p-adic Numbers

KJ Tim McDonald

Preface

As mathematics developed through the ages, its users came to accept a series of "new innovations" that were at first scorned by many. The natural or counting numbers gave way to the integers with the addition of the strange concept of negative numbers and indeed, zero. In turn the integers gave way to the rational numbers or fractions, including the exclusion of division by zero. Next came the concept of irrational numbers, numbers like $\sqrt{2}$ gained acceptance long before transcendental numbers like π and e but eventually all mathematicians came to accept the utility of these kinds of numbers in progressing the science of mathematics itself. The totality of the reals was accepted.

But then came the complex numbers and that strange symbol i, for imaginary numbers, even stranger its definition as $\sqrt{-1}$. Yet all mathematicians now accept the utility of proving theorems are true for complex numbers and therefore for real numbers which are just a subset of the complex ones.

Algebra seemed to be fully resolved in terms of how to find the solutions of polynomial equations and how to prove theorems previously regarded as unreachable such as Fermat's Last, the Prime Number theorem and a host of others, all by using complex or imaginary numbers and not real numbers.

So is that it? The natural numbers have been absorbed into the integers, the integers have been absorbed into the rationals, the rationals have been absorbed into the reals, the reals into the complex numbers. The fundamental theorem of algebra has proved that that's it for number sets, the complex numbers are all we need.

Really? In an effort to describe how all the real numbers can be derived from the rational numbers we are told the real numbers have been constructed from the rationals by using the absolute value function, $|.|$, to measure distances of numbers apart and by the use of particular sequences of the rationals.

But is this the only way to extend the rational numbers? Even if we accept the need to use the same particular sequences? Can we measure the distance between numbers in another way - not by the absolute value function?

Let's read on! Mathematics has not yet finished in diverging along paths even stranger than imaginary ones.

Contents

Chapter 1

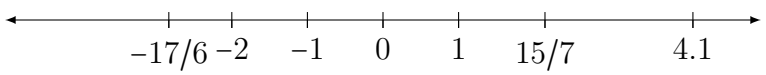
The completion of $\mathbb{Q}$ to form $\mathbb{R}$.

1.1 The real number line

As we learn mathematics we meet sets of numbers in this order:

$$\begin{aligned} \text{Natural numbers:} \quad & \mathbb{N} = \{1, 2, 3, \cdots\} \\ \text{Integers:} \quad & \mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\} \\ \text{Rationals:} \quad & \mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\} \end{aligned}$$

All of these numbers can be placed on a number line called the Real number line, often designated simply as $\mathbb{R}$.



We can begin to fill in the gaps between any two numbers a and b on the number line by simply inserting $\frac{a+b}{2}$ but no matter how much we fill it in with elements of $\mathbb{Q}$ there will still be gaps. Simplistically the completion of $\mathbb{Q}$ means adding in all the irrational numbers like $\sqrt{2}$ and π, and we call the completion $\mathbb{R}$, the set of all real numbers.

We need to be able to measure the distance between numbers on the number line and we do this by defining a norm on $\mathbb{Q}$ which leads to a distance function. But first let's generalize the properties of $\mathbb{Q}$.

1.2 Field

$\mathbb{Q}$ itself is the simplest example of a mathematical structure called a Field.

Definition 1. *A field, F, is a set with two mathematical binary operations usually called addition and multiplication, which satisfy:*

1. *Commutativity: For all* $a, b \in F$, $a + b = b + a$ *and* $ab = ba$
2. *Associativity: For all* $a, b, c \in F$, $a + (b + c) = (a + b) + c$ *and* $a(bc) = (ab)c$.
3. *Existence of identities: For all* $a \in F$ *there exists* 0 *and* 1 *in* F *such that* $a+0 = a$ *and* $a.1 = a$
4. *Existence of inverses: For all* $a \in F$ *there exists* $(-a), a^{-1}$ *in* F *such that* $a + (-a) = 0$ *and* $a.a^{-1} = 1$
5. *Distributivity: For all* $a, b, c \in F$ *we have* $a(b + c) = ab + ac$

1.3 Norm

Definition 2. *We define the absolute value function* $|.|$ *acting on* $x \in \mathbb{Q}$ *by,*

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

We call the absolute value function, $|.|$, a norm or, specifically, the Euclidean norm of dimension 1. It satisfies these three criteria.
For all $x, y \in \mathbb{Q}$:

1. $|x| = 0$ if and only if $x = 0$. This is true by definition of $|x|$.
2. $|xy| = |x||y|$ This is true since the numbers on both sides are made positive.
3. $|x + y| \leq |x| + |y|$ This is called the triangle inequality and is proved as follows.

Proof. We first note:

$$|x|^2 = x^2 \text{ (both sides are positive)} \tag{1.3.1}$$
$$xy \leq |x||y| \text{ (left side may be negative but the right side is positive.)} \tag{1.3.2}$$

Accordingly,

$$\begin{aligned} |x + y|^2 &= (x + y)(x + y) \text{ by (1.3.1)} \\ &= x^2 + 2xy + y^2 \\ &= |x|^2 + 2xy + |y|^2 \text{ by (1.3.1)} \\ &\leq |x|^2 + 2|x||y| + |y|^2 \text{ by (1.3.2)} \\ &= (|x| + |y|)^2 \\ \Rightarrow |x + y| &\leq |x| + |y| \text{ by taking the square root.} \end{aligned}$$

□

Definition 3. *Prompted by the above three criteria for the norm on $\mathbb{Q}$ we define a norm $\|.\|$ on a general field F by, for all $x, y \in F$,*

1. *$//x//=0$ if and only if $x=0$*
2. *$//x.y//=//x//.//y//$*
3. *$//x+y//\leq //x//+//y//$*

1.4 Distance Function or Metric

Definition 4. *We define the distance function for all $x, y \in \mathbb{Q}$ by:*

$$d(x, y) = |x - y|$$

We call d a metric on $\mathbb{Q}$.
We call $\mathbb{Q}$ a metric space, that is, a space with a distance measure.
Then $d(x, y)$ satisfies these three conditions:

1. $d(x, y) = 0$ if and only if $x = 0$. This is true by the first criteria for the norm, that $|x - y| = 0$ if and only if $x = y$.
2. $d(x, y) = d(y, x)$ This is true since $|x - y| = |y - x|$
3. $d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in \mathbb{Q}$

   Proof.

$$\begin{aligned} |x - y| &= |x - z + z - y| \\ &= |(x - z) + (z - y)| \\ &\leq |x - z| + |z - y| \text{ by the triangle inequality.} \end{aligned}$$

□

Definition 5. *Prompted by the definition of the distance function $d(x, y)$ on the field $\mathbb{Q}$ we define a distance function or metric on a set X containing elements x, y and having norm $\|.\|$, by,*

$$d(x, y) = \|x - y\| \text{ for all } x, y \in X$$

and accordingly we have,

1. *$d(x, y) = 0$ if and only if $x = y$*
2. *$d(x, y) = d(y, x)$*
3. *$d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in X$.*

The proofs of these three criteria are the same as those for the distance function in $\mathbb{Q}$ as above with $|.|$ replaced by $\|.\|$.

Chapter 2

Sequences and Cauchy Sequences

2.1 Sequences

Definition 6. *A sequence is an ordered list of numbers.*

For example $\{1, 3, 5, 9\}$ is a sequence.

Notation 1. *We use the symbol* $\{a_n\}_{n=0}^{n=3}$ *to mean the sequence* $\{a_0, a_1, a_2, a_3\}$. *For brevity, we often just use* $\{a_n\}$ *for an infinite sequence* $\{a_n\}_{n=0}^{n=\infty}$.

A sequence may be generated by a function thus:

$$f(n) = a_n,\ f(x) = x^2,\ x \in \mathbb{N}$$

This infinite sequence is $\{1, 4, 9, 16, \cdots\}$
We are interested in infinite sequences but they will be sequences that are "heading somewhere," unlike $\{1, 4, 9, 16, \ldots\}$ which is just getting larger and larger or "diverging to infinity."
For example the sequence generated by $f(n) = \dfrac{1}{n}$ is $\left\{1, \dfrac{1}{2}, \dfrac{1}{3}, \ldots\right\}$ and it is heading towards 0 or in mathematical language it has a final value or limit of 0.
We write $\lim\limits_{n\to\infty} \dfrac{1}{n} = 0$.
Of course $\dfrac{1}{n}$ is never actually zero but that is where it is heading. Thus the difference between it and 0 can be made as small as we like, $\dfrac{1}{1,000,000}, \dfrac{1}{100,000,000}$ and so on. We say the sequence converges to 0. Here is our definition.

Definition 7. *A sequence is convergent or has a limit* $a \in \mathbb{R}$ *if* $\lim\limits_{n\to\infty} |a_n - a| = 0$. *That is, for all* $\epsilon > 0$ *there exists an* $N \in \mathbb{N}$ *such that for all* $n > N$ *we have* $|a_n - a| < \epsilon$.

For example the sequence $\{a_n\}$ with $a_n = \frac{1}{n}$ has the limit $a = 0$. We choose any $\epsilon > 0$ and $N = \frac{1}{\epsilon}$. Then for any $n > N$ we have $n > \frac{1}{\epsilon}$ giving,

$$|a_n - 0| = |a_n| = \frac{1}{n} < \epsilon.$$

A particular case is given by $\epsilon = 10^{-6},\ N = \frac{1}{10^{-6}}$ so if $n > N$ then $n > 10^6$ and,

$$|a_n - 0| = |\frac{1}{n}| < 10^{-6} = \epsilon$$

2.2 Cauchy sequences

Again considering the sequence $\left\{\frac{1}{n}\right\} = \left\{1, \frac{1}{2}, \frac{1}{3}, \ldots\right\}$ we observe that the distance between succesive terms is getting smaller and smaller as n increases. Thus,

$$\frac{1}{10} - \frac{1}{11} = \frac{1}{110} > \frac{1}{20} - \frac{1}{21} = \frac{1}{420}$$

If we call two terms a_n and a_m then their difference $|a_n - a_m|$ can be made as small as we like. So we say for all $\epsilon > 0$ that we can find terms a_n and a_m such that $|a_n - a_m| < \epsilon$. There will be some number $N \in \mathbb{N}$ such that if n and m are greater that N then it will always be true that $|a_n - a_m| < \epsilon$. This gives us our definition of a Cauchy sequence.

Definition 8. *A sequence $\{a_n\}$ is a Cauchy sequence if for every $\epsilon > 0$ there exists an $N \in \mathbb{N}$ such that if $n, m > N$ then,*

$$|a_n - a_m| < \epsilon$$

We could also write,

$$\lim_{m,n\to\infty} |a_n - a_m| = 0.$$

For example, again consider the sequence $\{a_n\}$ where $a_n = \frac{1}{n}$. Choose any $\epsilon > 0$ say $\epsilon = 10^{-12}$. Then if n, m are chosen to be greater than $N = 10^{12}$ we would have $|a_n - a_m| < \epsilon$. For instance, let's take $n = 10^{13}$ and $m = 10^{14}$ and then

$$|a_n - a_m| = \left|\frac{1}{10^{13}} - \frac{1}{10^{14}}\right| < \left|\frac{1}{10^{13}}\right| = 10^{-13} < \epsilon$$

But we can choose any $\epsilon > 0$, say $\epsilon = 10^{-101}$ and we have an $N = 1/\epsilon = 10^{101}$ such that for $n, m > N$, say $n = 10^{202}$ and $m = 10^{507}$, we have,

$$|a_n - a_m| = \left|\frac{1}{10^{202}} - \frac{1}{10^{507}}\right| < \left|\frac{1}{10^{202}}\right| = 10^{-202} < \epsilon.$$

Here is the general proof.

Lemma 1.
The sequence $\{a_n\}$ *with* $a_n = \dfrac{1}{n}$ *is a Cauchy sequence.*

Proof. Let $\epsilon > 0$. Choose $N = \dfrac{2}{\epsilon}$. Then for all $n, m > N$, we have,

$$\begin{aligned}\left|\frac{1}{n} - \frac{1}{m}\right| &\leq \frac{1}{n} + \frac{1}{m} \\ &< \frac{1}{N} + \frac{1}{N} \text{ since } n, m > N \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon\end{aligned}$$

□

2.3 Importance of Cauchy sequences

It is often not possible to find the actual limit of a sequence and, indeed, it may not be necessary to find the limit, only that the limit exists, or, in other words, that the sequence converges. Hence the importance of the next theorem. We first need a lemma.

Lemma 2.
All Cauchy sequences are bounded, that is all the terms of the sequence are less that some M.

Proof. Let $\{a_n\}$ be a Cauchy sequence.
Set $\epsilon = 1$.
Then there exists an $N \in \mathbb{N}$ such that for all $m, n > N$ we have $|a_m - a_n|_p < 1$.
Set $m = N + 1 > N$. Then for all $n > N$ we have,

$$\begin{aligned}|a_n| &= |a_n - a_m + a_m| \\ &\leq |a_n - a_m| + |a_m| \\ &\leq 1 + |a_m| \\ &= 1 + |a_{N+1}|\end{aligned}$$

So $|a_n| \leq 1 + |a_{N+1}|$ for all $n > N$ and there are only a finite number of terms a_n, $n \leq N$.
Set $M = \max\left(|a_1|, |a_2|.\cdots, |a_N|, |1 + a_{N+1}|\right)$
Then for all $n \in \mathbb{N}$ we have $|a_n| \leq M$ so the sequence $\{a_n\}$ is bounded. □

Theorem 3.
A sequence $\{a_n\}$ *converges to a limit if and only if it is Cauchy.*

Proof. Assume $\{a_n\}$ has a limit A. Select any $\epsilon > 0$.
By definition of a limit, there is an $N \in \mathbb{N}$ such that if $n \geq N$ then $|a_n - A| < \frac{\epsilon}{2}$.
If $m, n > N$ then,

$$\begin{aligned} |a_n - a_m| &= |a_n - A + A - a_m| \\ &\leq |a_n - A| + |A - a_m| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} \\ &= \epsilon \end{aligned}$$

Thus $\{a_n\}$ is a Cauchy sequence.

****

Conversely suppose $\{a_n\}$ is Cauchy.
By the Bolzano-Weierstrasse theorem (which we will not prove), $\{a_n\}$ has a subsequence $\{a_{n_k}\}$ converging to a limit A.
Let us prove $\{a_n\} \to A$. We need to prove that for all $\epsilon > 0$ there is a $N \in \mathbb{N}$ such that for all $k \geq N$ that $|a_k - A| < \epsilon$.
Let $\frac{\epsilon}{2}$ be given.
As $a_{n_k} \to A$ then there is an $N \in \mathbb{N}$ such that for all $n_k \geq N$ we have,

$$|a_k - a_{n_k}| < \frac{\epsilon}{2}$$

As $\{a_n\}$ is Cauchy we also have an M such that for all $k, m \geq M$ that,

$$|a_{n_k} - A| < \frac{\epsilon}{2}$$

Put $K = max(N, M)$. Then for all $k, n_k, m > K$ we have,

$$\begin{aligned} |a_k - A| &= |(a_k - a_{n_k}) + (a_{n_k} - A)| \\ &\leq |a_k - a_{n_k}| + |a_{n_k} - A| \\ &\leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \end{aligned}$$

So $\{a_k\}$ converges to a limit A. □

Chapter 3

The real numbers $\mathbb{R}$

Definition 9. *We define the real numbers $\mathbb{R}$ as the completion of $\mathbb{Q}$ with respect to the distance function $d(x,y) = |x-y|$ defined on $\mathbb{Q}$. By completion we mean that every Cauchy sequence with terms in $\mathbb{Q}$ has a limit in $\mathbb{R}$.*

Let's identify various real numbers.

1. All rational numbers are in $\mathbb{R}$ since any rational number $\frac{a}{b}$ can generate a constant sequence,
$$a_0 = \frac{a}{b}, a_1 = \frac{a}{b}, a_2 = \frac{a}{b}, \cdots$$
and clearly this sequence is Cauchy since for all $\epsilon > 0$ we can choose any $N \in \mathbb{N}$ and any $n, m > N$ since,
$$|a_n - a_m| = \left|\frac{a}{b} - \frac{a}{b}\right| = 0 < \epsilon$$
Finally the sequence has the limit $\frac{a}{b}$ since for all $\epsilon > 0$,
$$\lim_{n\to\infty} \left|a_n - \frac{a}{b}\right| = \left|\frac{a}{b} - \frac{a}{b}\right| = 0 < \epsilon$$

2. Irrationals that are square roots, cube roots, etc are in $\mathbb{R}$. Let's take $\sqrt{2}$ for example. We begin with $1^2 < 2 < 2^2$ and use a calculator or spreadsheet to set up the calculations,
$$1^2 < 2 < 2^2$$
$$1.4^2 < 2 < 1.5^2$$
$$1.41^2 < 2 < 1.42^2$$
$$1.414^2 < 2 < 1.415^2$$
$$\cdots$$

We calculate $\sqrt{2} = 1.414213\cdots$ and set up the sequence,

$$a_0 = 1, a_1 = 1.4, a_2 = 1.41, a_3 = 1.414, a_4 = 1.4142, a_5 = 1.41421, a_6 = 1.414213, \cdots$$

This sequence is Cauchy since for any $\epsilon > 0$ we can choose an $N \in \mathbb{N}$ such that $10^{-N} < \epsilon$ and if, say, $n, m > N$ with $n > m$ then,

$$\begin{aligned} |a_n - a_m| &= b.10^{-m},\ 0 < b \leq 9 \\ &< 10^{-N} \\ &< \epsilon \end{aligned}$$

For example, if, say, $\epsilon = 0.0004$, then choose $N = 4$ and with $n = 5, m = 6$ we have

$$|a_6 - a_5| = 0.000003 < 0.0004 = \epsilon$$

We define $\sqrt{2}$ to be the limit of this Cauchy sequence since for all $\epsilon > 0$, there is an $N \in \mathbb{N}$ such that if $n \geq N$ then $|a_n - \sqrt{2}| < \epsilon$.

3. Numbers like π and e are called transcendental numbers since, unlike square roots, cube roots, etc, they are not the solution of an algebraic equation, $x^2 = 2,\ x^3 = 4, etc.$ But again we can calculate $\pi = 3.14159265358979323846264\cdots$ and $e = 2.71828182845904523536028747135 27\cdots$ to as many decimal places as we like using infinite series developed through calculus. We then set up an infinite sequence as above for $\sqrt{2}$ and define π and e to be the respective limits of their Cauchy sequences. So they are real numbers.

4. In an advanced algebra course we find there are many more numbers on the real number line called algebraic numbers defined as the solutions of polynomial equations of degree n,

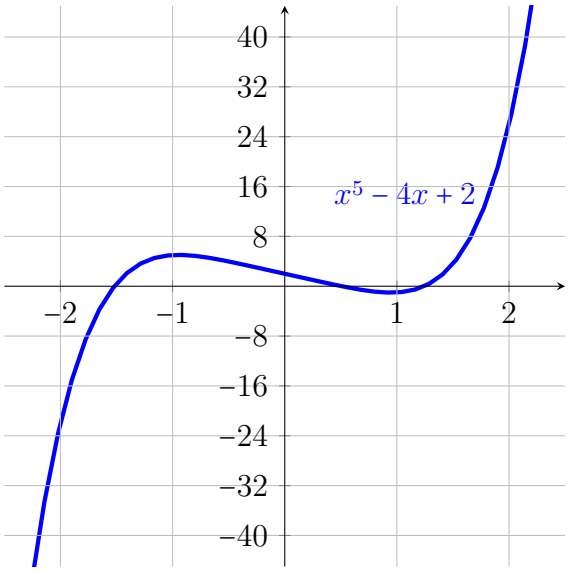
$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Many of these equations can be solved, thus:

$$x^6 - 3x^4 + x^2 - 3 = 0 \Rightarrow (x^2 - 3)(x^4 - 1) \Rightarrow x = \pm\sqrt{3}, \pm 1$$

All quadratic equations, $ax^2 + bx + c = 0$, can be solved by the quadratic formula, $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, and there are similar formulas involving radicals for cubic and quartic equations or polynomials of degree 3 and 4. However, there is a famous theorem in algebra which proves there are no such formulas for polynomial equations of degree 5 or higher. In other words we cannot find explicit solutions to all polynomial equations of degree 5 or more.
For example, $x^5 - 4x + 2 = 0$ cannot be solved for x, yet its graph below shows there are three real roots α, β, γ in these intervals,

$$-2 < \alpha < -1,\ 0 < \beta < 1,\ 1 < \gamma < 2$$



Again we can set up infinite Cauchy sequences using a calculator or spreadsheet which have the limits α, β and γ. For α we have this sequence:

α	$x^5 - 4x + 2$
− 1	5
− 1.5	0.406
− 1.51	0.19
− 1.518	0.112
− 1.5185	0.000274

The sequence of numbers in the α column is clearly Cauchy and we define its limit to be a root of the polynomial equation $x^5 - 4x + 2 = 0$. Similarly for β and γ. We have identified three more real numbers.

3.0.1 The way ahead

We started with a norm $|.|$ acting on elements of $\mathbb{Q}$ and used the norm to complete $\mathbb{Q}$ as a metric space in which all Cauchy sequences have a limit. We called this space $\mathbb{R}$, the set of all real numbers. The obvious question is whether there is another norm which can act on the elements of $\mathbb{Q}$ and be used to complete $\mathbb{Q}$ as a metric space in which all Cauchy sequences employing this norm converge to a limit. The answer is Yes and we call this new metric space the field of p-adic numbers.

Chapter 4

Introduction to p-adic numbers

4.1 Positive integers in p-adic form

We get our inspiration for p-adic numbers from fractions like $\frac{1}{3}$.

The rational number $\frac{1}{3} = 0.3333\cdots$ can also be written as:

$$\frac{1}{3} = 0 + 3\cdot 10^{-1} + 3\cdot 10^{-2} + 3\cdot 10^{-3} + \cdots = \sum_{n=0}^{\infty} 3.10^{-n}$$

We could call $\sum_{n=0}^{\infty} 3.10^{-n}$ the 10-adic expansion of $\frac{1}{3}$.

But from now on, the "p" in p-adic stands for "prime" and for any given prime p, positive integers can be written in p-adic form, for example,

$$p = 3: \ 73 = 1\cdot 3^0 + 0\cdot 3^1 + 2\cdot 3^2 + 2\cdot 3^3$$
$$p = 5: \ 73 = 3\cdot 5^0 + 4\cdot 5^1 + 2\cdot 5^2$$

In general for a prime p and a positive integer m, we have the p-adic expansion of m thus:

$$m = a_0p^0 + a_1p^1 + a_2p^2 + \cdots + a_np^n = \sum_{k=0}^{n} a_kp^k$$

with $a_i \in \mathbb{Z},\ 0 \le a_i \le p-1$. We call $\sum_{k=0}^{n} a_kp^k$ a p-adic number.

Note 1. *It is instructive to find the p-adic expansions of several positive integers by hand but it quickly becomes tedious. If you google "G-Pari" you can download a super-calculator by that name and also a user manual. When you open the calculator the prompt is gp >. If, for example, you type 173+O(5^ 3) where the "O" means order, then the calculator will return the 5-adic expansion of 173 up to the power of 5^3.*

4.2 Negative integers in p-adic form

Given the p-adic expansion of a positive integer it is then easy to write down the p-adic expansions of negative integers, since, for example, we have $73 + (-73) = 0$. For $p = 3$ we need to "fill in" this addition so that when we add the missing term in the -73 line to the corresponding term in the 73 line we need to get 0.

$$\begin{aligned} 73 &= 1 \cdot 3^0 + 0 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 \\ -73 &= \\ 0 &= \overline{0 \cdot 3^0 + 0 \cdot 3^1 + 0 \cdot 3^2 + 0 \cdot 3^3 \cdots} \end{aligned}$$

In the first column on the right side, the 3^0 term of 73 is 1.3^0 so the 3^0 term in -73 must be 2.3^0 so that the addition is $1.3^0 + 2.3^0 = 3.3^0 = 3^1$ leaving a 0 in the 3^0 column but bringing forward a 1 into the 3^1 column.

In the second column the 3^1 term of 73 is 0.3^1 but we have brought forward 1.3^1 from the first column, so we need the -73 term to be 2.3^1 to give a total of $3.3^1 = 3^2$ leaving the addition in the 3^1 column equal to zero but bringing forward 3^2 into the third column.

And so we continue, but we find the p-adic expansion of -73 has an infinite number of terms.

$$-73 = 2 \cdot 3^0 + 2 \cdot 3^1 + 0 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + 2.3^5 + \cdots$$

Note 2. *The obvious question is that the left side is -73 but the right side does not appear to be convergent according to our "normal" definition of convergence. Somehow we left the real world, we say we are in the world of p-adic numbers. How did we enter it? When we added 73 and -73 we generated an infinite string of 0's on the right side of* $0 = \cdots$. *But is this really 0? Let's study p−adic numbers some more before we seek an answer to that question.*

Notation 2. *If we omit the symbols for* $3^0,\ 3^1 \cdots$ *then we write the* 3*-adic expansions of 73 and -73 thus:*

$$\begin{aligned} 73 &= 1022 \\ -73 &= 230022222\cdots = 2300\overline{2} \end{aligned}$$

where, as for repeating decimals, $\overline{2}$ *means the repetition of the number or numbers under the overline, in this case 2.*

4.3 Rational numbers in p-adic form

Let p be a fixed prime number.
Consider the rational number $\dfrac{a}{b}$.
Now $a = p^k c_1$ and $b = p^j d_1$ where $gcd(p, c_1) = 1,\ gcd(p, d_1) = 1$

So that $\frac{a}{b} = p^n \frac{c_1}{d_1},\ n = k - j.$
Note n may be negative. Let,

$$\frac{c_1}{d_1} = a_0 + a_1 p^1 + a_2 p^2 + \cdots \tag{4.3.1}$$

Take *mod* p of both sides.

$$\begin{aligned} c_1 d_1^{-1} &\equiv a_0 + a_1 p + a_2 p^2 + \cdots (mod\ p) \\ \Rightarrow c_1 d_1^{-1} &\equiv a_0 (mod\ p) \end{aligned} \tag{4.3.2}$$

Solving (4.3.2) by inspection gives the value of a_0. Consider from (4.3.1),

$$\begin{aligned} c_1 d_1^{-1} - a_0 &= a_1 p^1 + a_2 p^2 + a_3 p^3 + \cdots \\ &= p(a_1 + a_2 p^1 + a_3 p^2 + \cdots) \\ &= p \frac{c_2}{d_2} \end{aligned}$$

where $c_2 d_2^{-1} = a_1 + a_2 p^1 + a_3 p^2 + \cdots$ Taking modulus p of both sides gives,

$$c_2 d_2^{-1} \equiv a_1 (mod\ p) \tag{4.3.3}$$

Solving (4.3.3) by inspection gives the value of a_1. If we continue in this way we have the general equations,

$$c_k d_k^{-1} \equiv a_{k-1} (mod\ p) \tag{4.3.4}$$

$$c_k d_k^{-1} - a_{k-1} = p c_{k+1} d_{k+1}^{-1} \tag{4.3.5}$$

For each value of k we solve (4.3.4) by inspection and then move on to (4.3.5).

Note 3. *If p divides a and/or b, we write a rational number in the form* $\frac{a}{b} = p^n \frac{c}{d}$ *where c and d are not divisible by p, then find the p-adic expansion of* $\frac{c}{d}$ *and finally multiply each term in its expansion by* p^n. *Let's do an example.*

Example 1. *Find the* 5*-adic expansion of* $\frac{2}{15}$
Now $\frac{2}{15} = 5^{-1}\frac{2}{3}$ *so we will find the* $5-$*adic expansion of* $\frac{2}{3}$ *and then multiply it by* 5^{-1}
From (4.3.4) with $k = 1,\ c_1 = 2,\ d_1 = 3$, *we have,*

$$\frac{2}{3} \equiv a_0 (mod\ 5) \Rightarrow 2 \equiv 3a_0 (mod\ 5) \Rightarrow a_0 = 4$$

By (4.3.5) with $k = 1$ *we have,*

$$\frac{2}{3} - 4 = -\frac{10}{3} = 5.\frac{-2}{3} \Rightarrow c_2 = -2,\ d_2 = 3$$

By (4.3.4) with $k = 2$ we have,

$$-\frac{2}{3} \equiv a_1 (mod\ 5) \Rightarrow 3a_1 + 2 \equiv 0 (\text{mod } 5) \Rightarrow a_1 = 1$$

By (4.3.5) with $k = 2$ we have,

$$-\frac{2}{3} - 1 = -\frac{5}{3} = 5 \cdot -\frac{1}{3} \Rightarrow c_3 = -1, d_3 = 3$$

By (4.3.4) with $k = 3$ we have,

$$-\frac{1}{3} \equiv a_2 (mod\ 5) \Rightarrow 3a_2 + 1 \equiv 0 (\text{mod } 5) \Rightarrow a_2 = 3$$

and so on.
We find,

$$\frac{2}{3} = 4 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots$$

so that

$$\begin{aligned} \frac{2}{15} &= 5^{-1}(4 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots) \\ &= 4 \cdot 5^{-1} + 1 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2 + 3 \cdot 5^3 + \cdots \end{aligned}$$

Notation 3. *In the compact form of a p-adic number we introduce a decimal point to separate the negative powers of p from the non-negative powers. Thus we would write,*

$$\frac{2}{15} = 4.1313\cdots = 4.\overline{13}$$

We extend the definition of the expansion of a p-dic number as follows.

Definition 10. *If N is a rational number, its p-adic expansion has the form,*

$$\begin{aligned} N &= a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1p^1 + a_2p^2 + \cdots \\ &= \sum_{n=-m}^{\infty} a_n p^n \\ &= a_{-m}a_{-m+1}\cdots.a_0a_1a_2\cdots \text{ (Note the decimal before } a_0.) \end{aligned}$$

and we call $\sum_{n=-m}^{\infty} a_n p^n$ a p−adic number.

4.4 Mathematical Operations on p-adic numbers

4.4.1 Addition

Let $p = 5$. Let's add:

$$\begin{aligned} \frac{2}{3} &= 4 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + \cdots = .4131313\cdots \\ \frac{5}{6} &= 0 \cdot 5^0 + 1 \cdot 5^1 + 4 \cdot 5^2 + \cdots = .0140404\cdots \end{aligned}$$

We add digits from left to right, each time applying *mod* 5 to the sum and carrying a 1 forward if the sum exceeds $p-1$.

$$\begin{aligned}\frac{2}{3} &= .413131313\cdots\\ \frac{5}{6} &= \underline{.014040404}\cdots\\ \frac{3}{2} &= .422222222\cdots\end{aligned}$$

4.4.2 Subtraction

Example 2. *Let $p = 5$. Asked,for example, to find $\frac{2}{3}-\frac{5}{6}$, we calculate the sum $\frac{2}{3}+(-\frac{5}{6})$ Using $0 = \frac{5}{6}+(-\frac{5}{6})$ we need to fill in the second row of:*

$$\begin{aligned}\frac{5}{6} &= .0140404040\cdots\\ -\frac{5}{6} &= \\ 0 &= \overline{.0000000000\cdots}\end{aligned}$$

Then,

$$-\frac{5}{6} = .0404040400\cdots$$

and

$$\begin{aligned}\frac{2}{3} &= .4131313131\cdots\\ +\frac{-5}{6} &= \underline{.0404040404\cdots}\\ \Rightarrow -\frac{1}{6} &= .4040404040 = .\overline{40}\end{aligned}$$

4.4.3 Multiplication

We work left to right and carry forward after applying *mod p* to each sum.

Example 3. *Let* $p = 5$.

$$\begin{aligned}
\frac{2}{3} &= .4\ 1\ 3\ 1\ 3\ 1\ 3\ 1\cdots \\
\times\frac{5}{6} &= \underline{.0\ 1\ 4\ 0\ 4\ 0\ 4\ 0\cdots} \\
&\quad 0\cdots \\
&\qquad 4\ 1\ 3\ 1\ 3\ 1\ 3\cdots \\
&\qquad\quad 1\ 2\ 3\ 1\ 3\ 1\cdots \\
&\qquad\qquad 0\cdots \\
&\qquad\qquad\quad 1\ 2\ 3\ 1\cdots \\
&\qquad\qquad\qquad 0\cdots \\
&\qquad\qquad\qquad\quad \underline{1\ 2\cdots} \\
\frac{5}{9} &= .0\ 4\ 2\ 0\ 1\ 2\ 4\ 3\cdots
\end{aligned}$$

4.4.4 Division

Example 4. *Consider*

$$\frac{24}{17} = \frac{0\cdot 3^0 + 2\cdot 3^1 + 2\cdot 3^2}{2\cdot 3^0 + 2\cdot 3^1 + 1\cdot 3^2} = \frac{.022}{.221}$$

Let,

$$\frac{24}{17} = a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$$

So, $24 = 17(a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots)$
Then in 3*-adics,*

$$0\cdot 3^0 + 2\cdot 3^1 + 2\cdot 3^2 = (2\cdot 3^0 + 2\cdot 3^1 + 1\cdot 3^2)(a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots)$$

We compare powers of 3 in this equation.

3^0 : $0 = 2a_0 \Rightarrow a_0 = 0$

3^1 : $2 = 2a_1 + 2a_0 \Rightarrow a_1 = 1$

3^2 : $2 = 2a_2 + 2a_1 + a_0 \Rightarrow a_2 = 0$

3^3 : $0 = 2a_3 + 2a_2 + a_1 = 2a_3 + 1 \Rightarrow a_3 = 1$

We have brought forward a 3^4 *term since the coefficient of* 3^3 *is 3.*

3^4 : $0 = 2a_4 + 2a_3 + a_2 + 1 = 2a_4 + 3 \Rightarrow a_4 = 0$

We have brought forward a 1.3^5 *term since the coefficient of* 3^4 *is 3.*

3^5 : $0 = 2a_5 + 2a_4 + a_3 + 1 = 2a_4 + 2 \Rightarrow a_5 = 2$

We have brought forward a 2.3^6 *term since the coefficient of* 3^5 *must be 6.*

3^6 : $0 = 2a_6 + 2a_5 + a_4 + 2 = 2a_6 + 6 \Rightarrow a_6 = 0$

We have brought forward a 2.3^7 *term since the coefficient of* 3^6 *is 6.*

$3^7: \ 0 = 2a_7 + 2a_6 + a_5 + 2 = 2a_7 + 4 \Rightarrow a_7 = 1$

We have brought forward a 2.3^8 *term since the coefficient of* 3^7 *is 6.*

$3^8: \ 0 = 2a_8 + 2a_7 + a_5 + 2 = 2a_8 + 4 \Rightarrow a_8 = 1$

We have brought forward a 2.3^9 *term since the coefficient of* 3^8 *is 6.*

$3^9: \ 0 = 2a_9 + 2a_8 + a_7 + 2 = 2a_9 + 5 \Rightarrow a_9 = 2$

We have brought forward a $1 \cdot 3^1 1$ *term since the coefficient of* 3^9 *is 9.*

We conclude,

$$\frac{24}{17} = 1 \cdot 3^0 + 0 \cdot 3^1 + 0 \cdot 3^2 + 1 \cdot 3^3 + 0 \cdot 2^4 + 2 \cdot 3^5 + 0 \cdot 2^6 + 1 \cdot 3^7 + 1 \cdot 3^8 + 2 \cdot 3^9 + \cdots$$

Chapter 5

The p-adic completion of $\mathbb{Q}$

5.1 p-adic numbers and Cauchy sequences

The norm we used to complete $\mathbb{Q}$ into $\mathbb{R}$ was the absolute value norm, $|x|$, and its associated distance function $d(x,y) = |x-y|$. Now all of the p-adic numbers we found in Chapter 4 can be written as the limiting values of a Cauchy sequence. Thus,

$$\frac{24}{17} = 1\cdot 3^0 + 0\cdot 3^1 + 0\cdot 3^2 + 1\cdot 3^3 + 0\cdot 3^4 + 2\cdot 3^5 + 0\cdot 3^6 + 1\cdot 3^7 + 1\cdot 3^8 + 2\cdot 3^9 + \cdots$$

can be set up as a sequence of partial sums,

$$1\cdot 3^0$$
$$1\cdot 3^0 + 0\cdot 3^1$$
$$1\cdot 3^0 + 0\cdot 3^1 + 0\cdot 3^2$$
$$1\cdot 3^0 + 0\cdot 3^1 + 0\cdot 3^2 + 1\cdot 3^3$$
$$1\cdot 3^0 + 0\cdot 3^1 + 0\cdot 3^2 + 1\cdot 3^3 + 0\cdot 3^4$$
$$\ldots$$
$$1\cdot 3^0 + 0\cdot 3^1 + 0\cdot 3^2 + 1\cdot 3^3 + 0\cdot 3^4 + 2\cdot 3^5 + 0\cdot 3^6 + 1\cdot 3^7 + 1\cdot 3^8 + 2\cdot 3^9$$
$$\ldots$$

which converge to $\frac{24}{17}$. But this sequence is not Cauchy if we use the absolute value norm since $|a_n - a_m|$ is some number $b.3^n,\ b \in \{1,2\}$ and this will never be less than ϵ for ALL $\epsilon > 0$ and specifically for $\epsilon = 3^{n-1}$.
The question is whether there is another norm besides the absolute value norm that will give us convergence of p-adic numbers. We would then be able to have the completion of $\mathbb{Q}$ into some other field that is not $\mathbb{R}$. We would call this $\mathbb{Q}_p$, the field of p-adic numbers, since all of them would be the limits of Cauchy sequences in $\mathbb{Q}$.

5.2 p-adic norm

We seek a completion of $\mathbb{Q}$ in which all p–adic numbers have a limit. Let's define a different norm on $\mathbb{Q}$.

Definition 11. *For any prime p we define the p-adic norm $|.|_p$ by,*

$$|x|_p = \begin{cases} p^{-ord_p x} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

where $ord_p x$ is the highest power of p that divides x.
We call $ord_p x$ the p-adic valuation of x.

Example 5.

$$|125|_5 = |5^3|_5 = 5^{-3}$$
$$|28|_7 = |4 \times 7^1|_7 = 7^{-1}$$
$$|192|_2 = |3 \times 64|_2 = |3 \times 2^6|_2 = 2^{-6}$$

Note 4. *Note $|x|_p = |y|_p$ if and only if $ord_p x = ord_p y$.*

We claim $|x|_p$ is a norm, obeying the same three conditions as set out in the general definition of a norm $||x||$ in Definition 3 on page 3, namely.
(1.) $|x|_p = 0$ if and only if $x = 0$. This is true by the definition of $|x|_p$.
(2.) $|xy|_p = |x|_p|y|_p$.

Proof. If $x = p^\alpha \frac{a}{b}$, $p \nmid a, b$ and $y = p^\beta \frac{c}{d}$, $p \nmid c, d$, then,

$$|xy|_p = \left| p^{\alpha+\beta} \frac{a}{b} \cdot \frac{c}{d} \right|_p = p^{-\alpha-\beta}$$

and,

$$|x|_p|y|_p = \left| p^\alpha \frac{a}{b} \right|_p \left| p^\beta \frac{c}{d} \right|_p = p^{-\alpha} p^{-\beta} = |xy|_p$$

□

(3.) $|x + y|_p < |x|_p + |y|_p$

Proof. Let $x = p^r \frac{a}{b}$, $y = p^s \frac{c}{d}$, $p \nmid a, b, c$ or d, and $a, b, c, d, r, s \in \mathbb{Z}$.
Case 1: $r = s$

$$x + y = p^r \left(\frac{ad + bc}{bd} \right)$$
$$\Rightarrow ord_p(x + y) \geq r \text{ since } p \nmid bd \text{ but } p \text{ may divide } ad + bc.$$
$$= min(ord_p x, ord_p y)$$

Then,

$$\begin{aligned} |x+y|_p &= p^{-ord_p(x+y)} \\ &\leq max(p^{-ord_p x}, p^{-ord_p y}) \\ &= max(|x|_p, |y|_p) \\ &\leq |x|_p + |y|p \end{aligned}$$

Case 2: $r \neq s$, say $s > r$

$$\begin{aligned} x+y &= p^r \left(\frac{a}{b} + p^{s-r}\frac{c}{d}\right) \\ &= p^r \left(\frac{ad + p^{s-r}bc}{bd}\right) \end{aligned}$$

Now since $s - r > 0$ and $p \nmid bd, p \nmid ad$ then,

$$ord_p(x+y) = r = min(ord_p x, ord_p y)$$

Then,

$$\begin{aligned} |x+y|_p &= p^{-ord_p(x+y)} \\ &\leq max(p^{-ord_p x}, p^{-ord_p y}) \\ &= max(|x|_p, |y|_p) \\ &\leq |x|_p + |y|_p \end{aligned} \tag{5.2.1}$$

□

Definition 12. *A norm $||.||$ is called non-Archimedean is it satisfies the condition,*

$$||xy|| \leq max(||x||, ||y||)$$

otherwise it is called Archimedean.

Hence since

$$|x+y|_p \leq max(|x|_p + |y|_p) \text{ by } (5.2.1)$$

$|.|_p$ is a non-Archimedean norm whereas the ordinary absolute value norm, $|.|$ is an Archimedean norm.

5.3 p-adic distance function

We claim $d(x,y) = |x-y|_p$ is a distance function on $\mathbb{Q}$ obeying the conditions set out in the definition of a general distance function in Definition 4 on page 3, namely, for all x, y in $\mathbb{Q}$,

1. $d(x,y) = 0$ if and only if $x = y$. This is true since $d(x,y) = 0 \Rightarrow |x-y|_p = 0$ and, by definition of the norm, $|x-y| = 0$ if and only if, $x - y = 0 \Rightarrow x = y$.

2. $d(x,y) = d(y,x)$. This is true since, by the second criteria of the norm, $|x|_p$,

$$d(x,y) = |x-y|_p = |y-x|_p = d(y,x)$$

3. $d(x,y) \leq d(x,z) + d(z,y)$ for all $z \in \mathbb{Q}$. This is true since,

$$\begin{aligned} d(x,y) &= |x-y|_p \\ &= |x-z+z-y|_p \\ &\leq |x-z|_p + |z-x|_p \text{ by Criteria 3 of the norm} \\ &= d(x,z) + d(z,y) \end{aligned}$$

Definition 13. *The metric induced by a non-Archimedean norm is called an ultra-metric. Hence $d(x,y) = |x-y|_p$ is an ultra-metric and it satisfies,*

$$d(x,y) \leq max(|x-y|_p, |y-z|_p) \text{ by (5.2.1),}$$

We also call $|x-z|_p \leq max(|x-y|_p, |y-z|_p)$ the strong triangle inequality.

5.4 Cauchy sequences using p-adic norms

We first redefine Cauchy sequences using p-adic norms.

Definition 14. *Using the p-adic norm, $|x|_p$, a sequence $\{a_n\}$ in $\mathbb{Q}$ is a p-adic Cauchy sequence if for all $\epsilon > 0$ there exists an $N \in \mathbb{N}$ such that if $m, n > N$ then $|a_n - a_m|_p > \epsilon$.*

Example 6.
In 3-adics we saw,

$$73 = 1.3^0 + 0.3^1 + 2.3^2 + 2.3^3$$

The finite sequence of partial sums,

$$\begin{aligned} &1.3^0 \\ &1.3^0 + 0.3^1 \\ &1.3^0 + 0.3^1 + 2.3^2 \\ &1.3^0 + 0.3^1 + 2.3^2 + 2.3^3 \end{aligned}$$

can be made infinite thus,

$$\begin{aligned} &1.3^0 + 0.3^1 + 2.3^2 + 2.3^3 + 0.3^4 \\ &1.3^0 + 0.3^1 + 2.3^2 + 2.3^3 + 0.3^4 + 0.3^5 \\ &\ldots \end{aligned}$$

where all the other terms of powers of 3 more than 3 have coefficient 0. Then for all $\epsilon > 0$ and for any $m, n > N = 3$, with say $n > m$, we have,

$$|a_n - a_m|_3 = |0 \cdot 3^{m+1} + 0 \cdot 3^{m+2} + \cdots|_3 = |0|_3 = 0 < \epsilon.$$

This is therefore a Cauchy sequence.

5.5 Another definition of p-adic Cauchy sequences

Theorem 4.
A sequence $\{a_n\}$ in $\mathbb{Q}_p$ is a Cauchy sequence if and only if

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

Proof. Given $\{a_n\}$ is Cauchy we have,

$$\lim_{m,n\to\infty} |a_m - a_n|_p = 0$$

Let $m = n + 1$. Then,

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

Conversely, assume $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$. This means that for any $\epsilon > 0$ there exists an $N \in \mathbb{N}$ such that for $n > N$ we have,

$$|a_{n+1} - a_n|_p < \epsilon.$$

Then for any $m > n > N$, using the strong triangle inequality, we have,

$$\begin{aligned} |a_m - a_n|_p &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + \cdots - a_n|_p \\ &\leq max(|a_m - a_{m-1}|_p, \cdots |a_{n+1} - a_n|_p) < \epsilon \end{aligned}$$

which completes the proof. □

5.6 Equivalence classes of Cauchy sequences

Definition 15. *There may be several Cauchy sequences with the same limit. This would occur if the beginning terms in the sequences $\{a_n\}$ and $\{b_n\}$ were different but the infinite "tail" of each sequence is the same, each heading to the same limit. We would have,*

$$|a_i - b_i|_p \to 0 \text{ as } i \to \infty.$$

We say these two Cauchy sequences are equivalent or belong to the same equivalence class.

For example we could have a term in $\{a_n\}$ of the form,

$$2.5^0 + 3.5^1 + 0.5^2 + \cdots + 4.5^k + 3.5^{k+1} + \cdots$$

and for the same value of n, a term in $\{b_n\}$ of the form,

$$3.5^0 + 1.5^1 + 3.5^2 + \cdots + 4.5^k + 3.5^{k+1} + \cdots$$

where beginning with the term in 5^k, the two sequences are the same. In this case, we say $\{a_n\}$ and $\{b_n\}$ belong to the same equivalence class of Cauchy sequences.

5.7 $\mathbb{Q}_p$, a completion of $\mathbb{Q}$.

Definition 16. *We define $\mathbb{Q}_p$, the field of p-adic numbers, to be the completion of $\mathbb{Q}$ with respect to the p–adic norm $|x|_p$. By completion we mean that every Cauchy sequence with terms in $\mathbb{Q}$ has a limit in $\mathbb{Q}_p$.*

5.8 Elements of $\mathbb{Q}_p$

By definition every p-adic number is of the form,

$$\begin{aligned}\sum_{n=-m}^{\infty} a_n p^n &= a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \ldots + a_0 + a_1 p^1 + a_2 p^2 + \ldots \\ &= a_{-m}a_{-m+1}\cdots.a_0 a_1 a_2 \ldots\end{aligned}$$

We can form a sequence $\{b_n\}$ from a p-adic number thus,

$$\begin{aligned} b_0 &= a_{-m}p^{-m} \\ b_1 &= a_{-m}p^{-m} + a_{-m+1}p^{-m+1} \\ &\cdots \\ b_n &= a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_k p^k \\ b_{n+1} &= a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_k p^k + a_{k+1}p^{k+1}\end{aligned}$$

Since $k \to \infty$ as $n \to \infty$, we have,

$$\begin{aligned}\lim_{n\to\infty} |b_{n+1} - b_n|_p &= \lim_{k\to\infty} |a_{k+1}p^{k+1}|_p \\ &= \lim_{k\to\infty} p^{-(k+1)} \\ &= 0\end{aligned}$$

then by Theorem 4, $\{b_n\}$ is a Cauchy sequence. We therefore conclude every p-adic number is an element of $\mathbb{Q}_p$.

We will see they are the only elements. That is we claim all the elements of $\mathbb{Q}_p$ are, according to Definition 10 on page 14, of the form,

$$\begin{aligned}\sum_{n=-m}^{\infty} a_n p^n &= a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \ldots + a_0 + a_1 p^1 + a_2 p^2 + \ldots \\ &= a_{-m}a_{-m+1}\cdots.a_0 a_1 a_2 \ldots\end{aligned}$$

We begin with a lemma and a reminder from elementary number theory that if $a, b \in \mathbb{Z}$ and the $gcd(a, b) = 1$, then there are integers x, y such that $ax + by = 1$.

Lemma 5.
If $x \in \mathbb{Q}$ and $|x|_p \leq 1$ then for any i there exists an integer α such that $|\alpha - x|_p \leq p^{-i}$. The integer α can be chosen in the the set $\{0, 1, 2, \cdots, p^{i-1}\}$ and is unique if chosen in this range.

Proof. Let $x = \dfrac{a}{b}$ be written in lowest terms and $|x|_p \leq 1$.
Since $|x|_p = \left|\dfrac{a}{b}\right|_p \leq 1$ then $p \nmid b$ otherwise $b = pb'$ and we have $|x|_p = \left|\dfrac{a}{pb'}\right|_p = p^1 > 1$.
Hence b and p^i are relatively prime. So, as we recalled, we can find integers m, n such that $mb + np^i = 1$.
Let $\alpha = am$. Then,

$$\begin{aligned}|\alpha - x|_p &= \left|am - \frac{a}{b}\right|_p \\ &= \left|\frac{a}{b}\right|_p |mb - 1|_p \\ &\leq |mb - 1|_p \text{ since } p \text{ may divide } a \\ &= |np^i|_p \\ &= |n|_p p^{-i} \\ &\leq p^{-i} \text{ since } p \text{ may divide } n\end{aligned}$$

Finally, using $|x + y|_p \leq max(|x|_p, |y|_p)$, we can add a multiple of p^i to α to get an integer between 0 and p^i for which $|\alpha - x|_p \leq p^{-i}$ still holds. □

We now have the key theorem.

Theorem 6.
Every equivalence class a in $\mathbb{Q}$ for which $|a|_p \leq 1$ has exactly one representative Cauchy sequence of the form $\{a_i\}$ for which,
(1) $0 \leq a_i < p^i$ for $i = 1, 2, 3, \ldots$
(2) $a_i \equiv a_{i+1} (\text{mod } p^i)$ for $i = 1, 2, 3, \ldots$

Proof.
We first prove uniqueness. If $\{b_i\}$ is a different sequence satisfying,
(1) $0 \leq b_i < p^i$ for $i = 1, 2, 3, \ldots$

(2) $b_i \equiv b_{i+1} (\text{mod } p^i)$ for $i = 1, 2, 3, \ldots$ then for one or more values of k, we have $a_k \neq b_k$. and then $a_k \not\equiv b_k (\text{mod } p^k)$ because by (1) both are less then p^k so p^k cannot divide their difference.
But then for all $i \geq k$ we have both,

$$p^k | a_i - a_k \Rightarrow a_i \equiv a_k (\text{mod } p^k)$$
$$p^k | b_i - b_k \Rightarrow b_i \equiv b_k (\text{mod } p^k)$$

But then since $a_k \neq b_k$ we have $a_i \neq b_i$ for all $i \geq k$. So, $\lim_{i \to \infty} |a_i - b_i|_p \neq 0$ so $\{b_i\}$ is not in the same equivalence class as $\{a_i\}$.

*****

Let $\{b_i\}$ be a Cauchy sequence representing a. We want to find an equivalent sequence $\{a_i\}$ satifying (1) and (2).
Since a is the limit of the sequence $\{b_i\}$ or $|b_i|_p \to |a|_p$ as $i \to \infty$ then $|b_i|_p \leq 1$ for all i.
Now the sequence $\{b_i\}$ is Cauchy so for every $j \in \mathbb{N}$ let $N(j)$ be a positive integer such that,

$$|b_i - b_j|_p \leq p^{-j} \text{ for all } i, j > N(j). \tag{5.8.1}$$

Again, since $\{b_i\}$ is Cauchy with the gap between successive terms becoming smaller and smaller, we may take the sequence $N(j)$ to be strictly increasing with j.
From Lemma 5 we can find integers $a_j,\ 0 \leq a_j < p^j$ such that

$$|a_j - b_{N(j)}|_p \leq \frac{1}{p^j} \tag{5.8.2}$$

Let us show $a_j \equiv a_{j+1} (\text{mod } p^j)$ and that the sequences $\{a_i\}$ and $\{b_i\}$ are in the same equivalence class. Now,

$$|a_{j+1} - b_{N(j)+1}|_p \leq \frac{1}{p^{j+1}} \text{ by (5.8.2) and} \frac{1}{p^{j+1}} < \frac{1}{p^j}$$
$$|b_{N(j)+1} - b_{N(j)}|_p \leq \frac{1}{p^j} \text{ by Theorem 4 since } \{b_n\} \text{ is Cauchy}$$
$$|a_j - b_{N(j)}|_p \leq \frac{1}{p^j} \text{ by (5.8.2)}$$

Then, using the strong triangle inequality,

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j)+1} + b_{N(j)+1} - b_{N(j)} - (a_j - b_{N(j)}|_p \\ &\leq max(|a_{j+1} - b_{N(j)+1}|_p, |b_{N(j)+1} - b_{N(j)}|_p, |(a_j - b_{N(j)}|_p) \\ &\leq max(\frac{1}{p^j}, \frac{1}{p^j}, \frac{1}{p^j}) \\ &= \frac{1}{p^j} \end{aligned}$$

so $p^j|(a_{j+1} - a_j)$ and we have shown $a_j \equiv a_{j+1} (\text{mod } p^j)$

Also, choose any j. We have,

$$\begin{aligned} |a_j - b_{N(j)}|_p &\leq \frac{1}{p^j} \text{ by (5.8.2)} \\ |b_i - b_{N(j)}|_p &\leq \frac{1}{p^j} \text{ since } \{b_i\} \text{ is Cauchy} \\ |a_i - a_j|_p &\leq \frac{1}{p^j} \end{aligned}$$

since $a_i < p^j$ and $a_j < p^j$ and hence $p^j \nmid a_i - a_j$ and $|a_i - a_j|_p \leq |p^j|_p = \frac{1}{p^j}$.
Accordingly, for $i \geq N(j)$ we have,

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |(b_i - b_{N(j)})|_p \\ &\leq max(\frac{1}{p^j}, \frac{1}{p^j}, \frac{1}{p^j}) \\ &= \frac{1}{p^j} \end{aligned}$$

Hence, $|a_i - b_i|_p \to 0$ as $i \to \infty$, making $\{b_i\}$ and $\{a_i\}$ equivalent sequences. □

****

We can now identify the elements of $\mathbb{Q}_p$.
If $a \in \mathbb{Q}_p$ with $|a|_p \leq 1$, meaning $p \nmid a$, and $\{a_i\}$ is the representative Cauchy sequence with limit a as $i \to \infty$ then since a_i is such that $0 \leq a_i < p^i$, we can write for integers d_i with $0 \leq d_i \leq p - 1$,

$$\begin{aligned} 0 < a_1 < p^1 &\Rightarrow a_1 = d_0 \\ 0 < a_2 < p^2 &\Rightarrow a_2 = d_0 + d_1 p^1 \\ 0 < a_3 < p^3 &\Rightarrow a_3 = d_0 + d_1 p^1 + d_2 p^2 \\ &\cdots \end{aligned}$$

So,

$$a_i = d_0 + d_1 p^1 + \cdots + d_{i-1} p^{i-1},\ 0 \leq d_i \leq p - 1,\ d_i \in \mathbb{Z}$$

Further, the condition $a_i \equiv a_{i+1} (\text{mod } p^i)$ for $i = 1, 2, 3, \ldots$ means that

$$a_{i+1} = d_0 + d_1 p^1 + \cdots + d_{i-1} p^{i-1} + d_i p^i,$$

since $a_{i+1} - a_i = d_i p^i \equiv 0 (\text{mod } p^i)$, where all the "$p$-adic digits" d_0 through d_{i-1} are all the same as for a_i. Thus a is represented by the convergent series,

$$a = \sum_{n=0}^{\infty} d_n p^n$$

Finally, if $|a|_p > 1$, meaning some power of p, say p^m, is a factor in the denominator of the rational number a then we can multiply a by that power of p, so as to get a p-adic number ap^m that satisfies $|b|_p = 1$. Then we can write,

$$a = \sum_{n=-m}^{\infty} d_n p^n$$

where $d_{-m} \neq 0$ and $d_n \in \{0, 1, 2, 3, \cdots, p-1\}$.
This representation of a is called the canonical p-adic expression of a. It has finitely many digits before the point and infinitely many after the point. As we saw, for example,

$$\begin{aligned} \frac{24}{17} &= 1.3^0 + 0.3^1 + 0.3^2 + 1.3^3 + 0.2^4 + 2.3^5 + 0.2^6 + 1.3^7 + 1.3^8 + 2.3^9 + \dots \\ &= 4.1313\dots \end{aligned}$$

We have shown every element of $\mathbb{Q}_p$ is of the form,

$$a = \sum_{n=-m}^{\infty} d_n p^n$$

where $d_n \in \{0, 1, 2, 3, \cdots, p-1\}$

Chapter 6

More on p-adic numbers

6.1 Convergence Test for p-adic sequences

Lemma 7.
Let $\{a_k\}$ be a sequence in $\mathbb{Q}_p$. Then $\{a_k\}$ converges in $\mathbb{Q}_p$ if and only if $\lim_{k\to\infty} |a_k|_p = 0$.

Proof. Suppose $\{a_k\}$ converges in $\mathbb{Q}_p$ to the limit α. Then,

$$a_n = \sum_{k=0}^{n} a_k - \sum_{k=0}^{n-1} a_k \to \alpha - \alpha = 0$$

This is true in both $\mathbb{R}$ and $\mathbb{Q}_p$.

Conversely, suppose $a_k \to 0$ as $k \to \infty$.
Let α_n have the p-adic expansion $\alpha_n = \sum_{k=0}^{n} a_k$.
Then for all m, n with $0 < m < n$, we have,

$$\begin{aligned} |\alpha_n - \alpha_m|_p &= |\sum_{k=0}^{n} a_k - \sum_{k=0}^{m} a_k|_p \\ &= |\sum_{k=m+1}^{n} a_k|_p \\ &\leq max(|a_{m+1}|_p, \cdots, |a_n|_p) \\ &\to 0 \quad \text{as} \quad m, n \to \infty \end{aligned}$$

So the partial sums α_n form a Cauchy sequence of elements of $\mathbb{Q}$ and hence, by definition of $\mathbb{Q}_p$, must converge to a limit in $\mathbb{Q}_p$. □

Note 5. *Lemma 7 also tells us that every p-adic number converges in $\mathbb{Q}_p$ since,*

$$\lim_{n\to\infty} |a_n p^n|_p = \lim_{n\to\infty} \frac{1}{p^n} = 0.$$

6.2 The p-adic expansion of -1

6.2.1 First method

Let p be a prime number. Let $S_\infty = 1 + p + p^2 + p^3 + \ldots$ Then we have,

$$\begin{aligned} S_\infty &= 1 + p + p^2 + p^3 + \ldots \\ pS_\infty &= \quad p + p^2 + p^3 + \ldots \\ pS_\infty - S_\infty &= -1 \\ S_\infty &= \frac{-1}{p-1} \\ \frac{-1}{p-1} &= 1 + p + p^2 + p^3 + \ldots \\ -1 &= (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \ldots \end{aligned}$$

For example,

$$-1 = 4 + 4.5 + 4.5^2 + 4.5^3 + \ldots$$

6.2.2 Second Method

We fill in the second line of the sum,

$$\begin{aligned} 1 &= 1 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + 0 \cdot p^3 + \ldots \\ \underline{-1} &= a_0 + a_1 p^1 + a_2 p^2 + a_3 p^3 + \ldots \\ 0 &= 0 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + 0 \cdot p^3 + \ldots \end{aligned}$$

We must have $a_0 = p - 1$ to have a 0 in the first column, That gives a sum of p so we bring $1 \cdot p$ forward into the second column. To have a 0 in the second column we then need $a_1 = p - 1$ which results in carrying $1 \cdot p^2$ into the third column nd so on.

6.3 x and $-x$ in general

In general we generate the p-adic expansion of a negative number from the expansion of its additive inverse as shown,

$$\begin{aligned} x &= a_0 p^0 + a_1 p^1 + a_2 p^2 + \ldots \\ \underline{-x} &= b_0 p^0 + b_1 p^1 + b_2 p^2 + \ldots \\ 0 &= 0 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + \ldots \end{aligned}$$

We need $b_0 = p - a_0$ so that the p^0 column adds to p which we carry forward into the p^1 column. We then need $b_1 = p - a_1 - 1$ which gives $0 \cdot p^1$ in the p^1 column and we bring forward $1 \cdot p^2$ into the p^2 column. All the other b_i coefficients will similarly be $b_i = p - a_i - 1$. We find,

$$-x = (p - a_0)p^0 + (p - a_1 - 1)p^1 + (p - a_2 - 1)p^2 + \ldots$$

For example, we have $59 = 2 \cdot 3^0 + 1 \cdot 3^1 + 0 \cdot 3^2 + 2 \cdot 3^3$ so that,

$$\begin{aligned} -59 &= (3-2)3^0 + (3-1-1)3^1 + (3-0-1)3^2 + (3-2-1)3^3 + (3-1)3^4 + \dots \\ &= 1 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + \dots \end{aligned}$$

We note that while a positive integer has a finite number of terms in its p-adic expansion, all negative integers, as well as rationals with a denominator greater than 1, have an infinite number of terms in their expansion. This is most easily seen for negative integers by multiplying the infinite p-adic expansion of -1 by the p-adic expansion of any positive integer.

6.4 The p-adic expansions of Square Roots

We first observe that not all square roots have p-adic expansions in all primes. In general if,

$$\sqrt{x} = a_0 p^0 + a_1 p^1 + a_2 p^2 + \dots$$

then, squaring, $x \equiv a_0^2 (\text{mod } p)$
Solutions of such equivalences are studied in number theory in a topic called quadratic residues and the equivalence is normally written $x^2 \equiv a (\text{mod } p)$. If the equivalence has a solution, we say a is a quadratic residue of p.

To find the quadratic residues of any prime p we square $1, 2, 3, \dots, \dfrac{p-1}{2}$ and take modulus p to see if we have an x and an a such that $x^2 \equiv a (\text{mod } p)$.
Let's take $p = 11$. We have,

$$\begin{aligned} 1^2 &\equiv 1 (\text{mod } 11) \\ 2^2 &\equiv 4 (\text{mod } 11) \\ 3^2 &\equiv 9 (\text{mod } 11) \\ 4^2 &\equiv 5 (\text{mod } 11) \\ 5^2 &\equiv 3 (\text{mod } 11) \end{aligned}$$

The values of a such that there is an x such that $x^2 \equiv a (\text{mod } 11)$ are $1, 4, 9, 5$, and 3.

This means, for numbers less than 11, we can find the 11-adic expansions of only the square roots of $1, 4, 9, 5, 3$. Of course, there are an infinitely many other values since $(11k+1)^2 \equiv 1 (\text{mod } 11), (11k+2)^2 \equiv 4 (\text{mod } 11)$, etc.

Example 7. *Let's find the* 7*-adic expansion of* $\sqrt{2}$*. Note* 2 *is a quadratic residue of* 7 *since* $3^2 \equiv 2 (\text{mod } 7)$*. In each step we operate mod* 7^k*,* $k = 1, 2, 3, \dots$*. Let,*

$$\begin{aligned} \sqrt{2} &= a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \dots \\ \textit{Square: } 2 &\equiv a_0^2 (\text{mod } 7) \\ \Rightarrow a_0 &= 3, 4 \end{aligned}$$

reflecting the fact that if $x^2 = 2$ *then* $x = \pm\sqrt{2}$. *Let's take* $a_0 = 3$.

$$\begin{aligned}\sqrt{2} &= 3 + a \cdot 7 + \cdots \\ \textit{Square: } 2 &= 9 + 6 \cdot 7a_1 (\text{mod } 7^2) \\ 7 + 42a_1 &\equiv 0 (\text{mod } 7^2) \\ a_1 &= 1\end{aligned}$$

We now have, (where we replace $2 \cdot 3$ *with* $7 - 1$*)*

$$\begin{aligned}\sqrt{2} &= 3 + 1 \cdot 7 + a_2 \cdot 7^2 + \cdots \\ \textit{Square: } 2 &= 9 + 1 \cdot 7^2 + 2 \cdot 3 \cdot 7 + 2 \cdot 3 \cdot a_2 \cdot 7^2 (\text{mod } 7^3) \\ 7 + 7^2 + 7^2 - 7 - a_2 \cdot 7^2 &\equiv 0 (\text{mod } 7^3) \\ (2 - a_2).7^2 &\equiv 0 (\text{mod } 7^3) \\ a_2 &= 2\end{aligned}$$

Then,

$$\begin{aligned}\sqrt{2} &= 3 + 1.7 + 2 \cdot 7^2 + a_3 \cdot 7^3 + \cdots \\ &\cdots \\ a_3 &= 6\end{aligned}$$

We then have,

$$\sqrt{2} = 3 + 1 \cdot 7^1 + 2 \cdot 7^2 + 6 \cdot 7^3 + \ldots$$

6.5 The p-adic expansions of Complex Numbers

The complex numbers are defined by,

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R},\ i = \sqrt{-1}\}$$

We know how to find the p-adic expansions of $a, b \in \mathbb{R}$, so let's address $i = \sqrt{-1}$. We choose $p = 5$. Let,

$$\sqrt{-1} = \sqrt{4 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots} = d_0 + d_1 \cdot 5^1 + d_2 \cdot 5^2 + d_3 \cdot 5^3 + \cdots$$

Squaring,

$$4 + 4 \cdot 5^1 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots = d_0^2 + 2 \cdot d_0 \cdot d_1 .5^1 + \cdots$$

So $d_0^2 = 4$ and $d_0 = \pm 2$ and we choose $d_0 = 2$ to have,

$$4 + 4 \cdot 5^1 + \cdots = 4 + 4d_1 \cdot 5 + \cdots$$

so we must have $d_1 = 1$ to give,

$$\begin{aligned} 4 + 4 \cdot 5^1 + 4 \cdot 5^2 + \cdots &= (2 + 1 \cdot 5^1 + d_2 \cdot 5^2 + \cdots)^2 \\ &= 4 + 4 \cdot 5^1 + (4d_2 + 1) \cdot 5^2 + \cdots \end{aligned}$$

which gives $d_2 = 2$ to give,

$$(4d_2 + 1) \cdot 5^2 = 9 \cdot 5^2 = 4.5^2 + 1 \cdot 5^3.$$

Continuing in this fashion we find the 5-adic expansion of $i = \sqrt{-1}$ is,

$$i = 0.2121342303220413240\ldots$$

****

The p-adic expansion of -1 in $\mathbb{Q}_p$ requires being able to solve,

$$\sqrt{-1} = \sqrt{(p-1) + (p-1)p^1 + (p-1)p^2 + \ldots}$$

By putting,

$$\sqrt{(p-1) + (p-1)p^1 + (p-1)p^2 + \ldots} = d_0 + d_1 p^1 + d_2 p^2 + \ldots$$

Squaring, we need to find d_0 from,

$$(p-1) + (p-1)p^1 + (p-1)p^2 + \ldots = d_0^2 + 2d_0 d_1 p^1 + \cdots$$

Therefore $p-1$ must be a square, namely, $p = 5, 17, 37, \ldots$ so that $p - 1 = 4, 16, 36, \ldots$ and $d_0 = 2, 4, 6, \ldots$.

This is really interesting since $\mathbb{C}$ is all we need to find roots of ploynomials with coefficients in $\mathbb{C}$, which includes $\mathbb{R}$, and yet $\mathbb{C}$ is contained in an infinite number of fields, $\mathbb{Q}_p$.

Mathematicians initially resisted the concept of imaginary numbers but then found them to be enormously useful in proving theorems, yet now along comes these p-adic numbers and their fields, $\mathbb{Q}_p$, many of which include $\mathbb{C}$. Will they also prove to be useful? Can some theorems that have for years, even centuries, resisted solutions using $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$, be proved using $\mathbb{Q}_p$?

Chapter 7

p-adic expansions of rationals - revisited

7.1 Key Theorem

Definition 17. *A real rational number has a purely periodic decimal expansion if it consists of only a repeated pattern of digits like* $\frac{1}{3} = 0.3.3.3.\ldots = \overline{3}$. *A similar definition applies to p-adics, so* $\frac{24}{17} = 4.\overline{13}$ *is not purely periodic, but* $-1 = \overline{p-1}$ *is.*

Note 6. *A purely periodic number such as* $\overline{d_0 d_1 d_2}$ *expands as,*

$$\begin{aligned} &d_0p^0 + d_1p^1 + d_2p^2 d_0p^3 + d_1p^4 + d_2p^5 + d_0p^6 + d_1p^7 + \cdots \\ &= (d_0p^0 + d_1p^1 + d_2p^2) + p^3(d_0p^0 + d_1p^1 + d_2p^2) + p^6(d_0p^0 + d_1p^1 + d_2p^2) + \cdots \\ &= (d_0p^0 + d_1p^1 + d_2p^2)(1 + p^3 + p^6 + \cdots) \end{aligned}$$

where $(1 + p^3 + p^6 + \cdots)$ *is an infinite geometric series.*

In Section 4.3 we showed a method of finding the p-adic expansions of rational numbers. The following describes another method.
We focus first on numbers with p-adic absolute value 1, which are p-adic expansions of the form $b_0 + b_1 \cdot p^1 + b_2 \cdot p^2 + \ldots, 0 \le b_i \le p-1, b_0 \neq 0$.

Theorem 8.
A rational number with p-adic absolute value 1 has a purely periodic expansion if and only if it lies in the real interval $[-1, 0)$.

Proof. A purely periodic p-adic expansion having p-adic absolute value 1 with a repeating block of k digits looks like $\overline{n_0 n_1 \ldots n_{k-1}}$ where $0 \le n_i \le p-1$ and $n_0 \neq 0$.

We can evaluate this as a fraction by summing a geometric series (see Note 6).

$$\begin{aligned}\overline{n_0n_1\dots n_{k-1}} &= 1(n_0n_1\dots n_{k-1}) + p^k(n_0n_1\dots n_{k-1}) + p^{2k}(n_0n_1\dots n_{k-1}) + \dots) \\ &= (n_0n_1\dots n_{k-1})(1 + p^k + p^{2k} + \dots) \\ &= \frac{n_0n_1\dots n_{k-1}}{1-p^k}. \end{aligned} \tag{7.1.1}$$

The numerator of (7.1.1) is the p-adic expansion of a positive integer between 1 and p^{k-1} and is not 0 since $n \neq 0$. We are dividing it by $-(p^k-1)$ so the purely periodic expansion $\overline{n_0n_1\dots n_{k-1}}$ is a rational number lying in the interval $[-1,0)$.

Conversely, let r be a rational number with p-adic absolute value 1 that lies in the interval $[-1,0)$. We will show r has the form (7.1.1) and then the calculations that led to (7.1.1) can be read in reverse to see r has a purely periodic p-adic expansion.

Since $|r|_p = 1$ and $r < 0$ we can write $r = \dfrac{a}{b}$ with numerator $a < 0$ and denominator $b \geq 1$ that are both not divisible by p. Since p and b are relatively prime, from elementary number theory we have $p^k \equiv 1 (\mathrm{mod}\ b)$ for some $k \geq 1$. Thus $p^k = 1 + bc$ for some positive integer c. So,

$$r = \frac{a}{b} = \frac{ac}{bc} = \frac{-ac}{1-p^k}$$

Put $N = -ac$. Since $a < 0$ then $N \in \mathbb{N}$. From $-1 \leq r < 0$ we get $-1 \leq \dfrac{N}{1-p^k} < 0$, so $0 < N \leq p^k - 1$. Thus the p-adic expansion of N has at most k digits or

$$N = n_0 + n_1p + n_2p^2 + \dots + n_{k-1}p^{k-1}$$

where the digits n_i are between 0 and $p-1$. Hence $r = \dfrac{N}{1-p^k}$ has the form (7.1.1). Since a and c are not divisible by p, $|N|_p = |-ac|_p = 1$ so $n_0 \neq 0$. □

We can now find the p-adic expansions of rationals in the interval $[-1,0)$.

7.2 Examples

Notation 4. *If we write a p-adic number as* 20011 *we need to state the value of p. Hence we add that value as a subscript. For example,*

$$20011_3 = 2\cdot 3^0 + 0\cdot 3^1 + 0\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4$$

7.2.1 p-adic expansion of negative rationals in $[-1,0)$

We start with $-\dfrac{5}{11}$ with $p = 3$. Its 3-adic absolute value $\left|-\dfrac{5}{11}\right|_3 = 1$.
From the proof of Theorem 4 if a rational number r lying in the interval $[-1,0)$ has

the form $r = \frac{a}{b}$ then there is a k for which $p^k \equiv 1 (\bmod\ b)$. So we solve $3^k \equiv 1 (\bmod\ 11)$ to find $k = 5$ and then $3^5 - 1 = 11 \cdot 22$, so we have,

$$-\frac{5}{11} = -\frac{5}{11} \cdot \frac{22}{22} = \frac{110}{1-3^5}$$

Now $110 = 2 \cdot 3^0 + 0 \cdot 3^1 + 0 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 + \ldots = 20011_3$ so, by reversing (7.1.1) of the theorem,

$$-\frac{5}{11} = \frac{20011_3}{1-3^5} = \overline{20011}$$

7.2.2 p-adic expansion of positive rationals in $(0, 1]$

We can find the p-adic expansion of $r = \frac{a}{b} \in (0, 1]$ by negating the expansion of $\frac{a}{b} \in [-1, 0)$. Consider $\frac{2}{5}$ and $p = 3$.
We solve $3^k \equiv 1 (\bmod\ 3)$ to find $k = 4$. Then $3^4 - 1 = 80 = 5 \cdot 16$. So,

$$-\frac{2}{5} = -\frac{2}{5} \cdot \frac{16}{16} = \frac{32}{1-3^4} = \frac{2101_3}{1-3^4} = \overline{2101}_3$$

Then we negate using $-x = (p - a_0)p^0 + (p - a_1 - 1)p^1 + \ldots$ as we found in Section 6.3 to find

$$\frac{2}{5} = 1 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + 1 \cdot 3^3 + 0 \cdot 3^4 + \ldots = \overline{11210}_3$$

7.2.3 p-adic expansion of all rationals

We can find the p-adic expansion of rationals $r \notin [-1, 0)$ by separating off an integer, doing the calculation for an $r \in [-1, 0)$ and then adding back in the p-adic expansion of the integer.
Consider $r = \frac{18}{5} = 4 - \frac{2}{5}$ where $p = 3$. We have from the previous example,

$$-\frac{2}{5} = \overline{2101}_3 \text{ and we also have,}$$
$$4 = 1 \cdot 3^0 + 1 \cdot 3^1 = 11_3$$
$$\text{Thus, } 4 - \frac{2}{5} = 21012101\ldots$$
$$+\ \underline{11}$$
$$\Rightarrow \frac{18}{5} = 0011\overline{2101}_3$$

7.2.4 Case: p divides the denominator

Consider $r = \frac{79}{18}$ and $p = 3$.
Now $r = \frac{79}{18} = 5 - \frac{11}{18}$ so we find the 3-adic expansion of $-\frac{11}{18}$ and add $5 = 2 \cdot 3^0 + 1 \cdot 3^1$.

But $3|18$ so we cannot solve $3^k \equiv 1 (\text{mod } 3)$ for k.
We write,

$$-\frac{11}{18} = \frac{1}{9}\left(-\frac{11}{2}\right) = \frac{1}{9}\cdot\left(-5-\frac{1}{2}\right)$$

We proceed as follows.

(1) Find the 3-adic expansion of $-\frac{1}{2}$.

$$\begin{aligned} -\frac{1}{2} &= 2^{-1}(-1) \\ &= 2^{-1}(2\cdot 3^0 + 2\cdot 3^1 + 2\cdot 3^2 + \ldots) \\ &= 1 + 1\cdot 3^1 + 1\cdot 3^2 + 1\cdot 3^3 + \ldots \end{aligned}$$

(2) Find the 3-adic expansion of -5.

$$\begin{aligned} -5 = 5(-1) &= 5(2\cdot 3^0 + 2\cdot 3^1 + 2\cdot 3^2 + \ldots) \\ &= 10\cdot 3^0 + 10\cdot 3^1 + 10\cdot 3^2 + 10\cdot 3^3 + \ldots \\ &= (1+3^2)(1.3^0 + 1\cdot 3^1 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + 1\cdot 3^5 + \ldots \\ &= 1.3^0 + 1\cdot 3^1 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + 1\cdot 3^5 + \ldots \\ &\qquad + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + 1\cdot 3^5 + \ldots \\ &= 1\cdot 3^0 + 1\cdot 3^1 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + \ldots \end{aligned}$$

(3) Calculate 3-adic expansion of $-5-\frac{1}{2}$

$$\begin{aligned} -\frac{1}{2} &= 1 + 1\cdot 3^1 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + \ldots \\ \underline{-5} &= 1\cdot 3^0 + 1\cdot 3^1 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + \ldots \\ -5-\frac{1}{2} &= 2\cdot 3^0 + 2\cdot 3^1 + 0\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + \ldots \end{aligned}$$

(4) Multiply last result by $\frac{1}{9} = 3^{-2}$

$$\begin{aligned} \frac{1}{9}\left(-5-\frac{1}{2}\right) &= 3^{-2}(2\cdot 3^0 + 2\cdot 3^1 + 0\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + \ldots) \\ &= 2\cdot 3^{-2} + 2\cdot 3^{-1} + 0\cdot 3^0 + 1\cdot 3^1 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + \ldots \end{aligned}$$

(5) Add $5 = 2\cdot 3^0 + 1.3^1$ to previous result.

$$\begin{aligned} \frac{79}{18} &= 2\cdot 3^{-2} + 2\cdot 3^{-1} + 0\cdot 3^0 + 1\cdot 3^1 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + \ldots \\ &\qquad + 2\cdot 3^0 + 1\cdot 3^1 \\ &= 2\cdot 3^{-2} + 2\cdot 3^{-1} + 2\cdot 3^0 + 2\cdot 3^1 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 \\ &= 22.22\overline{1}\ldots \end{aligned}$$

Chapter 8

Hensel's Lemma

We study the solutions modulus p of polynomial equations $f(x) = \sum_{j=0}^{n} c_j x^j = 0,\ c_j \in \mathbb{Z}$, where $f(x)$ has derivative $f'(x) = \sum_{j=1}^{n} j c_j x^{j-1}$.

Lemma 9. *(Hensel)*
Given a prime p and a polynomial $f(x)$ with integer coefficients, if a is a solution to

$$f(x) \equiv 0 (\text{mod } p^{n-1}),\ n \geq 2$$

then if $gcd(p, f'(a)) = 1$, there is a solution to

$$f(x) \equiv 0 (\text{mod } p^n)$$

of the form $b = a + kp^{n-1}$ where k satisfies,

$$\frac{f(a)}{p^{n-1}} + kf'(a) \equiv 0 (\text{mod } p)$$

Proof. We need to show there is a $b = a + kp^{n-1}$ such that $f(b) \equiv 0 (\text{mod } p^n)$ where k satisfies,

$$\frac{f(a)}{p^{n-1}} + kf'(a) \equiv 0 (\text{mod } p)$$

Since $f(a) \equiv 0 (\text{mod } p^{n-1})$ then $p^{n-1} | f(a)$ so $\frac{f(a)}{p^{n-1}} \in \mathbb{Z}$.
Consider the linear congruence,

$$f'(a)y \equiv -\frac{f(a)}{p^{n-1}} (\text{mod } p)$$

Since $gcd(f'(a), p) = 1$, this has a unique solution for y which we shall call k. Then,

$$f'(a)k \equiv -\frac{f(a)}{p^{n-1}} (\text{mod } p)$$

We have,

$$f(a) \equiv 0 (\text{mod } p^{n-1}) \text{ (given).} \tag{8.0.1}$$

$$f'(a)k \equiv -\frac{f(a)}{p^{n-1}} (\text{mod } p) \tag{8.0.2}$$

Let $b = a + kp^{n-1}$ and $f(x) = \sum_{i=0}^{n} c_i x^i$, so $f'(x) = \sum_{i=1}^{n} i c_i x^{i-1}$. Then,

$$\begin{aligned} f(b) &= f(a + kp^{n-1}) \\ &= \sum_{i=0}^{n} c_i (a + kp^{n-1})^i \\ &= \sum_{i=0}^{n} c_i (a^i + ia^{i-1}kp^{n-1} + \binom{i}{2} a^{i-2}k^2 p^{2(n-1)} + \ldots) \end{aligned}$$

where we used the binomial theorem. Now all the remaining terms as well as the one in a^{i-2} are $0 (\text{mod } p^n)$, giving,

$$f(b) \equiv \sum_{i=0}^{n} c_i a^i + kp^{n-1} \sum_{i=1}^{n} i a^{i-1} \ (\text{mod } p^n) \tag{8.0.3}$$

$$\Rightarrow f(b) \equiv f(a) + kp^{n-1} f'(a) (\text{mod } p^n) \tag{8.0.4}$$

By Equation (8.0.2),

$$\begin{aligned} kf'(a) &\equiv -\frac{f(a)}{p^{n-1}} (\text{mod } p) \\ \Rightarrow p^{n-1}(kf'(a)) &\equiv -f(a) (\text{mod } p^n), \text{ so by equation (8.0.4),} \\ f(b) &\equiv f(a) - f(a) (\text{mod } p^n) \text{ giving} \\ f(b) &\equiv 0 (\text{mod } p^n) \end{aligned}$$

□

An equivalent statement of the Lemma is easily obtained from the above. The statement

$$f(a) \equiv 0 (\text{mod } p^{n-1}) \Rightarrow \text{there is a } b \text{ such that } f(b) \equiv 0 (\text{mod } p^n)$$

gives,

$$\begin{aligned} &f(a_0) \equiv 0 (\text{mod } p) \Rightarrow \text{ there is an } a_1 \text{ such that } f(a_1) \equiv 0 (\text{mod } p^2) \\ &f(a_2) \equiv 0 (\text{mod } p^2) \Rightarrow \text{ there is an } a_2 \text{ such that } f(a_2) \equiv 0 (\text{mod } p^3) \\ &\text{etc.} \end{aligned}$$

So we have a sequence $\{a_n\}$ such that $f(a_n) \equiv 0 (\text{mod } p^{n+1})$.
Also, $b = a + kp^{n-1} \Rightarrow b \equiv a (\text{mod } p^{n-1})$ identifies the sequence as $a_{n+1} \equiv a_n (\text{mod } p^{n+1})$.

We can therefore restate the theorem as:
Given a polynomial $f(x)$ with integer coefficients and,

$$f(a) \equiv 0 (\text{mod } p) \text{ and } f'(a) \not\equiv 0 (\text{mod } p),$$

were $a \in \mathbb{Z}$ and p is a prime number, then we have solutions mod p^{n+1} for all $n \geq 0$, namely,

$$f(a_n) \equiv 0 (\text{mod } p^{n+1}) \tag{8.0.5}$$
$$a_{n+1} \equiv a_n (\text{mod } p^{n+1}) \tag{8.0.6}$$

In other words we have a sequence $\{a_n\} = \{a_0 = a, a_1, a_2, \ldots\}$ with each element of the sequence unique mod p^{n+1}.

Example 8. *Consider the polynomial $f(x) = x^2 + 1$ which has integer coefficients. It has two solutions $2, 3 (\text{mod } 5)$ that is $f(2) \equiv 4 + 1 (\text{mod } 5) \equiv 0 (\text{mod} 5)$ and similarly, $f(3) \equiv 0 (\text{mod} 5)$. Further $f'(x) = 2x$ so neither $f'(2) = 4$ nor $f'(3) = 6$ are divisible by 5. Then we can apply Hensel's Lemma.*
Take $a = 2$. Then we can start our sequence thus: $(a = 2, a_1, a_2, \ldots)$
Now, by (8.0.6) $a_1 \equiv 2 (\text{mod } 5) \Rightarrow a_1 = 2 + 5t$. Then, $f(2 + 5t) = (2 + 5t)^2 + 1$, gives,

$$\begin{aligned} 4 + 20t + 5^2 t + 1 &\equiv 0 (\text{mod } 5^2) \text{ by (8.0.5)} \\ \Rightarrow 5 + 20t &\equiv 0 (\text{mod } 5^2) \\ \Rightarrow t &= 1 \\ \Rightarrow a_1 &= 2 + 5 \cdot 1 = 7 \end{aligned}$$

We repeat the cycle.

$$\begin{aligned} a_2 &\equiv a_1 (\text{mod } 5^2) \text{ by (8.0.6)} \\ \Rightarrow a_2 &= 7 + 25t \\ \Rightarrow f(a_2) &= (7 + 25t)^2 + 1 \equiv 0 (\text{mod } 5^3) \text{ by (8.0.5)} \\ \Rightarrow t &= 2 \\ \Rightarrow a_2 &= 7 + 25 \cdot 2 = 57 \end{aligned}$$

We can continue in this way for as long as we like. We have the sequence beginning $(2, 7, 57, \ldots)$. But,

$$\begin{aligned} 2 &= 2 \\ 7 &= 2 + 1 \cdot 5^1 \\ 57 &= 2 + 1 \cdot 5 + 2 \cdot 5^2 \end{aligned}$$

The roots of $f(x) = x^2 + 1 = 0$ are $\pm\sqrt{-1} = \pm i$. We have produced the 5-adic expansion of

$$\sqrt{-1} = 2 + 1 \cdot 5^1 + 2 \cdot 5^2 + \ldots.$$

Note that any element of the sequence of partial sums of this expansion is a root of $f(x) = x^2 + 1$ *modulo 5.*
We could repeat the above analysis for $a = 3$ *and that would give us the* 5*-adic expansion of* $-\sqrt{-1} = -i$.

We begin to see the power of Hensel's Lemma. Provided we have an a such that $f(a) \equiv 0 (\text{mod } p)$ for a polynomial $f(x)$ with integer coefficients and provided the value of the derivative $f'(a) \not\equiv 0 (\text{mod } p)$ then we can produce an infinite number of other roots and their sequence will be the partial sums of the p-adic expansion of the root or roots of the equation. Let's do another example,

Example 9. *Consider* $f(x) = x^2 - 2$, *which has two solutions* $\pm 3 (\text{mod } 7)$.
We note $f'(x) = 2x$ *so both 3 and -3 satisfy* $f'(a) \not\equiv 0 (\text{mod } 7)$.
One sequence starts $(3, a_1, a_2, \ldots)$. *Now* $a_1 \equiv 3 (\text{mod } 7) \Rightarrow a_1 = 3 + 7t$. *Then, using (8.0.5) and (8.0.6),*

$$\begin{aligned} (3+7t)^2 - 2 &\equiv 0 (\text{mod} 7^2) \\ \Rightarrow t &= 1 \\ \Rightarrow a_1 &= 3 + 7 \cdot 1 = 10 \\ \Rightarrow a_2 &\equiv a_1 (\text{mod} 7^2) \\ \Rightarrow a_2 &= 10 + 49t \\ \Rightarrow (10+49t)^2 - 2 &\equiv 0 (\text{mod } 7^3) \\ \Rightarrow t &= 2) \\ \Rightarrow a_2 &= 10 + 49 \cdot 2 = 108 \end{aligned}$$

This sequence is $(3, 10, 108, \cdots)$ *and we have the partial sums,*

$$\begin{aligned} a &= 3 \\ a_1 &= 10 = 3 + 1 \cdot 7 \\ a_2 &= 108 = 3 + 1 \cdot 7 + 2 \cdot 7^2 \end{aligned}$$

giving the 7*-adic expansion of* $\sqrt{2}$ *as,*

$$\sqrt{2} = 3 + 1 \cdot 7 + 2 \cdot 7^2 + \ldots .$$

Example 10. *Consider* $f(x) = 2x + 1$, *with* $p = 3$.
Then $f(1) \equiv 3 (\text{mod } 3) = 0$.
We note $f'(x) = 2$ *so 1 satisfies* $f'(a) \not\equiv 0 (\text{mod } 3)$.
The sequence starts $(1, a_1, a_2, \ldots)$. *Now* $a_1 \equiv 1 (\text{mod } 3) \Rightarrow a_1 = 1 + 3t$. *Then, using*

(8.0.5) and (8.0.6),

$$\begin{aligned} 2(1+3t)+1 &\equiv 0(\text{mod } 3^2) \\ \Rightarrow t &= 1 \\ \Rightarrow a_1 &= 1+3\cdot 1 = 4. \\ \Rightarrow a_2 &\equiv a_1(\text{mod } 3^2) \\ \Rightarrow a_2 &= 4+9t \\ \Rightarrow 2(4+9t)+1 &\equiv 0(\text{mod } 3^3) \\ \Rightarrow t &= 1 \\ \Rightarrow a_2 &= 4+9\cdot 1 = 13 \end{aligned}$$

This sequence is $(1, 4, 13, \cdots)$ *and we have the partial sums,*

$$\begin{aligned} a &= 1 \\ a_1 &= 4 = 1+1\cdot 3 \\ a_2 &= 13 = 1+1\cdot 3+1\cdot 3^2 \end{aligned}$$

giving the 3*-adic expansion of* $-\frac{1}{2}$ *as,*

$$-\frac{1}{2} = 1+1\cdot 3+1\cdot 3^2+\ldots.$$

Example 11. *Solve* $x^2+3x+17 \equiv 0(\text{mod } 315)$.
Note $315 = 3^2\cdot 5\cdot 7$.
We choose the highest power of the prime factors of 315 and proceed as follows to solve $x^2+3x+17 \equiv 0(\text{mod } 9)$.
Now Hensel's Lemma gives us "lifts" from solutions of such equivalences at modulus p^{n-1} *to solutions modulus* p^n.
So we first consider,

$$\begin{aligned} x^2+3x+17 &\equiv 0(\text{mod } 3) \\ \Rightarrow x^2+2 &\equiv 0(\text{mod } 3) \\ \Rightarrow x_0 &= 1,\ x_0 = 2. \end{aligned}$$

We start with $x_0 = 1$ *and check* $f'(x) = 2x+3 \Rightarrow f'(1) = 5$ *so* $gcd(3,5) = 1$.
Again using (8.0.5) and (8.0.6), we solve,

$$\begin{aligned} kf'(1) &\equiv -\frac{f(1)}{3}(\text{mod } 3) \\ 5k &\equiv -7(\text{mod } 3) \\ 5k &\equiv 2(\text{mod } 3) \\ k &= 1 \\ x &= x_0+3k = 4 \end{aligned}$$

So $x = 4$ *is one solution to* $x^2 + 3x + 17 \equiv 0 (\text{mod } 9)$.
Now we put $x_0 = 2$, *the other solution to* $x^2 + 3x + 17 \equiv 0 (\text{mod } 3)$, *and repeat the "lifting" process.*
We check $gcd(3, f'(2)) = 1$ *is true and then solve,*

$$\begin{aligned} kf'(2) &\equiv -\frac{f(2)}{3} (\text{mod } 3) \\ 7k &\equiv -\frac{27}{3} (\text{mod } 3) \\ k &= 0 \end{aligned}$$

so $x = x_0 + 3k = 2$.
We do not need to continue the lifting process but if, say, instead of a factor of 3^2 *we had a factor of* 3^3 *then we would perform another "lift". We move on to the factors 5 and 7.*

$$\begin{aligned} & x^2 + 3x + 17 \equiv 0 (\text{mod } 5) \\ \Rightarrow\ & x^2 + 3x + 2 \equiv 0 (\text{mod } 5) \\ \Rightarrow\ & x = 3, 4 \\ & \textit{and} \\ & x^2 + 3x + 17 \equiv 0 (\text{mod } 7) \\ \Rightarrow\ & x^2 + 3x + 3 \equiv 0 (\text{mod } 7) \\ \Rightarrow\ & x = 1, 3 \end{aligned}$$

We need to solve the 8 combinations of,

$$x \equiv 2, 3 (\text{mod } 9),\ x \equiv 3, 4 (\text{mod } 5),\ x \equiv 1, 3 (\text{mod } 7).$$

We use the Chinese Remainder Theorem which shows us how to solve systems of linear congruences.

Theorem 10. *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 infinite number of solutions is given by,

$$x_0 = \left(\frac{m}{m_1}\right) b_1 a_1 + \left(\frac{m}{m_2}\right) b_2 a_2 + \ldots + \left(\frac{m}{m_r}\right) b_r a_r$$

where each b_i *is the solution of the linear congruence*

$$\left(\frac{m}{m_i}\right) b_i \equiv 1 (\text{mod } m_i)$$

Let's just solve $x \equiv 2(\text{mod } 9),\ x \equiv 3(\text{mod}5),\ x \equiv 1(\text{mod}7)$ *and leave the rest to you! We also leave to you finding the other values of* b_i *by inspection. The first one for* $\left(\frac{m}{m_1}\right) b_1 \equiv 1(\text{mod } m_1)$ *is,*

$$\begin{aligned} 35b_1 &\equiv 1(\text{mod } 9) \\ 8b_1 &\equiv 1(\text{mod } 9) \\ b_1 &= 8 \end{aligned}$$

Using the notation of the theorem,

$$\begin{aligned} m &= 315, m_1 = 9, m_2 = 5, m_3 = 9 \\ \frac{m}{m_1} &= 35, \frac{m}{m_2} = 63, \frac{m}{m_3} = 45, m = 315 \\ a_1 &= 2, a_2 = 3, a_3 = 1 \\ b_1 &= 8, b_2 = 2, b_3 = 5 \\ x_0 &= \sum_{i=1}^{3} \frac{m}{m_i} b_i a_i \\ x_0 &\equiv 8 \cdot 35 \cdot 2 + 2 \cdot 63 \cdot 3 + 5 \cdot 45 \cdot 7 (\text{mod } 315) \\ &\equiv 1163(\text{mod } 315) \\ &\equiv 218(\text{mod}315) \end{aligned}$$

Other solutions are 29, 38, 94, 148, 274, 283, all mod 315.
For instance with x=29,

$$x^2 + 3x + 17 = 29^2 + 3 \cdot 29 + 17 = 945 = 3 \cdot 315 \equiv 0(\text{mod } 315)$$