

Berkeley Math Circle. September 24, 2000.
A. Givental. Introduction to p -adic numbers

Definition. A *norm* on the field \mathbb{Q} of rational numbers is a function $r \mapsto \|r\|$ taking values in the set of non-negative real numbers satisfying (i) $\|r\| > 0$ unless $r = 0$; (ii) $\|rr'\| = \|r\| \cdot \|r'\|$; (iii) $\|r + r'\| \leq \|r\| + \|r'\|$.

Examples of norms: (a) $\|r\|_\infty := |r|$. (b) For any prime p put $\|r\|_p = 1/p^k$ if $r = p^k m/n$ where k is an integer, and m, n are not divisible by p . (c) The *trivial* norm $\|r\| = 1$ unless $r = 0$. (d) Norms *equivalent* to $\|\cdot\|_p$ are obtained as $\|\cdot\|_p^\alpha$ where $\alpha > 0$ for $p \neq \infty$ and $1 > \alpha > 0$ for $p = \infty$.

Theorem (Ostrovsky). *Any non-trivial norm on \mathbb{Q} is equivalent to one of $\|\cdot\|_p$ with $p = 2, 3, 5, 7, \dots, \infty$.*

Given a norm, one measures distances between x and y as $\|x - y\|$. The field \mathbb{Q}_p of *p -adic numbers* is constructed as the *completion* of \mathbb{Q} with respect to the norm $\|\cdot\|_p$. Informally speaking, it consists of all “things” which can be approximated by rationals as $\|\cdot\|_p$ -closely as desired. In fact we have $\mathbb{Q}_\infty = \mathbb{R}$, the field of real numbers.

For $p \neq \infty$, consider sequences $a = \dots a_n \dots a_2 a_1 a_0 . a_{-1} \dots a_{-m}$, of base- p digits, $a_i = 0, 1, \dots, p - 1$, infinite to the left. One can perform addition, subtraction, multiplication and division following the middle-school rules for base- p numbers. With these operations, the set of all such sequences forms the field of p -adic numbers \mathbb{Q}_p . One extends the norm to p -adic numbers by $\|a\|_p := p^{-k}$ where k is the position of the rightmost non-zero digit a_k .

Problems.

- (a) Show that any norm satisfies $\|0\| = 0, \|\pm 1\| = 1$.
(b) Explain in words the meaning of the inequality $\|r\|_p \leq 1$ for a rational number r .
(c) Show that a rational number r satisfying $\|r\|_p \leq 1$ for all primes p is an integer.
(d) Prove that $\|p^N!\|_p = (p^N - 1)/(p - 1)$. Let $s_p(n)$ denote the sum of base- p digits of n . Check that $n - s_p(n)$ is divisible by $p - 1$. Put $k_p(n) = (n - s_p(n))/(p - 1)$ and prove that $\|n!\|_p = 1/p^{k_p(n)}$.
- Show that in \mathbb{Q}_p
 - $p^n \rightarrow 0$ when $n \rightarrow \infty$.
 - For any integers a_k the series $a_0 + a_1 p + a_2 p^2 + \dots + a_k p^k + \dots$ converges.
 - $-1 = \dots aaaaa.0$ where $a = p - 1$.
 - Rational numbers are characterized as sequences of base- p digits infinite to the left and periodic beginning with some place.
 - The series $\ln(1 + x) = x - x^2/2 + x^3/3 - x^4/4 + \dots$ and $\exp(x) = 1 + x + x^2/2 + \dots + x^n/n! + \dots$ converge if and only if $\|x\|_p < 1$.

3. (a) Show that in \mathbb{Q}_5 the equation $x^2 = a$ has a solution if and only if the rightmost non-zero digit a_k of a has even position k and is equal to 1 or 4.

(b) Compute a few last digits of $\sqrt{-1}$ in \mathbb{Q}_5 . How many such roots are there?

(c) Describe p -adic numbers which have square roots in \mathbb{Q}_p for $p \neq 2$; for $p = 2$.

(d) For which 5-adic numbers a, b does the equation $x^2/a + y^2/b = 1$ has a solution (x, y) in \mathbb{Q}_5 ?

4. Denote \mathbb{Z}_p the set of p -adic integers, that is p -adic numbers a with $\|a\|_p \leq 1$.

(a) Check that all rational integer numbers are p -adic integers.

(b) Which rational numbers are p -adic integers?

(c) Show that p -adic integers can be approximated by rational integers as $\|\cdot\|_p$ -precisely as desired.

(d) Prove that any infinite sequence of p -adic integers has a subsequence convergent in \mathbb{Z}_p .

(e) Let $F(x)$ be a polynomial with integer rational coefficients. Derive from (d) that the equation $F(x) = 0$ has a solution in \mathbb{Z}_p if and only if the congruence $F(x) \equiv 0 \pmod{p^k}$ has a solution for each $k = 1, 2, 3, \dots$

5. Let a be an integer rational number. Prove that the sequence a^{p^n} converges in \mathbb{Z}_p when $n \rightarrow \infty$, and that the limit, denoted $\text{sgn}_p(a)$ and called p -adic sign of a , satisfies $\text{sgn}_p(a) \equiv a \pmod{p}$, $\text{sgn}_p(a)^p = \text{sgn}_p(a)$ and $\text{sgn}_p(ab) = \text{sgn}_p(a)\text{sgn}_p(b)$. Derive that the equation $x^p = x$ has p distinct solutions in \mathbb{Z}_p . Examine the example $p = 5$.

6. (a) Introduce \mathbb{Z}_{10} using decimal digits and their sequences $\dots a_2 a_1 a_0$. infinite to the left. Identify \mathbb{Z}_{10} with the Cartesian product $\mathbb{Z}_2 \times \mathbb{Z}_5$ equipped with component-wise operations of addition and multiplication.

(b) Show that for any natural k there exist exactly four k -digit endings, $\dots 000000$. $\dots 000001$. $\dots 890625$. $\dots 109376$. , which reproduce themselves under multiplication (that is $N_1 N_2$ has this ending whenever both N_1 and N_2 do).

7. The Hilbert symbol $(a, b)_p$ is defined to be 1 if the equation $x^2/a + y^2/b = 1$ has a solution (x, y) in \mathbb{Q}_p and -1 if it does not have a solution in \mathbb{Q}_p .

(a) Show that $(a, b)_p = 1$ if at least one of a, b has square roots in \mathbb{Q}_p , that $(a, b)_p = (b, a)_p$, $(a, -a)_p = 1$, and $(a, b)_\infty = -1$ if and only if both $a, b < 0$.

(b) Prove that $(a, bc)_p = (a, b)_p (a, c)_p$.

(c) Show that (a) and (b) reduce computation of Hilbert symbols to that of $(p, a)_p$ and $(b, c)_p$ with $\|a\|_p = \|b\|_p = \|c\|_p = 1$.

(d) Show that for $p \neq 2$ and a, b, c as in (c) we have $(p, a)_p = -1$ if and only if a has no square roots in \mathbb{Q}_p , and $(b, c)_p = 1$.

(e) Show that for given a, b the set of primes p such that $(a, b)_p = -1$ is finite.

Theorem (Hilbert). $(a, b)_2 (a, b)_3 \dots (a, b)_p \dots (a, b)_\infty = 1$.

Theorem (Hasse – Minkovsky). *The equation $x^2/a + y^2/b = 1$ has a solution (x, y) in \mathbb{Q} if and only if it has a solution in \mathbb{Q}_p for each $p = 2, 3, \dots, \infty$ (in other words — if $(a, b)_p = 1$ for all $p = 2, 3, \dots, \infty$).*