A Formal Note on p-adic Cryptography

Vasilisa Baginskaya

Abstract

We give a concise mathematical account of p-adic structures relevant to cryptography. The main point is double-edged: finite p-adic precision gives efficient arithmetic over $\mathbb{Z}/p^N\mathbb{Z}$, but the same structure gives lifting and local inversion attacks. All stated results are proved.

1 The p-adic ground field

Fix a prime p.

Definition 1.1. For $x \in \mathbb{Q}^\times$, write

$$x = p^k \frac{a}{b}, \qquad a, b \in \mathbb{Z}, \qquad p \nmid a, \quad p \nmid b.$$

Set $v_p(x) = k$, $v_p(0) = +\infty$, and

$$|x|_p = p^{-v_p(x)}, \qquad |0|_p = 0.$$

Lemma 1.2. *For all $x, y \in \mathbb{Q}$,*

$$v_p(xy) = v_p(x) + v_p(y).$$

If $x + y \neq 0$, then

$$v_p(x + y) \geq \min\{v_p(x), v_p(y)\}.$$

Proof. The multiplicative statement follows by adding the exponents of p in the reduced decompositions of x and y. For the additive statement, assume $x, y \neq 0$. Let $a = v_p(x)$, $b = v_p(y)$, and suppose $a \leq b$. Write

$$x = p^a u, \qquad y = p^b v,$$

where $u, v \in \mathbb{Q}$ have p-adic valuation 0. Then

$$x + y = p^a(u + p^{b-a}v).$$

Since $u + p^{b-a}v \in \mathbb{Q}$, its valuation is at least 0 when $b > a$, and at least 0 when $b = a$ unless cancellation increases the valuation. Hence $v_p(x + y) \geq a = \min\{a, b\}$. The cases with $x = 0$ or $y = 0$ are immediate. □

Theorem 1.3 (Strong triangle inequality)**.** *For all $x, y \in \mathbb{Q}$,*

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

Proof. If $x + y = 0$, the claim is clear. Otherwise,

$$v_p(x + y) \geq \min\{v_p(x), v_p(y)\}.$$

Multiplying by -1 in the exponent gives

$$p^{-v_p(x+y)} \leq p^{-\min\{v_p(x),v_p(y)\}} = \max\{p^{-v_p(x)}, p^{-v_p(y)}\}.$$

Thus $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. □

Definition 1.4. The field $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. Its valuation ring is

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

Theorem 1.5. *There is a canonical topological ring isomorphism*

$$\mathbb{Z}_p \cong \varprojlim_N \mathbb{Z}/p^N\mathbb{Z}.$$

Proof. For $x \in \mathbb{Z}$, let $\rho_N(x)$ be its residue class modulo p^N. The maps ρ_N are compatible with the transition maps

$$\mathbb{Z}/p^{N+1}\mathbb{Z} \to \mathbb{Z}/p^N\mathbb{Z}.$$

Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and ρ_N is continuous for the p-adic topology, ρ_N extends uniquely to a continuous ring map

$$\rho_N : \mathbb{Z}_p \to \mathbb{Z}/p^N\mathbb{Z}.$$

Thus we obtain a continuous ring homomorphism

$$\rho : \mathbb{Z}_p \to \varprojlim_N \mathbb{Z}/p^N\mathbb{Z}.$$

If $\rho(x) = 0$, then $x \in p^N\mathbb{Z}_p$ for every N. Hence $|x|_p \leq p^{-N}$ for every N, so $x = 0$. Thus ρ is injective.

For surjectivity, let $(a_N)_N$ be a compatible system with $a_N \in \mathbb{Z}/p^N\mathbb{Z}$. Choose integer representatives b_N of a_N. Compatibility implies

$$b_{N+1} \equiv b_N \pmod{p^N},$$

so

$$|b_{N+1} - b_N|_p \leq p^{-N}.$$

Thus (b_N) is Cauchy in $\mathbb{Z}_p$, hence converges to some $b \in \mathbb{Z}_p$. By continuity, $\rho_N(b) = a_N$ for each N. Thus ρ is surjective. The inverse-limit topology is exactly the topology defined by the ideals $p^N\mathbb{Z}_p$, so the isomorphism is topological. □

Theorem 1.6 (p-adic expansion)**.** *Every nonzero $x \in \mathbb{Q}_p$ has a unique expansion*

$$x = \sum_{n=M}^{\infty} a_n p^n, \qquad M \in \mathbb{Z}, \qquad a_n \in \{0, 1, \ldots, p-1\}, \qquad a_M \neq 0.$$

Proof. First suppose $x \in \mathbb{Z}_p$. Under the isomorphism

$$\mathbb{Z}_p \cong \varprojlim_N \mathbb{Z}/p^N\mathbb{Z},$$

the class of x modulo p^N has a unique representative

$$s_N = a_0 + a_1 p + \cdots + a_{N-1}p^{N-1}, \qquad a_i \in \{0, \ldots, p-1\}.$$

Compatibility of residues shows that the digit a_i is independent of all $N > i$. The partial sums s_N satisfy

$$x - s_N \in p^N \mathbb{Z}_p,$$

hence $s_N \to x$. Therefore

$$x = \sum_{n=0}^{\infty} a_n p^n.$$

If $x \in \mathbb{Q}_p^\times$, let $M = v_p(x)$. Then $p^{-M}x \in \mathbb{Z}_p^\times$, so

$$p^{-M}x = \sum_{n=0}^{\infty} b_n p^n$$

with $b_0 \neq 0$. Multiplying by p^M gives the desired expansion.

For uniqueness, suppose two expansions differ. Subtract them and let r be the first index at which their digits differ. The difference equals

$$p^r u,$$

where $u \in \mathbb{Z}_p^\times$, hence it is nonzero. Therefore the expansions are unique. □

2 Finite precision

Definition 2.1. A finite p-adic computation at precision N is a computation in

$$R_N = \mathbb{Z}_p/p^N\mathbb{Z}_p \cong \mathbb{Z}/p^N\mathbb{Z}.$$

Proposition 2.2. *The quotient map*

$$\pi_N : \mathbb{Z}_p \to R_N$$

keeps exactly the first N p-adic digits of an element of $\mathbb{Z}_p$.

Proof. If

$$x = \sum_{n=0}^{\infty} a_n p^n,$$

then

$$x - \sum_{n=0}^{N-1} a_n p^n = \sum_{n=N}^{\infty} a_n p^n \in p^N \mathbb{Z}_p.$$

Thus $\pi_N(x)$ is represented by

$$a_0 + a_1 p + \cdots + a_{N-1}p^{N-1}.$$

Conversely, these N digits determine the residue modulo p^N. Hence π_N keeps exactly those digits. □

3 Hensel lifting

Theorem 3.1 (Hensel's lemma)**.** *Let $f \in \mathbb{Z}_p[X]$. Suppose $a_1 \in \mathbb{Z}_p$ satisfies*

$$f(a_1) \equiv 0 \pmod{p}, \qquad f'(a_1) \not\equiv 0 \pmod{p}.$$

Then there exists a unique $a \in \mathbb{Z}_p$ such that

$$f(a) = 0, \qquad a \equiv a_1 \pmod{p}.$$

Proof. We construct $a_n \in \mathbb{Z}_p$ such that

$$f(a_n) \equiv 0 \pmod{p^n}, \qquad a_{n+1} \equiv a_n \pmod{p^n}.$$

Assume a_n has been constructed. Put

$$a_{n+1} = a_n + tp^n, \qquad t \in \{0, \dots, p-1\}.$$

Taylor expansion gives

$$f(a_n + tp^n) \equiv f(a_n) + tp^n f'(a_n) \pmod{p^{n+1}}.$$

Since $f(a_n) \equiv 0 \pmod{p^n}$, write $f(a_n) = p^n c$. We need

$$c + tf'(a_n) \equiv 0 \pmod{p}.$$

Because $f'(a_n) \equiv f'(a_1) \not\equiv 0 \pmod{p}$, this congruence has a unique solution $t \pmod{p}$. Thus a_{n+1} exists and is unique modulo p^{n+1}.

The sequence (a_n) is Cauchy because $a_{n+1} \equiv a_n \pmod{p^n}$. Let $a = \lim a_n \in \mathbb{Z}_p$. Since f is continuous, $f(a) = 0$. Also $a \equiv a_1 \pmod{p}$.

For uniqueness, suppose $b \equiv a_1 \pmod{p}$ and $f(b) = 0$. If $a \equiv b \pmod{p^n}$, write

$$b = a + up^n.$$

Taylor expansion modulo p^{n+1} gives

$$0 = f(b) \equiv f(a) + up^n f'(a) \equiv up^n f'(a) \pmod{p^{n+1}}.$$

Since $f'(a) \not\equiv 0 \pmod{p}$, we get $u \equiv 0 \pmod{p}$, hence $a \equiv b \pmod{p^{n+1}}$. Induction gives $a = b$. □

Corollary 3.2 (Lifting attack criterion)**.** *Let $f \in \mathbb{Z}_p[X]$, and suppose an attacker can find every simple root of f modulo p. Then every root $a \in \mathbb{Z}_p$ of f whose reduction modulo p is simple is computable to precision p^N in $O(N)$ lifting steps.*

Proof. A root a with simple reduction satisfies

$$f(\bar{a}) \equiv 0 \pmod{p}, \qquad f'(\bar{a}) \not\equiv 0 \pmod{p}.$$

Hensel's lemma gives a unique lift modulo p^N. The proof of Hensel's lemma explicitly computes one new p-adic digit at each step, so precision N requires $O(N)$ steps. □

4 Local inversion

Theorem 4.1 (p-adic inverse function theorem, one variable)**.** *Let $f \in \mathbb{Z}_p[[X]]$ converge on $\mathbb{Z}_p$. Suppose $x_0 \in \mathbb{Z}_p$ and*

$$f'(x_0) \in \mathbb{Z}_p^\times.$$

Then for every $y \in \mathbb{Z}_p$ sufficiently close to $f(x_0)$, there is a unique $x \in \mathbb{Z}_p$, sufficiently close to x_0, such that

$$f(x) = y.$$

Moreover, x can be recovered by Newton iteration.

Proof. Put $g(X) = f(X) - y$. For y sufficiently close to $f(x_0)$, we have

$$g(x_0) = f(x_0) - y \equiv 0 \pmod{p}.$$

Also

$$g'(x_0) = f'(x_0) \in \mathbb{Z}_p^\times.$$

Hensel's lemma applied to g gives a unique $x \equiv x_0 \pmod{p}$ satisfying $g(x) = 0$, hence $f(x) = y$. The lifting construction in Hensel's lemma is exactly Newton iteration modulo increasing powers of p. Therefore the inverse is locally unique and computable. □

Corollary 4.2. *A cryptographic map $f : \mathbb{Z}_p \to \mathbb{Z}_p$ whose derivative is a unit on a large known region is locally invertible on that region and is therefore not one-way there.*

Proof. If $f'(x) \in \mathbb{Z}_p^\times$, the preceding theorem gives a local inverse computable by Newton iteration. A one-way function must be hard to invert on typical inputs. Hence f cannot be one-way on any efficiently recognizable region where the theorem applies. □

5 Polynomial maps modulo p^N

Definition 5.1. A map

$$F_N : R_N \to R_N$$

is polynomial if there exists $f \in \mathbb{Z}[X]$ such that

$$F_N(x) = f(x) \bmod p^N.$$

Theorem 5.2. *Let $f \in \mathbb{Z}_p[X]$. If $f'(x) \in \mathbb{Z}_p^\times$ for every $x \in \mathbb{Z}_p$, then the induced map*

$$f_N : \mathbb{Z}/p^N\mathbb{Z} \to \mathbb{Z}/p^N\mathbb{Z}$$

is locally bijective at every residue class for every $N \geq 1$.

Proof. Fix $a \in \mathbb{Z}_p$ and $N \geq 1$. Let $y \equiv f(a) \pmod{p^N}$. To solve

$$f(x) \equiv y \pmod{p^N}$$

with $x \equiv a \pmod{p}$, apply Hensel's lemma to

$$g(X) = f(X) - y.$$

Modulo p, $g(a) \equiv 0$, and

$$g'(a) = f'(a) \in \mathbb{Z}_p^\times.$$

Thus there is a unique solution $x \in \mathbb{Z}_p$ with $x \equiv a \pmod{p}$. Reducing modulo p^N gives a unique solution in the residue ball $a + p\mathbb{Z}_p$. Hence f_N is bijective on each such lifted residue ball. □

Proposition 5.3 (Reduction attack)**.** *Let $f \in \mathbb{Z}_p[X]$. Suppose $y \in \mathbb{Z}_p$, and suppose every solution of*

$$f(x) \equiv y \pmod{p}$$

is simple. Then all solutions of

$$f(x) \equiv y \pmod{p^N}$$

can be found by solving the equation modulo p and Hensel-lifting each solution.

Proof. Let $\bar{x} \in \mathbb{F}_p$ be a solution modulo p. By assumption,

$$f'(\bar{x}) \not\equiv 0 \pmod{p}.$$

Hensel's lemma gives a unique lift modulo p^N. Conversely, any solution modulo p^N reduces to a solution modulo p. Therefore the set of solutions modulo p^N is exactly the set of Hensel lifts of the simple solutions modulo p. □

6 A finite p-adic cryptographic model

Definition 6.1. A finite p-adic public map at precision N is a function

$$F_N : (\mathbb{Z}/p^N\mathbb{Z})^m \to (\mathbb{Z}/p^N\mathbb{Z})^n$$

computed by polynomials with coefficients in $\mathbb{Z}/p^N\mathbb{Z}$.

Definition 6.2. The inversion problem for F_N is: given $y \in \mathrm{im}(F_N)$, find x such that

$$F_N(x) = y.$$

Proposition 6.3. *If $m = n = 1$, F_N is induced by $f \in \mathbb{Z}_p[X]$, and every relevant root of*

$$f(X) - y \equiv 0 \pmod{p}$$

is simple, then the inversion problem for F_N reduces to inversion over $\mathbb{F}_p$.

Proof. By the reduction attack proposition, every solution modulo p^N is the unique Hensel lift of a simple solution modulo p. Hence finding preimages modulo p^N requires only finding preimages modulo p, followed by deterministic lifting. □

Remark 6.4. Thus large N alone does not create security. A proposed p-adic cryptosystem must avoid easy reduction to $\mathbb{F}_p$, or must base security on a problem whose reduction remains hard.

7 Noisy linear equations

Definition 7.1. A p-adic noisy linear instance over R_N is

$$Ax = b + e \pmod{p^N},$$

where

$$A \in R_N^{r \times m}, \qquad x \in R_N^m, \qquad b, e \in R_N^r.$$

The error is p^t-small if

$$e \in p^t R_N^r.$$

Proposition 7.2. *If $e \in p^t R_N^r$, then*

$$Ax \equiv b \pmod{p^t}.$$

Proof. Since $e \in p^t R_N^r$, each coordinate of e is divisible by p^t. From

$$Ax = b + e \pmod{p^N},$$

reducing modulo p^t gives

$$Ax \equiv b \pmod{p^t}.$$

□

Corollary 7.3. *A p-adically small error leaks the exact linear relation modulo a lower power of p.*

Proof. This is precisely the congruence

$$Ax \equiv b \pmod{p^t}$$

proved above. □

Remark 7.4. This differs from ordinary LWE. In the Archimedean setting, small error does not usually vanish under reduction. In the p-adic setting, high divisibility means the error disappears modulo p^t. This leakage must be included in any security analysis.

8 Pseudorandom recurrences

Definition 8.1. Let $f : R_N \to R_N$. A p-adic recurrence is a sequence

$$x_{n+1} = f(x_n).$$

Theorem 8.2. *Every recurrence on R_N is eventually periodic.*

Proof. The set R_N has p^N elements. Therefore the sequence

$$x_0, x_1, x_2, \ldots$$

contains two equal terms among the first $p^N + 1$ terms. Suppose $x_i = x_j$ with $i < j$. Since the recurrence is deterministic,

$$x_{i+k} = x_{j+k}$$

for all $k \geq 0$. Hence the sequence is periodic after time i. □

Proposition 8.3. *If the reduction of a recurrence modulo p has period T, then the reduction modulo p of the sequence modulo p^N has period dividing T.*

Proof. Let $\bar{f} : \mathbb{F}_p \to \mathbb{F}_p$ be the reduction of f, and let $\bar{x}_n$ be the reduction of x_n. Then

$$\bar{x}_{n+1} = \bar{f}(\bar{x}_n).$$

If the orbit of $\bar{x}_0$ has period T, then

$$\bar{x}_{n+T} = \bar{x}_n$$

for all sufficiently large n. Therefore the visible sequence modulo p has period dividing T. □

Remark 8.4. A recurrence cannot be cryptographically pseudorandom if its low p-adic digit has a short detectable period.

9 Conclusion

The p-adic setting supplies efficient finite rings

$$\mathbb{Z}/p^N\mathbb{Z}$$

and a rich analytic theory. The same theory creates attacks: reduction modulo p, Hensel lifting, local inversion, and disappearance of p-adically small errors. Therefore p-adic arithmetic is not itself a security assumption. A secure p-adic cryptosystem must rest on a precise finite computational problem that remains hard after all natural p-adic reductions and liftings.