Introduction to p-adic Analysis

Travor Liu, May Jiang, Qing Su, Hantang Guo

Department of Mathematics
University College London

28 February 2024

Table of Contents

Table of Contents

Solve the equation

Solve $f(x) \equiv 0 \pmod{m}, m \in \mathbb{Z}$

Things to do:

1. Factorise $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$
2. Solve $f(x) \equiv 0 \pmod{{p_i}^{k_i}} \quad (i = 1, 2, \ldots, r)$
    1. $f(x) \equiv 0 \pmod{p}$
    2. $f(x) \equiv 0 \pmod{p^k}, \quad k \in \mathbb{Z}_{\geq 1}$
3. Use Chinese Remainder Theorem

Solve the equation

Theorem (Chinese Remainder Theorem)

Set $m_1, m_2, \ldots, m_s$ to be coprime $\mathbb{Z}_{\geq 1}$ Then for any integer $b_1, b_2, \ldots, b_s$, the linear congruence system

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_s \pmod{m_s} \end{cases}$$

has a unique solution in $\mathbb{Z}/m\mathbb{Z}$, where $m = m_1 m_2 \cdots m_s$.

Hensel's lemma

Since $f(x) \equiv 0 \pmod{p^j} \Rightarrow f(x) \equiv 0 \pmod{p^{j-1}}$, so given $f(a) \equiv 0 \pmod{p^j}$, $f(x) \equiv 0 \pmod{p^{j+1}}$ can be solved via $x = a + tp^j$.

$$\begin{aligned} f(a+tp^j) &= f(a) + tp^j f'(a) + \frac{t^2 p^{2j} f''(a)}{2!} + \cdots + \frac{t^n p^{nj} f^{(n)}(a)}{n!} \\ &= f(a) + tp^j f'(a) \pmod{p^{j+1}} \\ \Rightarrow tf'(a) &\equiv -f(a)p^{-j} \pmod{p} \end{aligned}$$

1. if $f'(a) \equiv 0 \pmod{p}$, $f(a+tp^j) \equiv f(a) \pmod{p^{j+1}}$ for all t.
   1. if $f(a) \equiv 0 \pmod{p^{j+1}}$, then $t \in \{0, 1, 2, \ldots, p-1\}$.
   2. if $f(a) \not\equiv 0 \pmod{p^{j+1}}$, then no solution.
2. if $f'(a) \not\equiv 0 \pmod{p}$, there will be an unique solution

Hensel's lemma

Theorem (Hensel's lemma)

Suppose that $f(x)$ is a polynomial with integer coefficients.

- *If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there exists a unique t s.t. $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$*
- *If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \equiv 0 \pmod{p}$, then there exists p ways to lift the solution.*

Hence, $a_{n+1} = a_n + t_n p^n$, and we can write the solution in forms of power series of p.
This expansion is invalid analytically, but makes a lot of sense number-theoretically.

Hensel example

Consider the polynomial $f(x) = x + 1 \equiv 0 \mod p^k$

- $x_1 = p - 1$
- $x_{k+1} = x_k + (p-1)p^k$

Since $f(-1) = 0$, we should have

$$-1 = (p-1)p^0 + (p-1)p^1 + (p-1)p^2 \cdots$$

Right?

Table of Contents

Completeness of real numbers

Real numbers = Rational numbers + Completeness

1. Least upper bound principle (requires $<$)
2. Every Cauchy sequence converges (requires $|\cdot|$)

Definition (Cauchy sequence)

$\{x_n\}$ is Cauchy iff

$$\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall m, n \in \mathbb{N} \quad (m, n > N \Rightarrow |x_m - x_n| < \varepsilon)$$

If we define an absolute value differently, then we should obtain different completions of $\mathbb{Q}$ using Cauchy sequences.

Absolute values

Definition (Absolute values)

$f : \mathbb{Q} \to \mathbb{R}$ is an absolute value iff

1. $f(x) \geq 0$ and $f(x) = 0$ iff $x = 0$
2. $f(xy) = f(x)f(y)$
3. $f(x + y) \leq f(x) + f(y)$

We consider absolute values producing the same completion of $\mathbb{Q}$ equivalent:

Definition (Equivalent absolute values)

Absolute values f, g are equivalent iff for all sequence $\{x_n\}$ and number L in $\mathbb{Q}$,

$$\lim_{n \to +\infty} f(x_n - L) = 0 \iff \lim_{n \to +\infty} g(x_n - L) = 0.$$

e.g. $f(x) = |x|$ and $g(x) = |x|^{1/2}$ are equivalent.

Classification of absolute values

Theorem (Ostrowski)

Every absolute value on $\mathbb{Q}$ is equivalent to exactly one of the following type:

1. *Trivial absolute value ($\mathbb{Q}$):* $f(x) = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$,
2. *Archimedean absolute value ($\mathbb{R}$):* $|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$,
3. *p-adic absolute value ($\mathbb{Q}_p$):* $|x|_p = p^{-\nu_p(x)}$ *for* $x \neq 0$.

p-adic absolute values

Definition (p-adic valuation)

For prime p and all nonzero rational x, $\nu_p(x)$ is the unique integer m satisfying

$$x = p^m \frac{h}{k} \quad (p \nmid hk).$$

Definition (p-adic absolute value)

For prime p, we have

$$|x|_p = \begin{cases} 0 & x = 0 \\ p^{-\nu_p(x)} & x \neq 0 \end{cases}$$

- $\nu_2(12) = 2, |12|_2 = 1/4; \nu_3(22/7) = 0, |22/7|_3 = 1$
- $\nu_p(xy) = \nu_p(x) + \nu_p(y); |x|_p \leq 1$ for all $x \in \mathbb{Z}$

Ultra-triangle inequality for $|x|_p$

For $x = p^a h_1/k_1$ and $y = p^b h_2/k_2$ such that $p \nmid h_1 h_2 k_1 k_2$ and $a \leq b$, there is

$$x + y = \frac{p^a h_1 k_2 + p^b h_2 k_1}{k_1 k_2} = p^a \frac{h_1 k_2 + p^{b-a} h_2 k_1}{k_1 k_2}.$$

Because $p^a h_1 k_2 + p^b h_2 k_1 \in \mathbb{Z}$, we have

$$\begin{aligned} |x + y|_p &= p^{-a} \frac{|h_1 k_2 + p^{b-a} h_2 k_1|_p}{|k_1 k_2|_p} = p^{-a} |h_1 k_2 + p^{b-a} h_2 k_1|_p \\ &\leq p^{-a} = |x|_p. \end{aligned}$$

$$\Rightarrow |x + y|_p \leq \max(|x|_p, |y|_p) \quad \text{(Non-Archimedean absolute value)}$$

Table of Contents

Convergence

Definition (p-adic convergence)

$\{x_n\} \in \mathbb{Q}_p$ converges to $L \in \mathbb{Q}_p$ iff $\lim_{n\to+\infty} |x_n - L|_p = 0$.

When $m > n$, there is

$$\begin{aligned} |x_m - x_n|_p &\le \max(|x_m - x_{m-1}|_p, |x_{m-1} - x_n|_p) \\ &\le \max(|x_m - x_{m-1}|_p, |x_{m-1} - x_{m-2}|_p, |x_{m-2} - x_n|_p) \\ &\le \cdots \le \max_{n<k\le m} |x_k - x_{k-1}|_p. \end{aligned}$$

Theorem (p-adic Cauchy's criterion)

$\{x_n\} \in \mathbb{Q}_p$ *converges in* $\mathbb{Q}_p$ *iff* $\lim_{n\to+\infty} |x_n - x_{n-1}|_p = 0$. *In other words, a series* $\sum_n a_n$ *converges in* $\mathbb{Q}_p$ *iff* $\lim_{n\to+\infty} |a_n|_p = 0$.

p-adic expansions

Theorem

Every element $x \in \mathbb{Q}_p$ is uniquely expressed as

$$x = a_{-k}p^{-k} + a_{-k+1}p^{1-k} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \ldots,$$

where $0 \leq a_n < p$ for all n and $a_{-k} \neq 0$, so $|x|_p = p^k$.

Sanity check: Let

$$x_n = a_{-k}p^{-k} + a_{-k+1}p^{1-k} + \cdots + a_{n-1}p^{n-1} + a_n p^n.$$

Then $|x_n - x_{n-1}|_p = |a_n p^n|_p \leq |p^n|_p = p^{-n} \to 0$.

Definition (p-adic integers)

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

Continuity and differentiability

Definition (p-adic continuity)

$f : \Omega \to \mathbb{Q}_p$ is continuous at $x \in \Omega$ iff $\lim_{y \to x} |f(y) - f(x)|_p = 0$.

Definition (p-adic derivative)

Let $f : \Omega \to \mathbb{Q}_p$, its derivative is defined as the p-adic limit

$$f'(x) = \lim_{y \to x} \frac{f(y) - f(x)}{y - x}.$$

Examples

- $f(x) = c$, $f'(x) = 0$;
- $f(x) = x^n$, $f'(x) = nx^{n-1}$.

Do we have a mean value theorem for $\mathbb{Q}_p$?

Failure of mean value theorem

Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be defined such that when

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \ldots,$$

there is

$$f(x) = a_0 + a_1 p^2 + a_2 p^4 + a_3 p^6 + \ldots$$

Theorem (Properties of f)

f is a nonconstant function on $\mathbb{Z}_p$ satisfying

- $f(x+y) = f(x) + f(y)$,
- $|f(x)|_p = |x|_p^2$,
- $f'(x) \equiv 0$.

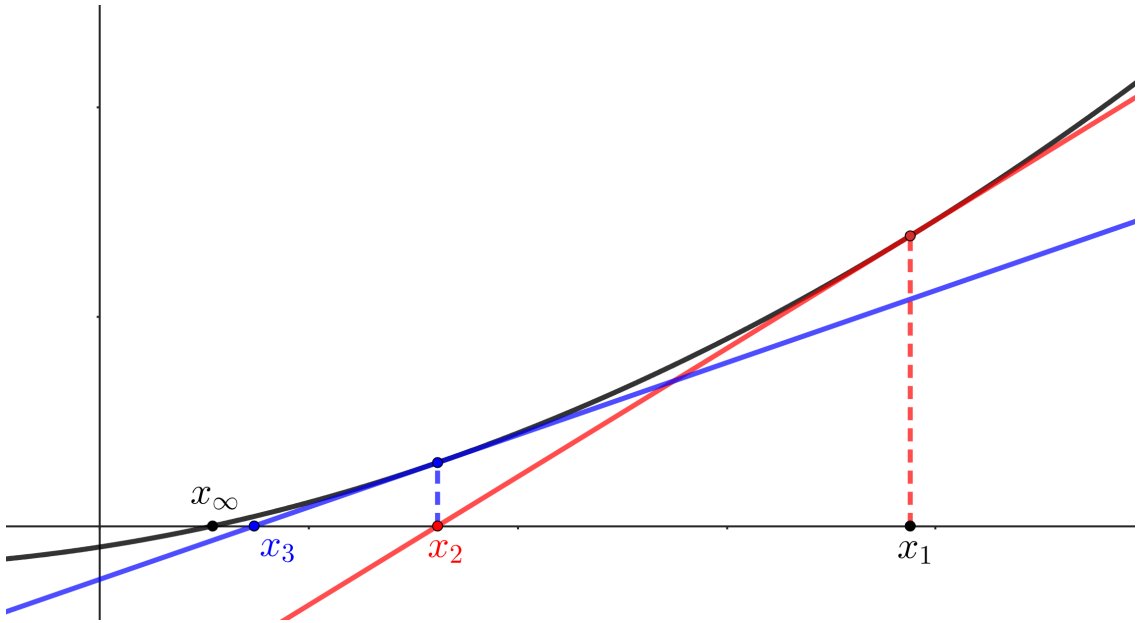
Due to the lack of MVT in $\mathbb{Q}_p$, we cannot study p-adic differentiable functions as in $\mathbb{R}$, so we focus on polynomials and power series.

Equation solving in $\mathbb{R}$

Theorem (Newton's method)

Let $f : \Omega \to \mathbb{R}$ be differentiable. $f(x) = 0$ can be solved iteratively using

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \quad x_1 \in \Omega, \quad f'(x_1) \neq 0.$$



Equation solving in $\mathbb{Q}_p$

Theorem (Hensel's lemma)

Let $f \in \mathbb{Z}_p[x]$. Suppose $\exists \alpha_1 \in \mathbb{Z}_p$ s.t. $|f(\alpha_1)| < 1$ and $|f'(\alpha_1)| = 1$.

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}, \quad n \geq 1$$

defines a convergent sequence whose limit $\alpha \in \mathbb{Z}_p$ is the unique p-adic integer such that $|\alpha - \alpha_1| < 1$ and $f(\alpha) = 0$.

Speeding up calculation

Theorem (Hensel's Lemma)

Let $f \in \mathbb{Z}_p[x]$ and $x_0 \in \mathbb{Z}_p$ s.t. $\nu_p(f'(x_0)) = c$ and $f(x_0) \equiv 0 \pmod{p^{2c+1}}$. Then, when

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

we have $\nu_p(f'(x_n)) = c$, $f(x_n) \equiv 0 \pmod{p^{2c+2^n}}$, and $x_{n+1} \equiv x_n \pmod{p^{c+2^n}}$ for all $n \in \mathbb{N}$.

Power series in $\mathbb{Q}_p$

Let $\langle a_n \rangle \in \mathbb{Q}_p$ be defined on $\mathbb{Z}_{\geq 0}$. Then

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$$

is a **power series** on $\mathbb{Q}_p$.

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} x^n}{n} = x - \frac{x^2}{2} + \frac{x^3}{3} + \dots$$

$$\sqrt{1+x} = \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} x^n = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \dots$$

Radius of convergence

Theorem (Radius of convergence)

For $f(x) = \sum_{n=0}^{\infty} a_n x^n$, *if* $0 \leq \rho \leq \infty$ *satisfies*

$$\frac{1}{\rho} = \limsup_{n \to +\infty} \sqrt[n]{|a_n|_p},$$

then $f(x)$ *converges for all* $|x|_p < \rho$ *and diverges for all* $|x|_p > \rho$.

Examples

- $f(x) = \exp(x)$, $\rho = p^{-1/(p-1)}$, but $\neg \exists x \in \mathbb{Q}_p \ |x|_p = p^{-1/(p-1)}$;
- $f(x) = \log(1+x)$, $\rho = 1$, diverges when $|x|_p = 1$;
- $f(x) = \sqrt{1+x}$, $\rho = 1$, diverges when $|x|_p = 1$.

Convergence of $\exp(x)$

Theorem (Legendre)

Let $n \in \mathbb{Z}_{\geq 1}$ be expanded as follows:

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_m p^m, \quad 0 \leq a_k < p, \quad a_m \neq 0$$

and let $s_n = a_0 + a_1 + \cdots + a_m$. Then $\nu_p(n!) = (n - s_n)/(p-1)$.

$$0 \leq s_n < p(m+1) \leq p(\log_p n + 1) \Rightarrow \frac{1 - \frac{p}{n}(\log_p n + 1)}{p-1} < \frac{\nu_p(n!)}{n} \leq \frac{1}{p-1}$$

$$\Rightarrow \lim_{n\to\infty} \frac{\nu_p(n!)}{n} = \frac{1}{p-1}$$

$$\rho^{-1} = \limsup_{n\to\infty} |1/n!|_p^{\frac{1}{n}} = \lim_{n\to\infty} p^{\frac{-\nu_p(\frac{1}{n!})}{n}} = \lim_{n\to\infty} p^{\frac{\nu_p(n!)}{n}} = p^{\frac{1}{p-1}} \Rightarrow \rho = p^{-\frac{1}{p-1}}.$$

Convergence of $\log(1+x)$

$$0 \leq \nu_p(n) \leq \log_p n \Rightarrow \lim_{n\to+\infty} \frac{\nu_p(n)}{n} = 0.$$

$$\rho^{-1} = \limsup_{n\to\infty} \left|\frac{(-1)^{n-1}}{n}\right|_p^{\frac{1}{n}} = \lim_{n\to\infty} p^{\frac{\nu_p(n)}{n}} = 1 \Rightarrow \rho = 1.$$

Theorem (p-adic Cauchy's criterion)

$\sum_n b_n$ converges in $\mathbb{Q}_p$ iff $\lim_{n\to+\infty} |b_n|_p = 0$.

When $b_n = \frac{(-1)^{n-1}x^n}{n}$ and $|x|_p = 1$, we have $|b_n|_p = |\frac{1}{n}|_p$.

$|b_n|_p = p^{\nu_p(n)} \geq 1 \not\to 0 \Rightarrow \log(1+x)$ diverges when $|x|_p = 1$.

Table of Contents

Sections of coding

Definition (Multiplicative inverse mod m)

Given some integer a, we wish to solve the equation

$$ab \equiv 1 \pmod{m} \tag{1}$$

Observe that (1) has a solution if and only if there exists integers b, k satisfying $ab + km = 1$, so we can be solve by Euclidean algorithm.

Definition (Fast powering algorithm)

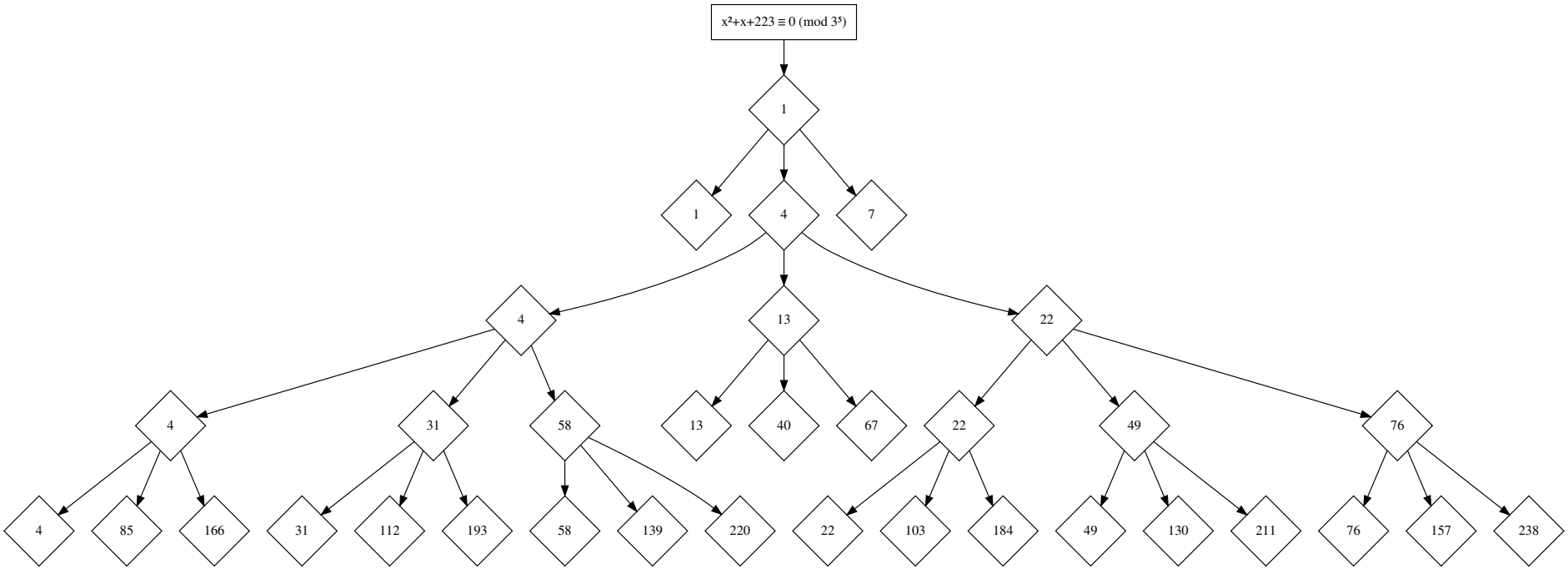
When we only want to find the value $x^n \mod m$, it is a waste to compute x^n and then take $\mod m$. In order to be efficient, we hope to reduce the number of multiplications and increase the number of $\mod m$'s so that we will only multiply small numbers.

Fast powering algorithm

```
def fast_power_modm(x,n,m):
    ret=1
    while n>0:
        if n%2!=0:
            ret=(ret*x) % m
        x=(x*x) % m
        n=n//2
    return ret % m
```

Solutions of $f(x) = x^2 + x + 223 \equiv 0 \pmod{3^5}$

The k'th layer solves $f(x) \equiv 0 \pmod{p^k}$.



Bibliography


Fernando Q. Gouvêa (2020).
p-adic Numbers: An Introduction (3rd ed.)


Keith Conrad.
Hensel's lemma
https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf


Keith Conrad.
Infinite series in p-adic fields
https://kconrad.math.uconn.edu/blurbs/gradnumthy/infseriespadic.pdf


Travor Liu.
Absolute values and Ostrowski's theorem
https://travorlzh.github.io/2023/05/11/absolute-values-and-ostrowskys-theorem.html