Computing Zeta Functions of Curves over Finite Fields

Fré Vercauteren

Katholieke Universiteit Leuven

30 July 2008
Introduction

$p$-adic Numbers

Satoh’s Algorithm
The Zeta Function and Weil Conjectures

Let $\overline{C}$ be a smooth projective curve over $\mathbb{F}_q$; the zeta function of $\overline{C}$ is

$$Z(T) = Z(\overline{C}; T) = \exp \left( \sum_{k=1}^{\infty} \frac{N_k T^k}{k} \right)$$

with $N_k$ the number of points on $\overline{C}$ with coordinates in $\mathbb{F}_{q^k}$.

Weil Conjectures:

- $Z(T)$ is a rational function over $\mathbb{Z}$ and can be written as
  $$\frac{P(T)}{(1 - T)(1 - qT)}$$

- $P(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$ with $g$ genus of $\overline{C}$ and $|\alpha_i| = \sqrt{q}$

- $P(T) = \sum_{i=0}^{2g} a_i T^i$ with $a_0 = 1$, $a_{2g} = q^g$ and $a_{g+i} = q^i a_{g-i}$
Ultimate Goal

- Given $\bar{C}$ over $\mathbb{F}_q$ of genus $g$, compute zeta function efficiently (at least polynomial time) for a bounded range of $q^g \leq 2^{512}$

- $q^g$ roughly the size of the group $J_C(\mathbb{F}_q)$

- Current situation:
  - Elliptic curves: efficient solution for all $\mathbb{F}_q$
  - Hyperelliptic curves: good solution for $\mathbb{F}_{p^n}$ and $p$ small, any genus allowed
  - Nondegenerate curves: decent solution for $\mathbb{F}_{p^n}$, $p$ small, small genus
Central Object: Frobenius Endomorphism

- Recall $a \in \overline{\mathbb{F}}_q$ is in $\mathbb{F}_q$ iff $a^q = a$
- Frobenius automorphism $\varphi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q : x \mapsto x^q$ induces
  - morphism $\varphi_q$ on $C(\overline{\mathbb{F}}_q)$
  - endomorphism $\varphi_q$ on $J_C(\overline{\mathbb{F}}_q)$
- $\mathbb{F}_q$-rational points are invariant under $\varphi_q$

\[ J_C(\overline{\mathbb{F}}_q) = \text{Ker}(1 - \varphi_q) \quad \# J_C(\overline{\mathbb{F}}_q) = \deg(1 - \varphi_q) \]

- Theorem: $P(T) = \chi(1/T)t^{2g}$
- Remark: for $q = p^n$, then $\varphi_q$ is composition of $n$ morphisms of degree $p$ (easy to handle for $p$ small)
Overview of Existing Approaches

- \( p \)-adic: Schoof’s algorithm and generalisations
  - consider the \( l \)-torsion as first order approximations of \( l \)-adic cohomology (cfr. representation on Tate module)
  - compute characteristic polynomial of Frobenius modulo \( l_i \), for various small \( l_i \) and recover \( \chi(T) \mod \prod l_i \).

- \( p \)-adic:
  - canonical lift
  - \( p \)-adic cohomology
  - \( p \)-adic deformation
**p-adic Numbers**

- **p-adic valuation** $\text{ord}_p(r)$ of $r \in \mathbb{Q}$ is $\rho$ with
  \[ r = p^\rho \frac{u}{v}, \quad \rho, u, v \in \mathbb{Z}, \quad p \nmid u, \ p \nmid v \]

- 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. $| \cdot |_p$,
  \[ \sum_{m} a_i p^i, \quad a_i \in \{0, 1, \ldots, p - 1\}, \quad m \in \mathbb{Z}. \]

- 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 $\mathbb{Z}_p/M \cong \mathbb{F}_p$. 

Fré Vercauteren  Computing Zeta Functions of Curves over Finite Fields
$p$-adic Numbers in Practice

- $\mathbb{Z}_p$: for fixed absolute precision $N$, compute modulo $p^N$
- $\mathbb{Q}_p$: write each element as $p^{\text{ord}_p(x)} u_x$ with $u_x \in \mathbb{Z}_p^\times$
- $\mathbb{Q}_p$: for fixed relative precision of $N$, $u_x \mod p^N$
- 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 $O(N \log p)^{1+\varepsilon}$
- 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 $\mathbb{Z}_q$
- $\text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) \cong \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \sigma \rangle$ with
  \[ \sigma : \mathbb{F}_q \rightarrow \mathbb{F}_q : x \mapsto x^p \]
- $\text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) = \langle \Sigma \rangle$ generated by Frobenius substitution
- Note: $\Sigma$ 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 $f_m(t) \equiv f(t) \mod p^m$
Frobenius Substitution

- 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 $\Sigma(a) = \sum_{i=0}^{n-1} a_i \Sigma(\theta)^i$

- If $\theta$ is $(q-1)$-th root of unity (Teichmüller lift), then $\Sigma(\theta) = \theta^p$

- Occurs when $f(t)|t^q - t$, i.e. is Teichmüller modulus
Newton Lifting

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

\[
\text{ord}_p(g'(a)) = k \quad \text{and} \quad \text{ord}_p(g(a)) = n + k
\]

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 \( \text{ord}_p(g'(z)) = k \).
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 mod $p^{n-k}$
- $g(a) \mod p^{2n}$, then $g(a) \equiv 0 \mod p^{n+k}$ and $g(a)/p^{n+k}$ known mod $p^{n-k}$
- Finally compute

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

where inversion and multiplication is computed mod $p^{n-k}$
Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$ with $q = p^n$.

Recall the $q$-th power Frobenius endomorphism $\varphi_q : E \rightarrow E : (x, y) \mapsto (x^q, y^q)$.

Characteristic polynomial of $\varphi_q$ was of the form

$$\chi(T) = T^2 - \text{Tr}(\varphi_q)T + \deg(\varphi_q) = T^2 - tT + q = 0$$

and $\#E(\mathbb{F}_q) = \chi(1) = q + 1 - t$.
Factorisation of $\chi(T)$ over $p$-adic’s

- $\mathbb{Q}_p$ is field of $p$-adic numbers, with valuation ring $\mathbb{Z}_p$
- Assume that $t \not\equiv 0 \mod p$, then
  \[ \chi(T) \equiv T^2 - tT \equiv T(T - t) \mod p \]

- Conclusion: $\chi(T)$ splits over $\mathbb{Z}_p$ as
  \[ \chi(T) = (T - \lambda)(T - \frac{q}{\lambda}) \]
  with $\lambda$ the unique root such that $\lambda \equiv t \mod p$ ($\lambda$ is unit)

- Conclusion: $t = \lambda + \frac{q}{\lambda}$, since $|t| \leq 2\sqrt{q}$ only need approximation of $\lambda$ modulo $p^N$ with $N > n/2 + 2$
How to Compute $\lambda$?

- Since $\lambda \in \mathbb{Z}_p$, need to lift the situation to $p$-adic integers
- Given elliptic curve $E$ over $\mathbb{F}_q$, can we find $E$ over $\mathbb{Z}_q$ s.t.
- Reduction of $E$ modulo $p$ equals $E$
- $E$ comes with “lifted Frobenius endomorphism $\mathcal{F}_q$” with the same characteristic polynomial

$$\chi(\varphi_q; T) = \chi(\mathcal{F}_q; T)$$

- Assume that we could compute $E$ and $\mathcal{F}_q$, then how to proceed?
How to Compute $\lambda$?

- Let $E : f(x, y) = 0$ over field $\mathbb{K}$, then there exists an invariant differential

$$
\omega = \frac{dx}{\partial f/\partial y}
$$

- Morphism $\phi : E_1 \to E_2$ induces by pullback a map $\Omega_2 \to \Omega_1$

$$
\phi^*(gdh) = \phi^*(g)d\phi^*(h) = (g \circ \phi)d(h \circ \phi)
$$

- Invariant: since $\tau^*_P\omega = \omega$

- Linearization: $\phi, \psi$ 2 isogenies from $E_1 \to E_2$ then

$$
(\phi \oplus \psi)^*\omega = \phi^*\omega + \psi^*\omega
$$

- Pullback of regular differential by isogeny again regular, so

$$
\phi^*\omega = c\omega, \ c \in \mathbb{K}
$$
How to Compute $\lambda$?

- Since $F_q$ satisfies $T^2 - tT + q = 0$, the constant $F_q^*\omega = c\omega$ satisfies

  $$c^2 - tc + q = 0$$

- Conclusion: $c$ is either $\lambda$ or $q/\lambda$ but which one?

- Use that $F_q \equiv \varphi_q \mod p$ and clearly $\varphi_q^*\overline{\omega} \equiv 0 \mod p$, so

  $$c = \frac{q}{\lambda}$$

- Efficiency: would need extra $n$ precision to recover $\lambda$ and trace $t$

- Solution: consider the dual $\hat{F}_q$ of $F_q$, then $\hat{F}_q^*\omega = \lambda \omega$
Canonical Lift

- The canonical lift $E$ of an ordinary elliptic curve $E$ over $\mathbb{F}_q$ is an elliptic curve over $\mathbb{Q}_q$ which satisfies:
  - the reduction of $E$ modulo $p$ equals $E$,
  - the ring homomorphism $\text{End}(E) \to \text{End}(E)$ induced by reduction modulo $p$ is an isomorphism.
- Deuring showed that the canonical lift $E$ always exists and is unique up to isomorphism.
Canonical Lift: Alternative Characterisation

- \( \mathcal{E} \) is the canonical lift of \( E \).
- Reduction modulo \( p \) induces an isomorphism \( \text{End}(\mathcal{E}) \cong \text{End}(E) \).
- The \( q \)-th power Frobenius \( F_q \in \text{End}(E) \) lifts to an endomorphism \( \mathcal{F}_q \in \text{End}(\mathcal{E}) \).
- The \( p \)-th power Frobenius isogeny \( F_p : E \to E^\sigma \) lifts to an isogeny \( \mathcal{F}_p : \mathcal{E} \to \mathcal{E}^\Sigma \), with \( \Sigma \) the Frobenius substitution.

Conclusion: last property implies that the \( j \)-invariant of \( \mathcal{E} \) has to satisfy

\[
\Phi_p(j(\mathcal{E}), \Sigma(j(\mathcal{E}))) = 0
\]
Canonical Lift: Lubin-Serre-Tate

- Let $E$ be an ordinary elliptic curve over $\mathbb{F}_q$ with $j$-invariant $j(E) \in \mathbb{F}_q \setminus \mathbb{F}_{p^2}$.
- Then the system of equations

$$\Phi_p(X, \Sigma(X)) = 0 \text{ and } X \equiv j(E) \pmod{p},$$

has a unique solution $J \in \mathbb{Z}_q$, which is the $j$-invariant of the canonical lift $\mathcal{E}$ of $E$ (defined up to isomorphism).

- Example: $\Phi_2(X, Y) = X^3 + Y^3 - X^2 Y^2 + 1488(XY^2 + X^2 Y) - 162000(X^2 + Y^2) + 4077375XY + 8748000000(X + Y) - 157464000000000$

- When $j(E) \in \mathbb{F}_{p^2}$, then isomorphic to curve over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, so can use simple enumeration.
Canonical Lift: Satoh’s Algorithm

- To compute $j(E) \mod p^N$, Satoh considered $E$ together with all its conjugates $E_i = E^{\sigma^i}$ with $0 \leq i < n$.
- Let $F_{p,i}$ denote the $p$-th power Frobenius isogeny, then
  \[ E_0 \xrightarrow{F_{p,0}} E_1 \xrightarrow{F_{p,1}} \cdots \xrightarrow{F_{p,n-2}} E_{n-1} \xrightarrow{F_{p,n-1}} E_0. \]
- Satoh lifts cycle $(E_0, E_1, \ldots, E_{n-1})$ simultaneously
Canonical Lift: Weierstrass Model

\[
p = 2 \quad : \quad y^2 + xy = x^3 + a_6, \quad j(E) = 1/a_6
\]
\[
p = 3 \quad : \quad y^2 = x^3 + x^2 + a_6, \quad j(E) = -1/a_6
\]
\[
p > 5 \quad : \quad y^2 = x^3 + 3ax + 2a, \quad j(E) = 1728a/(1 + a)
\]

Given \( j \)-invariant \( j(\mathcal{E}) \) of the canonical lift of \( E \), a Weierstrass model for \( \mathcal{E} \) is given by

\[
p = 2 \quad : \quad y^2 + xy = x^3 + 36\alpha x + \alpha, \quad \alpha = 1/(1728 - j(\mathcal{E}))
\]
\[
p = 3 \quad : \quad y^2 = x^3 + x^2/4 + 36\alpha x + \alpha, \quad \alpha = 1/(1728 - j(\mathcal{E}))
\]
\[
p > 5 \quad : \quad y^2 = x^3 + 3\alpha x + 2\alpha, \quad \alpha = j(\mathcal{E})/(1728 - j(\mathcal{E}))
\]
How to compute $\lambda$?

- From before: the dual $\hat{F}_q$ of $F_q$, then $\hat{F}_q^* \omega = \lambda \omega$
- The diagram implies

$$\hat{F}_q = \hat{F}_{p,0} \circ \hat{F}_{p,1} \circ \cdots \circ \hat{F}_{p,n-1}$$

- Consider $\omega_i = \omega^{\sum i}$ for $0 \leq i < n$ and let $c_i$ be defined by

$$\hat{F}_{p,i}^*(\omega_i) = c_i \omega_{i+1},$$

- Conclusion: $\lambda = \prod_{0 \leq i < d} c_i$

- Commutative squares are conjugates, so $c_i = \Sigma^i(c_0)$ and

$$\lambda = \text{No}_{\mathbb{Q}_q/\mathbb{Q}_p}(c_0)$$
How to compute $c_0$?

- Know equations of $\mathcal{E}_0$ and $\mathcal{E}_1$, assume we know $\text{Ker}\hat{\mathcal{F}}_{p,0}$
- Vélu’s formulas: compute an equation of $\mathcal{E}_1/\text{Ker}(\hat{\mathcal{F}}_{p,0})$ and isogeny $\nu_0$
- Since $\text{Ker}(\nu_0) = \text{Ker}(\hat{\mathcal{F}}_{p,0})$, there exists an isomorphism $\lambda_0 : \mathcal{E}_1/\text{Ker}(\hat{\mathcal{F}}_{p,0}) \rightarrow \mathcal{E}_0$ that makes diagram commutative
How to compute $c_0$?

- Vélu’s construction: chooses holomorphic differential such that action of $\nu_0$ is trivial
- Conclusion: it is sufficient to compute the action of $\lambda_0$ on $\omega_0$
Computing $\text{Ker}(\hat{F}_{p,0})$?

- Note that $\text{Ker}(\hat{F}_{p,0})$ is a subgroup of order $p$ of $E_1[p]$.
- Let $H_0(x) = \prod_{P \in (\text{Ker}(\hat{F}_{p,0}) \setminus \{O\})}/(x - x(P))$
- $H_0(x)$ divides the $p$-division polynomial $\psi_{p,1}(x)$ of $E_1$
- Lemma: $H_0(x) \in \mathbb{Z}_q[x]$ is the unique monic polynomial that divides $\psi_{p,1}(x)$ and such that $H_0(x)$ is squarefree modulo $p$ of degree $(p - 1)/2$
- Need to modify Hensel since reduction mod $p$ of $H_0(x)$ not coprime with $\psi_{p,1}$
How to compute $c_0$?

- For $p > 3$, $\mathcal{E}_1$ has equation $y^2 = x^3 + a_1 x + b_1$
- Vélu: $\mathcal{E}_1/\text{Ker}(\widehat{F}_{p,0})$ has equation $y^2 = x^3 + \alpha_1 x + \beta_1$

\[
\alpha_1 = (6 - 5p)a_1 - 30(h_{0,1}^2 - 2h_{0,2})
\]
\[
\beta_1 = (15 - 14p)b_1 - 70(-h_{0,1}^3 + 3h_{0,1}h_{0,2} - 3h_{0,3}) + 42a_1 h_{0,1}
\]

where $h_{0,k}$ is coefficient of $x^{(p-1)/2-k}$ in $H_0(x)$

- $\lambda_0$ to $\mathcal{E}_0 : y^2 = x^3 + a_0 x + b_0$ is $\lambda_0 : (x, y) \rightarrow (u_0^2 x, u_0^3 y)$ with

\[
u_0^2 = \frac{\alpha_1}{\beta_1} \frac{b_0}{a_0}
\]

- Let $\omega_0 = dx/y$ then $\lambda_0^*(\omega_0) = u_0^{-1} \omega_{1,K}$ with $\omega_{1,K} = dx/y$

- Conclusion: $c_0 = u_0^{-1}$
Satoh’s Algorithm: Example

Let $p = 5$, $d = 7$, $\mathbb{F}_{p^d} \simeq \mathbb{F}_p(\theta)$ with $\theta^7 + 3\theta + 3 = 0$

Elliptic curve $E : y^2 = x^3 + x + a_6$

\[ a_6 = 4\theta^6 + 3\theta^5 + 3\theta^4 + 3\theta^3 + 3\theta^2 + 3. \]

The $j$-invariant of canonical lift with precision 6 then is

\[ J_0 \equiv 6949T^6 + 6806T^5 + 14297T^4 + 2260T^3 + 13542T^2 + 13130T + 15215, \]

with $\mathbb{Z}_q \simeq \mathbb{Z}_p[T]/(G(T))$ and $G(T) = T^7 + 3T + 3$.

Values for $a$, $b$ of $E : y^2 = x^3 + ax + b$

\[ a \equiv 6981T^6 + 8408T^5 + 1033T^4 + 8867T^3 + 15614T^2 + 3514T + 675 \]
\[ b \equiv 4654T^6 + 397T^5 + 5897T^4 + 703T^3 + 5201T^2 + 7551T + 450 \]
Satoh’s Algorithm: Example

- Polynomial $H$ describing the kernel of $\mathcal{F}_p$

\[ H(x) \equiv x^2 + (1395 T^6 + 7906 T^5 + 3737 T^4 + 9221 T^3 + 9207 T^2 + 5403 T + 7401)x \]
\[ + 6090 T^6 + 206 T^5 + 5259 T^4 + 7576 T^3 + 3863 T^2 + 8903 T + 7926 \]

- Recover $\alpha$ and $\beta$ as

\[ \alpha \equiv 11086 T^6 + 2618 T^5 + 6983 T^4 + 13192 T^3 + 15324 T^2 + 13544 T + 10550 \]
\[ \beta \equiv 4940 T^6 + 3060 T^5 + 14966 T^4 + 6589 T^3 + 7934 T^2 + 6060 T + 12470 \]

- Norm of $(\alpha b)/(\beta a)$ and taking the square root,

\[ \text{Tr}(\varphi q) = 433 \quad \text{and} \quad \left| E(\mathbb{F}_{p^d}) \right| = 77693 \]