The p-adic Numbers

Author: Eiseart Dunne
Supervisor: Dr. David R. Wilkins
Date: 18/03/2011

Contents

1 Abstract

The goal of this project is to develop a background in the study of Hensel's p-adic numbers, including a discussion of non-Archimedean valuations, completion fields, Hensel's lemma, the topology of the p-adic numbers (and the Cantor set) and algebraic number theory. I intend to accurately convey the major ideas that I encounter in these fields in a readable way. The project also led me to develop two algorithms, implemented in Perl for applying Hensel's lemma to obtain sequences converging to the roots of arbitrary polynomials in the p-adic completion of $\mathbb{Q}$, the rational numbers, and $\mathbb{Q}(i)$, the Gaussian rationals. The content assumes a basic background in topology, metric analysis, commutative algebra and elementary number theory.

2 Introduction

"*God gave us the integers, all else is the work of man*"

- Leopold Kronecker

Logically, the journey between $\mathbb{N}$ and $\mathbb{C}$ has its roots in two primary motivations, one of which is algebraic and one of which is analytic or topological. These are:

i) Finding a superset that contain the roots of polynomials $\sum_{i=0}^{n} a_i x^i$.

ii) Finding a superset that contains the limits of Cauchy sequences $\{c_i\}_{i=1}^{\infty}$ with respect to the usual metric on

$\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$: $d(x,y) = |x-y|$ where $|x| = \left\{ \begin{array}{ll} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{array} \right\}$.

$\mathbb{Z}$ is built from $\mathbb{N}$ by considering the roots of simple polynomials of the form $x + a = 0$, $a \in \mathbb{N}$ and $\mathbb{Q}$ is obtained from $\mathbb{Z}$ by considering further roots of polynomials of the form $ax = b$, $a \neq 0, b \in \mathbb{Z}$. These steps are both algebraic, dealing with the operations of + and × that we may define on real and complex numbers and the roots of polynomials that can be built using both of these operations. We may travel further along the road to $\mathbb{R}$ through closing $\mathbb{Q}$ algebraically by adding, say, $\sqrt{2}$ which is the root of the polynomial $x^2 - 2$ and others like it. However, continuing in this manner still excludes transcendental numbers like π or e, for example, and there is a quicker way to add all irrational numbers to our set in one fell swoop, by moving to the analytic side of things. Using the notion of distance and convergence, we can add exotic, new elements to our set, that cannot be obtained algebraically, but by including objects to which the numbers in our previous set could become incredibly *close*. The superset of $\mathbb{Q}$ containing these elements happens to be the *complete* $\mathbb{R}$ (in fact, $\mathbb{Q}$ is said to be *dense* in $\mathbb{R}$). Finally, we may close $\mathbb{R}$ using the root of the polynomial $x^2 + 1 = 0$, creating $\mathbb{C}$, a set that is perfect in both algebraic and analytic terms, something both *algebraically closed* and *complete*.

Returning to when we had $\mathbb{Q}$, however, there is a subtle bifurcation in the journey from $\mathbb{N}$ to a complete, algebraically closed set. This bifurcation (and it is strictly a *bi*furcation as will be shown by way of *Ostrowski's theorem*) stems from the consideration that the notion of distance is arbitrary. Distance, in fact, can be defined in disparate ways. For example, the distance $d'(x,y) = |x-y|^2$ satisfies the same essential axioms of the previous one. This distance, however, differs from the original in such a trivial manner that completing $\mathbb{Q}$ with this distance leads to the same general result in the above process.

Towards the end of the 19th century Kurt Hensel formulated the p-adic numbers, a completion of the rational numbers with respect to a non-Euclidean metric, the topology of which departed from the previous in a non-trivial way. His discovery led to the development of valuation theory for fields and the p-adic numbers have become a tool for studying algebraic numbers over the rationals. This project is intended to provide a linear, intuitive introduction to the p-adic numbers. It draws on four texts: Andrew Baker's *An Introduction to p-adic Numbers and p-adic Analysis* [1], Borevič and Shafarevič's *Number Theory* [2], Neal Koblitz's *p-adic*

Numbers, p-adic Analysis and Zeta-Functions [3], Fernando Q. Gouvêa's *p-adic Numbers: An Introduction* [4] and William Stein's *Algebraic Number Theory, a Computational Approach* [5] in no particular order, except that which allowed me to develop my own thread of theory. The content is mostly expository insofar as that I prove few things that have not been mentioned in one of the texts - however I ensured that I personalised all the proofs of relevant theorems, for myself as much as for the sake of the project.

3 The p-adic Valuation and Metric

First, we recall some important definitions regarding analysis.

Definition: A nonempty set X together with a function $d : X \times X \to \mathbb{R}$ is called a metric space if the function d satisfies the following:

(i) $d(x,y) = 0 \Leftrightarrow x = y$, $\forall\ x,\ y \in X$.

(ii) $d(x,y) \geq 0$, $\forall\ x,\ y \in X$.

(iii) $d(x,y) = d(y,x)$, $\forall\ x,\ y \in X$.

(iv) $d(x,z) \leq d(x,y) + d(y,z)$, $\forall\ x,\ y,\ z \in X$.

We refer to d as the *metric* or *distance* defined on the set X.

Example: The Euclidean metric, $d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$, $x, y \in \mathbb{R}^n$, is an example of a metric.

Definition: A *valuation* (sometimes called a *norm*) on a field k is a mapping $v : k \to \mathbb{R}$ satisfying:

(i) $v(x) \geq 0$, $\forall x \in k$.

(ii) $v(x) = 0$ iff $x = 0$.

(iii) $v(xy) = v(x)v(y)$, $\forall x, y \in k$.

(iv) $v(x+y) \leq v(x) + v(y)$, $\forall x, y \in k$.

A direct consequence of (iii) is that $v(1) = v(-1) = 1$.

Example: The *trivial absolute value* v_1 on any field k is such that $v_1(0) = 0$ and $v_1(x) = 1$, $\forall x \neq 0 \in k$.

Theorem: Let X be a field on which a valuation v is defined. Then v gives rise to a metric $d(x,y) = v(x-y)$, $\forall\ x, y \in X$.

Proof: We must check each of the axioms of a metric. Firstly,

$$\begin{aligned} & d(x,y) = 0 \\ \iff & v(x-y) = 0 \\ \iff & x - y = 0 \\ \iff & x = y \end{aligned}$$

and so axiom (i) defining a metric is satisfied. Axiom (ii) defining a metric follows trivially from axiom (i) of a valuation. The symmetry condition follows from property (iii) of valuations since $v(-1) = 1$.

Finally,

$$\begin{aligned} d(x,z) &= v(x-z) \\ &= v(x-y+y-z) \\ &\leq v(x-y) + v(y-z) \\ &= d(x,y) + d(y,z) \end{aligned}$$

showing that the triangle inequality is satisfied. □

Definition: A *Cauchy sequence* in a metric space is a sequence $(x_n)_{n=1}^{\infty}$ such that, given any $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ with $d(x_{n_1}, x_{n_2}) < \varepsilon$ for all $n_1, n_2 > N$. The limit of a Cauchy sequence $(x_n)_{n=1}^{\infty}$ in a metric space is the unique point L: given any $\varepsilon > 0$, there exists an $N \in \mathbb{N}$ with $d(x_i, L) < \varepsilon$ for all $i > N$. Two Cauchy sequences, $(x_n)_{n=0}^{\infty}$ and $(y_n)_{n=0}^{\infty}$ are said to be equivalent if $\lim_{n\to\infty} d(x_n, y_n) = 0$.

A *complete* metric space is one in which every Cauchy sequence of points in the space converges to a limit in the space.

Definition: If (X,d) is a metric space and X' is a complete (with respect d) space containing X, the *completion* X^c of X is the intersection of all complete subspaces of X' containing X.

Example: Consider $\mathbb{R}\backslash\{0\}$ with the standard Euclidean metric. The sequence $(\frac{1}{n})_{n=1}^{\infty}$ is a Cauchy sequence that converges to a limit not contained in the space, namely 0. The completion of $\mathbb{R}\backslash\{0\}$ is $\mathbb{R}$.

Definition: Given any prime number p and integer z, let $\mathrm{ord}_p(z)$ be the highest power of p such that $p \mid z$. For any rational $q = \frac{a}{b}$, $a, b \in \mathbb{Z}$, let $\mathrm{ord}_p(q) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$.

Example: $\mathrm{ord}_7(98) = 2$ as 98 factors to 2.7^2.

Definition: The *p-adic norm* (or valuation) of a rational number x is

$$|x|_p = \begin{cases} 1/p^{\mathrm{ord}_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

This defines a valuation on the rational numbers as it clearly satisfies properties (i) and (ii) of valuations since p is positive. To prove property (iii), suppose $x, y \in \mathbb{Q}$. Then we may express

$$x = \frac{p^a m}{n},\ y = \frac{p^b r}{s}$$

for any prime p with $p \nmid r, s, m, n \in \mathbb{Z}$ (by the Fundamental Theorem of Arithmetic). Then $xy = \frac{p^{a+b}mr}{ns}$ and $p \nmid mr, ns$ (by the definition of a prime) and $|xy|_p = p^{-(a+b)} = |x|_p |y|_p$. So the property holds.

Assuming, without loss of generality, $a \leq b$, then

$$|x+y|_p = \left| \frac{p^a(sm + p^{b-a}nr)}{ns} \right|_p$$

and this must be less than $|x|_p$ as $(sm+p^{b-a}nr)$ factors as $(p^i)(v)$ for some $v \in \mathbb{Z}$, $i \in \mathbb{N}$. Then $p^{(i+a)} || \frac{p^a(sm+p^{b-a}nr)}{ns}$ implying that

$$|x|_p = p^{-a} \geq p^{-(i+a)} = |x+y|_p$$

so

$$|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$$

proving the property (iv) above.

Since every valuation induces an associated metric, the metric $d_p(x,y) = |x-y|_p$ is well-defined and will be referred to as the p-adic metric. This metric is also called *non-Archimedean* because is satisfies

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}$$

as shown above. This condition is stronger than the Triangle Inequality and gives rise to several strange phenomena.

3.1 Non-Archimedean Metric Spaces

An open ball with respect to a non-Archimedean metric has every point at its centre because

$$\begin{aligned} x, y \in B(z,\varepsilon) &\implies d(x,z) < \varepsilon \\ &\implies d(x,y) \leq \max(d(x,z), d(z,y)) < \varepsilon \\ &\implies x \in B(y,\varepsilon) \end{aligned}$$

Every triangle in a metric space under a non-Archimedean metric is isoceles. Suppose we have a triangle defined by points a, b and c. Then $d(a,b) \leq \max(d(a,c) + d(c,b))$. Now suppose that $d(a,c) < d(b,c)$. Then $d(a,b) \leq d(c,b)$. But $d(c,b) \leq \max\{d(a,c), d(b,a)\}$ and $d(c,b) > d(a,c)$ so $d(b,c) \leq d(b,a) \implies d(a,c) = d(b,a)$.

Corollary: Let $|.|_\alpha$ be a non-Archimedean valuation on a field k. If $x = y + z$ with $|z|_\alpha < |y|_\alpha$, then $|x|_\alpha = |y|_\alpha$.

Under the p-adic metric, open balls are vastly alien to the intuitive Euclidean open balls. The open ball of radius 1 about 0 with respect to the p-adic metric is the set

$$B_p(0,1) = \{x \in \mathbb{Q} : d_p(x,0) < 1\} = \{x \in \mathbb{Q} : |x|_p < 1\}$$

which is precisely the set

$$\{x \in \mathbb{Q} : x = \frac{p^n a}{b} \text{ with } p \nmid a, b \text{ and } n > 0\}$$

or the set of all $x \in \mathbb{Q}$ such that p divides the numerator of x more times than the denominator. Unlike the Euclidean metric, the p-adic metric does not respect the usual linear order on $\mathbb{Q}$. For example, taking the 2-adic metric, we find that $2 \in B_2(0,1)$ as $|2|_2 = \frac{1}{2} < 1$ and $4 \in B_2(0,1)$ as $|4|_2 = \frac{1}{4} < 1$ but $3 \notin B_2(0,1)$, even though $2 < 3 < 4$.

3.2 Examples:

We determine: $|-\frac{128}{7}|_2$, $|-13.23|_3$, $|9!|_3$
(Andrew Baker[1] p. 56)

- $\frac{128}{7} = \frac{2^7}{7}$ so $|-\frac{128}{7}|_2 = 2^{-7} = \frac{1}{128}$
- $13.23 = 13 + \frac{23}{100} = \frac{1323}{100} = \frac{3^3.49}{100}$ so $|-13.23|_3 = 3^{-3} = \frac{1}{27}$
- $9! = 9.8.7.6.5.4.3.2 = 3^2.8.7.3.2.5.4.3.2 = 3^4.8.7.5.4.2$ so $|9!|_3 = 3^{-4} = \frac{1}{3^4}$

We show that for $0 \neq x \in \mathbb{Q}$,

$$\prod_p |x|_p = \frac{1}{|x|}$$

where the product is taken over all primes $p = 2, 3, 5, 7...$
(Andrew Baker p. 56)

- Since $0 \neq x \in \mathbb{Q}$ then $x = \frac{m}{n}$ with $m, n \in \mathbb{Z}$. Also, by the Fundamental Theorem of Arithmetic, $|m| = p_1^{e_1} p_2^{e_2} p_3^{e_3} ... p_r^{e_r}$ and $|n| = q_1^{f_1} q_2^{f_2} q_3^{f_3} ... q_s^{f_s}$ for some primes p_i, q_i and $e_i, f_i \in \mathbb{N}$ (note that $|-x|_p = |x|_p$ so multiplication by a unit is not important here). Then $|m|_{p_i} = p_i^{-e_i}$ and $|\frac{1}{n}|_{q_i} = q_i^{f_i}$, and $|m|_p = 1$ for $p \notin \{p_1, p_2, ..., p_r\}$ and $|\frac{1}{n}|_p = 1$ for $p \notin \{q_1, q_2, ..., q_s\}$. But since $|m\frac{1}{n}|_p = |m|_p |\frac{1}{n}|_p$, then

$$\begin{aligned}
\prod_p |x|_p &= \prod_p |m|_p |\frac{1}{n}|_p \\
&= p_1^{-e_1} ... p_r^{-e_r} q_1^{f_1} ... q_s^{f_s} \\
&= \left|\frac{n}{m}\right| \\
&= \frac{1}{|x|}
\end{aligned}$$

as required.

If $x \in \mathbb{Q}$ and $|x|_p \leq 1$ for every prime p, we show that $x \in \mathbb{Z}$.
(Andrew Baker p. 56)

- Assume $x \in \mathbb{Q} \backslash \mathbb{Z}$. Then x can be expressed in the form $\frac{p_1^{e_1} ... p_r^{e_r}}{q_1^{f_1} ... q_s^{f_s}}$ with q_i, p_j prime, $e_i, f_j \in \mathbb{N}$ and $q_i \neq p_j \forall i, j$. Then for some prime p_0, we have $p_0 = q_i, 1 \leq i \leq s \Rightarrow |x|_{p_0} = p_0^{f_i}$. But since $f_i \in \mathbb{N}$, then $|x|_{p_0} = p_0^{f_i} > 1$. So $x \in \mathbb{Q} \backslash \mathbb{Z}$ cannot be true if $|x|_p \leq 1$ for all primes p. Therefore $|x|_p \leq 1$ for every prime $p \Rightarrow x \in \mathbb{Z}$.

4 Ostrowski's Theorem

Definition: Two valuations (or *absolute values*), v_a and v_b, on a field k are said to be *equivalent* if there exists a real number $c > 0$ such that $v_a(x) = (v_b(x))^c$ for all $x \in k$.

It is clear that equivalent valuations induce the same metric topology. For instance, assume that two valuations v_a and v_b defined on a field k are equivalent. Then for each $x \in k$, $v_a(x) = v_b(x)^c$ for a positive $c \in \mathbb{R}$. Any open ball $d_a(x, \varepsilon)$ in the "a-metric" is the same as the open ball $d_b(x, \varepsilon^{-c})$ in the "b-metric". As the metric topology on a set X is generated by unions and intersections of open balls, we conclude that v_a and v_b yield the same topology. The following important theorem by Ostrowski shows that there can only be two distinct

'types' of topologies on the rational numbers following from nontrivial valuations.

Theorem: (Ostrowski's Theorem) Every nontrivial valuation on $\mathbb{Q}$ is equivalent to the p-adic valuation or the usual absolute value.

Proof: It is sufficient to prove the result for each $n \in \mathbb{N}$ as the rest follows by the third property of absolute values. We also need not check $n = 1$ as the absolute value of 1 is 1 by the third property of the absolute value.

Lemma: (If $v_\tau : \mathbb{Q} \to \mathbb{R}$ is an absolute value and $v_\tau(n) > 1$ for some $n \in \mathbb{N}, > 1$, then v_τ is equivalent to the usual absolute value $|.| : \mathbb{Q} \to \mathbb{R}$).

Proof: Let $z > 1$ be a positive integer with $v_\tau(z) > 1$. Then

$$z = c_0 + c_1 n + c_2 n^2 + \ldots + c_m n^m$$

for some $n \in \mathbb{N}, > 1$, with $0 \leq c_i \leq n-1$, $c_m \neq 0$ and $m < \frac{\log(z)}{\log(n)}$. By the Triangle Inequality and the third property of absolute values,

$$v_\tau(z) \leq v_\tau(c_0) + \ldots + v_\tau(c^m) v_\tau(n^m)$$

and so

$$v_\tau(z) \leq (m+1)(n-1) v_\tau(n)^m$$

and also

$$v_\tau(z)^j \leq (mj+1)(n-1) v_\tau(n)^{mj}$$

similarly. Taking the jth root of the above, one has

$$v_\tau(z) \leq [(mj+1)(n-1)]^{1/j} v_\tau(n)^m$$

for all j and so letting $j \to \infty$ gives

$$v_\tau(z) \leq v_\tau(n)^m \leq v_\tau(n)^{\frac{\log(z)}{\log(n)}}$$

implying that $v_\tau(z)^{\frac{1}{\log z}} \leq v_\tau(n)^{\frac{1}{\log n}}$ and $v_\tau(n)^{\frac{1}{\log n}} \leq v_\tau(z)^{\frac{1}{\log z}}$ and the two are equal (since $v_\tau(n) > 1$). Since n was chosen arbitrarily we, in fact, have $v_\tau(z)^{\frac{1}{\log z}} = v_\tau(a)^{\frac{1}{\log a}}$, $\forall a \in \mathbb{N}$, with $a > 1$. Then $v_\tau(z)^{\frac{1}{\log z}} = c$ (with c some positive constant) $\Rightarrow v_\tau(z) = c^{\log(z)}$. There exists an $\alpha \in \mathbb{R}$ with $c^\alpha = e$ and so $v_\tau(z)^\alpha = c^{\alpha \log(z)} = e^{\log(z)} = |z|$. v_τ is equivalent to the usual absolute value on $\mathbb{Q}$. This completes the lemma. □

Lemma: (If $v_\tau : \mathbb{Q} \to \mathbb{R}$ is an absolute value and $v_\tau(n) \leq 1$ for all $n \in \mathbb{N}, > 1$, then v_τ is equivalent to the p-adic absolute value $|.|_p : \mathbb{Q} \to \mathbb{R}$).

Proof: Let $z \in \mathbb{N}, > 1$. We will assume that $v_\tau(z) < 1$. We can always find such a z since v_τ is nontrivial. Then, by the Fundamental Theorem of Arithmetic, $z = \prod_{i=1}^{r} p_i^{e_i}$ for distinct primes p_i and $e_i \in \mathbb{N}$. Also, $v_\tau(z) = \prod_{i=1}^{r} v_\tau(p_i^{e_i}) < 1 \Rightarrow \exists j$ such that $v_\tau(p_j) < 1$. Suppose $p_j \neq p_k$ with $v_\tau(p_k) < 1$. Then $\exists t \in \mathbb{N}$ such that $v_\tau(p_j)^t, v_\tau(p_k)^t < \frac{1}{2}$. Since $\gcd(p_j^t, p_k^t) = 1$, then the Euclidean algorithm ensures the existence of $m, n \in \mathbb{Z} : m p_j^t + n p_k^t = 1$. Then

$$1 \leq v_\tau(p_j)^t v_\tau(m) + v_\tau(p_k)^t v_\tau(n) < \frac{v_\tau(m) + v_\tau(n)}{2} < \frac{1+1}{2} = 1$$

which is impossible. So $v_\tau(p_i) = 1$ when $i \neq j \Rightarrow v_\tau(z) = v_\tau(p_j)^{e_j} < 1$. The map $f_c : \mathbb{R}^+ \to (0,1)$ with $f_c(x) = c^x$ for some constant $c \in (0,1)$ is surjective. Therefore, $\exists \alpha : (v_\tau(p_j)^{e_j})^\alpha = |z|_{p_j}$ and so v_τ is equivalent to the p_j-adic absolute value. This completes the lemma. □

It follows from the two lemmas that every nontrivial absolute value on the rational numbers is equivalent to the p-adic absolute value or the usual absolute value. □

5 $\mathbb{Q}_p$: The Completion of $\mathbb{Q}$ with respect to $|.|_p$

In the same way that $\mathbb{R}$ can be built from $\mathbb{Q}$ by adding to the former the limits of Cauchy sequences with elements in the space with respect to the standard metric, the p-adic metric has its own unique completion: $\mathbb{Q}_p$.

In concrete terms, sequences in $\mathbb{Q}$ that are Cauchy with respect to $|.|_p$ are ones that eventually have successive terms such that the last term is lesser than the next term by a large power of p.

Example: For some prime, p, take the simple sequence $(p^n)_{n=0}^{\infty}$. The distance $d_p(p^r, p^s)$ between two elements p^r and p^s of this sequence (with $r \leq s$) is $|p^r(1-p^{s-r})|_p = p^{-r}$. This sequence is Cauchy, since, given any $\varepsilon > 0$, we can find an $N \in \mathbb{N}$ such that $n_1, n_2 > N \Rightarrow d_p(p^{n_1}, p^{n_2}) < \varepsilon$. Certainly, we can find an N such that $0 < \frac{1}{N} < \varepsilon$. Then $n_1, n_2 > N \Rightarrow d_p(p^{n_1}, p^{n_2}) < \varepsilon$.

Example: Let p be any prime and $(x_n)_{n=0}^{\infty}$ be the sequence such that $x_n = n!$ for all $n \in \mathbb{N}$. Now, if $m \geq n$, then

$$|x_m - x_n|_p = |n![m(m-1)(m-2)...(n+1)-1]|_p$$

and for any prime p and any $k \in \mathbb{N}$, $p^k | n![m(m-1)(m-2)...(n+1)-1]$ for all $n \geq p^k$. Therefore $|x_m - x_n|_p < p^{-k}$ for large enough $m, n \in \mathbb{N}$ regardless of our choice of k. $(x_n)_{n=0}^{\infty}$ is Cauchy.

Representing irrational elements of $\mathbb{Q}_p$ in a lucid way is extremely challenging, as the elements themselves are not 'numbers' in the traditional sense, but limits of p-convergent rational sequences that diverge to infinity in the 'Euclidean' sense. Because of this, we can refer to the new elements appended to $\mathbb{Q}$ not in and of themselves, but equivalently by the sequences that converge to them. We may also say that two sequences, and thus, two elements of $\mathbb{Q}_p$, are equivalent and write $\{x_n\} \sim \{y_n\}$ if they both approach the same limit, (i.e $|x_n - y_n|_p \to 0$ as $n \to \infty$). This method of representation is consistent when applied to $\mathbb{Q}$ itself as, given any $x \in \mathbb{Q}$, we can let the sequence $(x_n)_{n=0}^{\infty} = x$, $\forall\ n \in \mathbb{N}$ refer to x, as this is Cauchy with x as its limit. More concretely, by way of the following theorem, we can describe each element of $\mathbb{Q}_p$ in a standard way.

5.1 The p-adic Integers: $\mathbb{Z}_p$

Theorem: (Canonical representation) For each equivalence class $\{a\} \in \mathbb{Q}_p$, with $|a|_p \leq 1$ we can find a unique representative Cauchy sequence composed of integers, (x_n), satisfying:

1. $0 \leq x_i \leq p^i$, for $i = 1, 2\ldots$
2. $x_{i+1} \equiv x_i \pmod{p^i}$ for $i = 1, 2\ldots$

Proof: First note that any such sequence must be unique. Assume not. Then there are two different Cauchy sequences $\{a_i\}$ and $\{b_i\}$ satisfying the above criteria. For some j, $a_j \neq b_j$ and then $a_j \not\equiv b_j \pmod{p^j}$ as each is less than p^j. By the second property, then, given any $k \geq j$, we have $a_k \equiv a_j \not\equiv b_j \equiv b_k \pmod{p^j}$. But then $\lim_{n\to\infty} a_n \neq \lim_{n\to\infty} b_n$ as $|a_n - b_n|_p > p^j$ for all $n \in \mathbb{N}$. Therefore $\{a_n\}$ must not be equivalent to $\{b_n\}$.
The proof of existence of a representative of the form stated in the theorem requires the use of the following lemma.

Lemma: Given any $x \in \mathbb{Q}$ with $|x|_p \leq 1$ we can find an integer $y \in [0,\ p^n - 1]$ such that $|x - y|_p \leq p^{-n}$ for any $n \in \mathbb{Z}$.

Proof: Let $x = \frac{a}{b}p^j$ with $\gcd(p, ab) = 1$ and $a, b \in \mathbb{Z}$. Certainly, $j \geq 0$ as $|x|_p \leq 1$. Now, b and p^k are coprime for every natural number k, so we can use Bézout's identity to express:

$$rp^n + sb = 1 \implies sb - 1 = rp^n$$

for some integers r and s. Now $sb \approx 1$ in a p-adic sense and $s \approx \frac{1}{b}$. So $as \approx x$ as

$$\begin{aligned} |as - x|_p &= |as - \tfrac{a}{b}|_p \\ &= |a|_p |s - \tfrac{1}{b}|_p \\ &= |\tfrac{a}{b}|_p |bs - 1|_p \\ &= |\tfrac{a}{b}|_p |rp^n|_p \\ &\leq \tfrac{1}{p^n} \end{aligned}$$

as $|x|_p \leq 1$ and $|r|_p \leq 1$. We can find such r, s for each n. By adding a suitable multiple of p^n to as. we can find a $y \in \mathbb{Z}$ of the required form. □

Let $(a_n)_{n=0}^{\infty}$ be a representative Cauchy sequence corresponding to our equivalence class $\{a\}$. As this sequence is Cauchy, let $(N_k)_{k=0}^{\infty}$ denote the monotone increasing sequence of natural numbers satisfying $i, j \geq N_k \implies |a_i - a_j|_p \leq p^{-k}$. By our lemma, for each $k \in \mathbb{N}$, we have an integer z_k satisfying $|z_k - a_{N_k}|_p \leq p^{-k}$ as long as $|a_{N_k}|_p \leq 1$. To show this consider N_1. Given any $n_1, n_2 \geq N_1$, we find

$$\begin{aligned} |a_{n_1}|_p &\leq |a_{n_1} + a_{n_2} - a_{n_2}|_p \\ &\leq \max\{\tfrac{1}{p}, |a_{n_2}|_p\} \end{aligned}$$

for all $n_2 \geq N_1$. But $|a_n|_p \to |a|_p \leq 1$ as $n \to \infty$, so $|a_{n_1}|_p \leq \max\{1, \frac{1}{p}\} = 1$.

We can now apply the lemma for each N_k to give integers x_k satisfying $|a_{N_k} - x_k|_p < p^{-k}$. Moreover $x_{k+1} \equiv x_k \pmod{p}$ as

$$\begin{aligned} |x_{k+1} - x_k|_p &= |x_{k+1} - a_{N_{k+1}} + a_{N_{k+1}} - x_k - a_{N_k} + a_{N_k}|_p \\ &\leq \max\{|x_{k+1} - a_{N_{k+1}}|_p, |x_k - a_{N_k}|_p, |a_{N_{k+1}} - a_{N_k}|_p\} \\ &= \max\{p^{-(k+1)}, p^{-k}, p^{-k}\} \\ &= p^{-k} \end{aligned}$$

and $|x_k - a_k| \to 0$ as $k \to \infty$, since

$$\begin{aligned} |x_k - a_k| &= |x_k - a_k + a_{N_j} - a_{N_j} + x_j - x_j|_p \\ &\leq \max\{|x_k - x_j|_p, |a_k - a_{N_j}|_p, |x_j - a_{N_j}|_p\} \\ &= p^{-j} \end{aligned}$$

so long as $k \geq N_j$. Therefore $(x_n)_{n=0}^{\infty}$ and $(a_n)_{n=0}^{\infty}$ are equivalent. □

This canonical representation can be extended intuitively to $x \in \mathbb{Q}_p$ with $|x|_p = p^i \not\leq 1$ since we can represent xp^i using the canonical representation to get a sequence $(x_n)_{n=0}^{\infty}$ determining xp^i and divide each term by p^i.

Definition: Let p be a prime number. A sequence of integers $(x_n)_{n=0}^{\infty}$ satisfying

$$x_n \equiv x_{n-1} \pmod{p^n}$$

for each $n \geq 1$ determines an object called a *p-adic integer*. Moreover, two sequences $(x_n)_{n=0}^{\infty}$ and $(y_n)_{n=0}^{\infty}$ determine the same p-adic integer iff

$$x_n \equiv y_n \pmod{p^{n+1}}$$

for all $n \geq 0$. The set of p-adic integers coincides with $\overline{B_p}(0,1)$.

The sequence $(x_n)_{n=0}^{\infty}$ is clearly Cauchy as $x_n = x_{n-1} + zp^n$, $(z \in \mathbb{Z})$, and so $\lim_{n\to\infty} |x_n - x_{n-1}|_p = 0$. Moreover, the sequence's limit is clearly not in $\mathbb{Q}$, unless it is eventually constant, thus in $\mathbb{Z}$, as it is not bounded in the usual analytic sense. The set of these p-adic integers will be called $\mathbb{Z}_p$. $\mathbb{Z}_p$ is a (commutative unital) ring with addition and multiplication defined pointwise on sequences in the set. This follows in a straightforward manner since each 'point' a sequence defining a p-adic integer is itself a rational number.

5.2 Hensel's Lemma

For specific examples of elements in $\mathbb{Z}_p$ that are not in $\mathbb{Q}$, we can ask ourselves the question: given a polynomial the coefficients of which are rational integers, but the roots of which are not, do the roots of this polynomial fall in $\mathbb{Z}_p$? As a simple analogy, take $\sqrt{2} \in \mathbb{R}$. This is one of the two roots of the quadratic polynomial $x^2 - 2 = 0$. A suitable Cauchy sequence whose elements are rational numbers which defines $\sqrt{2}$ can be obtained using the Newton-Raphson method to approximate $\sqrt{2}$. A similar iterative process can be done in the p-adic integers, utilising a result known as Hensel's lemma.

Theorem: (Hensel's Lemma) Suppose $f(x) = \sum_{j=0}^{k} c_j x^j$ is a polynomial whose coefficients are p-adic integers and there exists a p-adic integer a_0 such that $f(a_0) \equiv 0 \pmod{p}$ and $f'(a_0) \not\equiv 0 \pmod{p}$. Then there exists a unique p-adic integer, a such that $f(a) = 0$ and $a \equiv a_0 \pmod{p}$.

Proof: We will aim to prove that there exists a sequence $\{a_n\}_{n=1}^{\infty}$ with each $a_n \in \mathbb{Z}$ satisfying the following:

1. $f(a_n) \equiv 0 \pmod{p^{n+1}}$
2. $a_n \equiv a_{n-1} \pmod{p^n}$
3. $0 \leq a_n < p^{n+1}\ \forall n$

One element of $\{1, 2, \ldots, p-1\}$ is congruent to a_0 modulo p. Call this α. A suitable a_1 which satisfies the above three properties must be equivalent to $a_0 \pmod{p}$ and exist in $[0, p^{n+1})$. Therefore, this a_1 must be of the form $\alpha + b_1 p$ where $b_1 \in [0, p)$. Also, it must be so that $f(a_1) \equiv 0 \pmod{p^2}$ satisfying property 1, above.

$$\begin{aligned} f(\alpha + b_1 p) &= \sum_{j=0}^{k} c_j (\alpha + b_1 p)^j \\ &= \sum_{j=0}^{k} (c_j \alpha^j + \binom{j}{1} c_j \alpha^{j-1} (b_1 p) + \binom{j}{2} c_j \alpha^{j-2} (b_1 p)^2 + \ldots) \\ &\equiv \sum_{j=0}^{k} (c_j \alpha^j + j c_j \alpha^{j-1} (b_1 p)) \pmod{p^2} \\ &= \sum_{j=0}^{k} (c_j \alpha^j) + \sum_{j=0}^{k} (j c_j \alpha^{j-1} (b_1 p)) \\ &= f(\alpha) + f'(\alpha) b_1 p \end{aligned}$$

Now, $f(\alpha)$ is divisible by p as $f(\alpha) \equiv f(a_0) \equiv 0 \pmod{p}$ as assumed. So to check that $f(\alpha) + f'(\alpha) b_1 p \equiv 0 \pmod{p^2}$ equates to checking if $z + f'(\alpha) b_1 \equiv 0 \pmod{p}$ for some $z \in \{0, 1, 2, \ldots, p-1\}$. Since $f'(\alpha) \neq 0$ by assumption and all nonzero elements of $(\mathbb{Z}/p)^\times$ are invertible, we can find a suitable b_1 such that $z + f'(\alpha) b_1 \equiv 0 \pmod{p}$, namely such that $b_1 \equiv (-z)(f'(\alpha)^{-1}) \pmod{p}$. So we can set $a_1 = \alpha + b_1 p$, satisfying the 3 conditions above.

Proceeding by induction, assume that there is a sequence $\{a_1, a_2, a_3, \ldots, a_{n-1}\}$ satisfying the three conditions above. We wish to find an $a_n \equiv a_{n-1} \pmod{p^n}$ satisfying $0 \leq a_n < p^{n+1}\ \forall n$ and such that $f(a_n) \equiv 0 \pmod{p^{n+1}}$. Now,

$$f(a_n) = f(a_{n-1} + b_n p_n) \equiv f(a_{n-1}) + f'(a_{n-1}) b_n p^n \equiv 0 \pmod{p^{n+1}}$$

and since $p^n \mid f(a_{n-1})$ by assumption, any b_n satisfying the above must also satisfy $w + f'(a_{n-1}) b_n \equiv 0 \pmod{p}$ for some $w \in \{0, 1, 2, \ldots, p-1\}$. Also, $f(a_{n-1}) \not\equiv 0$ and so we can find a b_n satisfying this equation. By the induction principle, we can find the sequence $\{a_n\}_{n=0}^{\infty}$ for all $n \in \mathbb{N}$. a is the limit of this sequence and must therefore satisfy $f(a) = 0$ since it satisfies $f(a) \equiv 0 \pmod{p^n}$ for all $n \in \mathbb{N}$. $\square$

Hensel's lemma is constructive insofar as that it allows us not only to know whether the root of a specific polynomial falls in $\mathbb{Q}_p$ but it also gives us a way to construct an ongoing sequence of terms that converges to that root.

One can use Hensel's lemma to check, for example, if the polynomial $x^2 - 5 = 0$ has a solution in $\mathbb{Q}_{29}$. If there an a_0 can be found satisfying $f(a_0) \equiv 0 \pmod{29}$ and $f'(a_0) \not\equiv 0 \pmod{29}$, then a solution exists. The first condition can be checked here by verifying whether 5 is a *quadratic residue* modulo 29. Letting $x = 11$ gives $121 - 5 \equiv 0 \pmod{29}$ which is true, so a_0 is 11. Also, $2(11) \neq 0 \pmod{29}$, so the root of $x^2 - 5$ can be found in $\mathbb{Q}_{29}$. Continuing with the algorithm, we must now solve the congruence

$$\begin{array}{rll} & (11+29t)^2 & \equiv 5 \pmod{29^2} \\ \Rightarrow & 121 + 22.29t + 29^2t^2 & \equiv 5 \pmod{29^2} \\ \Rightarrow & 4.29 + 22.29t & \equiv 0 \pmod{29^2} \\ \Rightarrow & 4 + 22t & \equiv 0 \pmod{29} \\ \Rightarrow & 22t & \equiv 25 \pmod{29} \\ \Rightarrow & 4(22t) & \equiv 4(25) \pmod{29} \\ \Rightarrow & t & \equiv 13 \pmod{29} \end{array}$$

to get $t = 13$ and $a_1 = 11 + 13.29 = 388$, the second term in our Cauchy sequence (and second approximation in the p-adic analogue to the Newton-Raphson method).

The next congruence should now be

$$\begin{array}{rll} & (11 + 29.13 + 29^2t)^2 & \equiv 5 \pmod{29^3} \\ \Rightarrow & (388 + 29^2t)^2 & \equiv 5 \pmod{29^3} \\ \Rightarrow & 179 + 776t & \equiv 0 \pmod{29} \\ \Rightarrow & 5 + 22t & \equiv 0 \pmod{29} \\ \Rightarrow & 22t & \equiv 24 \pmod{29} \\ \Rightarrow & t & \equiv 9 \pmod{29} \end{array}$$

giving $t = 9$ and $a_2 = 11 + 13.29 + 9.29^2 = 7957$. The next step involves the equation

$$\begin{array}{rll} & (7957 + 29^3t)^2 & \equiv 5 \pmod{29^4} \\ \Rightarrow & 63,313,849 + 15914t.29^3 & \equiv 5 \pmod{29^4} \\ \Rightarrow & 2596 + 15914t & \equiv 0 \pmod{29} \\ \Rightarrow & 15 + 22t & \equiv 0 \pmod{29} \\ \Rightarrow & 22t & \equiv 14 \pmod{29} \\ \Rightarrow & t & \equiv 27 \pmod{29} \end{array}$$

so $t = 27$ and $a_3 = 11 + 13.29 + 9.29^2 + 27.29^3 = 666,460$. One can continue indefinitely in this manner to approximate the p-adic $\sqrt{5}$ to an arbitrary accuracy.

Note that when considering the initial congruence ($x^2 - 5 \equiv 0 \pmod{p}$) there are two choices for x, namely 11 and 18. Indeed $18^2 - 5 = 319 \equiv 0 \pmod{p}$. This is reflective of the fact that an nonzero element in $\mathbb{Z}/p\mathbb{Z}$ will have exactly two square roots if it has one. For assume $0 \leq x \leq p-1$ is a root. Then $-x \equiv p - x \pmod{p}$ is also a root. Using 18 in the place of 11 to generate a sequence approaching the p-adic $\sqrt{5}$ will generate an answer different to that above that also satisfies the polynomial:

$$\begin{array}{rll} & (18+29t)^2 & \equiv 5 \pmod{29^2} \\ \Rightarrow & 319 + 36.29t & \equiv 0 \pmod{29^2} \\ \Rightarrow & 11 + 7t & \equiv 0 \pmod{29} \\ \Rightarrow & t & \equiv 25(18) \pmod{29} \\ \Rightarrow & t & \equiv 15 \pmod{29} \end{array}$$

and so on as before.

The above calculation becomes quite time-consuming in even the first few steps, since the integers involved grow quickly. The Perl script in Appendix A automatically generates such a sequence of terms derived using the algorithm of Hensel's lemma.

The script takes a sequence of integers $a_0 \ldots a_m$ from the command line which define a polynomial $f(x) = \sum_{j=0}^{m} a_j x_j$ and requires two arguments, passed through the standard input when the user is prompted. The first argument is the number of iterations of the algorithm (i.e. the number of terms in the Cauchy sequence to be generated). The second is the relevant prime p whose completion we wish to check. The powerhouse behind this script is the subroutine "cauchy_ sequence" that generates the successive b_n of Hensel's lemma. It does so in precisely the same manner as the original calculations above and takes only the successively decrementing scalar `$iterations` of the sequence as an argument. Each other variable external to the subroutine is passed automatically by Perl and stays constant. The subroutine begins with a recursive call, checking if b_n is defined and $n \neq 0$. If not, the argument $n-1$ is passed back into the function and this continues until $n = 0$. The scalar `$sum` is unchanged in the first step and the following 'for' loop identifies an integer $0 \leq k \leq p-1$ that satisfies $f(k) \equiv 0 \pmod{p}$ and stores this integer in the first entry of the array `@a`. The next step is only executed once, on the first iteration of the algorithm. It checks whether the formal criteria for Hensel's lemma is satisfied (i.e. $f(k)$ is soluble mod p and the solution a_0 does not also satisfy the derivative of the polynomial). In the event that these criteria are not satisfied, the script exits and returns that a root cannot be found in $\mathbb{Q}_p$.

On successive iterations of "cauchy_ sequence", the scalar `$sum` is incremented by $b_{n-1}p^{n-1}$ and the 'for' loop following this assignment checks for any b_n that satisfies the equation

$$f(\sum_{i=0}^{n-1} b_i p^i + b_n p^n) \equiv 0 \pmod{p^{n+1}}$$

and we are guaranteed to find such a b_n by the lemma. This b_n is placed in the nth entry of `@a`. After `@a` contains as many entries as the number of iterations required, the array is printed to the terminal screen.

The following is a sample output that appears on the screen:

> **./p_adic_hensel.pl -5 0 1**
Please enter the number of iterations:
25
Please enter your prime:
29
{11, 13*29^1, 9*29^2, 27*29^3, 0*29^4, 3*29^5, 27*29^6, 28*29^7, 13*29^8, 18*29^9, 8*29^10, 17*29^11, 16*29^12, 25*29^13, 0*29^14, 20*29^15, 24*29^16, 27*29^17, 20*29^18, 26*29^19, 1*29^20, 2*29^21, 8*29^22, 6*29^23, 26*29^24...}

This output corroborates the sequence obtained from the workings out before the script was introduced. Note that the format of the output is $\{a_0, a_1, a_2 \ldots a_n\}$ where these refer to the terms of the series $\sum_{i=0}^{n} a_i$ such that this series, rather than printed sequence is the Cauchy sequence approaching $\sqrt{5}$. To check the second root of the polynomial, one can 'comment out' the command '`last;`' in the 79th line of the script. Using the same input as before, the modified script gives the following output:

{18, 15*29^1, 19*29^2, 1*29^3, 28*29^4, 25*29^5, 1*29^6, 0*29^7, 15*29^8, 10*29^9, 20*29^10, 11*29^11, 12*29^12, 3*29^13, 28*29^14, 8*29^15, 4*29^16, 1*29^17, 8*29^18, 2*29^19, 27*29^20, 26*29^21, 20*29^22, 22*29^23, 2*29^24...}

which was verified to the second term above. Now let's check a more complex polynomial, $f(x) = 32x^7 + 3x^6 + 7x^2 - 1$. This has a root in $\mathbb{Q}_{17}$, approximated by the output:

{13, 10*17^1, 16*17^2, 11*17^3, 11*17^4, 3*17^5, 10*17^6, 7*17^7, 10*17^8, 8*17^9, 10*17^10, 8*17^11, 10*17^12, 9*17^13, 5*17^14, 16*17^15, 15*17^16, 12*17^17, 1*17^18, 16*17^19, 6*17^20, 3*17^21, 6*17^22, 16*17^23, 14*17^24, 1*17^25, 12*17^26, 11*17^27, 8*17^28, 11*17^29, 7*17^30, 11*17^31, 8*17^32, 15*17^33, 13*17^34, 0*17^35, 0*17^36, 1*17^37, 13*17^38, 14*17^39, 6*17^40, 6*17^41, 5*17^42, 16*17^43, 15*17^44,

10*17^45, 11*17^46, 16*17^47, 10*17^48, 6*17^49...}

up to the first 50 terms obtained from Hensel's lemma.

By entering '0' when prompted to input the number of desired iterations, one can quickly check whether a p-adic square root is contained in $\mathbb{Q}_p$. For example, one can check whether $f(x) = x^2 - 7$ has roots in each $\{\mathbb{Q}_p : p \in \{2,3,5...,97\}\}$, to find out that

$$\sqrt{7} \in \mathbb{Q}_p \text{ when } p \in \{2,3,7,19,29,31,37,47,53,59,83\}$$

and not in $\mathbb{Q}_p$ for any other prime less than 100.

5.3 The Induced Metric on $\mathbb{Q}_p$

Proposition: There is a natural extension of $|.|_p$ to $\mathbb{Q}_p$ given by $x \in \mathbb{Q}_p \implies |x|_{(p)} = \lim_{n\to\infty} |x_n|_p$ where $(x_n)_{n=0}^{\infty}$ is a Cauchy sequence converging to x.

Proof: We need to check that this makes sense, is invariant under replacement of $(x_n)_{n=0}^{\infty}$ with $(y_n)_{n=0}^{\infty}$ where $(x_n)_{n=0}^{\infty} \sim (y_n)_{n=0}^{\infty}$ and that it is an extension of the previous valuation. Firstly, it must make sense since the $\lim_{n\to\infty} |x_n|_p$ exists as $(x_n)_{n=0}^{\infty}$ is Cauchy. Suppose that $(x_n)_{n=0}^{\infty} \not\to 0$ (otherwise x is $0 \in \mathbb{Q}_p$ and this case will follow when we prove the the other parts of the proposition). In particular, we can find $\varepsilon > 0$ so that $|x_n - 0| \geq \varepsilon$ for all n, because otherwise 0 would be the limit of the sequence. Since $(x_n)_{n=0}^{\infty}$ is Cauchy, for the same $\varepsilon > 0$ we can find n and m sufficiently large to satisfy $|x_n - x_m|_p < \varepsilon$. By the non-Archimedean property, then $|x_n - x_m|_p < \max\{|x_n|, |x_m|\}$ for large enough m, n to satisfy $|x_i| \geq \varepsilon$, $i = m, n$. Then $|x_n|_p = |x_m|_p$ for all m, n large enough and $|x_n|_p$ becomes constant. We can find the limit of an evenutally constant sequence, so the formulation makes sense. Also, if $x \in \mathbb{Q}$, then x can be represented by the constant sequence $(x)_{n=0}^{\infty}$ and $\lim_{n\to\infty} |x|_p = |x|_p$, so this valuation is strictly an extension (once we can prove the next aspect).

Next, suppose $(x_n)_{n=0}^{\infty}$ and $(\hat{x}_n)_{n=0}^{\infty}$ are equivalent sequences. Then $\lim_{n\to\infty} |x_n - \hat{x}_n|_p \to 0$. By the reverse triangle inequality, $\lim_{n\to\infty} |x_n - \hat{x}_n|_p \geq \lim_{n\to\infty} \left| |x_n|_p - |\hat{x}_n|_p \right|$. Then, by the Squeeze law, we get $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |\hat{x}_n|_p$, as required. □

This new $|.|_{(p)}$ (or just $|.|_p$ from now on) remains non-Archimedean. Let $(x_n)_{n=0}^{\infty}$, $(y_n)_{n=0}^{\infty}$ be representatives of classes of Cauchy sequences in $\mathbb{Q}_p$. Then,

$$\begin{aligned} \lim_{n\to\infty} |(x_n)_{n=0}^{\infty} + (y_n)_{n=0}^{\infty}|_p &= \lim_{n\to\infty} |(x_n + y_n)_{n=0}^{\infty}|_p \\ &\leq \lim_{n\to\infty} \max\{|(x_n)_{n=0}^{\infty}|_p, |(y_n)_{n=0}^{\infty}|_p\} \end{aligned}$$

Proposition: $(\mathbb{Q}_p, d_p)$ is a complete metric space.

Proof: Let $(x_n)_{n=0}^{\infty}$ be a Cauchy sequence in $\mathbb{Q}_p$. Then, each $x_n = (x_{n,i})_{i=0}^{\infty}$ is itself a Cauchy sequence. We need to check that for each Cauchy sequence $(x_n)_{n=0}^{\infty}$ that its limit $(y_n)_{n=0}^{\infty}$ can be found in $\mathbb{Q}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ (by our formulation of $\mathbb{Q}_p$ using Cauchy sequences in $\mathbb{Q}$), we can find a rational number as close as we like to the limit of any element in $\mathbb{Q}_p$. In particular, for each Cauchy sequence $(x_{n,i})_{i=0}^{\infty} \subset \mathbb{Q}$, we can find a rational number $y_n : |\lim_{i\to\infty}(x_{n,i}) - y_n|_p < \varepsilon$ for any $\varepsilon > 0$. For each n, then, we can let $\varepsilon = \frac{1}{n}$ to get

$$\lim_{n\to\infty} |\lim_{i\to\infty}(x_{n,i}) - y_n|_p < \lim_{n\to\infty} \frac{1}{n} = 0$$

so that we get $\lim_{n\to\infty} |\lim_{i\to\infty}(x_{n,i}) - y_n|_p \to 0$ by the Squeeze Law. Then $(y_n)_{n=0}^{\infty} = \lim_{n\to\infty} x_n$. It remains to prove that $(y_n)_{n=0}^{\infty}$ itself is Cauchy in $\mathbb{Q}$. But

$$|y_n - y_m|_p \leq \max\{|y_n - x_{n,i}|_p, |x_{n,i} - x_{m,i}|_p, |x_{m,i} - y_m|_p\}$$

and we can find $N \in \mathbb{N}$:

$$m,n > N \implies |y_n - x_{n,i}|_p, |x_{n,i} - x_{m,i}|_p, |x_{m,i} - y_m|_p < \varepsilon$$

and so $|y_n - y_m|_p < \varepsilon$. $(y_n)_{n=0}^{\infty} \in \mathbb{Q}_p$ is Cauchy and $\mathbb{Q}_p$ is complete. $\square$

However, as Hensel's lemma demonstrates, $\mathbb{Q}_p$ is not algebraically closed. For any $p > 2$, we can take the polynomial $f(x) = x^2 - m$ and choose m to be a quadratic nonresidue modulo p. Then we can never find a $y \in \mathbb{Q}_p$ satisfying $f(y) = 0$ because $|f(y)|_p > \frac{1}{p}$ always. Accordingly, one needs to construct a superset $\overline{\mathbb{Q}}_p \supset \mathbb{Q}_p$ to be able to solve arbitrary polynomials.

6 Topology of $\mathbb{Q}_p$

Let τ_p refer to the topology induced by the p-adic metric on the space $\mathbb{Q}_p$.

As a topological space, $\mathbb{Q}_p$ is Hausdorff, as any metric-induced topology on a space must be Hausdorff. It is also completely metrisable, as a the complete metric space. Since the rational numbers are both countable and dense in the space, $\mathbb{Q}_p$ is separable.

However $\mathbb{Q}_p$ is not compact which can be proven by contradiction. Fix some $x \in \mathbb{Q}_p$. Let $\mathscr{U} = \{B_p(x,n) : n \in \mathbb{N}\}$ be an open cover for $\mathbb{Q}_p$. Suppose that this open cover has a finite subcover, say

$$\{B_p(x,n_1), B_p(x,n_2), \ldots, B_p(x,n_s)\}$$

Let $N = \max\{n_1, \ldots, n_s\}$. Now, $B_p(x,n_i) \subseteq B_p(x,N)$, $\forall\ 0 \le i \le s$. There exists a $y \in \mathbb{Q}_p$ such that $y \notin B_p(x,N) \implies d(x,y)_p > N \implies |x-y|_p > N$. Letting $y = x + \frac{1}{p^j}$ for j large enough that $p^j > N$ gives such a y. Thus, this y is in none of the open sets in the finite subcover. Hence, $\mathscr{U}$ cannot have a finite subcover. Therefore $\mathbb{Q}_p$ cannot be compact and since the conditions of compactness and sequential compactness are equivalent in a space with a metric-induced topology, $\mathbb{Q}_p$ is not sequentially compact. It is, however, locally compact, and we will prove that $\mathbb{Z}_p$ is compact at the end of this chapter.

As a metric space, $\mathbb{Q}_p$ is first countable since at any point $x \in \mathbb{Q}$, the neighbourhood base $\{B_p(x, \frac{1}{n})\}_{n\in\mathbb{N}}$ is countable. $\mathbb{Q}_p$ is also second countable using the base $\mathscr{B} = \{B_p(q, \frac{1}{n}) : q \in \mathbb{Q}, n \in \mathbb{N}\}$. However, $\mathbb{Q}_p$ does not have a countable number of elements. We will discuss this in relation to the Cantor set, $\mathscr{C}$, later.

$(\mathbb{Q}_p, \tau_p)$ is disconnected. One may show this by proving that there exists a set that is both open and closed in the metric topology. Let $B_p(x,\varepsilon)$ be an open ball. Choose some $y \in \mathbb{Q}_p \setminus B_p(x,\varepsilon)$ such that $d_p(x,y) \ge \varepsilon$. Choose some $\delta < \varepsilon$. We need to prove that $B_p(y,\delta) \cap B_p(x,\varepsilon) = \emptyset$. Now choose some $z \in B_p(y,\delta)$:

$$\begin{aligned} \varepsilon &\le d_p(x,y) \\ &= |x - z + z - y|_p \\ &\le \max\{d_p(x-z), d_p(z-y)\} \\ &= \max\{d_p(x-z), \delta\} \\ &= d_p(x-z) \end{aligned}$$

$\implies \mathbb{Q}_p \setminus B_p(x,\varepsilon)$ is open $\implies B_p(x,\varepsilon)$ is closed and thus clopen in $(\mathbb{Q}_p, \tau_p)$. So $\mathbb{Q}_p \setminus B_p(x,\varepsilon) \cup B_p(x,\varepsilon) = \mathbb{Q}_p$ with both open $\implies \mathbb{Q}_p$ is not connected. This also works for any subspace X of $(\mathbb{Q}_p, \tau_p)$ with the subspace topology, as we can replace $\mathbb{Q}$ by X (or, indeed, any space with a topology induced from an Archimedean metric) in the above argument so long as our subspace has at least three elements. Moreover, since $\mathbb{Q}_p$ is Hausdorff, its subspaces must be Hausdorff, so a two-point subspace must also be disconnected, following from the definition of a Hausdorff topological space. Therefore, only the singleton sets and the empty set are connected in the p-adic numbers. Spaces satisfying this condition are known as *totally disconnected*.

We deduce the cardinality of $\mathbb{Z}_p$ by using the canonical representation of each $x \in \mathbb{Z}_p$ described prior to Hensel's lemma. Each sequence of natural numbers $(x_n)_{i=0}^{\infty}$ with $x_i \in [0,\ p)$ determines a p-adic integer, and, moreover, all p-adic integers are of this form. Therefore, $\mathbb{Z}_p$ has cardinality

$$\operatorname{card}(\mathbb{Z}_p) = \prod_{n=0}^{\infty} \operatorname{card}([0,1,\ldots,p))$$

and to this we can juxtapose the Cantor set, $\mathscr{C}$.

To construct the (ternary) Cantor set, take the interval $[0,1]$. In the first step, remove $(\frac{1}{3},\frac{2}{3})$ to get the union of two disjoint intervals $[0,\frac{1}{3}]\cup[\frac{2}{3},1]$. From each of these sets, remove the middle third as in the first step (leaving the union of four disjoint sets $[0,\frac{1}{9}]\cup[\frac{2}{9},\frac{1}{3}]\cup[\frac{2}{3},\frac{7}{9}]\cup[\frac{8}{9},1]$) and continue this process over infinitely many steps. The Cantor set is the set of points that are not omitted in this iterative process. Intuitively, in the first step we may choose a point in the first third or the last third of $[0,1]$ (call these I_0 and I_1 respectively). If we choose I_0, say, then in the second step we must choose from the first or last third of that interval (call these I_{00} and I_{01}, respectively). Continuing this process, we see that the Cantor set may be formed from the set of all sequences $(x_n)_{n=0}^{\infty}$ with each $x_i \in \{0,1\}$ (i.e. the set of all right-infinite binary expansions). Its cardinality therefore is given by

$$\text{card}(\mathscr{C}) = \prod_{n=1}^{\infty} \text{card}(\{0,1\}) = 2^{\text{card}(\mathbb{N})} = 2^{\aleph_0}$$

since $\text{card}(\mathbb{N}) = \aleph_0$, the cardinality of countably infinite sets. Using Cantor's diagonal argument on the set of real numbers expressed in binary, rather than decimal, terms, we find that $\text{card}(\mathbb{R}) = 2^{\aleph_0} = \text{card}(\mathscr{C})$ and that the Cantor set has the cardinality of the continuum. Returning to the p-adic integers, we have from above that each p-adic integer is determined by a sequence $(x_n)_{n=1}^{\infty}$ with each $x_i \in [0,p)$ and so $\text{card}(\mathbb{Z}_p) = p^{\aleph_0} = \aleph_1$, again by Cantor's diagonal argument applied to the real numbers represented by their p-nary expansion. Thus, the Cantor set $\mathscr{C}$, the reals $\mathbb{R}$ and the p-adic integers $\mathbb{Z}_p$ are equinumerous. As discussed briefly after the theorem regarding canonical representation of the p-adic integers, we can express any $x \in \mathbb{Q}_p \backslash \mathbb{Z}_p$ in canonical form by representing $xp^i \in \mathbb{Z}_p$ and then dividing each term by p^i to get a number in the form

$$\sum_{n=-i}^{\infty} a_n p^n$$

where the a_n are chosen from $[0,\ p)$ for $n \in [-i,\infty)$. Using this construction, it is clear the cardinality of $\mathbb{Q}_p$ is also that of the continuum, as we have a countable number of choices for i.

In fact, the p-adic integers are homeomorphic to the Cantor set as, if they are compactified by the addition of a single point (through Alexandroff compactification), are the p-adic numbers. The following proposition shows this explicitly for $p = 2$.

Proposition: Let $(\mathbb{Z}_2, d_2)$ be the set $\{x \in \mathbb{Q}_2 : |x|_2 \leq 1\}$ of 2-adic integers with the metric topology induced from the 2-adic valuation and let $(\mathscr{C}, d_\infty)$ be the Cantor set with the metric topology induced from the Euclidean norm. These two topological spaces are homeomorphic.

Proof: The elements of each of these sets can be denoted by sequences $(x_n)_{n=0}^{\infty}$ with each $x_i \in \{0,1\}$. In particular, each 2-adic integer can be represented in canonical form as $\sum_{n=0}^{\infty} x_n 2^n$ with $x_i \in \{0,1\}$ so this sequence is well defined. If two sequences in this representation, $(x_n)_{n=0}^{\infty}$ and $(y_n)_{n=0}^{\infty}$, differ in the jth term and no other term before j, the distance between them is

$$d_2((x_n)_{n=0}^{\infty},(y_n)_{n=0}^{\infty}) = \left|\sum_{k=j}^{\infty}(x_k - y_k)2^k\right|_2 = 2^{-j}$$

since the difference of the two numbers is divisible by 2^j and not divisible by any higher power of 2.

If two elements of the Cantor set under this representation differ in the jth term but no earlier term, then

the distance between them

$$\begin{aligned} d_\infty((x_n)_{n=0}^\infty,(y_n)_{n=0}^\infty) &= \left|\sum_{k=j}^\infty \frac{2(x_k-y_k)}{10^k}\right|_\infty \\ &\leq \sum_{k=j}^\infty \left|\frac{2(x_k-y_k)}{10^k}\right|_\infty \\ &\leq \sum_{k=j}^\infty \frac{2}{10^k} \\ &= \sum_{k=0}^\infty \frac{2}{10^k} - \sum_{k=j-1}^\infty \frac{2}{10^k} \\ &= \tfrac{2}{9}\left(\tfrac{1}{10}\right)^{j-1} \end{aligned}$$

is bounded above.

We can define a bijection $\varphi : \mathscr{C} \to \mathbb{Z}_2$ such that φ sends an element determined by the sequence $(x_n)_{n=0}^\infty$ in the Cantor set to the element determined by the same sequence in $\mathbb{Z}_2$. Since each element of each set is uniquely expressible in this way, this mapping is clearly a bijection. We prove that it is also continuous using the metric definition of continuity. Fix some $x \in \mathscr{C}$. Given an $\varepsilon > 0$, we can find a $j \in \mathbb{N}$ such that $2^{-(j+1)} < \varepsilon \leq 2^{-j}$. We can choose $\delta = \frac{2}{9}\left(\frac{1}{10}\right)^j$ so that

$$|x-y|_\infty < \delta \implies |\varphi(x)-\varphi(y)|_2 < \varepsilon$$

for any $y \in \mathscr{C}$. In particular, this δ implies that x and y have at least the first $j+1$ terms of their representative sequences in common, forcing $d_2(x,y) \leq 2^{-(j+1)} < \varepsilon$. Since this holds for any $\varepsilon > 0$ and $y \in \mathscr{C}$, φ is continuous.

To prove $\varphi^{-1} : \mathbb{Z}_2 \to \mathscr{C}$, the inverse of φ is continuous, fix some $x \in \mathbb{Z}$. Given any ε, we can find a $j \in \mathbb{N}$ such that $\frac{2}{9}\left(\frac{1}{10}\right)^j < \varepsilon \leq \frac{2}{9}\left(\frac{1}{10}\right)^{j-1}$. We can choose $\delta = 2^{-(j+1)}$ so that

$$|x-y|_2 < \delta \implies |\varphi^{-1}(x)-\varphi^{-1}(y)|_\infty < \varepsilon$$

is true. So φ^{-1} is continuous and, thus φ is a continuous, bijective map from $(\mathscr{C}, d_\infty)$ to $(\mathbb{Z}_2, d_2)$, with a continuous inverse. Therefore φ is a homeomorphism. □

Corollary: $\mathbb{Z}_p$ is compact and $\mathbb{Q}_p$ is locally compact.

Proof: $\mathbb{Z}_p$ is homeomorphic to $\mathscr{C}$. Since $\mathscr{C}$ is a bounded, closed subset of Euclidean space, it is compact (by the Heine-Borel theorem). Therefore $\mathbb{Z}_p$ is compact and, as $\mathbb{Z}_p$ is a compact neighbourhood of 0, $\mathbb{Q}_p$ is locally compact. □

7 Generalisations of the p-adic Valuation to Principal Ideal Domains

Definition: A *principal ideal domain* (PID) is an integral domain in which every ideal has a single generating element.

Definition:A *unique factorisation domain* (UFD) is an integral domain in which every ideal can be factorised as the product of prime ideals. Recall that a *prime ideal* of a ring R is an ideal $\mathfrak{p} \neq R$ such that $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ for $a, b \in R$. Every principal ideal domain is a unique factorisation domain.

Example: The Fundamental Theorem of Arithmetic is a symptom of the integers forming a principal ideal domain as every integer can be uniquely factorised, up to multiplication by a unit, as the product of primes, each of which generates an ideal. Given an integer $up_1^{e_1}p_2^{e_2}p_3^{e_3}...p_n^{e_n}$ where (p_i are distinct primes, $u \in \{\pm 1\}$ is

a unit and $e_i \in \mathbb{N}$), we can uniquely identify the integer as the element of $\bigcap_{i=1}^{n} \langle p_i \rangle^{e_i}$ (where $\langle p_k \rangle$ is the prime ideal generated by p_k) that is not in any other prime ideals but those in this intersection.

Definition: Given an integral domain D, one can construct a field

$$K = \{\frac{r_1}{r_2} : r_1, r_2 \neq 0 \in D\}$$

called the *field of fractions* of D. More strictly, we should talk about equivalence classes of such elements and set

$$\frac{r_1}{r_2} \sim \frac{r_1'}{r_2'} \iff r_1 r_2' = r_1' r_2$$

to avoid repetitively adding equivalent elements to the field. This is the smallest field containing D, as it is generated by adding the set $\{r^{-1} : r \in D\}$ of multiplicative inverses of elements in D.

The construction of a field of fractions gives rise to algebraic structures called *fractional ideals* of D. Considering K as a module over D, we can choose a nonzero submodule $M \subseteq K$ such that for some $D \ni r \neq 0$, $rM \subseteq D$. Then M is called a fractional ideal of D. A fractional ideal M is called *invertible* if there exists another fractional ideal M^{-1} such that $MM^{-1} = D$ where the product MM^{-1} is understood to be $\{m_1 m_1' + m_2 m_2' + \ldots m_n m_n' : m_i \in M, m_i' \in M^{-1}\}$. M^{-1} is called the inverse of M. Trivially, every ideal is also a fractional ideal and every fractional ideal is finitely generated over D as

$$rM = R \implies r^{-1} rM = r^{-1} R \implies M = r^{-1} R$$

and so M is generated by r^{-1}.

Example: The rationals are the field of fractions obtained from the integers. Let $\frac{1}{q}$ be the generator of a submodule M_q of $\mathbb{Q}$ over $\mathbb{Z}$. This submodule consists of elements of the form $\frac{z}{q}$ where z is any integer. This submodule is a fractional ideal of $\mathbb{Z}$ since $qM_q \subseteq \mathbb{Z}$.

Proposition: The set of fractional ideals, $\mathscr{F}$, of a principal ideal domain D forms an Abelian group under multiplication. In particular, for each fractional ideal $M \subset K$, $\exists\, M^{-1} \subset K$, the inverse of M in this group.

Proof: Firstly, we have D as the identity element of the group $\mathscr{F}$ of fractional ideals, as $MD = M$ for any $M \in \mathscr{F}$ since M as a module over D consists of linear combinations of elements in D and thus remains unchanged under multiplication. The proof of existence of inverses follows from the proof that each prime ideal $\mathfrak{p}$ has an inverse because any principal ideal domain is also a unique factorisation domain. We need to find a fractional ideal $\mathfrak{p}^{-1} : \mathfrak{p}\mathfrak{p}^{-1} = D$. Let $I = \{r \in K : r\mathfrak{p} \subseteq D\}$. Since $p \in \mathfrak{p}$ implies that $pI \subseteq D$, I is certainly a fractional ideal and $\mathfrak{p} \subseteq I$. But $\mathfrak{p}I \subseteq D$ and since D is a UFD, $\mathfrak{p}$ is a maximal ideal of D (since it is prime), either $\mathfrak{p} = I$ or $\mathfrak{p}I = D$. Suppose $\mathfrak{p} = I$. Then since $1 \in I$, $I = \mathfrak{p} = D$, the identity. So $\mathfrak{p}I = D$ and $I = \mathfrak{p}^{-1}$ and, by extension, every non-zero ideal, $\mathscr{I}$ of D has an inverse, composed of the inverses of the prime ideals whose product is $\mathscr{I}$. If M is a fractional ideal over D, then $\exists$ an $r \in D : rM \subseteq D$. But since M is a module rM is closed under addition and multiplication by elements of D. Therefore rM is an ideal. $\exists$ a fractional ideal $I : I(rM) = D$. But $Ir = I$ as I is a D-module. So $IM = D$ and $I = M^{-1}$. Finally, $\mathscr{F}$ is closed as the product of any finitely generated modules is finitely generated. $\mathscr{F}$ is an Abelian group. □

Lemma: (Unique Factorisation of Fractional Ideals) If D is a principal ideal domain and M a fractional ideal over D, then M is uniquely expressible as the product of positive and negative powers of prime ideals of D.

Proof: Let M be a fractional ideal of D. Then $rM \subseteq D$ is an ideal of D and we can say $rM = \prod_{i=0}^{k} \mathfrak{q}_i M = \prod_{i=0}^{n} \mathfrak{p}_i$ for

$\mathfrak{p}_i$ and $\mathfrak{q}_i$ prime ideals and unique up to order (by unique factorisation) with latter determined by r. Multiplying across by r^{-1}, we get $M = \prod_{i=0}^{n} \mathfrak{p}_i \prod_{i=0}^{k} \mathfrak{q}_i^{-1}$, as required. □

We can use this factorisation of fractional ideals to extend the theory of p-adic analysis on the rationals to $\mathfrak{p}$-adic analysis on any principal ideal domain, D, where $\mathfrak{p}$ is a non-zero prime ideal of D. Given a principal ideal domain D, with its field of fractions denoted by K, and a prime ideal $\mathfrak{p}$ of D, we can establish a $\mathfrak{p}$-adic metric on D as follows: for each $0 \neq x \in K$, xD is a fractional ideal of D and so is uniquely expressible as a product of powers of prime ideals $\prod_{i \in \mathscr{A}} \mathfrak{p}_i^{e_i}$ with $\mathfrak{p}_k \neq \mathfrak{p}_m$ if $m \neq k$ and $e_i \in \mathbb{Z}$. For our chosen prime ideal $\mathfrak{p}$, we define

$$|x|_{\mathfrak{p}} = k^{-\mathrm{ord}_{\mathfrak{p}}(x)}$$

where $1 < k \in \mathbb{R}$ is a real number and $\mathrm{ord}_{\mathfrak{p}}(x)$ is the power of $\mathfrak{p}$ in the product above. For $x = 0$, we let $\mathrm{ord}_{\mathfrak{p}}(x) = \infty$ so that $|x|_{\mathfrak{p}} = 0$. If D is a domain of real numbers, we may choose $k = p$ where $\mathfrak{p} = \langle p \rangle$ for clarity, but this is not necessary. Moreover, the same principle applies to the case of the rationals, but only the case where $k = p$ was discussed in the opening chapters of this project.

Proposition: $|.|_{\mathfrak{p}}$ determines a non-Archimedean valuation on the field K.

Proof: The first property of a valuation follows from our choice of $k > 1$ and the definition of $\mathrm{ord}_{\mathfrak{p}}(x)$ and the second follows from defining $\mathrm{ord}_{\mathfrak{p}}(0) = \infty$.

To prove the third property, choose x and $y \in K$. Now, xD as a fractional ideal can be represented as the product $\prod_{i \in \mathscr{A}} \mathfrak{p}_i^{e_{x_i}}$ of integral powers of prime ideals indexed by a set $\mathscr{A}$ and yD can be represented similarly as $\prod_{i \in \mathscr{A}} \mathfrak{p}_i^{e_{y_i}}$. Now,

$$xyD = xDyD = \prod_{i \in \mathscr{A}} \mathfrak{p}_i^{e_{x_i}} \mathfrak{p}_i^{e_{y_i}} = \prod_{i \in \mathscr{A}} \mathfrak{p}_i^{e_{x_i} + e_{y_i}}$$

and so, for a fixed prime ideal $\mathfrak{p}_i$,

$$|xy|_{\mathfrak{p}_i} = k^{-ord_{\mathfrak{p}_i}(xy)} = k^{-(e_{x_i} + e_{y_i})} = |x|_{\mathfrak{p}_i} |y|_{\mathfrak{p}_i}$$

proving the third property.

The non-Archimedean property, and by extension, the triangle inequality holds for $|.|_{\mathfrak{p}}$, for if $x, y \in K$ with $|x|_{\mathfrak{p}} \leq |y|_{\mathfrak{p}}$, then $\mathrm{ord}_{\mathfrak{p}}(x) \geq \mathrm{ord}_{\mathfrak{p}}(y)$. So, for some integers $m \geq n$, $x \in \mathfrak{p}^m$ and $y \in \mathfrak{p}^n$. Now, $x \in \mathfrak{p}^n$ also and therefore $(x+y) \in \mathfrak{p}^n$. So $\mathrm{ord}_{\mathfrak{p}}(x+y) \geq n \implies |x+y|_{\mathfrak{p}} \leq k^{-n} = |y|_{\mathfrak{p}} = \max\{|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}\}$ and $|.| : K \to [0, \infty)$ is a non-Archimedean valuation. □

As $(K, |.|_{\mathfrak{p}})$ is a field imbued with a non-Archimedean valuation, it is known as a non-Archimedean field. For $x, y \in K$, we can induce a metric from the above valuation, such that the distance, $d_{\mathfrak{p}}(x, y)$, between them is said to be small if $(x-y) \in \mathfrak{p}^j$ for a large j. This metric yields a completion $K_{\mathfrak{p}}$ of K. The set $R = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} \leq 1\}$ is known as the *valuation ring* of $(K, |.|_{\mathfrak{p}})$.

7.1 Hensel's Lemma in the General Case

Definition: Let $D[x] \ni f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial with coefficients in D. Then the formal derivative $f'(x)$ is defined as $\sum_{i=1}^{n} i a_i x^{i-1}$ where $ir = (i-1)r + r$ for $r \in D$ and $1 \leq i \in \mathbb{N}$.

Theorem: (Extending Hensel's Lemma) Let $K_{\mathfrak{p}}$ be a non-Archimedean field complete with respect to $\mathfrak{p}$, a non-zero prime ideal of $D_{\mathfrak{p}}$, the valuation ring of $K_{\mathfrak{p}}$. If $f(x) \in D_{\mathfrak{p}}[x]$, with $f'(x)$ its formal derivative, and $r_0 \in D_{\mathfrak{p}}$ satisfies

$$|f(r_0)|_{\mathfrak{p}} < |f'(r_0)^2|_{\mathfrak{p}}$$

then there exists a sequence $(r_k)_{k=0}^{\infty}$ and an element $\tilde{r} \in K_{\mathfrak{p}}$ satisfying

$$\tilde{r} = \lim_{i\to\infty} r_{i+1} = \lim_{i\to\infty}\left(r_i - \frac{f(r_i)}{f'(r_i)}\right)$$

and $f(\tilde{r}) = 0$.

Proof: As in the specific case of Hensel's lemma with $K_{\mathfrak{p}} = \mathbb{Q}_p$, we need to establish the existence of a sequence for which the following holds:

(i) $|f'(r_i)|_{\mathfrak{p}} = |f'(r_0)|_{\mathfrak{p}}$

(ii) $\left|\frac{f(r_i)}{f'(r_i)^2}\right|_{\mathfrak{p}} \leq \left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}^{2i}$

(iii) $|r_i - r_0|_{\mathfrak{p}} \leq \left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}$

with each $r_i \in D_{\mathfrak{p}}$.

These conditions hold for $i = 0$. We prove the rest by way of induction. Firstly,

$$\left|\frac{f(r_i)}{f'(r_i)^2}\right|_{\mathfrak{p}} \leq \left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}^{2i} \Longrightarrow \left|\frac{-f(r_i)}{f'(r_i)}\right|_{\mathfrak{p}} \leq \left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}^{2i} \left|f'(r_i)\right|_{\mathfrak{p}}$$

and $\left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}} < 1$ by assumption, so for $i \geq 1$,

$$\left|\frac{-f(r_i)}{f'(r_i)}\right|_{\mathfrak{p}} < \left|f'(r_i)\right|_{\mathfrak{p}}$$

which implies that $|f'(r_{i+1})|_{\mathfrak{p}} = |f'(r_i)|_{\mathfrak{p}} = |f'(r_0)|_{\mathfrak{p}}$ since Taylor's formula shows

$$f'(r_{i+1}) = f'(r_i - \frac{f(r_i)}{f'(r_i)}) = f'(r_i) - \delta\frac{f(r_i)}{f'(r_i)}$$

for some $\delta \in D_{\mathfrak{p}}$ and the non-Archimedean valuation $|.|_{\mathfrak{p}}$ gives

$$|f'(r_{i+1})|_{\mathfrak{p}} \leq \max\{|f'(r_i)|_{\mathfrak{p}}, \left|\delta\frac{-f(r_i)}{f'(r_i)}\right|_{\mathfrak{p}}\} = |f'(r_i)|_{\mathfrak{p}}$$

and

$$|f'(r_i)|_{\mathfrak{p}} \leq \max\{|f'(r_{i+1})|_{\mathfrak{p}}, \left|\delta\frac{-f(r_i)}{f'(r_i)}\right|_{\mathfrak{p}}\} = |f'(r_{i+1})|_{\mathfrak{p}}$$

as $f'(r_i) > \left|\frac{-f(r_i)}{f'(r_i)}\right|_{\mathfrak{p}} \geq |\delta|_{\mathfrak{p}} \left|\frac{-f(r_i)}{f'(r_i)}\right|_{\mathfrak{p}}$.
Next, Taylor's formula also gives

$$f(r_{i+1}) = f(r_i - \frac{f(r_i)}{f'(r_i)}) = \left[f(r_i) - f'(r_i)\frac{f(r_i)}{f'(r_i)}\right] + \varepsilon\left(\frac{-f(r_i)}{f'(r_i)}\right)^2$$

with $\varepsilon \in D_{\mathfrak{p}}$. The term in brackets evaluates to zero, giving

$$|f(r_{i+1})|_{\mathfrak{p}} = \left|\varepsilon\left(\frac{-f(r_i)}{f'(r_i)}\right)^2\right|_{\mathfrak{p}} \leq \left|\left(\frac{-f(r_i)}{f'(r_i)}\right)^2\right|_{\mathfrak{p}}$$

as $|\varepsilon|_{\mathfrak{p}} \leq 1$. Dividing across the inequality by $|f'(r_{i+1})^2|_{\mathfrak{p}}$ yields

$$\left|\frac{f(r_{i+1})}{f'(r_{i+1})^2}\right|_{\mathfrak{p}} \leq \left|\left(\frac{-f(r_i)/f'(r_i)}{f'(r_{i+1})}\right)^2\right|_{\mathfrak{p}}$$

and by using our previous result

$$\left|\frac{f(r_{i+1})}{f'(r_{i+1})^2}\right|_{\mathfrak{p}} \leq \left|\left(\frac{-f(r_i)/f'(r_i)}{f'(r_i)}\right)^2\right|_{\mathfrak{p}} \leq \left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}^{2i+1}$$

by induction. Lastly, $|r_{i+1}-r_i|_{\mathfrak{p}} \leq \left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}^{2i}\left|f'(r_0)\right|_{\mathfrak{p}} < \left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}$ since $\left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}} \leq 1$ and since

$$|r_{i+1}-r_i+r_i-r_0|_{\mathfrak{p}} \leq \max\{|r_{i+1}-r_i|_{\mathfrak{p}}, |r_i-r_0|_{\mathfrak{p}}\} < \left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}$$

the third condition holds.
Putting these results together, we can show that

$$\lim_{i\to\infty}|r_{i+1}-r_i|_{\mathfrak{p}} = \lim_{i\to\infty}\left|-\frac{f(r_i)}{f'(r_i)}\right|_{\mathfrak{p}} \leq \lim_{i\to\infty}\left|\frac{f(r_i)}{f'(r_i)^2}\right|_{\mathfrak{p}}^{2i}\left|f'(r_i)\right|_{\mathfrak{p}} = 0$$

so $(r_k)_{k=0}^{\infty}$ is Cauchy and approaches a limit $\tilde{r} \in D_{\mathfrak{p}}$ since $K_{\mathfrak{p}}$ is complete and $|r_i|_{\mathfrak{p}} \leq 1$ for all i. Also,

$$f(\tilde{r}) = \lim_{i\to\infty}|f(r_i)|_{\mathfrak{p}} \leq \lim_{i\to\infty}|f'(r_i)|_{\mathfrak{p}}\left|\frac{f(r_0)}{f'(r_0)^2}\right|_{\mathfrak{p}}^{2i} = 0$$

as $|f'(r_i)|_{\mathfrak{p}}$ is constant. □

Example: (Γ) Let $\Gamma = \mathbb{Z}(i) = \{a+bi : a,b \in \mathbb{Z}\}$ denote the set of Gaussian integers and $\mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$ be its field of fractions. Define the *Gaussian norm* to be the map $N(x) = x\overline{x}$. Let it be assumed (without proof) that the Gaussian integers are a principal ideal domain and that all primes are of the form of one of the following:

(i) $a+bi$ with $b = 3 \pmod 4$ and $a = 0$

(ii) $a+bi$ with $a = 3 \pmod 4$ and $b = 0$

(iii) $a+bi$ with $a \neq b \neq 0$ and $a^2+b^2 = p$ where p is a prime in $\mathbb{Z}$

and that anything of the above form is a prime. Then $\mathfrak{p} = 2+3i$ is a prime in the Gaussian integers and there exists a completion $\mathbb{Q}(i)_{\mathfrak{p}}$ of $\mathbb{Q}(i)$ with respect to $|.|_{\mathfrak{p}}$. Given a polynomial, say $f(x) = x^2+1+3i$, over $\mathbb{Z}(i)$, we can find out if this polynomial has a solution in $\mathbb{Z}(i)_{\mathfrak{p}} = \{x \in \mathbb{Q}(i)_{\mathfrak{p}} : |x|_{\mathfrak{p}} \leq 1\}$, the valuation ring of $\mathbb{Q}(i)_{\mathfrak{p}}$.

By Hensel's lemma, this amounts to finding an $r_0 \in \mathbb{Z}[i]_{\mathfrak{p}}$ such that

$$|r_0^2+1+3i|_{\mathfrak{p}} < |(2r_0)^2|_{\mathfrak{p}}$$

and $r_0 = 1$ is clearly a suitable choice as

$$c^{-1} = |1^2+1+3i|_{\mathfrak{p}} < |(2)^2|_{\mathfrak{p}} = 1$$

for some $c > 1$. Applying the next step

$$r_1 = 1 - \frac{f(1)}{f'(1)}$$

we get $r_1 = -\frac{3}{2}i$. The next step gives

$$r_2 = -\frac{3}{2}i - \frac{-\frac{9}{4}+1+3i}{-3i} = 1 - \frac{13}{12}i$$

and continuing in this way, we may get as close as we like to some $r \in \mathbb{Z}[i]_{\mathfrak{p}}$, satisfying $f(r) = 0$. We can check this, by looking at $f(r_1) = -\frac{9}{4}+1+3i = \frac{-5+12i}{4} = \frac{-(2+3i)^2}{4}$. Since $(2+3i) \nmid 4$, $|f(r_1)|_{\mathfrak{p}} = c^{-2}$. Similarly,

$f(r_2) = (1 - \frac{13}{12}i)^2 + 1 + 3i = \frac{119+120i}{144} = \frac{-1(2+3i)^3}{144}$ and again, since $(2+3i) \nmid 144$, $|f(r_2)|_{\mathfrak{p}} = c^{-3}$.

Example: ($\mathbb{Z}(\sqrt{3})$) We claim that $\mathbb{Z}(\sqrt{3})$ is a unique factorisation domain. This follows from proving that Euclid's algorithm is applicable to the domain. Firstly, we introduce a norm function

$$\mathcal{N} : \mathbb{Z}(\sqrt{3}) \to \mathbb{Z}$$

such that

$$\mathcal{N}(a + b\sqrt{3}) = a^2 - 3b^2$$

with a, $b \in \mathbb{Z}$. Now, given any a, $b \in \mathbb{Z}(\sqrt{3})$, $\frac{a}{b} = x + y\sqrt{3}$ with x, $y \in \mathbb{Q}$. There exist m, $n \in \mathbb{Z}$ with

$$|x - m|, |y - n| \leq \frac{1}{2}$$

and so:

$$-\frac{3}{4} \leq \mathcal{N}(\frac{a}{b} - m - n\sqrt{3}) = (x-m)^2 - 3(y-n)^2 \leq \frac{1}{4}$$

and we get

$$\left|\mathcal{N}(\frac{a}{b} - m - n\sqrt{3})\right| < 1$$

and setting $q = m + n\sqrt{3}$, this shows that

$$|\mathcal{N}(a - bq)| < |\mathcal{N}(b)|$$

proving that $\mathbb{Z}(\sqrt{3})$ is a Euclidean domain and hence a UFD.

$\sqrt{3}$ is prime in $\mathbb{Z}(\sqrt{3})$ and so we obtain a completion, $\mathbb{Q}(\sqrt{3})_{\sqrt{3}}$ of the field of fractions with respect to the $\sqrt{3}$-adic metric. Let $f(x) = \sqrt{3} + (2\sqrt{3}+4)x + 6x^2 + x^3$ be a polynomial whose coefficients all lie in the valuation ring of this completion. Now $|f(r_0)|_{\sqrt{3}} < |f'(r_0)^2|_{\sqrt{3}}$ is satisfied for $r_0 = 0$ since $\sqrt{3}|f(0) = \sqrt{3}$ and $\sqrt{3} \nmid f'(0) = 2\sqrt{3}+4$. This is true since $\sqrt{3} \nmid (1+\sqrt{3})^3(\sqrt{3}-1) = 4(\sqrt{3}+2)$ and $\mathcal{N}(2+\sqrt{3}) = 1 \implies 2+\sqrt{3}$ is a unit. Therefore we can apply Hensel's lemma to find a convergent sequence

$$(r_n)_{n=0}^{\infty} \to r : r_{i+1} = r_i - \frac{f(r_i)}{f'(r_i)}$$

and $f(r) = 0$.

The first step gives

$$r_1 = \sqrt{3} - \frac{8\sqrt{3}+24}{14\sqrt{3}+13} = \frac{5\sqrt{3}+18}{14\sqrt{3}+13}$$

and reiterating gives

$$r_2 = \frac{5\sqrt{3}+18}{14\sqrt{3}+13} - \left(\frac{144+69\sqrt{3}}{14\sqrt{3}+13} + \frac{2394+1080\sqrt{3}}{757+364\sqrt{3}} + \frac{7182+1995\sqrt{3}}{10598+2785\sqrt{3}}\right)$$

and so on.

As in the case of $\mathbb{Q}_p$ successive iterations of the sequence constructed in Hensel's lemma can become time consuming to work out. To deal with this I devised a Perl script (with three supplement modules) to extend p-adic analysis to the case of Γ. One possible method to have done this would have used Perl's `Math::Complex` module, however, the representations of rationals as decimals would have been unsuited to the situation, as the aim of the code should be to provide insight into Hensel's lemma, rather than generate approximants to real roots of polynomials. To ensure that the algorithm remains accurate in the rationals (i.e $\frac{1}{3}$ is never represented as $\frac{3333...333}{10000...000}$), there are three modules to accompany the main script: `polynomial.pm`, `complex.pm`

and `rational.pm`.

`rational.pm` overloads the operations of `+,-,/,*` and `""` to represent numbers in their numerator-denominator fashion, rather than that of a decimal. It includes a new class, created with the command `new rational(numerator, denominator)`. The operations are overloaded in the obvious way, with `""` interpretting a rational to be `"(numerator/denominator)"` for passing to `print`, except in the case that the numerator is 0 (returns `"0"`) or the denominator is 1 (returns `"denominator"`. A `gcd()` function is also included and used with the arithmetic operators to keep a rational in its lowest terms.

`complex.pm` overloads the above operators for complex numbers and includes a class initialised with `new complex(real,imaginary)`. `""` now interprets an object of this class as `"real+imaginary*i"`. It also includes `pow(number,power)`, an exponentiation function (n.b. this can only be used if the real and imaginary coefficients are rationals from the above package) and a `norm()` function that returns the product of a Gaussian rational with its conjugate.

`polynomial.pm` contains functions `f(coefficients, x)` and `f_derivative (coefficients, x)` that evaluates a polynomial determined by `coefficents` for a value `x`. It also, perhaps unsuited to its name, contains a function `extract()` that takes a complex rational $\frac{a}{b}+\frac{c}{d}i$ as its argument and returns an array of the values `(a, b, c, d)`. The final, and most *ad hoc*, function in `polynomial.pm` is `prime_valuation`. This function takes a complex number and a Gaussian prime as its arguments and returns $\mathrm{ord}_p(\text{numerator})-\mathrm{ord}_p(\text{denominator})$ where p is the prime in question. This is used to check the prerequisite condition of Hensel's lemma.

The main script takes the arguments determining the polynomial from the command line. It requires an argument of the form:

$$a_1,a_2,a_3,a_4\ \ b_1,b_2,b_3,b_4\ldots$$

where the corresponding polynomial is

$$\frac{a_1}{a_2}+\frac{a_3}{a_4}i+\left(\frac{b_1}{b_2}+\frac{b_3}{b_4}i\right)x\ldots$$

and so on. The user is then prompted to input a number in the form `a,b` (corresponding to $a+bi$), which is checked for primality in Γ, using the same criteria in the example above. If the number passes the test, the user is prompted for a number of the form `a,b,c,d` (corresponding to $\frac{a}{b}+\frac{c}{d}i$) as an approximate root to the polynomial. The condition of Hensel's lemma is checked and, if the root is suitable, the user is prompted for the number of desired iterations and the Cauchy sequence constructed in Hensel's lemma is generated to that number of iterations. The sequence is then printed to the screen.

Using the example from above, the programme outputs:

>./hensel_gaussian.pl 1,1,3,1 0,1,0,1 1,1,0,1

Please enter a Gaussian prime (in the form 'a,b' where the prime is a+bi):
2,3
Please enter an approximate root of the polynomial [(a,b,c,d)]
1,1,0,1
A root exists!
How many iterations?
5
0+(-3/2)*i

1+(-13/12)*i
(637/626)+(-11125/7512)*i
(757378333/728785444)+(-12615897541/8745425328)*i
(2011034665637538323965/1934099440191212213576)
+(-3348193535987763831613 3/23209193282294546562912)*i

and this corroborates the sequence obtained by hand above. With increasing iterations, the lines of output become quite long and difficult to deal to read, so the number of iterations should be kept small.

8 Conclusion

I will conclude with some closing remarks regarding important topics that were not touched upon in this project.

As Hensel's lemma showed, $\mathbb{Q}_p$, though complete, is not an algebraically closed field. However, such a field can be obtained from adding the roots of polynomials with p-adic coefficients and we can extend the non-Archimedean valuation $|.|_p$ to the closure, $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ by extending it individually to finite field extensions. Suppose $\mathbb{Q}_p(\tau)$ is one such extension. Then we define a mapping $\nu : \mathbb{Q}_p(\tau) \to \mathbb{Q}_p$ using any of the three following formulations (p. 60, Koblitz [3]):

(i) Let $A : \mathbb{Q}_p(\tau) \to \mathbb{Q}_p(\tau)$ be the $\mathbb{Q}_p$-linear map given by $Ax = \tau x$. Then $\nu(\tau) = \det(A)$.

(ii) $\nu(\tau) = (-1)^n a_n$ where n is the degree of the monic polynomial that τ satisfies and $a_n \in \mathbb{Q}_p$ is the constant term of this polynomial.

(iii) $\nu(\tau) = \prod_{i=1}^{n} \tau_i$ where each τ_i is a conjugate of $\tau_1 = \tau$ over $\mathbb{Q}_p$.

We may then set $||x||_p = |\nu(x)|_p$ for $x \in \overline{\mathbb{Q}}_p$ and check the necessary details to show that the resulting valuation is a well-defined, non-Archimedean extension of $|.|_p$. After extending this valuation to the whole of $\overline{\mathbb{Q}}_p$ and using it to complete the field, we obtain a complete and algebraically closed field, Ω_p, the p-adic analogue of the complex numbers.

The Hasse-Minowski principle, which applies to certain families of polynomials, such as quadratic forms, states that suitable polynomials are solvable over the rational numbers if and only if they are solvable in $\mathbb{Q}_p$ for each prime p as well as $\mathbb{R}$. This principle is also known as the local-global principle because it suggests that local structures (i.e. the completions) give insight into global structures like $\mathbb{Q}$ and its quadratic extensions.

As a last note, I would like to express my sincere thanks to my supervisor, Dr. David Wilkins, who has been immeasurably helpful in providing direction, discussion and food for thought throughout the course of the project.

A Code for Hensel's Lemma

```
#! /usr/bin/perl
use warnings;
use bignum;
use strict;

###
# A program applying Hensel's lemma to determine
# whether the square root of
# a number lies in the p-adic completion of the rational numbers.
###

our $polynomial_degree = $#ARGV;
our @a;
my $i;
our $sum = 0;
my $m;
my $q = 0;

print "Please enter number of iterations:\n";
our $iterations = <STDIN>;
chomp($iterations);
unless ($iterations =~ /^[+-]?\d+$/ )
{
 print "This is not a number!\n";
 exit;
}

print "Please enter your prime:\n";
our $prime = <STDIN>;
chomp($prime);
unless ($prime =~ /^[+-]?\d+$/ )
{
 print "This is not a number!\n";
 exit;
}

&cauchy_sequence($iterations);

print "{($a[0]";
for($i=1; $i< $iterations; $i++)
{
 print "), ";
 if($q >= 10)
 {
  print "\n";
  $q = 0;
 }
 for($m = 0; $m <= $i; $m++)
 {
  if($m != 0)
  {
   print "$a[$m]*$prime^$m";
   if($m != $i)
   {
print " + ";
   }
  }
  else
  {
   print "($a[$m] + ";
  }
   $q++;
 }
```

```
}
print ")...}\n";

sub cauchy_sequence
{
 my $k;
 my $j;
 my $n = 0;

 if ((not defined($a[$_[0]])) && ($_[0] != 0))
{
 &cauchy_sequence($_[0]-1);
}

unless($_[0] == 0)
{
 $sum += $a[$_[0]-1]*($prime**($_[0]-1));
}

for($k=0; $k < $prime; $k++)
{
 my $supersum = 0;
 for($n = 0; $n < $polynomial_degree +1; ++$n)
{
 $supersum += $ARGV[$n]*($sum + $k*$prime**$_[0])**$n;
}

 if($supersum%($prime**($_[0]+1)) == 0)
{
 $a[$_[0]] = $k;
 last;
}
}

if(not defined $a[0])
{
 print "The root of the polynomial is not in the
 $prime-adic completion of the rationals.\n";
 exit;
}
}
```

```
#! /usr/bin/perl

###
# A program to check Hensel's lemma for the field of
# fractions of the Gaussian integers
# and generate the corresponding Cauchy sequence
###

use strict;
use warnings;
use rational;
use polynomial;
use complex;
use bignum;

my @a;
my @b;

for(my $k = 0; $k <= $#ARGV; $k++)
{
 @a = (split/,/, $ARGV[$k]);
 if(scalar(@a) != 4)
 {
  print "Invalid polynomial format\n";
  exit;
 }
 push (@b, new complex(new rational($a[0],$a[1]),
 new rational($a[2],$a[3])));
}


my @prime_array;
my $instring;
my $real_part;
my $imag_part;
my $check;
my $i;
my $j;
my @array;

print "Please enter a Gaussian prime (in the form
'a,b' where the prime is a+bi):\n";
while(not defined($check))
{
$instring = <STDIN>;
chomp($instring);
@prime_array = split(/,/, $instring);
if(scalar(@prime_array != 2))
 {
  print "Please enter a number in the form specified!\n";
 }
else
 {
  $check++;
 }
}

$real_part = $prime_array[0];
$imag_part = $prime_array[1];

unless($real_part =~ /^[+-]?\d+$/ && $imag_part =~ /^[+-]?\d+$/)
{
 print "Non-numerical entry\n" and die $!;
}
```

```
if($imag_part != 0 && $real_part != 0)
{
 $check = $real_part*$real_part + $imag_part*$imag_part;
 if(&check_prime($check) != 1)
 {
  print "Number is not prime!\n";
  exit;
 }
}
elsif($imag_part == 0 && (abs($real_part)%4 == 3) &&
&check_prime(abs($real_part)))
{
}
elsif($real_part == 0 && (abs($imag_part)%4 == 3) &&
&check_prime(abs($imag_part)))
{
}
else
{
 print "Number is not prime!\n";
 exit;
}

my $prime = new complex(new rational($real_part,1),
new rational($imag_part,1));

$check = 0;
while($check == 0 )
{
 print "Please enter an approximate root of the polynomial [(a,b,c,d)]\n";
 our $root = <STDIN>;
 chomp($root);
 @array = split(/,/, $root);
 if(scalar(@array != 4))
 {
  print "Please enter number in the form specified!\n";
 }
 else
 {
 $check++;
 }
}
our $root = new complex(new rational($array[0],$array[1]),
new rational($array[2],$array[3]));


if ((polynomial::prime_valuation(
polynomial::f(@b, $root), $prime)) >
(polynomial::prime_valuation
(complex::pow(polynomial::f_derivative(@b, $root),2), $prime)))
{
print "A root exists!\n";
}
else
{
print "A root may not exist\n";
exit;
}


my @sequence;
print "How many iterations?\n";
my $iterations = <STDIN>;
chomp($iterations);
$root = new complex(new rational($array[0],$array[1]),
```

```
new rational($array[2],$array[3]));
for($i = 0; $i < $iterations; $i++)
{
$root = $root - polynomial::f(@b, $root)/
polynomial::f_derivative(@b, $root);
push (@sequence, $root);
}


foreach(@sequence)
{
 print "$_\n";
}

sub check_prime
{
 for($i = 0; $i <= $_[0]; $i++)
 {
  push(@array, $i)
 }

 for($i = 2; $i <= sqrt($_[0]); $i++)
 {
  unless($array[$i] = 0)
  {
   for($j = 1; $i*$j <= $_[0]; $j++)
   {
    $array[$i*$j] = 0;
   }
  }
 }
 if($array[$_[0]] == 0)
 {
  return 0;
 }
 else
 {
 return 1;
 }
}
```

```
#! /usr/bin/perl
use strict;
use warnings;
use bignum;

# A package to represent rational numbers

package rational;

sub new {
 my $class = shift;
 my $number =
 {
  _numerator => shift,
  _denominator => shift,
 };
 bless $number, $class;
}

sub gcd {
 my $a;
 my $b;
 if(abs($_[0]) > abs($_[1]))
 {
  $a = abs($_[0]);
  $b = abs($_[1]);
 }
 elsif(abs($_[1]) > abs($_[0]))
 {
  $a = abs($_[1]);
  $b = abs($_[0]);
 }
 else
 {
  return abs($_[0]);
 }
 if($b == 0)
 {
  return 0;
 }
  while($b != 0)
  {
   ($b, $a) = ($a % $b, $b);
  }
 return $a;
}

sub as_string {
if($_[0]{_numerator} == 0)
{
 return "0";
}

if($_[0]{_denominator} == 1)
{
 return "$_[0]{_numerator}";
}
 my $numerator = $_[0]{_numerator}/
 &gcd($_[0]{_numerator}, $_[0]{_denominator});
 my $denominator = $_[0]{_denominator}/
 &gcd($_[0]{_numerator}, $_[0]{_denominator});
 return "($numerator/$denominator)";
}
use overload ('""' => 'as_string');
```

```
sub add_rational {
 my $denominator = $_[0]{_denominator}*$_[1]{_denominator};
 my $numerator = $_[0]{_denominator}*$_[1]{_numerator} +
 $_[1]{_denominator}*$_[0]{_numerator};

 if(&gcd($numerator, $denominator) != 0)
 {
 return new rational($numerator/&gcd($numerator, $denominator),
 $denominator/&gcd($numerator, $denominator));
 }
 else
 {
 return new rational(0,1);
 }
}

use overload ('+' => 'add_rational');

sub subtract_rational {
 my $denominator = $_[0]{_denominator}*$_[1]{_denominator};
 my $numerator = $_[1]{_denominator}*$_[0]{_numerator}-
 $_[0]{_denominator}*$_[1]{_numerator};
 unless(&gcd($numerator, $denominator) == 0)
 {
  return new rational($numerator/&gcd($numerator, $denominator),
  $denominator/&gcd($numerator, $denominator));
 }
 else
 {
  return new rational(0,1);
 }
}

use overload ('-' => 'subtract_rational');

sub divide_rational {
 my $numerator = $_[0]{_numerator}*$_[1]{_denominator};
 my $denominator = $_[1]{_numerator}*$_[0]{_denominator};
 return new rational($numerator, $denominator);
}

use overload('/' => 'divide_rational');

sub multiply_rational {
 my $numerator = $_[0]{_numerator}*$_[1]{_numerator};
 my $denominator = $_[1]{_denominator}*$_[0]{_denominator };
unless(&gcd($numerator, $denominator) == 0)
 {
  return new rational($numerator/&gcd($numerator, $denominator),
  $denominator/&gcd($numerator, $denominator));
 }
 else
 {
  return new rational(0,1);
 }
}

use overload ('*' => 'multiply_rational');

sub pow {
 my $product = new rational(1,1);
 for(my $i = 0; $i < $_[1]; $i++)
 {
  $product = $product*$_[0];
 }
```

```
 return $product;
}

sub extract_integers {
return ($_[0]{_numerator}, $_[0]{_denominator});
}

1;
```

```
 # /usr/bin/perl

use strict;
use warnings;

# A package to represent complex numbers

package complex;

sub new
{
 my $class = shift;
 my $number =
 {
  _real => shift,
  _imag => shift,
 };
 bless $number, $class;
}

sub complex_string {
 my $real = $_[0]{_real};
 my $imag = $_[0]{_imag};
 return "$real+$imag*i";
}

use overload ('""' => 'complex_string');

sub add_complex {
return new complex($_[0]{_real} + $_[1]{_real},
$_[0]{_imag} + $_[1]{_imag} );
}

use overload ('+' => 'add_complex');

sub subtract_complex {
return new complex($_[0]{_real} - $_[1]{_real},
$_[0]{_imag} - $_[1]{_imag} );
}

use overload ('-' => 'subtract_complex');

sub multiply_complex {
return new complex(($_[0]{_real}*$_[1]{_real} -
$_[0]{_imag}*$_[1]{_imag}),
($_[0]{_real}*$_[1]{_imag}+$_[1]{_real}*$_[0]{_imag}));
}

use overload ('*' => 'multiply_complex');

sub divide_complex {

return new complex(
  ($_[0]{_real}*$_[1]{_real})/
  ($_[1]{_real}*$_[1]{_real} + $_[1]{_imag}*$_[1]{_imag})
+ ($_[0]{_imag}*$_[1]{_imag})/
  ($_[1]{_real}*$_[1]{_real} + $_[1]{_imag}*$_[1]{_imag})
,
  ($_[0]{_imag}*$_[1]{_real})/
  ($_[1]{_real}*$_[1]{_real} + $_[1]{_imag}*$_[1]{_imag})
- ($_[1]{_imag}*$_[0]{_real})/
  ($_[1]{_real}*$_[1]{_real} + $_[1]{_imag}*$_[1]{_imag})
);
}
```

```
use overload ('/' => 'divide_complex');

sub pow {
 my $product = new complex(new rational(1,1) , new rational(0,1));
 for(my $i = 0; $i < $_[1]; $i++)
 {
  $product = $product*$_[0];
 }
 return $product;
}


sub extract_rationals {
return($_[0]{_real}, $_[0]{_imag});
}


sub norm {
$_[0]{_real}*$_[0]{_real} + $_[0]{_imag}*$_[0]{_imag};
}
1;

 # /usr/bin/perl

#A package to check values of polynomials

use warnings;
use strict;
use bignum;

package polynomial;

sub f {
 my $sum = new complex(new rational(0 , 1), new rational(0 , 1));
 for(my $i = 0; $i < scalar(@_) -1; $i++)
 {
  $sum += complex::pow($_[scalar(@_)-1] , $i)*$_[$i];
 }
 return $sum;
}

sub f_derivative {
 my $sum = new complex(new rational(0 , 1), new rational(0 , 1));
 for(my $i = 1; $i < scalar(@_) -1; $i++)
 {
  $sum += complex::pow($_[scalar(@_)-1] , $i-1)*$_[$i]
  *(new complex(new rational($i,1), new rational(0,1)));
 }
 return $sum;
}

sub extract {
my @a;
my @c;
@a = complex::extract_rationals($_[0]);
foreach(@a)
{
 push(@c, rational::extract_integers($_));
}
return @c;
}

sub prime_valuation {
my $upstairs_count = 0;
my $downstairs_count = 0;
```

```
our @temparray = &extract($_[0]);
my $upstairs = new complex(new rational
($temparray[0]*$temparray[3],1),
new rational($temparray[2]*$temparray[1],1));
my $downstairs = new complex(new rational
($temparray[1]*$temparray[3],1),
 0, 1);
$upstairs = $upstairs/$_[1];
@temparray = extract($upstairs);
while($temparray[1] == 1 && $temparray[3] == 1)
{
$upstairs = $upstairs/$_[1];
@temparray = extract($upstairs);
$upstairs_count++;
}
$downstairs = $downstairs/$_[1];
@temparray = &extract($downstairs);
while($temparray[1] == 1 && $temparray[3] == 1)
{
$downstairs = $downstairs/$_[1];
@temparray = &extract($downstairs);
$downstairs_count++;
}
return $upstairs_count - $downstairs_count;
}

sub valuation {
my $check = complex::norm($_[0]);
our @temparray = rational::extract_integers($check);
print complex::norm($_[0]);
my $valuation = -1;
while($temparray[1] == 1)
{
$check = $check/complex::norm($_[1]);
$valuation++;
@temparray = rational::extract_integers($check);
}
return $valuation;
}
1;
```

References

[1] Andrew Baker, *An Introduction to p-adic Numbers and p-adic Analysis*, 2011, available at http://www.maths.gla.ac.uk/~ajb/dvi-ps/padicnotes.pdf

[2] Z.I. Borevič and I.R. Shafarevič, *Number Theory*, Academic Press, 1966.

[3] Neal Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Springer-Verlag, 1977

[4] Fernando Q. Gouvêa, *p-adic Numbers: An Introduction*, Springer-Verlag, 1993.

[5] William Stein, *Algebraic Number Theory, a Computational Approach*, 2010 available at http://modular.math.washington.edu/books/ant/ant.pdf.