INTRODUCTION TO p-ADIC NUMBERS (MA2316, FIFTH WEEK)

VLADIMIR DOTSENKO

Last time, we discussed Hensel's lemma which ensured that under some technical assumptions it is possible to "lift" a solution modulo p^n to a solution modulo p^{n+1}. Here lift means that the two solutions actually agree modulo a high power of p (at least $p^{n/2}$). This means that as we keep lifting solutions so that the equation is satisfied modulo higher and higher powers of p, the digits in the base p expansions of those solutions stabilise, since we are only adding multiples of higher and higher powers of p.

Example. *The equation* $x^2 \equiv 5 \pmod{11}$ *has a solution* $x = 4$. *Also,* $(x^2-5)' = 2x$, *so the value of the derivative at* $x = 4$ *is not divisible by* 11, *and hence Hensel's lemma is applicable, and we may lift solutions higher up. For modulo* 11^2 *solutions, look for it in the form* $4 + 11k$, *then*

$$(4+11k)^2 - 5 \equiv 11 + 88k = 11(1+8k) \pmod{11^2},$$

so $k = 4$ *would do. For modulo* 11^3 *solutions, look for it in the form* $4 + 11 \cdot 4 + 11^2 l = 48 + 11^2 l$. *We have*

$$(48+11^2 l)^2 - 5 \equiv 2299 + 2 \cdot 48 \cdot 11^2 l = 11^2(19+96l) \pmod{11^3}.$$

To satisfy the congruence modulo 11^3, *we need* $19 + 96l \equiv -3 - 3l \pmod{11}$, *so* $l = 10$, *and so on. Since at further steps we shall be adding multiples of* 11^3, *we may conclude that the last digit of the base* 11 *representation of each solution will be* 4, *the next-to-last one will be* 4, *the previous one* 10 *etc.*

These digits do stabilise, but of course the problem is that the numbers we construct generally keep growing, so their base p expansions get longer and longer. Therefore, this stabilisation of digits does not lead to an "honest" integer after infinitely many iterations. That infinite base p expansion does not make sense if we restrict ourselves to real or complex numbers. However, it turns out that there is a field where expansions like that naturally belong.

Definition. *We shall say that a function* $\|\cdot\|\colon \mathbb{Q} \to \mathbb{R}_+ = \{x \in \mathbb{R}\colon x \geq 0\}$ *is an* absolute value *if*

- $\|x\| = 0$ *if and only* $x = 0$,
- $\|x \cdot y\| = \|x\| \cdot \|y\|$ *for all* x, y,
- $\|x + y\| \leq \|x\| + \|y\|$.

Example. *The usual absolute value* $|x|$ *is an absolute value on* $\mathbb{Q}$.

Example. *The* p*-adic absolute value defined as*

$$\|x\|_p = \begin{cases} p^{-k}, & \text{if } 0 \neq x = p^k \frac{a}{b} \text{ with } \gcd(a,p) = \gcd(b,p) = 1, \\ 0, & \text{if } x = 0. \end{cases}$$

is an absolute value on $\mathbb{Q}$ *satisfying the "ultrametric inequality"*

$$\|x+y\|_p \leq \max(\|x\|_p, \|y\|_p).$$

In fact, and that is an interesting thing on its own, every absolute value on rationals can be derived from the two examples we just mentioned. Let us prove it.

Theorem 1 (Ostrowski)**.** *Suppose that $\|\cdot\|$ is an absolute value on rational numbers. Then either there exists a nonnegative real number c such that $\|x\| = |x|^c$ for all x or there exists a nonnegative real number c and a prime p such that $\|x\| = \|x\|_p^c$ for all x.*

Proof. Let us consider the values $\|n\|$, where n is a positive integer.

Suppose that $\|m\| > 1$ for some m. Let us take some other number n and consider the base n expansion of some power m^r:

$$m^r = a_0 n^k + a_1 n^{k-1} + \cdots + a_{k-1} n + a_k,$$

where $0 \le a_i \le n-1$, and $k \le \log_n(m^r) = r \log_n(m)$. We have

$$\|m\|^r = \|m^r\| \le \|a_0\|\|n\|^k + \|a_1\|\|n\|^{k-1} + \cdots + \|a_{k-1}\|\|n\| + \|a_k\| \le (k+1) \left(\max_{0 \le s \le n-1} \|s\| \right) \|n\|^k,$$

therefore

$$\|m\| \le \sqrt[r]{(k+1) \max_{0 \le s \le n-1} \|s\|} \|n\|^{\frac{k}{r}} \le C^{1/r} \|n\|^{\log_n(m)},$$

where $C = (k+1) \max\limits_{0 \le s \le n-1} \|s\|$ does not depend on r. Therefore, as $r \to \infty$, we have

$$\|m\| \le \|n\|^{\log_n(m)} = \|n\|^{\frac{\ln(m)}{\ln(n)}},$$

or

$$\|m\|^{\frac{1}{\ln(m)}} \le \|n\|^{\frac{1}{\ln(n)}}.$$

From this, we deduce that $\|n\| > 1$ for all $n > 1$, and then, swapping the roles of n and m, that

$$\|m\|^{\frac{1}{\ln(m)}} = \|n\|^{\frac{1}{\ln(n)}}.$$

Denoting $\|m\|^{\frac{1}{\ln(m)}} = e^c$, we see that $\|m\| = m^c$ for all positive integers $m > 1$. Also, $\|\pm 1\| = 1$ for any absolute value since $\|1\|^2 = \|1^2\| = \|1\| = \|(-1)^2\| = \|-1\|^2$, therefore $\|m\| = |m|^c$ for all integers m, and finally since $\left\|\frac{p}{q}\right\| \|q\| = \left\|\frac{p}{q} q\right\| = \|p\|$, we have $\|r\| = |r|^c$ for all rational numbers r.

The only case we have not covered yet is that of $\|n\| \le 1$ for all positive integers n (and hence for all integers n since $\|-1\| = 1$). Let us take the smallest positive n for which $\|n\| < 1$. (If no such n exists, it is easy to show that $\|r\| = 1$ for all rational r. This number must be prime, for if it is not a prime, $n = n_1 n_2$, we have $\|n\| = \|n_1\|\|n_2\|$, and by minimality of n we conclude that $\|n_1\| = \|n_2\| = 1$, a contradiction with $\|n\| < 1$. Thus $n = p$ is a prime number. Let us show that for all other primes q we have $\|q\| = 1$. Assume the contrary. Then there exists a number N such that $\|p\|^N < \frac{1}{2}$ and $\|q\|^N < \frac{1}{2}$. We have $ap^N + bq^N = 1$ for some integers a, b since p^N and q^N are coprime. Hence

$$1 = \|1\| = \|ap^N + bq^N\| \le \|a\|\|p\|^N + \|b\|\|q\|^N \le 1 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = 1,$$

a contradiction. Let $\|p\| = \lambda < 1$. Denoting $c = -\log_p \lambda$, we see that $\|p\| = \|p\|_p^c$. Also, for any other prime q we trivially have $\|q\| = \|q\|_p^c$, hence as above $\|n\| = \|n\|_p^c$ for all integers n, and $\|r\| = \|r\|_p^c$ for all rational numbers r. □

Back to the main topic, one of the ways to use an absolute value is to define a metric $d(x, y) = \|x - y\|$, and to complete $\mathbb{Q}$ with respect to that metric (that is, look at equivalence classes of Cauchy sequences with respect to that metric). If we take the usual absolute value, we get $\mathbb{R}$. If we take $\|\cdot\|_p$, we get what is called the field of p-adic numbers and is denoted $\mathbb{Q}_p$. A sequence of integer numbers is a Cauchy sequence if and only if their differences are divisible by higher and higher powers of p. Thus, the solutions constructed by the method of Hensel's lemma form a Cauchy

sequence, which converges in $\mathbb{Q}_p$ to an element which is a genuine solution to the corresponding equation.

If a polynomial equation has a rational solution, it has a p-adic solution, since $\mathbb{Q} \subset \mathbb{Q}_p$. Of course, the variety of roots for p-adic equations is wider,, for example in the beginning of this note we essentially proved that $\sqrt{5}$ exists in $\mathbb{Q}_{11}$. It turns out that there are classes of polynomial equations for which one can prove that they have rational solutions if and only if they have real solutions and they have p-adic solutions for all p. For example, all quadratic equations, possibly with many unknowns, satisfy that property ("Hasse–Minkowski principle"). This makes dealing with equations like that much easier, since checking existence of solutions in real numbers can be done using tricks from analysis, and checking existence of solutions in p-adic numbers usually just requires solving equations modulo p and applying Hensel's lemma. In our upcoming classes, we shall also discuss equations for which these methods are not applicable, and outline several approaches to them.