Computing zeta functions of hyperelliptic curves

Kiran S. Kedlaya

MIT, Department of Mathematics

Counting Points on Varieties
Lorentz Center, Leiden
Thursday, April 23, 2009

These slides are available at

`http://math.mit.edu/~kedlaya/papers/talks.shtml`

Financial support: NSF CAREER grant DMS-0545904, MIT NEC Research Support Fund, MIT Cecil and Ida Green Fund.

Contents

Contents

The zeta function problem

Throughout, p is a prime and $q = p^n$.

Definition

The *zeta function* of a variety X over $\mathbb{F}_q$ is the series

$$\zeta_X(T) = \prod_{x \in X \text{ closed}} (1 - T^{[\kappa(x):\mathbb{F}_q]})^{-1} = \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right),$$

which represents a rational function (Dwork, Grothendieck-Artin).

For X smooth proper of dimension d, for any Weil cohomology H^i,

$$\zeta_X(T) = \frac{P_1(T) \cdots P_{2d-1}(T)}{P_0(T) \cdots P_{2d}(T)}$$

for $P_i(T) = \det(1 - T\,\mathrm{Frob}_q, H^i(X))$. Also, $P_i(T) \in 1 + T\mathbb{Z}[T]$, and the $\mathbb{C}$-roots of $P_i(T)$ have norm $q^{-i/2}$ (Deligne).

The zeta function problem

Problem

Given a family of varieties (of fixed dimension!!), describe an efficient algorithm that, given an explicit variety X in the family, computes $\zeta_X(T)$.

In this talk, I'll only consider X to be a *hyperelliptic curve* of genus g over $\mathbb{F}_q$; for $p > 2$, X always has an affine model

$$y^2 = P(x), \qquad \deg(P) \in \{2g+1, 2g+2\}.$$

Besides being the simplest family that includes all genera, these have some interest in cryptography. (Standard target: $q^g \sim 2^{160}$.)

Problem (Open unless you allow quantum computing)

*Describe an algorithm to, given a hyperelliptic curve X of genus g over $\mathbb{F}_q$, compute $\zeta_X(T)$ in time polynomial in **all three** of $(\log p), n, g$.*

Plan for the talk

For X a curve of genus g over $\mathbb{F}_q$,

$$\zeta_X(T) = \frac{P_1(T)}{(1-T)(1-qT)}$$

where $P_1(T) \in 1 + T\mathbb{Z}[T]$, $\deg(P_1(T)) = 2g$, $P_1(T)$ has $\mathbb{C}$-roots of norm $q^{-1/2}$, and $P_1(T)$ is symmetric:

$$P_1(q/T) = T^{-2g} q^{-g} P_1(T).$$

I'll survey a number of techniques for computing $P_1(T)$. I'll distinguish polynomial/exponential time, but instead of finer asymptotics, I'll usually quote some sample/record CPU timings to *one* significant digit.

"sp" denotes a situation which is not entirely generic. E.g., the base field is $\mathbb{F}_p$ for p a Mersenne prime, or a field admitting an optimal normal basis.

Contents

Enumeration of points

For X given by $y^2 = P(x)$ with P having no repeated roots, compute

$$\#X(\mathbb{F}_{q^i}) = \sum_{x \in \mathbb{P}^1_{\mathbb{F}_{q^i}}} \#\{P \in X(\mathbb{F}_{q^i}) : x(P) = x\}$$

for $i = 1, \ldots, g$. Then recover $P_1(T)$ using symmetry.

Linear in q^g, so only sensible when q^g is very small.

Baby step-giant step

Shanks's algorithm for computing class groups of number fields is a *generic group algorithm*, so it can be applied to the class group of a function field, i.e., the group $J(\mathbb{F}_q)$ for J the Jacobian abelian variety. This helps because

$$\#J(\mathbb{F}_q) = P_1(1).$$

Improvements by Sutherland (generic), Matsuo-Chao-Tsujii (for curves).

Sample (K-Sutherland, 2009; 5s)

$g = 2, p = q \sim 2^{32}$.

This is likely the best way to compute 2^{32} coefficients of the L-series of a genus 2 curve over $\mathbb{Q}$. Useless *by itself* for $g \geq 3$, but combines with ℓ-adic and p-adic algorithms.

Sutherland's swindle

Assume $g = 2$ for concreteness.

Suppose you only want $P_1(T)$ for *some* hyperelliptic curve of a given genus. Easy: find one with $\#J(\mathbb{F}_q)$ *smooth*.

Now say you want $\#J(\mathbb{F}_q)$ nearly prime. Look for a curve X whose quadratic twist $\tilde{X}$ has Jacobian $\tilde{J}$ with $\#\tilde{J}(\mathbb{F}_q)$ smooth. This helps because

$$\#\tilde{J}(\mathbb{F}_q) = P_1(-1).$$

Record (Sutherland, 2007; 34h to find one example)

$g = 2, p = q \sim 2^{84}$.

Contents

Schoof's algorithm (genus 1)

For $\ell \leq 2\log q$ distinct from p, compute $\#X(\mathbb{F}_q) \pmod{\ell}$ by computing the action of Frobenius on the group

$$X(\overline{\mathbb{F}_q})[\ell] \cong \mathbb{F}_\ell^2$$

using division polynomials. This determines $\#X(\mathbb{F}_q)$ (and hence $P_1(T)$) in polynomial time in $\log q = n\log p$. Improvements by Elkies, Atkin; also Couveignes, Gaudry, Lercier, Mihăilescu, Morain, Schost, et al.

Record (Enge-Morain, 2006; 400d)

$g = 1, p = q \sim 2^{8300}$.

Schoof's algorithm (higher genus)

Pila noticed that for any *fixed* g, one can compute $P_1(T) \pmod{\ell}$ by forming a projective embedding of the Jacobian (ouch) and computing division polynomials. For g fixed, this computes $P_1(T)$ in time polynomial in $\log q$, but dependence on g is (at least) exponential.

This has only been attempted for $g = 2$. Improvements by Gaudry-Harley, Bernstein-Pitcher.

Record (Gaudry-Schost, 2008; 30d)

$g = 2, p = q \sim 2^{127}$. *(Sutherland's swindle is not competitive in this range.)*

Contents

General warning

Most *p*-adic algorithms have at least linear dependence on p, so are not practical unless p is relatively small.

In some cases, *square root* dependence on p is possible. This should allow $p \leq 2^{64}$.

Canonical lifts

Let X be an *ordinary* elliptic curve over $\mathbb{F}_q$. Then X has a unique lift to $\mathbb{Z}_q$ (the unramified extension of $\mathbb{Z}_p$ with residue field $\mathbb{F}_q$) preserving the endomorphism ring (Deuring; Serre-Tate).

Satoh (for $p \geq 5$; extended to $p = 3$ by Fouquet-Gaudry-Harley, $p = 2$ by Skjernaa) computes this lift using a Newton iteration involving the p-modular polynomial. Improvements by these authors, Taguchi, et al.

Record (Harley, 2002; 60h)

$g = 1, q = 2^{50021}$; $g = 1, q = 2^{130020}$ *(sp)*.

One can also handle genus 2, at least for $p = 2$ (using Richelot isogenies). For $g \geq 3$, the Jacobian lifts canonically *as a principally polarized abelian variety*, but not necessarily to a Jacobian.

AGM iteration

Mestre realized that for $p = 2$, the Newton iteration for canonical lifting induces the AGM (arithmetic-geometric mean) iteration on theta characteristics.

Record (Lercier-Lubicz, 2002; 80h)

$g = 1$, $q = 2^{100002}$ *(sp)*.

This generalizes to $g > 1$ but is exponential in g. However...

Record (Lercier-Lubicz, 2002; 30h)

$g = 2$, $q = 2^{16420}$.

Contents

A general fact

Using Dwork's proof of rationality of $\zeta_X(T)$, Lauder and Wan gave an algorithm which is polynomial time in p, n, g, and which generalizes vastly. Unfortunately, this is not practical.

Monsky-Washnitzer cohomology

Monsky and Washnitzer constructed an explicit p-adic Weil cohomology for *smooth affine* varieties, which can be described using algebraic de Rham cohomology (of a *noncanonical* lift of the curve).

Using this, Kedlaya (for $p \geq 3$; extended to $p = 2$ by Denef-Vercauteren) computed the Frobenius action for hyperelliptic curves.

Sample (Magma (Harrison), 2009; 60m)

$g = 2$, $q = 3^{200}$.

Sample (Magma (Harrison), 2009; 60m)

$g = 50$, $p = q = 3$.

MW cohomology in medium characteristic

The previous method is at best linear in p. Boston-Gaudry-Schost found an algorithm for computing $P_1(T) \pmod p$ with *square root* dependence on p. Key idea: a "baby step-giant step" algorithm of Chudnovsky-Chudnovsky for solving linear recurrences with polynomial coefficients.

Harvey adapted this to compute MW cohomology with square root dependence on p. For $g = 2$, this beats K-Sutherland for $p \geq 2^{32}$.

Record (Harvey, 2008; 20h)

$g = 3, p = q \sim 2^{53}$.

Record (Harvey, 2008; 40h)

$g = 4, p = q \sim 2^{44}$.

Frobenius actions on connections

Lauder suggested using deformations in *p*-adic cohomology, i.e., Picard-Fuchs equations (Gauss-Manin connections). Idea: make a pencil in which one member is "easy" and another is the desired curve. Using the easy member as an initial condition in a differential equation, compute a Frobenius action on the connection, then specialize.

Improvements by Gerkmann, Hubrechts, et al.

Sample (Magma (Hubrechts), 2009; 30m)

$g = 2$, $q = 3^{200}$.

This method should also improve on MW cohomology for g large, but this requires a different implementation. (Hubrechts takes the easy curve over $\mathbb{F}_p$ and uses MW cohomology; instead, should take a very symmetric curve for which the initial condition can be computed *exactly*.)

Contents

Other curves

Computing Frobenius on MW cohomology can be extended to superelliptic curves (Gaudry-Gürel), $C_{a,b}$-curves (Denef-Vercauteren), nondegenerate curves (Castryck-Denef-Vercauteren, but unimplemented).

Record (Denef-Vercauteren, 2004; 8h)

$g = 3$ *(a* $C_{3,4}$*-curve),* $q = 2^{96}$.

Record (Denef-Vercauteren, 2004; 12h)

$g = 4$ *(a* $C_{3,5}$*-curve),* $q = 2^{72}$.

Using connections should be applicable even more generally. Lauder: given any fixed curve X over $\mathbb{Z}[1/N]$, the zeta function of $X_{\mathbb{F}_p}$ can be computed in time $O(p^{2+\epsilon})$. (Is $O(p^{1/2+\epsilon})$ possible?)

Higher dimension

Except for some 2-dimensional motives (Edixhoven et al.), no known way to extend ℓ-adic methods.

p-adic methods may help. MW cohomology extends with some difficulty.

Record (Abbott-K-Roe, 2005; 30h)

Quartic K3 surface, $p = q = 19$.

Connections should be better. Some experiments by Kloosterman (surfaces), K (threefolds).

Also possible: fibering in curves (Lauder). Applied to experiments on average rank of elliptic curves over function fields.

The end