6 p-adic Numbers

Let p be a prime. Recall that any natural number n can be written in base p:

$$n = n_0 + n_1 \cdot p + n_2 \cdot p^2 + \cdots + n_r \cdot p^r$$

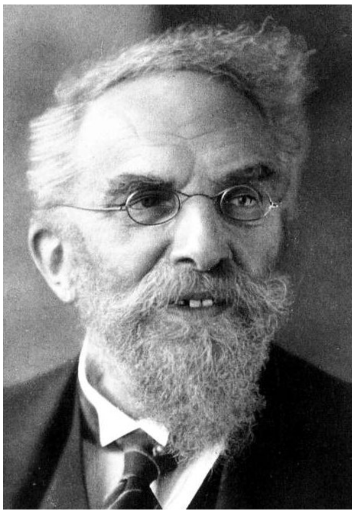
for some $r \geqslant 0$ and $0 \leqslant n_i < p$.

Definition. A **p-adic integer** is a formal sum[1]

$$a = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots = \sum_{i=0}^{\infty} a_i p^i$$

with $a_i \in \{0, 1, 2, \dots, p-1\}$ for all $i \geqslant 0$.

Such a sum is usually not convergent in $\mathbb{R}$ of course. The set of all p-adic integers is denoted by $\mathbb{Z}_p$. From the expansion in base p, we see that natural numbers can be viewed as p-adic integers with $a_i = 0$ for i bigger than some r. So $\mathbb{N} \subset \mathbb{Z}_p$.
The operation addition and multiplication are defined such as to extend the operations on $\mathbb{N}$, so they are done with "carry-over digits". For example take $p = 5$ and add the following two 5-adic integers.


Kurt Hensel (1861-1941) introduced p-adic numbers to mimic the use of power series in analysis.

$$\begin{aligned} a &= 1 + 3 \cdot 5 + 4 \cdot 5^2 + 1 \cdot 5^3 + \cdots \\ b &= 2 + 2 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + \cdots \end{aligned}$$

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

Similarly we do multiplication of 7-adic integers

$$\begin{aligned} a &= 1 + 2 \cdot 7 + 3 \cdot 7^2 + \cdots \\ b &= 3 + 2 \cdot 7 + 1 \cdot 7^2 + \cdots \end{aligned}$$

$$\begin{aligned} 1 \cdot b &= 3 + 2 \cdot 7 + 1 \cdot 7^2 + \cdots \\ 2 \cdot 7 \cdot b &= \qquad 6 \cdot 7 + 4 \cdot 7^2 + \cdots \\ 3 \cdot 7^2 \cdot b &= \qquad\qquad\quad 2 \cdot 7^2 + \cdots \end{aligned}$$

$$ab = 3 + 1 \cdot 7 + 1 \cdot 7^2 + \cdots$$

So p-adic numbers look much alike power series and that is why they would often be written as $ab = 3 + 1 \cdot 7 + 1 \cdot 7^2 + O(7^3)$. But note that the above operation are different than for power series because of the carrying-over.
It is not difficult, but tedious, to see that these operations satisfy the usual properties (associativity, commutativity, distributivity) and make the p-adic integers $\mathbb{Z}_p$ into a ring. The

[1] In some books you will find the notation $0, a_0 a_1 a_2 \dots$ which I will never use

subtraction is also well-defined and can be done as we are used to in base p:

$$\begin{aligned} a &= 3 + 1\cdot 5 + 2\cdot 5^2 + \cdots \\ b &= 4 + 0\cdot 5 + 2\cdot 5^2 + \cdots \\ \hline a-b &= 4 + 0\cdot 5 + 0\cdot 5^2 + \cdots \end{aligned}$$

In particular we must have -1 in $\mathbb{Z}_p$, indeed

$$\begin{aligned} a = 1 &= 1 + 0\cdot 5 + 0\cdot 5^2 + 0\cdot 5^3 + \cdots \\ b = 2 &= 2 + 0\cdot 5 + 0\cdot 5^2 + 0\cdot 5^3 + \cdots \\ \hline a-b = -1 &= 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + \cdots \end{aligned}$$

In general, -1 is written as a p-adic integer with all digits $a_i = p-1$. Since we can now multiply -1 with any natural number, we find that $\mathbb{Z} \subset \mathbb{Z}_p$. Though, not all integers are written as finite sums.
Another warning. We defined two p-adic integers to be equal if and only if all the coefficients are equal. Remember that the same is not true in $\mathbb{R}$, since we have $0.99999\ldots = 1.0000\ldots$

6.1 p-adic integers as sequences

To each p-adic integer $a = a_0 + a_1\cdot p + a_2\cdot p^2 + \cdots$ we can associate the sequence of partial sums:

$$\begin{aligned} s_1 &= a_0 \\ s_2 &= a_0 + a_1\cdot p \\ s_3 &= a_0 + a_1\cdot p + a_2\cdot p^2 \\ &\vdots \\ s_n &= a_0 + a_1\cdot p + a_2\cdot p^2 + \cdots + a_{n-1}\cdot p^{n-1} \end{aligned}$$

This sequence of natural numbers $(s_1, s_2, s_3, \ldots)$ satisfies the following definition.

Definition. A sequence $(s_1, s_2, \ldots)$ is **compatible** if $0 \leqslant s_n < p^n$ for all n and

$$s_m \equiv s_n \pmod{p^n} \qquad \text{for all } m > n.$$

Conversely, we can associate to any compatible sequence $(s_1, s_2, s_3, \ldots)$ a unique p-adic integer. So we could have defined the p-adic integer also as $\mathbb{Z}_p$ as the set of all compatible sequences. In this presentation[2] the additions are even easier to define. If a corresponds to the compatible sequence (s_n) and b to the compatible sequence (s'_n), then $a+b$ corresponds to the sequence $(s_n + s'_n \bmod p^n)$ and ab corresponds to the sequence $(s_n \cdot s'_n \bmod p^n)$.
In this notation, it is obvious that $\mathbb{Z}_p$ forms a ring. We will also write $a \bmod p^n$ for the n-th partial sum s_n of $a \in \mathbb{Z}_p$.

[2] often denoted by $\mathbb{Z}_p = \varprojlim_n {}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$.

6.2 p-adic units

We would like to know which elements in $\mathbb{Z}_p$ are units. A p-adic integer $a \in \mathbb{Z}_p$ is called a **p-adic unit** if there is a $b \in \mathbb{Z}_p$ such that $ab = 1$. The set of p-adic units is usually denoted by $\mathbb{Z}_p^\times$.
It is clear that $a = p$ is *not* a unit: Whatever b is, the p-adic integer pb will start with a 0 as the first digit. In fact, none of the p-adic integers $a = 0 + a_1 \cdot p + \cdots$ with a starting coefficient $a_0 = 0$ can be a p-adic unit by the same argument.

Lemma 6.1. *The p-adic units $\mathbb{Z}_p^\times$ are exactly the p-adic integers $a = a_0 + a_1 \cdot p + \cdots$ with $a_0 \neq 0$.*

Proof. It remains to prove that any a with $a_0 \neq 0$ is invertible. Consider its partial sums s_n of a. Since the first coefficient is not zero, s_n will be coprime to p. So there exists a $0 \leqslant t_n < p^n$ such that $s_n \cdot t_n \equiv 1 \pmod{p^n}$. Now for any $m > n$, the reduction of t_m modulo p^n satisfies $t_m \cdot s_n \equiv t_m \cdot s_m \equiv 1 \pmod{p^n}$, so $t_m \equiv t_n \pmod{p^n}$; meaning that the sequence (t_n) is compatible and so gives a p-adic integer b. By definition $ab \equiv 1 \pmod{p^n}$ for all n, so $ab = 1$. □

As a consequence, we find that $\frac{a}{b} \in \mathbb{Z}_p$ for all integers a and b provided that $p \nmid b$.

Example. Here is how we compute division and in particular inverses of p-adic units by using long division. We wish to find $\frac{11}{2}$ in $\mathbb{Z}_5$.

$$\begin{array}{r|r}
 & 3 + 3\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 2\cdot 5^4 + \cdots \\ \cline{2-2}
2 + 0\cdot 5 + \cdots & 1 + 2\cdot 5 + 0\cdot 5^2 + 0\cdot 5^3 + 0\cdot 5^4 + \cdots \\
 & 1 + 1\cdot 5 + 0\cdot 5^2 + 0\cdot 5^3 + 0\cdot 5^4 + \cdots \\ \cline{2-2}
 & 1\cdot 5 + 0\cdot 5^2 + 0\cdot 5^3 + 0\cdot 5^4 + \cdots \\
 & 1\cdot 5 + 1\cdot 5^2 + 0\cdot 5^3 + 0\cdot 5^4 + \cdots \\ \cline{2-2}
 & 4\cdot 5^2 + 4\cdot 5^3 + 4\cdot 5^4 + \cdots \\
 & 4\cdot 5^2 + 0\cdot 5^3 + 0\cdot 5^4 + \cdots \\ \cline{2-2}
 & 4\cdot 5^3 + 4\cdot 5^4 + \cdots \\
 & 4\cdot 5^3 + 0\cdot 5^4 + \cdots \\ \cline{2-2}
 & 4\cdot 5^4 + \cdots \\
 & 4\cdot 5^4 + \cdots \\ \cline{2-2}
 & 0 \ \ + \cdots
\end{array}$$

So we find $\frac{11}{2} = 3 + 3\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 2\cdot 5^4 + \cdots$ and the 2 will repeat them forever.

In fact it is not hard to see that the p-adic integers which have a period expansion are exactly those that belong to $\mathbb{Q}$; much like for the decimal digits in $\mathbb{R}$.

6.3 The p-adic numbers

To obtain a field from $\mathbb{Z}_p$, we need at least to add the element $\frac{1}{p}$. In fact that suffices. We define a **p-adic number** to be an expression of the form

$$a = a_{-r} \cdot \frac{1}{p^r} + a_{-r+1} \cdot \frac{1}{p^{r-1}} + \cdots + a_{-1} \cdot \frac{1}{p} + a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots = \sum_{i \geqslant -r} a_i \cdot p^i$$

for some $r \geqslant 0$ and $a_i \in \{0,1,2,\dots,p-1\}$ for all $i \geqslant -r$. The set of all p-adic number is denoted by $\mathbb{Q}_p$. We endow it with the same addition and multiplication. Then $\mathbb{Q}_p$ is a field[3] with these operations.
Any rational number can be written as $x = p^r \cdot \frac{a}{b}$ for some $r \in \mathbb{Z}$ and a, b integers that are coprime to p. Since $p^r \in \mathbb{Q}_p$ and $\frac{a}{b} \in \mathbb{Z}_p \subset \mathbb{Q}_p$, we find that $x \in \mathbb{Q}_p$. Hence $\mathbb{Q} \subset \mathbb{Q}_p$.

6.4 The absolute value

In particular, we see from lemma **??** that any prime $\ell \neq p$ is invertible in $\mathbb{Z}_p$. So we can no longer detect in $\mathbb{Z}_p$ if an integer is divisible by ℓ. But we can still do so for p. In fact, we have that p^r divides $a = a_0 + a_1 \cdot p + \cdots$ if and only if $a_i = 0$ for all $i < r$. Pushing this logic further we define $\operatorname{ord}_p(a)$ to be the smallest r such that $a_r \neq 0$. This makes sense now for all p-adic integers $a \in \mathbb{Q}_p$ not just integers if we allow $\operatorname{ord}_p(a) \in \mathbb{Z}$. We set $\operatorname{ord}_p(0) = \infty$.

Definition. We define the **absolute value** of a p-adic number $a \neq 0$ by

$$|a|_p = p^{-\operatorname{ord}_p(a)}$$

and $|0|_p = 0$.

The smaller the absolute value the more the p-adic number is divisible by p. For example $|p|_p = \frac{1}{p}$ and $|p^2|_p = \frac{1}{p^2}$.

Lemma 6.2. *(i).* $|a|_p \geqslant 0$*, and* $|a|_p = 0$ *if and only if* $a = 0$.

(ii). $|ab|_p = |a|_p \cdot |b|_p$.

(iii). $|a+b|_p \leqslant \max\{|a|_p, |b|_p\} \leqslant |a|_p + |b|_p$.

Proof. The first property is obvious. Let $a = a_r \cdot p^r + a_{r+1} \cdot p^{r+1} + \cdots$ and $b = b_s \cdot p^s + b_{s+1} \cdot p^{s+1} + \cdots$ with $a_r \neq 0$ and $b_s \neq 0$. So $\operatorname{ord}_p(a) = r$ and $\operatorname{ord}_p(b) = s$. Now $ab = a_r \cdot b_s p^{s+r} + \cdots$ gives that $\operatorname{ord}_p(ab) = r + s = \operatorname{ord}_p(a) + \operatorname{ord}_p(b)$.
Next, suppose that $r \neq s$. Then $a + b$ will start with $a_r p^r$ if $r < s$ and with $b_s p^s$ if $r > s$. So $\operatorname{ord}_p(a+b) = \min\{r, s\} = \min\{\operatorname{ord}_p(a), \operatorname{ord}_p(b)\}$.
Finally, if $r = s$, then $\operatorname{ord}_p(a+b)$ might be r, but could be higher[4]. But we still have $\operatorname{ord}_p(a+b) \geqslant \operatorname{ord}_p(a) = \operatorname{ord}_p(b)$.
Translating these results about ord_p to $|\cdot|_p$ give the results in the lemma. □

A p-adic number $a \in \mathbb{Q}_p$ satisfies $|a|_p \leqslant 1$ if and only if $a \in \mathbb{Z}_p$. Furthermore $|a|_p = 1$ if and only if $a \in \mathbb{Z}_p^\times$.
Having an absolute value, we can talk about convergence. A sequence $x_1, x_2, \dots$ of p-adic numbers converges to $x \in \mathbb{Q}_p$ if $|x - x_i|_p$ tends to zero in $\mathbb{R}$ as n grows.

Definition. A sequence (x_i) of p-adic numbers $x_i \in \mathbb{Q}_p$ is said to be a **Cauchy sequence** if, for any $\varepsilon > 0$, there exists a N such that $|x_i - x_j|_p < \varepsilon$ for all $i, j \geqslant N$.

Proposition 6.3. *Any Cauchy sequence in* $\mathbb{Q}_p$ *converges.*

Proof. Let (x_i) be a Cauchy sequence and let $n \geqslant 1$. By taking $\varepsilon = p^{-n}$, we find a N such that $|x_i - x_j|_p < p^{-n}$ for all $i, j \geqslant N$. This inequality just means that the digits of x_i and x_j agree at least up to the digit before p^n. Hence all elements x_i with $i \geqslant N$ have the same digits up to p^n. As we let n increase, we find a p-adic number a by taking the digits of x_i. By construction $|x_i - a|_p < p^{-n}$, so the sequence x_i converges to a. □

[3] Cantor's diagonal argument shows that $\mathbb{Q}_p$ is not countable.
[4] Example: $a = 2 \cdot 5 + 1 \cdot 5^2 + \cdots$ and $b = 3 \cdot 5 + 2 \cdot 5^2 + \cdots$.

6.5 Polynomial equations

Here is the main motivation to consider p-adic numbers. Let $f(X)$ be a polynomial with integer coefficients, say $f = f_0 + f_1\,X + \cdots + f_d\,X^d$. We say that $a \in \mathbb{Z}_p$ is a root of $f(X) = 0$ if $f(a) = f_0 + f_1\,a + \cdots + f_d\,a^d = 0$.

Lemma 6.4. *A polynomial $f(X) \in \mathbb{Z}[X]$ has a solution in $\mathbb{Z}_p$ if and only if it has a solution modulo p^n for all $n \geqslant 1$.*

Let $m > n$ be two natural numbers. Let x be a root of a polynomial $f(X) \in \mathbb{Z}[X]$ modulo p^m, i.e. $f(x) \equiv 0 \pmod{p^m}$. Then x is also a root modulo p^n. Conversely, let y be a root modulo p^n. Then it may or may not be true that there exists a x such that $x \equiv y \pmod{p^n}$ and x is a root modulo p^m. If so, we say that the root y can be **lifted** modulo p^m and each possible x is called a **lift**. For instance a sequence of $0 \leqslant s_n < p^n$ is compatible if s_m is a lift of s_n for all $m > n$.

Proof. $\Rightarrow$: If $a \in \mathbb{Z}_p$ is the root of $f(X)$, then the n-th partial sum s_n is a solution modulo p^n.
$\Leftarrow$: For each n, let x_n be a solution modulo p^n. Consider the values of all x_n modulo p. Among the p possible values, at least one of them, say s_1, will appear infinitely many times. Discard now from the sequence x_n all those which are not congruent to s_1 modulo p.
Next we consider values of all remaining x_n modulo p^2. Among the p possible values s_1, $s_1 + p$, $s_1 + 2p$, ..., $s_1 + (p-1)p$ at least one, say s_2, appears infinitely many times. Again we remove from the sequence all x_n that are not congruent to s_2 modulo p^2.
Continuing in this way, we construct inductively a compatible sequence s_n. Denote the corresponding p-adic integer by a. Now $f(a) \equiv f(s_n) \equiv 0 \pmod{p^n}$ for all n. So $f(a)$ is a p-adic integer all of which digits are zero, i.e. $f(a) = 0$. □

Remark. The lemma stays true if we allow the coefficients of f to be p-adic integers.

Here are a few examples.

Example. We consider the polynomial $f(X) = X^3 - 5\,X^2 + 18\,X + 216$ for $p = 3$. The solutions modulo 3 are 0 and 2. For $p^2 = 9$, we find the solutions 0, 3, 5, and 6. Next there are the solutions 0, 9, 18, and 23 modulo $p^3 = 27$. But modulo $p^4 = 81$ there is only one solution namely 77, similar for p^5 it is only 239 and then 725 modulo p^6. We can illustrate this best in the picture in figure **??**.
If there exists a 3-adic solution to $f(X) = 0$, then it has to be congruent to $725 = 2 + 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5$ modulo 3^6. In fact, there exists exactly one solution in $\mathbb{Z}_3$, namely

$$-4 \;=\; 2 + 1\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^5 + 2\cdot 3^6 + 2\cdot 3^7 + 2\cdot 3^8 + 2\cdot 3^9 + \cdots$$

Example. Consider the polynomial $f(X) = X^7 + X^5 + 4\,X^2 + 4$ for $p = 5$. Modulo p there are three solutions, namely $\{1, 2, 3\}$. But modulo all higher powers of p there are each time only two solution: for p^2, we have $\{7, 18\}$, the first is a lift of 2 modulo p^2 and the second is a lift of 3. The solution 1 can not be lifted modulo p^2. For p^3, we have $\{57, 68\}$, for p^4 it is $\{182, 443\}$, then $\{2057, 1068\}$, $\{14557, 1068\}$, $\{45807, 32318\}$, etc. If we write these solutions in base 5, we quickly see that they are the partial sums of the following two roots of $f(X)$ in $\mathbb{Z}_5$:

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

We will see later how one can quickly find these 5-adic solutions.

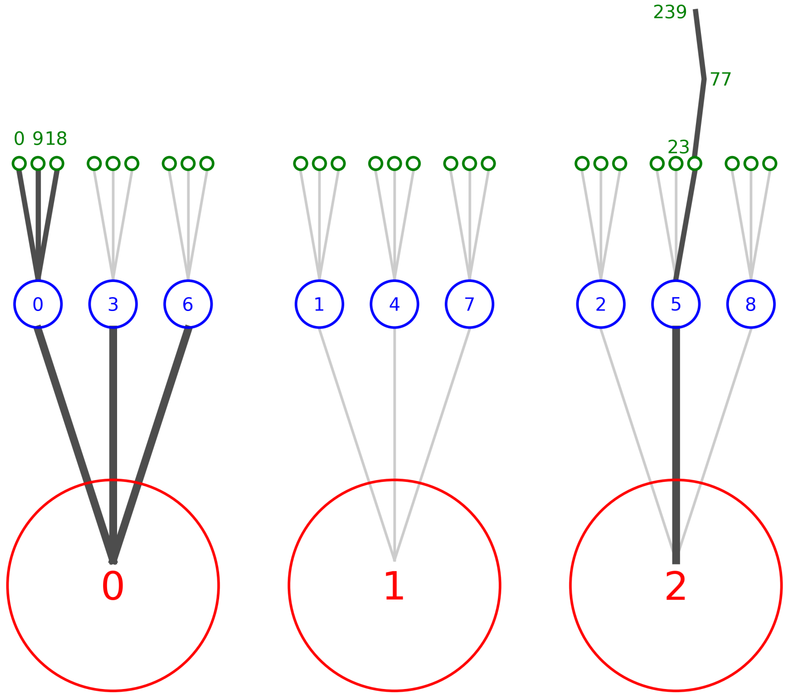


Figure 1: The lifts modulo powers of 3 of the solutions to $X^3 - 5\,X^2 + 18\,X + 216$

6.6 Hensel's lemma

For a polynomial $f(X) \in \mathbb{Z}_p[X]$ we write $f'(X) \in \mathbb{Z}_p[X]$ for its derivative.
The following is a fast method to find p-adic solutions of polynomials.

Theorem 6.5 (Hensel's lemma). *Let $f(X)$ be a polynomial in $\mathbb{Z}_p$. Suppose $x_0 \in \mathbb{Z}_p$ is such that $f(x_0) \equiv 0 \pmod{p}$ but $f'(x_0) \not\equiv 0 \pmod{p}$. Consider the sequence defined by*

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Then (x_n) converges to a root $x \in \mathbb{Z}_p$ of f with $x \equiv x_0 \pmod{p}$.

Example. Consider the previous example $f(X) = X^7 + X^5 + 4\,X^2 + 4$ for $p = 5$. Let us choose $a = 2$, as we have seen that this is a solution modulo p. Then $f'(2) = 544 = 4 + 3\cdot 5 + 5^2 + 4\cdot 5^3$ is not congruent to 0 modulo p, therefore the theorem applies. Indeed, here are the first few elements of the sequence:

$$\begin{aligned}
x_1 &= 2 + 1\cdot 5 + 1\cdot 5^2 + 2\cdot 5^3 + 4\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + 4\cdot 5^7 + 4\cdot 5^{11} + 1\cdot 5^{12} + \cdots\\
x_2 &= 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 2\cdot 5^4 + 4\cdot 5^5 + 4\cdot 5^6 + 2\cdot 5^7 + 1\cdot 5^8 + 3\cdot 5^{10} + \cdots\\
x_3 &= 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + 3\cdot 5^7 + 4\cdot 5^8 + 5^{10} + 3\cdot 5^{12} + \cdots\\
x_4 &= 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + 3\cdot 5^7 + 3\cdot 5^9 + 2\cdot 5^{10} + 2\cdot 5^{11} + \cdots\\
x_5 &= 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + 3\cdot 5^7 + 3\cdot 5^9 + 2\cdot 5^{10} + 2\cdot 5^{11} + \cdots
\end{aligned}$$

In fact the number of correct digits of a_n will be equal to 2^n as the precision doubles at each step. (One can see this from the proof below).
If one starts with another x_0 the sequence may converge to the other solution given above. For instance for $x = 1$, although the condition is not satisfied at the first step because $f'(1) \equiv 0 \pmod 5$. On the other hand we can certainly not start with $x_0 = 0$ as $f'(0) = 0$. With $x_0 = 25$, the series does not converge at all, it jumps around 5-adic numbers with $\mathrm{ord}_5(x_n) = -2$:

$$\begin{aligned}
x_1 &= 2\cdot 5^{-2} + 2\cdot 5^{-1} + 2 + 2\cdot 5 + 5^5 + \cdots\\
x_2 &= 5^{-2} + 4\cdot 5^{-1} + 2 + 3\cdot 5 + 2\cdot 5^3 + 2\cdot 5^5 + \cdots\\
x_3 &= 3\cdot 5^{-2} + 3\cdot 5^{-1} + 1 + 2\cdot 5 + 2\cdot 5^3 + 4\cdot 5^4 + 4\cdot 5^5 + \cdots\\
x_4 &= 4\cdot 5^{-2} + 3\cdot 5^{-1} + 4\cdot 5 + 3\cdot 5^3 + 3\cdot 5^4 + 5^5 + \cdots\\
x_5 &= 2\cdot 5^{-2} + 2 + 5 + 2\cdot 5^2 + 5^3 + 3\cdot 5^4 + 2\cdot 5^5 + \cdots\\
x_6 &= 5^{-2} + 3\cdot 5^{-1} + 4 + 5 + 4\cdot 5^2 + 2\cdot 5^3 + 4\cdot 5^4 + \cdots
\end{aligned}$$

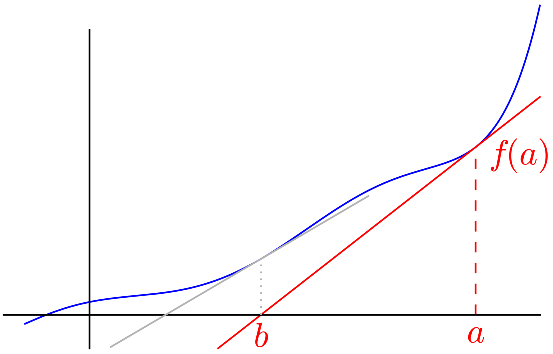
For the proof of the theorem, we will use the following lemma. Note this is nothing else but the Newton-Raphson method from numerical analysis, but of course translated to the p-adic absolute value.

Lemma 6.6. *Let $f(X)$ be a polynomial in $\mathbb{Z}_p[X]$ and let $0 < r \leqslant 1$. Suppose that $a \in \mathbb{Z}_p$ satisfies*

$$|f(a)|_p < r \qquad \text{and} \qquad f'(a) \neq 0 \qquad \text{and} \qquad \left|\frac{f(a)}{f'(a)^2}\right|_p < r.$$

Then $b = a - \frac{f(a)}{f'(a)}$ satisfies

$$|f(b)|_p < r^2 \qquad \text{and} \qquad \left|\frac{f(b)}{f'(b)^2}\right|_p < r^2.$$



Proof. By hypothesis $\delta = -f(a)/f'(a)$ belongs to $\mathbb{Z}_p$. Expanding $f(X+Y)$ in Y, we get

$$f(X+Y) = f(X) + f'(X)\cdot Y + g(X,Y)\cdot Y^2$$

for some $g(X,Y) \in \mathbb{Z}_p[X,Y]$. Putting $X = a$ and $Y = \delta$ and defining $c = g\big(a,\delta\big) \in \mathbb{Z}_p$, we get

$$\begin{aligned} f(b) &= f(a) + f'(a) \cdot \left(-\frac{f(a)}{f'(a)} \right) + c \frac{f(a)^2}{f'(a)^2} \\ &= c \cdot f(a) \cdot \frac{f(a)}{f'(a)^2} \end{aligned}$$

and hence

$$|f(b)|_p = |c|_p \cdot |f(a)|_p \cdot \left| \frac{f(a)}{f'(a)^2} \right|_p < 1 \cdot r \cdot r = r^2.$$

Similar we have

$$f'(X+Y) = f'(X) + h(X,Y) \cdot Y$$

with $h(X,Y) \in \mathbb{Z}_p[X,Y]$ and setting $c' = h(a,\delta) \in \mathbb{Z}_p$ gives

$$\begin{aligned} f'(b) &= f'(a) + c' \cdot \left(-\frac{f(a)}{f'(a)} \right) \\ &= f'(a) \cdot \left(1 - c' \cdot \frac{f(a)}{f'(a)^2} \right) \end{aligned}$$

and so

$$|f'(b)|_p = |f'(a)|_p \cdot \left| 1 - c' \cdot \frac{f(a)}{f'(a)^2} \right|_p = |f'(a)|_p$$

because $|c'|_p \cdot |f(a)/f'(a)^2|_p < 1 \cdot r \leqslant 1$. Finally, we get

$$\left| \frac{f(b)}{f'(b)^2} \right|_p = \frac{|c|_p \cdot |f(a)|_p^2}{|f'(a)|_p^4} < r^2.$$

□

Proof of theorem ??. Apply the lemma to x_0 with r between $\frac{1}{p}$ and 1. Then $|f(x_0)|_p < r$ because $f(x_0) \equiv 0 \pmod{p}$ and $|f(x_0)/f'(x_0)^2|_p < r$ because $f'(x_0) \not\equiv 0 \pmod{p}$. Hence $|f(x_1)|_p < r^2$.
Now, we apply repeatedly the previous lemma to x_n. So $|f(x_n)|_p < r^{2^n}$ shows that $f(x_n)$ converges (quadratically) to 0. We only need to show now that x_n forms a Cauchy sequence. Note first that

$$|x_{n+1} - x_n|_p = \left| \frac{f(x_n)}{f'(x_n)} \right|_p = \left| \frac{f(x_n)}{f'(x_n)^2} \right|_p \cdot |f'(x_n)|_p < r^{2^n} \cdot 1 < r^n$$

and so, for all $m > n$,

$$|x_m - x_n|_p \leqslant |x_m - x_{m-1}|_p + |x_{m-1} - x_{m-2}|_p + \cdots + |x_{n+1} - x_n|_p < r^{m-1} + r^{m-2} + \cdots + r^n = \frac{r^m - r^n}{r-1}$$

which is arbitrary small as $n \to \infty$, because $r < 1$. □

There are plenty of generalisations of Hensel's lemma. For instance one can not only detect roots, i.e. linear factors, of polynomials, but also factorisations of polynomials. Further the theory of Newton polygons provide a further tool to study p-adic polynomials (and power series).

6.7 Application of Hensel's lemma

Proposition 6.7. *Let p be an odd prime. Then there is an element $i \in \mathbb{Q}_p$ with $i^2 = -1$ if and only if $p \equiv 1 \pmod 4$.*

Proof. If there is such an $i \in \mathbb{Q}_p$, then it belongs to $\mathbb{Z}_p$, because $0 = \operatorname{ord}_p(-1) = 2\operatorname{ord}_p(i)$.
On the one hand, if $p \equiv 3 \pmod 4$, then -1 is not a square modulo p. Hence there is no solution to $X^2 + 1 = 0$ modulo p and so there cannot be a p-adic solution either.
On the other hand, if $p \equiv 1 \pmod 4$, then there is a x_0 such that x_0 is a solution to $f(X) = X^2 + 1 = 0$ modulo p. Since $x_0 \not\equiv 0 \pmod 4$, we have $f'(x_0) \not\equiv 0 \pmod p$. Hensel's lemma guarantees the existence of a solution to $f(X) = 0$ in $\mathbb{Z}_p$. □

Aside: If $p \equiv 3 \pmod 4$, we could consider the p-adic Gaussian integers $\mathbb{Z}_p[i]$. This is indeed very interesting. See the general theory of local fields.

Example. For $p = 5$, the two solutions[5] i and $-i$ are given by

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

These are the two solutions of $f(X) = X^7 + X^5 + 4X^2 + 4$ that we have encountered already. That is no surprise as $f(X) = (X^2+1)(X^5+4)$.

Proposition 6.8. *Let D be a non-zero integer and let p be an odd prime which does not divide D. Then there exists a $\alpha \in \mathbb{Q}_p$ with $\alpha^2 = D$ if and only if $(\frac{D}{p}) = +1$.*

The proof is as for the previous proposition. Typically we could denote $\alpha = \pm\sqrt{D}$.

Example. Since $(\frac{13}{101}) = +1$, there are two elements $\alpha = \pm\sqrt{13}$ in $\mathbb{Q}_{101}$ with $\alpha^2 = 13$. First we have to find solutions modulo p by running through all values. We find that 35 and 66 are square roots of 13 modulo 101. Then Hensel's lemma helps us to find the further 101-adic digits of $\sqrt{13}$:

$$66 + 54\cdot 101 + 47\cdot 101^2 + 6\cdot 101^3 + 33\cdot 101^4 + 60\cdot 101^5 + 41\cdot 101^6 + \cdots$$
$$35 + 46\cdot 101 + 53\cdot 101^2 + 94\cdot 101^3 + 67\cdot 101^4 + 40\cdot 101^5 + 59\cdot 101^6 + \cdots$$

Theorem 6.9. *All $p-1$-st roots of unity ζ, i.e. satisfying $\zeta^{p-1} = 1$, belong to $\mathbb{Z}_p$.*

Proof. Consider $f(X) = X^{p-1} - 1$. For each choice of $x_0 = 1, 2, \ldots, p-1$, we find one ζ using Hensel's lemma. □

If p is odd, once can show conversely that these are all roots of unity in $\mathbb{Q}_p$.

Example. Here are the 6-th roots of unity in $\mathbb{Z}_7$:

$$\begin{aligned}
&1\\
&2 + 4\cdot 7 + 6\cdot 7^2 + 3\cdot 7^3 + 2\cdot 7^5 + 6\cdot 7^6 + 2\cdot 7^7 + 4\cdot 7^8 + 3\cdot 7^9 + \cdots\\
&3 + 4\cdot 7 + 6\cdot 7^2 + 3\cdot 7^3 + 2\cdot 7^5 + 6\cdot 7^6 + 2\cdot 7^7 + 4\cdot 7^8 + 3\cdot 7^9 + \cdots\\
&4 + 2\cdot 7 + 3\cdot 7^3 + 6\cdot 7^4 + 4\cdot 7^5 + 4\cdot 7^7 + 2\cdot 7^8 + 3\cdot 7^9 + \cdots\\
&5 + 2\cdot 7 + 3\cdot 7^3 + 6\cdot 7^4 + 4\cdot 7^5 + 4\cdot 7^7 + 2\cdot 7^8 + 3\cdot 7^9 + \cdots\\
-1 =&6 + 6\cdot 7 + 6\cdot 7^2 + 6\cdot 7^3 + 6\cdot 7^4 + 6\cdot 7^5 + 6\cdot 7^6 + 6\cdot 7^7 + 6\cdot 7^8 + 6\cdot 7^9 + \cdots
\end{aligned}$$

[5] But we have no way of deciding "which is which"...

Theorem 6.10. *Let $n \geqslant 1$ and suppose p is odd. If ζ is a $p-1$-st root of unity congruent to a primitive element modulo p, then $g = \zeta \cdot (1+p) \bmod p^n$ is a primitive element modulo p^n.*

Proof. Take $k > 0$ with $g^k \equiv 1 \pmod{p^n}$. Because $1 \equiv g^k \equiv \zeta^k \pmod{p}$ and ζ is a primitive root modulo p, we must have that k is divisible by $p-1$. Start the proof by induction on n that p^{n-1} divides k with $n = 1$, which is clear. By induction k is divisible by p^{n-2}. Now

$$1 \equiv g^k = (1+p)^k = 1 + kp + \binom{k}{2}p^2 + \binom{k}{3}p^3 + \cdots + p^k \pmod{p^n}$$

But for $j \geqslant 2$, the term $\binom{k}{j}p^j = \frac{k}{j}\,p^j\,\binom{k-1}{j-1}$ is divisible by p^n. So $kp \equiv 0 \pmod{p^n}$ gives $p^{n-1} \mid k$. □

6.8 The Hasse principle

Let $f(X_1, X_2, \ldots, X_n) = 0$ be a polynomial equation with coefficients in $\mathbb{Z}$. If we find an integer m such that the equation has no solution modulo m, then there is no solution $(x_1, x_, \ldots x_n)$ with $x_i \in \mathbb{Z}$.
Suppose now, we have shown that, for all primes p, there is a solution with $x_i \in \mathbb{Z}_p$. Then there will be a solution modulo all integers m. Does this mean that there is a solution in $\mathbb{Z}$? Not necessarily: The equation $x^2 + y^2 + 5\,z^2 = -1$ has a solution in $\mathbb{Z}_p$ for all p. But since there is no solution in $\mathbb{R}$, there can not have a solution in integer either. Here is the first positive result.

Theorem 6.11 (Hasse-Minkowski)**.** *Let $f(X_1, X_2, \ldots, X_n) = \sum_{i \leqslant j} a_{ij} X_i X_j$ be a quadratic form with coefficients $a_{ij} \in \mathbb{Z}$. Suppose f has a solution in $\mathbb{Z}_p$ for all p and a solution in $\mathbb{R}$, then it also has a solution $\mathbb{Z}$.*

See Serre's *"Cours d'arithmétique"* for a proof. However, Selmer found that the equation $3x^3 + 4y^3 + 5z^3 = 0$ has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for all p, but none in $\mathbb{Q}$. To prove that this equation has no solution one has to do work hard. It won't suffice to look modulo m.
To check that an equation has solutions in $\mathbb{Z}_p$ for all primes p it is sufficient to find good solutions modulo p for all p. For sufficiently large p this is automatic by a theorem by Dwork (in the case of one equation) and Deligne (for systems of equations) on the so-called Weil conjecture. So in a finite number of computational steps one can determine if an equation has solutions modulo all integers $m > 1$.