p-adic cohomology and the computation of zeta functions

Kiran S. Kedlaya
University of California, Berkeley

Elliptic Curve Cryptography Workshop
September 24, 2002

See *Journal of the Ramanujan Mathematical Society* **16** (2001), 323–338 (or arxiv preprint math.AG/0105031).

Zeta functions and cryptography

For C an algebraic curve over a finite field $\mathbb{F}_q$, the $\mathbb{F}_q$-rational points of the Jacobian $J(C)$ form a group possibly useful for cryptography (e.g., for Diffie-Hellman exchange), but only if the order of the group is known.

The order is determined by the *zeta function* of C:

$$\zeta_C(t) = \frac{Q(t)}{(1-t)(1-qt)}$$

by the formula

$$\#J(\mathbb{F}_q) = Q(1).$$

Here P is a polynomial over $\mathbb{Z}$, which we want to compute.

More on the zeta function

In the formula

$$\zeta_C(t) = \frac{Q(t)}{(1-t)(1-qt)},$$

$Q(t)$ is monic over $\mathbb{Z}$ of degree $2g$ ($g =$ genus of C). Moreover, the roots of $Q(t)$ all have absolute value $\sqrt{q}$, and come in pairs: if α is a root, so is q/α. (This constrains the coefficients of $Q(t)$ to lie in some interval.)

If $\alpha_1, \dots, \alpha_{2g}$ are the roots of Q, then

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \alpha_1^n - \cdots - \alpha_{2g}^n.$$

Thus $Q(t)$ is determined by $\#C(\mathbb{F}_{q^n})$ for $n = 1, \dots, g$, or even by these counts modulo a suitably large integer N.

The situation in genus 1

For C an elliptic (genus 1) curve, the best general algorithm for computing $Q(t)$ is due to Schoof. (Roughly, compute $\#C(\mathbb{F}_q)$ modulo many small primes.)

In *small characteristic* ($q = p^n$ for p a small prime), methods of Satoh, Fouquet, Gaudry, Harley, Skjernaa, Mestre, etc., work better. (Roughly, compute $\#C(\mathbb{F}_q)$ modulo a large power of p.)

But all of these methods are specific to genus 1 (though some may be pushed to genus 2).

A general approach in small characteristic

Say $q = p^n$. Write $\mathbb{Q}_q$ for the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$ and $\mathbb{Z}_q$ for its ring of integers

A construction of Monsky and Washnitzer associates to C a $\mathbb{Q}_p$-vector space V (cohomology) and a linear transformation F (Frobenius) on V with characteristic polynomial $Q(t)$. If we can compute (approximately) the matrix of F on a basis of V, we can recover $Q(t)$.

In general, this should lead to a computation which is polynomial in p, n, g.

Example: hyperelliptic curves

We illustrate the construction for

$$C : y^2 = \overline{P}(x)$$

for $\overline{P}(x)$ a monic polynomial of degree $2g + 1$ over $\mathbb{F}_q$, where $q = p^n$ for p an *odd* prime. I.e., C is hyperelliptic of genus g with a rational Weierstrass point.

The Monsky-Washnitzer cohomology of C

Choose a monic polynomial $P(x)$ over $\mathbb{Z}_q$ congruent to $\overline{P}(x)$ modulo p. The ring R consists of power series

$$\sum_{i=0}^{\infty} \sum_{j=-\infty}^{\infty} a_{ij} x^i y^j$$

over $\mathbb{Z}_q$ such that $v_p(a_{ij})/(i + |j|)$ is eventually bounded away from 0 ("overconvergence"), modulo the relation $y^2 = P(x)$. (One can assume $a_{ij} = 0$ for $i > 2g$.)

This is the "weak completion" of the coordinate ring of the affine variety

$$S = \operatorname{Spec} \mathbb{Z}_q[x, y, y^{-1}]/(y^2 - P(x)).$$

(Note: $S/pS \cong R/pR$.)

Overconvergence in detail

The series

$$\sum_{i=0}^{\infty} x^{p^i}$$

is not p-adically convergent.

The series

$$\sum_{i=0}^{\infty} p^i x^{p^i}$$

is convergent, but not overconvergent.

The series

$$\sum_{i=0}^{\infty} p^i x^i$$

is overconvergent.

A basis in cohomology

The Monsky-Washnitzer cohomology space H is the set of differentials $r\,dx + s\,dy$ for $r, s \in R[\frac{1}{p}]$, modulo df and $f(2y\,dy - P'(x)\,dx)$ for any $f \in R[\frac{1}{p}]$.

This is a vector space over $\mathbb{Q}_q$, which we can split into plus and minus eigenspaces for the map $y \mapsto -y$ of R. The resulting spaces have bases

$$H_- : \quad \frac{x^i\,dx}{y} \quad (i = 0, \ldots, 2g-1)$$
$$H_+ : \quad \frac{x^i\,dx}{y^2} \quad (i = 0, \ldots, 2g).$$

We'll see why later.

Whither overconvergence?

Had we not imposed the overconvergence condition, then

$$\sum_{i=0}^{\infty} p^i x^{p^{2i}-1}\,dx$$

would not be zero in H, because its integral

$$\sum_{i=0}^{\infty} p^{-i} x^{p^{2i}}$$

does not converge. In fact, H would be infinite dimensional in this case.

A typical example in R is

$$\sum_{i=1}^{\infty} p^i x^{i-1}\,dx = d\left(\sum_{i=1}^{\infty} (p^i/i)x^i\right).$$

A trace formula

Let $F : R \to R$ be any map lifting the q-power Frobenius map $x \mapsto x^q$ modulo p and commuting with $y \mapsto -y$. Then F acts on differentials by pullback:

$$F(df) = d(F(f))$$

so induces a linear transformation on H_+ and H_-.

The Monsky-Washnitzer theory yields the following "Lefschetz trace formula":

$$\#X(\mathbb{F}_{q^r}) = q^r + 1 - \text{Trace}(F^r, H_-).$$

That is, the characteristic polynomial of F on H_- is $Q(t)$.

We'll construct an F as the n-th power of a map F_p lifting the p-power Frobenius $x \mapsto x^p$.

The trace formula in detail

Let Z be the set of Weierstrass points of C and $Y = C - Z$. Then Y is affine and $Y = \mathrm{Spec}(R/pR)$, so the MW construction yields

$$\begin{aligned}\#C(\mathbb{F}_{q^r}) - \#Z(\mathbb{F}_{q^r}) &= \#Y(\mathbb{F}_{q^r}) \\ &= q^r - \mathrm{Trace}(F^r, H).\end{aligned}$$

Let $\pi : C \to \mathbb{P}^1$ be the quotient by $y \mapsto -y$. Then $\mathbb{P}^1 - \pi(Z)$ is again affine, so

$$\begin{aligned}q^r + 1 - \#Z(\mathbb{F}_{q^r}) &= \#(\mathbb{P}^1 - \pi(Z))(\mathbb{F}_{q^r}) \\ &= q^r - \mathrm{Trace}(F^r, H_+).\end{aligned}$$

Subtracting these two yields

$$\#C(\mathbb{F}_{q^r}) = q^r + 1 - \mathrm{Trace}(F^r, H_-).$$

The Frobenius map

Recall that $\mathbb{Z}_q$ has a canonical map σ lifting the map $t \mapsto t^p$ modulo p. The "Frobenius" map $F_p : R \to R$ is given by

$$\begin{aligned} x &\mapsto x^p \\ y &\mapsto y^p(1 + pE)^{1/2} \\ &= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} p^i E^i, \end{aligned}$$

where $E = (P(x)^\sigma - P(x)^p)/(py^{2p})$. (The valuation of $\binom{1/2}{i}$ is $O(\log i)$, so this is overconvergent.) Extend F_p to H by sending $f\,dx$ to $f^\sigma\,d(x^p) = px^{p-1} f^\sigma\,dx$.

Warning: F_p is not linear on H, but rather σ-linear:

$$F_p(c\omega) = c^\sigma F_p(\omega).$$

In practice, compute $F_p(y)$ using a Newton iteration, not the power series.

What is the matrix?

We'd like to compute the matrix by which F_p, and by extension $F = F_p^n$, act on the basis $x^i\,dx/y$ $(i = 0, \ldots, 2g-1)$ of H_-.

To do this, we first apply F_p to each differential, then rewrite the result as an exact differential (which maps to 0 in H_-) plus a linear combination of basis elements.

So we need a procedure to "reduce" an arbitrary differential to a linear combination of basis elements, plus an exact differential.

Reduction of differentials, part 1

Given a differential $A(x)y^{-2s-1}\,dx$ with $\deg A \leq 2g$, write

$$A(x) = B(x)P(x) + C(x)P'(x)$$
$$\deg B \leq 2g-1, \qquad \deg C \leq 2g.$$

In H_-, we have the relation

$$\begin{aligned} 0 &\equiv d(C(x)y^{-2s+1}) \\ &\equiv C'(x)y^{-2s+1}\,dx + C(x)(-2s+1)y^{-2s}\,dy. \end{aligned}$$

Since $P'(x)\,dx = 2y\,dy$, we get

$$\frac{C(x)P'(x)\,dx}{y^{2s+1}} = \frac{2C(x)\,dy}{y^{2s}} \equiv \frac{2C'(x)\,dx}{(2s-1)y^{2s-1}}.$$

Thus

$$\frac{A(x)}{y^{2s+1}}\,dx \equiv \frac{(2s-1)B(x) + 2C'(x)}{(2s-1)y^{2s-1}}\,dx,$$

and we have reduced the exponent of y in the denominator.

Reduction of differentials, part 2

A similar argument allows one to eliminate large positive powers of y. Namely, given $A(x)y^{2s+1}\,dx$, first rewrite it as $A(x)P(x)^{s+1}\,dx/y$. Now use the relation

$$\begin{aligned} 0 &\equiv d(x^m y) \\ &\equiv m x^{m-1} y\,dx + x^m\,dy \\ &\equiv \frac{2m x^{m-1} P(x) + x^m P'(x)}{2y}\,dx \end{aligned}$$

to successively eliminate the highest powers of x. (The coefficient of x^{2g+m} in the numerator is $2m + (2g+1) \neq 0$.)

The algorithm (sketch, part 1)

Step 1: use Newton's iteration to compute $F_p(y^{-1})$ to "high accuracy".

Step 2: for $i = 0, \ldots, 2g-1$, compute an approximation of

$$\begin{aligned} F_p(x^i\,dx/y) &= F_p(y^{-1})F_p(x)^i F_p(dx) \\ &= F_p(y^{-1})x^{pi}px^{p-1}\,dx. \end{aligned}$$

and rewrite it as $\sum_i A_i(x)y^{2i+1}\,dx$ where each A_i has degree at most $2g$.

Step 3: take the finite sum $\sum_i A_i(x)y^{2i+1}\,dx$ and use the reduction procedures to obtain an equivalent differential of the form $A(x)\,dx/y$ with $\deg A \le 2g-1$.

The algorithm (sketch, part 2)

Step 4: let M be the matrix with M_{ij} equal to the coefficient of $x^i\,dx/y$ in the reduction of $F_p(x^j\,dx/y)$. Then the matrix by which $F = F_p^n$ acts on the basis $x^i\,dx/y$ of H_- is

$$M' = M M^{\sigma} \cdots M^{\sigma^{n-1}}.$$

Step 5: compute the characteristic polynomial of M' to high enough accuracy to determine $Q(t)$ and the α_i.

Precision

How accurate is accurate enough?

If $\deg A \leq 2g$ and A has coefficients in $\mathbb{Z}_q$, the reduction of $A(x)y^{2s+1}\,dx$ will have coefficients in $\mathbb{Z}_q$ if you multiply it by $p^{\log_p 2|s|+1}$.

So computing $O(gn)$ terms of

$$F_p(y^{-1}) = y^{-p} \sum_{i=0}^{\infty} \binom{-1/2}{i} p^i E^i$$

will give the needed $O(gn)$ places of precision in the final matrix. (And all constants are explicit.)

Asymptotics (for fixed p)

One must carry $O(gn)$ places of precision in all computations in order to get enough accuracy to uniquely determine the characteristic polynomial $Q(t)$. Moreover, each place of precision requires $O(n)$ bits, since we're working in $\mathbb{Z}_q$.

The limiting memory constraint is storing the approximation of $F(x^i\,dx/y)$. It consists of $O(gn)$ terms, each a polynomial of degree $2g$, each of whose coefficients requires $O(gn^2)$ bits to store. Thus it requires $O(g^3n^3)$ memory.

Asymptotics (for fixed p) continued

The limiting time constraint is reducing each of these $2g$ approximations. This requires eliminating $O(gn)$ powers of y; each such step requires $O(g^{1+\epsilon})$ operations on numbers of size $O(gn^2)$. This yields a total time of $O(g^{4+\epsilon}n^{3+\epsilon})$.

Generalizations and variations

The Monsky-Washnitzer theory applies to any smooth affine scheme; the main difficulties are:

- Computing a Frobenius lift;
- Finding an efficient reduction procedure for differentials.

Gaudry and Gurel treat the "superelliptic" case $y^n = f(x)$, where n is coprime to p. Denef and Vercauteren treat hyperelliptic curves in characteristic 2.

Related methods, based on work of Dwork, have been developed by Lauder and Wan.

The End