The World of p-adics

Isa Chou

ichou@unm.edu
University of New Mexico

Math 402, May 2024

Kurt Hensel

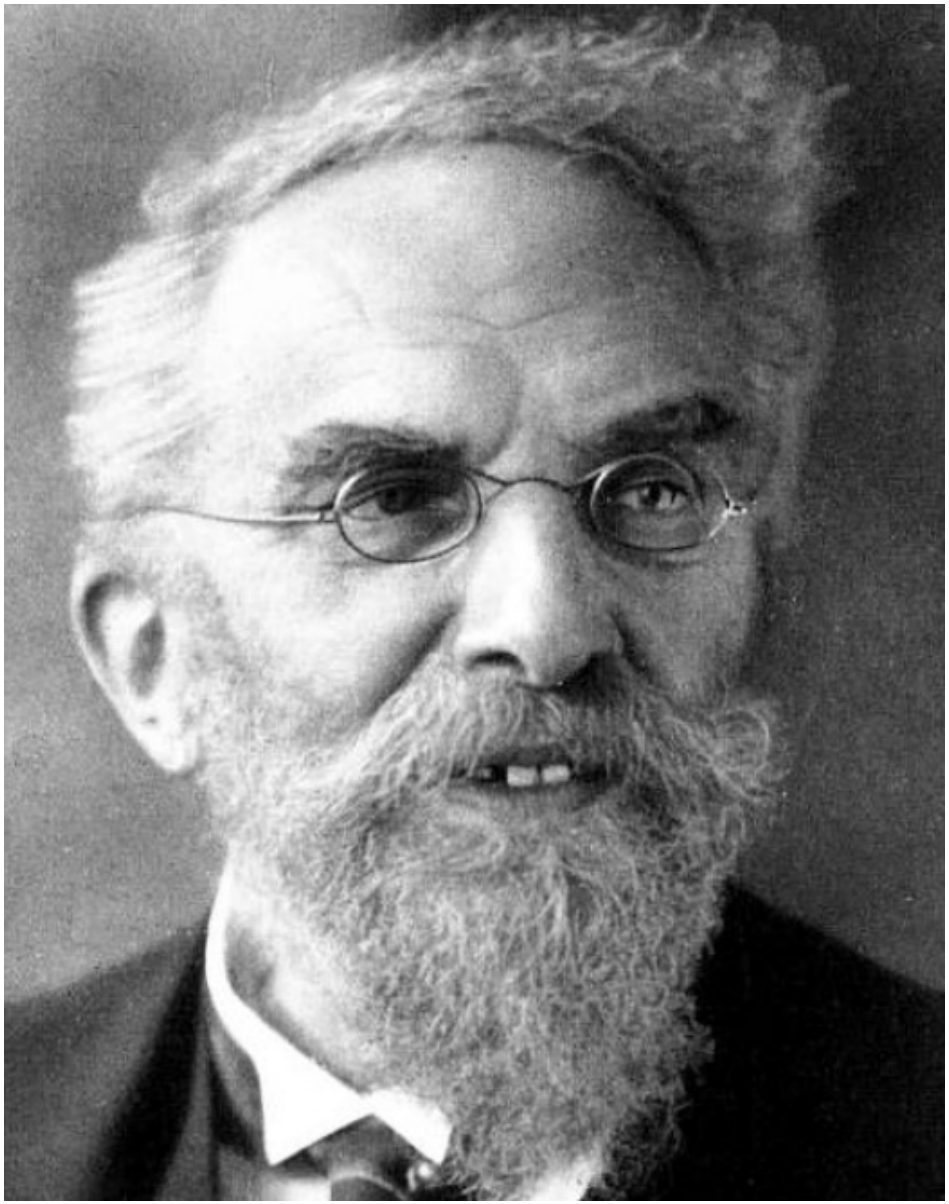
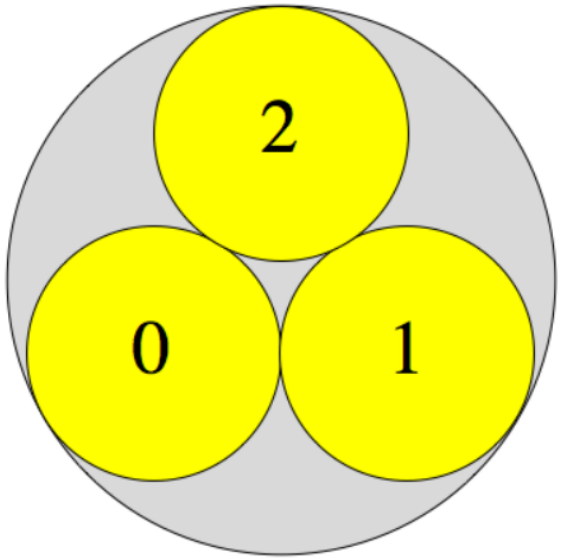
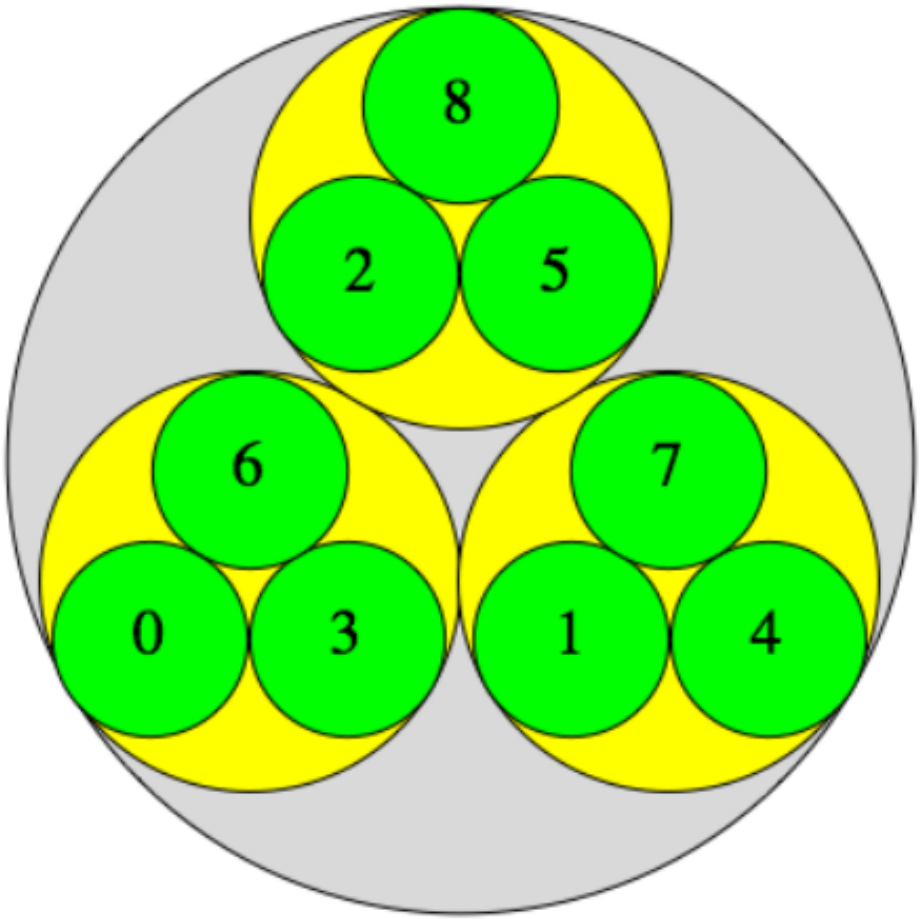


Table of Contents

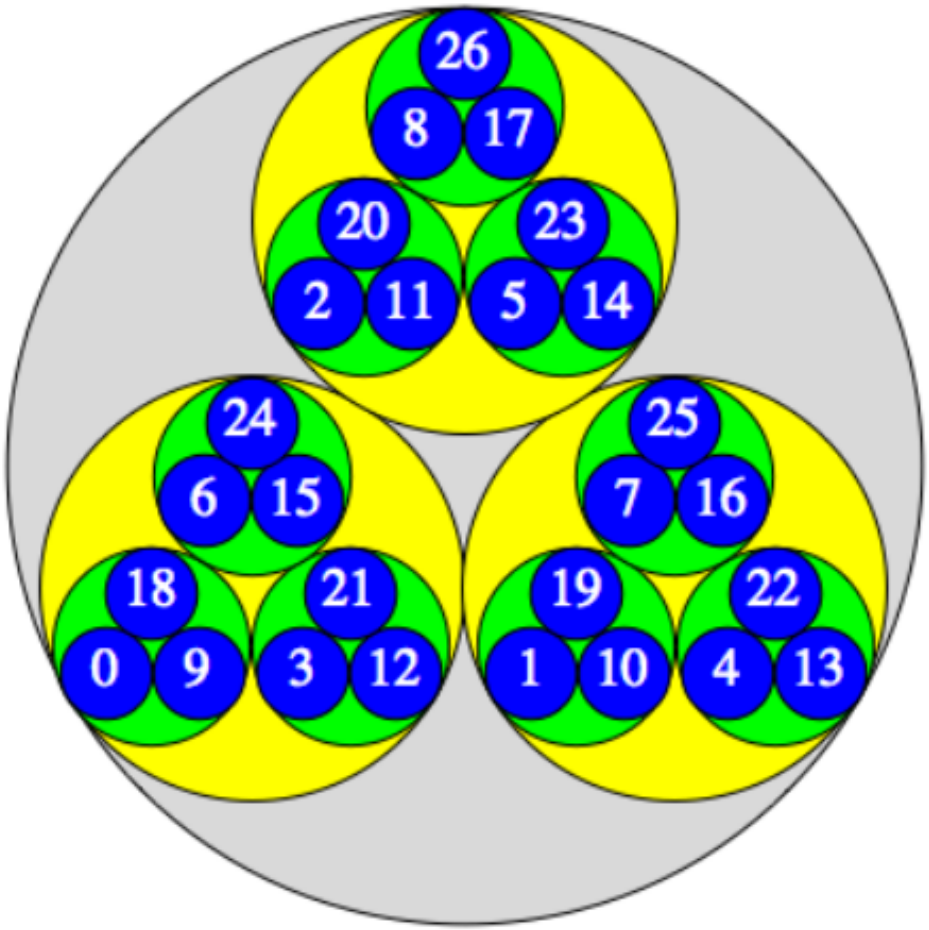
p-adic closeness



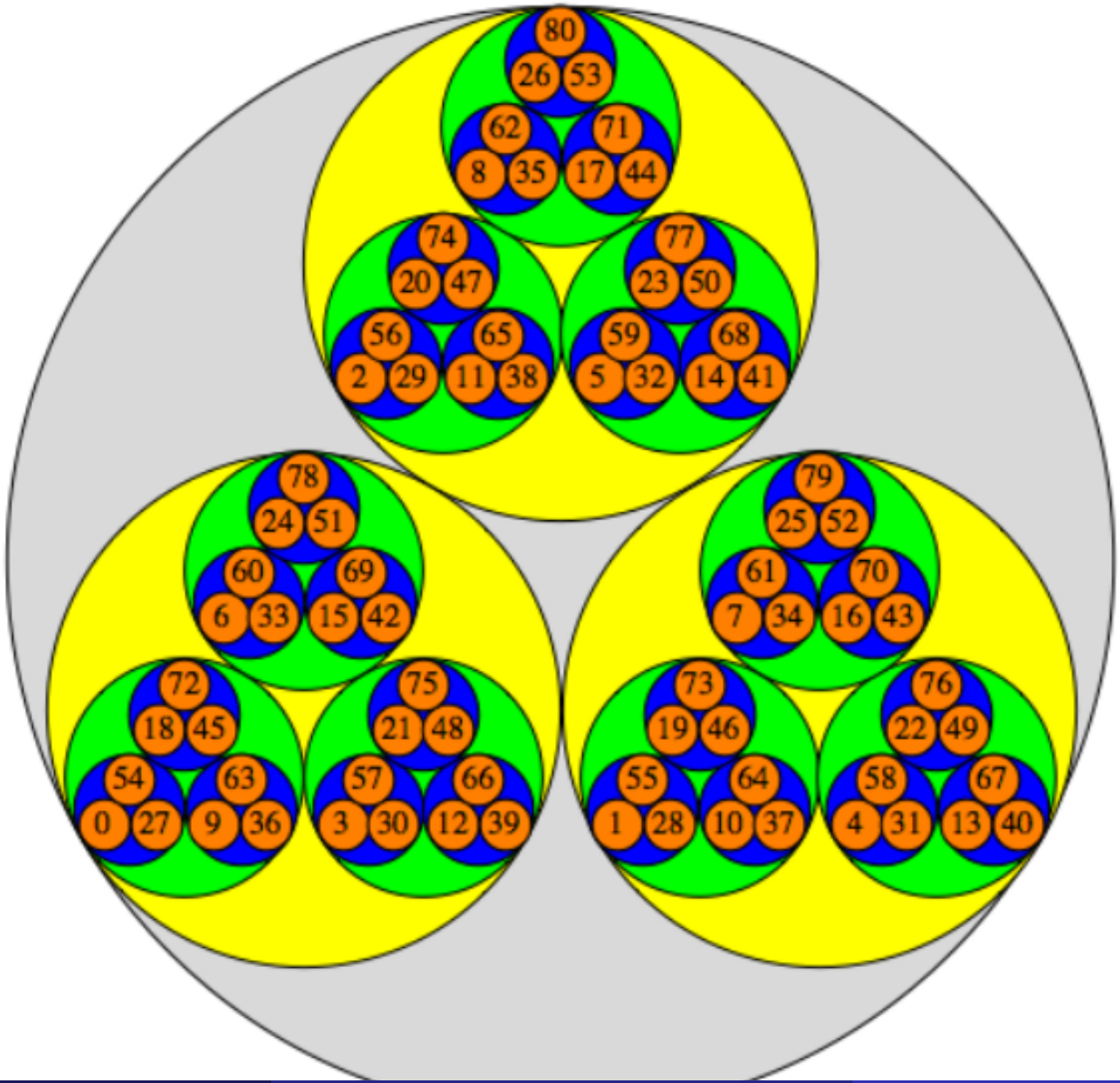
p-adic closeness



p-adic closeness



p-adic closeness



Absolute value and metric spaces

An absolute value is a function into the real numbers satisfying the following properties:

1. $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,
2. $|xy| = |x||y|$, and
3. $|x + y| \leq |x| + |y|$ (Triangle Inequality).

Absolute value and metric spaces

An absolute value is a function into the real numbers satisfying the following properties:

1. $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,
2. $|xy| = |x||y|$, and
3. $|x + y| \leq |x| + |y|$ (Triangle Inequality).

Additionally, if we have a stronger bound on the triangle inequality

$$|x + y| \leq \max\{|x|, |y|\}$$

the absolute value is called *non-Archimedean*.

Absolute value and metric spaces

An absolute value is a function into the real numbers satisfying the following properties:

1. $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,
2. $|xy| = |x||y|$, and
3. $|x + y| \leq |x| + |y|$ (Triangle Inequality).

Additionally, if we have a stronger bound on the triangle inequality

$$|x + y| \leq \max\{|x|, |y|\}$$

the absolute value is called *non-Archimedean*.
A metric on a set S is a function $d : S \times S \to \mathbb{R}_{\geq 0}$. An absolute value induces a metric defined by $d(x, y) = |x - y|$ for all $x, y \in S$.

Examples of absolute value

- The usual absolute value on $\mathbb{R}$ or $\mathbb{Q}$, which p-adic analysts call the Archimedian absolute value.

$$|x|_\infty = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

- The complex norm $\mathbb{C} \to \mathbb{R}, z \mapsto |z| = \sqrt{z\bar{z}}$ is also Archimedean.
- The trivial absolute value where $|x| = 1$ for $x \neq 0$, and $|0| = 0$.

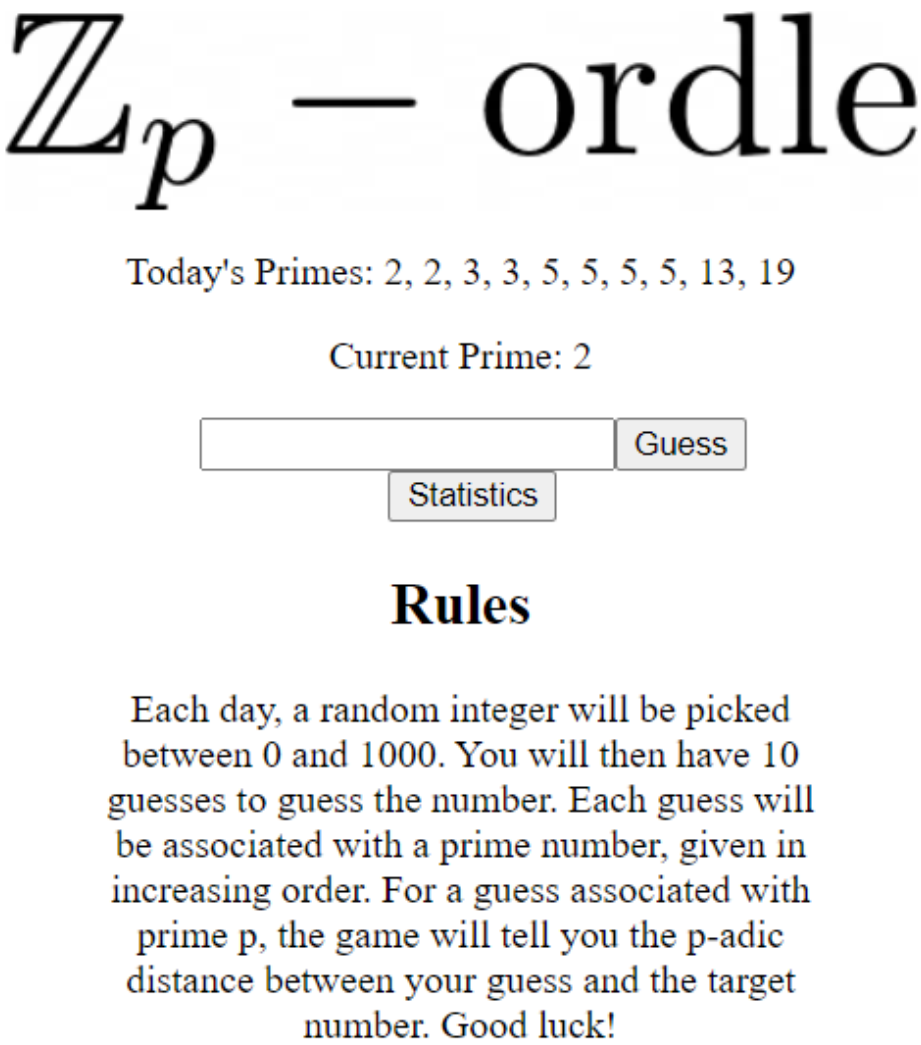
Examples of absolute value

- The usual absolute value on $\mathbb{R}$ or $\mathbb{Q}$, which p-adic analysts call the Archimedian absolute value.

$$|x|_\infty = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

- The complex norm $\mathbb{C} \to \mathbb{R}, z \mapsto |z| = \sqrt{z\bar{z}}$ is also Archimedean.
- The trivial absolute value where $|x| = 1$ for $x \neq 0$, and $|0| = 0$.
- The p-adic absolute value of q, $|q|_p$, defined such that when p is a fixed prime, for $q = \frac{p^a r}{s}$, $(r, s \in Z,\ p \nmid r, s)$, $|q|_p = p^{-a.}$ If $q = 0$, then $|q|_p$ is defined to be 0.

$\mathbb{Z}_p$-ordle



- An integer $0 \leq z \leq 1000$ is selected at random each day
- You have 10 guesses to find it, and 10 fixed primes p to do so with
- For each guess x, you will be given the absolute value $|x - z|_p$.
- Your goal is to raise the shared modulus - i.e, shrink the absolute value - so much that there are only a few equivalent numbers in the given range.
- When you guess the number, you have $|z - z|_p = 0$

$\mathbb{Z}_p$-ordle

- An integer $0 \leq z \leq 1000$ is selected at random each day
- You have 10 guesses to find it, and 10 fixed primes p to do so with
- For each guess x, you will be given the absolute value $|x - z|_p$.
- Your goal is to raise the shared modulus - i.e, shrink the absolute value - so much that there are only a few equivalent numbers in the given range.
- When you guess the number, you have $|z - z|_p = 0$

Ostrowski's Theorem

Two metrics d_1 and d_2 on a set X are equivalent if they are the same topologically, i.e, a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2.

Ostrowski's Theorem

Two metrics d_1 and d_2 on a set X are equivalent if they are the same topologically, i.e, a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2.

Ostrowski's Theorem.

Every non-trivial absolute value on the rational numbers $\mathbb{Q}$ is equivalent to either the usual real absolute value or a p-adic absolute value.

Also, $|\cdot|_p$ and $|\cdot|_q$ are nonisomorphic for $p \neq q$. So all but one absolute values on $\mathbb{Q}$ are p-adic!
p-adic analysts usually denote the usual Archimedean absolute value $|\cdot|_\infty$, because it functions like "mod ∞".

Table of Contents

$\mathbb{Z}$ is incomplete

- Unlike in $\mathbb{R}$, it is possible to have Cauchy sequences in $\mathbb{Z}$ that are not constant.

$\mathbb{Z}$ is incomplete

- Unlike in $\mathbb{R}$, it is possible to have Cauchy sequences in $\mathbb{Z}$ that are not constant.
- The sequence of partial sums

$$(a_n)_{n=0}^{\infty} = \sum_{i=0}^{n-1} p^i = (1+p), (1+p+p^2), (1+p+p^2+p^3)...$$

is Cauchy and does not live inside $\mathbb{Z}$ (when $p \neq 2$). In fact, its sum is $\dfrac{1}{1-p}$.

$\mathbb{Z}$ is incomplete

- Unlike in $\mathbb{R}$, it is possible to have Cauchy sequences in $\mathbb{Z}$ that are not constant.
- The sequence of partial sums

$$(a_n)_{n=0}^{\infty} = \sum_{i=0}^{n-1} p^i = (1+p), (1+p+p^2), (1+p+p^2+p^3)...$$

is Cauchy and does not live inside $\mathbb{Z}$ (when $p \neq 2$). In fact, its sum is $\frac{1}{1-p}$.

- For all nonnegative n, $a_n = \sum_{i=0}^{n-1} p^i$. Of course $1^n - p^n = (1-p)\sum_{i=0}^{n-1} p^i$, so $a_n = \sum_{i=0}^{n-1} p^i = \frac{1-p^n}{1-p}$. Now, because $\lim_{n\to\infty} \frac{1}{1-p} = \frac{1}{1-p}$ and $\lim_{n\to\infty} p^n = 0$,

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} \frac{1}{1-p} - \lim_{n\to\infty} p^n \cdot \lim_{n\to\infty} \frac{1}{1-p} = \frac{1}{1-p} - 0 = \frac{1}{1-p} \square$$

$\mathbb{Q}$ is incomplete too :(

- In 2-adics, let's build a sequence x_n such that $(x_n)^2 + 7 = 0$, which is clearly false for all $\mathbb{Q}$.

$\mathbb{Q}$ is incomplete too :(

- In 2-adics, let's build a sequence x_n such that $(x_n)^2 + 7 = 0$, which is clearly false for all $\mathbb{Q}$. Suppose inductively for some n we have an x_n such that $2^n \mid x_n^2 + 7$. If $2^{n+1} \mid x_n^2 + 7$, let $x_{n+1} := x_n$. Otherwise,

$$x_{n+1} := x_n + 2^{n-1} \implies (x_n + 2^{n-1})^2 + 7 = (x_n^2 + 7) + 2^n x_n + 2^{2n-2}$$

suffices (for $n \geq 3$).

$\mathbb{Q}$ is incomplete too :(

- In 2-adics, let's build a sequence x_n such that $(x_n)^2 + 7 = 0$, which is clearly false for all $\mathbb{Q}$. Suppose inductively for some n we have an x_n such that $2^n \mid x_n^2 + 7$. If $2^{n+1} \mid x_n^2 + 7$, let $x_{n+1} := x_n$. Otherwise,

$$x_{n+1} := x_n + 2^{n-1} \implies (x_n + 2^{n-1})^2 + 7 = (x_n^2 + 7) + 2^n x_n + 2^{2n-2}$$

suffices (for $n \geq 3$). Thus, it is possible to build a sequence whose limit is infinitely divisble by 2.

$\mathbb{Q}$ is incomplete too :(

- In 2-adics, let's build a sequence x_n such that $(x_n)^2 + 7 = 0$, which is clearly false for all $\mathbb{Q}$. Suppose inductively for some n we have an x_n such that $2^n \mid x_n^2 + 7$. If $2^{n+1} \mid x_n^2 + 7$, let $x_{n+1} := x_n$. Otherwise,

$$x_{n+1} := x_n + 2^{n-1} \implies (x_n + 2^{n-1})^2 + 7 = (x_n^2 + 7) + 2^n x_n + 2^{2n-2}$$

  suffices (for $n \geq 3$). Thus, it is possible to build a sequence whose limit is infinitely divisble by 2.
- For $p > 3$, the sequence $x_n = a^{p^n}$, where $1 < a < p - 1$, never converges in p.

Cauchy completion

Just like with $|\cdot|_\infty$ and $\mathbb{R}$, it's impossible to do calculus on $\mathbb{Q}$ until the "holes" have been filled in. We can complete $\mathbb{Q}$ with $|\cdot|_p$ in the same way we complete it with $|\cdot|_\infty$: include all the limits.
Define the *p-adic numbers* $\mathbb{Q}_p$ to be the Cauchy completion of the rationals: the set of all $lim_{n\to\infty} a_n$, where $(a_n)_{n=m}^{\infty}$ is a Cauchy sequence of rationals under the p-adic absolute value.

p-adic expansions

It is possible to rewrite every element of $\mathbb{Q}_p$ like so:

$$s = \sum_{n=k}^{\infty} a_n p^n = a_k p^k + a_{k+1} p^{k+1} + a_{k+2} p^{k+2} + \cdots$$

where k is a potentially negative integer and each a_n is a nonnegative integer less than p.

p-adic expansions

It is possible to rewrite every element of $\mathbb{Q}_p$ like so:

$$s = \sum_{n=k}^{\infty} a_n p^n = a_k p^k + a_{k+1} p^{k+1} + a_{k+2} p^{k+2} + \cdots$$

where k is a potentially negative integer and each a_n is a nonnegative integer less than p. When k is positive, every element of the sequence is an integer and so the resulting limit is in $\mathbb{Z}_p$.

5-adic expansion of 4/3

- Right off the bat, $\frac{4}{3}$ has no 5's (and no fifths). So our expansion starts at 0:

$$\frac{4}{3} = \sum_{n=0}^{\infty} a_n 5^n, \text{ where } 0 \leq a_n \leq 4$$

5-adic expansion of 4/3

- Right off the bat, $\frac{4}{3}$ has no 5's (and no fifths). So our expansion starts at 0:
$$\frac{4}{3} = \sum_{n=0}^{\infty} a_n 5^n, \text{ where } 0 \leq a_n \leq 4$$

- $\frac{4}{3} \equiv a_0 \pmod 5$, so $4 \equiv 3a_0 \pmod 5$,so $8 \equiv 6a_0 \pmod 5$ so $a_0 \equiv 3 \pmod 5$.

5-adic expansion of 4/3

- Right off the bat, $\frac{4}{3}$ has no 5's (and no fifths). So our expansion starts at 0:
$$\frac{4}{3} = \sum_{n=0}^{\infty} a_n 5^n, \text{ where } 0 \leq a_n \leq 4$$
- $\frac{4}{3} \equiv a_0 \pmod 5$, so $4 \equiv 3a_0 \pmod 5$,so $8 \equiv 6a_0 \pmod 5$ so $a_0 \equiv 3 \pmod 5$.
- Now, $\frac{4}{3} \equiv a_0 + 5a_1 \pmod{25}$. So $4 \equiv 3a_0 + 15a_1 \pmod{25} \implies 20 \equiv 15a_1 \pmod{25} \implies a_1 \equiv 3 \pmod 5$.

5-adic expansion of 4/3

- Right off the bat, $\frac{4}{3}$ has no 5's (and no fifths). So our expansion starts at 0:
$$\frac{4}{3} = \sum_{n=0}^{\infty} a_n 5^n, \text{ where } 0 \leq a_n \leq 4$$
- $\frac{4}{3} \equiv a_0 \pmod 5$, so $4 \equiv 3a_0 \pmod 5$,so $8 \equiv 6a_0 \pmod 5$ so $a_0 \equiv 3 \pmod 5$.
- Now, $\frac{4}{3} \equiv a_0 + 5a_1 \pmod{25}$. So $4 \equiv 3a_0 + 15a_1 \pmod{25} \implies 20 \equiv 15a_1 \pmod{25} \implies a_1 \equiv 3 \pmod 5$.
- Now, $\frac{4}{3} \equiv a_0 + 5a_1 + 25a_2 \pmod{125}$. We get $a_2 = 1 \cdots$

5-adic expansion of 4/3

- Right off the bat, $\frac{4}{3}$ has no 5's (and no fifths). So our expansion starts at 0:
$$\frac{4}{3} = \sum_{n=0}^{\infty} a_n 5^n, \text{ where } 0 \leq a_n \leq 4$$
- $\frac{4}{3} \equiv a_0 \pmod 5$, so $4 \equiv 3a_0 \pmod 5$,so $8 \equiv 6a_0 \pmod 5$ so $a_0 \equiv 3 \pmod 5$.
- Now, $\frac{4}{3} \equiv a_0 + 5a_1 \pmod{25}$. So $4 \equiv 3a_0 + 15a_1 \pmod{25} \implies 20 \equiv 15a_1 \pmod{25} \implies a_1 \equiv 3 \pmod 5$.
- Now, $\frac{4}{3} \equiv a_0 + 5a_1 + 25a_2 \pmod{125}$. We get $a_2 = 1 \cdots$
- After this, it alternates. We write the coefficients as if in base p: $\overline{133}_5$
- Let's check it.

Complex p-adics?

Complex p-adics?

It is possible, but messy.

Table of Contents

Solving Polynomials

In fact, finding the expansion of $\frac{4}{3}$ in 5-adics is a specific case of the broader *Hensel's Lemma*. So was building $\sqrt{-7}$ in 2-adics!

Solving Polynomials

In fact, finding the expansion of $\frac{4}{3}$ in 5-adics is a specific case of the broader *Hensel's Lemma*. So was building $\sqrt{-7}$ in 2-adics!
The idea of Hensel's Lemma is that we are able to construct roots to polynomials, that, when plugged in, become infinitely divisible by p and thus approximate 0.
Formally, we say:
Let $f(x) \in \mathbb{Z}[x], p$ a prime, and x_1 such that

$$f(x_1) = 0 \bmod p \quad \text{and} \quad f'(x_1) \neq 0 \bmod p$$

Then the recursion

$$x_{n+1} = x_n - f(x_n) \cdot f'(x_1)^{-1} \bmod p^{n+1}$$

(where $f'(x_1)^{-1}$ is an inverse modulo p) determines a sequence of integers x_n such that

$$f(x_n) = 0 \bmod p^n \text{ and } x_{n+1} = x_n \bmod p^n$$

.

Derivative!! (f)

Taylor series expansion!!

$$f(x+h) = f(x) + f'(x) \cdot h + E \cdot h^2$$

where $E \in \mathbb{Z}[x,h]$. If we have this, let $\delta = -f'(x_n)^{-1} \cdot f(x_n)$ describe the rate of change, as usual, with inverse modulo p^n, and evaluate

$$f(x_{n+1}) = f(x_n + \delta) = f(x_n) + f'(x_n) \cdot \delta + E \cdot \delta^2$$

$$= f(x_n) - f'(x_n) \cdot f'(x_n)^{-1} \cdot f(x_n) + E \cdot \delta^2 = f(x_n) - f(x_n) + E(x_n) \cdot \delta^2$$

$$= E \cdot \delta^2$$

As before, this means $f(x_n) = 0 \bmod p^n$.

Derivative!! (f)

Taylor series expansion!!

$$f(x+h) = f(x) + f'(x) \cdot h + E \cdot h^2$$

where $E \in \mathbb{Z}[x,h]$. If we have this, let $\delta = -f'(x_n)^{-1} \cdot f(x_n)$ describe the rate of change, as usual, with inverse modulo p^n, and evaluate

$$f(x_{n+1}) = f(x_n + \delta) = f(x_n) + f'(x_n) \cdot \delta + E \cdot \delta^2$$

$$= f(x_n) - f'(x_n) \cdot f'(x_n)^{-1} \cdot f(x_n) + E \cdot \delta^2 = f(x_n) - f(x_n) + E(x_n) \cdot \delta^2$$

$$= E \cdot \delta^2$$

As before, this means $f(x_n) = 0 \bmod p^n$. Then certainly $x_{n+1} = x_n \bmod p^n$.

Derivative!! (f)

Taylor series expansion!!

$$f(x+h) = f(x) + f'(x) \cdot h + E \cdot h^2$$

where $E \in \mathbb{Z}[x,h]$. If we have this, let $\delta = -f'(x_n)^{-1} \cdot f(x_n)$ describe the rate of change, as usual, with inverse modulo p^n, and evaluate

$$f(x_{n+1}) = f(x_n + \delta) = f(x_n) + f'(x_n) \cdot \delta + E \cdot \delta^2$$

$$= f(x_n) - f'(x_n) \cdot f'(x_n)^{-1} \cdot f(x_n) + E \cdot \delta^2 = f(x_n) - f(x_n) + E(x_n) \cdot \delta^2$$

$$= E \cdot \delta^2$$

As before, this means $f(x_n) = 0 \bmod p^n$. Then certainly $x_{n+1} = x_n \bmod p^n$. Since $f'(x_n) \neq 0 \bmod p$, so it has an inverse mod p^n, since f and f' have coefficients in $\mathbb{Z}$. And then $\delta = 0 \bmod p^n$, so $\delta^2 = 0 \bmod p^{2n}$.

Derivative!! (f)

Taylor series expansion!!

$$f(x+h) = f(x) + f'(x) \cdot h + E \cdot h^2$$

where $E \in \mathbb{Z}[x,h]$. If we have this, let $\delta = -f'(x_n)^{-1} \cdot f(x_n)$ describe the rate of change, as usual, with inverse modulo p^n, and evaluate

$$f(x_{n+1}) = f(x_n + \delta) = f(x_n) + f'(x_n) \cdot \delta + E \cdot \delta^2$$

$$= f(x_n) - f'(x_n) \cdot f'(x_n)^{-1} \cdot f(x_n) + E \cdot \delta^2 = f(x_n) - f(x_n) + E(x_n) \cdot \delta^2$$

$$= E \cdot \delta^2$$

As before, this means $f(x_n) = 0 \bmod p^n$. Then certainly $x_{n+1} = x_n \bmod p^n$. Since $f'(x_n) \neq 0 \bmod p$, so it has an inverse mod p^n, since f and f' have coefficients in $\mathbb{Z}$. And then $\delta = 0 \bmod p^n$, so $\delta^2 = 0 \bmod p^{2n}$. Since E is a polynomial with coefficients in $\mathbb{Z}$, $E \cdot \delta^2 = 0 \bmod p^{2n}$. That is,

$$f(x_{n+1}) = 0 \bmod p^{2n}$$

which is much better than 0 mod p^{n+1}. Yay!!!

Derivative!! (x)

Back to the expression

$$x_{n+1} = x_n - f(x_n) \cdot f'(x_n)^{-1} \bmod p^{n+1}$$

We have that $f(x_n) = 0 \bmod p^n$, so ETF $f'(x_n)^{-1}$ modulo p in order to know $x_{n+1} \bmod p^{n+1}$. Thus, ETS

$$f'(x_1)^{-1} = f'(x_n)^{-1} \bmod p$$

Now since by construction $x_{n+1} = x_n \bmod p^n$, for all n we have $x_n = x_1 \bmod p$. Since f' has coefficients in $\mathbb{Z}$, we have $f'(x_n) = f'(x_1)$ for all n. Since $f'(x_1) \neq 0 \bmod p$, the inverses mod p are all the same. We can't divide by p, the factorials occurring in the usual form of the Taylor expansion would become problematic. But, in fact, any polynomial $P(x) = \sum_i b_i x^i$ with coefficients in $\mathbb{Z}$ can be expanded p-adically:

$$P(x+h) = c_0 + c_1 \cdot h + c_2 \cdot h^2 + \ldots \qquad \text{(a finite expansion)}$$

with c_i polynomials in x by substituting $x + h$ in P and expanding in powers of h.

cont.

Thus, the issue is to see that, in this expansion

$$c_1(x) = f'(x)$$

Since the requisite expansion is linear in the polynomial P, it suffices to consider $P(x) = x^n$. Then by the Binomial Theorem

$$(x+h)^n = x^n + nx^{n-1} \cdot h + E \cdot h^2$$

where, indeed, E is a polynomial in x and h, with coefficients in $\mathbb{Z}$. Since nx^{n-1} is the derivative of x^n, we have the desired sort of Taylor expansion, and Hensel's procedure will succeed.

Thank you!!

Further reading:

- A. Baker: An Introduction to p-adic Numbers and p-adic Analysis
- M. Hamburg: Construction of $\mathbb{C}_p$ and Extension of p-adic Valuations to $\mathbb{C}$
- N. Koblitz: p-adic Numbers, p-adic Analysis, and Zeta Functions
- F. Bruhat: Lectures on Some Aspects of p-adic Analysis

Ostrowski's Theorem (proof)

Either there are integers n such that $|n| > 1$ or there are not.
If there are, then there is a smallest one n_0. For any n with $|n| > 1$.
Expand any arbitrary positive integer n in base n_0 as

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \ldots + a_r n_0^r$$

with $0 \leq a_i < n_0$. After a string of inequalities, conclude that

$$\|n\| \leq C n^{\alpha} \quad \text{for all } n$$

Now put n^N in place of n in the above inequality; then take Nth roots.
You get

$$\|n\| \leq \sqrt[N]{C}\, n^{\alpha}$$

Now let N go to infinity. $\|n\| = n^{\alpha}$, which is equivalent to $\|n\| = n$ topologically.

Ostrowski's Theorem (cont.)

If all integers have an absolute value ≤ 1, pick the smallest integer p whose absolute value is < 1 (exists by non triviality). Then p is prime by minimality. It is then possible to show by contradiction there are no other primes q such that $||q|| < 1$. Now, since any integer can be factored into powers of p and powers of other primes q, and since $||q|| = 1$, it is clear the powers of p are the only ones that "matter."