# An introduction to the algorithmic of $p$-adic numbers

David Lubicz[1]

[1] Universté de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

## Outline

1. Introduction
2. Basic definitions
3. First properties
4. Field extensions
5. Newton lift
6. Algorithmic $p-adic$ integers
7. Basic operations
8. A point counting algorithm

# When do we need *p*-adic numbers?

- In elliptic curve cryptography, most of time, the important objects to manipulate are finite fields $\mathbb{F}_q$.
- Sometimes, we would like to use formulas coming from the classical theory of elliptic curves over $\mathbb{C}$ but they have no meaning in characteristic $p$ because for instance they imply the evaluation of $1/p$.

# Cryptographic applications

Main cryptographic applications of $p$-adic numbers :

- point counting algorithms;
- CM-methods;
- isogeny computations.

# What are the *p*-adic numbers?

A dictionary :

| Function fields | Number theory |
|---|---|
| $\mathbb{C}[X]$ | $\mathbb{Z}$ |
| $\mathbb{C}(X)$ | $\mathbb{Q}$ |
| a monomial $(X-\alpha)$ | $p$ prime |
| finite extension of $\mathbb{C}(X)$ | finite extension of $\mathbb{Q}$ |
| Laurent series about $\alpha$ | $p$-adic numbers |

# Construction of $p$-adic numbers I

Let $p$ be a prime, let $A_n = \mathbb{Z}/p^n\mathbb{Z}$. We have a natural morphism

$$\phi : A_n \to A_{n-1}$$

provided by the reduction modulo $p^{n-1}$. The sequence

$$\dots A_n \to A_{n-1} \to \dots \to A_2 \to A_1$$

is an inverse system.

**Definition**

The ring of $p$-adic numbers is by definition $\mathbb{Z}_p = \varprojlim (A_n, \phi_n)$.

# Construction of $p$-adic numbers II

- An element of $a = \mathbb{Z}_p$ can be represented as a sequence of elements
$$a = (a_1, a_2, \ldots, a_n, \ldots)$$
with $a_i \in \mathbb{Z}/p^i\mathbb{Z}$ and $a_i \mod p^{i-1} = a_{i-1}$. The ring structure is the one inherited from that of $\mathbb{Z}/p^i\mathbb{Z}$.
- The neutral element is $(1, \ldots, 1, \ldots)$.
- There exists natural projections $p_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$, $a \mapsto a_i = a \mod p^i$.

# First properties I

## Proposition

- *Let $x \in \mathbb{Z}_p$, x is invertible if and only if $x \mod p$ is invertible. Let $x \in \mathbb{Z}_p$, there exists a unique $(u, n)$ where u is an invertible element of $\mathbb{Z}_p$ and n a positive integer such that*

$$x = p^n u.$$

- *The integer n is called the valuation of x and denoted by $v(x)$.*

# First properties II

- $\mathbb{Z}_p$ is a characteristic 0 ring;
- $\mathbb{Z}_p$ is integral;
- $\mathbb{Z}_p$ has a unique maximal ideal $\mathscr{O}_p = \{x \in \mathbb{Z}_p | v(x) > 0\}$;
- There is a canonical isomorphism $\mathbb{Z}_p/\mathscr{O}_p \simeq \mathbb{F}_p$.

# The field of $p$-adics

## Definition

The field of $p$-adic numbers noted $\mathbb{Q}_p$ is by definition the field of fractions of $\mathbb{Z}_p$.

- The valuation of $\mathbb{Z}_p$ extend immediately to $\mathbb{Q}_p$ by letting $v(x/y) = v(x) - v(y)$ for $x, y \in \mathbb{Z}_p$;
- $\mathbb{Q}_p$ comes with a norm called the $p$-adic norm given by $|x|_{\mathbb{Q}_p} = p^{-v(x)}$.

# Representation as a series I

## Definition

- An element $\pi \in \mathbb{Z}_p$ is called a uniformizing element if $v(\pi) = 1$.
- Let $p_1$ be the canonical projection from $\mathbb{Z}_p$ to $\mathbb{F}_p$. A map $\omega : \mathbb{F}_p \to \mathbb{Z}_p$ is a system of representatives of $\mathbb{F}_p$ if for all $x \in \mathbb{F}_p$ we have $p_1\left(\omega(x)\right) = x$.

## Definition

An element $x \in \mathbb{Z}_p$ is called a lift of an element $x_0 \in \mathbb{F}_p$ if $p_1(x) = x_0$. Consequently, for all $x \in \mathbb{F}_p$, $\omega(x)$ is a lift of $x$.

# Representation as a series II

Let $\pi$ be a uniformizing element of $\mathbb{Z}_p$, $\omega$ a system of representatives of $\mathbb{F}_p$ in $\mathbb{Z}_p$ and $x \in \mathbb{Z}_p$. Let $n = v(x)$, then $x/\pi^n$ is an invertible element of $\mathbb{Z}_p$ and there exists a unique $x_n \in \mathbb{F}_p$ such that $v\big(x - \pi^n \omega(x_n)\big) = n + 1$. Iterating this process, we obtain that

## Proposition

*There exists a unique sequence $(x_i)_{i \geqslant 0}$ of elements of $\mathbb{F}_p$ such that*

$$x = \sum_{i=0}^{\infty} \omega(x_i)\pi^i.$$

# Field extensions I

- Let $K$ be a finite extension of $\mathbb{Q}_p$ defined by an irreducible polynomial $m \in \mathbb{Q}_p[X]$.
- There exists a unique norm $|\cdot|_K$ on $K$ extending the $p$-adic norm on $\mathbb{Q}_p$.
- $\mathcal{R} = \{x \in K \mid |x|_K \leq 1\}$ is the valuation ring of $K$.
- $\mathcal{M} = \{x \in \mathcal{R} \mid |x|_K < 1\}$ is be the unique maximal ideal of $\mathcal{R}$.

# Field extension II

## Definition

Keeping the notation from above :

- The field $\mathbb{F}_q = \mathcal{R}/\mathcal{M}$ is an algebraic extension of $\mathbb{F}_p$, the degree of which is called the inertia degree of $K$ and is denoted by $f$.
- The absolute ramification index of $K$ is the integer $e = v_K\big(\psi(p)\big)$, where $\psi : \mathbb{Z} \to K$ is the canonical embedding of $\mathbb{Z}$ into $K$.

# Unramified extensions I

We have the

**Theorem**

*Let $d$ be the degree of $K/\mathbb{Q}_p$, then $d = ef$.*

**Definition**

Let $K/\mathbb{Q}_p$ be a finite extension. Then $K$ is called absolutely unramified if $e = 1$. An absolutely unramified extension of degree $d$ is denoted by $\mathbb{Q}_q$ with $q = p^d$ and its valuation ring by $\mathbb{Z}_q$.

# Unramified extensions II

## Proposition

- *Let $K$ be a finite extension of $\mathbb{Q}_p$ defined by an irreducible polynomial $m \in \mathbb{Q}_p[X]$.*
- *Denote by $P_1$ the reduction morphism $\mathcal{R}[X] \to \mathbb{F}_q[X]$ induced by $p_1$ and let $\overline{m}$ be the irreducible polynomial defined by $P_1(m)$.*
- *The extension $K/\mathbb{Q}_p$ is absolutely unramified if and only if $\deg m = \deg \overline{m}$. Let $d = \deg \overline{m}$ and $\mathbb{F}_q = \mathbb{F}_{p^d}$ the finite field defined by $\overline{m}$, then we have $p_1(\mathcal{R}) = \mathbb{F}_q$.*

# Unramified extensions III

The classification of unramified extension is given by their degree.

**Proposition**

*Let $K_1$ and $K_2$ be two unramified extensions of $\mathbb{Q}_p$ defined respectively by $m_1$ and $m_2$ then $K_1 \simeq K_2$ if and only if* $\deg m_1 = \deg m_2$.

# Unramified extensions IV

The Galois properties of unramified extensions of $\mathbb{Q}_p$ is the same as that of finite fields.

## Proposition

*An unramified extension $K$ of $\mathbb{Q}_p$ is Galois and its Galois group is cyclic generated by an element $\Sigma$ that reduces to the the Frobenius morphism on the residue field. We call this automorphism the Frobenius substitution on $K$.*

# Lefschetz principle I

The field $\mathbb{Q}_p$ and its unramified extensions enjoy several important properties:

- Their Galois groups reflect the structure of finite field extensions;
- Their are big enough to be characteristic 0 fields...
- ...but small enough so that there exists an field morphism $K \to \mathbb{C}$ for any $K$ finite extension of $\mathbb{Q}_p$.
- Warning : $\mathbb{Q}_p/\mathbb{Q}$ is NOT an algebraic extension.

# Lefschetz principle II

The so-called Lefschetz principle consists in

- lifting objects defined over finite fields over the $p$-adics,
- then embedding the $p$-adics into $\mathbb{C}$ where we can obtain algebraic relations using analytic methods,
- and then interpret these relations over finite fields by reduction modulo $p$.

# Newton lift I

## Proposition

*Let $K$ be an unramified extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{R}$ and norm $|\cdot|_K$. Let $f \in \mathcal{R}[X]$ and let $x_0 \in \mathcal{R}$ be such that*

$$|f(x_0)|_K < |f'(x_0)|_K^2$$

*then the sequence*

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

*converges quadratically towards a zero of $f$ in $\mathcal{R}$.*

# Newton lift II

- The quadratic convergence implies that the precision of the approximation nearly doubles at each iteration.
- More precisely, let $k = v_K\big(f'(x_0)\big)$ and let $x$ be the limit of the sequence (1). Suppose that $x_i$ is an approximation of $x$ to precision $n$, i.e. $v_K(x - x_i) \geq n$, then $x_{i+1} = x_i - f(x_i)/f'(x_i)$ is an approximation of $x$ to precision $2n - k$.

# Hensel lift

**Lemma (Hensel)**

*Let $f, A_k, B_k, U, V$ be polynomials with coefficients in $\mathcal{R}$ such that*

- $f \equiv A_k B_k \pmod{\mathcal{M}^k}$,
- $U(X)A_k(X) + V(X)B_k(X) = 1$, *with $A_k$ monic and* $\deg U(X) < \deg B_k(X)$ *and* $\deg V(X) < \deg A_k(X)$

*then there exist polynomials $A_{k+1}$ and $B_{k+1}$ satisfying the same conditions as above with $k$ replaced by $k+1$ and*

$$A_{k+1} \equiv A_k \pmod{\mathcal{M}^k}, \qquad B_{k+1} \equiv B_k \pmod{\mathcal{M}^k}.$$

# Representation of $p - adic$ integers

- In practice, one computes with $p$-adic integers up to some precision $N$.
- An element $a \in \mathbb{Z}_p$ is approximated by $p_N(a) \in \mathbb{Z}/p^N\mathbb{Z}$.
- The arithmetic reduces to the arithmetic modulo $p^N$.
- For a given precision $N$, each element takes $O(N \log p)$ space.

# Polynomial representation I

- Let $\mathbb{Q}_q$ be the unramified extension of $\mathbb{Q}_p$ of degree $d$. By proposition 3, $\mathbb{Q}_q$ is defined by any polynomial $M[X] \in \mathbb{Z}_p[X]$ such that $m = P_1(M) \in \mathbb{F}_p[X]$ is an irreducible degree $d$ polynomial. We can assume that $M$ is monic.
- As a consequence every $a \in \mathbb{Q}_q$ can be written as $a = \sum_{i=0}^{d-1} a_i X^i$ with $a_i \in \mathbb{Q}_p$ and every $b \in \mathbb{Z}_q$ can be written as $b = \sum_{i=0}^{d-1} b_i X^i$ with $b_i \in \mathbb{Z}_p$.
- In order to make the reduction modulo $M$ very fast, we choose $M$ sparse.

# Polynomial representation II

- In general, we work with $\mathbb{Z}_q$ up to precision $N$.
- This can be done by computing in $(\mathbb{Z}/N\mathbb{Z})[X]/(M_N)$ where $M_N$ is the reduction of $M$ modulo $p^N$.
- The size of an object is $O(dN\log(p))$.

# Polynomials representation III

Two common choices to speed up arithmetic in $\mathbb{Z}_q$ :

- sparse modulus representation : we deduce $M$ by lifting in a trivial way the coefficients of $m$. The reduction modulo $M$ of a polynomial of degree less than $2(d-1)$ takes $d(w-1)$ multiplication of a $\mathbb{Z}/N\mathbb{Z}$ element by a small integer and $dw$ subtractions in $\mathbb{Z}_p$ where $w$ is the number of non zero coefficients in $M$.
- Teichmüller modulus representation : We define $M$ as the unique polynomial over $\mathbb{Z}_p$ such that $M(X)|X^q - X$ and $M(X) \mod p = m(X)$. In this representation we have $\Sigma(X) = X^p$.

# Multiplication I

- The arithmetic in $\mathbb{Z}_p$ with precision $N$ is the same thing as the arithmetic in $\mathbb{Z}/p^N\mathbb{Z}$.
- The multiplication of two elements of $\mathbb{Z}_p$ takes $O(N^\mu)$ where $\mu$ is the exponent in the multiplication estimate of two integers ($\mu = 1 + \epsilon$ with FFT, $\mu = \log 3$ with Karatsuba, and $\mu = 2$ with school book method);

# Multiplication II

- The multiplications of two elements of $\mathbb{Z}_q$ is equivalent to the multiplication of two polynomials in $(\mathbb{Z}/N\mathbb{Z})[X]$ which take $O(d^\nu N^\mu)$ time (here $\nu$ is the exponent of the complexity function for the multiplication of two polynomials).
- In all the complexity of the multiplication of two *p*-adics is $O(d^\nu N^\mu)$.

# Computing inverse with Newton lift

In order to inverse $a \in \mathbb{Z}_q$ can be done by

- computing an inverse of $p_1(a) \in \mathbb{F}_q$;
- taking any lift $z_1 \in \mathbb{Z}_q$ of $1/p_1(a) \in \mathbb{F}_q$;
- $z_1$ is an approximation to precision 1 of the root of the polynomial $f(X) = 1 - aX$;
- lifting the root $z_1$ to a given precision with Newton.

# Computing inverse with Newton lift

**Inverse**
**Input:** A unit $a \in \mathbb{Z}_q$ and a precision $N$
**Output:** The inverse of $a$ to precision $N$

1. If $N = 1$ Then
2. $\quad$ $z \leftarrow 1/a \mod p$
3. Else
4. $\quad$ $z \leftarrow Inverse(a, \lceil \frac{N}{2} \rceil)$
5. $\quad$ $z \leftarrow z + z(1 - az) \mod p^N$
6. Return $z$

# Computing inverse with Newton lift

- We go through the $\log(N)$ iterations;
- The dominant operation is a multiplication of elements of $\mathbb{Z}_q$ with precision $N$ : this can be done in $O(d^\nu N^\mu)$ time;
- The overall complexity is $O(\log(N) d^\nu N^\mu)$.

# Computing square root with Newton lift

- In the same way it, one can compute the inverse square root of $a \in \mathbb{Z}_q$ to precision $N$ in time $O(\log(N) d^{\nu} N^{\mu})$;
- Principle: compute the square root mod $p$ and then do a Newton lift with the polynomial $f(X) = 1 - aX^2$;
- For a reference ([CFA$^+$06] pp. 248).

# The AGM algorithm I

**Elliptic curve AGM**

**Input:** An ordinary elliptic curve $E : y^2 + xy = x^3 + \overline{c}$ over $\mathbb{F}_{2^d}$ with $j(E) \neq 0$.

**Output:** The number of points on $E(\mathbb{F}_{2^d})$.

1. $N \leftarrow \lceil \frac{d}{2} \rceil + 3$
2. $a \leftarrow 1$ and $b \leftarrow (1 + 8c) \mod 2^4$
3. For $i = 5$ To $N$ Do
4. $\quad (a, b) \leftarrow ((a + b)/2, \sqrt{ab}) \mod 2^i$
5. $a_0 \leftarrow a$

# The AGM algorithm II

1. For $i = 0$ To $d - 1$ Do
2. $\quad (a, b) \leftarrow ((a + b)/2, \sqrt{ab}) \mod 2^N$
3. $t \leftarrow \dfrac{a_0}{a} \mod 2^{N-1}$
4. If $t^2 > 2^{d+2}$ Then $t \leftarrow t - 2^{N-1}$
5. Return $2^d + 1 - t$

# Complexity of the AGM algorithm

- You know everything you need to see that the complexity is quasi-cubic.

# The End

- Thank you for your attention.
- Any question?

Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors.
*Handbook of elliptic and hyperelliptic curve cryptography*.
Discrete Mathematics and its Applications (Boca Raton).
Chapman & Hall/CRC, Boca Raton, FL, 2006.

Neal Koblitz.
*p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*.
Springer-Verlag, New York, second edition, 1984.

Alain M. Robert.

*A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*.
Springer-Verlag, New York, 2000.

J.-P. Serre.
*A course in arithmetic*.
Springer-Verlag, New York, 1973.
Translated from the French, Graduate Texts in Mathematics, No. 7.

Jean-Pierre Serre.
*Local fields*, volume 67 of *Graduate Texts in Mathematics*.
Springer-Verlag, New York, 1979.
Translated from the French by Marvin Jay Greenberg.