Efficient p-Adic Arithmetic

Fré Vercauteren

Katholieke Universiteit Leuven

29-30 August 2005

p-adic Numbers

- p-adic valuation $\mathrm{ord}_p(r)$ of $r \in \mathbb{Q}$ is ρ with

$$r = p^\rho u/v, \quad \rho, u, v \in \mathbb{Z}, \quad p \nmid u,\ p \nmid v$$

- Non-archimedian p-adic norm $|r|_p = p^{-\rho}$
- Field of p-adic numbers $\mathbb{Q}_p$ is completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$,

$$\sum_m^\infty a_i p^i, \quad a_i \in \{0, 1, \dots, p-1\}, \quad m \in \mathbb{Z}.$$

- p-adic integers $\mathbb{Z}_p$ is the ring with $|\cdot|_p \leq 1$ or $m \geq 0$.
- Ideal $M = \{x \in \mathbb{Q}_p \mid |x|_p < 1\} = p\mathbb{Z}_p$ and $\mathbb{Z}_p/M \cong \mathbb{F}_p$.

p-adic Numbers in Practice

- $\mathbb{Z}_p$: for fixed absolute precision N, compute modulo p^N
- $\mathbb{Q}_p$: write each element as $p^{\mathrm{ord}_p(x)} u_x$ with $u_x \in \mathbb{Z}_p^\times$
- $\mathbb{Q}_p$: for fixed relative precision of N, $u_x \bmod p^N$
- No rounding off errors occur unlike floating point
- Loss of absolute precision on division by p
- Possible loss of relative precision when subtracting
- All operations asymptotically in time $O(\log pN)^{1+\varepsilon}$
- For $\log_2 p^N < 512$, schoolbook methods suffice

Unramified Extensions of p-adics

- K extension of $\mathbb{Q}_p$ of degree n with valuation ring R and maximal ideal $M_R = \{x \in K \mid |x|_p < 1\}$ of R
- K is called unramified iff its residue field $R/M_R \cong \mathbb{F}_q$
- K denoted with $\mathbb{Q}_q$ and its valuation ring with $\mathbb{Z}_q$
- $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) =< \sigma >$ with

$$\sigma : \mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^p$$

- $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) =< \Sigma >$ generated by Frobenius substitution
- Note: Σ is not simple p-powering !

Representation of $\mathbb{Q}_q$

- Let $\mathbb{F}_q \cong \mathbb{F}_p[t]/(\bar{f}(t))$ then $\mathbb{Q}_q$ can be constructed as
$$\mathbb{Q}_q \cong \mathbb{Q}_p[t]/(f(t)),$$
with $f(t)$ any lift of $\bar{f}(t)$ to $\mathbb{Z}_p[t]$.
- Different choices of $f(t)$ have different advantages.
- Valuation ring $\mathbb{Z}_q \cong \mathbb{Z}_p[t]/f(t)$; $a \in \mathbb{Z}_q$ represented as
$$a = \sum_{i=0}^{n-1} a_i t^i \,, \quad a_i \in \mathbb{Z}_p \,.$$
- Reduction mod p^m gives $(\mathbb{Z}/p^m\mathbb{Z})[t]/(f_m(t))$ with $f_m(t) \equiv f(t) \bmod p^m$

Sparse modulus representation of $\mathbb{Q}_q$

- Let $\bar{f}(t) = \sum_{i=0}^{n} \bar{f}_i t^i$ with $\bar{f}_i \in \mathbb{F}_p$ and $\bar{f}_n = 1$.
- Preserve the sparseness of $\bar{f}$, define

$$f(t) = \sum_{i=0}^{n} f_i t^i \,, 0 \leq f_i < p, f_i \equiv \bar{f}_i \bmod p$$

- Reduction mod f of a polynomial of degree $\leq 2(n-1)$
  - $n(w-1)$ multiplications of a $\mathbb{Z}_p$-element by a small integer
  - nw subtractions in $\mathbb{Z}_p$
  - w is the number of nonzero coefficients of f

Teichmüller Representation of $\mathbb{Q}_q$

- Let $\mathbb{F}_q \cong \mathbb{F}_p[t]/(\bar{f}(t))$, then since $\mathbb{F}_q$ is splitting field $t^q - t$ we have $\bar{f}(t)|t^q - t$
- Hensel's Lemma: let $g(t) \in \mathbb{Z}_q[t]$ with l.c. a unit and let $g(t) \equiv \bar{r}(t)\bar{s}(t) \bmod p$ with $\bar{r}, \bar{s}$ coprime, then exist unique $r, s \in \mathbb{Z}_q[t]$ with $g(t) = r(t)s(t)$.
- By Hensel, exists unique $f(t) \in \mathbb{Z}_p[t]$ such that

$$f(t)|t^{q-1} - 1 \quad \text{and} \quad f(t) \equiv \bar{f}(t) \bmod p$$

- $\mathbb{Q}_q \cong \mathbb{Q}_p[\theta]$ with $f(\theta) = 0$ and θ is $q - 1$-th root of unity.
- Practice: compute $f(t) \bmod p^m$ and need fast division with remainder

Gaussian Normal Basis Representation of $\mathbb{Q}_q$

- Basis of $\mathbb{Q}_q/\mathbb{Q}_p$ is called normal if its of the form

$$\{\Lambda(\alpha)\}_{\Lambda \in \mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)}$$

- Gauss period of type I generated by $n+1$-th root of unity
  - $n+1$ is prime different from p
  - $\gcd(n/e, n) = 1$, with e order of p modulo $n+1$
- Minimum polynomial of α is $\frac{t^{n+1}-1}{t-1} = t^n + t^{n+1} + \cdots + t + 1$
- Redundant representation modulo $t^{n+1} - 1$ speeds up operations

Frobenius Substitution: All Moduli

- Let $\mathbb{Z}_q \cong \mathbb{Z}_p[\theta] \cong \mathbb{Z}_p[t]/(f(t))$ with $f(t) = \sum_{i=0}^{n-1} f_i t^i$

$$0 = \Sigma(f(\theta)) = \sum_{i=0}^{n-1} f_i \Sigma(\theta)^i = f(\Sigma(\theta)) \,.$$

- Compute $\Sigma(\theta)$ as zero of $f(t)$ from $\Sigma(\theta) \equiv \theta^p \mod p$.
- Frobenius of $a = \sum_{i=0}^{n-1} a_i \theta^i \in \mathbb{Q}_q$ is $\Sigma(a) = \sum_{i=0}^{n-1} a_i \Sigma(\theta)^i$
- Horner: $O(n)$ multiplications $\Rightarrow O(n(nm)^{1+\varepsilon})$ time.
- Paterson-Stockmeyer: let $B = \lceil \sqrt{n} \rceil$ and rewrite

$$a(t) = \sum_{j=0}^{\lceil n/B \rceil} \left(\sum_{i=0}^{B-1} a_{i+Bj} t^i \right) t^{Bj} ,$$

compute $\Sigma(a)$ using $O(\sqrt{n})$ multiplications in $\mathbb{Z}_q$

Frobenius Substitution: Teichmüller Moduli

- $f(t)$ is Teichmüller modulus iff $f(t) | t^{q-1} - 1$, so zero θ of f is $q - 1$-th root of unity
- As before: $f(\Sigma(\theta)) = 0$, so $\Sigma(\theta)$ also $q - 1$-th root of unity
- Since $\Sigma(\theta) \equiv \theta^p \bmod p$ conclude that

$$\Sigma(\theta) = \theta^p$$

- Frobenius of $a = \sum_{i=0}^{n-1} a_i \theta^i \in \mathbb{Q}_q$ is

$$\Sigma(a) = \sum_{i=0}^{n-1} a_i \theta^{ip} \bmod f(t).$$

- Reduction modulo $f(t)$ takes at most $p - 1$ multiplications over $\mathbb{Z}_q$

Frobenius Substitution: Gaussian Normal Basis

- Gaussian Normal Basis of Type I embedded in

$$\mathbb{Z}_q[t]/(t^{n+1} - 1)$$

- θ is $n+1$-th root of unity, so as before $\Sigma(\theta) = \theta^p$
- Iterated Frobenius substitution:

$$\Sigma^k\left(\sum_{i=0}^{n} a_i \theta^i\right) = \sum_{i=0}^{n} a_i \theta^{ip^k} = a_0 + \sum_{j=1}^{n} a_{j/p^k \bmod n+1} \theta^j$$

Newton Lifting

- Theorem: Let $g \in \mathbb{Z}_q[X]$ and assume that $a \in \mathbb{Z}_q$ satisfies

$$\mathrm{ord}_p\big(g'(a)\big) = k \text{ and } \mathrm{ord}_p\big(g(a)\big) = n + k$$

for some $n > k$, then exists a unique root $b \in \mathbb{Z}_q$ of f with $b \equiv a \pmod{p^n}$.

- a is called an approximate root of g known to precision n.
- Newton iteration: compute

$$z = a - \frac{g(a)}{g'(a)}$$

then $z \equiv b \pmod{p^{2n-k}}$, $g(z) \equiv 0 \pmod{p^{2n}}$ and $\mathrm{ord}_p\big(g'(z)\big) = k$.

Newton Lifting: Minimal Precision

- z has to be correct modulo p^{2n-k}
- $g'(a)$ mod p^n, so $g'(a)/p^k$ is a unit known modp^{n-k}
- $g(a)$ mod p^{2n}, then $g(a) \equiv 0 \bmod p^{n+k}$ and $g(a)/p^{n+k}$ known modp^{n-k}
- Finally compute

$$z \equiv a - p^n \frac{g(a)/p^k}{g'(a)/p^k} \bmod p^{2n-k}$$

where inversion and multiplication is computed mod p^{n-k}

Newton Lifting: Algorithm

- **If** $N \leq n$ **Then**
- $z \leftarrow a$
- **Else**
- $N' \leftarrow \left\lceil \frac{N+k}{2} \right\rceil$
- $z \leftarrow$ Newton iteration (g, a, k, N')
- $z \leftarrow z - \dfrac{g(z)}{g'(z)} \pmod{p^N}$
- **Return** z

Convergence is quadratic, so complexity determined by last step only!

Newton Lifting: Applications

- Inverse of $a \in \mathbb{Z}_q^\times$, NL on $g(z) = az - 1$

$$z \leftarrow z + z(1 - az)$$

- Inverse square root of $a \in \mathbb{Z}_q$, NL on $g(z) = a^2 z - 1$

$$z \leftarrow z + z(1 - az^2)/2$$

- Actually faster than square root
- Teichmüller lift of element $\overline{a} \in \mathbb{F}_q^\times$, unique $q - 1$-th root of unity $a \in \mathbb{Z}_q$ such that $a \equiv \overline{a} \bmod p$
- NL on $g(z) = z^q - z$ starting from $\overline{a}$

Twisted Newton Lifting

- Polynomial $\Phi(X,Y) \in \mathbb{Z}_q[X,Y]$, consider the equation

$$\Phi(X, \Sigma(X)) = 0$$

- Solve from $\overline{x} \in \mathbb{F}_q$ with $\Phi(\overline{x}, \Sigma(\overline{x})) \equiv 0 \bmod p$.
- Assume we have $x_t \equiv x \bmod p^t$ and define $\delta = (x - x_t)/p^t$,

$$\begin{aligned} 0 &= \Phi(x, \Sigma(x)) = \Phi(x_t + p^t\delta_t, \Sigma(x_t + p^t\delta_t)) \\ &= \Phi(x_t, \Sigma(x_t)) + p^t \left(\frac{\partial \Phi}{\partial X}(x_t, \Sigma(x_t))\delta_t + \frac{\partial \Phi}{\partial Y}(x_t, \Sigma(x_t))\Sigma(\delta_t) \right) + O(p^{2t}) \end{aligned}$$

$$\boxed{\frac{\partial \Phi}{\partial Y}(x_t, \Sigma(x_t))\Sigma(\delta_t) + \frac{\partial \Phi}{\partial X}(x_t, \Sigma(x_t))\delta_t \equiv -\frac{\Phi(x_t, \Sigma(x_t))}{p^t} \bmod p^t}$$

Generalised Artin-Schreier Equations

- Hilbert 90: $x^p - x + \alpha = 0$ has solution iff $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 0$.
- Definition: generalised Artin-Schreier equation

$$a\Sigma(X) + bX + c = 0\,, \qquad a, b, c \in \mathbb{Z}_q, a \in \mathbb{Z}_q^{\times}\,.$$

- Let $\beta = b/a$ and $\gamma = c/a$, then $\Sigma(X) + \beta X + \gamma = 0$.
- Define β_i, γ_i by $\Sigma^i(X) = \beta_i X + \gamma_i$, then

$$\boxed{X = \Sigma^n(X) = \beta_n X + \gamma_n \Rightarrow X = \frac{\gamma_n}{1-\beta_n}}$$

- Recurrence relation via

$$\Sigma^{i+1}(X) = \Sigma(\Sigma^i(X)) = \Sigma(\beta_i X + \gamma_i) = \Sigma(\beta_i)(\beta_1 X + \gamma_1) + \Sigma(\gamma_i)$$

- Conclusion: $\beta_{i+1} = \beta_1 \Sigma(\beta_i)$ and $\gamma_{i+1} = \gamma_1 \Sigma(\beta_i) + \Sigma(\gamma_i)$

Lercier-Lubicz Algorithm: Gaussian Normal Basis

- Apply square and multiply with recurrence relation, i.e.

$$\Sigma^{2k}(X) = \Sigma^k(\Sigma^k(X)) = \Sigma^k(\beta_k X + \gamma_k) = \Sigma^k(\beta_k)(\beta_k X + \gamma_k) + \Sigma^k(\gamma_k)$$

$$\boxed{\beta_{2k} = \beta_k \Sigma^k(\beta_k) \qquad \gamma_{2k} = \gamma_k \Sigma^k(\beta_k) + \Sigma^k(\gamma_k)}$$

$$\Sigma^{2k+1}(X) = \Sigma(\Sigma^{2k}(X)) = \Sigma(\beta_{2k} X + \gamma_{2k}) = \Sigma(\beta_{2k})(\beta_1 X + \gamma_1) + \Sigma(\gamma_{2k})$$

$$\boxed{\beta_{2k+1} = \beta_1 \Sigma(\beta_{2k}) \qquad \gamma_{2k+1} = \gamma_1 \Sigma(\beta_{2k}) + \Sigma(\gamma_{2k})}$$

- $O(\log n)$ iterations needed to reach $\Sigma^n(X)$.
- $O(\log n)$ multiplications and iterated Frobenius substitutions.
- Conclusion: efficient for fields with Gaussian Normal Basis.

Lercier-Lubicz Algorithm

- **If** $k = 1$ **Then**
- $a_k \leftarrow a \bmod p^N$ and $b_k \leftarrow b \bmod p^N$
- **Else**
- $k' \leftarrow \left\lfloor \frac{k}{2} \right\rfloor$
- $a_{k'}, b_{k'} \leftarrow$ Lercier-Lubicz (a, b, k', N)
- $a_k \leftarrow a_{k'} \Sigma^{k'}(a_{k'}) \bmod p^N$
- $b_k \leftarrow b_{k'} \Sigma^{k'}(a_{k'}) + \Sigma^{k'}(b_{k'}) \bmod p^N$
- **If** $k \equiv 1 \pmod 2$ **Then**
- $b_k \leftarrow b\, \Sigma(a_k) + \Sigma(b_k) \bmod p^N$
- $a_k \leftarrow a\, \Sigma(a_k) \bmod p^N$
- **Return** a_k, b_k

Harley's Algorithm

- $a\Sigma(X) + bX + c = 0$ with $a, b, c \in \mathbb{Z}_q$, $a \in \mathbb{Z}_q^\times$, $b \in p\mathbb{Z}_q$.
- Algorithm computes $x_t \bmod p^t$, and let $\delta_t = (x - x_t)/p^t$

$$\begin{aligned} 0 = a\Sigma(x) + bx + c &= a\Sigma(x_t + p^t\delta_t) + b(x_t + p^t\delta_t) + c \\ &\equiv ap^t\Sigma(\delta_t) + bp^t\delta_t + (a\Sigma(x_t) + bx_t + c) \bmod p^{2t} \end{aligned}$$

$$\boxed{a\Sigma(\delta_t) + b\delta_t + \frac{a\Sigma(x_t) + bx_t + c}{p^t} \equiv 0 \bmod p^t}$$

- Base case $t = 1$

$$a\Sigma(X) + bX + c \equiv aX^p + c \equiv 0 \bmod p \Rightarrow x \equiv -(\frac{c}{a})^{p^{n-1}} \bmod p$$

Harley's Algorithm

- **If** $N = 1$ **Then**
- $x \leftarrow (-\gamma/\alpha)^{1/p} \pmod{p}$
- **Else**
- $N' \leftarrow \left\lceil \frac{N}{2} \right\rceil$
- $x' \leftarrow \text{Harley}\,(\alpha, \beta, \gamma, N')$
- $\gamma' \leftarrow \dfrac{\alpha\Sigma(x') + \beta x' + \gamma}{p^{N'}} \bmod p^{N-N'}$
- $\Delta' \leftarrow \text{Harley}\,(\alpha, \beta, \gamma', N - N')$
- $x \leftarrow \left(x' + p^{N'}\Delta'\right) \bmod p^N$
- **Return** x

Twisted Newton Lifting

- **If** $N \leq k + 1$ **Then**
- $\quad x \leftarrow x_0$
- **Else**
- $\quad N' \leftarrow \left\lceil \frac{N+k}{2} \right\rceil$
- $\quad x' \leftarrow$ Twisted Newton lift (ϕ, x_0, N')
- $\quad y' \leftarrow \Sigma(x') \bmod p^{N+k}$
- $\quad V \leftarrow \phi(x', y') \bmod p^{N+k}$
- $\quad \Delta_y \leftarrow \frac{\partial \phi}{\partial Y}(x', y') \bmod p^{N'}$
- $\quad \Delta_z \leftarrow \frac{\partial \phi}{\partial Z}(x', y') \bmod p^{N'}$
- $\quad \delta \leftarrow$ Artin–Schreier $(\Delta_z / p^k, \Delta_y / p^k, V / p^{N'+k}, N' - k)$
- $\quad x \leftarrow \left(x' + p^{N'} \delta\right) \bmod p^N$
- **Return** x

Application Twisted Newton Lifting

- Computing the Teichmüller lift of $\overline{a} \in \mathbb{F}_q$
- Find unique $q - 1$-th root of unity $a \in \mathbb{Z}_q$ with $a \equiv \overline{a} \bmod p$
- As before: $\Sigma(a) = a^p$, so solve the equation

$$\Sigma(X) = X^p \qquad \text{from } X \equiv \overline{a} \bmod p$$

Teichmüller Lift of Field Polynomial

- Let $\mathbb{F}_q \cong \mathbb{F}_p[t]/(\bar{f}(t))$ and let $f(t) \in \mathbb{Z}_p[t]$ such that

$$f(t) | t^{q-1} - 1 \quad \text{and} \quad f(t) \equiv \bar{f}(t) \bmod p$$

- If $f(\theta) = 0$, then $f(t) = \prod_{i=0}^{n-1}(t - \Sigma^i(\theta)) = \prod_{i=0}^{n-1}(t - \theta^{p^i})$
- Let ζ_p be formal p-th root of unity then

$$f(t^p) = \prod_{i=0}^{p-1} f(\zeta_p t) \qquad (\star)$$

- Use Newton iteration to compute $f(t)$ as the solution of $(\star)$
- Example $p = 2$: $f(t^2) = f(t)f(-t)$

Logarithm

- p-adic logarithmic function of $x \in \mathbb{Z}_q$ is defined by

$$\log(x) = \sum_{i=1}^{\infty} (-1)^{i-1} \frac{(x-1)^i}{i}$$

- $\log(x)$ converges for $\mathrm{ord}_p(x-1) > 0$
- Horner: $\log(a)$ up to precision N takes $O(N)$ multiplications
- Satoh, Skjernaa, and Taguchi: $\mathrm{ord}_p(a^{p^k} - 1) > k$

$$\log(a) \equiv p^{-k} \left(\log(a^{p^k}) \pmod{p^{N+k}} \right) \pmod{p^N}$$

- $a \in \mathbb{Z}_q / p^N \mathbb{Z}_q$, then a^{p^k} is well defined in $\mathbb{Z}_q / p^{N+k} \mathbb{Z}_q$
- $k \simeq \sqrt{N}$, then $\log(a) \pmod{p^N}$ in $O(\sqrt{N})$ multiplications

Exponential

- p-adic exponential function of $x \in \mathbb{Z}_q$ defined by

$$\exp(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}$$

- Need $\mathrm{ord}_p(x) > 1/(p-1)$, since $\mathrm{ord}_p(i!) \leq (i-1)/(p-1)$
- For $a \in \mathbb{Z}_p$, $\mathrm{ord}_p(a) \geq 1$ for $p \geq 3$ and $\mathrm{ord}_p(a) \geq 2$ for $p = 2$.

$$\exp(a) \equiv \exp(p)^{a/p} \pmod{p^N}, \quad \text{for } p \geq 3,$$
$$\exp(a) \equiv \exp(4)^{a/4} \pmod{2^N}, \quad \text{for } p = 2.$$

Trace

- The trace of $x \in \mathbb{Q}_q$ is

$$\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x) = x + \Sigma(x) + \cdots + \Sigma^{n-2}(x) + \Sigma^{n-1}(x) \in \mathbb{Q}_p$$

- Let $a \in \mathbb{Q}_q$, then $\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(p^k a) = p^k \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(a)$
- Assume that a is unit in $\mathbb{Z}_q$, and for $a = \sum_{i=0}^{n-1} a_i t^i$

$$\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(a) = \sum_{i=0}^{d-1} a_i \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(t^i).$$

- $\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(t^i)$ for $i = 0, \ldots, n-1$ using Newton's formula:

$$\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(t^i) + \sum_{j=1}^{i-1} \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(t^{i-j}) f_{d-j} + i f_{d-i} \equiv 0 \pmod{p^N},$$

Norm Computation

Analytic

- $a \in \mathbb{Z}_q$ is close to unity, i.e. $\mathrm{ord}_p(a-1) > \frac{1}{p-1}$ then

$$\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a) = \exp(\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(\log(a)))$$

Resultants

- $a = \sum_{i=0}^{n-1} a_i \theta^i \in \mathbb{Z}_q^\times$ and let $A(t) = \sum_{i=0}^{n-1} a_i t^i$

$$\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a) = \prod_{i=0}^{n-1} \Sigma^i(a) = \prod_{i=0}^{n-1} A(\Sigma^i(\theta))$$

- If $\mathbb{Z}_q \cong \mathbb{Z}_p[t]/(f(t))$, then $f(t) = \prod_{i=0}^{n-1}(t - \Sigma^i(\theta))$, thus

$$\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(a) = \prod_{i=0}^{n-1} A(\Sigma^i(\theta)) = \mathrm{Res}(f(t), A(t))$$