Counting points on genus 2 curves over finite fields

P. Gaudry

Joint work with R. Harley, É. Schost

Durham, July 28, 2000.

Overview

- Introduction
- Definitions, notations
- Schoof algorithm in genus 2
- Practical results, limitations
- Modular polynomials in genus 2
- Towards an Atkin's algorithm for genus 2

Introduction

Goal: Compute cardinality of curves or Jacobians over finite fields.

Elliptic curves: Schoof (1985), first polynomial-time algorithm. Improvements by Elkies, Atkin, Couveignes, Lercier, Morain, Müller, Dewaghe... Solved! (see however recent work by Satoh.)

Theoretical algorithms for higher genus:

- Pila (1990), polynomial-time algorithm for general abelian varieties
- Kampkötter (1991), specific to hyperelliptic curves
- Huang–Ierardi (1998), Jacobian of general curves

In practice: exponential algorithms, Shanks, Pollard. Combined with *approximations* for $g \geq 3$: Stein–Teske (1999).

Definitions, notations

We consider:

- $\mathcal{C}$: curve of genus 2 of equation $y^2 = f(x)$, with $\deg f = 5$, sqrfree, monic.
- $\mathbb{F}_q$: finite field, $q = p^n$ elements, $p \neq 2$.

Its Jacobian is $\mathrm{Jac}(\mathcal{C}) = \mathrm{Div}^0(\mathcal{C})/\mathrm{Pr}(\mathcal{C})$.

Mumford representation: each class represented by

$$D = \langle u(x), v(x) \rangle, \quad \text{with } \; u \,|\, v^2 - f \quad \text{and } \; \deg v < \deg u \leq 2$$

If $D = \sum P_i - r\infty$, with $P_i = (x_i, y_i)$, then $u(x) = \prod(x - x_i)$ and $v(x_i) = y_i$.

Rem: D is defined over $\mathbb{F}_q$ iff $u(x)$ and $v(x)$ are.

Group law: Computed by Cantor's algorithm.

Frobenius endomorphism

Denote by π the Frobenius endomorphism on $\mathrm{Jac}(\mathcal{C})/\overline{\mathbb{F}}_q$.

Thm:(Weil) As an element of $\mathrm{End}(\mathrm{Jac}(\mathcal{C}))$, it has an integer characteristic polynomial of the form

$$\chi(t) = t^4 - s_1 t^3 + s_2 t^2 - q s_1 t + q^2,$$

with all the roots having absolute value $\sqrt{q}$.

Csq: bounds $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 6q$.

Fact: we have $\#\mathrm{Jac}(\mathcal{C}) = \chi(1) = q^2 + 1 - s_1(q+1) + s_2$.

$\Rightarrow$ we can use Shanks' method or a square root algorithm based on the Birthday paradox.

Our goal: compute s_1 and s_2 (equivalent to compute $\chi(1)$) by a Schoof-like method.

Schoof's algorithm in genus 2

General idea: Find $\chi(t) \bmod \ell$ for sufficiently many primes ℓ and reconstruct by CRT.

Thm: If $(\ell, p) = 1$, then

$$\mathrm{Jac}(\mathcal{C})[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^4 \cong \mathbb{F}_\ell\text{-vector space of dim 4}$$

and π restricted to $\mathrm{Jac}[\ell]$ has char. pol. $\chi(t) \bmod \ell$.

Strategy:

- "Compute" $\mathrm{Jac}[\ell]$,
- Find the action of π on it,
- Deduce $\chi(t) \bmod \ell$.

ℓ-division ideal

Elliptic case: $E[\ell]$ is characterized by the division polynomial ψ_ℓ:

$$P = (x, y) \in E[\ell] \Leftrightarrow \psi_\ell(x) = 0.$$

Genus 2: Multivariate analogue:

$$D = \langle x^2 + u_1 x + u_0, v_1 x + v_0 \rangle \in \mathrm{Jac}[\ell] \Leftrightarrow f(u_0, u_1, v_0, v_1) = 0, \ \forall f \in I_\ell,$$

where I_ℓ is called the ℓ-division ideal.

Def: I_ℓ is the ideal of the variety of the ℓ-torsion divisors not in Θ, i.e. not of the form $\langle x - x_P, y_P \rangle$.

Rem: I_ℓ is a radical, 0-dimensional ideal in 4 variables.

Kampkötter's method

Lem: For $\ell \neq 2$, $\mathrm{Jac}[\ell] \setminus \Theta$ contains a $\mathbb{F}_\ell$-basis of $\mathrm{Jac}[\ell]$.

$\Longrightarrow$ The ideal I_ℓ is enough to find $\chi(t) \bmod \ell$.

Kampkötter found recurrence formulae for computing polynomials generating I_ℓ.

Let $D = \langle x^2 + U_1 x + U_0, V_1 x + V_0 \rangle$ defined over the quotient algebra $A = \mathbb{F}_q[U_0, U_1, V_0, V_1]/I_\ell$.

- One can compute +,-,*,/ in A: first compute a Gröbner basis of I_ℓ and deal with polynomials reduced modulo this basis.
- One can compute π in A, by raising to the power q.

$\Longrightarrow$ Deduce minimal polynomial of π and then its char. pol. $\chi(t) \bmod \ell$.

Problem: Slow, due to multivariate ideal manipulations.

Cantor's division polynomials

Let (x_P, y_P) be a point on $\mathcal{C}$ and consider $P = \langle x - x_P, y_P \rangle \in \mathrm{Jac}(\mathcal{C})$, then

$$[\ell]P = \left\langle x^2 + \frac{d_1(x_P)}{d_0(x_P)} x + \frac{d_2(x_P)}{d_0(x_P)},\ y_P \left(\frac{e_1(x_P)}{e_0(x_P)} x + \frac{e_2(x_P)}{e_0(x_P)} \right) \right\rangle ,$$

where $d_0, d_1, d_2, e_0, e_1, e_2$ polynomials, degree $O(\ell^2)$, computed by rec. formulae.

Change of variables: represent $D = \langle x^2 + u_1 x + u_0, v_1 x + v_0 \rangle$ by $D = P_1 + P_2$ with $P_1 = \langle x - x_1, y_1 \rangle$ and $P_2 = \langle x - x_2, y_2 \rangle$.

$[\ell]D = 0 \Leftrightarrow [\ell]P_1 = -[\ell]P_2 \Leftrightarrow$ system of polynomial equations

$$\begin{cases} E_1(x_1, x_2) & = & d_1(x_1)d_2(x_2) - d_1(x_2)d_2(x_1) & = & 0, \\ E_2(x_1, x_2) & = & d_0(x_1)d_2(x_2) - d_0(x_2)d_2(x_1) & = & 0, \\ F_1(x_1, x_2, y_1, y_2) & = & y_1 e_1(x_1)e_0(x_2) + y_2 e_1(x_2)e_0(x_1) & = & 0, \\ F_2(x_1, x_2, y_1, y_2) & = & y_1 e_2(x_1)e_0(x_2) + y_2 e_2(x_2)e_0(x_1) & = & 0, \end{cases}$$

Advantage: Two eq. involve only x_1 and x_2

$\Longrightarrow$ Eliminate x_2 by a resultant computation and get $R(x_1) = 0$ of degree $O(\ell^4)$.

Rem: Computed by evaluation / interpolation, without expanding the formulae: requires only univariate (fast) polynomial arithmetic.

It is now possible to compute a ℓ-torsion divisor D, find the pairs $(s_1, s_2) \bmod \ell$ s.t. $\pi^4(D) - s_1\pi^3(D) + s_2\pi^2(D) - s_1 q\pi(D) + q^2 D = 0$,
(iterate if necessary)

$\Longrightarrow$ Get $\chi(1) \bmod \ell$.

Practical results

- Implemented in Magma
- Feasible until $\ell = 13$
- Finish the computation by a $\sqrt{\ }$ algorithm (Birthday paradox method).

Exple: Let $\mathcal{C}$ defined by $y^2 = x^5 + 314159\ldots x^4 + \cdots$ over $\mathbb{F}_p$ with $p = 10^{19} + 51$.

Then $\quad \#\mathrm{Jac}(\mathcal{C}) = 99999999982871020671452277000281660080,$

$$s_1 = 1712898036 \ \text{ and } \ s_2 = 11452277089352355350.$$

Rem: Result computed modulo $2^8 \times 3 \times 5 \times 7 \times 11 \times 13 = 3843840$ in about 11 days. Finished by R. Harley with a parallel implementation: ≈ 50 days on a single station.

Limitations

Problem: Have to compute with polynomials of degree $O(\ell^4)$.

Question: Can we adapt Elkies–Atkin techniques for genus 2 in order to reduce the degree $O(\ell^4) \to O(\ell^3)$?

Elkies–Atkin for elliptic curves

Let E elliptic curve over $\mathbb{F}_q$, $(\ell, q) = 1$, $\chi(t) = t^2 - ct + q$.

Factorization pattern of $\Phi_\ell(X, j_E)$ (degree $\ell + 1$):

- $(1, \ell)$ or $(1, \dots, 1)$ if $c^2 - 4q \equiv 0 \bmod \ell$
- $(1, 1, r, \dots, r)$ if $c^2 - 4q \equiv \square \bmod \ell$
- $(r, \dots, r)$ if $c^2 - 4q \not\equiv \square \bmod \ell$

The pattern gives information about $c \bmod \ell$.

If there is a root in $\mathbb{F}_{q^k}$ one can construct a factor of ψ_ℓ of degree $k(\ell - 1)$.

Rem:

Roots of $\Phi_\ell(X, j_E)$ $\leftrightarrow$ ℓ-isogenies of E $\leftrightarrow$ subgroups of E of order ℓ.

Modular polynomials in genus 2

First idea: Use Igusa's invariants (j_1, j_2, j_3) and build an ideal s.t.

$$\mathcal{C}_{j_1,j_2,j_3} \text{ and } \mathcal{C}_{J_1,J_2,J_3} \text{ have } (\ell,\ell)\text{-isogenous Jacobians} \Leftrightarrow$$
$$f(j_1, j_2, j_3, J_1, J_2, J_3) = 0,\ \forall\ f \text{ in ideal.}$$

Problem: HUGE ! (even for $\ell = 2$)

Better construction: Find the minimal polynomial Ξ_ℓ of a parameter describing the subgroups of order ℓ in $\mathrm{Jac}[\ell]$. (cf Charlap–Coley–Robbins, 1991).

Gives less information, but enough for Atkin's algorithm.

Advantages:

- Only one polynomial instead of an ideal,
- Less variables,
- Still manageable for $\ell = 3\ \ (5?)$.

Construction of Ξ_ℓ: definition of ψ_ℓ

Take a generic curve $\mathcal{C}$ with equation $y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0$.

In the ideal I_ℓ of $\mathcal{C}$, consider the minimal polynomial ψ_ℓ of the coefficient u_1 in $D = \langle x^2 + u_1x + u_0, v_1x + v_0\rangle$.

Thm: The polynomial ψ_ℓ has the following properties

- It is a polynomial in U, f_0, f_1, f_2, f_3 over $\mathbb{Q}$,
- $\deg \psi_\ell = \frac{\ell^4-1}{2}$,
- It is homogeneous with weights 1 for U and $5-i$ for f_i.

Rem: Can be constructed with Cantor's division polynomials (for a fixed curve).

Construction of Ξ_ℓ: action on the roots of ψ_ℓ

By construction,

Root U of ψ_ℓ $\longleftrightarrow$ Pair $\{D, -D\}$ of ℓ-torsion divisors.

Define the multiplication by k for $k \in [1..\frac{\ell-1}{2}]$:

$$\begin{array}{ccc} \{D, -D\} & \mapsto & \{[k]D, -[k]D\} \\ U & \mapsto & h_k(U) \end{array}$$

Rem: $h_k(U)$ is also a root of ψ_ℓ and can be expressed by a polynomial in U.

Prop: $h_{k_1} \circ h_{k_2}(U) \equiv h_{k_2} \circ h_{k_1}(U) \equiv h_k(U) \mod \psi_\ell(U)$,

with $k = (\pm k_1 k_2 \bmod \ell) \in [1..\frac{\ell-1}{2}]$.

Rem: This is an explicit description of a cyclic subgroup of the Galois group of ψ_ℓ, isomorphic to $\mathbb{F}_\ell^*/\{\pm 1\}$.

Construction of Ξ_ℓ

Let

$$T = \sum_{1 \leq k \leq (\ell-1)/2} h_k(U),$$

Def: The minimal polynomial of T is called modular polynomial and denoted by $\Xi_\ell(T)$.

Rem: Min. polynomial means in the quotient algebra of I_ℓ.

Rem: Coefficients are rational fractions in f_0, f_1, f_2, f_3. Multiply by the denominators: one can assume that they are polynomials.

Thm: $\deg_T(\Xi_\ell) = \ell^3 + \ell^2 + \ell + 1$.

It is homogeneous with usual weights.

Computation of Ξ_ℓ

Prop: $\Xi_3(T)$ is a monic polynomial of degree 40 in T.

$\Longrightarrow$ It has at most 1747 monomials.

Rem: For $\ell = 3$, $\Xi_3(T) = \psi_3(U)$.

Naive technique: Compute its value for sufficiently many curves over $\mathbb{Q}$ and interpolate.

Better method: By É. Schost:

- Compute $\Xi_3(T)$ for a random curve over a finite field $\mathbb{F}_p$ (he took $p = 9001$),
- Lift the coefficients to $\mathbb{Q}_p$ with enough precision,
- Lift the scalar coefficients to polynomials.

All the liftings are done by Newton iterations.

Factorization patterns

Let $\mathcal{C}$ be a curve of genus 2 over $\mathbb{F}_q$.

Thm: Let $D \in \mathrm{Jac}(\mathcal{C})[\ell]/\overline{\mathbb{F}}_q$ and let $V = \mathrm{Span}_{\mathbb{F}_\ell}\{\pi^n(D);\ n \in \mathbb{N}\}$.

Let $P(t)$ the char. pol. of π restricted to V. Then the root of Ξ_ℓ corresponding to the subgroup generated by D lives in an extension of degree

$$\text{ord}^*(P) = \min\left\{k \in \mathbb{N}^* \text{ s.t. } \deg\left(t^k \bmod P(t)\right) = 0\right\}.$$

Rem: ord$^*(P)$ is the smallest k s.t. $\pi^k(D) = [\lambda]D$, with $\ell \in [1..\ell-1]$.

Hence: The reduction of the endomorphism π on $\mathrm{Jac}[\ell]$ determines

- $\chi(t) \bmod \ell$, and also $\#\mathrm{Jac} \bmod \ell$,
- The factorization pattern of Ξ_ℓ.

Patterns of Ξ_3

$p \equiv 2 \bmod 3$	
pattern	$\#\mathrm{Jac}(\mathcal{C}) \bmod 3$
$(10)^4$	2
$(2)^2(6)^6$	1
$(4)(12)^3$	1
$(2)^{20}$	1
$(1)^2(2)(4)(8)^4$	0
$(1)^2(2)(3)^2(6)^5$	0
$(1)^8(2)^{16}$	0
$(1)^5(2)^4(3)(6)^4$	0
$(4)^{10}$	1, 2

$p \equiv 1 \bmod 3$	
pattern	$\#\mathrm{Jac}(\mathcal{C}) \bmod 3$
$(5)^8$	1, 2
$(1)(2)^2(3)(4)^2(12)^2$	0, 2
$(1)^4(2)^2(4)^8$	0, 2
$(1)(3)^4(9)^3$	0, 1
$(1)^4(3)^{12}$	0, 1
$(1)^{40}$	0, 1
$(4)^{10}$	2
$(2)^2(6)^6$	1
$(2)^{20}$	1
$(1)^4(3)^{12}$	0
$(1)^2(2)(3)^2(6)^5$	0
$(1)^5(2)^4(3)(6)^4$	0
$(1)^8(2)^{16}$	0

Experimental verification

For $\ell = 3$: Pick a random curve over a small prime field $\mathbb{F}_p$,

- Plug its coefficients in $\Xi_3(T)$ and factor it,
- Compute $\chi(t) \bmod \ell$ by brute force algorithm,
- Compare with tables!

Result: We have found examples for almost all the cases.

For $\ell = 5$: Pick a random curve over a small prime field $\mathbb{F}_p$,

- Compute $\Xi_5(T)$ by for this special curve (not to costly), and factor it,
- Compute $\chi(t) \bmod \ell$ by brute force algorithm,
- Compare with the theory.

Problems: Degenerate when there is a ℓ-torsion divisor on Θ, or when there are multiples roots.

Atkin's algorithm in genus 2

Assume that all the (generic) Ξ_ℓ have been precomputed.

Algorithm:

1. While not enough information

   (a) Choose a new prime ℓ;

   (b) Compute the pattern of $\Xi_\ell(T)$;

   (c) Find the compatible values of $\chi(1) \bmod \ell$;

2. Recover $\chi(1)$ compatible with modular information.

Cost of one loop: Step (c) is negligible;

Finding the pattern costs a factorization of polynomial of deg $O(\ell^3)$;

Problem: Evaluating Ξ_ℓ at the coeff of the curve costs as many mult. as the number of monomials: $O(\ell^{12})$.

Limitations, perspectives

Rem: Constant in $O(\ell^{12})$ is small, and for $\ell = 3$, it is very fast. But even for $\ell = 5$, it will be very costly ($>$250 000 monomials).

$\Longrightarrow$ Computing (and storing) the generic modular polynomials $\Xi_\ell(T)$ will not be possible for interesting values of ℓ.

Question: Is it possible to compute $\Xi_\ell(T)$ for a given curve, with a cost lower than the subsequent factorization ?