Computing Zeta Functions of Curves over Finite Fields

Fré Vercauteren

Katholieke Universiteit Leuven

30 July 2008

The Zeta Function and Weil Conjectures

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

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

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

- $Z(T)$ is 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 $\overline{C}$ 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 φ_q on $C(\overline{\mathbb{F}}_q)$
  - endomorphism φ_q on $J_C(\overline{\mathbb{F}}_q)$
- $\mathbb{F}_q$-rational points are invariant under φ_q

$$J_C(\mathbb{F}_q) = \mathrm{Ker}(1 - \varphi_q) \qquad \# J_C(\mathbb{F}_q) = \deg(1 - \varphi_q)$$

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

Overview of Existing Approaches

- l-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 $\chi(T) \bmod \prod_i l_i$.
- p-adic:
  - canonical lift
  - p-adic cohomology
  - p-adic deformation

p-adic Numbers

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

$$r = p^\rho u/v, \quad \rho, u, v \in \mathbb{Z}, \quad p \not| \, u, \; p \not| \, v$$

- Non-archimedean 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 $O(N \log p)^{1+\varepsilon}$
- 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 $\mathbb{Z}_q$
- $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 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 $f_m(t) \equiv f(t) \bmod p^m$

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 $\Sigma(\theta) \equiv \theta^p \bmod p$.
- 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 θ 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

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

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 mod p^{n-k}
- $g(a)$ mod p^{2n}, then $g(a) \equiv 0 \bmod p^{n+k}$ and $g(a)/p^{n+k}$ known mod p^{n-k}
- Finally compute

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

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

Frobenius Endomorphism

- Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with $q = p^n$
- Recall the q-th power Frobenius endomorphism

$$\varphi_q : E \to E : (x, y) \mapsto (x^q, y^q)$$

- Characteristic polynomial of φ_q was of the form

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

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 $t \not\equiv 0 \bmod p$, then

$$\chi(T) \equiv T^2 - tT \equiv T(T - t) \bmod p$$

- Conclusion: $\chi(T)$ splits over $\mathbb{Z}_p$ as

$$\chi(T) = (T - \lambda)(T - \frac{q}{\lambda})$$

  with λ the unique root such that $\lambda \equiv t \bmod p$ (λ is unit)
- Conclusion: $t = \lambda + q/\lambda$, since $|t| \leq 2\sqrt{q}$ only need approximation of λ modulo p^N with $N > n/2 + 2$

How to Compute λ?

- 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 $\mathcal{E}$ over $\mathbb{Z}_q$ s.t.
- Reduction of $\mathcal{E}$ modulo p equals E
- $\mathcal{E}$ 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 $\mathcal{E}$ and $\mathcal{F}_q$, then how to proceed?

How to Compute λ?

- 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: ϕ, ψ 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 λ?

- Since $\mathcal{F}_q$ satisfies $T^2 - tT + q = 0$, the constant $\mathcal{F}_q^* \omega = c\omega$ satisfies
$$c^2 - tc + q = 0$$
- Conclusion: c is either λ or q/λ but which one?
- Use that $\mathcal{F}_q \equiv \varphi_q \bmod p$ and clearly $\varphi_q^* \overline{\omega} \equiv 0 \bmod p$, so
$$c = \frac{q}{\lambda}$$
- Efficiency: would need extra n precision to recover λ and trace t
- Solution: consider the dual $\widehat{\mathcal{F}}_q$ of $\mathcal{F}_q$, then $\widehat{\mathcal{F}}_q^* \omega = \lambda\omega$

Canonical Lift

- The canonical lift $\mathcal{E}$ of an ordinary elliptic curve E over $\mathbb{F}_q$ is an elliptic curve over $\mathbb{Q}_q$ which satisfies:
- the reduction of $\mathcal{E}$ modulo p equals E,
- the ring homomorphism $\mathrm{End}(\mathcal{E}) \to \mathrm{End}(E)$ induced by reduction modulo p is an isomorphism.
- Deuring showed that the canonical lift $\mathcal{E}$ 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 $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$.
- The q-th power Frobenius $F_q \in \mathrm{End}(E)$ lifts to an endomorphism $\mathcal{F}_q \in \mathrm{End}(\mathcal{E})$.
- 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 Σ the Frobenius substitution.

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

$$\Phi_p\big(j(\mathcal{E}), \Sigma\big(j(\mathcal{E})\big)\big) = 0$$

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

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

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: $\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488(XY^2 + X^2Y) - 162000(X^2 + Y^2) + 40773375XY + 8748000000(X + Y) - 157464000000000$
- 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 $j(\mathcal{E}) \bmod p^N$, 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

$$\begin{tikzcd}
\mathcal{E}_0 \arrow[r, "\mathcal{F}_{p,0}"] \arrow[d, "\pi_1"'] & \mathcal{E}_1 \arrow[r, "\mathcal{F}_{p,1}"] \arrow[d, "\pi_1"'] & \cdots \arrow[r, "\mathcal{F}_{p,n-2}"] & \mathcal{E}_{n-1} \arrow[r, "\mathcal{F}_{p,n-1}"] \arrow[d, "\pi_1"'] & \mathcal{E}_0 \arrow[d, "\pi_1"'] \\
E_0 \arrow[r, "F_{p,0}"] & E_1 \arrow[r, "F_{p,1}"] & \cdots \arrow[r, "F_{p,n-2}"] & E_{n-1} \arrow[r, "F_{p,n-1}"] & E_0,
\end{tikzcd}$$

Canonical Lift: Weierstrass Model

$$\begin{array}{lcll} p=2 & : & y^2+xy=x^3+a_6, & j(E)=1/a_6 \\ p=3 & : & y^2=x^3+x^2+a_6, & j(E)=-1/a_6 \\ p>5 & : & y^2=x^3+3ax+2a, & j(E)=1728a/(1+a) \end{array}$$

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

$$\begin{array}{lcll} p=2 & : & y^2+xy=x^3+36\alpha x+\alpha, & \alpha=1/\big(1728-j(\mathcal{E})\big) \\ p=3 & : & y^2=x^3+x^2/4+36\alpha x+\alpha, & \alpha=1/\big(1728-j(\mathcal{E})\big) \\ p>5 & : & y^2=x^3+3\alpha x+2\alpha, & \alpha=j(\mathcal{E})/\big(1728-j(\mathcal{E})\big) \end{array}$$

How to compute λ ?

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

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

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

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

- Conclusion: $\lambda = \prod_{0 \leq i < d} c_i$
- Commutative squares are conjugates, so $c_i = \Sigma^i(c_0)$ and

$$\lambda = \mathrm{No}_{\mathbb{Q}_q/\mathbb{Q}_p}(c_0)$$

How to compute c_0 ?

$$\begin{tikzcd} \mathcal{E}_1 \arrow[rr, "\widehat{\mathcal{F}}_{p,0}"] \arrow[dr, "\nu_0"'] & & \mathcal{E}_0 \\ & \mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0}) \arrow[ur, "\lambda_0"'] & \end{tikzcd}$$

- Know equations of $\mathcal{E}_0$ and $\mathcal{E}_1$, assume we know $\mathrm{Ker}\widehat{\mathcal{F}}_{p,0}$
- Vélu's formulas: compute an equation of $\mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$ and isogeny ν_0
- Since $\mathrm{Ker}(\nu_0) = \mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$, there exists an isomorphism $\lambda_0 : \mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0}) \to \mathcal{E}_0$ that makes diagram commutative

How to compute c_0 ?

$$\begin{tikzcd} \mathcal{E}_1 \arrow[rr, "\widehat{\mathcal{F}}_{p,0}"] \arrow[dr, "\nu_0"'] & & \mathcal{E}_0 \\ & \mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0}) \arrow[ur, "\lambda_0"'] & \end{tikzcd}$$

- Vélu's construction: choses holomorphic differential such that action of ν_0 is trivial
- Conclusion: it is sufficient to compute the action of λ_0 on ω_0

Computing $\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$?

- Note that $\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$ is a subgroup of order p of $\mathcal{E}_1[p]$.
- Let $H_0(x)$ be $H_0(x) = \prod_{P \in (\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0}) \setminus \{\mathcal{O}\})/\pm} (x - x(P))$
- $H_0(x)$ divides the p-division polynomial $\Psi_{p,1}(x)$ of $\mathcal{E}_1$
- 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 modifiy 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: $\mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$ 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 $H_0(x)$

- λ_0 to $\mathcal{E}_0 : y^2 = x^3 + a_0 x + b_0$ is $\lambda_0 : (x, y) \to (u_0^2 x, u_0^3 y)$ 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 $\mathcal{E} : y^2 = x^3 + ax + b$

$$\begin{aligned} a &\equiv 6981T^6 + 8408T^5 + 1033T^4 + 8867T^3 + 15614T^2 + 3514T + 675 \\ b &\equiv 4654T^6 + 397T^5 + 5897T^4 + 703T^3 + 5201T^2 + 7551T + 450 \end{aligned}$$

Satoh's Algorithm: Example

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

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

- Recover α and β as

$$\begin{aligned} \alpha &\equiv 11086T^6 + 2618T^5 + 6983T^4 + 13192T^3 + 15324T^2 + 13544T + 10550 \\ \beta &\equiv 4940T^6 + 3060T^5 + 14966T^4 + 6589T^3 + 7934T^2 + 6060T + 12470 \end{aligned}$$

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

$$\mathrm{Tr}(\varphi_q) = 433 \quad \text{and} \quad |E(\mathbb{F}_{p^d})| = 77693$$