P-ADIC NUMBERS

Let us begin by recalling how the real numbers $\mathbb{R}$ are defined starting from $\mathbb{Q}$. One begins with two ingredients: (i) the set of rational numbers $\mathbb{Q}$, and (ii) the ordinary absolute value $|\cdot|$. Now consider the set of Cauchy sequences in $\mathbb{Q}$, that is, the set of sequences $(a_n)_{n=1}^{\infty}$ satisfying the property that whenever $\varepsilon > 0$, there exists $N = N(\varepsilon)$ such that whenever $n > m > N(\varepsilon)$, one has $|a_n - a_m| < \varepsilon$. Define

$$\mathcal{R} = \{(a_n)_{n=1}^{\infty} : a_n \in \mathbb{Q} \text{ for each } n, \text{ and } (a_n) \text{ is a Cauchy sequence}\}.$$

One can show that $\mathcal{R}$ forms a ring under addition and multiplication defined coordinatewise in the obvious fashion. Now identify two Cauchy sequences (a_n) and (b_n) when $\lim_{n\to\infty} |a_n - b_n| = 0$. Modulo this equivalence, we may label Cauchy sequences, say $\alpha = (a_n)$, and then call the set of all of these elements the real numbers. [A more precise treatment would show that the set $\mathcal{I}$ of Cauchy sequences with limit 0 forms an ideal in $\mathcal{R}$, and then that the quotient $\mathcal{R}/\mathcal{I}$ inherits the axioms for a field, and that $|\cdot|$ can be extended to $\mathcal{R}/\mathcal{I}$ with the usual properties for the real numbers satisfied with this definition of $|\cdot|$. But we are being sketchy here, and so we will not get bogged down in such details.] One can prove that $\mathbb{R}$ is complete with respect to the absolute value $|\cdot|$ inherited from $\mathbb{Q}$, and we refer to $\mathbb{R}$ as being the completion of $\mathbb{Q}$ with respect to $|\cdot|$.

We now define a substitute for the absolute value that measures the power of a given prime dividing the argument.

Definition 0.1. Let p be a prime number. Any non-zero rational number α can be written uniquely in the form $\alpha = p^r u/v$, where $u \in \mathbb{Z}$, $v \in \mathbb{N}$ and $r \in \mathbb{Z}$, such that $p \nmid uv$ and $(u, v) = 1$. We define the *p-adic absolute value* $|\cdot|_p$ by setting $|0|_p = 0$, and when $\alpha \in \mathbb{Q} \setminus \{0\}$, by putting $|\alpha|_p = p^{-r}$, with r defined as above.

Exercises (i) Show that $|\alpha|_p \geqslant 0$ for all $\alpha \in \mathbb{Q}$, with equality only for $\alpha = 0$; (ii) that $|\alpha\beta|_p = |\alpha|_p|\beta|_p$ for all $\alpha, \beta \in \mathbb{Q}$; (iii) that $|\alpha + \beta|_p \leqslant \max\{|\alpha|_p, |\beta|_p\}$ for all $\alpha, \beta \in \mathbb{Q}$.

The last inequality is known as the *ultrametric inequality*, and constitutes a stronger version of the triangle inequality.

Now define Cauchy sequences in $\mathbb{Q}$ with respect to $|\cdot|_p$ just as in the classical situation above. We say that $(a_n)_{n=1}^{\infty}$ is Cauchy with respect to the p-adic absolute value if, whenever $\varepsilon > 0$, there exists a positive number $N(\varepsilon)$ such that whenever $n > m > N(\varepsilon)$, one has $|a_n - a_m|_p < \varepsilon$. Define next

$$\mathcal{Q}_p = \{(a_n)_{n=1}^{\infty} : a_n \in \mathbb{Q} \text{ for each } n, \text{ and } (a_n) \text{ is Cauchy with respect to } |\cdot|_p\}.$$

One can show that $\mathcal{Q}_p$ forms a ring under addition and multiplication defined coordinatewise in the obvious fashion. Now identify two Cauchy sequences (a_n)

and (b_n) when $\lim_{n\to\infty} |a_n - b_n|_p = 0$. Modulo this equivalence, we may label Cauchy sequences, say $\alpha = (a_n)$, and then call the set of all of these elements the p-adic numbers $\mathbb{Q}_p$. [Again, a more precise treatment would show that the set $\mathcal{I}_p$ of Cauchy sequences with limit 0 forms an ideal in $\mathcal{Q}_p$, and then that the quotient $\mathcal{Q}_p/\mathcal{I}_p$ inherits the axioms for a field, and that $|\cdot|_p$ can be extended to $\mathcal{Q}_p/\mathcal{I}_p$ with properties analogous to those satisfied by $|\cdot|_p$ on $\mathbb{Q}$ enjoyed by $|\cdot|_p$ on $\mathbb{Q}_p$. Again, we are being sketchy here, and so we avoid getting bogged down in such details.] One can prove that $\mathbb{Q}_p$ is complete with respect to the p-adic absolute value $|\cdot|_p$ inherited from $\mathbb{Q}$, and we refer to $\mathbb{Q}_p$ as being the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Example 0.2 (Conway and Sloane)**.** We give an example of a sequence in $\mathbb{Q}$ with respect to $|\cdot|_5$ that has a limit in $\mathbb{Q}_5$ that can be interpreted as $2/3$. Consider the sequence $(a_n)_{n=1}^{\infty}$ defined by $a_1 = 4$, $a_2 = 34$, $a_3 = 334$, $\ldots$, and in general $a_n = \lceil 10^n/3 \rceil$. Then for every natural number n, one has $3a_n - 2 = 10^n$, and hence $|3a_n - 2|_5 = 5^{-n}$. Thus we see that $\lim_{n\to\infty} |3a_n - 2|_5 = 0$, whence (a_n) converges in the 5-adic sense to $2/3$.

Remark 0.3. One has $\sum_{n=0}^{\infty} a_n$ converges in $\mathbb{Q}_p \iff \lim_{n\to\infty} a_n = 0$.

Write s_N for the partial sum $\sum_{n=0}^{N} a_n$. Then in order to justify this remark, note on the one hand that if $\sum_{n=0}^{\infty} a_n$ converges, then

$$\lim_{N\to\infty} a_N = \lim_{N\to\infty} (s_N - s_{N-1}) = \lim_{N\to\infty} s_N - \lim_{M\to\infty} s_M = 0.$$

On the other hand, if $\lim_{n\to\infty} a_n = 0$, then given any positive number ε, there exists a positive number $N(\varepsilon)$ such that whenever $n > N(\varepsilon)$, then one has $|a_n|_p < \varepsilon$. But then whenever $N > M > N(\varepsilon)$, one has

$$|s_N - s_M|_p = |a_{M+1} + \cdots + a_N|_p \leqslant \max_{M<n\leqslant N} |a_n|_p < \varepsilon,$$

by making use of the ultrametric inequality. Thus we see that (s_N) is a Cauchy sequence with respect to $|\cdot|_p$, and hence has a limit.

The set of p-adic numbers with absolute value at most 1 is known as the p-adic *integers* $\mathbb{Z}_p$, so that $\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leqslant 1\}$. Notice that the set of integers $\mathbb{Z}$ can be naturally embedded into $\mathbb{Z}_p$, and likewise $\mathbb{Q}$ can be naturally embedded into $\mathbb{Q}_p$.

Fact 0.4. If $\alpha \in \mathbb{Q}_p$, then for some non-negative integer N, one can write α in the shape

$$\alpha = \sum_{n=-N}^{\infty} a_n p^n,$$

in which the coefficients a_i lie in the set $\{0, 1, \ldots, p-1\}$.

One can check, for example, that in $\mathbb{Q}_7$,

$$\frac{1}{5} = 3 + 1\cdot 7 + 4\cdot 7^2 + 5\cdot 7^3 + 2\cdot 7^4 + 1\cdot 7^5 + \ldots.$$

Theorem 0.5 (Hensel's lemma revisited). *Let $f \in \mathbb{Z}_p[x]$, and suppose that a is an integer satisfying the condition $|f(a)|_p < |f'(a)|_p^2$. Then there exists a unique p-adic integer α such that*

$$f(\alpha) = 0 \quad \textit{and} \quad |\alpha - a|_p \leqslant |f'(a)|_p^{-1}|f(a)|_p.$$

Example 0.6. We saw earlier that the congruence $2^2 + 1 \equiv 0 \pmod 5$ gives rise to a chain of solutions to the congruence $x^2 + 1 \equiv 0 \pmod{5^n}$. On writing $f(x) = x^2 + 1$, we have $|f(2)|_5 = |5|_5 = 5^{-1}$, and $|f'(2)|_5 = |2 \cdot 2|_5 = 1$, whence $|f(2)|_5 < |f'(2)|_5^2$. Then it follows from the 5-adic version of Hensel's lemma that there exists $\alpha \in \mathbb{Z}_5$ for which $f(\alpha) = 0$ and $|\alpha - 2|_5 \leqslant 5^{-1}$. If we simply choose the truncation of the 5-adic expansion of α modulo 5^n, say α_n, then of course we obtain a solution $x = \alpha_n$ of the congruence $x^2 + 1 \pmod{5^n}$. In this sense, the 5-adic solution $x = \alpha$ of the equation $x^2 + 1 = 0$ encodes information concerning all of the associated congruences modulo 5^n.

We finish this sketch of the p-adic numbers by pointing out that the interaction between completion and algebraic closure is not as simple for the p-adic numbers as for the real numbers. Thus, the completion of $\mathbb{Q}$ with respect to the ordinary absolute value $|\cdot|$ is $\mathbb{R}$, and the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$, the latter being both complete and algebraically closed. Given a prime number p on the other hand, the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$ is $\mathbb{Q}_p$, and the algebraic closure of $\mathbb{Q}_p$ is a larger field $\overline{\mathbb{Q}}_p$. It transpires that $\overline{\mathbb{Q}}_p$ is not itself complete (in contrast to the situation for $\mathbb{C}$). It is possible to extend the absolute value $|\cdot|_p$ to a p-adic absolute value $\|\cdot\|_p$ on $\overline{\mathbb{Q}}_p$, then complete the latter with respect to $\|\cdot\|_p$. The result is a field $\widehat{\overline{\mathbb{Q}}}_p$ which is both complete and algebraically closed. This represents the proper p-adic analogue of the complex numbers.

Figure 3.