,

p-adic cohomology and zeta functions: the case of hyperelliptic curves

Kiran S. Kedlaya
University of California, Berkeley

Computational Aspects of Algebraic Curves, and Cryptography

University of Florida

March 3, 2003

These slides are available at
`math.berkeley.edu/~kedlaya`.

NEXT

Outline of the talk

1. Review of zeta functions

2. p-adic cohomology and zeta functions

3. The case of hyperelliptic curves

4. Computational issues

5. Where to go from here

NEXT

Zeta functions

zeta function of a variety $X/\mathbb{F}_q$:

$$\zeta_X(t) = \exp\left(\sum_{n=1}^{\infty} \frac{t^n}{n} \# X(\mathbb{F}_{q^n})\right).$$

By the Weil conjectures, this is a rational function of t with integer coefficients.

Zeta functions

zeta function of a variety $X/\mathbb{F}_q$:

$$\zeta_X(t) = \exp\left(\sum_{n=1}^{\infty} \frac{t^n}{n} \# X(\mathbb{F}_{q^n})\right).$$

By the Weil conjectures, this is a rational function of t with integer coefficients.

C: a smooth, projective, geometrically connected curve of genus g over $\mathbb{F}_q$. By Riemann-Roch,

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

where $Q(t) \in \mathbb{Z}[t]$, $\deg(Q) = 2g$.

Zeta functions

zeta function of a variety $X/\mathbb{F}_q$:

$$\zeta_X(t) = \exp\left(\sum_{n=1}^{\infty} \frac{t^n}{n} \# X(\mathbb{F}_{q^n})\right).$$

By the Weil conjectures, this is a rational function of t with integer coefficients.

C: a smooth, projective, geometrically connected curve of genus g over $\mathbb{F}_q$. By Riemann-Roch,

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

where $Q(t) \in \mathbb{Z}[t]$, $\deg(Q) = 2g$.

Relevance to cryptography: the order of the Jacobian group $J(C)(\mathbb{F}_q)$ is $Q(1)$.

NEXT

More on zeta functions

We have

$$Q(t) = (1 - t\alpha_1) \cdots (1 - t\alpha_{2g})$$

for some algebraic integers α_i with

$$\alpha_i \alpha_{i+g} = q, \qquad |\alpha_i| = \sqrt{q}.$$

Moreover,

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

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

NEXT

The situation in genus 1

For $g = 1$, the best general algorithm for computing $Q(t)$ is due to Schoof. (Roughly, compute $\#C(\mathbb{F}_q)$ modulo ℓ for enough small primes ℓ.)

The situation in genus 1

For $g = 1$, the best general algorithm for computing $Q(t)$ is due to Schoof. (Roughly, compute $\#C(\mathbb{F}_q)$ modulo ℓ for enough small primes ℓ.)

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.)

The situation in genus 1

For $g = 1$, the best general algorithm for computing $Q(t)$ is due to Schoof. (Roughly, compute $\#C(\mathbb{F}_q)$ modulo ℓ for enough small primes ℓ.)

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). We will focus on more general methods in the small characteristic case.

NEXT

Cohomology and zeta functions

There are various constructions in algebraic geometry that associate to C a vector space $H^1(C)$ over some field of characteristic zero and an endomorphism F of $H^1(C)$ such that

$$\#C(\mathbb{F}_{q^i}) = q^i + 1 - \mathrm{Tr}(F^i).$$

In this case, the characteristic polynomial of F is precisely $Q(t)$.

Cohomology and zeta functions

There are various constructions in algebraic geometry that associate to C a vector space $H^1(C)$ over some field of characteristic zero and an endomorphism F of $H^1(C)$ such that

$$\#C(\mathbb{F}_{q^i}) = q^i + 1 - \mathrm{Tr}(F^i).$$

In this case, the characteristic polynomial of F is precisely $Q(t)$.

In the case of small characteristic ($q = p^n$), using p-adic analysis one can construct such an $H^1(C)$ in a computationally effective manner. The resulting algorithms are polynomial in p, n, g.

NEXT

p-adic cohomology

$\mathbb{Q}_q$: the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$

p-adic cohomology

$\mathbb{Q}_q$: the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$

For any variety X over $\mathbb{F}_q$, Berthelot's rigid cohomology produces vector spaces $H^j_{\mathrm{rig}}(X)$ and $H^j_{c,\mathrm{rig}}(X)$ over $\mathbb{Q}_q$ (which coincide for X proper), and endomorphisms F such that

$$\#X(\mathbb{F}_{q^i}) = \sum_j (-1)^j \operatorname{Tr}(F^i, H^j_{c,\mathrm{rig}}(X)).$$

p-adic cohomology

$\mathbb{Q}_q$: the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$

For any variety X over $\mathbb{F}_q$, Berthelot's rigid cohomology produces vector spaces $H^j_{\mathrm{rig}}(X)$ and $H^j_{c,\mathrm{rig}}(X)$ over $\mathbb{Q}_q$ (which coincide for X proper), and endomorphisms F such that

$$\#X(\mathbb{F}_{q^i}) = \sum_j (-1)^j \operatorname{Tr}(F^i, H^j_{c,\mathrm{rig}}(X)).$$

Goal: make this fact computationally useful by working in a related theory for smooth affine varieties (Monsky-Washnitzer cohomology).

NEXT

Monsky-Washnitzer cohomology

Let W_n be the ring of power series in $x_1, \ldots, x_n$ over $\mathbb{Z}_q$ which converge for

$$|x_1|, \ldots, |x_n| \leq 1 + \epsilon$$

for some $\epsilon > 0$. That is,

$$\sum_I c_I x^I \in W_n \Leftrightarrow \liminf_{|I| \to \infty} \frac{v_p(c_I)}{|I|} > 0.$$

Monsky-Washnitzer cohomology

Let W_n be the ring of power series in $x_1, \dots, x_n$ over $\mathbb{Z}_q$ which converge for

$$|x_1|, \dots, |x_n| \leq 1 + \epsilon$$

for some $\epsilon > 0$. That is,

$$\sum_I c_I x^I \in W_n \Leftrightarrow \liminf_{|I| \to \infty} \frac{v_p(c_I)}{|I|} > 0.$$

Given a smooth affine variety

$$X = \operatorname{Spec} \overline{A} \qquad \text{over } \mathbb{F}_q,$$

choose a saturated ideal $\mathfrak{a}$ of some W_n such that $(W_n/\mathfrak{a}) \otimes_{\mathbb{Z}_q} \mathbb{F}_q \cong \overline{A}$. Put $A = W_n/\mathfrak{a}$. Then $H^i_{MW}(X)$ is the de Rham cohomology of $A[\frac{1}{p}]$, and F is induced by any ring map $A \to A$ reducing to q-powering mod p.

NEXT

Hyperelliptic curves in odd characteristic

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.

Hyperelliptic curves in odd characteristic

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.

We work with the affine subvariety C' obtained from C by removing the Weierstrass points; its coordinate ring is

$$\overline{A} = \mathbb{F}_q[x, y, z]/(y^2 - P(x), yz - 1).$$

NEXT

The MW ring of C'

Choose a monic polynomial $P(x)$ over $\mathbb{Z}_q$ congruent to $\overline{P}(x)$ modulo p. Then the ring A 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, modulo the relation $y^2 = P(x)$. (One can assume $a_{ij} = 0$ for $i > 2g$.)

NEXT

The MW cohomology of C'

Ω^1: module over $A[\frac{1}{p}]$ generated by dx and dy, modulo relation $2y\,dy = P'(x)\,dx$

The MW cohomology of C'

Ω^1: module over $A[\frac{1}{p}]$ generated by dx and dy, modulo relation $2y\,dy = P'(x)\,dx$

$H^1_{MW}(A)$: quotient of Ω^1 by $\mathbb{Q}_q$-span of elements $f_x\,dx + f_y\,dy$ for $f \in A[\frac{1}{p}]$

The MW cohomology of C'

Ω^1: module over $A[\frac{1}{p}]$ generated by dx and dy, modulo relation $2y\,dy = P'(x)\,dx$

$H^1_{MW}(A)$: quotient of Ω^1 by $\mathbb{Q}_q$-span of elements $f_x\,dx + f_y\,dy$ for $f \in A[\frac{1}{p}]$

H_+, H_-: eigenspaces of $H^1_{MW}(A)$ of eigenvalue $+1$ and -1 under $y \mapsto -y$.

The MW cohomology of C'

Ω^1: module over $A[\frac{1}{p}]$ generated by dx and dy, modulo relation $2y\,dy = P'(x)\,dx$

$H^1_{MW}(A)$: quotient of Ω^1 by $\mathbb{Q}_q$-span of elements $f_x\,dx + f_y\,dy$ for $f \in A[\frac{1}{p}]$

H_+, H_-: eigenspaces of $H^1_{MW}(A)$ of eigenvalue $+1$ and -1 under $y \mapsto -y$.

Then

$$H_- \cong H^1_{\mathrm{rig}}(C)$$
$$H_+ \cong H^1_{\mathrm{rig}}(\mathbb{P}^1 - \{\text{branch points}\})$$

so we need only compute on H_-.

NEXT

A basis for H_-

H_- is spanned over $\mathbb{Q}_q$ by

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

A basis for H_-

H_- is spanned over $\mathbb{Q}_q$ by

$$\frac{x^i\,dx}{y} \qquad (i = 0, \dots, 2g-1).$$

To put elements in this form, use the relations

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

and

$$0 \equiv \frac{2mx^{m-1}P(x) + x^m P'(x)}{2y}\,dx$$

derived on the next two slides.

NEXT

More on the relations (part 1)

Given $A(x)$ with $\deg A \leq 2g$, write

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

More on the relations (part 1)

Given $A(x)$ with $\deg A \le 2g$, write

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

In H_-, we have the relation

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

More on the relations (part 1)

Given $A(x)$ with deg $A \le 2g$, write

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

In H_-, we have the relation

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

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

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

More on the relations (part 1)

Given $A(x)$ 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

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

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

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

Thus we have as promised

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

NEXT

Source of the relations (part 2)

Given $A(x)y^{2s+1}\,dx$, first rewrite it as

$$A(x)P(x)^{s+1}\,dx/y.$$

We 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 $2m + (2g+1) \neq 0$.)

NEXT

A Frobenius map

Recall that $\mathbb{Z}_q$ has a canonical map σ lifting the map $t \mapsto t^p$ modulo p.

Define a σ-linear ring map $F_p : A \to A$ by

$$x \mapsto x^p$$

$$y \mapsto y^p \left(\frac{P(x)^\sigma}{P(x)^p} \right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} p^i \left(\frac{P(x)^\sigma - P(x)^p}{pP(x)^p} \right)^i .$$

Then $F_q = (F_p)^n$ is $\mathbb{Z}_q$-linear, and

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

NEXT

The recipe for computing ζ_C (part 1)

We now have a recipe for computing ζ_C:

1. Determine the degree of p-adic accuracy to which the following computations should be performed.

The recipe for computing ζ_C (part 1)

We now have a recipe for computing ζ_C:

1. Determine the degree of p-adic accuracy to which the following computations should be performed.

2. Use a Newton iteration to compute an approximation to $F_p(y)$ (truncating high powers of y).

The recipe for computing ζ_C (part 1)

We now have a recipe for computing ζ_C:

1. Determine the degree of p-adic accuracy to which the following computations should be performed.

2. Use a Newton iteration to compute an approximation to $F_p(y)$ (truncating high powers of y).

3. Apply F_p to $x^i\,dx/y$ for $i = 0, \ldots, 2g-1$ in succession (again truncating) and rewrite the result in terms of $x^i\,dx/y$ using the relations in H_-.

NEXT

The recipe for computing ζ_C (part 2)

4. Form the matrix M over $\mathbb{Q}_q$ with

$$F_p\left(\frac{x^j\,dx}{y}\right) \equiv \sum_{i=0}^{2g-1} M_{ij}\frac{x^i\,dx}{y}$$

   and compute $N = M^{\sigma^{n-1}} \cdots M^{\sigma} M$. Then N is the matrix through which $F_q = F_p^n$ acts on the $x^i\,dx/y$.

The recipe for computing ζ_C (part 2)

4. Form the matrix M over $\mathbb{Q}_q$ with

$$F_p\left(\frac{x^j\,dx}{y}\right) \equiv \sum_{i=0}^{2g-1} M_{ij}\frac{x^i\,dx}{y}$$

   and compute $N = M^{\sigma^{n-1}} \cdots M^{\sigma} M$. Then N is the matrix through which $F_q = F_p^n$ acts on the $x^i\,dx/y$.

5. Compute the characteristic polynomial of N modulo a high power of p, and replace each coefficient with its smallest integer approximation. The result is the numerator $Q(t)$ of the zeta function $\zeta_C(t)$.

NEXT

Estimating precision

The most mysterious part of analyzing the p-adic precision requirement is what happens when one reduces differentials.

Estimating precision

The most mysterious part of analyzing the p-adic precision requirement is what happens when one reduces differentials.

Fact: when reducing $\omega = B(x)\,dx/y^{2s+1}$ for $\deg B \leq 2g-1$ with integral coefficients, the final answer only involves denominators of valuation $\leq \log_p |2s+1|$.

Estimating precision

The most mysterious part of analyzing the p-adic precision requirement is what happens when one reduces differentials.

Fact: when reducing $\omega = B(x)\,dx/y^{2s+1}$ for $\deg B \leq 2g-1$ with integral coefficients, the final answer only involves denominators of valuation $\leq \log_p |2s+1|$.

Idea of proof: the difference between ω and its reduction can be found by integrating the polar parts at the zeroes of P.

Estimating precision

The most mysterious part of analyzing the p-adic precision requirement is what happens when one reduces differentials.

Fact: when reducing $\omega = B(x)\,dx/y^{2s+1}$ for $\deg B \leq 2g-1$ with integral coefficients, the final answer only involves denominators of valuation $\leq \log_p |2s+1|$.

Idea of proof: the difference between ω and its reduction can be found by integrating the polar parts at the zeroes of P.

Upshot: one can perform the reduction in fixed precision, filling in undetermined high-order digits arbitrarily. These garbage digits will cancel themselves out in the end.

NEXT

Hyperelliptic curves in characteristic 2

Denef and Vercauteren extend this recipe to $p = 2$. They take the hyperelliptic to be

$$C : y^2 + \overline{h}(x) = \overline{f}(x)$$

with $\deg(\overline{f}) = 2g + 1$, $\deg(\overline{h}) = g$, and each root of $\overline{h}$ also a root of $\overline{f}$.

Hyperelliptic curves in characteristic 2

Denef and Vercauteren extend this recipe to $p = 2$. They take the hyperelliptic to be

$$C : y^2 + \overline{h}(x) = \overline{f}(x)$$

with $\deg(\overline{f}) = 2g + 1$, $\deg(\overline{h}) = g$, and each root of $\overline{h}$ also a root of $\overline{f}$.

In this case, one works with the affine curve

$$C' = C - \{\text{branch points of } x : C \to \mathbb{P}^1\},$$

lifts $\overline{f}$ and $\overline{h}$ to polynomials f and h of the same degree, and forms the MW algebra of overconvergent series

$$\sum_{i,j,k} c_{i,j,k} x^i y^j h(x)^k$$

modulo $y^2 + h(x)y = f(x)$.

NEXT

Complexity analysis

For $p \neq 2$ fixed, the algorithm requires $\mathcal{O}(g^4 n^3)$ time and $\mathcal{O}(g^3 n^3)$ memory when performed using asymptotically fast arithmetic. (Optimal methods for $g = 1$ require $\mathcal{O}(n^2)$ time and memory.) For $p = 2$, the runtime is currently $\mathcal{O}(g^5 n^3)$.

Frederik Vercauteren has computed some examples, e.g., of a genus 2 curve over $\mathbb{F}_{3^{48}}$ (in Magma), of a genus 2 curve over $\mathbb{F}_{2^{160}}$, and of a genus 350 curve over $\mathbb{F}_2$ (both in C).

NEXT

Generalizations and variations (part 1)

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;

and to a lesser extent analyzing the precision requirements.

NEXT

Generalizations and variations (part 2)

Gaudry and Gurel consider "superelliptic" curves

$$y^r = P(x) \qquad (p \nmid r);$$

Vercauteren is studying $C_{a,b}$ curves (which admit a map to $\mathbb{P}^1$ totally ramified at some place).

One can also think about higher dimensional varieties; e.g., see Gerkmann's talk.

Related methods have been developed by Lauder and Wan. In particular, Lauder's "deformation theory" method seems well-suited to higher dimensional varieties.

NEXT

References

K.S.Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *J. Ramanujan Math. Soc.* **16** (2001), 323–338.

J. Denef and F. Vercauteren, An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2, preprint available at

```
www.wis.kuleuven.ac.be/
    algebra/denef_papers/
```

M. van der Put, The cohomology of Monsky and Washnitzer, in Introductions aux cohomologies p-adiques (Luminy, 1984), *Mém. Soc. Math. France (N.S.)* **23** (1986), 33–59.

END