Chapter 14

p-adic numbers

At the end of the 19th century, Hensel invented p-adic numbers as a number theoretical analogue of power series in complex analysis. It took more than 25 years before p-adic numbers were taken seriously by number theorists: this was when Hasse, around 1920, proved the Local-Global Principle for quadratic forms over $\mathbb{Q}$: a quadratic form in n variables with rational constants represents 0 nontrivially if and only if the quadratic form represents 0 nontrivially in each p-adic completion of $\mathbb{Q}$. The point is that checking representability in p-adic fields is something that can be done easily, and in a finite number of steps.

So what are p-adic numbers? Actually there are several ways of introducing them.

The Naive Approach

Let us solve the congruences $x^2 \equiv -1 \bmod 5^n$ for $n \geq 1$.

For $n = 1$ there are two solutions: $x \equiv \pm 2 \bmod 3$. In order to find a solution for $n = 2$, note that if $x^2 \equiv -1 \bmod 5^2$, then $x^2 \equiv -1 \bmod 5$ and therefore $x \equiv \pm 2 \bmod 5$. Thus we can try to find x by writing $x = 2 + 5y$; then $0 \equiv x^2 + 1 \equiv 5 + 20y \bmod 5^2$, hence $5^2 \mid (5 + 20y)$ or $5 \mid (1 + 4y)$. This yields $y \equiv 1 \bmod 5$, and our solution is $x \equiv 2 + 5 \bmod 5^2$.

Now assume that we have determined $x \in \mathbb{N}$ with $x^2 \equiv -1 \bmod 5^n$; in order to find a solution modulo 5^{n+1}, write $a = x + 5^n y$. From $x^2 \equiv -1 \bmod 5^n$ we get $x^2 + 1 = 5^n b$. Thus $0 \equiv a^2 + 1 \equiv x^2 + 1 + 2xy5^n \equiv 5^n(b + 2xy) \bmod 5^{n+1}$. This implies $b + 2xy \equiv 0 \bmod 5$, and since $5 \nmid 2x$, this congruence must have a unique solution modulo 5.

Thus we have proved: there exist integers x_k with $0 \leq x_k < 5$ such that for every $n \geq 1$ the integer $X_n = x_0 + 5x_1 + 5^2x_2 + \ldots + 5^{n-1}x_{n-1}$ solves the congruence $X_n^2 \equiv -1 \bmod 5^n$.

Of course the sequence (X_n) does not converge, so it does not seem to make sense of defining

$$x = x_0 + 5x_1 + 5^2x_2 + \ldots$$

Yet this is exactly what Hensel did. Such an expression is called a 5-adic integers, and the set of all 5-adic integers forms a ring.

In fact, fix a prime number p and consider formal power series in p:

$$a = a_0 + a_1 p + a_2 p^2 + \ldots, \tag{14.1}$$

where $0 \le a_i \le p-1$. The key word here is *formal*, that is, you negelct things like convergence. Now you can clearly add, subtract and multiply such power series; for example, let us add the 5-adic numbers

$$\begin{array}{ccccccccc} 3 & + & 2\cdot 5 & + & 0\cdot 5^2 & + & 4\cdot 5^3 & + \ldots \\ 1 & + & 4\cdot 5 & + & 2\cdot 5^2 & + & 2\cdot 5^3 & + \ldots \\ \hline 4 & + & 6\cdot 5 & + & 2\cdot 5^2 & + & 6\cdot 5^3 & + \ldots. \end{array}$$

Now observe that $6 = 1+5$, hence $6\cdot 5 = 1\cdot 5 + 1\cdot 5^2$, hence we carry 1 and find

$$4 + 6\cdot 5 + 2\cdot 5^2 + 6\cdot 5^3 + \ldots = 4 + 1\cdot 5 + 3\cdot 5^2 + 1\cdot 5^3 + \ldots,$$

where we have carried another 1 at the coefficient of 5^3. Clearly we can also multiply p-adic numbers this way, so we get a ring $\mathbb{Z}_p$, the ring of p-adic integers, whose neutral element is $0 = 0 + 0\cdot p + 0\cdot p^2 + \ldots$ and whose unit element is $1 = 1 + 0\cdot p + 0\cdot p^2 + \ldots$. Note that $\mathbb{Z}_p$ contains $\mathbb{Z}$ as a subring: every natural number a actually has a *finite* expansion into a p-adic series. What about -1?. Well,

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

Actually, this is not too surprising: consider the geometric series $\frac{1}{1-x} = 1 + x + x^2 + \ldots$ and plug in p: then $\frac{1}{1-p} = 1 + p + p^2 + \ldots$, and multiplying through by $p-1$ gives you the p-adic expansion of -1 above. Actually, the “equation”

$$-1 = 1 + 2 + 4 + 8 + \ldots$$

can be found in Euler’s work (where, of course, it didn’t make too much sense).

Let us now become familiar with the p-adic numbers by proving a few simple results.

Lemma 14.1. *$\mathbb{Z}$ is a subring of $\mathbb{Z}_p$.*

Proof. Every positive integer n can be written as a “finite” p-adic number: $n = a_0 + a_1 p + \ldots + a_m p^m$. In fact, define a_0 by $0 \le a_0 < p$ and $n \equiv a_0 \bmod p$; then let $n_1 = (n - a_0)/p$ and define a_1 by $0 \le a_1 < p$ and $n_1 \equiv a_1 \bmod p$; now repeat until $n_m = 0$.

Next, $-1 = (p-1)(1 + p + p^2 + \ldots) \in \mathbb{Z}_p$; thus every integer is also a p-adic integer. □

Lemma 14.2. *The prime $p \in \mathbb{Z}$ is also prime in $\mathbb{Z}_p$.*

Proof. Assume that $a, b \in \mathbb{Z}_p$ and that $p \mid ab$. Write $a = a_0 + a_1 p + a_2 p^2 + \ldots$ and $b = b_0 + b_1 p + b_2 p^2 + \ldots$ with $0 \le a_i, b_i < p$. Then $ab = a_0 b_0 + p(a_0 b_1 + a_1 b_0) + \ldots$ is divisible by p; this implies that $p \mid a_0 b_0$ in the usual integers, and since p is prime there, we have $p \mid a_0$ or $p \mid b_0$. Because of $0 \le a_i, b_i < p$ this is only possible if $a_0 = 0$ or $b_0 = 0$, and then $a = p(a_1 + a_2 p + \ldots)$ or $b = p(b_1 + b_2 p + \ldots)$, i.e., $p \mid a$ or $p \mid b$. $\square$

Next we claim that p is the only prime in $\mathbb{Z}_p$:

Lemma 14.3. *Assume that $a \in \mathbb{Z}_p$ is not divisible by p. Then a is a unit.*

Proof. Write $a = a_0 + a_1 p + a_2 p^2 + \ldots$ with $0 \le a_i < p$. Then $p \nmid a$ means $a_0 \ne 0$, i.e., $1 \le a_0 \le p - 1$. We now construct a p-adic integer $b = b_0 + b_1 p + b_2 p^2 + \ldots$ with $ab = 1$. We must have $1 = ab \equiv a_0 b_0 \bmod p$, and there is a unique b_0 with $1 \le b_0 \le p - 1$ and $a_0 b_0 \equiv 1 \bmod p$.

Next we find $1 = ab \equiv a_0 b_0 + p(a_1 b_0 + a_0 b_1) \bmod p^2$. Since $a_0 b_0 \equiv 1 \bmod p$ we have $a_0 b_0 - 1 = pc_0$, and now $0 \equiv pc_0 + p(a_1 b_0 + a_0 b_1) \bmod p^2$. This is equivalent to $a_1 b_0 + a_0 b_1 + c_0 \equiv 0 \bmod p$, which is a linear congruence in b_1 (all the other numbers in there are known); since $a_0 b_1 \equiv -c_0 - a_1 b_0 \bmod p$ has a unique solution (again because $p \nmid a_0$), we have found a unique b_1 with $1 \le b_1 \le p - 1$.

Now we proceed by induction and show that, once we have constructed b_0, …, b_n, we can determine b_{n+1} from a linear congruence $a_0 b_{n+1} \equiv$ something $\bmod p$. This is left as an exercise.

Now put $b = b_0 + b_1 p + \ldots$. Then $ab \equiv 1 \bmod p^n$ for every n, hence $p^n \mid (ab - 1)$ for every n, and this is only possible if $ab = 1$. $\square$

Lemma 14.4. *Every nonzero p-adic integer can be written uniquely in the form $a = p^n u$ for some integer $n \ge 0$ and some unit $u \in \mathbb{Z}_p$.*

Proof. Write $a = a_0 + a_1 p + a_2 p^2 + \ldots$ with $0 \le a_i < p$. Let n be the smallest exponent for which a_n is nonzero. Then $a = a_n p^n + a_{n+1} p^{n+1} + \ldots = p^n(a_n + a_{n+1} p + \ldots)$, and since $p \nmid a_n$, the p-adic number in the brackets is a unit. $\square$

Lemma 14.5. *$\mathbb{Z}_p$ is a domain.*

Proof. In fact, assume that $ab = 0$ for $a, b \in \mathbb{Z}_p$. If a and b are nonzero, then we can write $a = p^m u$ and $b = p^n v$ for units u, v; but then uv is a unit, hence nonzero, and then $ab = p^{m+n} uv$ is nonzero too. $\square$

We now introduce the field $\mathbb{Q}_p$ of p-adic numbers. It consists of quotients $\frac{a}{b}$ with $a, b \in \mathbb{Z}_p$ and $b \ne 0$. Writing $a = p^m u$ and $b = p^n v$ for units u, v we see that $\frac{a}{b} = p^{m-n} uv^{-1}$. Thus p-adic numbers are just a power of p (possibly with negativ exponent) times a unit in $\mathbb{Z}_p$.

14.1 Valuations

The usual absolute value in the rational or real numbers has the following property:

- $|x| \geq 0$ for $x \in \mathbb{Q}$; $|x| = 0$ if and only if $x = 0$;
- $|xy| = |x| \cdot |y|$;
- $|x + y| \leq |x| + |y|$ (triangle inequality).

It turns out that there are more functions with these properties. Let $p > 0$ be a prime number; any $a \in \mathbb{Q}^\times$ can be written uniquely as $a = p^m b$, where $b = \frac{r}{s}$ is a fraction whose numerator and denominator are not divisible by p: $p \nmid rs$. Now put $|a|_p = p^{-m}$ and $|0|_p = 0$. This function $|\cdot|_p$ has the following properties:

- $|a|_p \geq 0$ and $|a|_p = 0$ if and only if $a = 0$;
- $|ab|_p = |a|_p |b|_p$. In fact, write $a = p^m \frac{r}{s}$ and $b = p^n \frac{t}{u}$, where $p \nmid rstu$. Then $ab = p^{m+n} \frac{rt}{su}$, hence $|ab|_p = p^{-m-n} = |a|_p |b|_p$.
- $|a+b|_p \leq |a|_p + |b|_p$. In fact, we will prove the stronger statement $|a+b|_p \leq \max\{|a|_p, |b|_p\}$. Write $a = p^m \frac{r}{s}$ and $b = p^n \frac{t}{u}$, where $p \nmid rstu$, and assume that $m \leq n$. (hence $|a|_p \geq |b|_p$). Then $a + b = p^m(\frac{r}{s} + p^{n-m}\frac{t}{u}) = p^m(ru + p^{n-m}st)/su$, and therefore $|a + b|_p = |a|_p |ru + p^{n-m}st|_p |tu|_p^{-1}$. Now $|tu|_p = 1$ since $p \nmid tu$, and $|ru + p^{n-m}st|_p \leq 1$ because $|c| \leq 1$ for any integer c, hence $|a + b|_p \leq |a|_p = \max\{|a|_p, |b|_p\}$ as claimed.

Using these valuations $|\cdot|_p$ instead of the usual absolute value (which we will often denote by $|\cdot|_\infty$ from now on) we can define Cauchy sequence and the notion of a limit. We say that a sequence (a_n) of rational numbers is Cauchy if for every $\varepsilon > 0$ there is an N such that $|a_m - a_n|_p < \varepsilon$ for all $m, n > N$; we say it converges to $a \in \mathbb{Q}$ if for every $\varepsilon > 0$ there is an N such that $|a_n - a|_p < \varepsilon$ for all $n > N$.

Cauchy sequences and converging sequences with respect to $|\cdot|_p$ form rings. The set $\mathcal{N}$ of null sequences (sequences converging to 0) actually is an ideal in the ring $\mathcal{C}$ of Cauchy sequences, and the quotient ring $\mathcal{C}/\mathcal{N}$ (residue classes of Cauchy sequences modulo null sequences) turns out to be a field, namely the field of p-adic numbers $\mathbb{Q}_p$. The reals can be constructed in the same way using the usual absolute value, and we often write $\mathbb{R} = \mathbb{Q}_\infty$.

These new fields have strange properties. For example, the sequence $a_n = p^n$ is a null sequence with respect to $|\cdot|_p$. Moreover, $\lim_n(1 + p + \ldots + p^n) = \frac{1}{1-p}$ with respect to $|\cdot|_p$. In fact,

$$1 + p + \ldots + p^n - \frac{1}{1-p} = \frac{1 - p^{n+1}}{1-p} - \frac{1}{1-p} = \frac{p^n}{p-1},$$

hence $|1 + p + \ldots + p^n - \frac{1}{1-p}|_p = p^{-n}$. This clearly can be made as small as we wish.

We can extend the valuation $|\cdot|_p$ defind on $\mathbb{Q}$ to a valuation on $\mathbb{Q}_p$ by writing $x = p^m u$ for some unit $u \in \mathbb{Z}_p^\times$ and putting $|x|_p = p^{-m}$.

Let us now return to the sequence X_n with $X_n^2 \equiv -1 \bmod 5^n$ defined above. The sequence X_n clearly is Cauchy, so its limit must be a 5-adic number. We claim that $X = \lim X_n$ satisfies $X^2 = -1$. Given $\varepsilon > 0$ we can choose n so large that $|X - X_n|_p < \varepsilon$. Then $|X^2 + 1|_p = |X^2 - X_n^2|_p + |X_n^2 + 1|_p = |X - X_n|_p |X - X_n|_p + |X_n^2 + 1|_p \le \varepsilon + p^{-n-1}$ since $X_n^2 \equiv -1 \bmod p^{n+1}$. Clearly $\varepsilon + p^{-n-1}$ can be made as small as we wish, hence $X^2 + 1 = 0$.