p-adic numbers and the Hasse-Minkowski Theorem

Tahseen Rabbani

Abstract

Given a polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, determing the existence of integral roots is a standard topic covered in an introductory number theory course. In this paper, we will extend our considerations to roots in $\mathbb{Q}$. Using p-adic numbers, the existence of rational solutions can be readily acertained under select conditions, especially for quadratic forms.

1 Introduction

Let p be a prime number. For any integer, x, we can represent it in base p as a power series expansion, that is,

$$x = \sum_{n=0}^{k} a_n p^n \tag{1}$$

where $a_n \in [0, p-1]$ and there exists some N, such that for all $n > N$, $a_n = 0$. We call such a representation a p-adic expansion. As we will see shortly, it is convenient to denote the p-adic expansion of an integer as a decimal, $\ldots a_m \ldots a_2 a_1 a_0$, where a_m is the last positive coefficient in the series representation. There is a one-to-one correspondence between the series representation and decimal representation. Furthermore, such p-adic expansions over $\mathbb{Z}$ preserve addition and multiplication, that is, if $(x)_p$ denotes the p-adic expansion of $x \in \mathbb{Z}$, we have that for x, $y \in \mathbb{Z}$, $(x+y)_p$=$((x)_p$+$(y)_p)_p$ and $(x \cdot y)_p$=$((x)_p(y)_p)_p$.

Addition and multiplication of two p-adic expansions proceeds componentwise, ensuring coefficients are in $[0, p-1]$ by "carrying" any term p^n with coefficient $a_n > p-1$ to higher powers of p. We present examples of both operations.

1.1 Addition

Let $p = 7$. Consider $x = 6 + 6 \cdot 7 + 6 \cdot 7^2 + 0 \cdot 7^3 + 0 \cdot 7^4 + \dots$ and $y = 1 + 0 \cdot 7 + 0 \cdot 7^2 + 0 \cdot 7^3 + \dots$ After converting both numbers to their respective decimal representations, addition proceeds as follows:

$$\begin{array}{rr} & \overset{1\,1\,1}{} \\ & \dots 00666 \\ + & \dots 00001 \\ \hline & \dots 01000 \end{array}$$

Which, converting back to series representation, yields the representation of 0 in the 7-adic's.

1.2 Multiplication

Let $p = 3$. We will find the 3-adic representation of 200 by calculating $20 \cdot 10$ in base 3.

Note that $20 = 2+0\cdot3+2\cdot3^2+0\cdot3^3+\dots$ and $10 = 1+0\cdot3+1\cdot3^2+0\cdot3^3+\dots$, so we have

$$\begin{array}{rr} & \dots 00202 \\ \times & \dots 00101 \\ \hline & \overset{1}{\dots} 00202 \\ & +\dots 00000 \\ & +\dots 20200 \\ \hline & \dots 21102 \end{array}$$

Converting back to a series a representation, we find that $2 + 0 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 = 200$.

1.3 Representation of -1

Given that p-adic expansions preserve multiplication in $\mathbb{Z}$, we simply need to derive the p-adic expansion of -1 to acquire the p-adic expansions of negative integers. By preservation of addition, we should have that

$$((1)_p + (-1)_p)_p = \sum_{n=0}^{\infty} 0 \cdot p^n$$

This implies we should have a contiuous carry to the right. So, $-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \dots$, since,

$$\underbrace{1+(p-1)}+(p-1)\cdot p+(p-1)\cdot p^2+(p-1)\cdot p^3+\ldots=$$
$$=\underbrace{p+(p-1)p}+(p-1)p^2+(p-1)p^3+\ldots$$
$$=\underbrace{p^2+(p-1)p^2}+(p-1)p^3+\ldots$$
$$=\ldots$$
$$=0$$

1.4 $\mathbb{Z}_p$

It is clear any power series representation of an integer base p must terminate at some finite power of p. However, if one allows for infinite series (with index ≥ 0), the class of p-adic integers are obtained.

Definition 1.1 *Let p be a prime number. The p-adic integers consists of the set*

$$\mathbb{Z}_p = \{\sum_{n=0}^{\infty} a_n p^n : 0 \leq a_n \leq p-1\} \tag{2}$$

It is clear that every integer's p-adic representation is in $\mathbb{Z}_p$. However, one may also find the p-adic representation of non-integral rational numbers in $\mathbb{Z}_p$. For example, in base 5

$$\frac{-1}{4} = \frac{1}{1-5} = 1+5+5^2+5^3+\ldots$$

which is clearly in $\mathbb{Z}_p$. Note that this derivation is a simple application of the sum formula for infinite geometric series. With respect to carry-over addition and multiplication as previously defined, $\mathbb{Z}_p$ forms a ring and the p-adic representations of $\mathbb{Z}$ form a subring of $\mathbb{Z}_p$.

1.5 Representation of Rational Numbers

So far we have discussed p-adic expansions of the integers and rational numbers which strictly assume positive powers of p in their representations. However, we can generalize and allow for terms which contain negative powers of p, in which case, we can uniquely represent every element of $\mathbb{Q}$. It is important to note that p-adic expansions of rational numbers preserve multiplication and addition in $\mathbb{Q}$, and addition/multiplication over these expansions proceeds in the same manner as described before, maintaining the notion of digit "carrying." With these facts in mind, we will determine the coefficients in the p-adic expansion of an arbitrary rational number.

Definition 1.2 *Let p be a prime number. The p-adic valuation of $\mathbb{Z}$*

$$v_p : \mathbb{Z} - \{0\} \to \mathbb{Z}$$

is defined as the following: for $x \in \mathbb{Z} - \{0\}$, $v_p(x) = n \in \mathbb{N}$, such that $x = p^n x'$ and $p \nmid x'$. The p-adic valuation on $\mathbb{Z}$ is more commonly known as $ord_p(x)$. We may extend v_p to $\mathbb{Q}$ by letting $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ for $\frac{a}{b} \in \mathbb{Q}$, $\frac{a}{b} \neq 0$.

By convention, we let $v_p(0) = +\infty$.

Example We calculate $v_7(56/29)$.

$56 = 7 \cdot 8$ and $29 = 7^0 \cdot 29$. So,

$$v_7(56/29) = v_7(56) - v_7(29) = 1 - 0 = 1$$

With v_p at our disposal, we describe a procedure to determine the p-adic coefficients of a fraction $\neq 0$.

For $x \in \mathbb{Q}$, if $n_0 = v_p(x)$, then $x = \sum_{n=n_0}^{\infty} a_n p^n$, where $0 \leq a_n \leq p - 1$.

$$\begin{aligned} x &= a_{n_0} p^{n_0} + a_{n_0+1} p^{n_0+1} + a_{n_0+2} p^{n_0+2} + \dots \\ &= p^{n_0}(a_{n_0} + a_{n_0+1} p + a_{n_0+2} p^2 + \dots) \\ &= p^{n_0} \cdot \frac{x_1}{y_1} \end{aligned}$$

where $p \nmid x_1$, $p \nmid y_1$, and $\gcd(x_1, y_1)$=1. Then,

$$\frac{x_1}{y_1} = a_{n_0} + a_{n_0+1} p + a_{n_0+2} p^2 + \dots$$

Reducing modulo p,

$$\begin{aligned} x_1 \cdot y_1^{-1} &\equiv a_{n_0} + a_{n_0+1} p + a_{n_0+2} p^2 + \dots \mod p \\ &\equiv a_{n_0} \end{aligned}$$

Having solved for a_{n_0} , we have

$$\begin{aligned} \frac{x_1}{y_1} - a_{n_0} &= p(a_{n_0+1} + a_{n_0+2} p + a_{n_0+3} p^2 + \dots) \\ &= p \cdot \frac{x_2}{y_2} \end{aligned}$$

where $p \nmid x_2$, $p \nmid y_2$, and $\gcd(x_2, y_2)$=1. Then,

$$\frac{x_2}{y_2} = a_{n_0+1} + a_{n_0+2} p + a_{n_0+3} p^2 + \dots$$

Reducing modulo p,

$$\begin{aligned} x_2 \cdot y_2^{-1} &\equiv a_{n_0+1} + a_{n_0+2}p + a_{n_0+3}p^2 + \dots \mod p \\ &\equiv a_{n_0+1} \end{aligned}$$

At first glance,this procedure seems rather useless in presenting a concise series or decimal representation of a rational number for which the expansion contains infinitely many non-zero terms, but in fact, the p-adic expansion of a rational number has repeating digits, so we continue this process so forth until the period is discovered, and appropriately denote the expansion as a repeating decimal (or series).

Proposition 1.3 *If $x \in \mathbb{Q}$, then the p-adic expansion of x has repeating coefficients.*

Proof. If we can show for $x = \frac{a}{b} \in \mathbb{Q}$ that

$$x = c + \frac{d}{1 - p^r}$$

for c, $d \in \mathbb{Z}^+$, then we shall have the desired conclusion, since the p-adic expansion of c and d will have a finite number of nonzero terms, and the p-adic expansion of $\frac{1}{1-p^r}$ has repeating coefficients (to see this, derive this expansion as a geometric series).

We consider the scenario where $p \nmid b$ since if p does divide b and $b = p^r b'$, then we analyze a/b' and the extra factor of $1/p^r$ will not eliminate the possibility of repeating coefficients (since its p-adic expansion only has one non-zero term). So let $-1 \leq a/b \leq 0$, since if this is not the case, we can add an integer, j, such that $a/b + j$ is between -1 and 0, and since j has a finite nonzero expansion, this will not change the possibility of the repeating coefficients.

Now we consider $\mathbb{Z}/b\mathbb{Z}$. Since $p \nmid b$, we have that the order of p in $\mathbb{Z}/b\mathbb{Z}$ is b, so there exists m, $n > 0$ such that $p^m \equiv p^n \mod b$. Without loss of generality, let $m > n$, then $p^{m-n} \equiv 1 \mod b$, hence there is a d such that $db = p^{m-n} - 1$. Thus,

$$x = \frac{a}{b} = \frac{ad}{bd} = \frac{-ad}{1 - p^{m-n}}$$

. Hence, $x = \frac{a}{b}$ must have a repeating expansion. ∎

Since every rational number has a repeating p-adic expansion, the algorithm presented above would be used to derive coefficients until the period is exhibited.

2 The Field of p-adic Numbers

A complete characterization of the p-adic numbers,

$$\mathbb{Q}_p = \{\sum_{n=n_0}^{\infty} a_n p^n : n_0 \in \mathbb{Z}, 0 \leq a_n \leq p-1\} \tag{3}$$

In other words, $\mathbb{Q}_p$ is the set of all finite-tailed Laurent series in powers of p. By finite-tailed, we mean the expansion is finite to the left. With respect to addition and multiplication as described before ("carrying"), $\mathbb{Q}_p$ forms a field. We would, however, like to describe the topology of $\mathbb{Q}_p$. To do this, we will first develop an absolute value for the p-adic numbers.

2.1 The p-adic absolute value

An absolute value for a field $\mathbb{K}$ is a function $|\cdot| : \mathbb{K} \to \mathbb{R}_+$ which satisfies the following,

i) $|x| = 0 \Leftrightarrow x = 0$

ii) $|xy| = |x||y|$ for all x,y $\in \mathbb{K}$

iii) $|x + y| \leq |x| + |y|$ for all x,y $\in \mathbb{K}$

Furthermore, an absolute value is called non-archimidean if,

iv) $|x + y| \leq \max\{|x|, |y|\}$ for all x,y $\in \mathbb{K}$. It is clear that this property implies iii), hence this is a stronger condition.

Definition 2.1 *Let $\mathbb{K}$ be a field and $|\cdot|$ an absolute value over $\mathbb{K}$. The distance between two elements x,y $\in \mathbb{K}$, is defined as $d(x, y) := |x - y|$. We call this distance function the metric induced by $|\cdot|$.*

Definition 2.2 *For $x \in \mathbb{Q}$, the p-adic absolute value, $|\cdot|_p$, of x is defined as follows,*

$$|x|_p = p^{-v_p(x)}$$

if $x \neq 0$, and $|0|_p = 0$.

Lemma 2.3 *$|\cdot|_p$ defines a non-archimedean absolute value on $\mathbb{Q}$.*

Proof. For the first property of an absolute value, $|0|_p = 0$ by definition, and for a nonzero $x \in \mathbb{Q}$, it is not possible for $p^{-v_p(x)} = 0$ since p is nonzero. For the second property, let x,$y \in \mathbb{Q}$. Then, $|x|_p|y|_p = p^{-v_p(x)-v_p(y)}$. By the Fundamental Theorem of Arithmetic, $v_p(xy) = v_p(x) + v_p(y)$, so $|xy|_p = p^{-v_p(x)-v_p(y)} = |x|_p|y|_p$. Next, we show $|\cdot|_p$ is non-archimedean, which will subsequently induce property iii). If $x = 0$, $y = 0$, or $x + y = 0$ then

property iv) clearly follows. So let $x = \frac{a}{b}$, $y = \frac{c}{d}$, $x + y = \frac{ad+bc}{bd}$ and

$$\begin{aligned} v_p(x+y) &= v_p(ad+bc) - v_p(b) - v_p(d) \\ &\geq \min(v_p(ad), v_p(bc)) - v_p(b) - v_p(d) \\ &= \min(v_p(ad), v_p(bc)) - v_p(b) - v_p(d) \\ &= \min(v_p(a) - v_p(b), v_p(c) - v_p(d)) \\ &= \min(v_p(x), v_p(y)) \end{aligned}$$

So,

$$\begin{aligned} |x+y|_p &= \frac{1}{p^{v_p(x+y)}} \\ &\leq \frac{1}{p^{\min(v_p(x), v_p(y))}} \\ &= \max(|x|_p, |y|_p) \end{aligned}$$

Hence, $|\cdot|_p$ is a non-archimedean absolute value. ∎

2.2 A Completion of $\mathbb{Q}$ to $\mathbb{Q}_p$

Definition 2.4 *Let $\mathbb{K}$ be a field and $|\cdot|$ and absolute value over $\mathbb{K}$. A sequence of elements x_n is called a Cauchy sequence if for all $\epsilon > 0$, there exists an $M \in \mathbb{N}$ such that for all n,m $\geq M$, $|x_n - x_m| < \epsilon$. We refer to $\mathbb{K}$ as **complete** if every Cauchy sequence of elements in $\mathbb{K}$ has a limit.*

$\mathbb{Q}$ is not complete with respect to the standard absolute value. To see this, note that we can construct a sequence converging to $\sqrt{2}$. In fact, $\mathbb{R}$ is a completion of $\mathbb{Q}$ with respect to the standard absolute value. We will see that with respect to $|\cdot|_p$, $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$.

Definition 2.5 *Let $|\cdot|_p$ be the p-adic absolute value on $\mathbb{Q}$. Let $\mathcal{C}$ (or $\mathcal{C}_p(\mathbb{Q})$) denote the set of all Cauchy sequences in $\mathbb{Q}$ with respect to $|\cdot|_p$.*

$$\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) = \{(x_n) : (x_n) \text{ is a Cauchy sequence with respect to } |\cdot|_p\}$$

Proposition 2.6 *Defining*

$$(x_n) + (y_n) = (x_n + y_n)(x_n) \cdot (y_n) = (x_n y_n)$$

turns $\mathcal{C}$ into a commutative ring with unity.

We can embed $\mathbb{Q}$ in $\mathcal{C}$ simply by sending a rational x to the constant sequence (x) in $\mathcal{C}$. We have yet to develop a machinery by which we are able to classify sequences which converge to the same limit as equivalent. The development of a particular quotient ring will help achieve this.

Definition 2.7 *Let $\mathcal{N} \subset \mathcal{C}$ be the ideal*

$$\mathcal{N} = \{(x_n) : x_n \to 0\} = \{(x_n) : \lim_{x\to\infty} |x|_p = 0\}.$$

Lemma 2.8 *$\mathcal{N}$ is a maximal ideal of $\mathcal{C}$.*

To "mod out" equivalent sequences in $\mathcal{C}$, we simply take the quotient of the ring $\mathcal{C}$ by its ideal $\mathcal{N}$. Since $\mathcal{N}$ is maximal, this will form a field. In fact, we define

$$\mathbb{Q}_p = \mathcal{C}\,/_{\mathcal{N}}$$

This refined construction of $\mathbb{Q}_p$ represents a completion of $\mathbb{Q}$ to $\mathbb{Q}_p$. We will not present a complete algebraic argument for this fact.

3 Local-Global Principle

Given an equation $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, finding roots in $\mathbb{Z}$ is a standard question in Diophantine analysis. A natural extension of this question is whether roots exist in $\mathbb{Q}$. The development of p-adic numbers helped to define existence criterion in regards to this question. The local-global principle asserts that the existence or nonexistence of roots to such equations in $\mathbb{Q}$ (global) can be detected by searching for roots in $\mathbb{Q}_p$ for $p \leq \infty$. By convention, $\mathbb{Q}_\infty = \mathbb{R}$.

It simple to embed $\mathbb{Q}$ in $\mathbb{Q}_p$. Simply send a rational x to its p-adic expansion. It immediately follows that if there is no solution in $\mathbb{Q}_p$ for some p, then there is no solution in $\mathbb{Q}$. The converse, however, is not true. As an example, we will show $(X^2-2)(X^2-17)(X^2-34)$ has a root in $\mathbb{Q}_p$ for $p \leq \infty$ but not in $\mathbb{Q}$. Before we explicitly show this, an important theorem is established.

Definition 3.1 *The p-adic integers is defined as the set*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \geq 1\}$$

Equivalently, this set consists entirely of expansions with no negative powers of p.

Theorem 3.2 *(Hensel's Lemma) Let $f(X) \in \mathbb{Z}_p[X]$ and $\alpha \in \mathbb{Z}_p$ satisfy the following conditions,*

$$f(\alpha) \equiv 0 \mod p$$

and

$$f'(\alpha) \not\equiv 0 \mod p$$

where $f'(X)$ is the formal derivative of $f(X)$. Then there exists an α_1 such that $f(\alpha_1) \equiv 0$ and $\alpha_1 \equiv \alpha \mod p$.

Lemma 3.3 *We may replace the second condition of Hensel's lemma, $f'(\alpha) \not\equiv 0 \mod p$, with the weaker condition $|F(\alpha_1)|_p < |F'(\alpha_1)_p|^2$.*

Example $(X^2-2)(X^2-17)(X^2-34)$ has roots in $\mathbb{Q}_p$ for $p \leq \infty$, but no roots in $\mathbb{Q}$.

Case 1 $\mathbb{Q}_p$ for $p \neq 2, 17$

For such p, if 2 or 17 is a square modulo p, then we have an α in $\mathbb{Z}_p$ such that $\alpha^2 - 2$ (or $\alpha^2 - 17$) $\equiv 0 \mod p$. Furthermore, $f'(\alpha) = 2\alpha \not\equiv 0 \mod p$, since $p \nmid 2$, and if $p \mid \alpha$, we would have -2 (or -17) $\equiv 0 \mod p$. So we may apply Hensel's lemma and conclude there is a solution in $\mathbb{Z}_p$ to $X^2 - 2 = 0$ (or $X^2 - 17 = 0$), thus this is also a root of the original equation. Otherwise, if neither 2 or 17 is a square modulo p, by a standard property of quadratic residues, their product is a square modulo p, so we have a solution, $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 \equiv 0 \mod p$. By the same argument above, $2\alpha \not\equiv 0 \mod p$, so we may apply Hensel's Lemma.

Case 2 $\mathbb{Q}_2$

We consider the equation $f(X) = X^2 - 17 = 0$. We observe that $X^2 - 17 \equiv 0 \mod p$ is equivalent to $X^2 - 1 \equiv 0 \mod p$, which indeed has a solution in $\mathbb{Z}_p$, $\alpha = 1$. Furthermore $|f(\alpha)|_2 = |-16|_2 = 1/16 < |f'(\alpha)|_2^2 = |2|_2^2 = 1/4$. So by the strengthened version of Hensel's lemma, f has a root in $\mathbb{Z}_2$. Clearly, this is also a root to the original equation.

Case 3 $\mathbb{Q}_{17}$

We consider the equation $f(X) = X^2 - 2$. 2 is a square modulo 17, since $6^2 \equiv 36 \equiv 2 \mod 17$, so there is a root in $\mathbb{Z}_{17}$ which satisfies the first hypothesis of Hensel's lemma. Taking the derivative, we see that $2(6) \not\equiv 0 \mod 17$, so there is a root of $f(X)$ in $\mathbb{Z}_{17}$, by Hensel's lemma. Clearly, this is also a root of our original equation.

Case 4 $\mathbb{Q}_\infty = \mathbb{R}$

We have many roots to this equation in $\mathbb{R}$, none of which are rational, so this proves our claim.

With this in mind, we will explore scenarios in which the p-adic fields help us determine the existence of rational solutions to equations known as quadratic forms.

Definition 3.4 *For a field $\mathbb{F}$, a quadratic form is a homogeneous polynomial $\in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree 2.*

We now introduce an important result connecting p-adic numbers to quadratic forms.

Theorem 3.5 *(Hasse-Minkowski) Let*

$$f(X_1, X_2, \ldots, X_n) \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$$

be a quadratic form. Then f has a non-trivial root in $\mathbb{Q}^n$ if and only if it has a non-trivial root in $\mathbb{Q}_p^n$ for $p \leq \infty$.

Example We show that $f(x, y, z) = 5x^2 + 7y^2 - 13z^2$ has a non-trivial rational root.

Case 1 $\mathbb{Q}_p$, where $p \neq 2, 5, 7, 13$.

To work with this case, we establish an importance proposition.

Proposition 3.6 *Let $\mathbb{K}$ be a finite field. Then every quadratic form over $\mathbb{K}$ in at least 3 variables has a non-trivial root.*

With this proposition at our disposable, we establish there is a nontrivial root (x_0, y_0, z_0) of f modulo p (since the integers modulo p form a finite field). Assume $p \nmid x_0$ (we will see why this is a fair assumption). Then let

$$h(x) = 5x^2 + 7y_0^2 - 13z_0^2$$

h has a root, namely x_0, modulo p. Furthermore, $h'(x_0) = 10x_0 = 2 \cdot 5 \cdot x_0 \not\equiv 0 \mod p$, since $p \nmid 2, 5, x_0$. So by Hensel's lemma, (x_0, y_0, z_0) lifts to a root of f in $\mathbb{Z}_p$. If we had assumed $p \nmid y_0$ or z_0, it is easy to see why the derivatives would have posed no issue to apply Hensel's lemma.

Case 2 $\mathbb{Q}_2$

Set $y_0 = 0$ and $z_0 = 1$, then let

$$h(x) = 5x^2 + 7y_0^2 - 13z_0^2 = 5x^2 - 13$$

$x = 1$ is a root of $h(x)$ modulo 2. Furthermore, $|h(1)|_2 < |h'(1)|_2^2$, so by Hensel's lemma, we have root of f in $\mathbb{Z}_2$.

Case 3 $\mathbb{Q}_5$

Set $x_0 = 0$, $y_0 = 2$, then let

$$h(z) = 5x_0^2 + 7y_0^2 - 13z^2 = 28 - z^2$$

$z = 1$ is a root of $h(z)$ modulo 5. Furthemore, $h'(1) \equiv 1 \not\equiv 0 \mod 5$, hence we may apply Hensel's lemma. So there is a root of f in $\mathbb{Z}_5$.

Case 4 $\mathbb{Q}_7$

Set $x_0 = 2$, $y_0 = 0$, then let

$$h(z) = 5x_0^2 + 7y_0^2 - 13z^2 = 20 - 13z^2$$

$z = 1$ is a root of $h(z)$ modulo 7. Furthemore, $h'(1) \equiv 5 \not\equiv 0 \mod 7$, hence we may apply Hensel's lemma. So there is a root of f in $\mathbb{Z}_7$.

Case 3 $\mathbb{Q}_{13}$

Set $x_0 = 3$, $z_0 = 0$, then let

$$h(y) = 5x_0^2 + 7y^2 - 13z_0^2 = 45 + 7z^2$$

$y = 1$ is a root of $h(y)$ modulo 13. Furthemore, $h'(1) \equiv 1 \not\equiv 0 \mod 13$, hence we may apply Hensel's lemma. So there is a root of f in $\mathbb{Z}_{13}$.

Case 4 $\mathbb{Q}_\infty = \mathbb{R}$

Set $x_0 = 0$ and let y_0 be some nonzero constant. Then clearly we will be able to find an appropriate z_0 in $\mathbb{R}$.

Since we have found roots of f for all $\mathbb{Q}_p$, by the Hasse-Minkowski theorem, there is a rational root of f.

Acknowledgements

I would like to express my gratitude to Dr. Mikhail Ershov for his feedback and assistance with this paper and the lecture I delivered on this topic.

References

[1] J. Hatley, *Hasse-Minkowski and the Local-to-Global Principle*, http://www.math.umass.edu/ hatley/Capstone.pdf

[2] T. Herwig, *The p-adic Completion of Q and Hensel's Lemma*, http://www.math.uchicago.edu/ may/VIGRE/VIGRE2011/REUPapers/Herwig.pdf

[3] F. Gouvêa, *p-adic Numbers: An Introduction*, Springer. New York, NY, 1997.