On Mestre's algorithm for counting points of hyperelliptic curves of genus 2

Pierrick Gaudry

gaudry@lix.polytechnique.fr

http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/

February 2003, Bordeaux.

Cryptographical context

- Cryptosystems based on elliptic curves are now viewed as a reasonnable alternative to RSA and classical discrete log-based systems.
- Genus 2 hyperelliptic curves have the same advantages (small key size, small signatures...)
- More complicated group law vs smaller base field.
- Recent improvements showed that runtimes are comparable with elliptic curves.

Algorithms for counting points

1. Algorithms based on Schoof's idea

Work for any characteristic.

Reasonnably fast for elliptic curves, complicated for genus 2 curves, intractable for more complicated curves.

2. Algorithms based on p-adic lifting

Work only in small characteristic.

- Canonical lift (Satoh's algorithm)

  Elliptic curves

  Genus 2 curves in characteristic 2

- Arbitrary lift

  Wide class of curves

  Kedlaya: Monsky-Washnitzer cohomology

  Lauder-Wan: Dwork's proof of the rationality of Zeta function

What size do we want to handle ?

For crypto: size of the Jacobian must be at least 2^{160}.

Records: several thousands of bits.

Genus 2 curves in characteristic 2

Base field: $\mathbb{F}_q$ with $q = 2^n$.

Let C be a curve over $\mathbb{F}_q$ with equation $y^2 + h(x)y = f(x)$, where f and h are polynomials of degree 5 and 2.

NB: not always possible, assume that only one place at infinity.

Frobenius endomorphism: Σ : $x \mapsto x^q$ extends coordinate-wise to $C/\overline{\mathbb{F}}_q$ and linearly to $\mathrm{Jac}(C)$ thus giving an endomorphism which verifies

$$\chi(\Sigma) = \Sigma^4 - s_1\Sigma^3 + s_2\Sigma^2 - qs_1\Sigma + q^2\mathrm{Id} = 0,$$

And the order of the jacobian is

$$\#\mathrm{Jac}(C)/\mathbb{F}_q = \chi(1) = q^2 + 1 - s_1(q+1) + s_2.$$

The ring $\mathbb{Z}_q$ (a.k.a. $W(\mathbb{F}_q)$)

We need to work with elements of the p-adic ring above $\mathbb{F}_q$:

Write $\mathbb{F}_q = \mathbb{F}_2[t]/(\overline{f}(t))$, where $\overline{f}(t)$ is irreducible of degree n.

Then take the ring of integers of the degree n unramified extension of $\mathbb{Q}_2$:

$$\mathbb{Z}_q := \mathbb{Z}_2[t]/(f(t)),$$

where $f(t)$ is obtained by lifting the coefficients of $\overline{f}(t)$ to $\mathbb{Z}_2$.

Each $z \in \mathbb{Z}_q$ can be represented by a polynomial

$$z = z_0 + z_1 t + \cdots + z_{n-1} t^{n-1},$$

where the z_i's are integers modulo 2^N, (N is the precision).

There is a ring automorphism σ fixing $\mathbb{Z}_2$, lifting the 2-nd power Frobenius of $\mathbb{F}_q$.

Computations in $\mathbb{Z}_q$

- Multiplications and additions: classical algorithms for polynomials over integers modulo 2^N.
- Inverse, square root: Newton iteration.
- Frobenius substitution:
  - General case: precompute t^σ usgin a Newton iteration, and subsitute with Horner.
  - Cyclotomic representation (Satoh): If the polynomial defining $\mathbb{Z}_q$ is chosen to divide $X^q - X$, then $t^\sigma = t^2$, and Frobenius substitution costs one multiplication. (But dense defining poly $\Longrightarrow$ expensive reduction)

Canonical lift

A canonical lift of C is a curve $\mathfrak{C}/\mathbb{Z}_q$ such that

$$\operatorname{End}(\operatorname{Jac}(\mathfrak{C})) \cong \operatorname{End}(\operatorname{Jac}(C)) \quad \text{and} \quad \mathfrak{C} \equiv C \mod 2.$$

For Satoh's algorithm, the key theorem was:

Thm: (Lubin–Serre–Tate) If E is an ordinary elliptic curve, then there exists a canonical lift $\mathfrak{E}$, which is unique up to isomorphism. Moreover

$$\Phi_2(j(\mathfrak{E}), j(\mathfrak{E})^\sigma) = 0,$$

where σ is the 2-nd power Frobenius automorphism of $\mathbb{Z}_q$.

Φ_2 is the 2-nd modular equation, which vanishes when there is a 2-isogeny between the two curves whose invariants are plugged.

Canonical lift: Theoretical considerations

How does the LST theorem extend to non-elliptic curves?

- It is possible to lift an ordinary abelian variety together with a polarization.
- Thus, the principal polarization corresponding to the curve can be lifted to a principal polarization.
- However in general principally polarized abelian variety are not jacobian varieties.

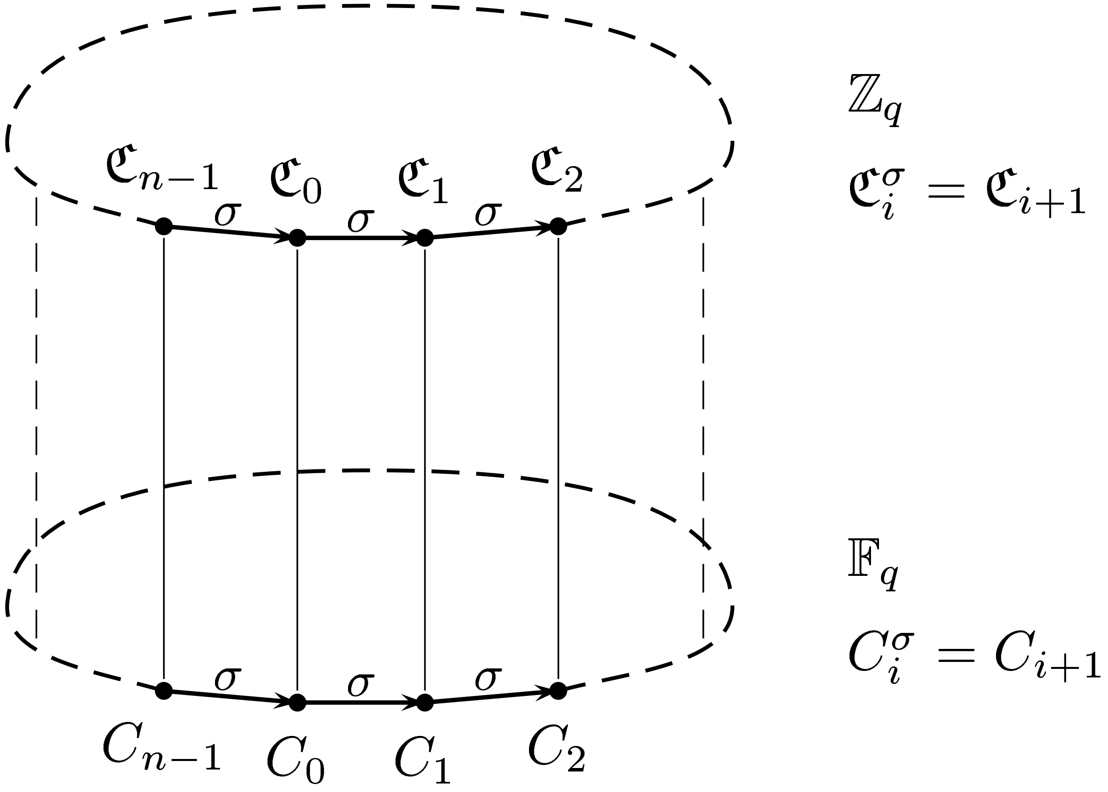
- In the particular case of genus 2 and 3, p.p.a.v. are jacobians.
- In genus 2 all curves are hyperelliptic.

[See work of Oort.]

$\Longrightarrow$ In genus 2, it is possible to canonically lift the Jacobian of C.

In genus 3, it is possible to canonically lift the Jacobian of C, but the lifted curve might be non-hyperellitpic.

σ: 2-nd power Frobenius



$\mathrm{Jac}(\mathfrak{C}_{i+1})$ is $(2,2)$-isogenous to $\mathrm{Jac}(\mathfrak{C}_i)$
$\mathrm{Jac}(C_{i+1})$ is $(2,2)$-isogenous to $\mathrm{Jac}(C_i)$

General strategy

1. Compute the canonical lift $\mathfrak{C}$;
2. Compute explicitly the action of σ upstairs;
3. Compose these actions to get the action of Σ upstairs;
4. Deduce the action of Σ downstairs.

Computations are done at some finite precision 2^k, the characteristic polynomial χ of Σ is then computed modulo 2^k. If k is large enough, this is enough to conclude with the Hasse-Weil bounds.

Richelot's isogeny

In 1836, Richelot derived some magic formulae to compute quickly integrals of the form

$$\int \frac{(a\cos^2 t + b\sin^2 t)dt}{\sqrt{(1-c^2\sin^2 t)(1-l^2\sin^2 t)(1-m^2\sin^2 t)}}.$$

These integrals can be transformed into integrals of the form

$$\int \frac{x^i dx}{\sqrt{F(x)}},$$

where $F(x)$ is a polynomial of degree 5 or 6.

Richelot’s isogeny (2)

Richelot’s formulae are an explicit expression for a $(2, 2)$-isogeny from the jacobian of the curve $y^2 = F(x)$.

Revisited in 1865 by Königsberger: the formulae are explained in terms of theta functions.

Put in a more geometrical point of view in 1901 by Humbert.

See Bost–Mestre (1988) for a modern treatment.

Explicit $(2,2)$-isogeny

Def: If S and T are monic polynomials of degree 2, define

$$[S,T](x) = S'(x)T(x) - S(x)T'(x).$$

Thm: Let C of equation $y^2 = P(x)Q(x)R(x)$, where P, Q, R are monic of degree 2. Let C' the curve given by

$$\Delta y^2 = [Q,R](x)\,[R,P](x)\,[P,Q](x),$$

where Δ is the determinant of P, Q, R in the basis $1, x, x^2$.

Then $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C')$ are $(2,2)$-isogenous abelian varieties. Moreover everything can be made explicit.

The Richelot sequence in 2-adics

Idea: Group together pairs of roots which are close p-adically.

Lemma: It is possible to define an infinite sequence of genus 2 curves as follows (the square roots always exist):

Let C be a curve over $\mathbb{Z}_q$ with equation

$$y^2 = P(x)Q(x)R(x),$$

where $P = (x - p_1)(x - p_2)$, $Q = (x - q_1)(x - q_2)$ and $R = (x - 2r_1)(x - 2r_2)$, with

$$p_1 \equiv p_2 \mod 4, \;\; q_1 \equiv q_2 \mod 4, \;\; r_1 \equiv r_2 \mod 2.$$

Define $U = [Q, R]$, $V = [R, P]$, $U = [P, Q]$, and C' the curve with equation $y^2 = U(x)V(x)W(x)$.

Then

- The roots of U, V, W are all defined over $\mathbb{Z}_q$.
- Writing them $u_1, 2u_2$ (resp. $v_1, 2v_2$ and w_1, w_2), there is an ordering such that

$$u_1 \equiv w_1 \mod 4, \;\; v_1 \equiv w_2 \mod 4, \;\; u_2 \equiv v_2 \mod 2.$$

Therefore, we can apply again the operation with C', and continue.

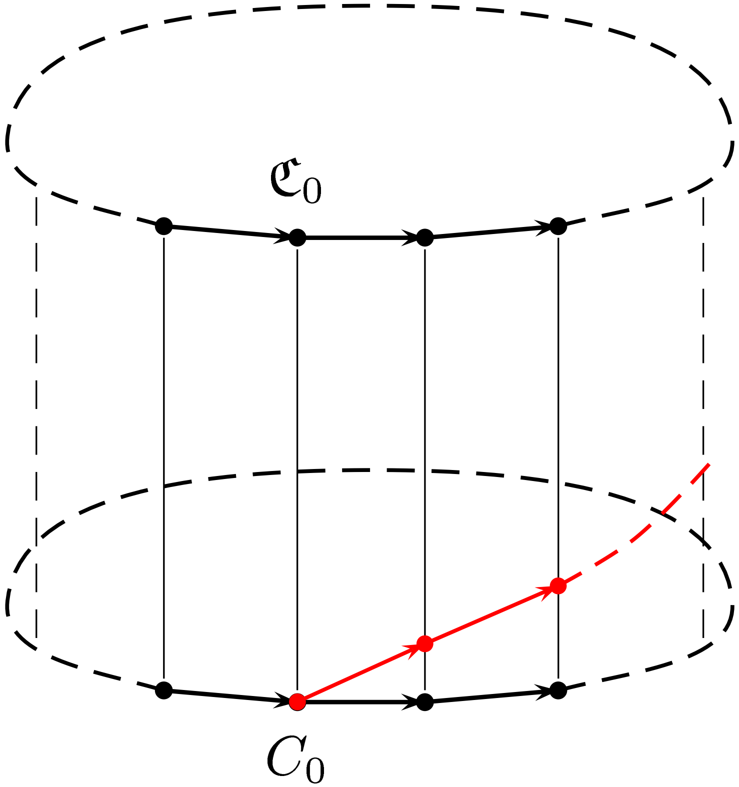
Link with the canonical lift

If the proper initialization is made, we get:

Thm: *(unprecise statement)* Following one step of the Richelot sequence:

- we move from a curve to its conjugate (mod 2);
- we get one bit of precision closer to the canonical lift

Proof: postponed...


$\mathfrak{C}_0$
C_0

Iteration

At each step, we are given $P(x)$, $Q(x)$, $R(x)$, monic of degree 2, with roots of P (resp. Q, R) congruent modulo 2.

- Compute the brackets. *(a few products)*
- Normalize them. *(3 inverses and 6 prods)*
- Find the 6 roots. *(3 square roots and some prods)*
- Form the new $U(x)$, $V(x)$, $W(x)$, regroup roots which are congruent mod 2. *(a few products)*

Getting $\chi(T)$

Assume $\mathfrak{C}$ has been lifted canonically with enough precision.

Do one more Richelot isogeny

$$\phi : \mathfrak{C} \longrightarrow \mathfrak{C}^\sigma,$$

and make explicit the action of ϕ on the basis of differentials:

$$\phi^* \begin{pmatrix} \frac{dx}{y} \\ \frac{x\,dx}{y} \end{pmatrix} = M \begin{pmatrix} \frac{dx}{y} \\ \frac{x\,dx}{y} \end{pmatrix},$$

where M is a 2×2 matrix.

Then eigenvalues of $M M^\sigma \cdots M^{\sigma^{n-1}}$ are roots of $\chi(T)$ and the 2 other roots are conjugates.

Complexity

Hasse-Weil bound:

$$|s_1| \leq 4\sqrt{q} \quad \text{and} \quad |s_2| \leq 6q.$$

$\Longrightarrow$ $O(n)$ iterations at precision $O(n)$

Each step costs a constant number of products in $\mathbb{Z}_q$ at precision $O(n)$.

Fast norm computation *à la* Satoh extends to matrices.

Overall complexity is in $O(n^{3+\varepsilon})$.

$\Longrightarrow$ Very fast in practice: 2-5 times slower than AGM for elliptic curves for comparable group size.

But...

Fact: Nowadays, AGM is not the fastest algorithm for elliptic curves...

Question: Can we apply the same improvements to genus 2 ?

Review of improvements to AGM for elliptic curves

Main idea: Go back to a modular polynomial relating invariants of two consecutive curves.

$\Longrightarrow$ Solve $\Phi_2(J, J^\sigma) = 0$.

- SST algorithm: Hensel lifting with cheap updates at each step using partial derivatives. Complexity in $O(n^{2.5+\varepsilon})$.
- Harley's algorithm: Mix SST with a Newton-like lift. Gets a complexity in $O(n^{2+\varepsilon})$ for the lift.
- Kim et al., Lercier-Lubicz: In the case where a Gaussian Normal Basis is available, complexity in $O(n^{2+\varepsilon})$ for the whole point-counting.

Modular equations in genus 2

First idea: use Igusa's invariants.

The associated modular equations are huge.

Second idea: use the Rosenhain's invariants.

A curve $\mathfrak{C}$ of genus 2 is in Rosenhain form if it has an equation

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

There are 120 triples (λ, μ, ν) giving isomorphic curves.

6 choices for the root thrown at infinity, then 5 choices for the roots thrown to 0, and 4 choices for the root thrown to 1.

Rosenhain-Richelot sequence

A curve C in the Richelot sequence can be put in the form

$$y^2 = x(x-1)(x-\lambda_0)(x-\lambda_1)(x-\lambda_\infty)$$

over the local field, with

$$\lambda_0 \equiv 0 \mod 2, \quad \lambda_1 \equiv 1 \mod 2, \quad \mathrm{Ord}(\lambda_\infty) < 0.$$

We can apply the Richelot explicit isogeny, and renormalize to a Rosenhain form.

With a good ordering (well defined using valuations, etc...), we obtain

$$y^2 = x(x-1)(x-\lambda'_0)(x-\lambda'_1)(x-\lambda'_\infty)$$

with λ'_0 close to λ_0^σ, and so on.

The formal derivation of these imply some square roots.

Cleaning them gives modular equations

$$\begin{cases} \Phi_0(\lambda_0', \lambda_0, \lambda_1, \lambda_\infty) = 0 \\ \Phi_1(\lambda_1', \lambda_0, \lambda_1, \lambda_\infty) = 0 \\ \Phi_\infty(\lambda_\infty', \lambda_0, \lambda_1, \lambda_\infty) = 0 \end{cases}$$

These equations are big but still manageable.

$\Longrightarrow$ it is possible to design an SST-like lifting algorithm in genus 2.

NB: Need to deal with some additional linear algebra (Jacobian matrix).

Key Point: Analyzing the valuations involved in this matrix shows that the Hensel lifting converges. (i.e. proves the Thm)

Formulae

It is better to keep the system with the square roots as indeterminates.

More equations and variables, but smaller size.

For all variables, the subscript indicates the value modulo 2.

$$
\left\{
\begin{array}{rcl}
0 & = & u_1^2 - 2\lambda_\infty u_1 + \lambda_\infty(1+\lambda_1) - \lambda_1 \\
 & & \scriptstyle 0 = u_\infty + u_1 + 2\lambda_\infty \\
0 & = & v_0^2 - 2\lambda_\infty v_0 + \lambda_0\lambda_\infty \\
 & & \scriptstyle 0 = v_\infty + v_0 + 2\lambda_\infty \\
0 & = & (\lambda_0 - 1 - \lambda_1)w_0^2 + 2\lambda_1 w_0 - \lambda_0\lambda_1 \\
 & & \scriptstyle 0 = (\lambda_0 - 1 - \lambda_1)(w_0 + w_1) - 2\lambda_1 \\
0 & = & (u_1 - v_0)(u_\infty - v_\infty)\lambda'_\infty - (u_1 - v_\infty)(u_\infty - v_0) \\
0 & = & (u_1 - v_0)(w_1 - v_\infty)\lambda'_1 - (u_1 - v_\infty)(w_1 - v_0) \\
0 & = & (u_1 - v_0)(w_0 - v_\infty)\lambda'_0 - (u_1 - v_\infty)(w_0 - v_0)
\end{array}
\right.
$$

$$
\lambda'_0 = {\lambda_0}^\sigma, \quad \lambda'_1 = {\lambda_1}^\sigma, \quad \lambda'_\infty = {\lambda_\infty}^\sigma
$$

With this system, it is straightforward to:

- Rewrite the algorithm as a Hensel lifting.

  Complexity in $O(n^3 + \varepsilon)$.

- Apply the SST improvement. (implemented but...)

  Complexity in $O(n^{2.5} + \varepsilon)$.

- Apply Harley's improvement. (not yet implemented)

  Complexity in $O(n^2 + \varepsilon)$.

The final matrix norm computation is still slow, and is now the bottleneck.

Initialization

At the begining, we have a curve over $\mathbb{F}_q$ with an equation

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

Lift it to $\mathbb{Z}_q$ and normalize as

$$y^2 = F(x) = 4f(x) + h(x)^2.$$

Apply one Richelot step formally (usually in an extension), and transform into the Rosenhain form.

The easy case is when $h(x)$ splits over $\mathbb{F}_q[x]$:

$$h(x) = x^2 + h_1 x + h_0 = (x - \rho_1)(x - \rho_2)$$

Define

$$\mu_\infty = 1/h_1^2, \quad \mu_0 = \frac{f(\rho_1)h_1^2 + f'(\rho_1^2)}{h_1^6}, \quad \mu_1 = \frac{f(\rho_2)h_1^2 + f'(\rho_2^2)}{h_1^6}$$

Then initialization for the Richelot-Rosenhain formula is

$$\lambda_0 = 4\mu_0, \quad \lambda_1 = 1 + 4\mu_1, \quad \lambda_\infty = \frac{\mu_\infty}{4}$$

A few words about the new Mestre's algorithm (implemented by Lercier-Lubicz)

General idea: Forget about the curve... Wrok with the abelian variety!

Thm:(Borchardt's mean) Let a, b, c, d be the 4 theta constants with characteristic ... associated to a 2-dimensional abelian variety A. Then a', b', c', d' defined by

$$\begin{cases} a' &= \frac{1}{4}(a+b+c+d) \\ b' &= \frac{1}{2}(\sqrt{ab}+\sqrt{cd}) \\ c' &= \frac{1}{2}(\sqrt{ac}+\sqrt{bd}) \\ d' &= \frac{1}{2}(\sqrt{ad}+\sqrt{bc}) \end{cases}$$

are the same theta constants for an abelian variety A' which is $(2,2)$-isogenous to A.

Formula of Thomae

Good news: It is possible to get information about the Frobenius action without going back to the representation of the abelian variety as a Jacobian of a curve!

Denote by A_i, B_i, C_i, D_i the sequence of theta constants obtained using the Borchardt's formulae.

Thm: (Thomae, Mestre) With the appropriate initialization,

$$\frac{A_i}{A_{i+n}}$$

converges to the product of the eigenvalues of the Frobenius which are units.

$\Longrightarrow$ Characteristic polynomial can be deduced using LLL (for instance).

Borchardt vs Richelot

- Lifing formulae are much simpler for B than for R;
- Required lifting precision is $\approx n$ for R but $\approx \frac{3n}{2}$ for B;
- Norm of an element for B vs norm of a 2×2 matrix for R;

Everything is in the constants!!!

Hard to tell which one is better.

NB: At any stage it is possible to switch from a method to another one... Maybe the optimal is a mix of both.