The p-adic Numbers

Akhil Mathew

ABSTRACT. These are notes for the presentation I am giving today, which itself is intended to conclude the independent study on algebraic number theory I took with Professor Candiotti this spring.

The standard absolute value on $\mathbb{R}$: A review

Recall the following properties of the regular absolute value $|\cdot|_\infty$ on $\mathbb{R}$:

- $|x|_\infty \geq 0$ with equality iff $x = 0$
- $|xy|_\infty = |x|_\infty |y|_\infty$, $x, y \in \mathbb{R}$
- $|x + y|_\infty \leq |x|_\infty + |y|_\infty$ (Triangle inequality)

The standard absolute value induces a notion of *distance* between two elements of $\mathbb{R}$, the distance between x, y being

$$|x - y|_\infty .$$

Absolute values are studied on more general fields in algebra.

The p-adic valuation on $\mathbb{Q}$

We define the p-adic valuation: If $x \neq 0$ is an integer, p a fixed prime, p^r the maximum power dividing x,

$$\boxed{|x|_p = \left(\frac{1}{2}\right)^r .}$$

If $r \in \mathbb{Q}$, we have $r = a/b$ for $a, b \in \mathbb{Z}$, and we set

$$|r|_p = \frac{|a|_p}{|b|_p}.$$

This is the *p-adic absolute value*, defined only on $\mathbb{Q}$. (Also $|0|_p = 0$.)

- $|x|_p \geq 0$ with equality iff $x = 0$
- $|xy|_p = |x|_p |y|_p$, $x, y \in \mathbb{Q}$
- $|x + y|_p \leq \max(|x|_p , |y|_p)$ (Non-archimedean inequality: this is *stronger* than the Triangle Inequality)

---

p-adic Distance

We can define a new *distance* and thus a topology on $\mathbb{Q}$ from the valuation $|\cdot|_p$: the distance between x, y is

$$|x - y|_p .$$

x, y are close *iff $x - y$ is divisible by a high power of p.*

A sequence $\{a_n\}$ in $\mathbb{Q}$ *converges p-adically* to a if to all $\epsilon > 0$, there exists M such that

$$n > M \text{ implies } |a_n - a|_p < \epsilon, \text{ or } \lim |a_n - a|_p = 0.$$

A sequence $\{a_n\}$ is *p-adically Cauchy* if to $\epsilon > 0$, there is S s.t.

$$m, n > S \to |a_n - a_m|_p < \epsilon.$$

Unlike in $\mathbb{R}$, a p-adically Cauchy sequence *need not converge p-adically!*

Completions and $\mathbb{Q}_p$

$\mathbb{R}$ is the *completion* (= filling in holes appropriately) of $\mathbb{Q}$ w.r.t. the standard absolute value.

The *p-adic numbers* $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ w.r.t. the valuation $|\cdot|_p$.

- Addition, subtraction, multiplication, division extend to the completion—$\mathbb{Q}_p$ is a *field*
- $\mathbb{Q} \subset \mathbb{Q}_p$, just as $\mathbb{Q} \subset \mathbb{R} = \mathbb{Q}_\infty$
- The absolute value $|\cdot|_p$ extends to $\mathbb{Q}_p$ by continuity ($\mathbb{Q}$ is dense in $\mathbb{Q}_p$)
- $\mathbb{Q}_p$ is complete with respect to the extended $|\cdot|_p$: *Any Cauchy sequence in $\mathbb{Q}_p$ has a limit in $\mathbb{Q}_p$*

Infinite sums in $\mathbb{Q}_p$

Let $\{a_n\}$ be a sequence in $\mathbb{Q}_p$. We say that $\sum_{j=0}^{\infty} a_j = a$ *converges* to $a \in \mathbb{Q}_p$ if the partial sums $S_n = \sum_{j=0}^{n} a_j$ converge to a.

THEOREM. *The sum $\sum_{j=0}^{\infty} a_j$ converges if and only if $\lim a_j = 0$.*

PROOF. One implication: straightforward. Suppose $a_j \to 0$; pick $\epsilon > 0$ and choose N large so that $n > N \to |a_n|_p < \epsilon$. Then

$$m, n > N \text{ means } |S_n - S_m|_p = \left| \sum_{j=\min(m,n)+1}^{\max(m,n)} a_n \right|_p \leq \max_{j > N} |a_j|_p < \epsilon,$$

so the partial sums are Cauchy and consequently converge. □

An example

By substituting $x = 2$ in the identity $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots$, Euler erroneously concluded $1 + 2 + 4 + \cdots = -1$ in $\mathbb{R}$.

EXAMPLE. *In $\mathbb{Q}_2$,*

$$1 + 2 + 4 + 8 + \cdots = -1.$$

Indeed,

$$S_n = \sum_{j=0}^{n} 2^j = 2^{n+1} - 1,$$

so

$$|S_n - (-1)|_2 = (0.5)^{n+1} \to 0 \text{ as } n \to \infty.$$

COROLLARY. *$\mathbb{Q}_2$ is not an ordered field.*

The Heine-Borel Theorem

THEOREM (Heine-Borel). *A set in $\mathbb{R}$ is compact if it is closed and bounded.*

This makes sense for $\mathbb{Q}_p$ too, where point-set topology works similarly.
Let $A \subset \mathbb{Q}_p$. A is *open* if for $x \in A$, there is $s > 0$ s.t.

$$N_s(x) \equiv \{y : |y - x|_p < s\} \subset A;$$

A is *closed* if $\mathbb{Q}_p - A$ is open. $B \subset \mathbb{Q}_p$ is *compact* if every open covering of B has a finite subcovering. C is called *bounded* if there exists $M > 0$ such that $x \in C$ implies $|x|_p \leq C$.
Notice how similar these notions are to $\mathbb{R}$!

THEOREM (p-adic Heine-Borel). *A set in $\mathbb{Q}_p$ is compact if it is closed and bounded.*

The ring $\mathbb{Z}_p$

We define

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\};$$

this is the analog of the unit interval in $\mathbb{R}$.

THEOREM. *$\mathbb{Z}_p$ is a ring.*

PROOF. If $|x|_p \leq 1, |y|_p \leq 1$, then $|xy|_p = |x|_p |y|_p \leq 1$. Also $|x + y|_p \leq \max(|x|_p, |y|_p) \leq 1$. □

Notice how important the nonarchimedean property is.
Now $\mathbb{Z} \subset \mathbb{Z}_p$, and in fact $m/n \in \mathbb{Z}_p$ if $p \nmid n$.

THEOREM. *The ideals of $\mathbb{Z}_p$ are of the form $p^r \mathbb{Z}_p$ for $r \geq 0$. $\mathbb{Z}_p$ is thus a principal ideal domain.*

The p-adic expansion

A real number $x \in [0, 1]$ can be represented by a sum $\sum_{n \geq 0} b_n 2^{-n}$ where each $b_n \in \{0, 1\}$—the binary expansion. For p-adic numbers, the sum goes in the opposite direction:

THEOREM. *Any element $x \in \mathbb{Z}_p$ can be expressed uniquely as an infinite sum*

$$x = \sum_{n \geq 0} a_n p^n = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \ldots,$$

where each $a_n = 0, 1, \ldots,$ or $p - 1$.

For $x \in \mathbb{Q}_p$, we have a similar expansion, but we may have a finite number of terms $a_n p^n$ with $n < 0$.

Addition via Power Series

EXAMPLE. *Given two p-adic integers x, y represented by $\{a_n\}, \{b_n\}$, we can add the power series term-by-term*

$$x + y = a_0 + b_0 + p(a_1 + b_1) + p^2(a_2 + b_2) + \ldots$$

and then "carry" to put this expansion in the canonical form with each coefficient in $\{0, 1, \ldots, p-1\}$. To multiply, we pretend we have two power series, multiply, and then do the reduction.

Consider the 5-adic numbers

$$x = 1 + 3(5) + 4(5^2) + \ldots, y = 2 + 4(5) + 3(5^2) + \ldots;$$

then

$$x + y = 3 + 2(5) + 3(5^2) + \ldots.$$

Square Roots of p-adic Integers near 1

Let $p \neq 2$.

Using the binomial series, we can take square roots of numerous p-adic integers.

THEOREM. *Let $x = 1 + p\alpha$, for $\alpha \in \mathbb{Z}_p$. Then there is $y \in \mathbb{Z}_p$ such that $y^2 = x$.*

PROOF. We take

$$y = 1 + \binom{1/2}{1} p\alpha + \binom{1/2}{2} (p\alpha)^2 + \ldots;$$

this is just the binomial series, and can be seen to converge because $|p|_p < 1$. □

EXAMPLE. *$\sqrt{7} \in \mathbb{Q}_3$ because $7 = 1 + 2(3)$.*

Square Roots, Part II ($p \neq 2$)

Given a p-adic integer $x \in \mathbb{Z}_p$, we can write $x = x_0 + p\alpha$, where $x_0 \in \mathbb{Z} \cap \{0, 1, \ldots, p-1\}$ and $\alpha \in \mathbb{Z}_p$ by the canonical expansion.

THEOREM. *Suppose $x_0 \neq 0$. x is a square in $\mathbb{Z}_p$ if and only if x_0 is a square mod p, i.e. if there exists $y_0 \in \mathbb{Z}$ such that*

$$y_0^2 \equiv x_0 \mod p.$$

In other words, one can tell if x is a square by looking at the residue of its first term mod p!

The Mahler Expansion

The *Mahler expansion* is a p-adic analog of Taylor expansions.

A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is *continuous* at $x_0 \in \mathbb{Z}_p$ if, to each $\epsilon > 0$, there is a $\delta > 0$ such that

$$|x - x_0|_p < \delta \to |f(x) - f(x_0)|_p < \epsilon.$$

Continuous functions can be expressed in terms of the *binomial coefficients* defined by

$$\binom{x}{n} = \frac{x(x-1)\ldots(x-n)}{n!}; \text{ this is a function on } \mathbb{Z}_p.$$

THEOREM (Mahler). *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be continuous. Then there exists a sequence $\{\beta_n\} \subset \mathbb{Q}_p$, with $\lim \beta_n = 0$, such that*

$$f(x) = \sum_{n=0}^{\infty} \beta_n \binom{x}{n}; \; x \in \mathbb{Z}_p.$$

Extensions of $\mathbb{Q}_p$ and $\mathbb{Q}$

A finite field extension $K/\mathbb{Q}_p$ is called a *local field*.

THEOREM. *Let $K/\mathbb{Q}_p$ be a local field. Then the absolute value $|\cdot|_p$ can be extended uniquely to K; with respect to the new absolute value, K is complete.*

The study of these local fields is an important aspect of algebraic number theory. E.g., compare the ring $\mathbb{Z}_p$ to the ring of elements of K whose absolute value is ≤ 1.

An extension L/K of fields is called *abelian* if it is Galois and the Galois group is abelian. Using local class field theory, one proves:

THEOREM (Local Kronecker-Weber). *Let $K/\mathbb{Q}_p$ be a finite abelian extension, so K is a local field. Then there exists a root of unity ζ_n such that $K \subset \mathbb{Q}_p(\zeta_n)$.*

Why does $\mathbb{Q}_p$ Matter?

The Hasse Principle: If something is true for $\mathbb{Q}_p$, all p, and for $\mathbb{R}$, then it is true for $\mathbb{Q}$.

We give examples.

THEOREM. *Suppose $x \in \mathbb{Q}$ and x has a square root in each field $\mathbb{Q}_p$ and in $\mathbb{R}$ (i.e. is positive). Then x has a square root in $\mathbb{Q}$ itself.*

THEOREM (Hasse-Minkowski). *Suppose a quadratic form (a homogeneous polynomial of degree 2 in several variables) $Q(X) = \sum_{i,j} a_{ij} X_i X_j$ over $\mathbb{Q}$ has a nontrivial root in each $\mathbb{Q}_p$ and in $\mathbb{R}$. Then Q has a nontrivial root in $\mathbb{Q}$.*

THEOREM (Global Kronecker-Weber). *Let $K/\mathbb{Q}$ be a finite abelian extension. Then $K \subset \mathbb{Q}(\zeta_n)$ for some n.*

References

[1] George Bachman. *Introduction to p-Adic Numbers and Valuation Theory*. Academic Press, 1964.
[2] Nicolas Bourbaki. *Commutative Algebra*. Hermann, 1972.
[3] J.W.S. Cassels. *Local Fields*. Cambridge University Press, 1986.
[4] Morris Kline. Euler and infinite series. *Mathematics Magazine*, 56(5):307–314, 1983.
[5] Serge Lang. *Algebraic Number Theory*. Springer, 1994.
[6] Kurt Mahler. *Introduction to p-Adic Numbers and their Functions*. Cambridge University Press, 1973.
[7] Jean-Pierre Serre. *Local Fields*. Springer, 1979.
[8] Jean-Pierre Serre. *A Course in Arithmetic*. Springer, 1996.