x) = 4f^{-1}(x) - 3 = 4\frac{x+3}{4} - 3 = x$$

You can check the other condition $f^{-1}(f(x)) = x$. ◇

18.1.2 Sketching the graphs of inverse functions

Since we interchanged variables to obtain the inverse function, it follows that if (b, a) lies on the graph of a function, then (a, b) lies on the graph of its inverse. This means the graph of $f^{-1}(x)$ is the reflection of the graph of $f(x)$ in the line $y = x$ as shown in Figure 35.

Note the point (b, a) on the graph of $f(x)$ reflects to become the point (a, b) on the graph of $f^{-1}(x)$ as follows. From (b, a) on the graph of $y = f(x)$ we measure the shortest distance to a point on the line $y = x$ and then go the same distance in the same direction on the other side of $y = x$ to locate (a, b) on the graph of $y = f^{-1}(x)$.

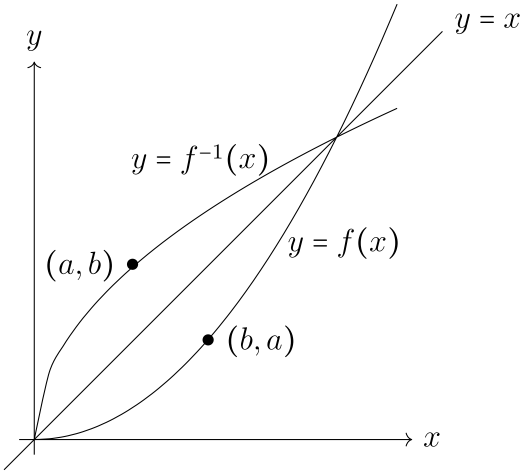


Figure 35

18.2 Logarithmic Functions

Definition 68. *logarithmic function with base b*
The inverse of the exponential function $y = f(x) = b^x$ with base b is called the logarithmic function $y = f^{-1}(x) = \log_b x$, with base b.

We obtain the inverse function of $y = b^x$ as usual by interchanging the variables to get $x = b^y$. We cannot solve $x = b^y$ for $y = f(x)$ so we invent a new function defined as $y = \log_b x$ to mean $x = b^y$. So we have the equivalence,

$$y = log_b x \Leftrightarrow x = b^y$$

The first expression is in logarithmic form, the second is in exponential form. Note, that a logarithm therefore is an exponent, y is the power or exponent to which the base b must be raised to get x.

Example 94. *Some equivalent statements are:*

(a) $2^3 = 8 \Leftrightarrow \log_2 8 = 3$

(b) $10^2 = 100 \Leftrightarrow \log_{10} 100 = 2$

(c) $\log_6 216 = 3 \Leftrightarrow 216 = 6^3$ $\diamond$

18.2.1 Graphs of logarithmic functions

Since the logarithmic function is the inverse of the exponential function, the graph of $y = \log_b x$ is obtained by reflecting the graph of $y = b^x$ in the line $y = x$. See Figure 36.

Note 24. *Every graph of* $y = \log_b x$,

(a) passes though (1,0)

(b) approaches the negative $y-$*axis asymptotically*

(c) grows very slowly as $x \to \infty$, *for example* $\log_{10} 10 = 1, \log_{10} 1000 = 3$

(d) The domain of $y = \log_b x$ *is* $(0, \infty)$ *or* $x > 0$ *only.*

(e) The logarithm of negative numbers and zero is undefined. You cannot evaluate the logarithm of a negative number or zero

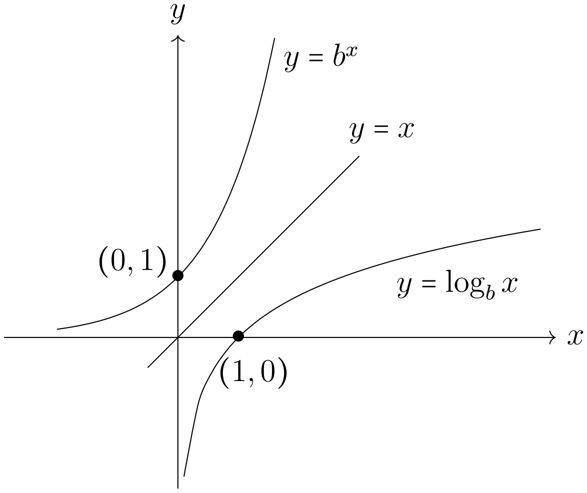


Figure 36

18.3 The Natural Logarithmic Function

Definition 69. *natural logarithmic function*
We define the natural logarithmic function $y = \log_e x$ *or simply* $y = \log x$ *as the inverse of the natural exponential function* $y = e^x$.
We form the inverse function, as usual, by interchanging the variables x, y *and making*

y the subject of the new equation. To do this we needed notation for a new function since we cannot solve $x = e^y$ for y. We define $y = \log x$ to mean $x = e^y$. Accordingly, since $f(f^{-1}(x)) = f^{-1}(f(x)) = x$ we have

$$e^{\log x} = x \textit{ and } \log e^x = x \textit{ for all } x$$

18.4 Derivative of the Natural Logarithmic Function

Theorem 137.

$$\frac{d}{dx}(\log|x|) = \frac{1}{x}, \ \ x \neq 0$$

Proof. We use $y = \log x \Leftrightarrow x = e^y$ and the chain rule, Theorem 63, page 89.

$$\begin{aligned} x = e^y &\Rightarrow \frac{d}{dx}x = \frac{d}{dx}e^y \\ &\Rightarrow 1 = \frac{de^y}{dy}\frac{dy}{dx} = e^y\frac{dy}{dx} \\ &\Rightarrow \frac{dy}{dx} = \frac{1}{e^y} = \frac{1}{x} \\ &\Rightarrow \frac{d}{dx}\log x = \frac{1}{x} \end{aligned}$$

More generally, since for $x > 0$ we have,

$$\frac{d}{dx}\log|x| = \frac{d}{dx}\log x = \frac{1}{x}$$

and, for $x < 0$ we have,

$$\frac{d}{dx}\log|x| = \frac{d}{dx}\log(-x) = \frac{d\log(-x)}{d(-x)}\frac{d(-x)}{dx} = \frac{1}{-x}\cdot(-1) = \frac{1}{x}$$

We conclude,

$$\frac{d}{dx}\log|x| = \frac{1}{x} \text{ for all } x \text{ except } x = 0.$$

□

18.5 Alternative definition of $\log x$

Definition 70. *We could also define,*

$$\log x = \int_1^x \frac{1}{t}\ dt$$

Graphically, $\log x$ *is the area under the curve* $f(t) = \dfrac{1}{t}$ *for* $1 \le t \le x$*. See Figure 37.*

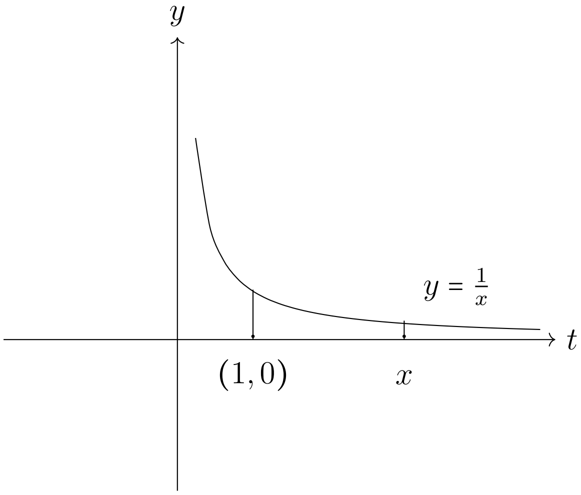


Figure 37

By Theorem 66, First Fundamental Theorem of Calculus, page 94, we have,

$$\frac{d}{dx}(\log x) = \frac{d}{dx}\int_1^x \frac{1}{t}\ dt = \frac{1}{x}$$

as in Theorem 137, so that in general,

$$\int \frac{1}{x}\ dx = \log x + c$$

We can then develop the usual laws of logarithms from this definition.

18.6 Laws of Logarithms

Lemma 138.

$$\log 1 = 0$$

Proof.

$$\log 1 = \int_1^1 \frac{1}{t}\ dt = 0$$

□

Lemma 139.

$$\log xy = \log x + \log y$$

Proof.

$$\log xy = \int_1^{xy} \frac{1}{t}\,dt = \int_1^{x} \frac{1}{t}\,dt + \int_x^{xy} \frac{1}{t}\,dt \text{ by Theorem 70, page 97}$$

In the second integral we put $u = \frac{t}{x} \Rightarrow \frac{du}{dt} = \frac{1}{x} \Rightarrow du = \frac{dt}{x}$ and change the limits of integration to,

$$t = x \Rightarrow u = \frac{x}{x} = 1, t = xy \Rightarrow u = \frac{xy}{x} = y$$

to give,

$$\int_x^{xy} \frac{1}{t}\,dt = \int_1^{y} \frac{1}{u}\,du = \log y - \log 1 = \log y$$

Hence,

$$\log xy = \int_1^{x} \frac{1}{t}\,dt + \int_1^{y} \frac{1}{u}\,du = \log x + \log y$$

□

Note 25. *The logarithm of an infinite product.*
The result $\log xy = \log x + \log y$ *extends to,*

$$\log\left(\prod_{n=1}^{\infty} f(n)\right) = \sum_{n=1}^{\infty} \log(f(n))$$

We have for example,

$$\log xyz = \log(xy)z = \log xy + \log z = \log x + \log y + \log z$$

and we continue in this manner to show the logarithm of the product of any number of variables is just the sum of their logarithms.

Lemma 140.

$$\log \frac{x}{y} = \log x - \log y$$

Proof.

$$\log x = \log\left(y \cdot \frac{x}{y}\right) = \log y + \log \frac{x}{y} \text{ by Lemma 139}$$
$$\Rightarrow \log \frac{x}{y} = \log x - \log y$$

□

Lemma 141.

$$\log x^p = p \log x$$

Proof.

$$\frac{d}{dx}(\log x^p) = \frac{d\log x^p}{dx^p} \cdot \frac{dx^p}{dx} = \frac{1}{x^p} \cdot px^{p-1} = \frac{p}{x}$$

Also,

$$\frac{d}{dx}(p\log x) = p \cdot \frac{1}{x}$$

Therefore, since the two left side derivatives both equal $\frac{p}{x}$ we have,

$$\log x^p = p\log x + c$$

But putting $x = 1$ shows $c = 0$. □

We would then define the natural exponential function $f^{-1}(x) = e^x$ as the inverse of the natural logarithm function $f(x) = \log x$, and then the definition

$$f(f^{-1}(x)) = x \text{ and } f^{-1}(x)) = x$$

gives,

$$\log e^x = x,\ \ e^{\log x} = x$$

We can then go ahead and prove the exponential laws for the base e.

18.7 Exponential Laws for Base e.

Lemma 142.

$$e^{x+y} = e^x \cdot e^y$$

Proof. Let,

$$x = \log u \Leftrightarrow u = e^x$$
$$y = \log v \Leftrightarrow v = e^y$$

Then,

$$e^{x+y} = e^{\log u + \log v} = e^{\log uv} = uv = e^x \cdot e^y$$

□

Lemma 143.

$$e^{x-y} = \frac{e^x}{e^y}$$

Lemma 144.

$$(e^x)^y = e^{xy}$$

The final two proofs are left to the reader.

Note 26. *To prove the exponential laws for any real base a we use* $e^{\log x} = x$ *and argue as follows in proving (say) the first law.*

$$\begin{aligned} a^x \cdot a^y &= e^{\log a^x} \cdot e^{\log a^y} \\ &= e^{x \log a} \cdot e^{y \log a} \\ &= e^{x \log a + y \log a} \\ &= e^{(x+y) \log a} \\ &= e^{\log a^{x+y}} \\ &= a^{x+y} \end{aligned}$$

18.8 $\log x$ and $\ln x$

When students of mathematics are first introduced to the logarithm function, the symbol $\ln x$ is used for the natural logarithm function.
The reason is that historically the abbreviation log was used for logarithms to base 10 and in the days before handheld calculators and computers, using tables of logs to base 10 was the only way to do complex arithmetic calculations like $1000 \times 456 \div 3489^3$
But those days are long gone (where long gone means 30 years!) and mathematicians have now taken back the log symbol to mean the natural logarithm, the inverse of the natural exponential function.
So we will always use,

$$\log x \text{ for } \ln x$$

18.9 The derivative of $\log g(x)$.

To differentiate $\log g(x)$ we use the chain rule thus,

$$\begin{aligned} \frac{d}{dx} \log g(x) &= \frac{d \log g(x)}{dg(x)} \cdot \frac{dg(x)}{dx} \\ &= \frac{g'(x)}{g(x)} \end{aligned}$$

Example 95. *With* $g(x) = \sin x$,

$$\frac{d}{dx} \log(\sin x) = \frac{\cos x}{\sin x} \qquad \diamond$$

It therefore follows that,

$$\int \frac{g'(x)}{g(x)}\, dx = \log g(x) + c$$

Example 96. *With* $g(x) = x^4 + 6 \Rightarrow g'(x) = 4x^3$ *we first take care of the 4 and then just use the result above thus,*

$$\int \frac{x^3}{x^4 + 6}\, dx = \frac{1}{4} \int \frac{4x^3}{x^4 + 6}\, dx = \frac{1}{4} \log(x^4 + 6) + c. \qquad \diamond$$

18.10 Technique of logarithmic differentiation

We can differentiate complicated functions by using the product and quotient rules but it is often much simpler to proceed as in the following example. We use the logarithm properties, the derivative of $\log g(x)$ and the chain rule.

Example 97. *To differentiate*

$$y = \frac{(x^3-1)^4\sqrt{3x-1}}{x^2+4}$$

we take logs of both sides and use the rules of logarithms to expand the right side,

$$\log y = 4\log(x^3-1) + \frac{1}{2}\log(3x-1) - \log(x^2+4)$$

then differentiate both sides with respect to x *using the chain rule on the left side and the derivative of* $\log g(x)$ *on the right.*

$$\begin{aligned}
\frac{d\log y}{dx} &= \frac{4}{x^3-1}\cdot 3x^2 + \frac{1}{2}\cdot\frac{3}{3x-1} - \frac{2x}{x^2+4} \\
\Rightarrow \frac{d\log y}{dy}\cdot\frac{dy}{dx} &= \left(\frac{12x^2}{x^3-1} + \frac{1}{2}\cdot\frac{3}{3x-1} - \frac{2x}{x^2+4}\right) \\
\Rightarrow \frac{1}{y}\cdot\frac{dy}{dx} &= \left(\frac{12x^2}{x^3-1} + \frac{1}{2}\cdot\frac{3}{3x-1} - \frac{2x}{x^2+4}\right) \\
\Rightarrow \frac{dy}{dx} &= y\cdot\left(\frac{12x^2}{x^3-1} + \frac{1}{2}\cdot\frac{3}{3x-1} - \frac{2x}{x^2+4}\right) \\
\Rightarrow \frac{dy}{dx} &= \frac{(x^3-1)^4\sqrt{3x-1}}{x^2+4}\cdot\left(\frac{12x^2}{x^3-1} + \frac{1}{2}\cdot\frac{3}{3x-1} - \frac{2x}{x^2+4}\right)
\end{aligned}$$

18.11 Taylor Series of $\log(1+x)$.

Theorem 145.

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots = \sum_{k=0}^{\infty}(-1)^k\frac{x^{k+1}}{k+1},\ |x|<1$$

Proof. Consider the convergent geometric series,

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots, |x| < 1$$

Integrating with respect to x and using $\int \dfrac{g'(x)}{g(x)}\ dx = \log(g(x)) + c$ gives,

$$\begin{aligned}
\int \frac{1}{1-x}\ dx &= \int (1 + x + x^2 + \ldots + x^k + \ldots)\ dx,\ |x| < 1 \\
-\int \frac{-1}{1-x}\ dx &= \int (1 + x + x^2 + \ldots + x^k + \ldots)\ dx,\ |x| < 1 \\
-\log(1-x) &= x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \ldots + \frac{x^{k+1}}{k+1} + \ldots + c,\ |x| < 1
\end{aligned}$$

Substituting $x = 0$ gives $c = 0$ and substituting $-x$ for x gives,

$$\begin{aligned}
\log(1+x) &= x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots + (-1)^k \frac{x^{k+1}}{k+1} + \ldots,\ |x| < 1 \qquad (18.11.1) \\
&= \sum_{k=0}^{\infty} (-1)^k \frac{x^{k+1}}{k+1},\ |x| < 1
\end{aligned}$$

Substituting $y = 1 + x \Rightarrow x = y - 1$ into $|x| < 1 \Rightarrow -1 < x < 1$, we have,

$$0 < y - 1 < 2 \Rightarrow 0 < y < 2$$

and thus,

$$\begin{aligned}
\log y &= (y-1) + \frac{(y-1)^2}{2} + \frac{(y-1)^3}{3} - \frac{(y-1)^4}{4} + \ldots \\
&= \sum_{k=0}^{\infty} (-1)^k \frac{(y-1)^{k+1}}{k+1},\ 0 < y < 2
\end{aligned}$$

or in the variable x,

$$\log x = \sum_{k=0}^{\infty} (-1)^k \frac{(x-1)^{k+1}}{k+1},\ 0 < x < 2$$

□

Note 27. *Putting* $x = 2$ *we have,*

$$\log 2 = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots$$

This happens to be a fact but can we really do this since the Taylor series is only true for $0 < x < 2$*?*
The dilemma is solved by applying a convergence test we did not prove, namely, the alternating series test which states,

$$\sum_{n=1}^{\infty} (-1)^{n+1} a_n \text{ converges if and only if } \lim_{n\to\infty} a_n = 0.$$

This is true for the alternating series $\sum_{n=1}^{\infty} (-1)^{n+1} \dfrac{1}{n}$ *since* $\lim_{n\to\infty} \dfrac{1}{n} = 0$*. We could therefore write the Taylor series for* $\log x$ *as,*

$$\log x = \sum_{n=0}^{\infty} (-1)^n \frac{(x-1)^{n+1}}{n+1},\ 0 < x \le 2.$$

Part VIII – Exotic Tastings - continued

Provisioned with sufficient theory of exponential, logarithmic and trigonometric functions and in particular their related Taylor series, we can now sample our final exotic tasting, namely the Euler Zeta function. We find its values at even natural numbers.

We are finished with our Shopping Excursions and ready to tackle the full menu.

Chapter 19

Euler's Zeta Function

In Chapter 17 we developed the formulas for summing finite series of the type $\sum\limits_{n=1}^{m} n^s,\ s \in \mathbb{N}$. These formulas contained the Bernoulli numbers.

We now consider the reciprocal analogues, they will, however, be infinite series. They are called Euler zeta functions and have the form,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},\ s \in \mathbb{R}.$$

By the p-series test, Theorem 77, page 105, they converge only for $s > 1$.

If $s = 1$ then $\zeta(1) = \sum\limits_{n=1}^{\infty} \dfrac{1}{n}$ is the harmonic series which, as we proved in Theorem 72, page 101, diverges. We will develop a formula for $\zeta(2k),\ k \in \mathbb{N}$. It may come as little surprise that this formula also contains the Bernoulli numbers.

We first explore $\sin(nx)$ and $\cos(nx)$ where n is a positive integer so that we can give a rigorous proof that,

$$\frac{\sin \pi x}{\pi x} = \prod_{r=1}^{\infty} \left(1 - \frac{x^2}{r^2}\right)$$

Course: Tasting Plate III

Ingredients

Trigonometrical functions and identities

Euler's Zeta Function

Bernoulli numbers and their theory

Directions

Follow Euler and first prove the classic infinite product formula for $\dfrac{\sin \pi x}{\pi x}$ and then find the formula for $\zeta(2k),\ k \in \mathbb{N}$.

19.1 A Trigonometric Exploration

We use the addition formulas of Theorem 111, page 163, to obtain the double angle formulas by putting A for B.

$$\sin(A+B) = \sin A\cos B + \cos A\sin B \Rightarrow \sin 2A = 2\sin A\cos A$$
$$\cos(A+B) = \cos A\cos B - \sin A\sin B \Rightarrow \cos 2A = \cos^2 A - \sin^2 A$$

Using the Pythagorean Identity from Theorem 108, page 160, namely,

$$\begin{aligned} &\sin^2 A + \cos^2 A = 1 \\ &\Rightarrow \sin^2 A = 1 - \cos^A \\ &\Rightarrow \cos^2 A = 1 - \sin^2 A \end{aligned}$$

we derive,

$$\begin{aligned} \cos 2A &= \cos^2 A - \sin^2 A \\ &= 2\cos^2 A - 1 \\ &= 1 - 2\sin^2 A \end{aligned}$$

Then, again using the addition formulas,

$$\begin{aligned} \sin 3x = \sin(2x+x) &= \sin 2x\cos x + \cos 2x\sin x \\ &= 2\sin x\cos^2 x + (1-2\sin^2 x)\sin x \\ &= 2\sin x(1-\sin^2 x) + \sin x(1-2\sin^2 x) \\ &= 3\sin x - 4\sin^3 x \\ &= P_3(\sin x)\ \textit{say}, \end{aligned} \tag{19.1.1}$$

where $P_3(\sin x)$ means a polynomial in $\sin x$ of degree 3.
Similarly,

$$\begin{aligned} \cos 3x &= \cos(2x+x) \\ &= \cos 2x\cos x - \sin 2x\sin x \\ &= (1-2\sin^2 x)\cos x - 2\sin^2 x\cos x \\ &= \cos x(1-4\sin^2 x) \\ &= \cos x Q_{3-1}(\sin x)\ \textit{say} \end{aligned} \tag{19.1.2}$$

where $Q_{3-1}(\sin x)$ is a polynomial in $\sin x$ of degree $3-1$. (we want the subscript to reflect the starting value of $\cos 3x$.)
Further,

$$\begin{aligned} \sin 5x = \sin(3x+2x) &= \sin 3x\cos 2x + \cos 3x\sin 2x \\ &= (3\sin x - 4\sin^3 x)(1-2\sin^2 x) + (\cos x(1-4\sin^2 x))(2\sin x\cos x) \\ &= (3\sin x - 4\sin^3 x)(1-2\sin^2 x) + (1-4\sin^2 x)(2\sin x\cos^2 x) \\ &= (3\sin x - 4\sin^3 x)(1-2\sin^2 x) + (1-4\sin^2 x)(2\sin x(1-\sin^2 x)) \\ &= P_5(\sin x)\ \textit{say}. \end{aligned}$$

This exploration suggests the following lemma which we prove by induction.

Lemma 146.
Let $n = 2k + 1$ be a positive odd integer. Then,

$$\begin{aligned}\sin(nx) &= P_n(\sin x)\\ \cos(nx) &= \cos x\ Q_{n-1}(\sin x)\end{aligned}$$

where $P_n(\sin x), Q_{n-1}(\sin x)$ are polynomials in the variable $\sin x$ of degree at most n and $n - 1$ respectively.

Proof. We use induction on k where $n = 2k + 1$.
Let $S(k)$ be the statements,

$$\begin{aligned}\sin(nx) &= P_n(\sin x)\\ \cos(nx) &= \cos x\ Q_{n-1}(\sin x)\end{aligned}$$

where $P_n(\sin x)$ and $Q_{n-1}(\sin x)$ are polynomials in $\sin x$ of degree at most $n = 2k + 1$ and $n - 1 = 2k$ respectively.

Basis Step: $S(1)$ is true since by (19.1.1) and (19.1.2) we have $\sin 3x = P_3(\sin x)$ and $\cos 3x = \cos x Q_{3-1}(\sin x)$ (Remember $n = 2k + 1$.)

Supposition step: Assume $S(k - 1)$ is true, that is,

$$\sin(2k - 1) = P_{2k-1}(\sin x) \tag{19.1.3}$$

$$\cos(2k - 1) = \cos x\ Q_{2k-2}(\sin x) \tag{19.1.4}$$

Induction Step: We want to show $S(k)$ is true, that is, $\sin(2k + 1)x$ is a polynomial in $\sin x$ of degree at most $2k + 1$ and $\cos(2k + 1)x$ is $\cos x$ times a polynomial in $\sin x$ of degree at most $2k$. We have[1],

$$\begin{aligned}&\sin(2k + 1)x\\ &= \sin((2k - 1)x + 2x)\\ &= \sin(2k - 1)x \cos 2x + \cos(2k - 1)x \sin 2x\\ &\text{which, using (19.1.3) and (19.1.4),}\\ &= P_{2k-1}(\sin x)(1 - 2\sin^2 x) + \cos x\ Q_{2k-2}(\sin x) 2 \sin x \cos x\\ &= P_{2k-1}(\sin x) + P_{2k+1}(\sin x) + \sin x(1 - \sin^2 x) Q_{2k-1}(\sin x)\\ &= P_{2k-1}(\sin x) + P_{2k+1}(\sin x) + Q_{2k-1}(\sin x) - Q_{2k+1}(\sin x)\end{aligned}$$

which is a polynomial in $\sin x$ of degree at most $2k + 1$ and, similarly,

$$\begin{aligned}\cos(2k + 1)x &= \cos((2k - 1)x + 2x)\\ &= \cos(2k - 1)x \cos 2x - \sin(2k - 1)x \sin 2x\\ &= \cos x\ Q_{2k-2}(\sin x)(1 - 2\sin^2 x) - 2 \sin x \cos x P_{2k-1}(\sin x)\\ &= \cos x\{Q_{2k-2}(\sin x) + Q_{2k}(\sin x) - P_{2k}(\sin x)\}\end{aligned}$$

[1] Note -1 or any integer is "absorbed" into $P_n(\sin x)$ or $Q_{n-1}(\sin x)$.
For example $3P_n(\sin x) = P_n(\sin x)$.

is a polynomial in $\sin x$ of degree at most $2k$ multiplied by $\cos x$. □

19.2 Infinite product for $\sin \pi x / \pi x$

Theorem 147.

$$\frac{\sin \pi x}{\pi x} = \prod_{r=1}^{\infty}\left(1 - \frac{x^2}{r^2}\right)$$

Proof. By Lemma 146 let,

$$\sin nx = P_n(\sin x) = b_0 + b_1 \sin x + b_2 \sin^2 x + \ldots + b_n \sin^n x$$

Putting $x = 0$ gives $0 = b_0$. Differentiating with respect to x gives,

$$n \cos nx = b_1 \cos x + 2b_2 \sin x \cos x + 2b_2 \sin x \cos x + \ldots + nb_n \sin^{n-1} x \cos x$$

Putting $x = 0$ gives $n = b_1$. We then have,

$$\sin nx = n \sin x + b_2 \sin^2 x + \ldots + b_n sin^n x$$

So we have,

$$\begin{aligned} \frac{\sin nx}{n \sin x} &= 1 + a_1 \sin x + a_2 \sin^2 x + \ldots + a_{n-1} \sin^{n-1} x, \ \ \textit{say} \\ &= 1 + a_1 \sin x + a_2 \sin^2 x + \ldots + a_{2k} \sin^{2k} x \qquad (19.2.1) \end{aligned}$$

where we put $n = 2k + 1$ (remember in the statement of Lemma 146 that n is odd), and $\frac{b_n}{n} = a_{2k}, a_i \in \mathbb{Q}$.

Note that for $x = \pm\frac{k\pi}{n}$ that $\sin nx = 0$, so the left side of (19.2.1) vanishes for these values of x. So the $2k$ values of x,

$$x \in \left\{\pm \sin\left(\frac{\pi}{n}\right), \pm \sin\left(\frac{2\pi}{n}\right), \pm \sin\left(\frac{3\pi}{n}\right), \ldots, \pm \sin\left(\frac{k\pi}{n}\right)\right\}$$

are distinct numbers at which $\frac{\sin nx}{n \sin x}$ vanishes or each $x \pm \sin\left(\frac{k\pi}{2}\right)$ is a factor.

Since $\frac{\sin nx}{n \sin x}$ has degree $2k$ and constant term 1 and a polynomial of degree n can have at most n factors, it must factor as,

$$\frac{\sin nx}{n \sin x}$$

$$= \overbrace{\left(1 - \frac{\sin x}{\sin\frac{\pi}{n}}\right)\left(1 - \frac{\sin x}{-\sin\frac{\pi}{n}}\right)}\overbrace{\left(1 - \frac{\sin x}{\sin\frac{2\pi}{n}}\right)\left(1 - \frac{\sin x}{-\sin\frac{2\pi}{n}}\right)}\cdots\overbrace{\left(1 - \frac{\sin x}{\sin\frac{k\pi}{n}}\right)\left(1 - \frac{\sin x}{-\sin\frac{k\pi}{n}}\right)}$$

$$= \prod_{r=1}^{k}\left(1 - \frac{\sin^2 x}{\sin^2\frac{\pi r}{n}}\right)$$

Putting $x = \dfrac{\pi x}{n}$, we have,

$$\frac{\sin \pi x}{n \sin\left(\dfrac{\pi x}{n}\right)} = \prod_{r=1}^{k} \left(1 - \frac{\sin^2 \dfrac{\pi x}{n}}{\sin^2 \dfrac{\pi r}{n}} \right) \tag{19.2.2}$$

We claim that taking the limit as $n = 2k + 1 \to \infty$ gives for the left side of (4.2.2),

$$\lim_{n\to\infty} \frac{\sin \pi x}{n \sin\left(\dfrac{\pi x}{n}\right)} = \frac{\sin \pi x}{\pi x} \tag{19.2.3}$$

To show this we begin via Theorem 112 on page 164 with $\lim\limits_{h\to 0} \dfrac{\sin h}{h} = 1$. Putting $k = \dfrac{1}{h}$ and noting $h \to 0 \Rightarrow k = \dfrac{1}{h} \to \infty$, gives,

$$\lim_{k\to\infty} k \sin \frac{1}{k} = 1.$$

Putting $k = \dfrac{n}{\pi x}$ and noting $k \to \infty \Rightarrow n = 2k + 1 \to \infty$ gives

$$\lim_{n\to\infty} \frac{n}{\pi x} \sin\left(\frac{\pi x}{n}\right) = 1 \tag{19.2.4}$$

So multiplying the left side of (19.2.3) by the left side of (19.2.4) which is just 1, we conclude,

$$\lim_{n\to\infty} \frac{\sin \pi x}{n \sin\left(\dfrac{\pi x}{n}\right)} = \lim_{n\to\infty} \frac{\sin \pi x}{n \sin\left(\dfrac{\pi x}{n}\right)} \times \lim_{n\to\infty} \frac{n}{\pi x} \sin\left(\frac{\pi x}{n}\right) = \frac{\sin \pi x}{\pi x} \tag{19.2.5}$$

Taking the limit as $n = 2k + 1 \to \infty$ gives for the right side of (19.2.2),

$$\lim_{n\to\infty} \prod_{r=1}^{k} \left(1 - \frac{\sin^2\left(\dfrac{\pi x}{n}\right)}{\sin^2\left(\dfrac{\pi r}{n}\right)} \right)$$

$$= \lim_{n\to\infty} \prod_{r=1}^{k} \left(1 - \frac{\sin^2\left(\dfrac{\pi x}{n}\right)}{\left(\dfrac{\pi x}{n}\right)^2} \times \frac{\left(\dfrac{\pi r}{n}\right)^2}{\sin^2\left(\dfrac{\pi r}{n}\right)} \times \frac{\left(\dfrac{\pi x}{n}\right)^2}{\left(\dfrac{\pi r}{n}\right)^2} \right)$$

by inserting $\dfrac{\left(\dfrac{\pi r}{n}\right)^2}{\left(\dfrac{\pi r}{n}\right)^2}$ and $\dfrac{\left(\dfrac{\pi x}{n}\right)^2}{\left(\dfrac{\pi x}{n}\right)^2}$

$$= \prod_{r=1}^{\infty}\left(1 - 1 \cdot 1 \cdot \frac{x^2}{r^2}\right)$$

using $\lim_{h\to 0} \frac{\sin h}{h} = 1$ in the forms $h = \frac{\pi x}{n}$, $h = \frac{\pi r}{n}$ so $\lim_{n\to\infty} \frac{\sin \pi x/n}{\pi x/n} = \lim_{n\to\infty} \frac{\sin \pi r/n}{\pi r/n} = 1$

$$= \prod_{r=1}^{\infty}\left(1 - \frac{x^2}{r^2}\right)$$

We conclude from (19.2.5) and (19.2.6) that,

$$\frac{\sin \pi x}{\pi x} = \prod_{r=1}^{\infty}\left(1 - \frac{x^2}{r^2}\right) \tag{19.2.6}$$

□

We are now prepared to find values of $\zeta(2k)$.

19.3 Hyperbolic Functions

Definition 71. *hyperbolic sine function*
We define the hyperbolic sine function $\sinh x$ *by,*

$$\sinh x = \frac{e^x - e^{-x}}{2}$$

Lemma 148. *For all* $x \in \mathbb{R}$,

$$\frac{\sinh \pi x}{\pi x} = \prod_{n=1}^{\infty}\left(1 + \frac{x^2}{n^2}\right) \tag{19.3.1}$$

Proof. From Equation (15.5.1) of Corollary 121 on page 174,

$$\begin{aligned}
\sin x &= \frac{e^{ix} - e^{-ix}}{2i} \\
\Rightarrow -i \sin ix &= -i \frac{e^{i^2 x} - e^{-i^2 x}}{2i} \quad \text{putting } x = ix \text{ and multiplying by } -i \\
&= \frac{e^x - e^{-x}}{2} \\
\Rightarrow -i \sin ix &= \sinh x
\end{aligned} \tag{19.3.2}$$

By putting $x = ix$ in (19.2.6) we have,

$$\begin{aligned}
\frac{\sin \pi x}{\pi x} &= \prod_{r=1}^{\infty}\left(1 - \frac{x^2}{r^2}\right) \text{ gives,} \\
\frac{\sin i\pi x}{i\pi x} &= \prod_{r=1}^{\infty}\left(1 - \frac{(ix)^2}{r^2}\right) \\
\frac{\sin i\pi x}{i\pi x} &= \prod_{r=1}^{\infty}\left(1 + \frac{x^2}{r^2}\right)
\end{aligned} \tag{19.3.3}$$

Therefore using (19.3.2),

$$\begin{aligned}\frac{\sinh \pi x}{\pi x} &= -\frac{i \sin i\pi x}{\pi x} \\ &= \frac{\sin i\pi x}{i\pi x} \\ &= \prod_{r=1}^{\infty}\left(1+\frac{x^2}{r^2}\right) \text{ by (19.3.3)} \qquad (19.3.4)\end{aligned}$$

□

19.4 Formula for $\zeta(2k)$

Theorem 149.

$$\zeta(2k) = (-1)^{k+1}\pi^{2k}\frac{2^{2k-1}}{(2k)!}B_{2k}$$

where B_n is the n^{th} Bernoulli number.

Proof.
We have by taking logarithms of both sides[2] of (19.3.4) multiplied by πx that,

$$\begin{aligned}\sinh \pi x &= \pi x \prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right) \\ \Rightarrow \log\sinh \pi x &= \log\left\{\pi x \prod_{r=1}^{\infty}\left(1+\frac{x^2}{r^2}\right)\right\} \qquad (19.4.1)\end{aligned}$$

The left side of (19.4.1) becomes,

$$\begin{aligned}\log\sinh \pi x &= \log\left[\frac{e^{\pi x}-e^{-\pi x}}{2}\right] \\ &= \log\left[\frac{e^{\pi x}}{2}(1-e^{-2\pi x})\right] \\ &= \log e^{\pi x} + \log(1-e^{-2\pi x}) - \log 2 \\ &= \pi x + \log(1-e^{-2\pi x}) - \log 2 \qquad (19.4.2)\end{aligned}$$

The right side of (19.4.1) is dealt with by again noting Note 25 on page 213 and substituting $x = e^{-2\pi x}$ in the Taylor series expansion[3] of $\log(1+x)$, namely,

$$\log(1+x) = \sum_{k=0}^{\infty}\frac{(-1)^k x^{k+1}}{k+1} = \sum_{k=1}^{\infty}\frac{x^k}{k}, \ |x| < 1.$$

[2] Refer to Note 25, page 213 for the logarithm of an infinite product

[3] Refer to Section 18.11, equation (18.11.1) on page 216.

We have for the right side of (19.4.1),

$$\log\left\{\pi x\prod_{r=1}^{\infty}\left(1+\frac{x^2}{r^2}\right)\right\} = \log\pi+\log x+\sum_{n=1}^{\infty}\log\left(1+\frac{x^2}{n^2}\right)$$

$$= \log\pi+\log x+\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^{2k}}{kn^{2k}} \qquad (19.4.3)$$

Inserting (19.4.2) and (19.4.3) into (19.4.1), noting $\zeta(2k) = \sum_1^\infty \frac{1}{n^{2k}}$ and assuming we can interchange the order of summation, we now have,

$$\pi x+\log(1-e^{-2\pi x})-\log 2 = \log\pi+\log x+\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^{2k}}{kn^{2k}}$$

$$= \log\pi+\log x+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^{2k}}{k}\sum_{n=1}^{\infty}\frac{1}{n^{2k}}$$

$$= \log\pi+\log x+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^{2k}}{k}\zeta(2k)$$

Differentiating with respect to x we have,

$$\pi+\frac{2\pi e^{-2\pi x}}{1-e^{-2\pi x}} = \frac{1}{x}+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{2k}{k}x^{2k-1}\zeta(2k)$$

Multiplying by x,

$$\pi x+\frac{2\pi x e^{-2\pi x}}{1-e^{-2\pi x}} = 1+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{2k}{k}x^{2k}\zeta(2k)$$

Putting $\frac{x}{2}$ for x we have,

$$\frac{\pi x}{2}+\frac{2\pi\frac{x}{2}e^{-2\pi\frac{x}{2}}}{1-e^{-2\pi\frac{x}{2}}} = 1+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{2k}{k}\frac{x^{2k}}{2^{2k}}\zeta(2k)$$

$$\frac{\pi x}{2}+\left(\frac{\pi x e^{-\pi x}}{1-e^{-\pi x}}\right) = 1+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{2k}{k}\frac{x^{2k}}{2^{2k}}\zeta(2k)$$

Multiplying numerator and denominator of the second term on the left side by $e^{\pi x}$ we have,

$$\frac{\pi x}{2}+\left(\frac{\pi x e^{-\pi x}}{1-e^{-\pi x}}\times\frac{e^{\pi x}}{e^{\pi x}}\right) = 1+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{2k}{k}\frac{x^{2k}}{2^{2k}}\zeta(2k)$$

$$\frac{\pi x}{2}+\frac{\pi x}{e^{\pi x}-1} = 1+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^{2k}}{2^{2k-1}}\zeta(2k)$$

Recall, the Bernoulli numbers are defined by,

$$\frac{x}{e^x-1} = B_0+\frac{B_1}{1!}x+\frac{B_2}{2!}x^2+\frac{B_3}{3!}x^3\ldots = \sum_{k=0}^{\infty}\frac{B_k}{k!}x^k$$

So here with πx replacing x, we have,

$$\sum_{k=0}^{\infty} \frac{B_k}{k!}(\pi x)^k + \frac{\pi x}{2} = 1 + \sum_{k=0}^{\infty}(-1)^{k+1}\frac{x^{2k}}{2^{2k-1}}\zeta(2k)$$

Comparing powers of x^{2k} gives,

$$\frac{B_{2k}}{(2k)!}\pi^{2k} = (-1)^{k+1}\frac{\zeta(2k)}{2^{2k-1}}$$
$$\Rightarrow \zeta(2k) = (-1)^{k+1}\pi^{2k}\frac{2^{2k-1}}{(2k)!}B_{2k}$$

□

Example 98. *Using the values of B_{2k} we found via Theorem 135 on page 201,*

$$\begin{aligned} k &= 1, & \zeta(2) &= \sum_{n=1}^{\infty}\frac{1}{n^2} = (-1)^2\pi^2\frac{2}{2!}B_2 = \frac{\pi^2}{6} \\ k &= 2, & \zeta(4) &= \sum_{n=1}^{\infty}\frac{1}{n^4} = (-1)^3\pi^4\frac{2^3}{4!}B_4 = \frac{\pi^4}{90} \\ k &= 3, & \zeta(6) &= \sum_{n=1}^{\infty}\frac{1}{n^6} = \frac{\pi^6}{945} \end{aligned}$$

Note 28.
We defined above the hyperbolic sine function $\sinh x = \dfrac{e^x - e^{-x}}{2}$. *There is a corresponding hyperbolic cosine function* $\cosh x = \dfrac{e^x + e^{-x}}{2}$. *You can complete the algebra and show* $\cosh^2 x - \sinh^2 x = 1$. *These functions which parallel the trigonometric sine and cosine functions for which* $\cos^2 x + \sin^2 x = 1$, *are called hyperbolic functions since they are very useful in the mathematics of hyperbolas with equations* $\dfrac{x^2}{a^2} - \dfrac{y^2}{b^2} = 1$ *and graphs like this:*

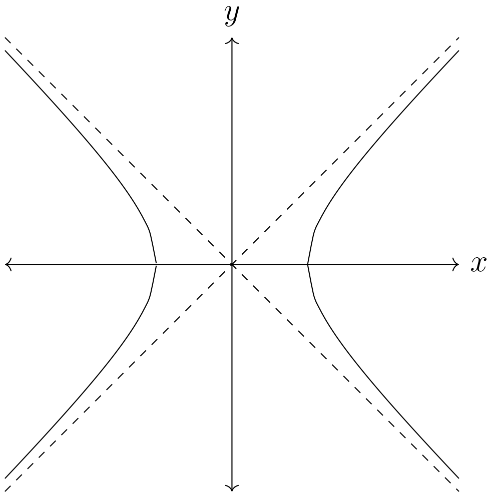


Figure 37

just as the sine and cosine functions are very useful in the mathematics of ellipses with equations $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$ *and graphs like this,*

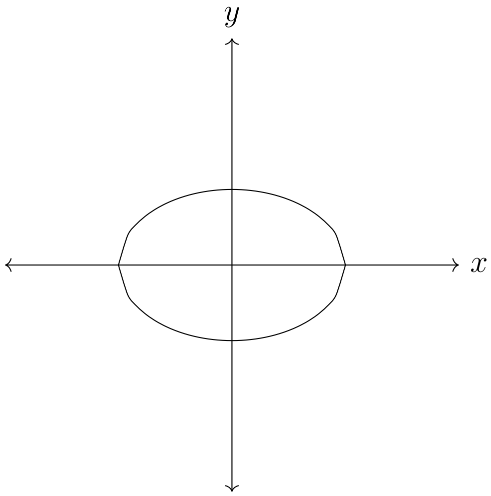


Figure 38

Part VIII

A Prime Banquet

The Entrée Courses

Euclid to Gauss to Dirichlet

Primes have always fascinated mathematicians. They are the building blocks of the integers as evidenced by the fundamental theorem of arithmetic, yet they seem out of control, random and uncountable. In Chapter 28 we shall study the Riemann Hypothesis which many mathematicans hope should provide the long-sought control.

In ancient times, Euclid proved there are an infinity of primes.

In 1837, Dirichlet proved one of the most remarkable theorems of analytic number theory, namely there are an infinite number of primes in any arithmetic progression given by $a + bn, gcd(a, b) = 1, a, b, n \in \mathbb{N}$. For example,

$$\begin{aligned}
\{p|p = 4n + 1\} &= \{5, 13, 17, \ldots, 101, 109, 113, \ldots\}\\
\{p|p = 6n + 5\} &= \{5, 11, 17, 23, \ldots, 107, \ldots\}\\
\{p|p = 11n + 7\} &= \{7, 29, 73, \ldots\}\\
\{p|p = 72n + 37\} &= \{37, 109, 181, \ldots\}
\end{aligned}$$

The proofs that there are an infinite number of primes of the forms $4n + 1$ and $4n + 3$ are particular examples of this general proof. We begin with them.

It is easy to prove there are an infinite number of primes of the form $4n + 3$. This proof, also due to Euclid, uses the same method as that for proving the infinitude of primes.

The proof that there are an infinite number of primes of the form $4n + 1$ is more difficult. It is instructive to prove it in several different ways. Each requires the development of a suitable framework. The last of these proofs that we consider is a special case of Dirichlet's theorem in the $a = 1, b = 4$ or $4n + 1$ case.

As a bonus, we will also find another proof of the $4n + 3$ case.

Chapter 20

All Primes and $4n + 3$ Primes

Course: *Entrée I*
Ingredients
Primes
Arithmetic progressions
Congruences
Directions
Prove there are an infinite number of primes.
Prove there are an infinite number of primes of the form $4n + 3$

20.1 General observations

Note 29.
Before we begin this series of proofs, let us make a general observation about numbers of the forms $4n + 1$ *and* $4n + 3$. *All odd numbers, and therefore primes other than 2, are of the form* $4n + 1$ *or* $4n + 3$ *which for the odd primes we can also state as each prime* p *satisfies either* $p \equiv 1 (\text{mod } 4)$ *or* $p \equiv 3 (\text{mod } 4)$.

- *If we multiply two primes of the form* $4n + 1$ *we get a number of the form* $4n + 1$ *since,*
$$(4k + 1)(4j + 1) = 4(4kj + j + k) + 1 \equiv 1 (\text{mod } 4)$$

- *If we multiply a* $4n + 1$ *prime by a* $4k + 3$ *prime we get a number of the form* $4k + 3$ *since,*
$$(4k + 1)(4j + 3) = 4(4kj + j + k) + 3 \equiv 3 (\text{mod } 4)$$

- *If we multiply two primes of the form* $4n + 3$ *we get a number of the form* $4n + 1$ *since,*
$$(4k + 3)(4j + 3) = 4(4kj + j + k + 2) + 1 \equiv 1 (\text{mod } 4)$$

It therefore follows that a number of the form $4n + 1$ must factor as an even or zero number of primes of the form $4k + 3$ and any number of primes of the form $4n + 1$.

Whereas a number of the form $4n + 3$ must factor as an odd number (at least one) of primes of the form $4k + 3$ and any number of primes of the form $4n + 1$.

20.2 Infinitude of primes

Definition 72. *prime number*
A prime is any natural number other than 1 which is divisible only by 1 and itself.

The proof that there are an infinite number of primes is ancient! The list begins $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Theorem 150. *(Euclid)*
There are an infinite number of primes.

Proof.
Suppose not and that $p_1, p_2, \ldots, p_n$ are all the primes.
Consider the number $N = p_1 p_2 \cdots p_n + 1$.
By the Fundamental Theorem of Arithmetic, Theorem 19 on page 43 we can factor N as a unique product of primes, say $N = q_1 q_2 \cdots q_s$, where we may have $s = 1$ making N itself a prime.
Now no q_i is equal to any of the primes $p_1, p_2, \ldots, p_n$ since none of these divide N in each case the division leaving a remainder of 1, whereas all the q_i do divide N. Thus there are prime/s different to $p_1, p_2, \ldots, p_n$ and the supposition there are a finite number of primes is incorrect. □

20.3 Primes in an arithmetic progression

Definition 73. *arithmetic progression*
An arithmetic progression is a sequence of numbers generated by adding the same number (the common difference d) to generate the next number. If a is the first term, the progression will be,

$$a, (a + d), (a + 2d), \ldots$$

where the n^{th} term will be $a + (n - 1)d$.

Example 99. *For example, if we begin with 7 and the common difference is 5 then we generate,*

$$7, 7 + 5, 7 + 5 + 5, 7 + 5 + 5 + 5, \ldots = 7, 12, 17, 22, \ldots$$

Dirichlet's Theorem is that any arithmetic progression generates an infinite number of primes if $gcd(a, d) = 1$. We begin with $a = 3, d = 4$ or the $4n + 3$ numbers.

20.4 Primes of the form $4n + 3$.

We first need a more extensive introduction ot the theory of congruences.

20.4.1 Congruences

Definition 74. *congruence*
Let m be a positive integer. If m divides the difference $a - b$ of two integers a, b, we say "a is congruent to b modulo m," and we write,

$$m|a - b \Leftrightarrow a \equiv b(\text{mod } m)$$

Note that,

$$m|a - b \Rightarrow a - b = mk \Rightarrow a = b + mk, k \in \mathbb{Z}$$

so that,

$$a \equiv b(\text{mod } m) \Leftrightarrow a = b + mk, k \in \mathbb{Z}$$

We say a and b are incongruent modulo m if $a \not\equiv b(\text{mod } m)$

.

Example 100.

$$\begin{aligned}23 = 5 \times 4 + 3 &\Leftrightarrow 23 \equiv 3(\text{mod } 5)\\ 23 = 5 \times 3 + 8 &\Leftrightarrow 23 \equiv 8(\text{mod } 5)\\ 23 = 5 \times 2 + 13 &\Leftrightarrow 23 \equiv 13(\text{mod } 5)\\ 23 = 5 \times -3 + 38 &\Leftrightarrow 23 \equiv 38(\text{mod } 5) \qquad \diamond\end{aligned}$$

Definition 75. *residue*
If $a \equiv b(\text{mod } m)$, b is called a residue of a modulo m. It is any possible remainder when a is divided by m.

Example 101. *In the previous example the residues of* 23 *modulo* 5 *are* 3, 8, 13 *and* 38.

Note 30. *In this example we call* 3 *the least non-negative remainder when* 23 *is divided by* 5. *Unless otherwise specified, given $a \equiv b(\text{ mod } m)$ we will always assume b is the least non-negative residue. Thus, for example, the solution to* $37(\text{mod } 11)$ *will unambiguously be* 4 *unless we clearly state otherwise.*

Definition 76. *complete residue system*
The set of integers $\{0, 1, 2, 3, \ldots, m - 1\}$ is called a complete residue system modulo m since when any integer n is divided by m the least non-negative solutions to $n(\text{mod } m)$ are $1, 2, 3, \ldots, m - 1$.

Example 102. *If any integer n is divided by* 7 *the least non-negative remainders are* 0, 1, 2, 3, 4, 5 *and* 6. $\diamond$

Theorem 151. *(Congruences)*
Let m be a positive integer and a, b, c be integers.

(i) $a \equiv b(\text{mod } m) \Rightarrow b \equiv a(\text{mod } m)$

(ii) $a \equiv b(\text{mod } m), b \equiv c(\text{mod } m) \Rightarrow a \equiv c(\text{mod } m)$

(iii) $a \equiv b(\text{mod } m), c \equiv d(\text{mod } m) \Rightarrow a \pm c \equiv b \pm d(\text{mod } m)$

(iv) $a \equiv b(\text{mod } m) \Rightarrow ac \equiv bc(\text{mod } m)$ *for all* $c \in \mathbb{Z}$

(v) For all $c \in \mathbb{Z}$ *where* $c|a, c|b$ *we have* $a \equiv b(\text{mod } m)$ *if and only if* $\frac{a}{c} \equiv \frac{b}{c}(\text{mod } m)$

(vi) $ca \equiv cb(\text{mod } m) \Rightarrow a \equiv b(\text{mod } m)$ *if* $gcd(a, b) = 1$.

(vii) $a \equiv b(\text{mod } m), c \equiv d(\text{mod } m) \Rightarrow ac \equiv bd(\text{mod } m)$

(viii) $a \equiv b(\text{mod } m) \Rightarrow a^n \equiv b^n(\text{mod } m)$ *for all* $n \in \mathbb{N}$.

(ix) If $d|m, d > 0$, *and* $a \equiv b(\text{mod } m)$ *then* $a \equiv b(\text{mod } d)$

Proof.
The proofs are mostly left to the reader. They all proceed from the definition,

$$a \equiv b(\text{mod } m) \Rightarrow a = b + mk, k \in \mathbb{Z}.$$

For example, the proof of (iii), which we will use later, is

$$\begin{aligned} & a \equiv b(\text{mod } m), c \equiv d(\text{mod } m) \\ & \Leftrightarrow a - b = mk, c - d = mj \\ & \Rightarrow (a \pm c) \mp (b \pm d) = m(k \pm j) = ml, l \in \mathbb{Z} \\ & \Rightarrow a \pm c \equiv b \pm d(\text{mod } m) \end{aligned}$$

We will also use (vii) $a \equiv b(\text{mod } m), c \equiv d(\text{mod } m) \Rightarrow ac \equiv bd(\text{mod } m)$ whose proof is as follows.

$$\begin{aligned} & a \equiv b(\text{mod } m) \Rightarrow a = b + km \\ & c \equiv d(\text{mod } m) \Rightarrow c = d + jm \\ & \Rightarrow ac = bd + m(bj + dk + kjm) \\ & \Rightarrow ac \equiv cd(\text{mod } m) \end{aligned}$$

□

20.5 Proof of the $4n + 3$ case

We can now prove the case $p = 4n + 3, n \in \mathbb{N}$.

Theorem 152.
There are an infinite number of primes p of the form $p = 4n+3, n \in \mathbb{N}$ or $p \equiv 3(\mod 4)$.

Proof. Suppose $3, 7, 11, \ldots, p_n$ are all the primes of the form $p = 4n + 3, n \in \mathbb{N}$. Consider,

$$M = (4 \cdot 3 \cdot 7 \cdot 11 \cdots p_n) + 3$$

Then $M \equiv 3(\text{mod } 4)$ and none of the finite number of primes of the form $4n + 3$ can divide M since each would leave a remainder of 3.
Write $M = q_1 q_2 \cdots q_s$ as the product of primes. At least[1] one of the primes q_i must be of the form $4n + 3$ since the product of two primes of the form $p = 4n + 1$ is again of the form $4n + 1$.
But no q_i is among the set $3, 7, 11, \ldots, p_n$ since if M is divided by any of these numbers there is a remainder of 3. So there exists another prime of the form $4n + 3$ and the supposition is incorrect and there are an infinite number of primes of the form $4n + 3$. □

[1] See Note 29 on page 231

Chapter 21

Primes of the form $4n + 1$: Method 1

There are an infinite number of primes p of the form $4n + 1$ or $p \equiv 1(\text{mod } 4)$.
We will prove this theorem using five different methods. Each method allows us to explore a different branch of number theory.

The first method of proof uses Fermat's Little Theorem. The framework we need is Euclid's totient function $\phi(m)$ and a little more of the theory of congruences.

Course: *Entrée II*
Ingredients
Euler's totient function
Linear congruences
Directions
Solve linear congruences
Prove Euler's Theorem
Prove Fermat's Little Theorem
Prove there are an infinite number of primes of the form $4n + 1$

21.1 Euler's Totient Function

Definition 77. *relatively prime*
Two natural numbers a, b are relatively prime if gcd$(a, b) = 1$.

Example 103. *6 and 7 are relatively prime since gcd$(6, 7) = 1$.*
6 and 1 are relatively prime since gcd$(6, 1) = 1$
3 and 6 and not relatively prime since gcd$(3, 6) = 3$. ◇

Definition 78. *Euler's totient function*
The function $\phi(m)$ denotes the number of positive integers less than or equal to m that are relatively prime to m. This function $\phi(m)$ is called the Euler totient function. We define $\phi(1) = 1$.

Example 104.
$\phi(10) = 4$ *since only the numbers* $1, 9, 7, 3$ *less than* 10 *are relatively prime to* 10.
$\phi(11) = 10$ *since all natural numbers less* 11 *are relatively prime to it.* $\diamond$

Note that in general for all primes p that $\phi(p) = p - 1$ since $gcd(p, n) = 1$ for all natural numbers n less than p or for $\{1, 2, 3, 4, \ldots, p-1\}$.

21.2 Congruence Lemmas

Definition 79. *linear equation*
A linear equation in the variables x, y *is of the form* $ax + by = c$.

Definition 80. *linear congruence*
A linear congruence is of the form $x \equiv y(\text{mod } n)$ *which is equivalent to the linear equation* $x = y + km$.

Let us now investigate the integer solutions of the linear congruence $ax \equiv b(\text{mod } n)$. We are building up the theory of congruences we began with the Chinese Remainder Theorem, Theorem 81 on page 119.

Theorem 153. *(Solution of Linear Congruences)*
The linear congruence,

$$ax \equiv b(\text{mod } n), \tag{21.2.1}$$

a) has solutions if and only if $gcd(a, n)$ *divides* b.

b) if $gcd(a, n) = 1$, *the congruence has a unique solution.*

Proof. a) Consider $ax \equiv b(\text{mod } n)$. Suppose there is a solution x_0 such that we have $ax_0 \equiv b(\text{ mod } n)$. There there exists a y_0 such that $ax_0 = b+ny_0$ by definition of a congruence.
Thus x_0, y_0 is a solution of the linear equation $ax - ny = b$. But by the Theorem 15(b), page 41, $ax \equiv b(\text{mod } n) \Leftrightarrow ax - ny = b$ has solutions if and only if $gcd(a, n)|b$.

b) Suppose $gcd(a, n) = 1$. From Theorem 78, page 110, if $x = x_0$ and $y = y_0$ is a particular solution of $ax \equiv (\text{mod } n) \Leftrightarrow ax - ny = b$, the general solution for all $k \in \mathbb{Z}$ is,

$$x = x_0 + nk, \;\; y = y_0 + ak.$$

But for all $k \in \mathbb{Z}$, $x_0 + nk \equiv x_0(\text{mod } n)$.
Hence $x \equiv x_0(\text{mod } n)$ is the only solution of $ax \equiv b(\text{mod } n)$.

□

Let us now prove the theorem concerning primes of the form $4n + 1$. We first need a lemma and two famous classic theorems of Euler and Fermat.

Lemma 154.
Let a, m be any positive integers such that $gcd(a, m) = 1$.
Let $\{x_1, x_2, \dots, x_n\}$ be the set of all the positive integers less than m with $gcd(x_i, m) = 1$ for $1 \leq i \leq n$.
Then $ax_i \equiv x_j (\bmod m)$ for some $i \neq j, 1 \leq i, j \leq n$. In other words, the set $\{ax_1, ax_2, \dots, ax_n\}$ has the same residues modulo m as does $\{x_1, x_2, \dots, x_n\}$.
By definition the number of elements in both sets is $\phi(m)$.

Proof. Let a, m be any positive integers such that $gcd(a, m) = 1$.
Let $\{x_1, x_2, \dots, x_n\}$ be the set of all the positive integers less than m with $gcd(x_i, m) = 1$ for $1 \leq i \leq n$.
Suppose $\{ax_1, ax_2, \dots, ax_n\}$ has $\{y_1, y_2, \dots y_n\}$ as residues modulo n.
We need to show $y_i \neq y_j$ for all $i \neq j$ so there are n distinct values of y_j. We then need to show any $y_j = x_i$ for some $i : 1 \leq i \leq n$ so that $\{y_1, y_2, \dots, y_n\} = \{x_1, x_2, \dots, x_n\}$.
Beginning with $\{ax_1, ax_2, \dots, ax_n\}$ having $\{y_1, y_2, \dots y_n\}$ as residues modulo n we have,

$$\begin{aligned} ax_i &\equiv y_j (\text{mod } m) \text{ for some} j : 1 \leq j \leq n \\ \Leftrightarrow ax_i - y_j &= km \text{ for some} k \in \mathbb{Z} \end{aligned}$$

We claim $gcd(y_j, m) = 1$.
For suppose $gcd(y_j, m) = d, d > 1$, making $y_j = cd, m = ld$. Then,

$$ax_i + y_j = km \Rightarrow ax_i - cd = kld \Rightarrow d(c + lk) = ax_i$$

So either $d | a$ making $gcd(a, m) = d$ or $d | x_i$ making $gcd(x_i, m) = d$, which both contradict the assumptions unless $d = 1$. Hence, $gcd(y_j, m) = 1$.
But if $gcd(y_j, m) = 1$ and $gcd(x_i, m) = 1$ then $y_j = x_i$ for some i.
We cannot have $y_j = y_i$ since that would mean

$$\begin{aligned} ax_i &\equiv ax_j (\text{mod } m) \\ \Rightarrow a(x_i - x_j) &\equiv 0 (\text{mod } m) \\ \Rightarrow m &\mid a(x_i - x_j) \end{aligned}$$

But $m \nmid a$ and we cannot have $m \mid (x_i - x_j)$ since both x_i and x_j are less than m. We conclude the y_j are all distinct and therefore,

$$\{y_1, y_2, \dots, y_n\} = \{x_1, x_2, \dots, x_n\}$$

and,

$$ax_i \equiv x_j (\text{mod } m)$$

for some $i \neq j, 1 \leq i, j \leq n$. □

Example 105. *Take $m = 12, a = 5$ and note $gcd(12,5) = 1$.*
First the set $\{1,5,7,11\}$ are the positive integers less than and relatively prime to 12. Consider the same set with each element multiplied by 5, that is, $\{5,25,35,55\}$. Then,

$$\begin{aligned} 5 &\equiv 5(\text{mod } 12) \\ 25 &\equiv 1(\text{mod } 12) \\ 35 &\equiv 11(\text{mod } 12) \\ 55 &\equiv 7(\text{mod } 12) \end{aligned}$$

shows the two sets have the same residues $1,5,7,11$ modulo 12. ◇

21.3 Euler's and Fermat's Theorems

Recall $\phi(n)$ is the number of positive integers less than n that are relatively prime to n and if p is a prime then $\phi(p) = p - 1$.

Theorem 155. *(Euler's Theorem)*
If $gcd(a,m) = 1$ then $a^{\phi(m)} \equiv 1(\text{mod } m)$.

Proof.
Let $a, m \in \mathbb{N}$ with $gcd(a,m) = 1$.
Let $r_1, r_2, \ldots, r_s$ be all the positive integers less than m that are relatively prime to n, making Euler's $\phi(m) = s$. By Lemma 154, page 238 and Theorem 151(vii), page 234,

$$\begin{aligned} & ar_1 ar_2 \cdots ar_s \equiv r_1 r_2 \cdots r_s (\text{mod } m) \\ & \Rightarrow a^s r_1 r_2 \cdots r_s \equiv r_1 r_2 \cdots r_s (\text{mod } m) \\ & \Leftrightarrow a^s \equiv 1(\text{mod } m) \end{aligned}$$

Or, $a^{\phi(m)} \equiv 1(\text{mod } m)$. □

Theorem 156. *(Fermat's Little Theorem)*
If p is a prime then for all $a \in \mathbb{N}$,

$$a^p \equiv a(\text{mod } p) \Leftrightarrow a^{p-1} \equiv 1(\text{mod } p)$$

Proof.
Let p be a prime and $a \in \mathbb{N}$. There are two cases.
Case 1: If $p|a \Rightarrow a = kp$ then $a(\text{mod } p) = kp(\text{mod } p) = 0$ and $a^p = k^p p^p \equiv 0(\text{mod } p)$ so $a^p \equiv a(\text{mod } p)$, both being 0.
Case 2: If $p \nmid a$ then $gcd(a,p) = 1$ so by Euler's Theorem 155,

$$a^{\phi(p)} = a^{p-1} \equiv 1(\text{mod } p)$$

Then, $a^{p-1} \equiv 1(\text{mod } p) \Rightarrow a^p \equiv a(\text{mod } p)$.

□

21.4 Method 1 Proof

Theorem 157.
There are an infinite number of primes p of the form $4n+1$ or $p \equiv 1 (\text{mod } 4)$.

Proof.
Let N be a positive integer. Let,

$$\begin{aligned} M &= [N(N-1)(N-2)\cdots 2\cdot 1]^2 + 1 \\ &= [N!]^2 + 1 \end{aligned}$$

Then N is odd.
Let p be a prime number greater than N such that $p|M$. We note p must exist since either M has no factors and $p = M$ or M has prime factors none of which can be the numbers $1, 2, \ldots, N$ since each of them leaves a remainder of 1 when it divides N. Then,

$$\begin{aligned} & M \equiv 0 (\text{mod } p) \\ & \Rightarrow [N!]^2 + 1 \equiv 0 (\text{mod } p) \\ & \Rightarrow [N!]^2 \equiv -1 (\text{mod } p) \\ & \Rightarrow \left([N!]^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (\text{mod } p) \\ & \Rightarrow [N!]^{p-1} \equiv (-1)^{\frac{p-1}{2}} (\text{mod } p) \qquad (21.4.1) \end{aligned}$$

Substitute $a = N!$ in Fermat's Little Theorem 156, namely $a^{p-1} \equiv 1 (\text{mod } m)$, to give,

$$\begin{aligned} & [N!]^{p-1} \equiv 1 (\text{mod } p) \qquad (21.4.2) \\ & \Rightarrow 1 (\text{mod } p) \equiv (-1)^{\frac{p-1}{2}} (\text{mod } p), \text{ by (21.4.1) and (21.4.2)} \\ & \Rightarrow 1 = (-1)^{\frac{p-1}{2}} \\ & \Rightarrow \frac{p-1}{2} = 2k, k \in \mathbb{Z} - \{0\} \\ & \Rightarrow p = 4k + 1 \end{aligned}$$

Since $p > N$ and we can have take N as large as we like, then we can find a
$p = 4k+1$ as large as we like. So there are an infinite number of primes p of the form $p \equiv 1 (\text{mod } 4)$. □

Chapter 22

Primes of the form $4n + 1$: Method 2

The second method again uses Fermat's Little Theorem 156 and is elegantly brief.

Course: *Entrée III*
Ingredients
Congruences
Fermat's Little Theorem
Directions
Investigate prime factors of two squares
Prove there are an infinite number of primes of the form $4n + 1$ by method 2.

22.1 The Key Lemma

Lemma 158.
The sum of two squares cannot have a prime factor p of the form $p = 4n + 3$ or $p \equiv 3 (\text{mod } 4)$.

Proof. Suppose a prime p of the form $p = 4n+3$ divides the sum a^2+b^2 of two squares of two integers a, b.
By Fermat's Little Theorem 156 since p is a prime,

$$a^{p-1} \equiv 1 (\text{mod } p) \textit{ and } b^{p-1} \equiv 1 (\text{mod } p)$$

Hence by Theorem 151(iii) on page 234,

$$a^{p-1} + b^{p-1} \equiv 2 (\text{mod } p).$$

On the other hand, if $p = 4n + 3$ then since $x^n + y^n$ factors if n is odd,

$$\begin{aligned} a^{p-1} + b^{p-1} &= a^{4k+2} + b^{4k+2} \\ &= (a^2)^{2k+1} + (b^2)^{2k+1} \\ &= (a^2 + b^2)(a^{2k-1} - \ldots + b^{2k-1}) \\ &\equiv 0 (\text{mod } p) \text{ since we supposed } \ p | a^2 + b^2 \end{aligned}$$

This is a contradiction to $a^{p-1} + b^{p-1} \equiv 2(\text{mod } p)$ so no prime of the form $p = 4n+3$ divides a^2+b^2. □

22.2 Method 2: Proof

Theorem 159. *There are an infinite number of primes p of the form $p = 4n+1$ or $p \equiv 1(\text{mod } 4)$.*

Proof. Suppose there are only the finite number $\{5, 13, 17, \ldots, p_n\}$.
Consider,

$$N = (2 \cdot 5 \cdot 13 \cdots p_n)^2 + 1 = A^2 + 1^2, \text{ where } gcd(A, 1) = 1$$

By Lemma 158, no prime of the form $p \equiv 3(\text{mod } 4)$ divides N since N is the sum of two squares.
Therefore the prime factors of N are all of the form $p = 4n+1$ and none of them can be in the finite set $\{5, 13, 17, \ldots, p_n\}$ since each of these numbers leaves a remainder of 1 when it divides N so is not a factor of N. This is a contradiction so there are an infinite number of primes p of the form $p = 4n+1$ or $p \equiv 1(\text{mod } 4)$. □

Chapter 23

Primes of the form $4n+1$: Method 3

The third method uses the theory of quadratic residues, another classic of number theory, largely due to Gauss.

Course: *Entrée IV*
Ingredients
Congruences
Quadratic residues
Directions
Prove a theorem about the number of quadratic residues and non-residues.
Learn how to find quadratic residues and non-residues.
Prove Wilson's Theorem.
Prove Euler's Criterion and a Corollary.
Prove there are an infinite number of primes of the form $4n+1$ by method 3.

23.1 Quadratic Residues

Definition 81. *quadratic residue*
Let m be an integer greater than 1 and $a \in \mathbb{Z}$. Suppose $gcd(a,m) = 1$. Then a is called a quadratic residue[1] *of m if the equation $x^2 \equiv a(\text{mod } m)$ has a solution. If there is no solution, then a is called a quadratic non-residue of m.*

Example 106. *$gcd(5,11) = 1$ and $4^2 \equiv 5(\text{mod } 11)$ so 5 is a quadratic residue of* 11.

Theorem 160.
Let p be an odd prime. Then there are exactly $\dfrac{p-1}{2}$ incongruent[2] *quadratic residues and exactly $\dfrac{p-1}{2}$ incongruent quadratic non-residues modulo p.*

[1] $x^2 \equiv a(\text{mod } m)$ means a is a residue and $x^2 = a + km$ means we are dealing with a quadratic equation, hence the name "quadratic residues."

[2] Incongruent means if a, b are quadratic residues of p then $a \not\equiv b(\text{mod } p)$.

Proof. Let p be an odd prime. Then the numbers $a = 1, 2, \ldots, \frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-1$ all satisfy $gcd(a, p) = 1$ since a prime cannot divide any positive integer less than itself. Now the numbers,

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

are all incongruent since for any two of these squares we can call r, s if $r^2 \equiv s^2 (\bmod\ p)$ then,

$$r \equiv s (\text{mod } p) \text{ or } r \equiv -s (\text{mod } p) \Rightarrow p | r - s \text{ or } p | r + s.$$

But since both r and s are less than $\frac{p-1}{2}$, neither their sum nor their difference can be divisible by p. Hence for each $x \in \left\{1, 2, \ldots, \left(\frac{p-1}{2}\right)\right\}$ we have by $x^2 \equiv a (\text{mod } p)$, where each a is different, a set of $\frac{p-1}{2}$ quadratic residues.
Also since, $(p-r)^2 = p(p-2r) + r^2$, we have,

$$r^2 \equiv (p-r)^2 (\text{mod } p).$$

Accordingly the numbers,

$$\left(\frac{p+1}{2}\right)^2, \left(\frac{p+3}{2}\right)^2, \ldots, (p-2)^2, (p-1)^2$$

produce the same quadratic residues as do,

$$1^2, 2^2, \ldots, \left(\frac{p-3}{2}\right)^2, \left(\frac{p-1}{2}\right)^2$$

and there can be no more and no less. Hence there are exactly $\frac{p-1}{2}$ incongruent quadratic residues and therefore exactly $\frac{p-1}{2}$ incongruent quadratic non-residues modulo p. □

23.2 Finding Quadratic Residues and Non-residues

The proof of the above theorem shows us how to find the quadratic residues of p. We simply square,

$$x = 1, 2, 3, \ldots, \frac{p-1}{2},$$

calculate their values (mod p) and read off the values of a in $x^2 \equiv a (\text{mod } p)$.

Example 107. *For example, for $p = 11$ we square $1, 2, 3, 4, 5$ and take their modulus 11 and read off the values of a in $x^2 \equiv a(\text{mod } 11)$.*

$$\begin{aligned}1^2 &= 1 \equiv 1(\text{mod } 11)\\ 2^2 &= 4 \equiv 4(\text{mod } 11)\\ 3^2 &= 9 \equiv 9(\text{mod } 11)\\ 4^2 &= 16 \equiv 5(\text{mod } 11)\\ 5^2 &= 25 \equiv 3(\text{mod } 11)\end{aligned}$$

So the quadratic residues are 1,4,9,5 and 3 and the quadratic non-residues are the rest, namely, 2,6,7,8 and 10. ◇

23.3 Wilson's Theorem

Theorem 161. *(Wilson[3])*
Let $p > 1$ be an integer. Then p is prime if and only if

$$(p-1)! \equiv -1(\text{mod } p).$$

Proof.
Clearly $(2-1)! = 1 \equiv -1(\text{mod } 2)$ and $(3-1)! = 2 \equiv -1(\text{mod } 3)$ so we may assume $p > 3$.
To prove $(p-1)! \equiv -1(\text{mod } p) \Rightarrow p$ is prime we prove the contrapositive statement that if p is not prime (that is p is composite) then $(p-1)! \not\equiv -1(\text{mod } p)$.
Let p be composite. Then its positive divisors are in the set of integers
$\{1, 2, 3, 4, \ldots, p-1\}$ so that[4]

$$\begin{aligned}p|1\cdot 2\cdot 3\cdot 4\cdots(p-1) &\Rightarrow 1\cdot 2\cdot 3\cdot 4\cdots(p-1) \equiv 0(\text{mod } p)\\ &\Rightarrow (p-1)! \equiv 0(\text{mod } p)\end{aligned}$$

so we cannot have $(p-1)! \equiv -1(\text{mod } p)$. Therefore if $(p-1)! \equiv -1(\text{mod } p)$ then p is a prime.

*****

Let p be prime. For the converse we need to prove $(p-1)! \equiv -1(\text{mod } p)$.
Now for p prime, each of the integers $1, 2, , 3\ldots, p-1$ is relatively prime to p.
We know by the Solution of Linear Congruences, Theorem 153 on page 237,
$ax \equiv b(\text{mod } m)$ has a solution if and only if $gcd(a, m) = 1$. So, for each of these integers less than p and therefore relatively prime to p there is another unique integer

[3] See also Theorem 102 on page 142

[4] For example, if $p = 12$ its positive divisors are 1,2,3,4,6 and they are elements of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

b modulo p such that $ab \equiv 1(\text{mod } p)$.
Since p is prime, if a, b are both 1 or a, b are both[5] $p-1$ then $ab \equiv 1(\text{mod } p)$.
If we omit 1 and $p-1$ the other numbers in $\{1, 2, 3, 4, \dots, p-1\}$ can be grouped into pairs whose product modulo p is 1, showing,

$$2 \times 3 \times 4 \times \cdots \times (p-2) \equiv 1(\text{mod } p) \Rightarrow (p-2)! \equiv 1(\text{mod } p)$$

Multiplying both sides by $p-1$ gives,

$$(p-1)! \equiv p-1(\text{mod } p) \equiv -1(\text{mod } p)$$

□

Definition 82. *Legendre symbol*
If p is an odd prime and gcd$(a, p) = 1$, we define the Legendre symbol (a/p) by,

$$\begin{aligned} (a/p) &= 1 && \text{if } a \text{ is a quadratic residue of } p \\ (a/p) &= -1 && \text{if } a \text{ is a quadratic non-residue of } p. \end{aligned}$$

Example 108. *For example, using the results of Example 107 above,* $(4/11) = 1$ *and* $(6/11) = -1$.

Theorem 162. *(Euler's Criterion)*
Let p be an odd prime and gcd$(a, p) = 1$. Then,

$$(a/p) \equiv a^{\frac{p-1}{2}}(\text{mod } p) \Leftrightarrow a^{\frac{p-1}{2}} \equiv (a/p)(\text{mod } p)$$

Proof.
Case 1: Let a be a quadratic non-residue of p so that $(a/p) = -1$. We want to show $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$.
Let $b \in \{1, 2, \dots, p-1\}$
The congruence $bx \equiv a(\text{mod } p)$ has, modulo p, a unique solution $\bar{b}$ by Theorem 153, page 237. Note $\bar{b} \neq b$ otherwise we would have $b^2 \equiv a(\text{mod } p)$ and a would be a quadratic residue of p.
It follows that the residue classes $\{1, 2, 3, \dots, p-1\}$ modulo p fall into $\dfrac{p-1}{2}$ pairs $b, \bar{b}$ such that $b\bar{b} \equiv a(\text{mod } p)$. Therefore,

$$\begin{aligned} (p-1)! &= 1 \times 2 \times \cdots \times (p-1) \\ &\equiv \overbrace{a \times a \times \ldots \times a}^{\frac{p-1}{2}}(\text{mod } p) \\ \Rightarrow (p-1)! &\equiv a^{\frac{p-1}{2}}(\text{mod } p) \end{aligned} \tag{23.3.1}$$

By Wilson's Theorem 161, $(p-1)! \equiv -1(\text{mod } p)$ so substituting into (23.3.1),

$$a^{\frac{p-1}{2}} \equiv -1(\text{mod } p) \Rightarrow a^{\frac{p-1}{2}} \equiv (a/p)(\text{mod } p)$$

[5] For the latter, $(p-1)(p-1) = p(p-2) + 1 \equiv 1(\text{mod } p)$.

***

Case 2: Let a be a quadratic residue of p so that $(a/p) = 1$. We want to show $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$.

By definition of a quadratic residue, the congruence $x^2 \equiv a(\text{mod } p)$ has a solution x. Suppose y is also a solution so that $y^2 \equiv a(\text{mod } p)$. Then we have,

$$x^2 - y^2 \equiv 0(\text{mod } p) \Rightarrow (x-y)(x+y) \equiv 0(\text{mod } p)$$

So either

$$(x-y) \equiv 0(\text{mod } p) \text{ or } (x+y) \equiv 0(\text{mod } p) \text{ so } x \equiv \pm y(\text{mod } p)$$

It follows that when $c(\text{mod } p)$ is one solution of $x^2 \equiv a(\text{mod } p)$ then so is $-c(\text{ mod } p) = p-c(\text{ mod } p)$. These solutions are distinct since p is odd[6]. Furthermore, we conclude these are the only two solutions. Note $(-c)^2 \equiv a(\text{mod } p)$.

Now isolate $c, p-c$ from $\{1,2,3,\ldots,p-1\}$. The remaining integers fall, modulo p, into $\dfrac{p-3}{2}$ pairs $b, \bar{b}$ such that $b\bar{b} \equiv a(\text{mod } p)$. Then,

$$\begin{aligned}(p-1)! &= 1 \times 2 \times \cdots \times c \times \cdots \times (p-c) \times \cdots \times (p-1)\\ &\equiv \overbrace{a \times a \cdots \times a}^{\frac{p-3}{2}} \times c \times (p-c)(\text{mod } p)\\ &\equiv a^{\frac{p-3}{2}}(-c^2)(\text{mod } p) \text{ since } p-c \equiv -c(\text{mod } p)\\ &\equiv a^{\frac{p-3}{3}}(-a)(\text{mod } p) \text{ since } c^2 \equiv a(\text{mod } p)\\ \Rightarrow (p-1)! &\equiv -a^{\frac{p-1}{2}}(\text{mod } p) \end{aligned} \tag{23.3.2}$$

Since by Wilson's Theorem 161 we have $(p-1)! \equiv -1(\text{mod } p)$ then substituting (26.1.2), $-a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$,

$$a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$$

We conclude for a quadratic residue $(a/p) = 1$ that,

$$a^{\frac{p-1}{2}} \equiv (a/p)(\text{mod } p)$$

So whether a quadratic residue or a quadratic non-residue, $a^{\frac{p-1}{2}} \equiv (a/p)(\text{mod } p)$. □

Theorem 163.

Let p be any odd prime. Then $(-1/p) = 1$ if and only if $p \equiv 1(\text{mod } 4)$.

Proof.

Put $a = -1$ in the statement of Theorem 162, namely $(a/p) \equiv a^{\frac{p-1}{2}}(\text{mod } p)$, to give,

$$(-1/p) \equiv (-1)^{\frac{p-1}{2}}(\text{mod } p)$$

and note $\dfrac{p-1}{2}$ is even if and only if $p \equiv 1(\text{mod } 4)$.

Then $(-1/p) = 1$ if and only if $p \equiv 1(\text{mod } 4)$. □

[6] We cannot have $c = p - c$ since then $p = 2c$ making p even

23.4 Method 3 Proof

Theorem 164.
There are an infinite number of primes p of the form $p = 4n+1$ or $p \equiv 1(\text{mod } 4)$.

Proof.
Suppose there are only a finite number of primes of the form $4n+1$ say, $5, 13, \ldots, p_n$. Consider,

$$N = (2 \times 5 \times 13 \times \cdots \times p_n)^2 + 1$$

Suppose p is a (necessarily odd) prime divisor of N say $(2 \times 5 \times 13 \times \cdots \times p_n)^2 + 1 = kp$. Then since,

$$(2 \times 5 \times 13 \times \cdots \times p_n)^2 = -1 \Rightarrow (2 \times 5 \times 13 \times \cdots \times p_n)^2 \equiv -1(\text{mod } p)$$

making -1 a quadratic residue of p or $(-1/p) = -1$, so by Theorem 163 we must have $p \equiv 1(\text{mod } 4)$.
Clearly $p \notin \{2, 5, 13, \ldots, p_n\}$ since each of these leave a remainder of 1 when they divide N. So we have a contradiction and there are an infinite number of primes p of the form $p = 4n+1$ or $p \equiv 1(\text{mod } 4)$. □

Note 31. *We have used only what we need of the theory of quadratic residues, a very rich area of Number Theory. Indeed we find here one of Gauss's favorite and challenging theorems, so much so he labelled it "aurema theorema" or the "golden theorem." We call it the quadratic reciprocity law. It states: If p and q are distinct primes then,*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless p, q are both of the form $4n+3$, in which case $\left(\frac{p}{q}\right) \neq \left(\frac{q}{p}\right)$.

Chapter 24

Primes of the form $4n+1$: Method 4

This proof requires an introduction to an important arithmetic function, the Möbius function $\mu(n)$ and the framework of introductory abstract algebra.
This will be our first proof in the algebraic branch of number theory. We actually use algebra to show in a different way that if $x^2 \equiv -1 (\text{mod } p)$ then the prime p is of the form $p \equiv 1 (\text{mod } 4)$.

Course: *Entrée V*
Ingredients
Möbius function
Euler's totient function
Groups
Examples of groups
Cyclic groups
The multiplicative group $\mathbb{Z}/p\mathbb{Z}$
Directions
Prove the theory of the Möbius function
Prove the theorems of Euler's totient function
Prove the relationship between the Möbius and totient functions
Prove the multiplicative group $\mathbb{Z}/p\mathbb{Z}$ is cyclic
Prove there are an infinite number of primes of the form $4n+1$ by method 4.

24.1 The Möbius function

Definition 83. *arithmetic function*
An arithmetic function is any function whose domain is $\mathbb{Z}$, that is, it can be written as,

$$f(n), n \in \mathbb{Z}$$

Example 109. *$f : \mathbb{N} \to \mathbb{R}$ where $f(n) = \sqrt{n}$ is an arithmetic function.*

Definition 84. *Möbius function*
The arithmetic function called the Möbius function[1] $\mu(n)$ *is defined by,*

$$\mu(n) = \begin{cases} 1 & if\ n = 1 \\ 0 & if\ p^2|n \text{ for some prime } p \\ (-1)^r & if\ n = p_1p_2\cdots p_r \text{ where the } p_i \text{ are distinct primes.} \end{cases}$$

Example 110.

$$\begin{aligned} \mu(2) &= -1 \\ \mu(4) &= \mu(2^2) = 0 \\ \mu(30) &= \mu(2\times 3\times 5) = (-1)^3 = -1 \qquad\qquad \diamond \end{aligned}$$

Definition 85. *multiplicative function*
A multiplicative function is an arithmetic function $f(n)$ of a positive integer n with the property that $f(1) = 1$ and if $gcd(a,b) = 1$, then $f(ab) = f(a)f(b)$.

Example 111. $f : \mathbb{N} \to \mathbb{R}$ *where* $f(n) = \sqrt{n}$ *is also a multiplicative function since* $\sqrt{ab} = \sqrt{a}\sqrt{b}$.

Theorem 165.
μ is a multiplicative function, that is for any $m, n \in \mathbb{Z}^+$ with $gcd(m,n) = 1$,

$$\mu(mn) = \mu(m)\mu(n)$$

Proof.
Suppose $gcd(m,n) = 1$. Let the prime factorizations of m, n be,

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r} \text{ and } m = q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s}$$

Then $\mu(mn) = 0 = \mu(m)\mu(n)$ if any of the exponents of either m or n exceeds 1. And if all the $r+s$ exponents α_i and β_j equal 1 then

$$\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$$

□

Theorem 166.
If $n > 1$ then $\sum_{d|n} \mu(d) = 0$ where the d are the divisors of n including 1.

Proof.
We use induction.
Let $S(t)$ be the statement $\sum_{d|n} \mu(d) = 0$ where $n = p_1^{\alpha_1}p_1^{\alpha_1}\cdots p_t^{\alpha_t}$ is the product of t distinct primes.

[1] μ = mu

Basis Step: Then S(1) is true since if $n = p^\alpha$ then the successive powers of p all divide p^α and we have, since $\mu(n) = 0$ if $p^2|n$ and $\mu(p) = -1$,

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^\alpha) = 1 - 1 + 0 + \ldots + 0 = 0$$

Assumption Step: Suppose S(t) is true, that is $\sum\limits_{d|n} \mu(d) = 0$ where $n = p_1^{\alpha_1} p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ is the product of t distinct primes.
Inductive Step: Consider S(t+1).
We want to show $\sum\limits_{d|N} \mu(d) = 0$ is true for $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} = np_{t+1}^{\alpha_{t+1}}$.
Write $N = np^\alpha$ where for convenience p^α replaces $p_{t+1}^{\alpha_{t+1}}$. Then[2],

$$\begin{aligned}\sum_{d|N} \mu(d) &= \sum_{d|n} \mu(d) + \sum_{d|n} \mu(pd) + \sum_{d|n} \mu(p^2 d) + \ldots + \sum_{d|n} \mu(p^\alpha d)\\
&= 0 + \sum_{d|n} \mu(pd) + \sum_{d|n} \mu(p^2 d) + \ldots + \sum_{d|n} \mu(p^\alpha d) \text{ assuming S(t) is true}\\
&= 0 + \sum_{d|n} \mu(pd) + 0 + 0 + \ldots + 0 \text{ since each zero term was a power of a prime} > 1\\
&= 0 + \sum_{d|n} \mu(p)\mu(d) \text{ since } \mu \text{ is multiplicative}\\
&= 0 - \sum_{d|n} \mu(d) \text{ since } \mu(p) = -1 \text{ by definition of } \mu\\
&= 0 \text{ assuming S(t) is true}\end{aligned}$$

□

Note 32.
This note deals with double sums, handling them can be tricky.
A double sum is conducted in two steps. First evaluate the inner sum, (the one on the right), and then evaluate the outer sum.
Note that if an index (i, j, k, etc.) is not controlled by the sum it is attached to, its

[2] If for example the divisors of n are $1, a, b, c, ab, ac, ba, abc$ then the divisors of $N = p^3 n$ are

$$\begin{aligned}&1, a, b, c, ab, ac, bc, abc\\
&p, pa, pb, pc, pab, pac, pbc, pabc\\
&p^2, p^2a, p^2b, p^2c, p^2ab, p^2ac, p^2bc, p^2abc\\
&p^3, p^3a, p^3b, p^3c, p^3ab, p^3ac, p^3bc, p^3abc\end{aligned}$$

that is, the divisors of n multiplied by successive powers of p from 0 to 3.

terms may be taken outside (it's just the distributive law.) For example,

$$\begin{aligned}\sum_{j=1}^{4}\sum_{k=1}^{3}6kj &= \sum_{j=1}^{4}\left(\sum_{k=1}^{3}6kj\right)\\ &= \sum_{j=1}^{4}j\left(\sum_{k=1}^{3}6k\right)\\ &= \sum_{j=1}^{4}j\times 6(1+2+3)\\ &= \sum_{j=1}^{4}36j\\ &= 36(1+2+3+4)\\ &= 360\end{aligned}$$

The main procedure in the following theorem and its converse is to combine a double sum like,

$$\sum_{dd'=n}\mu(d)\sum_{e|d'}g(e) \tag{24.1.1}$$

into a single sum over the product of the indices thus,

$$\sum_{deh=n}\mu(d)g(e) \tag{24.1.2}$$

and then separate out this single sum into a double sum in which the order is reversed, namely,

$$\sum_{eh'=n}g(c)\sum_{d|h'}\mu(d) \tag{24.1.3}$$

Example 112. *We claim for $n=6$,*

$$\sum_{dd'=6}\mu(d)\sum_{e|d'}g(e)=\sum_{deh=6}\mu(d)g(e)$$

If $dd'=6$ then the dd' pairs are $(1,6),(2,3),(3,2)$ and $(6,1)$. Hence,

$$\begin{aligned}&\sum_{dd'=6}\mu(d)\sum_{e|d'}g(e)\\ &=\mu(1)\sum_{e|6}g(e)+\mu(2)\sum_{e|3}g(e)+\mu(3)\sum_{e|2}g(e)+\mu(6)\sum_{e|1}g(e)\\ &=\mu(1)[g(1)+g(2)+g(3)+g(6)]+\mu(2)[g(1)+g(3)]\\ &\qquad+\mu(3)[g(1)+g(2)]+\mu(2\times 3)[g(1)]\\ &=g(1)+g(2)+g(3)+g(6)-g(1)-g(3)-g(1)-g(2)+g(1)+g(6)\\ &=g(6)\end{aligned}$$

whereas for $\sum\limits_{deh=6} \mu(d)g(e)$ *the possible cobinations of* d, e *and* h *and their contributions to the sum are:*

$$\begin{aligned}
(1,1,6):&\ \mu(1)g(1) = +g(1)\\
(1,2,3):&\ \mu(1)g(2) = +g(2)\\
(1,3,2):&\ \mu(1)g(3) = +g(3)\\
(2,1,3):&\ \mu(2)g(1) = -g(1)\\
(2,3,1):&\ \mu(2)g(3) = -g(3)\\
(3,2,1):&\ \mu(3)g(2) = -g(2)\\
(6,1,1):&\ \mu(6)g(1) = -g(1)\\
(1,6,1):&\ \mu(1)g(6) = +g(6)\\
(3,1,2):&\ \mu(3)g(1) = -g(1)
\end{aligned}$$

leaving only $g(6)$. ◇

Theorem 167. *(Möbius Inversion Formula)*
If $f(n), g(n)$ *are two arithmetic functions, then,*

$$f(n) = \sum_{d|n} g(d) \text{ if and only if } g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

Proof.
First we suppose $f(n) = \sum\limits_{d|n} g(d)$. Then, writing $d|n$ as $dd' = n$ we have,

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{dd'=n} \mu(d) f(d') \tag{24.1.4}$$

Substituting $f(n) = \sum\limits_{d|n} g(d)$ in the form $f(d') = \sum\limits_{e|d'} g(e)$ we have,

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{dd'=n} \mu(d) \sum_{e|d'} g(e) \tag{24.1.5}$$

Writing $e|d'$ as $d' = eh$ we have,

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{dd'=n} \mu(d) \sum_{d'=eh} g(e) \tag{24.1.6}$$

We combine this double sum into a single sum by replacing d' with eh in $dd' = n$ to give the single sum,

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{deh=n} \mu(d) g(e) \tag{24.1.7}$$

We now reverse the process and separate the single sum into a double sum by reversing the functions and writing $h' = dh$ so $d|h'$ and returning to the form of (24.1.5),

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{eh'=n} g(e) \sum_{d|h'} \mu(d) \tag{24.1.8}$$

Since $\sum_{d|h'} \mu(d) = 0$ if $h' > 0$ and by definition is $\mu(1) = 1$ if $h' = 1$, we have left on the right side only $\sum_{e=n} g(e)$ giving,

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = g(n) \tag{24.1.9}$$

*****

Conversely, suppose $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$. Then,

$$\begin{aligned}\sum_{d|n} g(d) &= \sum_{d|n} \sum_{d'|d} \mu(d') f\left(\frac{d}{d'}\right)\\ &= \sum_{d'ef=n} \mu(d') f(e)\\ &= \sum_{eh'=n} f(e) \sum_{d'|h'} \mu(d')\end{aligned}$$

As above, since $\sum_{d|h'} \mu(d) = 0$ if $h' > 0$ and by definition is 1 if $h' = 1$ we have left on the right side only $f(n)$ so,

$$\sum_{d|n} g(d) = f(n) \tag{24.1.10}$$

□

24.2 Euler's Totient Function

Recall Euler's Totient function $\phi(n)$ is the number of numbers less than n that are relatively prime to n.

Theorem 168.
For p a prime and α a positive integer,

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

Proof.
There are p^α numbers less than or equal to p^α and the only positive numbers less than p^α that are not relatively prime to p^α are $p^{\alpha-1}$ multiples of p, namely $p, 2p, 3p, \ldots, p^{\alpha-1}$.
□

Theorem 169.
Let $n \in \mathbb{N}$ with prime decomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Then,

(a) $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ *where p is a prime.*

(b) $\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_s^{\alpha_s}) = \prod_{i=1}^{s} \phi(p_i^{\alpha_i}$

Proof.

(a) Let the prime decomposition of n be $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Then by Theorem 168,

$$\phi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) \text{ for all } i : 1 \le i \le s)$$

Since ϕ is multiplicative we have,

$$\begin{aligned} \phi(n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}) \\ &= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_t^{\alpha_t}) \\ &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1^{\alpha_1}}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2^{\alpha_2}}\right) \cdots p_s^{\alpha_s}\left(1 - \frac{1}{p_s^{\alpha_s}}\right) \\ &= n \prod_{p|n}\left(1 - \frac{1}{p}\right) \end{aligned}$$

(b)

$$\begin{aligned} \phi(n) &= n \prod_{p|n}\left(1 - \frac{1}{p}\right) \text{ by (a)} \\ &= n \prod_{i=1}^{s} (1 - \frac{1}{p_i^{\alpha_i}}) \text{ since only } p_1 \text{ to } p_s \text{ divide } n \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right) \\ &= \prod_{i=1}^{s}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) \text{ by grouping each } p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^{s} \phi\left(p_i^{\alpha_i}\right) \text{ by Theorem 168} \end{aligned}$$

□

Theorem 170.
Euler's totient function ϕ is multiplicative, that is for $m, n \in \mathbb{Z}^+$ with $gcd(m, n) = 1$ we have,

$$\phi(mn) = \phi(n)\phi(m)$$

Proof.
Let

$$n = p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_r 1^{\alpha_r}, \quad m = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

Then,

$$\begin{aligned}\phi(nm) &= \phi(p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}) \\ &= \phi(p_1^{\alpha_1})\phi(p_1^{\alpha_2}) \cdots \phi(p_r^{\alpha_r}) \times \phi(q_1^{\beta_1})\phi(q_2^{\beta_2}) \cdots \phi(q_s^{\beta_s}) \\ &= \phi(n)\phi(m)\end{aligned}$$

so ϕ is a multiplicative function. □

Theorem 171. *Let $n \in \mathbb{N}$. Then,*

$$\sum_{d|n} \phi(d) = n.$$

Proof.
Let $d|n, d > 0$ and let,

$$S_d = \{m \in \mathbb{Z} \mid 1 \le m \le n, gcd(m,n) = d\}$$

Now $gcd(m,n) = d$ if and only if[3] $gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.
Hence the number of integers in S_d is equal to the number of positive integers not exceeding $\frac{n}{d}$ that are relatively prime to $\frac{n}{d}$. That is the number of elements, $|S_d|$, is,

$$|S_d| = \phi\left(\frac{n}{d}\right)$$

Since every integer from 1 to n inclusive is an element of one and only one S_d we have,

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$$

But as d runs over the positive divisors of n we have that $\frac{n}{d}$ runs over the positive divisors of n so that[4],

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$$

□

[3] $gcd(m,n) = d$ if and only if $m = kd, n = jd$ where j,k have no common factors other than 1, that is $gcd(k,j) = 1 \Rightarrow gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

[4] For example, if $n = 10$ we have,

$$\sum_{d|10} \phi(d) = \phi(1) + \phi(2) + \phi(5) + \phi(10) \text{ and,}$$

$$\sum_{d|10} \phi\left(\frac{10}{d}\right) = \phi\left(\frac{10}{1}\right) + \phi\left(\frac{10}{2}\right) + \phi\left(\frac{10}{5}\right) + \phi\left(\frac{10}{10}\right) = \phi(1) + \phi(5) + \phi(2) + \phi(1) = \sum_{d|10} \phi(d).$$

Corollary 172.
The Möbius function and Euler's Totient function are related as follows:

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Proof.
From Theorem 171 we have,

$$\sum_{d|n} \phi(d) = n.$$

Apply the Möbius Inversion Theorem 167, page 253 to obtain,

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

From Theorem 169, page 255 we have,

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Hence,

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

□

24.3 Group Theory

There are literally dozens of text books on group theory which is the corner stone of abstract algebra. Again we will cherry-pick at a very elementary level and just take the minimum we need. Let's first categorize the description of the mathematical operations that act on numbers.

Definition 86. *binary and unitary operations*
There are two types of operations, binary and unitary, on numbers. The basic binary operations are $\{+, -, \times, \div\}$ *and the unitary operations include taking the square root (or any root) and raising a number to a power, that is* $\sqrt[n]{x}$ *and* x^n*. A binary operation requires an input of two numbers, e.g.,* $5 + 7 = 12$*, while a unitary operation requires an input of one number, e.g.,* $\sqrt{9} = 3$*.*

And now groups.

A group is an abstract mathematical object. Its inspiration is an abstraction from the axioms of integers, fractions, real and complex numbers. Each of these is a set and the binary arithmetic operations apply to each. A group requires a set and one binary operation, generally regarded as either addition or multiplication.

Definition 87. *group and group axioms*
In abstract terms we define a group as a set G together with a binary operation $*$, written $(G,*)$, such that the following axioms, taken from $\{\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}\}$, are satisfied:

1. *Closure law: For all $a,b \in G$, we have $a*b \in G$, that is, the result of a binary operation acting on any two elements of the group is another element of the group. We say the group is closed under $*$.*
2. *Associative law: For all $a,b,c \in G$ we have $a*(b*c) = (a*b)*c$*
3. *Identity law: There is an identity element $e \in G$ such that for all $a \in G$ we have $a*e = e*a = a$*
4. *Inverses law: For all $a \in G$ there is an element $b \in G$ such that $a*b = b*a = e$ and we write this b as a^{-1}.*

Example 113. *For an example of each axiom, when applied to $(\mathbb{Z},+)$ we have statements such as,*

1. *Closure:* $5,7 \in \mathbb{Z}$ *and* $5+7 = 12 \in \mathbb{Z}$
2. *Associativity:* $2+(3+4) = (2+3)+4$
3. *Identity:* $e = 0$ *since* $3+0 = 0+3 = 3$
4. *Inverses:* -3 *is the inverse of* 3 *since* $3+(-3) = (-3)+3 = 0$ *or, more commonly* $3-3 = 0$ ◇

Definition 88. *commutative or abelian group*
If a group $(G,*)$ satisfies $a*b = b*a$ for all $a,b \in G$ we say the group is commutative or abelian (after Niels Abel, the Norwegian algebraicist).

Clearly, $(\mathbb{Z},+)$ is abelian since $3+2 = 2+3$, etc.

Lemma 173.
A group obeys the cancellation law $a*b = a*c \Rightarrow b = c$.

Proof. Let $a,b,c \in G$ where $(G,*)$ is a group.

$$\begin{aligned}
&a*b = a*c\\
&\Rightarrow a^{-1}*(a*b) = a^{-1}*(a*c)\\
&\Rightarrow (a^{-1}*a)*b = (a^{-1}*a)*c\\
&\Rightarrow e*b = e*c\\
&\Rightarrow b = c
\end{aligned}$$

where we used the inverse, associative and identity axioms of groups. □

For the sake of simplicity we refer to a group $(G, *)$ as just G since the binary operation is mostly specified elsewhere. Along these lines we then drop the use of $*$ and just say statements like $a(bc) = (ab)c$ which can be understood to mean $a \times (b \times c) = (a \times b) \times c$ if the operation is multiplication or $a + (b + c) = (a + b) + c$ if the operation is ordinary addition. But we will find there are other binary operations besides the arithmetic ones.

Further, for inverses, a^{-1} suits multiplication, giving the usual $aa^{-1} = a/a = 1$ but it means $-a$ when we are dealing with addition, thus $a + (-a) = 0$, and of course we generally drop the parentheses and write $a - a = 0$. The inverse elements for the arithmetic operations are 0 for addition and 1 for multiplication and we call -6 the additive inverse of 6 and $\frac{1}{6}$ the multiplicative inverse of 6.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are obviously all groups under the operation of addition. The only group axiom that causes an issue with the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under the operation of multiplication is the inverse law and the existence of multiplicative inverses. No integer has a multiplicative inverse that is also an integer, for example, $1/7$ is the multiplicative inverse of 7 but $1/7 \notin \mathbb{Z}$, failing closure, so $(\mathbb{Z}, \times)$ is not a group.

For each of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, the element 0 does not have a multiplicative inverse, that is there is no element b such that $0 \times b = 1$. But we can still form groups simply by deleting the element 0. So we have the multiplicative groups $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$ where the exponent $\times$ means the zero element has been removed. Thus, for example, $\mathbb{C}^\times = \mathbb{C} - \{0\}$ or $\mathbb{C}/\{0\}$.

So we have four additive groups, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, and three multiplicative groups $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$. They are all infinite in size and they form the "inspiration" for an infinity of other groups, some finite, some infinite.

Notation 5. *The number of elements in the group G is written $|G|$.*
For an infinite group we use $|G| = \aleph_0$ spoken as "aleph naught" or "aleph null" where aleph is the first letter of the Hebrew alphabet.

24.4 Congruence and Finite Groups

24.4.1 The Additive Group $\mathbb{Z}_n$

Definition 89. *$\mathbb{Z}_n$ and addition modulo n*
$\mathbb{Z}_n$ is the set of all possible smallest positive remainders when the integers are divided by n. That is,

$$\mathbb{Z}_n = \{0, 1, 2, ..., n - 1\}$$

In words, $\mathbb{Z}_n$ is the set of all integers modulo n where we note that when an integer is divided by n, no remainder can be greater than $n - 1$.
Accordingly $|\mathbb{Z}_n| = n$.

Example 114. *For example, $\mathbb{Z}_5 = \{0,1,2,3,4\}$ with operation modulo 5, meaning any integer is replaced by its least positive remainder when divided by 5. Thus,*

$$0,1,2,3,4,5,6,7,8,9,10,11,...$$

becomes,

$$0,1,2,3,4,0,1,2,3,4,0,1,...$$

leaving only the elements $0,1,2,3,4$.
If we set up what we can call an operations table for all possible combinations of the elements of $\mathbb{Z}_5 = \{0,1,2,3,4\}$ *under addition modulo 5, we have,*

Mod 5	*0*	*1*	*2*	*3*	*4*
0	*0*	*1*	*2*	*3*	*4*
1	*1*	*2*	*3*	*4*	*0*
2	*2*	*3*	*4*	*0*	*1*
3	*3*	*4*	*0*	*1*	*2*
4	*4*	*0*	*1*	*2*	*3*

where we used $4+4=8\equiv 3(\text{mod } 5)$ *etc.*

You can easily see the set $\mathbb{Z}_5$ *is closed under addition modulo 5, meaning only its elements* $0,1,2,3,4$ *are found in the table, that the associative law holds, that there is an identity 0 (e.g.,* $0+3=3$ *) and that every element has an additive inverse, the pairs being* $(0,0),(1,4),(2,3)$. *So* $\mathbb{Z}_5$ *is a group.* ◇

Since we can specify any positive integer n for $\mathbb{Z}_n$, we already have an infinite number of finite groups once we prove the next theorem, that the set $\mathbb{Z}_n$ together with the operation of addition modulo n is a group.

Theorem 174.
The set $\mathbb{Z}_n$ *together with the operation of addition modulo* n *is a group.*

Proof. We need to prove the four group axioms in Definition 87 on page 258 hold.

1. Closure, that is, if $a,b\in\mathbb{Z}_n$ so does $a+b(\text{ mod } n)$, that is $a+b\equiv c(\text{ mod } n)$ where $c<n$.
   This is so since a,b are less than n so $a+b<2n$ and either $a+b=c<n$ and we are done, or $a+b=n+c$ where we must have $c<n$, and therefore n divides the difference $a+b-c$ so by Definition 23, page 67, $a+b\equiv c(\text{mod } n)$.

2. Associative Law, that is if $a,b,c\in\mathbb{Z}_n$ then $a+(b+c)=(a+b)+c$. This is true since a,b,c are also integers.

3. Identity element is 0.

4. Inverse Law. Given $a\in\mathbb{Z}_n,\ 0\le a\le n-1$, then $(n-a)+a=0$ making $n-a$ the inverse of a.

Hence $\mathbb{Z}_n$ is a group. □

24.4.2 The Multiplicative Group $\mathbb{Z}/n\mathbb{Z}$

We now extend the multiplicative set $\mathbb{Z}_p^*$ we used in Chapter 13 without needing that it is also a group.

Definition 90. *multiplicative group* $\mathbb{Z}/n\mathbb{Z}$
If we divide the integers by $n \in \mathbb{N}$ *the possible remainders are* $\{0, 1, 2, \ldots, n-1.\}$ *Thus division by* n *separates the integers into* $n-1$ *subsets which we call cosets and we label them thus,*

$$\begin{aligned}
[0]_n &= \{0, n, 2n, \ldots, \} \\
[1]_n &= \{1, n+1, 2n+1, \ldots, \} \\
[2]_n &= \{2, n+2, 2n+2, \ldots, \} \\
&\ldots \\
[n-1]_n &= \{n-1, n+(n-1), 2n+(n-1), \ldots, \}
\end{aligned}$$

Accordingly $[a]_n$ *is the set of all integers with a least non-negative remainder of* a *when divided by* n*. Thus we note that in general,*

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a(\text{mod } n\}$$

We define,

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n$$

Example 115. *For example* $\mathbb{Z}/5\mathbb{Z}$ *separates the integers into the five cosets,*

$$\begin{aligned}
[0]_5 &= \{0, \pm 5, \pm 10, \ldots\} \\
[1]_5 &= \{1, 6, 11, \ldots\} \cup \{-4, -9, -14, \ldots\} \\
[2]_5 &= \{2, 7, 12, \ldots\} \cup \{-3, -8, -13, \ldots\} \\
[3]_5 &= \{3, 8, 13, \ldots\} \cup \{-2, -7, -12, \ldots\} \\
[4]_5 &= \{4, 9, 14, \ldots\} \cup \{-1, -6, -11, \ldots\}
\end{aligned}$$

Note the elements x *of* $[2]_5$ *satisfy* $x \equiv 2(\text{mod } 5)$*, similarly the other cosets.* ◇

We next prove $\mathbb{Z}/n\mathbb{Z}$ is a multiplicative group. To form a group we delete the zero coset $[0]_n$ since 0 cannot have an inverse and for brevity continue to denote $\mathbb{Z}/n\mathbb{Z} - \{[0]_n\}$ by $\mathbb{Z}_n/n\mathbb{Z}$. We define the operation we need by,

Definition 91. *coset multiplication*
We define coset multiplication of elements $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ *by*

$$[a]_n[b]_n = [ab]_n$$

This definition makes sense since,

$$\begin{aligned} x \in [a]_n &\Rightarrow x \equiv a (\text{mod } n) \Rightarrow x = a + jn, j \in \mathbb{Z} \text{ and} \\ y \in [b]_n &\Rightarrow y \equiv b (\text{mod } n) \Rightarrow y = b + kn, k \in \mathbb{Z} \\ &\Rightarrow xy = ab + n(aj + bk + kjn) \equiv ab (\text{mod } n) \\ &\Rightarrow xy \in [ab]_n. \end{aligned}$$

Theorem 175.
For p a prime, $\mathbb{Z}/n\mathbb{Z}$ is a group under coset multiplication.

Proof. We need to show the four group axioms of Definition 87 on page 258 hold.

1) Closure: The definition $[a]_n[b]_n = [ab]_n$ shows the multiplication of two cosets results in another coset.

2) Identity: The identity element is $[1]_n$ since $[a]_n[1]_n = [a \times 1]_n = [a]_n$.

3) Inverses: To show the inverse of $y \in \mathbb{Z}/n\mathbb{Z}$ exists in $\mathbb{Z}/n\mathbb{Z}$ we use Corollary 16 on page 42 which states that for $x, y \in \mathbb{Z}$ that there exist integers a, b such that $ax + by = 1$ if and only if $gcd(x, y) = 1$.
We let $x = p$ and $y \in \{1, 2, \ldots, p - 1\}$ so that $gcd(x, y) = 1$.
Then $ap + by = 1 \Leftrightarrow by = 1 - ap$ means there exists a b such that $by \equiv 1(\text{mod } p)$ which in turn means $y^{-1} = b$ exists.

4) Associativity: This holds since it is true for a, b, c which are integers. Thus we have,

$$[a]_n([b]_n[c]_n) = [a_n][bc]_n = [a(bc)]_n = [(ab)c]_n = [ab]_n[c]_n = ([a]_n[b_n])[c]_n$$

Hence $\mathbb{Z}/n\mathbb{Z}$ is a group under coset multiplication. □

24.4.3 Cyclic Groups

A cyclic group is a group that can be generated by one of its elements meaning every element in the group can be formed from that one element by repeated applications of the binary operation. Symbolically we use only addition and multiplication, but the binary operations take many other forms.

Definition 92. *cyclic group*[5] $< a >$
We define the cyclic group $< a >$ generated by the element a in the group G as,

- *for multiplication, $< a >= \{x \in G \mid x = a^n \ for \ some \ n \in \mathbb{Z}\}$.*
- *for addition, $< a >= \{x \in G \mid x = \underbrace{a + a + \cdots + a}_{n} = na \ for \ some \ n \in \mathbb{Z}.\}$*

[5] We prove $< a >$ is a group in Theorem 176, part (1) on page 263

Example 116. *For example,* $(\mathbb{Z}_5, addition\ modulo\ 5)$ *is a finite cyclic group generated by 2 since,*

$$\begin{aligned}
&2 = 2,\\
&2 + 2 = 4,\\
&2 + 2 + 2 = 1,\\
&2 + 2 + 2 + 2 = 3,\\
&2 + 2 + 2 + 2 + 2 = 0
\end{aligned}$$

are all elements of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$*.*
Note any further addition of 2's always yields one of these five elements, for example $102 \times 2 \equiv 4 \pmod{5}$. ◇

In general the additive group $(\mathbb{Z}_n,\ modulo\, n) = \{0, 1, 2, \cdots, n-1\}$ is obviously cyclic by definition. It can be generated by any element a provided $gcd(a, n) = 1$.
(Try $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with $a = 3, 4$.)
The simplest example of an infinite cyclic group is $\mathbb{Z}$ which is generated by 1 since $n \times 1, n \in \mathbb{Z}$ gives us all the integers. We could also use -1.
We want to show $\mathbb{Z}/n\mathbb{Z} = \{[1]_n, [2]_n, \ldots, [n-1]_m\}$ is a cyclic group under coset multiplication.
Let us first note that the word "order" is used in two different ways when we are dealing with elements and groups.

Definition 93. *order of a group*
The order of a group G *is the number of elements in the group. We use* $|G|$ *as the symbol for the order of a group.*

Example 117. $|\mathbb{Z}_5| = |\{0, 1, 2, 3, 4\}| = 5$
The order of $\mathbb{Q}$ *is infinite.* ◇

Definition 94. *order of a group element*
Let G *be a group with identity* e *and let* $a \in G$*. If there is a positive integer* n *such that* $a^n = e$*, then* a *is said to have finite order. The smallest such positive integer is called the order of* a*, written* $|a|$*.*

Example 118. $2 \in \mathbb{Z}_5$ *and* $|2| = 4$ *since* $2^4 \equiv 1 \pmod{5}$.

We now prove a theorem that gives a test as to whether a finite group is cyclic.

Theorem 176.

(1) Let G *be a group under multilpication.*
If $a \in G$ *then* $< a >= \{x \in G \mid x = a^k\ for\ some\ k \in \mathbb{Z}\}$ *is also a group under the same operation as for* G*.*

(2) *If the order of a is n, that is $|a| = n$, then the cyclic subgroup $< a >$ is a finite group of n elements given by*

$$< a >= \{e, a, a^2, \cdots, a^{n-1}\}$$

and therefore $| < a > | = n = |a|$.

(3) *A finite group G is cyclic if and only if there exists an element $a \in G$ such that the order of G equals the order of a, that is, $|a| = |G|$.*

Proof. (1) To show $< a >$ is a group, we use the criteria for a group from Definition 87 on page 258.

- Closure: $< a >= \{x \in G \mid x = a^k \; for \; some \; k \in \mathbb{Z}\}$ is closed since if $a^i, a^j \in< a >$ then $a^i a^j = a^{i+j} \in< a >$ since $i + j \in \mathbb{Z}$.
- Associativity follows from $a^i \times (a^j \times a^k) = (a^i \times a^j) \times a^k = a^{i+j+k}$.
- The identity element is $e = a^0 = 1$ since $a^0 \times a^k = a^k$. Note also $a^n = 1$, so $e = a^0 = a^n = 1$.
- Inverses exist since $(a^n)^{-1} = a^{-n}$ and $-n \in \mathbb{Z}$ so that $a^n(a^n)^{-1} = a^0 = 1$.

Therefore $< a >$ is a group.

(2) We want to show if $a \in G$ and $|a| = n$ then the cyclic group $< a >= \{x \in G \mid x = a^k \; for \; some \; k \in \mathbb{Z}\}$ is a finite group of n elements given by $< a >= \{e, a, a^2, \ldots, a^{n-1}\}$ and therefore $| < a > | = n = |a|$.
Given $|a| = n$ we can write any integer k divided by n as $k = qn + r, 0 \le r \le n - 1$. Then,

$$a^k = a^{qn+r} = (a^n)^q a^r = e^q \times a^r = a^r, \;\; 0 \le r \le n - 1.$$

Thus, all the integer powers, a^k, separate out into just the n elements a^r with powers $0 \le r \le n - 1$. So,

$$< a >= \{e, a, a^2, \cdots, a^{n-1}\},$$

and therefore $| < a > | = n = |a|$.

(3) Suppose a finite group G is cyclic and generated by $a \in G$ where the order of a is $|a| = n$. Then by (2) $G =< a >= \{e, a, a^2, \cdots, a^{n-1}\}$ and clearly the respective orders $|a| = |G|$ since both equal n.

*****

Conversely, suppose $a \in G$ and $|a| = n = |G|$. Then $a^1, a^2, \cdots, a^n = e$ all belong to G and since $|G| = n$, there can be no other elements. Then G is cyclic by (2).

□

Note 33. *Part (3) of Theorem 176 has given us an easy test for a finite group to be cyclic, namely, a group G is cyclic if and only if it contains an element a of order $|G|$, that is, $a^n = 1$ where n is the number of elements in the group G or $n = |G|$.*
In particular, to show $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group we need to show there is an element a whose order $|a| = p - 1$.

24.5 More on Groups

We proceed with a further set of theorems, corollaries and lemmas on our way to showing for $p \in \mathbb{P}$ that $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group.

Theorem 177.
Let G be a group and $a \in G$. Then for all $i, j \in \mathbb{Z}$ if a has the finite order $|a| = n$ then $a^i = a^j$ if and only if n divides $i - j$.

Proof.
If and only if means we must prove two implications, one the converse of the other:

(i) If n divides $i = j$ then $a^i = a^j$.

(ii) If $a^i = a^j$ then $n|(i - j)$.

***

(i) Suppose n divides $i - j$. Then $i - j = nk$ for some $k \in \mathbb{Z}$. Hence,

$$a^i = a^{nk+j} = (a^n)^k a^j = e^k a^j = ea^j = a^j$$

(ii) Conversely, suppose $a^i = a^j$. Then $a^{i-j} = a^0 = e$.
By the Division Algorithm, Theorem 13, page 39,

$$i - j = qn + r, 0 \le r < n.$$

Then,

$$e = a^{i-j} = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r,\ 0 \le r < n$$

Since $0 \le r < n$ and n is the least positive integer such that $a^n = e$ we must have $r = 0$. Then,

$$i - j = qn \Rightarrow n|(i - j).$$

□

Corollary 178.
Let G be a group and $a \in G$ be an element of finite order, say $|a| = n$. Then for all $k \in \mathbb{Z}$, $a^k = e$ if and only if $n|k$.

Proof.
Suppose $a^k = e \Rightarrow a^k = a^0$. By Theorem **??** with $i = k, j = 0$ we have $n|(k-0) \Rightarrow n|k$.

***

Conversely, suppose $n|k \Rightarrow k = nm, m \in \mathbb{Z}$.
Then $a^k = a^{nm} = (a^n)^m = e^m = e$. □

Let's recall some arithmetic definitions and theorems.

Definition 95. *least common multiple*
The least common multiple of two integers a, b, denoted $lcm(a,b)$, is the least number that is a multiple of a and b. (As distinct from the greatest common divisor or $gcd(a,b)$ which is the greatest number that is a multiple of a and b.)

Example 119. *For example, to find $lcm(18,60)$ we fully factor both numbers into powers of primes and then take the greatest power of each prime to form the lcm. Thus $18 = 2^1 \times 3^2$ and $60 = 2^2 \times 3^1 \times 5^1$ so $lcm(18,60) = 2^2 \times 3^2 \times 5 = 180$.* ◇

Note 34.
On the other hand, to find $gcd(a,b)$ we take the smallest power of each prime in their prime decompositions so in the previous example $gcd(18,60) = 2^1 \times 3^1 \times 5^0 = 6$.

It is a theorem that $gcd(a,b) \times lcm(a,b) = ab$.
To prove this we let $gcd(a,b) = p$ so that $a = pq, b = pr$ with $gcd(q,r) = 1$.
Then $lcm(a,b) = pqr$ and $gcd(a,b) \times lcm(a,b) = p^2qr = ab$.

In the above example $a \times b = 18 \times 60 = 1080$ and $gcd(18,60) \times lcm(18,60) = 6 \times 180 = 1080$.

Theorem 179.
Let $G =< a >$ be a cyclic group with generator a of order $|a| = |G| = |< a >| = n$. Then for all powers $a^s \in G$ we have the order of a^s is given by,

$$|a^s| = \frac{n}{gcd(n,s)}$$

Proof.
Let $G =< a >$ be a cyclic group with generator a of order $|a| = |G| = |< a >| = n$.
Let the order of a^s be k, that is k is the least integer such that $(a^s)^k = a^{sk} = e$.
So sk is the least multiple of s.
By Corollary 178, $a^{sk} = e$ if and only if $sk|n$ where n is the least integer such that $a^n = e$.
Now $sk|n \Rightarrow sk = mn, m \in \mathbb{Z}$ and therefore sk is the least multiple of n.
But if sk is the least multiple of s and also of n then $sk = lcm(s,n)$. That is to say,

$$sk = lcm(n,s) \Rightarrow k = \frac{lcm(n,s)}{s}.$$

Now for any integers a, b we have $gcd(a, b) \times lcm(a, b) = ab$.
Then,

$$|a^s| = k = \frac{lcm(n, s)}{s} = \frac{sn}{s \times gcd(n, s)} = \frac{n}{gcd(n, s)}$$

□

Lemma 180.
The polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$$

has at most n distinct roots[6].

Proof.
We use induction.
Let $S(n)$ be the statement,

$$g(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n, a_0 \neq 0$$

has at most n distinct roots.
Basic Step: $S(1) : g(x) = a_0x + a_1$ has at most 1 root is true since $-\dfrac{a_1}{a_0}$ is the only root.
Assumption Step: Assume $S(n)$ is true.
Induction Step: We need to show the statement $S(n+1)$ that the polynomial

$$f(x) = a_0x^{n+1} + a_1x^n + \ldots + a_nx + a_{n+1}$$

has at most $n+1$ distinct roots is true.
If $f(x)$ has no roots, we are done. Otherwise, suppose α is a root.
Then $f(x) = (x - \alpha)g(x)$ where $g(x)$ has degree n.
If β is another different root, that is $f(\beta) = 0$, then

$$0 = f(\beta) = (\beta - \alpha)g(\beta) \Rightarrow g(\beta) = 0.$$

That is, any other distinct root of $f(x)$ is also a root of $g(x)$.
By assumption, $g(x)$ has at most n roots. Therefore $f(x)$ has at most $n+1$ distinct roots namely α and the roots of $g(x)$. □

[6] A root of a polynomial in the variable x is a value of x for which the polynomial equals 0. For example 2 is a root of $f(x) = x^3 - 8$ since $2^3 - 8 = 0$. It follows that if a is a root then $(x - a)$ is a factor of $f(x)$. Here $x^3 - 8 = (x - 2)(x^2 + 2x + 4)$ so $x - 2$ is a factor of $x^3 - 8$.

24.5.1 Roots of Unity

We wish to identify the roots of the equation $x^d \equiv 1(\text{mod } p)$ where p is a prime.
We now use the Euler's formula $e^{\pi i} = -1$ proved in Theorem 119 on page 173. We observe for $x = e^{\frac{2\pi i}{d}k}$ that we can always have only $1 \leq k \leq d$ or d distinct values of x since any larger value of k reduces to $1 \leq k \leq d$ by using $e^{2\pi i} = 1$. For example, if $k = jd + f, f < d$ then.

$$e^{\frac{2\pi i(jd+f)}{d}} = (e^{2\pi i})^j \times e^{\frac{2\pi i f}{d}} = e^{\frac{2\pi i f}{d}} \text{ where } 1 \leq f \leq d.$$

These d solutions of $x^d = 1$ are the d^{th} roots of unity $e^{\frac{2\pi i}{d}k}, 1 \leq k \leq d$. Since there are d roots of the equation $x^d = 1$ then by Lemma 180 there can be no more.

We now show the roots of unity are a group.

Theorem 181.
The n^{th} roots of unity form a cyclic group under multiplication modulo n.

Proof. The n^{th} roots of unity are,

$$\{e^{2\pi i\frac{k}{n}} \mid 1 \leq k \leq n\} = \{e^{2\pi i\frac{1}{n}}, e^{2\pi i\frac{2}{n}}, \ldots, e^{2\pi i\frac{n}{n}} = 1\} =< e^{2\pi i\frac{1}{n}} >$$

Clearly this satisfies Definition 92, page 262, of a cyclic group generated by an element $a = e^{2\pi i\frac{1}{n}}$ since we have the replacements,

$$\{a, a^2, \ldots, a^n = e\} = \{e^{2\pi i\frac{1}{n}}, e^{2\pi i\frac{2}{n}}, \ldots, e^{2\pi i\frac{n}{n}} = e^{2\pi i} = 1\}$$

It remains to be proved it is a group. But we have,

- Closure: Consider $e^{2\pi i\frac{k}{n}} \cdot e^{2\pi i\frac{j}{n}} = e^{2\pi i\frac{j+k}{n}}$. Under multiplication modulo n we can have $j + k \leq n$ so the product is an element of the set.
- Identity: $e^{2\pi i\frac{n}{n}} = 1$.
- Inverses: $e^{2\pi i\frac{k}{n}} \cdot e^{2\pi i\frac{n-k}{n}} = 1$ so $e^{2\pi i\frac{k}{n}}$ has the inverse $e^{2\pi i\frac{n-k}{n}}$.
- Associativity: Obvious.

So the n^{th} roots of unity are a group. □

24.6 Conclusion

Theorem 182.
The multiplicative group $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$ is cyclic.

Proof. We will use Theorem 176 (3), page 263 to prove this, namely a finite group G is cyclic if and only if there is an element $a \in G$ of order $|a| = |G|$. Specifically we need to show there is an element $a \in \mathbb{Z}/p\mathbb{Z}$ such that $|a| = |\mathbb{Z}/p\mathbb{Z}| = p - 1$.
For any divisor $d \mid p - 1$ let $\Psi(d)$ be the number of elements of $\mathbb{Z}/p\mathbb{Z}$ of order d. By Theorem 181 the elements of $\mathbb{Z}/p\mathbb{Z}$ satisfying $x^d \equiv 1(\text{mod } p)$ form a group of order or size d. Now by Corollary 178, page 265, for any element of order c less than d we must have $c \mid d$. Thus we can separate out the elements of $\mathbb{Z}/p\mathbb{Z}$ into various subsets all of which have the same order c where $c \mid d$. Then the sum total of all the number of elements in all those subsets must equal d, or using $\Psi(c)$ is the number of elements of $\mathbb{Z}/p\mathbb{Z}$ of order c,

$$\sum_{c|d} \Psi(c) = d.$$

Now, by the Möbius Inversion Theorem 167 on page 253,

$$\sum_{c|d} \Psi(c) = d \Rightarrow \Psi(d) = \sum_{c|d} \mu(c)\frac{d}{c}$$

and by Corollary 172, page 257, we can use Euler's Totient function $\phi(n)$, specifically the result,

$$\phi(d) = \sum_{c|d} \mu(c)\frac{d}{c}$$

to show

$$\Psi(d) = \phi(d) \text{ for all } d|p-1$$

In particular,

$$\Psi(p-1) = \phi(p-1) > 1 \ for \ p > 2$$

or the number of elements of $\mathbb{Z}/p\mathbb{Z}$ of order $p - 1$ is $\phi(p-1)$.
Since the case $p = 2$ is trivial, we have shown in all cases the existence of an element of order $p - 1$.
Thus $\mathbb{Z}/p\mathbb{Z}$ is cyclic. □

Theorem 183.
Let p be a prime such that $x^2 + 1 \equiv 0(\text{mod } p)$ for some x. Then $p \equiv 1(\text{mod } 4)$.

Proof. Consider the multiplicative group $\mathbb{Z}/p\mathbb{Z}$
Since p is a prime, by Theorem 182 this group is cyclic. Then,

$$x^2 + 1 \equiv 0(\text{mod } p) \Rightarrow x^2 \equiv -1(\text{mod } p) \Rightarrow x^4 \equiv 1(\text{mod } p).$$

So x has order 4 in $\mathbb{Z}/p\mathbb{Z}$.
Since $|\mathbb{Z}/p\mathbb{Z}| = p-1$, by Theorem 179, page 266, we have,

$$\begin{aligned} 4 &= \frac{p-1}{gcd(p-1,4)} \\ &\Rightarrow p = 1 - 4 \times gcd(p-1,4) \\ &\Rightarrow p \equiv 1(\text{mod } 4). \end{aligned}$$

□

Theorem 184.
There are an infinite number of primes p of the form $p = 4n+1, n \in \mathbb{N}$ or $p \equiv 1(\text{ mod } 4)$.

Proof. Suppose there are only the finite number $5, 13, 17, \ldots, p_n$ of primes of the form $p = 4n+1, n \in \mathbb{N}$.
Consider $N = (2 \times 5 \times 13 \times 17 \times \cdots \times p_n)^2 + 1$.
Suppose p is a (necessarily odd) prime divisor of N.
Then since,

$$(2 \times 5 \times 13 \times 17 \times \cdots \times p_n)^2 + 1 \equiv 0(\text{mod } p)$$

by Theorem 183 we must have $p \equiv 1(\text{mod } 4)$.
Clearly $p \notin \{2, 5, 13, 17, \ldots, p_n\}$ since no element of this set divides N, each leaving a remainder of 1.
So we have a contradiction showing there are an infinite number of primes p of the form $p = 4n+1, n \in \mathbb{N}$ or $p \equiv 1(\text{mod } 4)$. □

Chapter 25

Primes of the form $4n+1$: Method 5

Our final proof there are an infinite number of primes of the form $4n + 1$ is due to Dirichlet. We are re-introduced to the Zeta function which is of fundamental importance in number theory. It was first studied by Euler as an elementary function and later as a complex function by Riemann.

This proof of the $4n + 1$ case is based on Dirichlet's general theorem regarding primes in arithmetic progressions. The proof of the general theorem is much more complicated.

Course: *Entrée VI*
Ingredients
The Euler Zeta Function $\zeta(s)$
The functions $\xi(m), L(s), Q(s)$
Directions
Prove the Euler product formula for $\zeta(s)$
Investigate the behavior of $\zeta(s)$ as $s \to \infty$
Follow Euler's proof on the infinitude of primes
Derive the product formulas for $L(s), Q(s)$
Follow Dirichlet's proofs of the $4n + 3$ and $4n + 1$ cases.

25.1 Zeta Function $\zeta(s)$

Definition 96. *Euler Zeta function*
The Euler Zeta function is defined by,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

For $s \in \mathbb{R}$, the function converges for all $s > 1$. This was the function studied by Euler. For $s \in \mathbb{C}$, the function converges for all s where $Re(s) > 1$. This was the function studied by Riemann.
Both convergence results may be proved by the Integral Test, Theorem 76 on page

104, for convergence of an infinite series[1]. You can earn a million dollar prize by being the first to prove the celebrated Riemann hypothesis concerning the zeros of the Riemann Zeta function. We will describe the challenge later.
In this chapter we need only the Euler Zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ which we discussed previously in Chapter 19 for values of $s = 2k, k \in \mathbb{Z}^+$.

Theorem 185. *(Euler product)*
For $p \in \mathbb{P}$, where $\mathbb{P}$ is the set of all primes, and $n \in \mathbb{N}$,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

where the product is over all primes.

Proof. For each value of n in $\sum_{n=1}^{\infty} \frac{1}{n^s}$ we have the unique factorization into products of prime numbers,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then .

$$\frac{1}{n^s} = \frac{1}{p_1^{\alpha_1}} \cdot \frac{1}{p_1^{\alpha_1}} \cdots \frac{1}{p_k^{\alpha_k}}.$$

Consider,

$$\left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \dots\right)\left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \dots\right) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right)$$

Each term $\frac{1}{n^s}$ is found once and only once among these products[2]. Thus,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right)$$

[1] To show $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges for $s > 1$ we need to show $\int_1^{\infty} \frac{1}{x^s} dx$ converges for $s > 1$. Now,

$$\int_1^{\infty} \frac{1}{x^s} dx = \int_1^{\infty} x^{-s}\ dx = \left[\frac{1}{-s+1} x^{-s+1}\right]_1^{\infty} = \begin{cases} \left[\frac{1}{s-1}\frac{1}{x^{s-1}}\right]_1^{\infty} = \frac{-1}{s-1} \text{ for } s > 1 \\ \left[\frac{1}{s-1}\frac{1}{x^{-s+1}}\right]_1^{\infty} = \infty \text{ for } s \le 1 \end{cases}$$

Hence the integral converges for $s > 1$ but not for $s \le 1$ and the infinite sum follows suit.

[2] This is so since by the Fundamental Theorem of Arithmetic any integer can be written as the product of powers of primes so, for example, if $n = 2^3 3^2 5^4$ then $\frac{1}{n^s} = \frac{1}{2^{3s} 3^{2s} 5^{4s}}$ so we can form $\frac{1}{n^s}$ by selecting $\frac{1}{2^{3s}}$ from the first product, $\frac{1}{3^{2s}}$ from the second, $\frac{1}{5^{4s}}$ from the third and 1 from every other term to ∞. We can clearly form any $\frac{1}{n^s}$ in a similar manner.

Each term on the right side is an infinite geometric series with first term $a = 1$ and common ratio $r = \dfrac{1}{p^s} < 1$ which can be summed by the formula,

$$S_\infty = \frac{a}{1-r} = \frac{1}{1-\dfrac{1}{p^s}}$$

Then,

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p \frac{1}{1-\dfrac{1}{p^s}} \tag{25.1.1}$$

which we call the Euler product decomposition. □

Lemma 186.

$$\lim_{s\to 1^+}\zeta(s) = +\infty$$

Proof.
$\zeta(s)$ is monotonic as a function of s by which we mean it is a constantly increasing function. It follows that $\lim\limits_{s\to 1^+}\zeta(s)$ is either ∞ or some finite number[3] k.
Suppose $\lim\limits_{s\to 1^+}\zeta(s) = k$. Then,

$$k \geq \lim_{s\to 1^+}\zeta(s) = \lim_{s\to 1+}\sum_{n=1}^{\infty}\frac{1}{n^s} = \sum_{n=1}^{\infty}\frac{1}{n}$$

In the limit as $s \to 1^+$ we would have $k > \sum\limits_{n=1}^{\infty}\dfrac{1}{n}$ for all $m > 1$.
But the right side is the harmonic series which does not converge[4], a contradiction to $\lim\limits_{s\to 1^+}\zeta(s) = k$.
Hence $\lim\limits_{s\to 1^+}\zeta(s) = +\infty$. □

Corollary 187.
The number of factors in the Euler product,

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p \frac{1}{1-\dfrac{1}{p^s}}$$

is infinite.

[3] $\sum\limits_{n=0}^{\infty}\dfrac{1}{2^n}$ is an example of a monotonic function with a finite limit (of 2).

[4] See Theorem 72 on page 101

Proof. If the number of factors in $\prod_p \dfrac{1}{1-\dfrac{1}{p^s}}$ is finite then,

$$\lim_{s\to 1^+}\zeta(s) = \lim_{s\to 1^+}\prod_p \frac{1}{1-\dfrac{1}{p^s}} = \prod_p \frac{1}{1-\dfrac{1}{p^1}} < \infty$$

which contradicts Lemma 186. □

25.2 Infinitude of Primes

We include here, in a corollary sense, an alternative proof due to Euler that there are an infinite number of primes. The proof requires the natural logarithm function. The proof also requires finding the limit of an infinite double sum so we will do that as an exercise.

Note 35. *We claim,*

$$\sum_p \sum_{n=2}^{\infty} \frac{1}{n}\cdot\frac{1}{p^{ns}} < 2 \text{ for } s \to 1^+.$$

We take each prime in turn so the contributions to this double sum are,

$$\begin{aligned}
p = 2 &: \frac{1}{2}\cdot\frac{1}{2^2} + \frac{1}{3}\cdot\frac{1}{2^3} + \frac{1}{4}\cdot\frac{1}{2^4} + \dots \\
p = 3 &: \frac{1}{2}\cdot\frac{1}{3^2} + \frac{1}{3}\cdot\frac{1}{3^3} + \frac{1}{4}\cdot\frac{1}{3^4} + \dots \\
p = 5 &: \frac{1}{2}\cdot\frac{1}{5^2} + \frac{1}{3}\cdot\frac{1}{5^3} + \frac{1}{4}\cdot\frac{1}{5^4} + \dots \\
&\dots
\end{aligned}$$

Although the contribution of each prime is a series of infinite terms we do not assume this series of contributions is infinite otherwise we assume our objective. We rearrange and substitute as follows with $s = 1$,

$$\sum_p \sum_{n=2}^{\infty} \frac{1}{n}\cdot\frac{1}{p^n} = \frac{1}{2}\left(\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{5^2}+\dots\right) + \frac{1}{3}\left(\frac{1}{2^3}+\frac{1}{3^3}+\frac{1}{5^3}+\dots\right) + \frac{1}{4}\left(\frac{1}{2^4}+\frac{1}{3^4}+\frac{1}{5^4}+\dots\right) + \dots$$

We create an inequality by adding in all natural numbers and not just the primes thus,

$$\begin{aligned}
\sum_p \sum_{n=2}^{\infty} \frac{1}{n}\cdot\frac{1}{p^n} < {} & \frac{1}{2}\left(\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{5^2}+\dots\right) + \frac{1}{3}\left(\frac{1}{2^3}+\frac{1}{3^3}+\frac{1}{5^3}+\dots\right) + \frac{1}{4}\left(\frac{1}{2^4}+\frac{1}{3^4}+\frac{1}{5^4}+\dots\right) \\
& + \frac{1}{5}\left(\frac{1}{2^5}+\frac{1}{3^5}+\frac{1}{5^5}+\dots\right) + \frac{1}{6}\left(\frac{1}{2^6}+\frac{1}{3^6}+\frac{1}{5^6}+\dots\right) + \frac{1}{7}\left(\frac{1}{2^7}+\frac{1}{3^7}+\frac{1}{5^7}+\dots\right) \\
& + \frac{1}{8}\left(\frac{1}{2^8}+\frac{1}{3^8}+\frac{1}{5^8}+\dots\right) + \dots
\end{aligned}$$

We drop off the leading fractions to give the stronger inequality,

$$\sum_p \sum_{n=2}^{\infty} \frac{1}{n} \cdot \frac{1}{p^n} < \left(\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \ldots\right) + \left(\frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{5^3} + \ldots\right) + \left(\frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{5^4} + \ldots\right)$$
$$+ \left(\frac{1}{2^5} + \frac{1}{3^5} + \frac{1}{5^5} + \ldots\right) + \left(\frac{1}{2^6} + \frac{1}{3^6} + \frac{1}{5^6} + \ldots\right) + \left(\frac{1}{2^7} + \frac{1}{3^7} + \frac{1}{5^7} + \ldots\right)$$
$$+ \left(\frac{1}{2^8} + \frac{1}{3^8} + \frac{1}{5^8} + \ldots\right) + \ldots$$

Note each of the ellipses ... now means we have an infinite number of terms in each pair of parentheses (...) and an infinite number of such pairs. We rearrange as folloows,

$$\sum_p \sum_{n=2}^{\infty} \frac{1}{n} \cdot \frac{1}{p^s} < \left(\frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \ldots\right) + \left(\frac{1}{3^2} + \frac{1}{3^3} + \frac{1}{3^4} + \ldots\right)\left(\frac{1}{4^2} + \frac{1}{4^3} + \frac{1}{4^4} + \ldots\right) + \ldots$$

Each of these bracketed terms is an infinite geometric series with a common ratio less than 1 so we have,

$$\begin{aligned}
&\sum_p \sum_{n=2}^{\infty} \frac{1}{n} \cdot \frac{1}{p^n} < \frac{\frac{1}{2^2}}{1-\frac{1}{2}} + \frac{\frac{1}{3^2}}{1-\frac{1}{3}} + \frac{\frac{1}{4^2}}{1-\frac{1}{4}} + \ldots + \frac{\frac{1}{n^2}}{1-\frac{1}{n}} + \ldots \\
&= \frac{1}{1\cdot 2} + \frac{1}{3\cdot 2} + \frac{1}{4\cdot 3} + \ldots + \frac{1}{n(n-1)} + \ldots \\
&< \frac{1}{1} + \frac{1}{2\cdot 2} + \frac{1}{3\cdot 3} + \ldots + \frac{1}{(n-1)(n-1)} + \ldots, \textit{ since } \frac{1}{n} < \frac{1}{n-1} \\
&= \sum_{n=2}^{\infty} \frac{1}{(n-1)^2} \\
&= \sum_{m=1}^{\infty} \frac{1}{m^2}, \textit{ where we put } m = n-1 \\
&= \zeta(2) = \frac{\pi^2}{6} \textit{ (See Theorem 149 page 225 and its Example.)} \\
&< 2
\end{aligned}$$

Theorem 188. *(Euler)*
The sum $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverges (so there are infinitely many primes).

Proof.

$$\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}}$$

so taking logs and using Note 25 on page 213 we have,

$$\log\zeta(s) = \log\prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_p \log\frac{1}{1-\frac{1}{p^s}} \tag{25.2.1}$$

Now[5] for $|x| < 1$,

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots \tag{25.2.2}$$

Integrating both sides with respect to x gives[6]

$$\log\frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \dots = \sum_{n=1}^{\infty}\frac{x^n}{n}$$

Substituting $x = \dfrac{1}{p^s}$ we have,

$$\log\frac{1}{1-\dfrac{1}{p^s}} = \sum_{n=1}^{\infty}\left(\frac{1}{p^s}\right)^n \cdot \frac{1}{n} \tag{25.2.3}$$

So substituting (25.2.1) into (25.2.3) we have,

$$\log\zeta(s) = \sum_p \log\frac{1}{1-\dfrac{1}{p^s}} = \sum_p\sum_{n=1}^{\infty}\left(\frac{1}{p^s}\right)^n \cdot \frac{1}{n} = \sum_p \frac{1}{p^s} + \sum_p\sum_{n=2}^{\infty}\frac{1}{n}\cdot\frac{1}{p^{ns}} < \sum_p\frac{1}{p^s} + 2,$$

since the double series on the right is less than 2 for $s > 1$ (See Note 35, page 274 and note obviously $\sum_p \frac{1}{p} > \sum_p \frac{1}{p^s}$ for all $s > 1$). Then,

$$\sum_p \frac{1}{p^s} > \log\zeta(s) - 2 \Rightarrow \sum_p\frac{1}{p^s} \to \infty$$

since $\log\zeta(s) \to \infty$ by Lemma 186. Hence there are infinitely many primes. □

25.3 Dirichlet's Proofs

We can now read Dirichlet's proof of the p=$4n+1$ case. As a bonus we also get his proof of the p=$4n+3$ case. We need some new notation and three new functions.

Notation 6.
For the even integers we use $\mathbb{E} = \{2n | n \in \mathbb{Z}\}$.
Note that even integers must be of the form $4n$ or $4n+2$.
For the odd integers we use $\mathbb{O} = \{2n+1 | n \in \mathbb{Z}\}.\}$
Note that odd integers must be of the form $4n+1$ or $4n+3$.

[5] This is just the sum of an infinite geometric series with $|r| = |x| < 1$.

[6] Using $\int \frac{g'(x)}{g(x)}\,dx = \log g(x)$ we have,

$$\int\frac{1}{1-x}\,dx = -\int\frac{-1}{1-x}\,dx = -\log(1-x) = \log 1 - \log(1-x) = \log\frac{1}{1-x}$$

25.3.1 The χ function

Definition 97. *chi function χ*

We define the function $\chi : \mathbb{Z} \to \mathbb{C}$ by $\chi(m) = \begin{cases} (-1)^{\frac{m-1}{2}}, & m \in \mathbb{O} \\ 0, & m \in \mathbb{E} \end{cases}$ where $\chi : \mathbb{Z} \to \mathbb{C}$ means χ maps or changes integers into complex numbers. So for the odd integers $\chi(4n+1) = 1$ and $\chi(4n+3) = -1$ and for all the even integers $\chi(2n) = 0$.

Lemma 189.
χ is a strictly multiplicative function, that is for all $m_i, m_j \in \mathbb{Z}$,

$$\chi(m_1 m_2) = \chi(m_1)\chi(m_2)$$

Proof. Let $m_1, m_2 \in \mathbb{Z}$. The cases where one is odd and the other even or both are even can be dealt with together. If either of $m_1, m_2 \in \mathbb{E}$ then $m_1 m_2 \in \mathbb{E}$ so that

$$\chi(m_1 m_2) = \chi(m_1)\chi(m_2) \text{ for all } m_j \in \mathbb{Z}$$

since both sides of the equation are 0.
The other case is if both $m_1, m_2 \in \mathbb{O}$ and then for $j = 1, 2$ we have $\chi(m_j) = \pm 1$ since we either have $(-1)^{\frac{4n+1-1}{2}} = +1$ or $(-1)^{\frac{4n-1-1}{2}} = -1$. The possibilities for $\chi(m_1 m_2)$ *and* $\chi(m_1)\chi(m_2)$ with $m_1, m_2 = 4n \pm 1$ are shown in this table.

m_1	m_2	$m_1 m_2$	$\chi(m_1)$	$\chi(m_2)$	$\chi(m_1)\cdot\chi(m_2)$	$\chi(m_1 m_2)$
$4n+1$	$4n+1$	$4n+1$	1	1	1	1
$4n+1$	$4n-1$	$4n-1$	1	-1	-1	-1
$4n-1$	$4n-1$	$4n+1$	-1	-1	1	1

In each case $\chi(m_1 m_2) = \chi(m_1)\chi(m_2)$ so the Lemma is true. □

25.3.2 The $L(s)$ and $Q(s)$ Functions

Dirichlet defined two functions $L(s)$ and $Q(s)$ related to the zeta function $\zeta(s)$. First,

$$\begin{aligned} Q(s) &= \left(1 - \frac{1}{2^s}\right)\zeta(s) \\ &= \left(1 - \frac{1}{2^s}\right)\sum_{n=1}^{\infty}\frac{1}{n^s} \\ &= \sum_{n=1}^{\infty}\frac{1}{n^s} - \sum_{n=1}^{\infty}\frac{1}{(2n)^s} \\ &= 1 + \frac{1}{3^s} + \frac{1}{5^s} + \dots \text{ since all the even values cancel} \\ &= \sum_{o \in \mathbb{O}}\frac{1}{o^s} \end{aligned}$$

where o runs over the positive odd integers.
$Q(s)$ has an Euler product decomposition as follows,

$$Q(s) = \left(1 - \frac{1}{2^s}\right)\sum_{n=1}^{\infty}\frac{1}{n^s} = \left(1 - \frac{1}{2^s}\right)\prod_{p}\frac{1}{1 - \dfrac{1}{p^s}} \text{ using (25.1.1)}$$

We extract the first term of the product to obtain,

$$Q(s) = \left(1 - \frac{1}{2^s}\right)\left(\frac{1}{1 - \dfrac{1}{2^s}}\right)\prod_{p>2}\frac{1}{1 - \dfrac{1}{p^s}}$$

$$\Rightarrow Q(s) = \prod_{p>2}\frac{1}{1 - \dfrac{1}{p^s}} \tag{25.3.1}$$

since the first term in 2^s cancels.
Second, he defined,

$$L(s) = \sum_{o\in\mathbb{O}}\frac{(-1)^{\frac{o-1}{2}}}{o^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} + \dots$$

For $o \in \mathbb{O}$ since we defined $\chi(m) = (-1)^{\frac{m-1}{2}}$, $m \in \mathbb{O}$ and $\chi(m) = 0$ for $m \in \mathbb{E}$, we can write,

$$L(s) = \sum_{m=1}^{\infty}\frac{\chi(m)}{m^s} = \sum_{o=1}^{\infty}\frac{\chi(o)}{o^s}$$

Then,

$$L(s) = \prod_{\substack{p\in\mathbb{P}\\ p\neq 2}}\frac{1}{1 - \dfrac{\chi(p)}{p^s}} \tag{25.3.2}$$

This is so since, similar to the proof of Theorem 185 on page 272,

$$\begin{aligned}
\prod_{\substack{p\in\mathbb{P}\\ p\neq 2}}\frac{1}{1 - \dfrac{\chi(p)}{p^s}} &= \prod_{\substack{p\in\mathbb{P}\\ p\neq 2}}\left(1 + \frac{\chi(p)}{p^s} + \left(\frac{\chi(p)}{p^s}\right)^2 + \left(\frac{\chi(p)}{p^s}\right)^3 + \dots\right) \\
&= 1 + \sum_{k_i=0}^{\infty}\prod_{\substack{p_i\in\mathbb{P}\\ p_i\neq 2}}\left(\frac{\chi(p_i)}{p_i^s}\right)^{k_i} \\
&= 1 + \sum_{k_i=0}^{\infty}\frac{\chi\left(\prod\limits_{\substack{p_i\in\mathbb{P}\\ p_i\neq 2}} p^{k_i}\right)}{\left(\prod\limits_{\substack{p_i\in\mathbb{P}\\ p_i\neq 2}} p^{k_i}\right)^s},
\end{aligned}$$

since χ is multiplicative.

$$= \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}$$

$$= L(s)$$

by the Fundamental Theorem of Arithmetic.

25.4 Proof of $4n+3$ Case

These new functions can be used to prove there are an infinite number of primes in the two arithmetic progressions $4n \pm 1$.

Theorem 190. *(Dirichlet)*
There are an infinite number of primes of the form $4n+3$.

Proof. We use (25.3.1) and (25.3.2) above and consider,

$$\frac{L(s)}{Q(s)} = \prod_{\substack{p\in\mathbb{P}\\ p\neq 2}} \frac{1-\dfrac{1}{p^s}}{1-\dfrac{\chi(p)}{p^s}} = \prod_{p\equiv 3(\mod 4)} \frac{1-\dfrac{1}{p^s}}{1+\dfrac{1}{p^s}}$$

since,

$$\chi(p) = +1 \ for \ p \equiv 1(\text{mod } 4)$$

thus cancelling all the terms with $p \equiv 1(\text{mod } 4)$ and because,

$$\chi(p) = -1 \ for \ p \equiv 3(\text{mod } 4)$$

then all the remaining denominator terms have $\chi(p) = -1$.
Now assume there are finitely many primes of the form $p \equiv 3(\text{mod } 4)$. Then, the product on the right is a finite product, hence well-defined at $s=1$ and certainly not equal to 0.
But at $s=1$, $\dfrac{L(s)}{Q(s)} \to 0$ since

$$\frac{L(s)}{Q(s)} = \frac{1-\dfrac{1}{3}+\dfrac{1}{5}-\dots}{1+\dfrac{1}{3}+\dfrac{1}{5}+\dots}$$

is an alternating[7] harmonic-like series (which converges) divided by an harmonic-like[8] series (which does not converge) giving, if you like, a constant divided by infinity. This is a contradiction, hence there are infinitely many primes $p \equiv 3(\text{mod } 4)$. □

[7] We can just say $\lim_{n\to\infty} \frac{1}{n} = 0$ so this series converges

[8] Similar to the proof that the harmonic series does not converge given in Theorem 72 on page

25.5 Proof of $4n+1$ Case

Theorem 191. *(Dirichlet)*
There are an infinite number of primes of the form $p \equiv 1 (\text{mod } 4)$.

Proof. Using (25.3.1) and (25.3.2) consider,

$$\begin{aligned}
\frac{Q(2s)}{Q(s)L(s)} &= \prod_{\substack{p\in\mathbb{P}\\ p\neq 2}} \frac{\left(1-\dfrac{1}{p^s}\right)\left(1-\dfrac{\chi(p)}{p^s}\right)}{\left(1-\dfrac{1}{p^{2s}}\right)} \\
&= \prod_{\substack{p\in\mathbb{P}\\ p\neq 2}} \frac{\left(1-\dfrac{1}{p^s}\right)\left(1-\dfrac{\chi(p)}{p^s}\right)}{\left(1-\dfrac{1}{p^s}\right)\left(1+\dfrac{1}{p^s}\right)} \\
&= \prod_{\substack{p\in\mathbb{P}\\ p\neq 2}} \frac{1-\dfrac{\chi(p)}{p^s}}{1+\dfrac{1}{p^s}} \\
&= \prod_{p\equiv 1(\text{ mod } 4)} \frac{1-\dfrac{1}{p^s}}{1+\dfrac{1}{p^s}}
\end{aligned}$$

since $\chi(p) = -1$ for $p \equiv 3(\text{mod } 4)$ and $\chi(p) = +1$ for $p \equiv 1(\text{mod } 4)$ so that all the terms with $p \equiv 3(\text{ mod } 4)$ will cancel out and all the remaining numerator terms have $\chi(p) = +1$.
Now assume there are finitely many primes $p \equiv 1(\text{mod } 4)$. Then, the product on the right is a finite product, hence well-defined at $s = 1$ and certainly not equal to 0. But (we build the contradiction),

$$Q(2) = \sum_{o\in\mathbb{O}} \frac{1}{o^2} = \frac{1}{1^2} + \frac{1}{3^2} + \frac{1}{5^2} + \ldots < \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots$$

101, we group the terms and replace each term in a group by the end group element of the form $\frac{1}{3^n}$. Thus,

$$\begin{aligned}
&1 + \frac{1}{3} + (\frac{1}{5} + \frac{1}{7} + \frac{1}{9}) + (\frac{1}{11} + \frac{1}{13} + \ldots + \frac{1}{27}) + (\frac{1}{29} + \ldots + \frac{1}{81}) + \ldots \\
&> 1 + \frac{1}{3} + (\frac{1}{9} + \frac{1}{9} + \frac{1}{9}) + (\frac{1}{27} + \frac{1}{27} + \ldots + \frac{1}{27}) + (\frac{1}{81} + \ldots + \frac{1}{81}) + \ldots \\
&> 1 + \frac{1}{3} + \frac{1}{3} + \frac{1}{3} + \ldots \\
&\to \infty
\end{aligned}$$

which is a convergent p–series[9] with $p > 1$ and,

$$L(1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \ldots = 1 - \frac{1}{3} + \left(\frac{1}{5} - \frac{1}{7}\right) + \left(\frac{1}{9} - \frac{1}{11} +\right) + \ldots > \frac{2}{3},$$

since all the paired terms following $1 - \dfrac{1}{3}$ are positive. Also, from the definition of $Q(s)$,

$$\lim_{s \to 1} Q(s) = \lim_{s \to 1} \left(1 - \frac{1}{2^s}\right) \zeta(s) = \infty \text{ by Lemma 186, page 273}$$

Therefore if we write $\lim_{s \to 1} Q(s) = Q$ and $\lim_{s \to 1} L(s) = L$ then

$$\lim_{s \to 1} \frac{Q(2s)}{L(s)Q(s)} = \frac{Q(2)}{L(1)Q(1)} = \frac{Q}{L \times \infty} = 0$$

This is a contradiction, hence there are infinitely many primes $p \equiv 1 (\text{mod } 4)$. □

[9] Refer to Theorem 79 on page 112.

Part IX

Sorbet – Gamma Function

A sorbet to cleanse the palate.

The final new function we will discuss is the Gamma Function, initially developed separately by Euler and Weierstrasse, although as we shall see, their definitions prove to be equivalent. The challenge was to find a continuous function of a variable that was the same as factorial $n, (n!)$, when the variable took positive integer values. Achievements of this kind are remarkable.

Applications of the Gamma Function are numerous. One we will consider later is in connection with the Riemann Zeta function and the famous Riemann Hypothesis.

Chapter 26

Gamma Function

Course: Sorbet
Ingredients
Euler-Mascheroni Constant emanating from the harmonic series
Calculus on the complex plane
Weierstrasse Gamma Function
Euler Gamma Function
Directions
Prove the lemma properties of the Weierstrasse Gamma Function.
Prove the equivalence of the Weierstrasse and Euler Gamma Functions.
Prove the duplication formula.

We start with further consideration of the harmonic series $\sum\limits_{n=1}^{\infty} \dfrac{1}{n}$ which we have already proved (in Theorem 72, page 101) is not convergent. However, its divergence is very slow, paralleling the divergence of $\log x$ as $x \to \infty$. Indeed their difference is a small constant.

26.1 Euler-Mascheroni Constant

Definition 98. *Euler-Macheroni constant*
The Euler-Mascheroni constant γ is defined by,

$$\gamma = \lim_{m\to\infty}\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{m}-\log m\right) = 0.5772157\ldots$$

Lemma 192.
The constant γ exists.

Proof.

Consider,

$$\begin{aligned} u_n = \int_0^1 \frac{t}{n(n+t)}\ dt &= \int_0^1 \frac{1}{n}\ dt - \int_0^1 \frac{1}{n+t}\ dt \\ &= \left[\frac{1}{n}t - \log(n+t)\right]_0^1 \\ &= \frac{1}{n} - (\log(n+1) - \log n) \end{aligned}$$

Hence, noting $\log 1 = 0$,

$$\begin{aligned} \sum_{n=1}^{m} u_n &= \sum_{n=1}^{m} \frac{1}{n} - \sum_{n=1}^{m} (\log(n+1) - \log n) \\ &= \sum_{n=1}^{m} \frac{1}{n} - (\cancel{\log 2} - \log 1 + \xcancel{\log 3} - \cancel{\log 2} + \log 4 - \xcancel{\log 3} + \ldots + \\ &\qquad + \cancel{\log m} - \xcancel{\log(m-1)} + \log(m+1) - \cancel{\log m}) \\ &= \sum_{n=1}^{m} \frac{1}{n} - \log(m+1) \\ \Rightarrow \sum_{n=1}^{m} u_n + \log(m+1) &= \frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{m} \end{aligned}$$

Therefore subtracting $\log m$ from both sides and taking the limit as $m \to \infty$ we have,

$$\begin{aligned} \lim_{m\to\infty}\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{m} - \log m\right) &= \lim_{m\to\infty}\left(\sum_{n=1}^{m} u_n + \log(m+1) - \log m\right) \\ &= \lim_{m\to\infty} \sum_{n=1}^{m} u_n + \lim_{m\to\infty} \log\left(\frac{m+1}{m}\right) \\ &= \sum_{n=1}^{\infty} u_n, \end{aligned} \tag{26.1.1}$$

since $\lim\limits_{m\to\infty} \log\left(\dfrac{m+1}{m}\right) = \lim\limits_{m\to\infty} \log(1 + \dfrac{1}{m}) = \log 1 = 0$.

Now for $t \in [0,1]$ we have $\dfrac{t}{n(n+t)} < \dfrac{1}{n^2}$.

So $u_n = \int\limits_0^1 \dfrac{t}{n(n+t)}\ dt$ is positive and less than $\int\limits_0^1 \dfrac{1}{n^2}\ dt = \dfrac{1}{n^2}$ and therefore, by the $p-$ test[1], $\sum\limits_{n=1}^{\infty} u_n$ converges and by (26.1.1) since,

$$\lim_{m\to\infty}\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{m} - \log m\right) = \sum_{n=1}^{\infty} u_n,$$

then $\lim\limits_{m\to\infty}\left(\dfrac{1}{1} + \dfrac{1}{2} + \dfrac{1}{3} + \ldots + \dfrac{1}{m} - \log m\right)$ converges to a finite number we call γ. □

[1] See Theorem 77, page 105

26.2 Observations on Calculus on the Complex Plane

We will be dealing with complex numbers and the complex number plane. We have not discussed differentiation on the complex plane, but it is sufficient to note that,

1. Differentiable real functions parallel holomorphic complex functions and,

2. Division by zero or multiples of zero occurring at a real point of a function of a real variable corresponds to simple poles or poles of higher order occurring at a complex point of a function of a complex variable.

Definition 99. *holomorphic function*
A holomorphic function is a complex-valued function of one or more complex variables that is differentiable in a neighborhood of every point in its domain. We will also call such functions analytic functions if the function has only one variable.

Definition 100. *pole*
A function f has a pole of order n at a point $z = z_0$ if $f(z) = \dfrac{g(z)}{(z-z_0)^n}$ and $(z-z_0)\nmid g(z)$ where $g(z)$ is a holomorphic function.
Accordingly the function $(z-z_0)^n f(z)$ is also holomorphic.
If $n = 1$, we say f has a simple pole at $z = z_0$.

Example 120.
$f(z) = \dfrac{1}{z}$ has a simple pole at $z = 0$ since $zf(z) = 1$ and $\dfrac{d}{dz}(zf(z)) = 0$ exists at $z = 0$.
$f(z) = \dfrac{z^2}{(z-1)^3}$ has a pole of order 3 at $z = 1$ and $\dfrac{d}{dx}(z-1)^3 f(z) = \dfrac{d}{dx} z^2 = 2z$ exists at $z = 1$.

Let us proceed.

26.3 Weierstrasse Gamma Function

Definition 101. *The Gamma Function $\Gamma(z)$ defined by Weierstrasse is,*

$$\frac{1}{\Gamma(z)} = ze^{\gamma z} \prod_{n=1}^{\infty} \left\{ \left(1 + \frac{z}{n}\right) e^{-\frac{z}{n}} \right\}, \ z \in \mathbb{C}$$

where γ is the Euler-Mascheroni constant.

Obviously, inverting the definition, $\Gamma(z)$ is analytic or holomorphic everywhere except at $z = 0$ and for any values of n for which $\dfrac{z}{n} = -1$, that is at $z = -1, -2, \dots$ since we can at the same time have $n = 1, 2, \dots$.
We can now build the lemmas and theorems resulting from this definition.

Lemma 193.

$$\Gamma(1) = 1$$

Proof. Noting $\gamma = \lim_{m\to\infty}\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{m}-\log m\right)$,

$$\begin{aligned}
\frac{1}{\Gamma(1)} &= e^{\gamma}\prod_{n=1}^{\infty}\left\{\left(1+\frac{1}{n}\right)e^{-\frac{1}{n}}\right\}\\
&= \lim_{m\to\infty}\left\{e^{\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{m}-\log m}\left[\left(1+\frac{1}{1}\right)e^{-\frac{1}{1}}\right]\left[\left(1+\frac{1}{2}\right)e^{-\frac{1}{2}}\right]\cdots\left[\left(1+\frac{1}{m}\right)e^{-\frac{1}{m}}\right]\right\}\\
&= \lim_{m\to\infty} e^{-logm}\left(\frac{\cancel{2}}{1}\times\frac{3}{\cancel{2}}\times\cdots\times\frac{m+1}{\cancel{m}}\right)\\
&\text{since all the exponentials } e^{\frac{1}{m}}\text{, etc. cancel}\\
&= \lim_{m\to\infty}\left(\frac{m+1}{m}\right) \text{ since } e^{-\log m} = e^{\log\frac{1}{m}} = \frac{1}{m}\\
&= \lim_{m\to\infty}\left(1+\frac{1}{m}\right) = 1
\end{aligned}$$

□

Lemma 194.

$$\Gamma'(1) = -\gamma$$

Proof. Taking logs of both sides of,

$$\frac{1}{\Gamma(z)} = ze^{\gamma z}\prod_{n=1}^{\infty}\left\{\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right\}$$

we obtain,

$$-\log\Gamma(z) = \log z + \log e^{\gamma z} + \sum_{n=1}^{\infty}\left\{\log\left(1+\frac{z}{n}\right)+\log e^{-\frac{z}{n}}\right\}$$

Differentiating both sides with respect to z and noting $\log e^{\gamma z} = \gamma z$ and $\log e^{-\frac{z}{n}} = -\frac{z}{n}$ gives,

$$-\frac{\Gamma'(z)}{\Gamma(z)} = \frac{1}{z}+\gamma+\sum_{n=1}^{\infty}\left(\frac{\frac{1}{n}}{1+\frac{z}{n}}-\frac{1}{n}\right)$$

Then,

$$\begin{aligned}
-\frac{\Gamma'(1)}{\Gamma(1)} &= 1+\gamma-\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right)\\
&= 1+\gamma-\left(\frac{1}{1}-\cancel{\frac{1}{2}}+\cancel{\frac{1}{2}}-\cancel{\frac{1}{3}}+\cancel{\frac{1}{3}}-\cancel{\frac{1}{4}}+\cancel{\frac{1}{4}}-\ldots\right)\\
&= \gamma
\end{aligned}$$

By Lemma 193, $\Gamma'(1) = -\gamma$. □

In the next lemma we use a "trick", namely, $m = \prod_{n=1}^{m-1}\left(1+\frac{1}{n}\right)$ since,

$$\left(1+\frac{1}{1}\right)\left(1+\frac{1}{2}\right)\left(1+\frac{1}{3}\right)\cdots\left(1+\frac{1}{m-1}\right) = \cancel{2}\cdot\frac{\cancel{3}}{\cancel{2}}\cdot\frac{4}{\cancel{3}}\cdots\frac{\cancel{m-1}}{m-2}\cdot\frac{m}{\cancel{m-1}} = m$$

so we have the result we will use below,

$$m^{-z} = \prod_{n=1}^{m-1}\left(1+\frac{1}{n}\right)^{-z}$$

Lemma 195. *(Euler)*

$$\Gamma(z) = \frac{1}{z}\prod_{n=1}^{\infty}\left\{\left(1+\frac{1}{n}\right)^{z}\left(1+\frac{z}{n}\right)^{-1}\right\} \text{ provided } z \neq 0,-1,-2,\ldots.$$

Proof.
We substitute $\gamma = \lim_{m\to\infty}\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{m}-\log m\right)$ into the definition of $\frac{1}{\Gamma(z)}$,

$$\frac{1}{\Gamma(z)} = ze^{\gamma z}\prod_{n=1}^{\infty}\left\{\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right\}$$

$$= z\left[\lim_{m\to\infty} e^{\left(1+\frac{1}{2}+\ldots+\frac{1}{m}-\log m\right)z}\right]\left[\lim_{m\to\infty}\prod_{n=1}^{\infty}\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right]$$

$$= z\lim_{m\to\infty}\left[e^{-z\log m}e^{\left(1+\frac{1}{2}+\ldots+\frac{1}{m}\right)z}e^{\left(-\frac{1}{1}\right)z}e^{\left(-\frac{1}{2}\right)z}\cdots e^{\left(-\frac{1}{m}\right)z}\prod_{n=1}^{m}\left(1+\frac{z}{n}\right)\right]$$

$$= z\lim_{m\to\infty}\left[m^{-z}\prod_{n=1}^{m}\left(1+\frac{z}{n}\right)\right]$$

since $e^{-z\log m} = -m^{z}$ and all the powers of e^{z} cancel.

$$= z\lim_{m\to\infty}\left[\prod_{n=1}^{m-1}\left(1+\frac{1}{n}\right)^{-z}\prod_{n=1}^{m}\left(1+\frac{z}{n}\right)\right] \text{ where we used the "trick" above.}$$

$$= z\lim_{m\to\infty}\left[\left(1+\frac{1}{m}\right)^{z}\cdot\left(1+\frac{1}{m}\right)^{-z}\cdot\prod_{n=1}^{m-1}\left(1+\frac{1}{n}\right)^{-z}\cdot\prod_{n=1}^{m}\left(1+\frac{z}{n}\right)\right]$$

where we multiplied by the first two terms which are inverses so we could increase the first product thus,

$$= z\lim_{m\to\infty}\left[\left(1+\frac{1}{m}\right)^{z}\cdot\prod_{n=1}^{m}\left(1+\frac{1}{n}\right)^{-z}\cdot\prod_{n=1}^{m}\left(1+\frac{z}{n}\right)\right]$$

$$= z\lim_{m\to\infty}\left[\prod_{n=1}^{m}\left(1+\frac{1}{n}\right)^{-z}\cdot\prod_{n=1}^{m}\left(1+\frac{z}{n}\right)\right]$$

since $\lim_{m\to\infty}\left(1+\frac{1}{m}\right)^{z} = 0.$

$$\Rightarrow \Gamma(z) = \frac{1}{z}\prod_{n=1}^{\infty}\left[\left(1+\frac{1}{n}\right)^{z}\left(1+\frac{z}{n}\right)^{-1}\right]$$

provided $z \neq 0, -1, -2, \ldots$ so (there is no division by 0 when $n = 1, 2, \ldots$). □

Theorem 196.

$$\Gamma(z+1) = z\Gamma(z) \quad \textit{if } z \neq 0, -1, -2, \ldots.$$

Proof.
By definition,

$$\begin{aligned}\frac{1}{\Gamma(z)} &= ze^{\gamma z}\prod_{n=1}^{\infty}\left\{\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right\}\\ &= ze^{\gamma z}\lim_{m\to\infty}\prod_{n=1}^{m}\left\{\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right\}\end{aligned}$$

Hence,

$$\begin{aligned}\frac{\Gamma(z+1)}{\Gamma(z)} &= \frac{ze^{\gamma z}\prod_{n=1}^{\infty}\left\{\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right\}}{(z+1)e^{\gamma(z+1)}\prod_{n=1}^{\infty}\left\{\left(1+\frac{z+1}{n}\right)e^{-\frac{z+1}{n}}\right\}}\\ &= \frac{z}{z+1}e^{-\gamma}\lim_{m\to\infty}\prod_{n=1}^{m}\left\{\left(\frac{z+n}{z+n+1}\right)e^{\frac{1}{n}}\right\}\\ &= \frac{z}{z+1}\lim_{m\to\infty}\prod_{n=1}^{m}e^{-\gamma+\frac{1}{1}+\frac{1}{2}+\cdots}\left(\frac{z+n}{z+n+1}\right)\\ &= \frac{z}{z+1}\lim_{m\to\infty}\prod_{n=1}^{m}e^{\log m}\left(\frac{z+n}{z+n+1}\right)\\ &\text{where we used } \gamma = \lim_{m\to\infty}\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{m}-\log m\right).\\ &= \frac{z}{\cancel{z+1}}\lim_{m\to\infty}\left(m\cdot\frac{\cancel{z+1}}{\cancel{z+2}}\cdot\frac{\cancel{z+2}}{z+3}\cdots\frac{z+m-1}{\cancel{z+m}}\cdots\frac{\cancel{z+m}}{z+m+1}\right)\\ &\text{where we used } e^{\log m} = m\\ &= z\lim_{m\to\infty}\left(\frac{m}{z+m+1}\right)\\ &= z\end{aligned}$$

since $\lim_{m\to\infty}\dfrac{m}{m+z+1} = \lim_{m\to\infty}\dfrac{1}{1+\dfrac{z}{m}+\dfrac{1}{m}} = 1.$ □

Corollary 197.

$$\Gamma(n+1) = n! \textit{ for } \; n \in \mathbb{N}$$

Proof.

$$\Gamma(n+1) = n\Gamma(n) = n(n-1)\Gamma(n-1) = \ldots = n(n-1)(n-2)\cdots\Gamma(1) = n!$$

□

We now express the gamma function as an infinite fraction.

Theorem 198.

$$\Gamma(z) = \lim_{n\to\infty} \frac{n!}{z(z+1)(z+2)\cdots(z+n)} n^z \tag{26.3.1}$$

Proof.
By Lemma 195,

$$\begin{aligned}
\Gamma(z) &= \frac{1}{z}\prod_{n=1}^{\infty}\left\{\left(1+\frac{1}{n}\right)^z\left(1+\frac{z}{n}\right)^{-1}\right\} \\
&= \lim_{m\to\infty}\frac{1}{z}\cdot\left(1+\frac{1}{1}\right)^z\cdot\left(1+\frac{1}{2}\right)^z\cdots\left(1+\frac{1}{m}\right)^z\cdot\left(1+\frac{z}{1}\right)^{-1}\times\left(1+\frac{z}{2}\right)^{-1}\cdots\left(1+\frac{z}{m}\right)^{-1} \\
&= \lim_{m\to\infty}\frac{1}{z}\cdot\cancel{2^z}\cdot\frac{\cancel{3^z}}{\cancel{2^z}}\cdot\cdots\cdot\frac{(m+1)^z}{\cancel{m^z}}\times\frac{1}{1+z}\cdot\frac{2}{2+z}\cdots\frac{m}{m+z} \\
&= \lim_{m\to\infty}\frac{m!(m+1)^z}{z(1+z)(2+z)\cdots(m+z)}
\end{aligned}$$

We put $n-1=m$,

$$= \lim_{n\to\infty}\frac{(n-1)!n^z}{z(z+1)(z+2)\cdots(n+z-1)}$$

Another "trick" - we multiply by $\lim_{n\to\infty}\frac{n}{n+z} = 1$.

$$\begin{aligned}
&= \lim_{n\to\infty}\frac{n}{n+z}\cdot\frac{(n-1)!n^z}{z(z+1)(z+2)\cdots(n+z-1)} \\
&= \lim_{n\to\infty}\frac{n!}{z(z+1)(z+2)\cdots(z+n)}n^z
\end{aligned}$$

□

The proof of this next "famous" lemma needs complex analysis at least up to the residue theorem. That was not available to Euler. He argued, some say "recklessly", as follows. For the purists we proved the Lemma rigorously as Equation (19.2.6) of Theorem 147 on page 222 with $z = \pi x$.

Lemma 199. *(Euler)*

$$\frac{\sin z}{z} = \prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right)$$

Proof. From Theorem 118, page 172,

$$\begin{aligned} \sin z &= z - \frac{z^3}{3!} + \frac{z^5}{5!} - \dots \\ \Rightarrow \frac{\sin z}{z} &= 1 - \frac{z^2}{3!} + \frac{z^4}{5!} + \dots \\ &= (1-a_1)(1-a_2)\cdots \text{ ("recklessly" saying an infinite sum factors)} \end{aligned}$$

Now we proved in Theorem 112 on page 164 that $\lim_{z\to 0} \frac{\sin z}{z} = 1$. We know[2] $\sin z$ has an infinite number of zeros at $0, \pm\pi, \pm 2\pi, \dots$ and therefore the factors of $\frac{\sin z}{z}$ must be the pairs,

$$\begin{aligned} \frac{\sin z}{z} &= \overbrace{\left(1-\frac{z}{\pi}\right)\left(1+\frac{z}{\pi}\right)}\overbrace{\left(1-\frac{z}{2\pi}\right)\left(1+\frac{z}{2\pi}\right)}\cdots \\ &= \left(1-\frac{z^2}{\pi^2}\right)\left(1-\frac{z^2}{(2\pi)^2}\right)\cdots \\ &= \prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right) \qquad (26.3.2) \end{aligned}$$

□

Theorem 200.

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}$$

Proof.
We can invert Euler's (26.3.2) above into,

$$\frac{z}{\sin z} = \prod_{n=1}^{\infty} \frac{1}{\left(1-\frac{z^2}{n^2\pi^2}\right)}$$

and then replace z with πz to obtain,

$$\frac{\pi z}{\sin \pi z} = \prod_{n=1}^{\infty} \frac{1}{\left(1-\frac{z^2}{n^2}\right)} \qquad (26.3.3)$$

Now, by Theorems 196 and 198,

$$\Gamma(z+1) = z\Gamma(z) = \lim_{n\to\infty} \frac{n!}{(z+1)(z+2)\cdots(z+n)} n^z \qquad (26.3.4)$$

[2] See Note 22 on page 160

Let $n^z = e^{z \log n}$ and use Euler-Mascheroni's constant $\gamma = \lim_{n\to\infty}\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}-\log n\right)$ so that,

$$\lim_{n\to\infty} n^z = \lim_{n\to\infty} e^{z\log n} = \lim_{n\to\infty} e^{z\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}-\gamma\right)} \tag{26.3.5}$$

Then, distributing the terms in (26.3.5) across (26.3.4) and unpacking $n!$ we have,

$$\begin{aligned}\Gamma(z+1) &= \lim_{n\to\infty} e^{-\gamma z}\left(\frac{1\cdot e^z}{1+z}\right)\left(\frac{2\cdot e^{\frac{z}{2}}}{2+z}\right)\left(\frac{3\cdot e^{\frac{z}{3}}}{3+z}\right)\cdots\left(\frac{n\cdot e^{\frac{z}{n}}}{n+z}\right)\\ &= e^{-\gamma z}\lim_{n\to\infty}\left(\frac{e^z}{1+z}\right)\left(\frac{e^{\frac{z}{2}}}{1+\frac{z}{2}}\right)\left(\frac{e^{\frac{z}{3}}}{1+\frac{z}{3}}\right)\cdots\left(\frac{e^{\frac{z}{n}}}{1+\frac{z}{n}}\right)\\ &= e^{-\gamma z}\prod_{n=1}^{\infty}\frac{e^{\frac{z}{n}}}{1+\frac{z}{n}} \qquad (26.3.6)\end{aligned}$$

So, putting $z = -z$,

$$\Gamma(1-z) = e^{\gamma z}\prod_{n=1}^{\infty}\frac{e^{\frac{-z}{n}}}{1-\frac{z}{n}} \tag{26.3.7}$$

Now, $\Gamma(z+1) = z\Gamma(z)$ so we have from (26.3.6) and (26.3.7) both,

$$\Gamma(z) = \frac{\Gamma(z+1)}{z} = \frac{e^{-\gamma z}}{z}\prod_{n=1}^{\infty}\frac{e^{\frac{z}{n}}}{1+\frac{z}{n}}, \tag{26.3.8}$$

and using $\Gamma(1-z) = -z\Gamma(z)$,

$$\Gamma(-z) = \frac{\Gamma(1-z)}{-z} = \frac{e^{\gamma z}}{-z}\prod_{n=1}^{\infty}\frac{e^{\frac{-z}{n}}}{1-\frac{z}{n}} \tag{26.3.9}$$

Then by (26.3.8) and (26.3.9),

$$\begin{aligned}\Gamma(z)\Gamma(-z) &= \left(\frac{e^{-\gamma z}}{z}\prod_{n=1}^{\infty}\frac{e^{\frac{z}{n}}}{1+\frac{z}{n}}\right)\left(\frac{e^{\gamma z}}{-z}\prod_{n=1}^{\infty}\frac{e^{\frac{-z}{n}}}{1-\frac{z}{n}}\right)\\ &= -\frac{1}{z^2}\prod_{n=1}^{\infty}\left(\frac{1}{1-\frac{z^2}{n^2}}\right)\\ &= -\frac{1}{z^2}\frac{\pi z}{\sin \pi z} \text{ by (26.3.3) of Theorem 200,}\\ &= -\frac{\pi}{z\sin\pi z}\end{aligned}$$

Hence substituting,

$$\Gamma(z+1) = z\Gamma z \Rightarrow \Gamma(-z+1) = -z\Gamma(-z) \Rightarrow \Gamma(-z) = \frac{\Gamma(1-z)}{-z}$$

we have,

$$\Gamma(z)\frac{\Gamma(1-z)}{-z} = -\frac{\pi}{z\sin \pi z} \qquad (26.3.10)$$

$$\Rightarrow \Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z} \qquad (26.3.11)$$

□

Corollary 201.

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$$

Proof.
Put $z = \frac{1}{2}$ in formula (26.3.11) of the above theorem, note $\sin\frac{\pi}{2} = 1$, to obtain,

$$\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{1}{2}\right) = \frac{\pi}{\sin\frac{\pi}{2}} = \pi \Rightarrow \Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$$

□

26.4 Euler Gamma Function

Euler defined the Gamma Function by,

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\ dt$$

We will now show the Euler and Weierstrasse definitions of the Gamma Function are actually the same, that is,

$$\Gamma(z) = \frac{e^{-\gamma z}}{z}\prod_{n=1}^{\infty}\frac{e^{\frac{z}{n}}}{1+\dfrac{z}{n}} = \int_0^\infty e^{-t}t^{z-1}\ dt$$

We begin with a lemma.

Lemma 202.

$$\lim_{n\to\infty}\left[e^{-t} - \left(1-\frac{t}{n}\right)^n\right] = 0$$

$$\Rightarrow e^{-t} = \lim_{n\to\infty}\left(1-\frac{t}{n}\right)^n$$

$$\Rightarrow e^{t} = \lim_{n\to\infty}\left(1+\frac{t}{n}\right)^n \quad \textit{by putting } -t = t$$

Proof.
Consider,

$$\begin{aligned} f(x) &= t\log x \\ \Rightarrow f'(x) &= \frac{t}{x} \\ \Rightarrow f'(1) &= t. \end{aligned}$$

Then, by definition of the derivative evaluated at $x = 1$,

$$\begin{aligned} t = f'(1) &= \lim_{h\to 0}\frac{f(x+h)-f(x)}{h}\bigg|_{x=1} \\ &= \lim_{h\to 0}\frac{t\log(x+h)-t\log x}{h}\bigg|_{x=1} \\ &= \lim_{h\to 0}\frac{t\log(1+h)-t\log 1}{h} \\ &= \lim_{h\to 0}\frac{t\log(1+h)-0}{h} \\ &= \lim_{h\to 0}\frac{t}{h}\log(1+h) \\ \Rightarrow t &= \lim_{h\to 0}\log(1+h)^{\frac{t}{h}} \end{aligned} \tag{26.4.1}$$

Then, assuming we can take a limit inside and using $e^{\log x} = x$,

$$\begin{aligned} \lim_{h\to 0}(1+h)^{\frac{t}{h}} &= \lim_{h\to 0} e^{\log(1+h)^{\frac{t}{h}}} \\ &= e^{\lim\limits_{h\to 0}\log(1+h)^{\frac{t}{h}}} \\ &= e^t \ by\ (26.4.1) \end{aligned}$$

Putting $h = \dfrac{t}{n}$, and noting $h \to 0 \Rightarrow n \to \infty$. we get,

$$e^t = \lim_{n\to\infty}\left(1+\frac{t}{n}\right)^n \text{ and } e^{-t} = \lim_{n\to\infty}\left(1-\frac{t}{n}\right)^n \tag{26.4.2}$$

□

Theorem 203. *(Equivalence of the Euler and Weierstrasse Definitions)*

$$\Gamma(z) = \frac{e^{-\gamma z}}{z}\prod_{n=1}^{\infty}\frac{e^{\frac{z}{n}}}{1+\dfrac{z}{n}} \Leftrightarrow \Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\ dt$$

Proof. Let,

$$\Pi(z,n) = \int_0^n \left(1-\frac{t}{n}\right)^n\ t^{z-1}\ dt$$

Putting $t = nr$ we have both $dt = n\ dr$ and $0 \leq t \leq n$ replaced by $0 \leq r \leq 1$. We obtain,

$$\Pi(z,n) = n^z \int_0^1 (1-r)^n r^{z-1}\ dr$$

We use repeated integration by parts noting the variable is r.
First, putting $u = (1-r)^n, v' = r^{z-1} \Rightarrow u' = -n(1-r)^{n-1}, v = \frac{r^z}{z}$ we have,

$$\begin{aligned}\Pi(z,n) &= \left(\left[\frac{r^z}{z}(1-r)^n\right]_0^1 + \frac{n}{z}\int_0^1 (1-r)^{n-1} r^z\ dr\right) n^z \\ &= 0 + \left(\frac{n}{z}\int_0^1 (1-r)^{n-1} r^z\ dr\right) n^z\end{aligned}$$

Next, putting $u = (1-r)^{n-1}, v' = r^z \Rightarrow u' = -(n-1)(1-r)^{n-2}, v = \frac{r^{z+1}}{z+1}$ we have,

$$\begin{aligned}\Pi(z,n) &= \left(\left[\frac{r^{z+1}}{z}(1-r)^{n-1}\right]_0^1 + \frac{n}{z}\cdot\frac{n-1}{z+1}\int_0^1 (1-r)^{n-2} r^{z+1}\ dr\right) n^z \\ &= 0 + \left(\frac{n}{z}\cdot\frac{n-1}{z+1}\int_0^1 (1-r)^{n-2} r^{z+1}\ dr\right) n^z \\ &\cdots\cdots \\ &= \frac{n!}{z(z+1)(z+2)\cdots(z+n)} n^z\end{aligned}$$

since the $(1-r)$ term under the integral will disappear when we have,

$$\int\limits_0^1 r^{z+n-1}\ dr = \frac{1}{z+n}.$$

Hence by equation (26.3.1) of Theorem 198, page 290,

$$\lim_{n\to\infty} \Pi(z,n) = \Gamma(z)$$

Consequently,

$$\Gamma(z) = \lim_{n\to\infty} \int_0^n \left(1 - \frac{t}{n}\right)^n\ t^{z-1}\ dt$$

Let $\Gamma_1(z) = \int_0^\infty e^{-t} t^{z-1}\ dt$. We will show $\Gamma_1(z) = \Gamma(z)$.

Note that $\int_0^\infty e^{-t} t^{z-1}\ dt$ is an analytic function of z and therefore converges when the real part of z is greater than 0 or $Re(z) > 0$, but the integral does not converge when $Re(z) \leq 0$ since the consequential denominator $\frac{1}{t^{|Re(z)|}} \to \infty$ as $t \to 0$.

Since $\int_0^\infty e^{-t}t^{z-1}\ dt$ is convergent, it follows that just as the n^{th} term a_n of a convergent infinite series must obey $\lim\limits_{n\to 0} a_n = 0$, so the convergent infinite series,

$$\int_0^\infty e^{-t}t^{z-1}\ dt = \int_0^1 e^{-t}t^{z-1}\ dt + \int_1^2 e^{-t}t^{z-1}\ dt + \ldots \int_n^\infty e^{-t}t^{z-1}\ dt$$

must obey

$$\int_n^\infty e^{-t}t^{z-1}\ dt = 0 \tag{26.4.3}$$

Then, using,

$$\Gamma_1(z) = \int_0^\infty e^{-t}t^{z-1}\ dt = \int_0^n e^{-t}t^{z-1}\ dt + \int_n^\infty e^{-t}t^{z-1}\ dt$$

we obtain,

$$\begin{aligned}\Gamma(z) - \Gamma_1(z) &= \lim_{n\to\infty}\left[\int_0^n \left(1 - \frac{t}{n}\right)^n t^{z-1}\ dt - \int_0^n e^{-t}t^{z-1}\ dt - \int_n^\infty e^{-t}t^{z-1}\ dt\right]\\ &= \lim_{n\to\infty}\int_0^n \left[\left(1 - \frac{t}{n}\right)^n - e^{-t}\right] t^{z-1}\ dt - 0 \text{ by (26.4.3)}\\ &= 0 \ \text{ due to (26.4.2) of Lemma 202.}\end{aligned}$$

We have proved,

$$\Gamma(z) = \frac{e^{-\gamma z}}{z}\prod_{n=1}^\infty \frac{e^{\frac{z}{n}}}{1 + \dfrac{z}{n}} \Leftrightarrow \Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\ dt$$

□

We could, therefore, have developed the theory of the Gamma Function by starting with $\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\ dt$. For example,

Theorem 204.

$$\Gamma(z+1) = z\Gamma(z)$$

Proof.
Given $\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\ dt$ we have,

$$\Gamma(z+1) = \int_0^\infty e^{-t}t^{z-1+1}\ dt = \int_0^\infty e^{-t}t^{z}\ dt$$

We use integration by parts, putting $u = t^z, v' = e^{-t} \Rightarrow u' = zt^{z-1}, v = -e^{-t}$ to get,

$$\Gamma(z+1) = [-e^{-t}t^z]_0^\infty + z\int_0^\infty e^{-t}t^{z-1}\ dt = 0 + z\Gamma(z) = z\Gamma(z).$$

□

Theorem 205.

$$\Gamma(1) = 1$$

Proof.

$$\Gamma(1) = \int_0^\infty e^{-t}\ dt = \left[-e^{-t}\right]_0^\infty = 0 + e^0 = 1$$

□

26.5 Duplication Formula

Finally, there are many examples in mathematics and number theory of recursive type formulas and/or duplication formulas as well as functional equations combining more than one function together into a formula.

Here is the one relating to the Gamma Function due to Legendre which we will also use in the final chapter.

Theorem 206. *(Duplication Formula)*

$$2^{2z-1}\Gamma(z)\Gamma\left(z+\frac{1}{2}\right) = \sqrt{\pi}\ \Gamma(2z)$$

Proof.
Since $\Gamma(z+1) = z\Gamma(z)$,

$$\begin{aligned}
\Gamma\left(z+\frac{1}{2}\right) = \Gamma\left(\frac{2z+1}{2}\right) &= \left(\frac{2z-1}{2}\right)\Gamma\left(\frac{2z-1}{2}\right)\\
&= \left(\frac{2z-1}{2}\right)\left(\frac{2z-3}{2}\right)\Gamma\left(\frac{2z-3}{2}\right)\\
&\dots\\
&= \overbrace{\left(\frac{2z-1}{2}\right)\left(\frac{2z-3}{2}\right)\cdots\frac{3}{2}\cdot\frac{1}{2}}^{z\ terms}\cdot\Gamma\left(\frac{1}{2}\right)\\
&= \frac{(2z-1)(2z-3)\cdots 3\cdot 1}{2^z}\sqrt{\pi}\text{ by Lemma 201} \qquad (26.5.1)
\end{aligned}$$

We also have, using $\Gamma(z+1) = z\Gamma(z)$,

$$\begin{aligned}
\frac{\Gamma(2z+1)}{2^z\Gamma(z+1)} &= \frac{(2z)(2z-1)(2z-2)(2z-3)\cdots 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{2^z(z)(z-1)(z-2)\cdots 3\cdot 2\cdot 1}\\
&= \frac{(2z)(2z-1)\cdot 2(z-1)\cdot(2z-3)\cdot 2(z-2)\cdots(2\cdot 3)\cdot 5\cdot(2\cdot 2)\cdot 3\cdot(2\cdot 1)}{2^z(z)(z-1)(z-2)\cdots 3\cdot 2\cdot 1}\\
&= (2z-1)(2z-3)\cdots 5\cdot 3\cdot 1 \qquad (26.5.2)
\end{aligned}$$

since there are also 2^z $2's$ in the numerator and each term in the denominator cancels with its corresponding term in the numerator.
Comparing these two results (26.5.1) and (26.5.2) we have,

$$\begin{aligned}
&\Gamma\left(z+\frac{1}{2}\right)=\frac{\Gamma(2z+1)}{2^z\cdot 2^z\cdot\Gamma(z+1)}\sqrt{\pi}\\
&\Rightarrow 2^{2z}\Gamma(z+1)\Gamma\left(z+\frac{1}{2}\right)=\Gamma(2z+1)\sqrt{\pi}\\
&\Rightarrow 2^{2z}z\Gamma(z)\Gamma\left(z+\frac{1}{2}\right)=2z\cdot\Gamma(2z)\sqrt{\pi}\text{ (using }\Gamma(z+1)=z\cdot\Gamma(z)\text{ on both sides)}\\
&\Rightarrow 2^{2z-1}\Gamma(z)\Gamma\left(z+\frac{1}{2}\right)=\Gamma(2z)\sqrt{\pi}
\end{aligned}$$

□

The Gamma Function combines with other functions to give us some wonderful results. For example Riemann used it in conjunction with his Zeta function, which we will discuss in the final chapter.

Part X

20th Century Banquet

Counting the Primes: Euler to Selberg

How many primes are there less than or equal to a given number x? The symbol is $\pi(x)$. By the late 18th century, tables of primes existed up to about 400,000. Gauss is reputed to have hired an assistant whose main task was to determine primes. His primary method was to divide any odd number x by the primes less than its square root. Of course, the majority of numbers can be readily eliminated as divisible by $2, 3$ or 5.

- In 1798 Legendre conjectured $\pi(x) = \dfrac{x}{\log x - A(x)}$ where $A(x)$ is a constant depending on x.
- In 1792, the 15-year old Carl Gauss conjectured that $\pi(x)$ and the logarithmic integral of x defined by $Li(x) = \int\limits_2^x \dfrac{dt}{\log t}$ become equal as $x \to \infty$.

Since, by integration by parts, $\int\limits_2^x \dfrac{dt}{\log t} = \dfrac{x}{\log x}$, this implies,

$$\pi(x) \to \frac{x}{\log x} \ as\ x \to \infty$$

Just as the search to prove Fermat's Last Theorem dominated the 20th century, so the search to prove the Prime Number Theorem (PNT),

$$\pi(x) \to \frac{x}{\log x} \ as\ x \to \infty$$

dominated the 19th century. Using complex analysis it was finally proved independently in 1896 by de la Vall*é*e Pousson and Hadamard. They used techniques of a complex variable due to Riemann in his paper "On the number of primes less than a given magnitude"' ' which we will discuss in the final chapter.

It had taken so long to prove the theorem that almost no-one believed it could be proved by elementary methods. Stunning the mathematical world of 1949, it was proved, using elementary methods, again independently, by Selberg and Erdös. The breakthrough they needed had been done 50 years before by the Russian mathematician Chebyshev.

To prove $\pi(x) \to \dfrac{x}{\log x}$ *as* $x \to \infty$ which is equivalent to $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x/\log x} = 1$, Chebyshev proved there exist positive constants C_1, C_2 such that,

$$C_1 < \frac{\pi(x)}{x/\log x} < C_2$$

Selberg and Erdös proved $C_1 = C_2 = 1$. We will follow the trail to Selberg's proof.

We include as a final dessert in our prime number banquet, Bertrand's Postulate:

There is always a prime between n *and* $2n$ *if* $n > 2$.

since its proof uses similar techniques.

Chapter 27

Counting the Primes

Course: Banquet Style
Ingredients
Prime numbers and $\pi(x)$, the number of primes less than or equal to x.
Sieve of Erasthosthenes
Sets
Big-O and little-o notation
Möbius function
Greatest integer function
Directions
Use the Sieve of Erasthosthenes
Prove a theorem on the cardinality of the union of sets
Prove Legendre's Theorem for $\pi(x)$
Follow Chebyshev in finding bounds for $\pi(x)$
Follow Selberg in proving the prime number theorem by elementary techniques.

Definition 102. *prime and composite numbers*
A prime number is a natural number greater than 1 that is not divisible by any other number except itself and 1. In other words, it has no factors other than itself and 1. Numbers that are not prime are called composite. In other words, they have factors other than themselves and 1.

Example 121.
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$ *are prime numbers. So is 197.*
$4, 6, 8, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, \ldots$ *are composite numbers. So is* $57 = 3 \times 19$. ◇

We note that $\sqrt{64} < \sqrt{76} < \sqrt{81}$ means $\sqrt{76}$ lies between 8 and 9. We further note that one of each of the pairs of factors of 76 is less than 8 $(1, 2, 4 < 8\ )$ and the other is greater than 8 $(76, 38, 19 > 8)$. Therefore in order to find the factors of 76, it is sufficient to divide 76 by the numbers less than 8. In turn, since any composite number less than 8 is the product of smaller primes (e.g., $4 = 2 \times 2$), to determine whether 76 is prime or composite, it is sufficient to divide it only by the primes less than 8, namely, 2,5 and 7. Consequently we have this algorithm.

27.1 Algorithm for determining whether a number is prime.

To determine whether a number is prime, divide it by the primes less than its square root. If there are no remainders then the number is prime.

Example 122.

$$\sqrt{169} < \sqrt{181} < \sqrt{196} \Rightarrow 13 < \sqrt{181} < 14,$$

so to determine whether 181 is prime, we divide it by $2, 3, 5, 7, 11, 13$. *Note that divisibility by 2 and 5 is obviously not true since it is not an even number and it does not end in 0 or 5. For the others,*

$$181 \equiv 1(\text{mod } 3),\ 6(\text{mod } 7),\ 5(\text{mod } 11),\ 12(\text{mod } 13)$$

so that 181 is a prime.

27.2 Sieve of Erasthosthenes

In ancient times, the Greek Mathematician Erasthosthenes developed a sieve to determine prime numbers. You can do it for yourself using the table below.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132

The number 1 is not regarded as a prime number. The number 2 is a prime number, so circle it and then go through the table and cross out every number divisible by 2, that is every second number from 2 on, namely, 4, 6, 8, etc. You will see that the first number not crossed out or circled is 3. So 3 is a prime. Circle it and then proceed to cross out every third number from 3 on, namely, 6, 9, 12, etc. The next number not crossed out or circled is 5. So keep repeating the process until you reach 11. The circled numbers are the prime numbers. The crossed out numbers are the composite numbers.

You end up with:

	2	3	5	7		11
13			17	19		23
			29	31		
37			41	43		47
			53		59	
61				67		71
73				79		83
			89			
97			101	103		107
109			113			
				127		131

The distribution of the primes has no apparent pattern.

It can easily be proved there is no non-constant polynomial function $P(n)$ with integer coefficients that generates the primes, but interestingly Euler first noticed (in 1772) that the quadratic polynomial $P(n) = n^2 - n + 41$ generates primes for all $n < 41$. They are,

41	43	47	53	61	71	83	97	113	131	151	173	197
223	251	281	313	347	383	421	461	503	547	593	641	743
797	853	911	971	1033	1097	1163	1231	1301	1373	1447	1523	1601

The differences between the primes are 2,4,6,8,...
For $n = 41$, $P(n)$ produces the square number $1681 = 41^2$ ending the streak.
$p = 41$ is the largest known value of p for which $P(n) = n^2 - n + p$ generates primes up to p^2. Other values are $p = 2, 3, 5, 11, 17$. No other values of p are known.

27.3 $\pi(x)$ - the number of primes $\leq x$.

Definition 103. *We define $\pi(x)$ to be the number of primes less than or equal to a given number x, that is,*

$$\pi(x) = \sum_{p \leq x} 1, \ \ p \in \mathbb{P}$$

Example 123.
$\pi(2) = 0, \ \pi(3) = 1, \ \pi(100) = 25, \ \pi(1,000) = 168, \ \pi(1,000,000) = 78,498$

One of the earliest formulas for $\pi(x)$ is due to Legendre. Its strict proof requires a lemma from set theory.

27.4 Cardinality of a Union of Sets

Definition 104. *cardinality of a set*
The cardinality $|A|$ of a set A is the number of objects it contains.

Example 124.
$A = \{2, 4, 7\} \Rightarrow |A| = 3$

The cardinality of a union of sets is given by the following lemma.

Lemma 207.
Suppose $A_1, A_2, \ldots, A_n$ are sets. Then,

$$\begin{aligned}
&|A_1 \cup A_2 \cup \ldots \cup A_n| \\
&= \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i,j \le n} |A_i \cup A_j| + \sum_{1 \le i,j,k \le 1} |A_i \cup A_j \cup A_k| - \ldots \\
&\qquad + (-1)^{m+1} \sum_{1 \le i_1, i_2, \ldots, i_m \le n} |A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_m| + \ldots \\
&\qquad\qquad + (-1)^{n+1} |A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n|
\end{aligned}$$

Proof.
The proof is by induction. We first prove the statement of the theorem for $n = 2$, namely,

$$|A_1 \cup A_2| = \sum_{1 \le i \le 2} |A_i| + (-1)^3 |A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cup A_2|$$

We first note if $A \cup B = \phi$[1] or A, B are disjoint sets, then clearly $|A \cup B| = |A| + |B|$ and by induction, if $A_1, A_2, \ldots, A_n$ are all disjoint then,

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{1 \le i \le n} |A_i|$$

Then in general noting $A - B$ and $A \cap B$ are disjoint sets and that $A = (A - B) \cup (A \cap B)$ as we see from Figure 37,

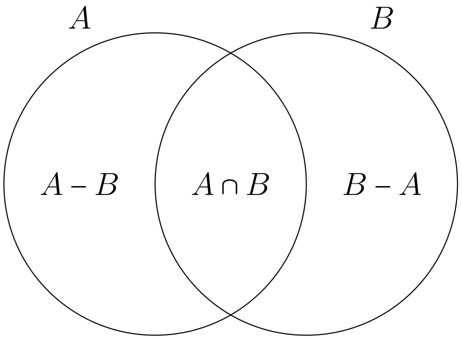


Figure 37

[1] The Greek letter phi, ϕ, is the symbol for the empty set, thus $\phi = \{\ \}$.

then,

$$A_1 = (A_1 - A_2) \cup (A_1 \cap A_2) \Rightarrow |A_1| = |A_1 - A_2| + |A_1 \cap A_2| \tag{27.4.1}$$

$$A_2 = (A_2 - A_1) \cup (A_1 \cap A_2) \Rightarrow |A_2| = |A_2 - A_1| + |A_1 \cap A_2| \tag{27.4.2}$$

Then (again referring to Figure 37) since,

$$A_1 \cup A_2 = (A_1 \cap A_2) \cup (A_1 - A_2) \cup (A_2 - A_1) \tag{27.4.3}$$

and the sets on the right side are all disjoint, having no elements in common, then rearranging (27.4.1),

$$|A_1 - A_2| = |A_1| - |A_1 \cup A_2|$$

and rearranging (27.4.2),

$$|A_2 - A_1| = |A_2| - |A_1 \cap A_2|$$

so, by (27.4.3),

$$\begin{aligned} |A_1 \cup A_2| &= |A_1 - A_2| + |A_1 \cap A_2| + |A_2 - A_1| \\ &= |A_1| - |A_1 \cap A_2| + |A_1 \cap A_2| + |A_2| - |A_1 \cap A_2| \\ &= |A_1| + |A_2| - |A_1 \cap A_2| \end{aligned} \tag{27.4.4}$$

Given sets A, B, C obey the distribution law of union over intersection,

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \tag{27.4.5}$$

which extends by induction to,

$$(A_1 \cup A_2 \cup \ldots \cup A_n) \cap B = (A_1 \cap b) \cup (A_2 \cap b) \cup \ldots \cup (A_n \cap B)$$

then, for $n = 3$,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |(A_1 \cup A_2) \cup A_3| \\ &= |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| \text{ by (27.4.3)} \\ &= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - |(A_1 \cap A_3) \cup (A_2 \cap A_3)| \text{ by (27.4.4) and (27.4.5)} \\ &= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - |A_1 \cap A_3| - |(A_2 \cap A_3| + |A_1 \cap A_3 \cap A_2 \cap A_3| \\ &= \sum_{1 \le i \le 3} |A_i| - \sum_{1 \le i,j \le 3} |A_i \cap A_j| + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

So the statement is true for $n = 3$ also. We will omit the details of the inductive step (it's all about keeping the notation under control) and conclude inductively that,

$$\begin{aligned} &|A_1 \cup A_2 \cup \ldots \cup A_n| \\ &= \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i,j \le n} |A_i \cup A_j| + \sum_{1 \le i,j,k \le 1} |A_i \cup A_j \cup A_k| - \ldots \\ &\qquad + (-1)^{m+1} \sum_{1 \le i_1, i_2, \ldots, i_m \le n} |A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_m| + \ldots \\ &\qquad\qquad + (-1)^{n+1} |A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n| \end{aligned}$$

□

27.5 Legendre's Theorem

Definition 105. *greatest integer function*
We define the greatest integer function $[x]$ to mean the greatest integer less than or equal to the real number x. A useful way of interpreting $[x]$ is to say, given $[x]$, there are a pair of successive integers $n, n+1$ such that $n \le x < n+1$ where $[x] = n$.

Example 125.

$$[1.6] = 1,\ [-2.4] = -3,\ [7] = 7$$

Note 36. *Let's investigate $[2x] - 2[x]$.*
There are two possibilities. With $n \le x < n+1$ and $0 \le \delta < \frac{1}{2}$ we have either of,
Case 1: $x = n + \frac{1}{2} + \delta \Rightarrow [x] = n$, making $2x = 2n + 1 + 2\delta \Rightarrow [2x] = 2n + 1$ giving $[2x] - 2[x] = 1$.
Case 2: $x = n + \delta \Rightarrow [x] = n$, making $2x = 2n + 2\delta \Rightarrow [2x] = 2n$ giving $[2x] - 2[x] = 0$.

Theorem 208. *(Legendre)*
The number of primes less than or equal to a real number x, denoted $\pi(x)$, is given by,

$$\pi(x) = \sum_{d|P} \mu(d) \left[\frac{x}{d}\right] + \pi(\sqrt{x}) - 1$$

where $P = \prod_{k=1}^{n} p_k$ is the product of all the primes p_k less than or equal to x and $\mu(d)$ is the Möbius function.

Proof.
The method we use to find all the primes less than x is to count all the numbers divisible by any prime less than the square root of x. This means we eliminate all the composite numbers less than x but we also eliminate the primes less than the square root of x, however, we do not eliminate the number 1. Hence we will need the correction term $+\pi(\sqrt{x}) - 1$. Let's begin.

Let A_1 be all the natural numbers less than or equal to x, that is $|A_1| = [x]$.
Let A_2 be all the numbers less than x that are divisible by 2, then $|A_2| = \left[\frac{x}{2}\right]$.
Let A_3 be all the numbers less than x that are divisible by 3, then $|A_3| = \left[\frac{x}{3}\right]$.
...
Finally, let A_{p_n} be all the numbers less than x that are divisible by p_n where p_n is the n^{th} and largest prime less than $\sqrt{x}$, then $|A_{p_n}| = \left[\frac{x}{p_n}\right]$
Let,

$$P = \prod_{p=2}^{p_n} p = \prod_{p \le \sqrt{x}} p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p_n$$

be the product of all the primes less than or equal to $\sqrt{x}$. Let $\mu(d)$ be the Möbius function and p and $p_i,\ i \in \mathbb{Z}^+$ denote primes. Thus, as we previously defined it,

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ 0 & \text{if } p^2 | d \\ (-1)^r & \text{if } d = p_1 p_2 \cdots p_r,\ p_i \neq p_j\ for\ i \leq r \leq j. \end{cases}$$

*****

Let's first look at two examples of the general proof.
First, we note that if $\sqrt{x} < 5$ we have by,

$$|A_i \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

that the number of composite numbers divisible by 2 or 3, that is, less than or equal to x is,

$$\left[\frac{x}{2}\right] + \left[\frac{x}{3}\right] - \left[\frac{x}{2 \cdot 3}\right]$$

Therefore, the number of primes less than or equal to x would be,

$$[x] - \left[\frac{x}{2}\right] - \left[\frac{x}{3}\right] + \left[\frac{x}{2 \cdot 3}\right]$$

together with the correction term $+\pi(\sqrt{x}) - 1$.
Using our definition of P and the Möbius function, we write,

$$\begin{aligned} \pi(x) - \pi(\sqrt{x}) + 1 &= [x] - \left[\frac{x}{2}\right] - \left[\frac{x}{3}\right] + \left[\frac{x}{2 \cdot 3}\right] \\ &= \mu(1)\,[x] + \mu(2)\left[\frac{x}{2}\right] + \mu(3)\left[\frac{x}{3}\right] + \mu(2 \cdot 3)\left[\frac{x}{2 \cdot 3}\right] \\ &= \sum_{d|P} \mu(d)\left[\frac{x}{d}\right] \end{aligned}$$

For the second example we note that if $\sqrt{x} < 7$ we have by,

$$|A_i \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

that the number of composite numbers divisible by 2 or 3 or 5, that is, less than or equal to x is,

$$\left[\frac{x}{2}\right] + \left[\frac{x}{3}\right] + \left[\frac{x}{5}\right] - \left[\frac{x}{2 \cdot 3}\right] - \left[\frac{x}{2 \cdot 5}\right] - \left[\frac{x}{3 \cdot 5}\right] + \left[\frac{x}{2 \cdot 3 \cdot 5}\right]$$

Therefore, we have,

$$\begin{aligned}
&\pi(x) - \pi(\sqrt{x}) + 1 \\
&= [x] - \left[\frac{x}{2}\right] - \left[\frac{x}{3}\right] - \left[\frac{x}{5}\right] + \left[\frac{x}{2\cdot 3}\right] + \left[\frac{x}{2\cdot 5}\right] + \left[\frac{x}{3\cdot 5}\right] - \left[\frac{x}{2\cdot 3\cdot 5}\right] \\
&= \mu(1)\,[x] + \mu(2)\left[\frac{x}{2}\right] + \mu(3)\left[\frac{x}{3}\right] + \mu(5)\left[\frac{x}{5}\right] + \mu(2\cdot 3)\left[\frac{x}{2\cdot 3}\right] \\
&\qquad + \mu(2\cdot 5)\left[\frac{x}{2\cdot 5}\right] + \mu(3\cdot 5)\left[\frac{x}{3\cdot 5}\right] + \mu(2\cdot 3\cdot 5)\left[\frac{x}{2\cdot 3\cdot 5}\right] \\
&= \sum_{d|P} \mu(d)\left[\frac{x}{d}\right]
\end{aligned}$$

*****

The general proof follows by extending the sets A_i. Since,

$$\begin{aligned}
|\bigcup_{i=1}^{n} A_i| &= |A_1 \cup A_2 \cup \ldots \cup A_n| \\
&= \sum_{1\le i\le n} |A_i| - \sum_{1\le i,j\le n} |A_i \cup A_j| + \sum_{1\le i,j,k\le 1} |A_i \cup A_j \cup A_k| - \ldots \\
&\qquad + (-1)^{m+1} \sum_{1\le i_1,i_2,\ldots,i_m\le n} |A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_m| + \ldots \\
&\qquad\qquad + (-1)^{n+1} |A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n|
\end{aligned}$$

then,

$$\pi(x) = \sum_{d|P} \mu(d)\left[\frac{x}{d}\right] + \pi(\sqrt{x}) - 1$$

□

Example 126.

$$\begin{aligned}
&\sum_{d|2\cdot 3\cdot 5} \mu(d)\left[\frac{48}{d}\right] + \pi(\sqrt{48}) - 1 \\
&= \mu(1)\left[\frac{48}{1}\right] + \mu(2)\left[\frac{48}{2}\right] + \mu(3)\left[\frac{48}{3}\right] + \mu(5)\left[\frac{48}{5}\right] + \mu(2\cdot 3)\left[\frac{48}{2\cdot 3}\right] \\
&\qquad + \mu(2\cdot 5)\left[\frac{48}{2\cdot 5}\right] + \mu(3\cdot 5)\left[\frac{48}{3\cdot 5}\right] + \mu(2\cdot 3\cdot 5)\left[\frac{48}{2\cdot 3\cdot 5}\right] + 3 - 1 \\
&= (48 - 24 - 16 - 9 + 8 + 4 + 3 - 1) + 3 - 1 \\
&= 15
\end{aligned}$$

The primes less than or equal to 48 are 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47. There are 15. ◇

27.6 Approximations to $\pi(x)$.

As the above example shows, the formula is a little tedious to apply. If we observe that

$$\frac{x}{d} = \left[\frac{x}{d}\right] + \frac{r}{d}$$

where $r \equiv x(\text{mod } d)$ so $r < d$, then since $\dfrac{r}{d}$ is relatively small and may be positive or negative, this suggests ignoring it. The above example then becomes, with correction factor $3 - 1$,

$$\begin{aligned}\pi(48) &= \frac{48}{1} - \frac{48}{2} - \frac{48}{3} - \frac{48}{5} + \frac{48}{6} + \frac{48}{10} + \frac{48}{15} - \frac{48}{30} + 3 - 1\\ &= 48\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) + 2\\ &\approx 48\prod_{p\le\sqrt{48}}\left(1-\frac{1}{p}\right) + 2\end{aligned}$$

In this particular example,

$$\begin{aligned}\pi(48) &= 48\prod_{p\le\sqrt{48}}\left(1-\frac{1}{p}\right) + 2\\ &= 48\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} + 2\\ &= 12.8 + 2 = 14.8\end{aligned}$$

In general, if,

$$\pi(x) = \sum_{d|P}\mu(d)\left[\frac{x}{d}\right] + \pi(\sqrt{x}) - 1,$$

we write,

$$\pi_A(x) \approx x\prod_{p=2}^{p_n}\left(1-\frac{1}{p}\right) + \pi(p_n) - 1$$

where p_n is the largest prime less than or equal to the square root of x. The following table shows the comparisons for various values of x.

x	$\pi_A(x)$	$\pi(x)$	% difference
1,000	163	168	3
5,000	666	669	0.4
10,000	1,227	1,229	0.2
40,000	4,201	4,203	0.05
80,000	7,910	7,837	0.9
1,000,000	81,132	88,710	9
100,000,000	6,084,577	5,761,455	6

For small values of x the approximation is useful, but as x grows it becomes useless. Mathematicians such as Meissel and Lehmer have improved the formula but this line of attack on counting primes seems to be limited.

27.7 The Prime Number Theorem

The Prime Number Theorem (PNT) is,

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$$

that is as $x \to \infty$ we have $\pi(x) \to \dfrac{x}{\log x}$.
Using complex analysis, de la Vallée Pousson and Hadamard independently proved the PNT in 1896. Stunning the mathematical world in 1949, it was proved, using elementary methods, again independently, by Selberg and Erdös.

27.8 Chebyshev's Theorem

The breakthrough, however, had been done 50 years before by the Russian mathematician Chebyshev. To prove,

$$\pi(x) \to \frac{x}{\log x}$$

as $x \to \infty$ which is equivalent to,

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$$

he proved there exist positive constants C_1, C_2 such that,

$$C_1 < \frac{\pi(x)}{x\log x} < C_2.$$

The challenge to the mathematical world was to show $C_1 = C_2 = 1$ as $x \to \infty$. Let us consider how to approach this problem.

We will be using the great integer function in what follows. You may wish to revisit the definition and Note 36 on 306. We again note a useful way of interpreting $[x] = n$ is to say there are a pair of successive integers $n, n+1$ such that $n \le x < n+1$. We also have Note 36 on page 306 that $[2x] - [x] = 0, 1$.

Lemma 209. *For $n \ge 2$ consider the prime factorization,*

$$n! = \prod_{p\le n} p^{k_p} = 2^{k_1}3^{k_3}5^{k_5}\cdots,$$

where $k_p \in \mathbb{Z}^+$. Then the powers $2^{k_2}, 3^{k_3}, \dots$ are given for any prime p by,

$$k_p = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]$$

Proof. Consider the integers $1, 2, \dots, n$ and their divisibility by a prime p where the number of these integers divisible by p is denoted k_p.
The ones divisible by p are $p, 2p, 3p, \dots l_1 p$ where $l_1 p \le n < (l_1 + 1)p$. Then,

$$\begin{aligned}
&l_1 p \le n < (l_1 + 1)p \\
&\Rightarrow l_1 \le \frac{n}{p} < l_1 + 1 \\
&\Rightarrow l_1 = \left[\frac{n}{p}\right] \text{ where } \left[\frac{n}{p}\right] \text{ is the greatest integer function}
\end{aligned}$$

Similarly, the ones divisible by p^2 are $p^2, 2p^2, 3p^2, \dots, l_2 p^2$ where

$$l_2 p^2 \le n < (l_2 + 1)p^2 \Rightarrow l_2 = \left[\frac{n}{p^2}\right]$$

Similarly the number divisible by p^3 is $l_3 = \left[\frac{n}{p^3}\right]$. Once we reach $p^r > n$ then we note $\left[\frac{n}{p^r}\right] = 0$. Thus $\left[\frac{n}{p^s}\right] = 0$ for $s > r$ to ∞. We conclude,

$$\begin{aligned}
k_p &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots + \left[\frac{n}{p^{r-1}}\right] + 0 + 0 + \dots \\
\Rightarrow k_p &= \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right] \qquad (27.8.1)
\end{aligned}$$

□

Corollary 210.

$$\log n! = \sum_{p \le n} k_p \log p = \sum_{p \le n} \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right] \log p \qquad (27.8.2)$$

$$\log(2n)! = \sum_{p \le 2n} \sum_{r=1}^{\infty} \left[\frac{2n}{p^r}\right] \log p \qquad (27.8.3)$$

Proof. Using (27.8.1) and the prime factorization of $n!$ as in Lemma 209,

$$\begin{aligned}
n! &= \prod_{p \le n} p^{k_p} \\
\Rightarrow \log n! &= \log \prod_{p \le n} p^{k_p} \\
&= \sum_{p \le n} \log p^{k_p} \\
&= \sum_{p \le n} k_p \log p \\
&= \sum_{p \le n} \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right] \log p
\end{aligned}$$

Any value of n has its own values of k_p as defined in the previous lemma so we can subsitute $2n$ for n and obtain via $2n's$ values of $k_p's$

$$\log(2n)! = \sum_{p\leq 2n}\sum_{r=1}^{\infty}\left[\frac{2n}{p^r}\right]\log p$$

□

Note we can increase the sum for $\log n!$ writing $\log n! = \sum_{p\leq 2n}\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]\log p$ since for any prime p such that $n \leq p \leq 2n$ we have $\left[\frac{n}{p^r}\right] = 0$.

Now we can find some Chebyshev-like boundaries for $\pi(x)$.

Theorem 211.
For $n \geq 2$,

$$\frac{1}{6}\frac{n}{\log n} < \pi(n) < 9\frac{n}{\log n}$$

Proof. By the Binomial Theorem 85, page 130,

$$\begin{aligned} 2^{2n} &= (1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \binom{2n}{2} + \ldots + \binom{2n}{2n} \\ &\Rightarrow \binom{2n}{m} < 2^{2n} \text{ for all } 0 \leq m \leq 2n \end{aligned}$$

In particular if $m = n$, then $\binom{2n}{n} \leq 2^{2n}$.
On the other hand,

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{2n}{n}\frac{2n-1}{n-1}\frac{2n-2}{n-2}\cdots\frac{2n-n+1}{1}\cdot\frac{\cancel{n}!}{\cancel{n}!} \geq 2^n$$

since[2] $\frac{2n-k}{n-k} \geq 2$ for $k = 0, 1, \ldots, n-1$.
Putting these two results together and taking logs gives,

$$2^n \leq \binom{2n}{n} \leq 2^{2n} \Rightarrow n\log 2 \leq \log\binom{2n}{n} \leq 2n\log 2$$

Then, since[3] $\frac{1}{2} < \log 2 \Rightarrow \frac{n}{2} < n\log 2$ and $\log 2 < 1 \Rightarrow 2n\log 2 < 2n$, we have,

$$\frac{n}{2} < n\log 2 \leq \log\binom{2n}{n} \leq 2n\log 2 \leq 2n \tag{27.8.4}$$

[2] $\frac{2n-k}{n-k} = \frac{2n-2k+k}{n-k} = 2 + \frac{k}{n-k} \geq 2$

[3] $\log 2 = \log_e 2 = ln2 = 0.6931\ldots$

On the other hand, defining,

$$m_p = \sum_{r=1}^{\infty}\left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right)$$

we have,

$$\begin{aligned}
\log\binom{2n}{n} &= \log\frac{(2n)!}{n!n!}\\
&= \log(2n)! - 2\log n!\\
&= \sum_{p\le 2n}\sum_{r=1}^{\infty}\left[\frac{2n}{p^r}\right]\log p - \sum_{p\le 2n}\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]\log p \text{ by (27.8.2 and (27.8.3)}\\
&= \sum_{p\le 2n} m_p \log p \qquad (27.8.5)
\end{aligned}$$

since for $p > 2n$, $\left[\frac{2n}{p}\right] - \left[\frac{n}{p}\right] = 0$. Also,

$$\begin{aligned}
m_p &= \sum_{r=1}^{\infty}\left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right) \qquad (27.8.6)\\
&= \sum_{1\le r\le \frac{\log 2n}{\log p}}\left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right)
\end{aligned}$$

since $\left[\frac{2n}{p^r}\right] = 0$ if $p^r > 2n$ which means $r > \frac{\log 2n}{\log p}$.

Now using Note 36 on page 306, $[2x] - 2[x] = 0$ *or* 1. Therefore we have,

$$\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right] = 0 \text{ or } 1 \Rightarrow \left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right] \le 1$$

so that by (27.8.6),

$$\begin{aligned}
m_p &\le \sum_{1\le r\le \frac{\log 2n}{\log p}} 1\\
&= \frac{\log 2n}{\log p} \qquad (27.8.7)
\end{aligned}$$

Putting (27.8.4), (27.8.5) and (27.8.7) together and noting $\sum_{p\le 2n} 1 = \pi(2n)$,

$$\frac{n}{2} < \log\binom{2n}{n} = \sum_{p\le 2n} m_p\log p \le \sum_{p\le 2n}\frac{\log(2n)}{\cancel{\log p}}\cancel{\log p} = \log(2n)\sum_{p\le 2n} 1 = \log(2n)\cdot\pi(2n)$$

so that $\frac{n}{2} < \log(2n)\cdot\pi(2n)$ giving,

$$\pi(2n) > \frac{1}{2}\frac{n}{\log(2n)} = \frac{1}{4}\frac{2n}{\log(2n)} \text{ (multiplying by } \frac{2}{2})$$

Now, for even numbers,

$$\pi(2n) > \frac{1}{4}\frac{2n}{\log(2n)} > \frac{1}{6}\frac{2n}{\log(2n)} \text{ (since } \frac{1}{4} > \frac{1}{6})$$

whereas for odd numbers,

$$\begin{aligned}\pi(2n+1) &\geq \pi(2n)\\ &> \frac{1}{4}\frac{2n+1}{\log(2n+1)}\\ &> \frac{1}{4}\cdot\frac{2n+1}{\log(2n+1)}\cdot\frac{2n}{2n+1} \text{ since } \frac{2n}{2n+1} < 1,\\ &> \frac{1}{4}\cdot\frac{2n+1}{\log(2n+1)}\cdot\frac{2}{3}\\ &\text{since } n \geq 1 \Rightarrow 2n \geq 2 \Rightarrow 6n \geq 4n+2 \Rightarrow \frac{2n}{2n+1} \geq \frac{2}{3}\\ &> \frac{1}{6}\frac{2n+1}{\log(2n+1)}\end{aligned}$$

So for all n we have,

$$\pi(n) > \frac{1}{6}\frac{n}{\log n}$$

*****

We now show $\pi(n) < 9\frac{n}{\log n}$. We insert a lemma.

Lemma 212.

$$m_p = 1 \textit{ if } n < p \leq 2n.$$

Proof. Since,

$$n < p \leq 2n \Rightarrow \frac{1}{n} > \frac{1}{p} \geq \frac{1}{2n} \Rightarrow 1 > \frac{n}{p} \geq \frac{1}{2} \Rightarrow \frac{1}{2} \leq \frac{n}{p} < 1$$

then,

$$\left[\frac{n}{p}\right] = 0 \text{ and so } \left[\frac{n}{p^r}\right] = 0 \text{ for } r \geq 1 \tag{27.8.8}$$

Also since if $n < p$ and $r > 1$ then $p^r \geq 2p > 2n$ so that,

$$\left[\frac{2n}{p^r}\right] = \begin{cases}0, & \text{if } r > 1\\ 1, & \text{if } r = 1\end{cases} \tag{27.8.9}$$

then using (27.8.9),

$$\begin{aligned} m_p &= \sum_{r=1}^{\infty}\left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right) \\ &= \left[\frac{2n}{p}\right] - \sum_{r=2}^{\infty}\left[\frac{2n}{p^r}\right] - 2\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right] \text{ (taking out the } r = 1 \text{ term)} \\ &= \left[\frac{2n}{p}\right] - 0 - 0 \text{ noting if } \left[\frac{2n}{p^r}\right] = 0 \text{ then certainly } \left[\frac{n}{p^r}\right] = 0 \\ &= 1 \end{aligned}$$

□

*****

We return to the proof that $\pi(n) < 9\dfrac{n}{\log n}$. From (27.8.5),

$$\begin{aligned} \log\binom{2n}{n} &= \sum_{p\le 2n} m_p \log p \\ &= \sum_{p\le n} m_p \log p + \sum_{n<p\le 2n} m_p \log p \end{aligned}$$

Since $\log\dbinom{2n}{n} = \sum\limits_{p\le 2n} m_p \log p$ then the smaller sum,

$$\sum_{n<p\le 2n} m_p \log p < \log\binom{2n}{n} \le 2n \text{ by (27.8.4)}$$

Since by Lemma 212 for $n \le p \le 2n$ we have $m_p = 1$ then,

$$\sum_{n<p\le 2n} \log p < 2n$$

***

Consider the special case, $n = 2^{j-1},\ j = 1, 2, \ldots$. Here,

$$\sum_{2^{j-1}<p<2^j} \log p < 2 \cdot 2^{j-1} = 2^j$$

We sum this inequality over $j = 1, 2, 3, \ldots, k$

$$\text{Left side} = \sum_{2^0<p\le 2^1} \log p + \sum_{2^1<p\le 2^2} \log p + \ldots + \sum_{2^{k-1}<p\le 2^k} \log p = \sum_{p\le 2^k} \log p$$

$$\text{Right side} = 2 + 2^2 + 2^3 + \ldots + 2^k = \sum_{j=1}^{k} 2^k = 2^{k+1} - 2 < 2^{k+1}$$

where on the right side we used the sum of a geometric series,

$$a + ar + ar^2 + \ldots + ar^{k-1} = a\frac{1-r^k}{1-r}$$

Then,

$$\sum_{p\le 2^k} \log p < 2^{k+1}$$

Now in general any number lies between consecutive powers of 2, so if $2^{k-1} < n \le 2^k$ then $4(2^{k-1}) = 2^{k+1} < 4n$ and,

$$\sum_{p\le n} \log p \le \sum_{p\le 2^k} \log p < 2^{k+1} < 4n \tag{27.8.10}$$

Furthermore, we find an estimate from below,

$$\sum_{p\le n} \log p \ge \sum_{\sqrt{n}<p\le n} \log p \ge \sum_{\sqrt{n}<p\le n} \log\sqrt{n} = \log\sqrt{n} \sum_{\sqrt{n}<p\le n} 1$$

where we replaced p with its lower bound $\sqrt{n}$.
Then since, $\sum_{\sqrt{n}\le p\le n} 1 = \sum_{p\le n} 1 - \sum_{p\le\sqrt{n}} 1 = \pi(n) - \pi(\sqrt{n})$,

$$\begin{aligned} &\sum_{p\le n} \log p = \log\sqrt{n}\left(\pi(n) - \pi(\sqrt{n})\right) \\ \Rightarrow &\sum_{p\le n} \log p \ge \log\sqrt{n}\left(\pi(n) - \sqrt{n}\right) \end{aligned} \tag{27.8.11}$$

since $\pi(\sqrt{n})$ is less than $\sqrt{n}$.
We subtract $\sum_{p\le n} \log p < 4n$ from (27.8.10) to obtain,

$$\begin{aligned} &\log\sqrt{n}\left(\pi(n) - \sqrt{n}\right) < 4n \\ &\Rightarrow \pi(n) < \frac{4n}{\log\sqrt{n}} + \sqrt{n},\ n \ge 2. \end{aligned} \tag{27.8.12}$$

Consider the function $f(x) = \dfrac{x}{\log x}$. Let's find its minimum point where $f'(x) = 0$.
Differentiating, $f'(x) = \dfrac{\log x - 1}{(\log x)^2} = 0 \Rightarrow \log x = 1 \Rightarrow x = e$ where e is the exponential number.
Differentiating again, $f''(x) = \dfrac{(\log x)^2\frac{1}{x} - (\log x - 1)(2\log x \times \frac{1}{x})}{(\log x)^4} = \dfrac{1}{e}$ at $x = e$.
Since $f(e) = \dfrac{e}{\log e} = e$, then e is the global minimum of $f(x)$ or $e < \dfrac{x}{\log x}$ for all x.

Putting $x = \sqrt{n}$ in $f(x) = \dfrac{x}{\log x}$ this implies,

$$\begin{aligned} e &\leq \frac{\sqrt{n}}{\log\sqrt{n}} \text{ for all } n \\ 1 &\leq \frac{\sqrt{n}}{e\log\sqrt{n}} \\ \Rightarrow \sqrt{n} &\leq \frac{n}{e\log\sqrt{n}} \qquad (27.8.13) \end{aligned}$$

So by (27.8.12) and (27.8.13), noting $\log\sqrt{n} = \dfrac{1}{2}\log n$,

$$\Rightarrow \pi(n) < \frac{4n}{\log\sqrt{n}} + \frac{n}{e\log\sqrt{n}} = \frac{8n}{\log n} + \frac{1}{e}\frac{2n}{\log n} < 9\frac{n}{\log n}$$

since $\dfrac{2}{e} = \dfrac{2}{2.7.18\ldots} < 1$. Our two results give us,

$$\frac{1}{6} < \frac{\pi(n)\log n}{n} < 9$$

□

Chebyshev actually proved,

$$\frac{7}{8} < \frac{\pi(x)\log x}{x} < \frac{9}{8}$$

Before we proceed, we need some further notation.

27.9 Big-O and Little-o Notation

Definition 106. *Big-O Notation*
Let f and g be two functions defined on some subset of the real numbers. We say $f(x) = O(g(x))$ if $f(x)$ that has the property that,

$$\lim_{x\to\infty}\frac{|f(x)|}{|g(x)|} < K$$

for some finite number $K \in \mathbb{R}$.
Intuitively this means f does not grow faster than g.

Example 127.

$$\lim_{x\to\infty}\frac{|2x+\sqrt{x}|}{|x|} = 2 \Rightarrow 2x + \sqrt{x} = O(x)$$

Definition 107. *Little-o Notation*
Let f and g be two functions defined on some subset of the real numbers. We say $f(x) = o(g(x))$ if $f(x)$ that has the property that,

$$\lim_{x\to\infty} \frac{|f(x)|}{|g(x)|} = 0$$

Intuitively $f(x) = o(g(x))$ means $g(x)$ is growing much faster than $f(x)$ so that $\frac{|f(x)|}{|g(x)|} \to 0$ as x increases in value.

Example 128.

$$\lim_{x\to\infty} \frac{|x|}{x^2} = 0 \Rightarrow x = o(x^2).$$

Note 37. *If a function $g(x)$ consists of terms in powers of x, not necessarily integer powers, then $O(g(x))$ is any power of x equal to or larger than the greatest power and $o(g(x))$ is any power of x less than the greatest power*

Example 129. *If $g(x) = 4x^3 - 7x^2 + 3\sqrt{x} = 4x^3 - 7x^2 + 3x^{\frac{1}{2}}$ then,*

$$O(g(x)) = x^3, x^4, etc.$$
$$o(g(x)) = \sqrt{x}, x, x^2 \qquad \diamond$$

If each of $g_i(x),\ i = 1, 2, 3\ldots$ satisfies $O(g_i(x)) = x^i$ then,

$$O(g_1(x)) + O(g_2(x)) + \ldots = x^k$$

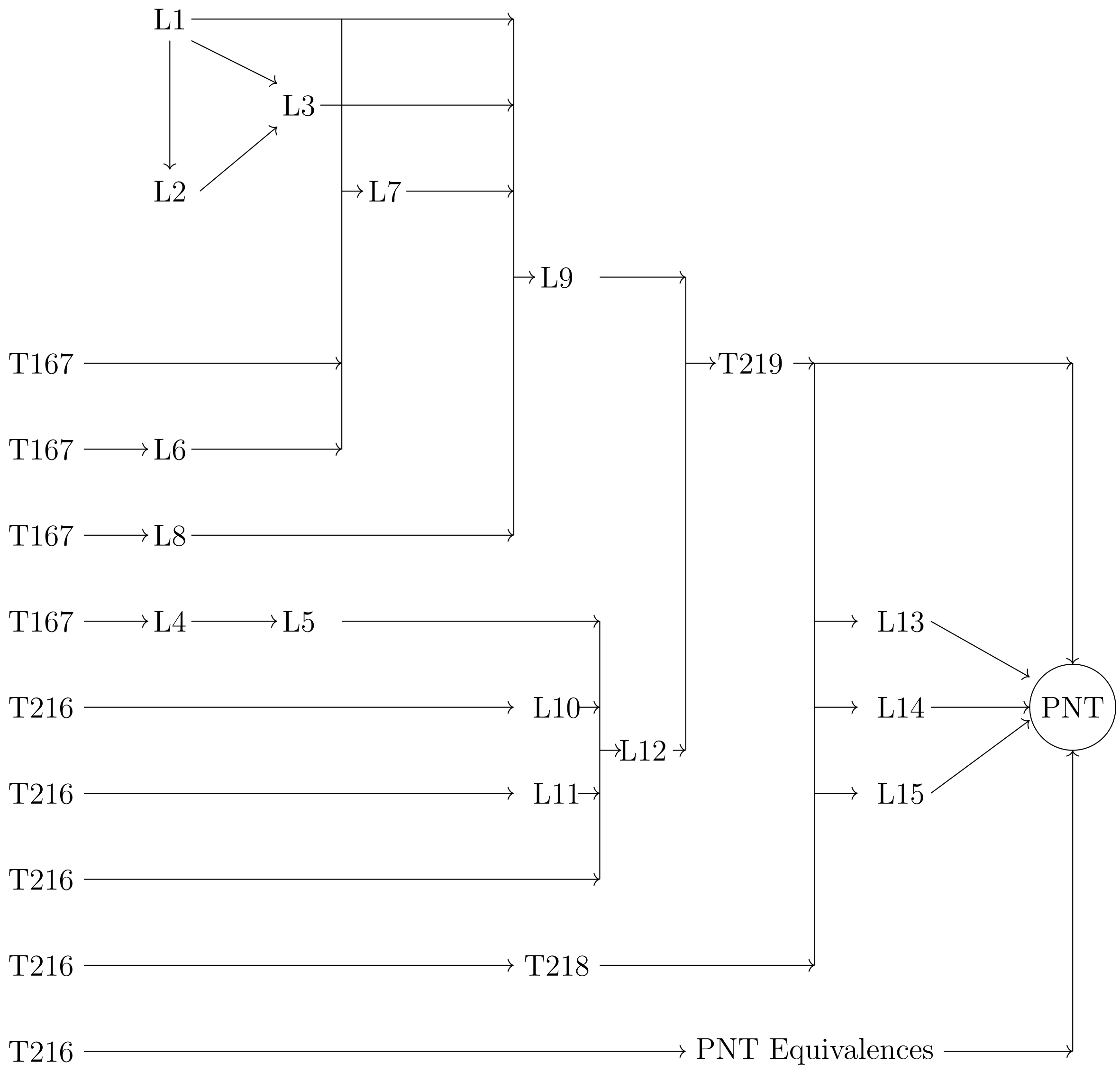
where k is the greatest of the powers of i.
If each of $g_i(x),\ i = 1, 2, 3\ldots$ satisfies $o(g_i(x)) = x^i$ then,

$$o(g_1(x)) + o(g_2(x)) + \ldots = x^j$$

where j is the least of the powers of x^i.

27.10 Selberg's Proof of the PNT

Selberg's proof of the Prime Number Theorem is set out in several texts including Nagell's "'Number Theory" and we will use that as a guide. There are 5 theorems and 15 lemmas. Many of these are quite long. We will not prove any of these lemmas so we just number them 1 to 15. We will assume them and prove the theorems. This will give a taste of how Selberg proceeded and leave the garnishments for your further study. The Pathway for Selberg's proof of the PNT is illustrated diagrammatically below. "T167" is Theorem 167 and "L9" is Lemma 9, etc.



Selberg's Pathway to the PNT

27.10.1 Equivalences to PNT

Mathematicians realized early on that it is easier to deal with other functions than $\pi(x)$ that involved the logarithm function and in particular the property $\log xy = \log x + \log y$. Let's first recall $\pi(x)$.

Definition 108. *pi function*
We define the pi function, the number of primes p less than or equal to x by,

$$\pi(x) = \sum_{p \le x} 1$$

That is as we progressively examine the numbers from 1 to x we add a 1 for each prime we encounter.

Example 130.

$$\begin{aligned}\pi(20) &= 1+1+1+1+1+1+1+1 = 8 \text{ \textit{matching} } 2,3,5,7,11,13,17,19\\ \pi(60) &= |\{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59\}| = 17 \qquad \diamond\end{aligned}$$

Definition 109. *theta function*
We define the Theta Function by,

$$\theta(x) = \sum_{p \le x} \log p$$

Example 131.

$$\theta(60) = \log 2 + \log 3 + \ldots + \log 59$$

We now prove that the prime number theorem is equivalent to a statement for either of these two functions, that is,

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = \lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$$

What Selberg actually proved is that as $x \to \infty$,

$$1 \le \frac{\theta(x)}{x} \le 1 \Rightarrow \lim_{x\to\infty} \frac{\theta(x)}{x} = 1$$

We need several theorems and lemmas.

Theorem 213.

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0.$$

Proof. In Theorem 211, page 312 we proved,

$$\frac{1}{6} < \frac{\pi(n)\log n}{n} < 9$$

This implies Chebyshev's proof that there are positive constants C_1, C_2 such that,

$$C_1 \frac{1}{\log x} < \frac{\pi(x)}{x} < C_2 \frac{1}{\log x} \text{ for all } x \in \mathbb{R}^+$$

Since $\lim_{x\to\infty} \dfrac{1}{\log x} = 0$, by the Squeeze Theorem 65, page 93, we have,

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0$$

□

Note 38.
We note $0 < \log\left(1+\frac{1}{n}\right) < \frac{1}{n}$ *which we prove as follows. We put* $x = \frac{1}{n}$ *in the series,*

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots,\ \ 0 \le x < 2$$

and group the terms thus,

$$\log\left(1+\frac{1}{n}\right) = \frac{1}{n} + \left(-\frac{1}{2n^2} + \frac{1}{3n^3}\right) + \left(-\frac{1}{4n^4} + \frac{1}{5n^5}\right) + \ldots$$

Then each of the braketed pairs is of the form,

$$\frac{-1}{na^n} + \frac{1}{(n+1)a^{n+1}} = \frac{-(n+1)a+n}{n(n+1)a^{n+1}} = \frac{n(1-a)-a}{n(n+1)a^{n+1}} < 0 \text{ since } a \ge 2$$

Therefore $\log\left(1+\frac{1}{n}\right) < \frac{1}{n}$.

Theorem 214.
As $x \to \infty$,

$$\theta(x) = \pi(x)\log x + o(x)$$

Proof. Note,

$$\pi(n) - \pi(n-1) = \begin{cases} 1 \text{ if } n = p \\ 0 \text{ if } n \ne p \end{cases}$$

where p is a prime, so that,

$$\log n \times [\pi(n) - \pi(n-1)] = \begin{cases} \log p\ if\ n = p \\ 0 \qquad if\ n \ne p \end{cases}$$

Now noting $\pi(1) = 0$,

$$\begin{aligned}
\theta(x) &= \sum_{p\le x}\log p \\
&= \sum_{2\le n\le x}\log n\,[\pi(n) - \pi(n-1)] \\
&= \log 2[\pi(2)-\pi(1)] + \log 3[\pi(3)-\pi(2)] + \log 4[\pi(4)-\pi(3)] + \ldots \\
&\qquad + \log[x][\pi(x) - \pi(x-1)] \\
&= \pi(2)[\log 2 - \log 3] + \pi(3)[\log 3 - \log 4] + \ldots \\
&\qquad + \pi(x-1)[\log([x]-1) - \log[x]) + \pi(x)\log[x] \\
&\text{(where we rearranged the terms in the previous line)} \\
&= -\pi(2)\log\frac{3}{2} - \pi(3)\log\frac{4}{3} + \ldots + \pi(x-1)\frac{\log[x]}{\log[x]-1} + \pi(x)\log[x]
\end{aligned}$$

$$\Rightarrow \theta(x) = \pi(x)\log[x] - \sum_{2\le n\le x-1}\pi(n)\log\left(1+\frac{1}{n}\right) \tag{27.10.1}$$

We have replaced $\pi(x-1)\dfrac{\log[x]}{\log[x]-1}$ with the last term in $\sum\limits_{2\le n\le x-1}\pi(n)\log\left(\dfrac{n+1}{n}\right)$. We can obviously do this if $x-1=n$ since then $[x]=n+1$ and $\pi(x-1)=\pi(n)$. Otherwise $x-1\le n<x$ so $\pi(x-1)=\pi(n)$ and $[x]=n$.

Furthermore, since $\lim\limits_{x\to\infty}\dfrac{\pi(x)}{x}=0$, for all $\epsilon>0$ there is a natural number N such that for all integers $n>N$, we have $\pi(n)\le\epsilon n$. This is so since $\dfrac{\pi(x)}{x}$ is getting smaller and smaller as $x\to\infty$ so for any positive number ϵ, $\dfrac{\pi(x)}{x}$ will be less than ϵ for some value of x which we label N. Reverting to integers we can say for all $\epsilon>0$ we can make $\dfrac{\pi(x)}{x}<\epsilon$ by choosing $x=N$. Using $\pi(x)<\epsilon x$ together with the fact that, by Note 38 above, $\log\left(1+\dfrac{1}{n}\right)<\dfrac{1}{n}$, and applying the sum to both sides, we have,

$$\begin{aligned}\sum_{2\le n\le x-1}\pi(n)\log\left(1+\frac{1}{n}\right)&\le\sum_{2\le n\le x-1}\epsilon n\frac{1}{n}\\&\le\epsilon\sum_{2\le n\le x-1}1\\&\le\epsilon(x-2)\\&\le\epsilon x\end{aligned}$$

so that,

$$\sum_{2\le n\le x-1}\pi(n)\log\left(1+\frac{1}{n}\right)=o(x)$$

since we have the condition “for all ϵ” which means we can take $\epsilon\to0$.

By (27.10.1),

$$\begin{aligned}\theta(x)&=\pi(x)\log[x]-\sum_{2\le n\le x-1}\pi(n)\log\left(1+\frac{1}{n}\right)\\&=\pi(x)\log x+o(x)\end{aligned}\tag{27.10.2}$$

□

Corollary 215.

$$\lim_{x\to\infty}\frac{\theta(x)}{x}=\lim_{x\to\infty}\frac{\pi(x)\log x}{x}$$

Proof. Uing (27.10.2),

$$\begin{aligned}\frac{\theta(x)}{x}&=\frac{\pi(x)\log x}{x}+\frac{o(x)}{x}\\\Rightarrow\lim_{x\to\infty}\frac{\theta(x)}{x}&=\lim_{x\to\infty}\frac{\pi(x)\log x}{x}+\lim_{x\to\infty}\frac{o(x)}{x}\end{aligned}$$

and by definition of $o(x)$, $\lim_{x\to\infty} \dfrac{o(x)}{x} = 0$, so we have our result,

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = \lim_{x\to\infty} \frac{\pi(x)\log x}{x} \tag{27.10.3}$$

□

Note 39. *The Prime Number Theorem can therefore be proved for either of the following,*

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1 \textit{ or } \lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$$

Selberg actually proved $\lim_{x\to\infty} \dfrac{\theta(x)}{x} = 1$ *after Chebyshev proved the following result.*

Theorem 216. *(Chebyshev)*
There exist positive constants C_1, C_2 such that,

$$C_1 x < \theta(x) < C_2 x$$

Proof. Using (27.10.3),

$$C_1 < \frac{\pi(x)\log x}{x} < C_2 \Rightarrow C_1 < \frac{\theta(x)}{x} + \frac{o(x)}{x} < C_2 \Rightarrow C_1 < \frac{\theta(x)}{x} < C_2$$

when x is sufficiently large since again $\lim_{x\to\infty} \dfrac{o(x)}{x} = 0$. □

27.10.2 Two Critical Theorems

As the pathway for Selberg's proof of the PNT shows, there are two major theorems T218 and T219 that are needed for the proofs of the final three lemmas L13, L14 and L15 and thence the PNT itself. Let us now prove T218. We first need a lemma.

Lemma 217.
For all integers $h \geq 2$,

$$(h-1)\log\left(1 + \frac{1}{h-1}\right) < 1$$

Proof. We have from Theorem 145, page 216,

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots \text{ if } -1 < x < 1.$$

Putting $x = \dfrac{1}{h-1}$ we have,

$$\log\left(1 + \frac{1}{h-1}\right) = \frac{1}{h-1} + \left[-\frac{1}{2(h-1)^2} + \frac{1}{3(h-1)^3}\right] + \left[-\frac{1}{4(h-1)^4} + \frac{1}{5(h-1)^5}\right] + \ldots$$

If we group the terms in pairs as shown and multiply by $h-1$ then,

$$(h-1)\log\left(1+\frac{1}{h-1}\right) = 1+\left[-\frac{1}{2(h-1)^1}+\frac{1}{3(h-1)^2}\right]+\left[-\frac{1}{4(h-1)^3}+\frac{1}{5(h-1)^4}\right]+\ldots$$

$$= 1+\sum_{k=2}^{\infty}\left[-\frac{1}{k(h-1)^{k-1}}+\frac{1}{(k+1)(h-1)^k}\right]$$

But,

$$\frac{1}{(k+1)(h-1)^k}-\frac{1}{k(h-1)^{k-1}} = \frac{1}{(h-1)^{k-1}}\left[\frac{1}{(k+1)(h-1)}-\frac{1}{k}\right]$$

$$= \frac{1}{(h-1)^{k-1}}\left[\frac{k-(k+1)(h-1)}{k(k+1)(h-1)}\right]$$

$$= \frac{1}{(h-1)^{k-1}}\left[\frac{2k+1-h(k+1)}{k(k+1)(h-1)}\right]$$

which is less than 0 if $h \geq 2$ since the numerator is $(2-h)k+(1-h)$, making,

$$(h-1)\log\left(1+\frac{1}{h-1}\right) < 1$$

□

Theorem 218.

$$\sum_{p\leq x}\frac{\log p}{p} = \log x + \phi(x)$$

where ϕ is a bounded function of x such that $|\phi(x)| < k, k \in \mathbb{R}^+$.

Proof. From equation (27.8.2) of Corollary 210, page 311,

$$\log n! = \sum_{p\leq n}\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]\log p$$

$$= \sum_{p\leq n}\left[\frac{n}{p}\right]\log p + \sum_{p\leq n}\sum_{r=2}^{\infty}\left[\frac{n}{p^r}\right]\log p$$

(where we separated the $r=1$ term)

$$\leq \sum_{p\leq n}\left[\frac{n}{p}\right]\log p + \sum_{p\leq n}\left[\left(\frac{n}{p^2}\right)+\left(\frac{n}{p^3}\right)+\ldots\right]\log p$$

where we use $\left[\frac{n}{p}\right] \leq \left(\frac{n}{p}\right)$. The second sum on the right side contains an infinite geometric series with $a = \frac{n}{p^2}$ and $r = \frac{1}{p} < 1$ hence, using $S_\infty = \frac{a}{1-r}$,

$$\log n! \leq \sum_{p\leq n}\left[\frac{n}{p}\right]\log p + \sum_{p\leq n}\left(\frac{n/p^2}{1-1/p}\right)\log p$$

$$\Rightarrow \sum_{p\leq n}\left[\frac{n}{p}\right]\log p \geq \log n! - \sum_{p\leq n}\left(\frac{n}{p(p-1)}\right)\log p \qquad (27.10.4)$$

The introduction of $\theta(n) = \sum_{p\le n} \log p$ follows by applying $\sum_{p\le n} \log p$ to each term of $\frac{n}{p} > \left[\frac{n}{p}\right] > \frac{n}{p} - 1$ to obtain,

$$\begin{aligned}
&\sum_{p\le n}\left(\frac{n}{p}\right)\log p > \sum_{p\le n}\left[\frac{n}{p}\right]\log p > \sum_{p\le n}\left(\frac{n}{p}\right)\log p - \sum_{p\le n}\log p \\
&\Rightarrow \sum_{p\le n}\left(\frac{n}{p}\right)\log p > \sum_{p\le n}\left[\frac{n}{p}\right]\log p > \sum_{p\le n}\left(\frac{n}{p}\right)\log p - \theta(n) \\
&\Rightarrow \theta(n) + \sum_{p\le n}\left[\frac{n}{p}\right]\log p > \sum_{p\le n}\left(\frac{n}{p}\right)\log p \qquad (27.10.5)
\end{aligned}$$

From (27.10.3) and (27.10.4) we have,

$$\begin{aligned}
&\theta(n) > \sum_{p\le n}\left(\frac{n}{p}\right)\log p - \log n! + \sum_{p\le n}\left(\frac{n}{p(p-1)}\right)\log p \\
\Rightarrow\ &\theta(n) > \sum_{p\le n}\left(\frac{n}{p}\right)\log p - \log n! + \sum_{p\le n}\left(\frac{n}{p-1}\right)\log p - \sum_{p\le n}\left(\frac{n}{p}\right)\log p \\
\Rightarrow\ &\theta(n) > -\log n! + \sum_{p\le n}\left(\frac{n}{p}\right)\log p, \text{ since } \frac{1}{p-1} > \frac{1}{p}
\end{aligned}$$

But, $C_1 < \frac{\theta(n)}{n} < C_2$ implies $\frac{\theta(n)}{n}$ is bounded so $\pm(-\frac{1}{n}\log n! + \sum_{p\le n}\left(\frac{1}{p}\right)\log p)$ is also bounded, say,

$$-\alpha < \frac{1}{n}\log n! - \sum_{p\le n}\left(\frac{1}{p}\right)\log p < \alpha \qquad (27.10.6)$$

where α is a function of n such that $|\alpha| < K, K \in \mathbb{R}^+$.

***

We now apply Lemma 217 to the algebraic identity,

$$h = \frac{h^h}{(h-1)^{h-1}} \cdot \frac{(h-1)^{h-1}}{h^{h-1}} = \frac{h^h}{(h-1)^{h-1}} \cdot \frac{1}{\left(1 + \frac{1}{h-1}\right)^{h-1}}$$

for $h \ge 2$. Taking logs, we have,

$$\begin{aligned}
&\log h = h\log h - (h-1)\log(h-1) - (h-1)\log\left(1 + \frac{1}{h-1}\right) \\
&\Rightarrow \log h < h\log h - (h-1)\log(h-1) \qquad (27.10.7)
\end{aligned}$$

Applying the Lemma, we also have the inequalities,

$$\begin{aligned}
&(h-1)\log\left(1+\frac{1}{h-1}\right) < 1\\
&\Rightarrow (h-1)\log\left(\frac{h}{h-1}\right) < 1\\
&\Rightarrow (h-1)\log h - (h-1)\log(h-1) < 1\\
&\Rightarrow h\log h - \log h - (h-1)\log(h-1) < 1\\
&\Rightarrow h\log h - (h-1)\log(h-1) - 1 < \log h \qquad (27.10.8)
\end{aligned}$$

and (27.10.6) together with (27.10.7) gives,

$$h\log h - (h-1)\log(h-1) - 1 < \log h < h\log h - (h-1)\log(h-1)$$

and therefore,

$$\sum_{h=2}^{n}[h\log h - (h-1)\log(h-1) - 1] < \sum_{h=2}^{n}\log h < \sum_{h=2}^{n}[h\log h - (h-1)\log(h-1)] \qquad (27.10.9)$$

Now,

$$\begin{aligned}
&\sum_{h=2}^{n}[h\log h - (h-1)\log(h-1)]\\
&= 2\log 2 - 1\log 1 + 3\log 3 - 2\log 2 + \ldots + n\log n - (n-1)\log(n-1)\\
&= n\log n
\end{aligned}$$

and,

$$\sum_{h=2}^{n} -1 = -(n-1)$$

and,

$$\sum_{h=2}^{n}\log h = \log 2 + \log 3 + \ldots \log n = \log 2\cdot 3\cdots n = \log n!$$

Hence (27.10.8) yields,

$$\begin{aligned}
&n\log n - (n-1) < \log n! < n\log n\\
&\Rightarrow \log n - \frac{(n-1)}{n} < \frac{\log n!}{n} < \log n \qquad (27.10.10)
\end{aligned}$$

We also have (27.10.5), namely,

$$-\alpha < \frac{1}{n}\log n! - \sum_{p\le n}\left(\frac{1}{p}\right)\log p < \alpha$$

Subtracting, (27.10.9)-(27.10.5), we have,

$$\log n - \frac{(n-1)}{n} + \alpha < \sum_{p \le n} \frac{\log p}{p} < \log n - \alpha$$
$$\Rightarrow -\frac{(n-1)}{n} + \alpha < \sum_{p \le n} \frac{\log p}{p} - \log n < -\alpha$$

Hence, $\sum_{p \le n} \frac{\log p}{p} - \log n$ is bounded by a function of n, so with x replacing n,

$$\sum_{p \le x} \frac{\log p}{p} = \log x + \phi$$

where ϕ is a bounded function of x such that $|\phi(x)| < k, k \in \mathbb{R}^+$ so we can also write

$$\sum_{p \le \sqrt{x}} \frac{\log p}{p} = \log x + O(1)$$

. □

27.10.3 Selberg's Asymptotic Formula

The crucial Theorem 219 in Selberg's proof (and in that of Erdös) is of Selberg's asymptotic formula. In turn, the proof of the asymptotic formula requires two lemmas, L9 and L12. L9 was the end point of a series of known results largely dependent on the Möbius function, while L12 is itself a major result due to Selberg, being the culmination of a series of lemmas mostly emanating from Chebyshev's Theorem 216. Let us, for now, assume L9 and L12 and proceed to prove T219 and then the PNT. We assume,

Lemma 9.
$$\sum_{d \le x} \frac{\mu(d)}{d} \left(\log \frac{x}{d}\right)^2 = 2 \log x + O(1)$$

Lemma 12.
$$\sum_{n \le x} f(n) = (\log x)\theta(x) + \sum_{p \le \sqrt{x}} \theta\left(\frac{x}{p}\right) + o(x \log x)$$

where, referencing Lemma 9, for $\lambda(d) = \mu(d)\left(\log \frac{x}{d}\right)^2$ *we put* $f(n) = \sum_{d|n} \lambda(d)$.

Theorem 219. *(Selberg's Asymptotic formula)*

$$\theta(x)\log x + \sum_{p \le \sqrt{x}} \theta\left(\frac{x}{p}\right) \log p - 2x \log x = o(x \log x) \tag{27.10.11}$$

Proof. According to Lemma 12, the left-hand side of the required equation is equal to,

$$\sum_{n\le x} f(n) - 2x\log x + o(x\log x)$$

According to the definition of $f(n)$ in Lemma 12 we have,

$$\sum_{n\le x} f(n) = \sum_{n\le x}\sum_{d|n}\lambda(d)$$

Hence[4],

$$\begin{aligned}\sum_{d\le x} f(n) &= \sum_{d\le x}\lambda(d)\left[\frac{x}{d}\right]\\ &= \sum_{d\le x}\lambda(d)\left(\frac{x}{d}-\epsilon_d\right),\ 0\le\epsilon_d<1\\ &= \sum_{d\le x}\lambda(d)\frac{x}{d}-\epsilon_d\sum_{d\le x}\lambda(d)\end{aligned}$$

Now by definition,

$$\begin{aligned}&\lambda(d) = \mu(d)\left(\log\frac{x}{d}\right)^2\\ \Rightarrow&|\epsilon_d\lambda(d)| = |\epsilon_d\mu(d)|\left(\log\frac{x}{d}\right)^2 = \left(\log\frac{x}{d}\right)^2 = o(x\log x)\\ \Rightarrow&\epsilon_d\sum_{d\le x}\lambda(d) = o(x\log x)\end{aligned}$$

Hence,

$$\begin{aligned}\sum_{n\le x} f(n) &= \sum_{d\le x}\lambda(d)\frac{x}{d} + o(x\log x)\\ &= \sum_{d\le x} x\frac{\mu(d)}{d}\left(\log\frac{x}{d}\right)^2 + o(x\log x)\end{aligned}$$

[4] Why is $\sum_{n\le x}\sum_{d|n}\lambda(d) = \sum_{d\le x}\lambda(d)\left[\frac{x}{d}\right]$?
Let's take an example with $x = 5$. Then,

$$\begin{aligned}\sum_{n\le 5}\sum_{d|n}\lambda(d) &= \sum_{n=1}\sum_{d|1}\lambda(1) + \sum_{n=2}\sum_{d|2}\lambda(2) + \sum_{n=3}\sum_{d|3}\lambda(3) + \sum_{n=4}\sum_{d|4}\lambda(4) + \sum_{n=5}\sum_{d|5}\lambda(5)\\ &= \lambda(1) + (\lambda(1)+\lambda(2)) + (\lambda(1)+\lambda(3)) + (\lambda(4)+\lambda(2)+\lambda(1)) + (\lambda(1)+\lambda(5))\\ &= 5\lambda(1) + 2\lambda(2) + \lambda(3) + \lambda(4) + \lambda(5)\end{aligned}$$

while,

$$\begin{aligned}\sum_{d\le 5}\lambda(d)\left[\frac{5}{d}\right] &= \lambda(1)\left[\frac{5}{1}\right] + \lambda(2)\left[\frac{5}{2}\right] + \lambda(3)\left[\frac{5}{3}\right] + \lambda(4)\left[\frac{5}{4}\right] + \lambda(5)\left[\frac{5}{5}\right]\\ &= 5\lambda(1) + 2\lambda(2) + \lambda(3) + \lambda(4) + \lambda(5)\end{aligned}$$

By Lemma 9,

$$\begin{aligned} &x \sum_{d \le x} \frac{\mu(d)}{d} \left(\log \frac{x}{d} \right)^2 = 2 \log x + O(1) \\ &\Rightarrow \sum_{n \le x} f(n) = 2x \log x + o(x \log x) + O(1)) \end{aligned}$$

Hence the left side of the Theorem's equation (27.10.10) becomes,

$$\begin{aligned} &\theta(x) \log x + \sum_{p \le \sqrt{x}} \theta\left(\frac{x}{p}\right) \log p - 2x \log x \\ &= \sum_{n \le x} f(n) - 2x \log x + o(x \log x) \\ &= 2x \log x + o(x \log x) - 2x \log x + o(x \log x) + O(1) \\ &= o(x \log x) \end{aligned}$$

Note $O(1)$ is "absorbed by" $o(x \log x)$ and $o(x \log x) + o(x \log x) = o(x \log x)$. □

27.10.4 Proof of the Prime Number Theorem

Definition 110. *limit inferior, limit superior*
We define the limit inferior, lim inf, *and the limit superior,* lim sup, *to be the limiting bounds of a function $f(x)$ as $x \to \infty$ and write*

$$\liminf_{x \to \infty} \; f(x) < f(x) < \limsup_{x \to \infty} \; f(x)$$

Theorem 220. *(Prime Number Theorem)*

$$\lim_{x \to \infty} \frac{\theta(x)}{x} = 1$$

Proof. Let $a = \liminf_{x \to \infty} \dfrac{\theta(x)}{x}$ and $A = \limsup_{x \to \infty} \dfrac{\theta(x)}{x}$. We want to prove $a = A = 1$.
We first prove $a + A = 2$.
Choose x large so that

$$\theta(x) = ax + o(x)$$

Then since[5],

$$\theta(x) \le Ax + o(x) \Rightarrow \theta\left(\frac{x}{p}\right) \le A\left(\frac{x}{p} + o(x)\right)$$

it follows from Selberg's asymptotic formula,

$$\theta(x) \log x + \sum_{p \le \sqrt{x}} \theta\left(\frac{x}{p}\right) \log p - 2x \log x = o(x \log x) \tag{27.10.12}$$

[5] Note if $\theta(x)$ equals its lim inf then it must be less than or equal to its lim sup and vice versa.

that[6],

$$ax\log x + o(x\log x) + \sum_{p\leq\sqrt{x}} A\frac{x}{p}\log p \geq 2x\log x + o(x\log x)$$

Using Chebyshev's result in Theorem 218 that,

$$\sum_{p\leq\sqrt{x}} \frac{\log p}{p} \to \log x + O(1) \text{ as } x \to \infty$$

we have,

$$\begin{aligned} &ax\log x + o(x\log x) + Ax\log x \geq 2x\log x + o(x\log x) \\ &\Rightarrow a + A \geq 2. \end{aligned}$$

On the other hand we can choose x so large that,

$$\theta(x) = Ax + o(x)$$

Then, since

$$\theta(x) \geq ax + o(x)$$

it immediately follows as before that,

$$Ax\log x + o(x\log x) + \sum_{p\leq\sqrt{x}} a\frac{x}{p}\log p \leq 2x\log x + o(x\log x)$$

from which we get,

$$a + A \leq 2$$

Thus,

$$a + A = 2$$

We now write Selberg's asymptotic formula in Theorem 219 in the form,

$$\frac{\theta(x)}{x} + \sum_{p\leq x} \frac{\theta(x/p)}{x/p}\frac{\log p}{p\log x} = 2 + O\left(\frac{1}{\log x}\right)$$

We choose x large so that $\dfrac{\theta(x/p)}{x/p}$ is near A. Since $a + A = 2$ it follows from the asymptotic formula and Chebyshev's Theorem 218 that $\sum_{p\leq x}\dfrac{\log p}{p\log x} \to 1$ as $x \to \infty$, that $\dfrac{\theta(x)}{x}$ must be near a for most primes $p \leq x$. If S denotes the set of primes for which this is not true, then we have,

$$\frac{\sum\limits_{\substack{p\leq x\\ p\in S}} \dfrac{\log p}{p}}{\sum\limits_{p\leq x} \dfrac{\log p}{p}} \to 0 \; as \; x \to \infty$$

[6] Note $o(x)$ is "absorbed by" $o(x\log x)$.

Now we choose a small prime $q \in S$ such that $\dfrac{\theta(x/q)}{x/q}$ is near a. Rewriting the asymptotic formula with x replaced by $\dfrac{x}{q}$, the same argument as above leads us to conclude that $\dfrac{\theta(x/q)}{x/q}$ is near A for most primes $p \leq \dfrac{x}{q}$. It follows that

$$\theta(x/p) \approx ax/p$$

for most primes $p \leq x$, and,

$$\theta(x/pq) \approx Ax/pq$$

for most primes $p \leq x/q$.
A contradiction is obtained (using Erdös's idea of non-overlapping intervals which we have not discussed) unless $a = A$ and therefore,

$$a = A = 1$$

□

Let us now consider the outline of the pathways to the two Lemmas 9 and 12.

27.10.5 Pathway to Lemma 9

The Theorem and Lemmas leading to Lemma 9 all depend on the Möbius function, studied earlier in Chapter 24. These results were well-known. We proved the first two earlier.

Theorem 166.

$$\sum_{d|n} \mu(d) = 0$$

Lemma 1. *(Euler Macheroni Constant and Harmonic Series)*
There exists a constant γ such that,

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

Lemma 2.
There exists a constant c such that,

$$\sum_{n \leq x} \frac{\log n}{n} = \frac{1}{2}(\log x)^2 + c + O\left(\frac{\log x}{x}\right)$$

We use lemmas 1 and 2 to prove Lemma 3.

Lemma 3.
If $\tau(n)$ denotes the number of positive dividers of n then,

$$\sum_{n \leq x} \frac{\tau(n)}{n} = \frac{1}{2}(\log x)^2 + 2\gamma \log x + \gamma^2 - 2c + O\left(\frac{\log x}{\sqrt{x}}\right)$$

We need only Theorem 166 to prove Lemmas 6 and 8.

Lemma 6.

$$\left|\sum_{d=1}^{x}\frac{\mu(d)}{d}\le 1\right|$$

Lemma 8.

$$\sum_{d|n}\mu(d)\tau\left(\frac{n}{d}\right)=1$$

Next, we use Lemmas 1, 6 and 8 together with Theorem 164 to prove,

Lemma 7.

$$\sum_{d\le x}\frac{\mu(d)}{d}\log\frac{x}{d}=O(1)$$

Finally, we use Lemmas 1, 6, 7 and 8 to prove Lemma 9.

Lemma 9.

$$\sum_{d\le x}\frac{\mu(d)}{d}\left(\log\frac{x}{d}\right)^2=2\log x+O(1)$$

27.10.6 Pathway to Lemma 12

The Theorem and Lemmas leading to Lemma 12 depend on the Möbius function but also on the critical theorem of Chebyshev that there exist bounding constants C_1, C_2 such that,

$$C_1<\frac{\theta(x)}{x}<C_2$$

Lemma 4 was also a well-known lemma from the study of the Möbius function.

Lemma 4.
Defining $\phi_h(n)=\sum_{d|n}\mu(d)(\log d)^h$, *we have,*

$$\phi_h(n)=0$$

if n *is divisible by more than* h *different primes.*

We finally switch to sums over primes to prove Lemma 12. The sequence of lemmas is,

Lemma 10.

$$\sum_{p\le x}(\log p)\left(\log\frac{x}{p}\right)=o(x\log x)$$

Lemma 11.

$$\sum_{p^\alpha \leq x} \log p = O(x), \ \ \alpha \in \mathbb{N}$$

Finally, we can obtain,

Lemma 12.

$$\sum_{n\leq x} f(n) = (\log x)\theta(x) + 2 \sum_{p\leq\sqrt{x}} \theta\left(\frac{x}{p}\right) + o(x \log x)$$

where for $\lambda(d) = \mu(d)\left(\log \frac{x}{d}\right)^2$ *we put* $f(n) = \sum_{d|n} \lambda(d)$.

27.11 Lemmas 13-15

Finally we need Lemmas 13, 14 and 15 that feed into the PNT.

Lemma 13.

If $\limsup_{x\to\infty} \frac{\theta(x)}{x} = A$ *and* $\liminf_{x\to\infty} \frac{\theta(x)}{x} = a$ *then* $a + A = 2$.

The proof of Lemma 13 has been included in our proof of the PNT.

Lemma 14.
If λ *is a given number greater than* a *and if the sum* $S(x) = \sum \frac{\log p}{p}$ *extends over all primes* $p \leq x$ *and such that* $\theta\left(\frac{x}{p}\right) \geq \frac{\lambda x}{p}$ *then the quotient* $\frac{S(x)}{\log x}$ *tends to 0 for* $x \to \infty$.

Lemma 15.
If μ *is a given positive number* $< A$ *and if the sum*

$$R(x) = \sum \left(\frac{\log p}{p}\right)\left(\frac{\log q}{q}\right)$$

extends over all the primes p *and* q *that satisfy the conditions,*

$$p \leq \sqrt{x}, \ q \leq \sqrt{\frac{x}{p}}, \ \theta\left(\frac{x}{pq}\right) \leq \frac{\mu x}{pq},$$

then the quotient $\frac{R(x)}{(\log x)^2}$ *tends to 0 for* $x \to \infty$.

Chapter 28

Bertrand's Postulate

Bertrand postulated (an educated "guess") that there is always a prime number between any integer greater than 1 and double that integer. That is, for every natural number $n > 1$, there is a prime number p such that $n < p < 2n$. This is now a theorem.

Course: Dessert
Ingredients
Primes
Binomial Coefficients and Binomial Theorem
Factorials
Logarithms
Directions
Study the binomial coefficient $\binom{2n}{n}$ *and derive inequalities for it in terms of powers of 2 and powers of prime numbers.*
Find the highest powers of the primes that divide n!
Prove Bertrand's conjecture

28.1 Preliminaries

Lemma 221.
The product $\prod_{r\le p\le n} p$ *is a divisor of* $\binom{n}{r}$ *so* $\prod_{r\le p\le n} p < \binom{n}{r}$.

Proof. We may assume $r < \frac{n}{2}$ since given,

$$\binom{n}{r} = \binom{n}{n-r} = \frac{n!}{(n-r)!r!},$$

then if $r > \frac{n}{2}$ then,

$$-r < -\frac{n}{2} \Rightarrow n - r < n - \frac{n}{2} = \frac{n}{2}$$

So if we have $\binom{n}{r}$ with $r > \frac{n}{2}$ then we replace it with $\binom{n}{n-r}$ with $r < \frac{n}{2}$.
Then since[1] the formula

$$n(n-1)\cdots(n-r+1) = \binom{n}{r} \cdot r(r-1)\cdots 1$$

shows any prime in the range n to $n-r+1$ is bigger than r and must therefore divide $\binom{n}{r}$. Accordingly, the product $\prod_{r \le p \le n} p$ is a divisor of $\binom{n}{r}$. □

Lemma 222.

$$2\binom{2k+1}{k+1} \le 2^{2k+1}$$

Proof. We first note $\binom{2k+1}{k+1} = \binom{2k+1}{k}$. Then,

$$\begin{aligned} 2\binom{2k+1}{k+1} &= \binom{2k+1}{k} + \binom{2k+1}{k+1} \\ &\le \binom{2k+1}{0} + \binom{2k+1}{1} + \ldots + \binom{2k+1}{k} + \binom{2k+1}{k+1} + \ldots + \binom{2k+1}{2k+1} \end{aligned}$$

which is the binomial expansion of $(1+1)^{2k+1} = 2^{2k+1}$. □

Theorem 223.
Let $n \ge 2$ be an integer, then $\prod_{p \le n} p < 4^n$ where the product on the left is of all primes less than or equal to n.

Proof. The proof is by induction.
Basis step: If $n = 2$ then the statement $2 < 4^2$ is obviously true.
Assumption step: Let us now assume the statement is true of all integers less than n, that is, $\prod_{p \le n-1} p < 4^{n-1}$ is true. Since there are no primes between $2k$ and $2k+1$ we may assume n is odd, say $n = 2k+1$. Then the assumption is $\prod_{p \le 2k} p < 4^{2k}$ for all integers less than or equal to $2k$ and, in particular since $k+1 < 2k$ our assumption becomes $\prod_{p \le k+1} p < 4^{k+1}$.
Inductive step: We want to prove $\prod_{p \le n} p < 4^n$ is true for $n > k+1$.
From Lemma 221 we have $\prod_{k+1 < p \le n} p < \binom{n}{k+1}$.
From Lemma 222 we have $\binom{2k+1}{k+1} < 2^{2k}$.

[1] $\frac{n}{2} > r \Rightarrow n > 2r \Rightarrow n - r + 1 > 2r - r + 1 \Rightarrow n - r + 1 > r + 1 > r$.

From the inductive assumption we have $\prod\limits_{p \le k+1} p < 4^{k+1}$.

Hence,

$$\begin{aligned}\prod_{p \le n} p &= \prod_{p \le k+1} p \cdot \prod_{k+1 < p \le n} p \\ &< 4^{k+1} \cdot \binom{n}{k+1} \\ &= 4^{k+1} \cdot \binom{2k+1}{k+1} \\ &< 4^{k+1} \cdot 2^{2k} \\ &= 4^n.\end{aligned}$$

□

We have already encountered k_p and m_p in Chapter 27 but we will repeat the introductory lemmas and corollaries.

Lemma 224.
For $n \ge 2, n \in \mathbb{Z}$, consider the prime factorizations

$$\begin{aligned} n! &= \prod_{p \le n} p^{k_p} = 2^{k_2} 3^{k_3} \cdots, k_p \in \mathbb{Z}^+ \\ (2n)! &= \prod_{p \le 2n} p^{l_p} = 2^{l_2} 3^{l_3} \cdots, l_p \in \mathbb{Z}^+ \end{aligned}$$

Then $k_p = \prod\limits_{r=1}^{\infty} \left[\dfrac{n}{p^r}\right]$ and $l_p = \prod\limits_{r=1}^{\infty} \left[\dfrac{2n}{p^r}\right]$.
That is, $n!$ contains the prime factor p k_p times and $(2n)!$ contains the prime factor p l_p times.

Proof. Consider the integers $1, 2, 3, \ldots, n$.
The ones divisible by p are $p, 2p, 3p, \ldots, m_1 p$ where $m_1 p \le n < (m_1 + 1)p$. Then,

$$m_1 p \le n < (m_1 + 1)p \Rightarrow m_1 \le \frac{n}{p} < m_1 + 1 \Rightarrow m_1 = \left[\frac{n}{p}\right].$$

Similarly, the ones divisible by p^2 are $p^2, 2p^2, 3p^2, \ldots, m_2 p^2$ where

$$m_2 p \le n < (m_2 + 1)p \Rightarrow m_2 = \left[\frac{n}{p^2}\right].$$

Noting $\left[\dfrac{n}{p^r}\right] = 0$ for $p^r > n$, we conclude $k_p = \prod\limits_{r=1}^{\infty} \left[\dfrac{n}{p^r}\right]$.
Similarly, $l_p = \prod\limits_{r=1}^{\infty} \left[\dfrac{2n}{p^r}\right]$. □

Corollary 225.
The binomial coefficient $\binom{2n}{n}$ *contains the prime factor* p *exactly,*

$$m_p = \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right)$$

times. That is, m_p *is the largest power of* p *that divides* $\binom{2n}{n}$.

Proof. Since $\binom{2n}{n} = \frac{(2n)!}{n!n!}$, by Lemma 224 the numerator contains the prime factor p exactly $\sum_{k=1}^{\infty}\left[\frac{2n}{p^k}\right]$ times while the denominator contains the prime factor p exactly $2\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$ times. So $\binom{2n}{n}$ contains the prime factor p exactly

$$m_p = \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right)$$

times. □

Corollary 226.

$$\log n! = \sum_{p\le n} k_p \log p = \sum_{p\le n}\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]\log p$$

$$\log(2n)! = \sum_{p\le 2n} k_p \log p = \sum_{p\le 2n}\sum_{r=1}^{\infty}\left[\frac{2n}{p^r}\right]\log p$$

Proof. Using Lemma 224,

$$n! = \prod_{p\le n} p^{k_p} \Rightarrow \log n! = \sum_{p\le n} k_p \log p = \sum_{p\le n}\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]\log p$$

Similarly,

$$(2n)! = \sum_{p\le 2n}\sum_{r=1}^{\infty}\left[\frac{2n}{p^r}\right]\log p$$

□

Corollary 227.

$$p^{m_p} \le 2n \tag{28.1.1}$$

Proof. By Corollary 226, with,

$$m_p = \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right),$$

we have,

$$\begin{aligned}
\log\binom{2n}{n} &= \log\frac{(2n)!}{n!n!} = \log(2n)! - 2\log n! \\
&= \sum_{p\leq 2n}\sum_{r=0}^{\infty}\left[\frac{2n}{p^r}\right]\log p - 2\sum_{p\leq n}\sum_{r=0}^{\infty}\left[\frac{n}{p^r}\right]\log p \\
&= \sum_{p\leq 2n} m_p \log p,
\end{aligned}$$

where we replaced $\prod\limits_{p\leq n}$ with $\prod\limits_{p\leq 2n}$ since beyond $2n$, $\left[\frac{2n}{p}\right] = 0$ and $\left[\frac{n}{p}\right] = 0$. Also,

$$\begin{aligned}
m_p &= \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) \\
\Rightarrow m_p &= \sum_{1\leq r\leq \frac{\log 2n}{\log p}}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) \qquad (28.1.2)
\end{aligned}$$

since $\left[\frac{2n}{p^r}\right] = 0$ if $p^r > 2n$ or $r > \dfrac{\log 2n}{\log p}$.

Now, for $x \in \mathbb{R}$, we have $x = [x] + \delta, 0 \leq \delta < 1$, so that,

$$[2x] - 2[x] = 2[x] + 2\delta - 2[x] = 2\delta = \begin{cases} 0 \text{ if } 0 \leq \delta < \frac{1}{2} \\ 1 \text{ if } \delta \geq \frac{1}{2} \end{cases}$$

Therefore,

$$\begin{aligned}
&\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right] = 0 \text{ or } 1 \\
&\Rightarrow \left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right] \leq 1 \\
&\Rightarrow m_p \leq \sum_{1\leq r\leq \frac{\log 2n}{\log p}} 1 \ (using(28.1.2)) \\
&\Rightarrow m_p \leq \frac{\log 2n}{\log p} \\
&\Rightarrow m_p \log p \leq \log 2n \\
&\Rightarrow \log p^{m_p} \leq \log 2n \\
&\Rightarrow p^{m_p} \leq 2n.
\end{aligned}$$

□

Corollary 228.
If $\sqrt{2n} < p$ *then* $m_p \leq 1$.

Proof.
Let $\sqrt{2n} < p$. By Corollary 227,

$$p^{m_p} \leq 2n \Rightarrow m_p \leq \frac{\log 2n}{\log p}$$

Using $p \geq \sqrt{2n} \Rightarrow \log p > \frac{1}{2} \log 2n$ we have,

$$\begin{aligned} m_p &\leq \frac{\log 2n}{\log p} \\ \Rightarrow m_p &< \frac{\log 2n}{\frac{1}{2}\log 2n} \\ \Rightarrow m_p &< 2 \\ \Rightarrow m_p &\leq 1 \end{aligned}$$

□

Corollary 229.
If $\frac{2n}{3} < p \leq n$ *then* $m_p = 0$.

Proof. First,

$$\begin{aligned} \frac{2n}{3} < p \leq n \Rightarrow \frac{3}{2} > \frac{n}{p} \geq 1 \\ \Rightarrow \left[\frac{n}{p}\right] = 1 \\ \Rightarrow \left[\frac{n}{p^r}\right] = 0 \text{ if } r > 1. \end{aligned}$$

Second,

$$\begin{aligned} \frac{2n}{3} < p \leq n \Rightarrow 3 > \frac{2n}{p} \geq 2 \Rightarrow \left[\frac{2n}{p}\right] = 2 \\ \Rightarrow \left[\frac{2n}{p^r}\right] = 0 \text{ if } r > 1. \end{aligned}$$

Therefore, separating out the terms with $r > 1$,

$$\begin{aligned} m_p &= \sum_{r=1}^{\infty} \left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right) \\ &= \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] + \sum_{r=2}^{\infty} \left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right) \\ &= 2 - 2 + 0 = 0 \end{aligned}$$

□

Lemma 230.

$$4^n \leq 2n\binom{2n}{n}$$

Proof. Considering the binomial expansion of $(1+1)^{2n} = 2^{2n} = 4^n$ we have,

$$\begin{aligned}
4^n &= (1+1)^{2n} \\
&= \sum_{k=0}^{2n}\binom{2n}{k} \\
&= \binom{2n}{0} + \overbrace{\binom{2n}{1} + \binom{2n}{2} + \ldots + \binom{2n}{n} + \ldots + \binom{2n}{2n-2} + \binom{2n}{2n-1}}^{\text{2n-1 terms}} + \binom{2n}{2n} \\
&= 2 + \overbrace{\binom{2n}{1} + \binom{2n}{2} + \ldots + \binom{2n}{n} + \ldots + \binom{2n}{2n-2} + \binom{2n}{2n-1}}^{\text{2n-1 terms}} \\
&\text{since } \binom{2n}{0} = \binom{2n}{2n} = 1 \\
&\leq \binom{2n}{n} + \overbrace{\binom{2n}{n} + \binom{2n}{n} + \ldots + \binom{2n}{n}}^{2n-1 \text{terms}} \text{ since } \binom{2n}{n} > 2 \\
&\leq 2n\binom{2n}{n}
\end{aligned}$$

□

28.2 Bertrand's Postulate

Theorem 231. *(Bertrand's Postulate)*
For every natural number $n > 1$ there is a prime number p such that $n < p < 2n$.

Proof. The proof is by contradiction. Let's assume for some natural number $n > 1$ there are no primes p such that $n < p < 2n$. By Corollary 225, page 337, $\binom{2n}{n}$ contains the prime factor p exactly

$$m_p = \sum_{r=1}^{\infty}\left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right)$$

times and obviously does not contain any prime larger than $2n$. We can therefore write,

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{m_p}$$

Applying the assumption that there are no primes p with $n < p < 2n$ we can write,

$$\binom{2n}{n} = \prod_{p<n} p^{m_p}$$

Applying Corollary 229, which states "if $\frac{2n}{3} < p \leq n$ then $m_p = 0$" we can limit the sum further to

$$\binom{2n}{n} = \prod_{p \leq \frac{2n}{3}} p^{m_p}$$

We split this product into

$$\binom{2n}{n} = \prod_{p \leq \sqrt{2n}} p^{m_p} \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{m_p}$$

By Corollary 228, which showed "if $\sqrt{2n} < p$ then $m_p \leq 1$" the second product is less than $\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p$ and certainly therefore less than $\prod_{p \leq \frac{2n}{3}} p$ yielding,

$$\binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} p^{m_p} \cdot \prod_{p \leq \frac{2n}{3}} p$$

Applying Corollary 227 which showed "$p^{m_p} \leq 2n$" we then have,

$$\binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \cdot \prod_{p \leq \frac{2n}{3}} p$$

Applying Theorem 223 which showed "$\prod_{p \leq n} p < 4^n$" to the second product yields,

$$\binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \cdot 4^{\frac{2n}{3}}$$

We almost there. The product $\prod_{p \leq \sqrt{2n}} 2n$ is $2n$ raised to the power of the number of primes less than $\sqrt{2n}$. This number is clearly less than $\frac{\sqrt{2n}}{2}$ since every second integer is even and we can omit the number 1, giving,

$$\binom{2n}{n} \leq (2n)^{\frac{\sqrt{2n}}{2}-1} \cdot 4^{\frac{2n}{3}} \tag{28.2.1}$$

Finally, by Lemma 230, we have the fact that

$$2n\binom{2n}{n} \geq \sum_{k=0}^{n} \binom{2n}{k} = 4^n$$

so that,

$$\frac{1}{2n\binom{2n}{n}} \le \frac{1}{4^n} \tag{28.2.2}$$

Multiplying (28.2.3) and (28.2.4) yields,

$$\frac{1}{2n} < \frac{(2n)^{\sqrt{2n}/2-1} \cdot 4^{\frac{2n}{3}}}{4^n}$$

Multiplying by $2n$,

$$\begin{aligned} 1 &< \frac{(2n)^{\sqrt{2n}/2}}{4^{\frac{n}{3}}} \\ &\Rightarrow 4^{\frac{n}{3}} < (2n)^{\sqrt{2n}/2} \\ &\Rightarrow 4^{\frac{2n}{3}} < (2n)^{\sqrt{2n}} \text{ (by squaring both sides.)} \end{aligned}$$

Then, taking logs,

$$\log 4^{\frac{2n}{3}} < \log(2n)^{\sqrt{2n}} \Rightarrow \frac{2n}{3}\log 4 < \sqrt{2n}\log 2n$$

Putting $n = 2^{2k+1}$ gives,

$$\begin{aligned} \frac{2}{3}\left(2^{2k+1}\right)\log 4 < \sqrt{2^{2k+2}}\log(2^{2k+2}) \\ = \sqrt{2^{2(k+1)}} \cdot (k+1) \cdot \log(2^2) \\ = 2^{k+1} \cdot (k+1) \cdot \log 4 \end{aligned}$$

Cancelling, we have,

$$\frac{2}{3}2^k < k+1 \Rightarrow 2^k < \frac{3}{2}(k+1)$$

This is false if $k \ge 3$ or $n = 2^{2k+1} = 2^7 = 128$ so the assumption that for every natural number $n > 1$ there are no primes p such that $n < p < 2n$ is false for all $n > 128$. We can manually check values of n less than 128 or we can note it suffices to check that

$$2, 3, 5, 7, 13, 23, 43, 83, 163$$

is a sequence of primes where each is smaller than twice the previous one.

□

Part XI

After-Glow

Riemann

The German mathematician Bernard Riemann was a master mathematician, a ground-breaker. His work opened up research fields combining analysis with geometry, revolutionizing integral calculus, developing complex variable theory and opening up topology.

However, he wrote only one short 8-page article on number theory which was published in 1859 as “On the number of primes less than a given magnitude”. The article contained a comment reminiscent of the comment Fermat left in the margin of his copy of Diophantus’ Arithmetica now known as Fermat’s Last Theorem. Riemann’s comment is known as the Riemann Hypothesis. It has now defied proof for or to the contrary for over 150 years. There is currently a $1,000,000 prize for a proof or counter-proof.

Enrico Bombieri, a major contributor to 20th century number theory states “In the opinion of many mathematicians, the Riemann Hypothesis is … probably the most important open problem in pure mathematics”.

A host of mathematical proofs contain the caveat that “if the Riemann Hypothesis is true, then …!”

The mathematical world is holding its breath.

Chapter 29

The Riemann Hypothesis

Course: Post-prandial
Ingredients
The Riemann Zeta Function
The Gamma Function
Bernoulli Numbers
Directions
Follow Riemann's thinking as he expounds his ground-breaking paper on the number of primes less than a given magnitude.

29.1 First Steps with Riemann

In his paper Riemann takes as his starting point the Euler Zeta Function together with the product formula from Theorem 185 on page 272,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p}},\ Re(s) > 1 \tag{29.1.1}$$

He combines this with Euler's Gamma Function,

$$\Gamma(s) = \int_0^{\infty} e^{-x} x^{s-1}\ dx,\ s > -1 \tag{29.1.2}$$

$$= (s-1)! \text{ if } s \in \mathbb{N} \tag{29.1.3}$$

$$= \lim_{n \to \infty} \frac{n! n^s}{s(s+1)(s+2)\cdots(s+n)} \tag{29.1.4}$$

$$= \frac{1}{s} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right)^{-1} \left(1 + \frac{1}{n}\right)^{s} \tag{29.1.5}$$

where the last three results were proved in Chapter 26 (Theorem 196, Theorem 198, Lemma 195).
Equation (29.1.5) shows the limit of Equation (29.1.4) exists for all s except

$s = 0, -1, -2, -3, \ldots$. In particular, $\Gamma(s)$ is an analytic (think, differentiable in $\mathbb{C}$) function of the complex variable s which has simple poles at $s = 0, -1, -2, -3, \ldots$. It has no zeros. Euler's $\zeta(s)$ is defined only for $Re(s) > 1$. Riemann defined a function $\zeta(s)$ which is the same as Euler's when $s > 1$ but is valid (analytic) for all s except for a simple pole at $s = 1$. The mathematical process for doing this is called analytic continuation. There is a theorem in complex analysis which states that if such an extended function in the complex plane agrees with the real function on the Cartesian plane, then this complex function is unique.

Let us follow Riemann's reasoning.

29.2 The Riemann Zeta Function

We start with

$$\Gamma(s) = \int_0^\infty e^{-x} x^{s-1}\, dx$$

Putting nx for x gives,

$$\begin{aligned} \Gamma(s) &= \int_0^\infty e^{-nx} n^{s-1} x^{s-1}\, (n\, dx) \\ \Rightarrow \frac{\Gamma(s)}{n^s} &= \int_0^\infty e^{-nx} x^{s-1}\, dx \end{aligned}$$

Taking the infinite sum over both sides and assuming we can take the summation inside the integral gives,

$$\Gamma(s) \sum_{n=1}^{\infty} \frac{1}{n^s} = \int_0^\infty \sum_{n=1}^{\infty} e^{-nx} x^{s-1}\, dx$$

The infinite sum of the interior geometric series on the right side is,

$$\sum_{n=1}^{\infty} e^{-nx} = e^{-x} + (e^{-x})^2 + \ldots = \frac{e^{-x}}{1 - e^{-x}} = \frac{1}{e^x - 1}$$

As a result, Riemann obtained,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty \frac{x^s}{e^x - 1} \frac{dx}{x} \tag{29.2.1}$$

A full understanding of what follows requires a knowledge of the simpler findings of integration over a path on the complex number plane. But we can get the general idea.

Next, Riemann considered this contour integral on the $\mathbb{C}$ plane,

$$\int_\infty^\infty \frac{(-x)^s}{e^x - 1} \frac{dx}{x}$$

where the path of integration is from +∞ along the real axis to a circle radius δ taken counterclockwise around the origin and then returning along the real axis to +∞ thus,

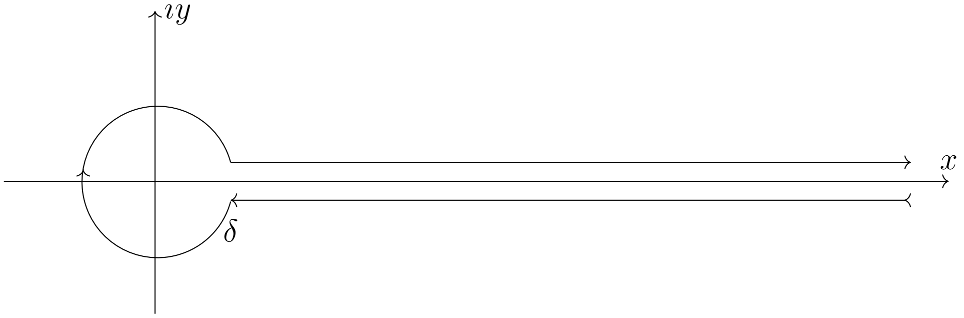


Figure 38

Just as we can separate an integral on an interval (or path) on the real number plane into for example,

$$\int_a^b f(x)\ dx = \int_a^c f(x)\ dx + \int_c^b f(x)\ dx$$

so we are able to write,

$$\int_\infty^\infty \frac{(-x)^s}{e^x-1}\frac{dx}{x} = \int_\infty^\delta \frac{(-x)^s}{e^x-1}\frac{dx}{x} + \int_{|x|=\delta} \frac{(-x)^s}{e^x-1}\frac{dx}{x} + \int_\delta^\infty \frac{(-x)^s}{e^x-1}\frac{dx}{x}$$

where the integral around the circle of radius δ is an integral around all values of x for which the magnitude of x is $|x| = \delta$.
Let us recall the polar representation $x = re^{i\theta}$ of complex numbers together with the inverse function relationship $e^{\log x} = x \Rightarrow x^s = e^{s\log x}$ and Euler's equation $e^{\pm\pi i} = -1$, then we have,

$$(-x)^s = (e^{\pm\pi i}x)^s = (e^{\pm\pi i}e^{\log x})^s = e^{s(\log x \pm \pi i)}$$

- For the path from +∞ to δ along the real axis we can write $(-x)^s = e^{s(\log x - i\pi)}$ using the minus value here since the path is to the left.

- For the path around the circle radius δ we can write $x = \delta e^{i\theta}$ so that $|x| = \delta$ is replaced by $0 \le \theta \le 2\pi$. Then, $\dfrac{dx}{x} = \dfrac{\delta i e^{i\theta}}{\delta e^{i\theta}} d\theta = i\ d\theta$ so that,

$$\int_{|x|=\delta} \dots \frac{dx}{x} = \int_0^{2\pi} \dots i\ d\theta$$

- For the path from δ to ∞ back along the real axis we can write $(-x)^s = e^{s(\log x + i\pi)}$ using the plus sign here since the path is to the right.

It is then a fact that, for $s > 1$ as $\delta \to 0$, the middle integral around the circle approaches zero, giving,

$$\begin{aligned}\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x} &= \int_{\infty}^{0}\frac{(-x)^s}{e^x-1}\frac{dx}{x}+\int_{0}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x}\\ &= \int_{\infty}^{0}\frac{e^{s(\log x-i\pi)}}{e^x-1}\frac{dx}{x}+\int_{0}^{\infty}\frac{e^{s(\log x+i\pi)}}{e^x-1}\frac{dx}{x}\\ &= -\int_{0}^{\infty}\frac{e^{s(\log x-i\pi)}}{e^x-1}\frac{dx}{x}+\int_{0}^{\infty}\frac{e^{s(\log x+i\pi)}}{e^x-1}\frac{dx}{x}\\ &= \int_{0}^{\infty}(e^{i\pi s}-e^{-i\pi s})\frac{x^s}{e^x-1}\frac{dx}{x}\ \text{since } e^{s\log x}=x^s\end{aligned}$$

From Corollary 121, page 174, we have $\sin\theta = \dfrac{e^{i\theta}-e^{-i\theta}}{2i}$. Then,

$$\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x} = 2i\sin\pi s\int_{0}^{\infty}\frac{x^s}{e^x-1}\frac{dx}{x}$$

From Theorem 200, page 291 in our study of the Gamma Function we can use,

$$\sin\pi s = \frac{\pi}{\Gamma(s)\Gamma(1-s)}$$

to obtain

$$\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x} = 2i\frac{\pi}{\Gamma(s)\Gamma(1-s)}\int_{0}^{\infty}\frac{x^s}{e^x-1}\frac{dx}{x},$$

so that multiplying both sides by $\dfrac{\Gamma(1-s)}{2\pi i}$,

$$\begin{aligned}\frac{\Gamma(1-s)}{2\pi i}\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x} &= \frac{\Gamma(1-s)}{2\pi i}\cdot 2i\cdot\frac{\pi}{\Gamma(s)\Gamma(1-s)}\int_{0}^{\infty}\frac{x^s}{e^x-1}\frac{dx}{x}\\ &= \frac{1}{\Gamma(s)}\int_{0}^{\infty}\frac{x^s}{e^x-1}\frac{dx}{x}\end{aligned}$$

making,

$$\frac{\Gamma(1-s)}{2\pi i}\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x} = \sum_{n=1}^{\infty}\frac{1}{n^s}$$

where we used Equation (29.2.1) in the final step.
In other words, if $\zeta(s)$ is defined by the formula,

$$\zeta(s) = \frac{\Gamma(1-s)}{2\pi i}\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x}$$

then, for $Re(s) > 1$, $\zeta(s)$ is equal to Euler's Zeta Function, $\zeta(s) = \sum_{n=1}^{\infty}\dfrac{1}{n^s},\ s > 1$.

Definition 111. *Riemann Zeta Function*

$$\zeta(s) = \frac{\Gamma(1-s)}{2\pi i}\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x}$$

is called the Riemann Zeta Function. It is identical with the Euler Zeta function for $Re(s) > 1$.

29.3 The pole of $\zeta(s)$

Since, using (29.1.4),

$$\Gamma(1-s) = \lim_{n\to\infty}\frac{1\cdot 2\cdot 3\cdots n}{(1-s)(2-s)(3-s)\cdots(n-s)}n^{1-s}$$

has simple poles (think "infinite discontinuities") at $s = 1, 2, 3, \ldots$ but at $s = 2, 3, 4, \ldots$ the Riemann and Euler functions coincide at $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$ which has no poles at $s = 2, 3, 4, \ldots$, then the integral $\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x}$ must have simple zeros at $s = 2, 3, 4, \ldots$, that cancel[1] the simple poles of $\Gamma(1-s)$.

At $s = 1$, $\Gamma(1-s)$ also has a simple pole and this coincides with the fact that $\zeta(1) = \sum_{n=1}^{\infty}\frac{1}{n^1}$ is the divergent Harmonic series. In other words $\zeta(s)$ has just the simple pole at $s = 1$. Thus, the Riemann Zeta Function,

$$\zeta(s) = \frac{\Gamma(1-s)}{2\pi i}\int_{\infty}^{\infty}\frac{(-x)^s}{e^x-1}\frac{dx}{x} \qquad (29.3.1)$$

defines a function which is analytic at all points on the complex plane except for the simple pole at $s = 1$.

29.4 The Trivial Zeros of $\zeta(s)$

Recall the Bernoulli numbers are generated by the infinite series,

$$\frac{x}{e^x-1} = \sum_{m=0}^{\infty}\frac{B_m}{m!}x^m \qquad (29.4.1)$$

[1] You may wish to revisit Section 26.2 on page 286. For example $\frac{1}{x^2-1}$ has divisions by zero (think, simple poles) at $x = \pm 1$. So if the product $f(x) \times \frac{1}{x^2-1}$ has no divisions by zero at all then for some other function $g(x)$, $f(x)$ must be $(x^2-1)\cdot g(x)$ where the zeros due to $f(\pm 1)$ cancel the divisions by zero of $\frac{1}{x^2-1}$.

Note also from Corollary 197 on page 289 that

$$\Gamma(n+1) = n! \tag{29.4.2}$$

When $s = -n$ with $\delta = 1$, where δ is as in Figure 38, Equation (29.3.1) becomes,

$$\begin{aligned}
\zeta(-n) &= \frac{\Gamma(n+1)}{2\pi i}\int_{\infty}^{\infty}\frac{(-x)^{-n}}{e^x-1}\frac{dx}{x}\\
&= \frac{n!}{2\pi i}\int_{\infty}^{\infty}\frac{x}{e^x-1}(-1)^n(x)^{-n-1}\frac{dx}{x}\\
&= \frac{n!}{2\pi i}\int_{\infty}^{\infty}\left(\sum_{n=0}^{\infty}\frac{B_m}{m!}x^m\right)(-1)^n x^{-n-1}\frac{dx}{x} && (29.4.3)\\
&= \frac{n!}{2\pi i}\sum_{n=0}^{\infty}\frac{B_m}{m!}\int_{\infty}^{\infty}(-1)^n x^{m-n-1}\frac{dx}{x} && (29.4.4)
\end{aligned}$$

Now,

$$\begin{aligned}
\int_{\infty}^{\infty} x^{m-n-1}\frac{dx}{x} &= \int_{\infty}^{1} x^{m-n-1}\frac{dx}{x} + \int_{|x|=1} x^{m-n-1}\ \frac{dx}{x} + \int_{1}^{\infty} x^{m-n-1}\ \frac{dx}{x}\\
&= \int_{|x|=1} x^{m-n-1}\ \frac{dx}{x}
\end{aligned}$$

since for real powers the first and third integrals cancel by $\int_{\infty}^{1} = -\int_{1}^{\infty}$
Now on $|x| = 1$ which is a circle of radius 1 centered at the origin we have,

$$x = e^{i\theta},\ 0 \le \theta \le 2\pi \text{ and } \frac{dx}{x} = \frac{ie^{i\theta}}{e^{i\theta}} = id\theta,$$

Hence,

$$\begin{aligned}
\int_{|x|=1} x^{m-n-1}\ \frac{dx}{x} &= \int_{0}^{2\pi} i\ e^{i\theta(m-n-1}\ d\theta\\
&= \left[\frac{i}{i(m-n-1)}e^{i\theta(m-n-1)}\right]_{o}^{2\pi} \text{provided } \ m-n-1 \ne 0\\
&= \frac{i}{i(m-n-1)}\left(e^{2\pi i(m-n-1)}-1\right)\\
&= 1-1 = 0 \text{ since } e^{2\pi i} = 1
\end{aligned}$$

unless $m = n+1$, in which case,

$$\int_{0}^{2\pi} i\ x^{m-n-1}\ d\theta = \int_{0}^{2\pi}\ i\ d\theta = [i\theta]_0^{2\pi} = 2\pi i$$

Accordingly, in the infinite sum of Bernoulli numbers, only the term in B_{n+1} survives, giving, from (29.4.4),

$$\zeta(-n) = (-1)^n\frac{n!}{2\pi i}\frac{B_{n+1}}{(n+1)!}\cdot 2\pi i = (-1)^n\frac{B_{n+1}}{n+1}$$

Since all the odd Bernoulli numbers are 0 then $B_{n+1} = 0$ for $n = 2k, k \geq 1$ making,

$$\zeta(-2k) = 0 \text{ for } k \geq 1 \Rightarrow \zeta(-2) = \zeta(-4) = \zeta(-6) = \ldots = 0$$

The values $s = -2, -4, -6, \ldots$ are called the trivial zeros of $\zeta(s)$. The Riemann Hypothesis is that the other or non-trivial zeros of $\zeta(s)$ have $Re(s) = \frac{1}{2}$. Let's examine this more closely. We continue to follow Riemann.

29.5 Functional Equation of $\zeta(s)$

We will deal with $Re(s) > 1$ so we can use Euler's Gamma function which is equivalent to Riemann's for $Re(s) > 1$. We begin with,

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty e^{-x} x^{\frac{s}{2}} \frac{dx}{x}$$

We substitute $x = n^2 \pi x \Rightarrow \frac{dx}{x} = \frac{n^2 \pi dx}{n^2 \pi x} = \frac{dx}{x}$ to obtain,

$$\begin{aligned}
\Gamma\left(\frac{s}{2}\right) &= \int_0^\infty e^{-n^2\pi x} \left(n^s \pi^{\frac{s}{2}} x^{\frac{s}{2}}\right) \frac{dx}{x} \\
\Rightarrow \frac{1}{n^s} \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) &= \int_0^\infty e^{-n^2\pi x} x^{\frac{s}{2}} \frac{dx}{x}, \;\; Re(s) > 1 \\
\Rightarrow \sum_{n=1}^\infty \frac{1}{n^s} \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) &= \sum_{n=1}^\infty \int_0^\infty \left(e^{-n^2\pi x}\right) x^{\frac{s}{2}} \frac{dx}{x}, \;\; Re(s) > 1 \\
\Rightarrow \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) &= \int_0^\infty \left(\sum_{n=1}^\infty e^{-n^2\pi x}\right) x^{\frac{s}{2}} \frac{dx}{x}, \;\; Re(s) > 1 \text{ using } \zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s} \\
&= \int_0^\infty \Psi(x) x^{\frac{s}{2}} \frac{dx}{x}, \;\; \text{where } \Psi(x) = \sum_{n=1}^\infty e^{-n^2\pi x} \\
&= \int_1^\infty \Psi(x) x^{\frac{s}{2}} \frac{dx}{x} + \int_0^1 \Psi(x) x^{\frac{s}{2}} \frac{dx}{x} \qquad (29.5.1)
\end{aligned}$$

If, in the integral on the right, we put $x = \frac{1}{x}$, so that $\frac{dx}{x} = -\frac{1}{x^2} x dx = -\frac{dx}{x}$, and note the limits of integration change with 0 to 1 becoming ∞ to 1, we have,

$$\begin{aligned}
\int_0^1 \Psi(x) x^{\frac{s}{2}} \frac{dx}{x} &= -\int_\infty^1 \Psi\left(\frac{1}{x}\right) x^{-\frac{s}{2}} \frac{dx}{x} \\
&= \int_1^\infty \Psi\left(\frac{1}{x}\right) x^{-\frac{s}{2}} \frac{dx}{x}
\end{aligned}$$

Assuming Jacobi's functional equation of the Psi function, namely,

$$\frac{1 + 2\Psi(x)}{1 + 2\Psi\left(\frac{1}{x}\right)} = \frac{1}{\sqrt{x}} \Rightarrow \Psi\left(\frac{1}{x}\right) = \frac{\sqrt{x}(1 + 2\Psi(x)) - 1}{2} = x^{\frac{1}{2}} \Psi(x) + \frac{x^{\frac{1}{2}}}{2} - \frac{1}{2}$$

we have from (29.5.1),

$$\begin{aligned}\Rightarrow \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \int_1^\infty \Psi(x)x^{\frac{s}{2}}\frac{dx}{x} + \int_1^\infty \left[x^{\frac{1}{2}}\Psi(x) + \frac{x^{\frac{1}{2}}}{2} - \frac{1}{2}\right]x^{-\frac{s}{2}}\frac{dx}{x}\\ &= \int_1^\infty \Psi(x)\left[x^{\frac{s}{2}} + x^{\frac{1-s}{2}}\right]\frac{dx}{x} + \frac{1}{2}\int_1^\infty \left[x^{\frac{s-1}{2}} + x^{-\frac{s}{2}}\right]\frac{dx}{x}\end{aligned}$$

Now, $\int\limits_1^\infty x^{-a}\frac{dx}{x} = \frac{1}{a}$ for $a > 0$ so the second integral becomes,

$$\frac{1}{2}\left[\frac{1}{(s-1)/2} - \frac{1}{s/2}\right] = \frac{1}{s(s-1)} \text{ for } s > 1.$$

Therefore for $s > 1$,

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_1^\infty \Psi(x)\left[x^{\frac{s}{2}} + x^{\frac{1-s}{2}}\right]\frac{dx}{x} - \frac{1}{s(s-1)} \tag{29.5.2}$$

If we put $s = 1 - s$ we have,

$$\pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) = \int_1^\infty \Psi(x)\left[x^{\frac{1-s}{2}} + x^{\frac{s}{2}}\right]\frac{dx}{x} - \frac{1}{s(s-1)} \tag{29.5.3}$$

and we note that the right side remains the same as it was in (29.5.2). Hence, (29.5.2) and (29.5.3) together give,

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) \tag{29.5.4}$$

This is called the functional equation of the Zeta function. It says the left side is invariant (unchanged) when $1 - s$ is substituted for s.

29.6 The Non-Trivial Zeros of $\zeta(s)$

We have from (29.1.4),

$$\Gamma\left(\frac{s}{2}\right) = \lim_{n\to\infty} \frac{n!n^{\frac{s}{2}}}{\frac{s}{2}\left(\frac{s}{2}+1\right)\left(\frac{s}{2}+2\right)\cdots\left(\frac{s}{2}+n\right)}$$

Except for $\frac{s}{2}$ one of each of the terms in the denominator is zero when $s = -2, -4, -6, \ldots,$ corresponding to the trivial zeros of $\zeta(s)$ which in the product $\Gamma\left(\frac{s}{2}\right)\zeta(s)$ will therefore cancel out.

Also we know $\zeta(s)$ has a pole (think infinite discontinuity) at $s = 1$. Therefore the

left side of the functional equation, $\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ has poles only at $s = 0, 1$.
Therefore the function,

$$\xi(s) = s(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

formed by multiplying the left side of (29.5.4) by $s(s-1)$ is an entire function, (no discontinuities), meaning it is analytic (differentiable) for all s. It has the simple functional equation,

$$\xi(s) = \xi(1-s)$$

since,

$$\begin{aligned}
\xi(1-s) &= (1-s)(-s)\pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) \\
&= s(s-1)\pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) \\
&= s(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) \text{ by } (29.5.4) \\
&= \xi(s)
\end{aligned}$$

We have eliminated the trivial zeros of $\xi(s)$ by the preceding discussion.
It follows that the non-trivial zeros of $\xi(s)$ are the zeros of $\zeta(s)$. But $\zeta(s)$ has no zeros at all for $Re(s) > 1$.
Then $\xi(s) = \xi(1-s)$ tells us that $\xi(s)$ has no zeros at all[2] for $Re(s) < 0$. Thus, all the non-trivial zeros of both $\xi(s)$ and therefore $\zeta(s)$ lie in the so-called critical strip $0 \leq Re(s) \leq 1$. See Figure 39 below.

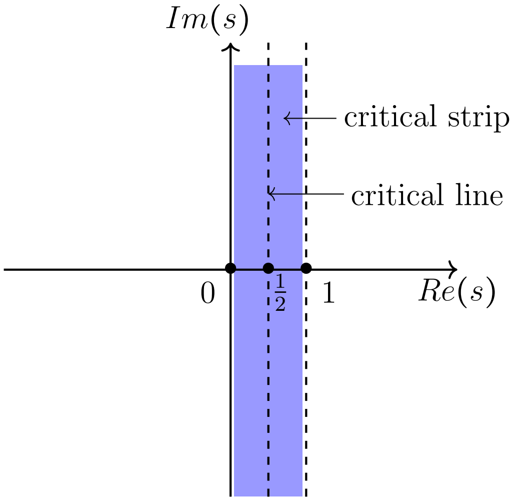


Figure 39

[2] For example if $s = 1 + \delta > 1$ is excluded then so is $1 - s = 1 - 1 - \delta = -\delta < 0$

We can go further. If $s = \frac{1}{2} + it$ is a zero of $\xi(s)$ then,

$$\begin{aligned} &\xi(s) = \xi(1-s) \\ &\Rightarrow \xi\left(\frac{1}{2} + it\right) = \xi\left(1 - \frac{1}{2} - it\right) = \xi\left(\frac{1}{2} - it\right) \end{aligned}$$

So if $\xi\left(\frac{1}{2} + it\right) = 0$ then $\xi\left(\frac{1}{2} - it\right) = 0$. This tells us that all the non-trivial zeros of $\zeta(s)$ are equally spaced on either side of the critical line $Re(s) = \frac{1}{2}$.

29.7 Riemann Hypothesis

The Riemann Hypothesis is that all the non-trivial zeros of $\zeta(s)$ actually lie on the critical line meaning they all have $Re(s) = \frac{1}{2}$.

It turns out that finding non-trivial zeros of $\zeta(s)$ is tedious but relatively straightforward, being achieved through the method of Euler-Maclaurin summation. Computers have been used to calculate the zeros for t in $\zeta(s) = \zeta(\sigma + it)$ up to 4.2 trillion. In all cases, $Re(s) = \sigma = \frac{1}{2}$. Strong evidence, but not a proof!

If you are interested in the conclusion to Riemann's paper, you can find a translation in "Riemann's Zeta Function" by H.M. Edwards.

Bibliography

[1] Adler, A., and Coury, J.E., *The Theory of Numbers*, Jones and Bartlett, London, 1995

[2] Andrews, G.E., *Number Theory*, Dover Publications, NY, 1971

[3] Burton, D.M.¡ *Elementary Number Theory*, McGraw Hill, India, 2012

[4] Cassells, J.W.S., and Fröhlich, A., *Algebraic Number Theory*, Academic Press, USA, 1967

[5] Frahleigh, J.B., *A First Course in Abstract Algebra,* 3rd ed., Addison-Wesley, USA, 1982

[6] Fröhlich, A., and Taylor, M.J., *Algebraic Number Theory*, Cambridge University Press, 1991

[7] Guy, R., *Unsolved Problems in Number Theory*, 3rd. ed., Springer, USA, 2004

[8] Hardy, G.H., and Wright, E.M., *An Introduction to the Theory of Numbers*, 6th. ed., Oxford University Press, 2008

[9] Hasse, H., *Number Theory*, Sprimger, (translation), 2002

[10] Ireland, K., and Rosen, M., *A Classical Introduction to Modern Number Theory*, Springer USA, 1990

[11] Jameson, G.J.O., *The Prime Number Theorem*, Cambridge University Press, Cambridge, 2003

[12] Jones, G.A., and Jones, M.J., *Elementary Number Theory*, Springer, London, 2005

[13] Lang, S., *Algebaic Number Theory*, Springer, USA, 1994

[14] Nagell, T., *Introduction to Number Theory*, Wiley and Sons, NY, 1951

[15] Narkiewicz, W., *Number Theory*, World Scientific, Singapore, (translation), 1983

[16] Papantonopoulou, A., *Algebra, Pure and Applied,* Prentice Hall, NJ, 2002

[17] Ribenboim, P., *The New Book of Prime Number Records*, Springer, NY, 1995

Index

absolute value, 39, 55
algebraic integer, 62, 190
algebraic number, 62, 190
angle, 155
antiderivative, 88
area, 28
area function, 92
arithmetic function, 249
arithmetic progression, 232
associates, 66
associativity, 19

Bernoulli numbers, 196
Big-O notation, 317
binary operations, 257
binomial coefficient, 128
binomial theorem, 130

cardinality of a set, 304
change of variables, 99
chinese remainder theorem, 119
closure, 19
commutativity, 19
complete residue system, 233
complex conjugate, 56
complex number plane, 56
complex numbers, 9, 56
composite number, 301
composition of functions, 207
congruence, 67, 118, 233
convergence of infinite series, 102
coset multiplication, 261
cosine fiunction, 158
cyclic group, 262
cyclic subgroup, 262

definite integral, 92
degree, 156
derivative, 82
derivative of a function at a point, 82
differentiable, 82
differentiation
    chain rule, 88
distributivity, 19
divisible, 63
divisor, 63

euclidean algorithm, 113
Euler gamma function, 293
Euler product, 272
Euler's totient function, 236, 255
Euler-Mascheroni constant, 284
Euler-Riemann Zeta function, 271
even function, 198
even integer, 21
exponential function, 153

factorial, 128
Fermat's two squares theorem, 132, 145
First Fundamental Theorem of Calculus, 94
Fundamental Theorem of Calculus
    First, 94
    Second, 95

gamma function, 284
Gaussian integers, 132

complex conjugate, 133
division, 134
Euclidean algorithm, 139
magnitude, 133
norm, 133
prime, 135
relatively prime, 136
sum and product, 132
unit, 134
generalized Bernoulli function, 199
generator, 147
geometric series, 103
geometric series convergence, 103
gradient of curve, 81
gradient of line, 81
greatest common divisor, 22, 40
greatest integer function, 306
group and group axioms, 258
groups
$\mathbb{Z}_n$, 259
abelian, 258
axioms, 258
associative, 258
closure, 258
identity, 258
inverses, 258
cancellation law, 258
commutative, 258

holomorphic function, 286
hyperbolic sine function, 224

identity
additive, 19
multiplicative, 19
incongruence, 67
indefinite integral, 88, 89
infinite series, 100
integers, 9
axioms, 18
even, 21
odd, 21
integral test for convergence, 104
integrand, 88, 92
inverse functions, 207

least common multiple, 266
Legrendre symbol, 246
limit inferior, 329
limit superior, 329
limits of integration, 92
linear combination, 41
linear congruence, 237
linear equation, 237
little-o notation, 318
logarithmic function, 209

Möbius function, 250
magnitude of complex number, 56
mathematical proofs
contradiction, 22
mathematical induction, 23
multiplicative function, 250
multiplicative group $\mathbb{Z}/n\mathbb{Z}$, 261

natural exponential function, 154
natural numbers, 9
natutal logarithmic function, 210
norm, 63

odd function, 198
odd integer, 21
order of a
group, 263
order of a group element, 148, 263

p-series test, 105
partial sum, 102
Pascal's triangle, 128
pi function, 319
polar coordinates on complex number plane, 57
pole, 286
prime number, 232, 301
primes in $k(\rho)$, 66
primitive Pythagorean triples, 31
pythagorean theorem, 29
Pythagorean triples, 31

quadratic residue, 243

radian, 157
ratio test for convergence, 104
rational numbers, 9
real numbers, 9
relatively prime, 236
residue, 67, 118, 233
Riemann Hypothesis, 354
Riemann zeta function, 349
roots of unity, 174
rules of differentiation, 84
  constant multiple rule, 86
  constant rule, 84
  extended power rule, 87
  power rule, 85
  product rule, 86
  quotient rule, 87
  sum rule, 85

second fundamental theorem of calculus, 95
set, 8
set notation, 8
sine function, 158
slope of line, 81
slope of tangent, 81
smooth function, 168

tan function, 158
taylor series, 168
the χ function, 277
theta function, 320
triangle inequality in $\mathbb{C}$, 60

unit circle, 158
unitary operations, 257
unity, 64

zeta function, 271