Computing cardinalities of $\mathbb{Q}$-curve reductions over finite fields

F. MORAIN, C. SCRIBOT, B. SMITH

Laboratoire d'Informatique de l'École polytechnique

ANTS XII, August 30, 2016

SEA you in 10 years!

(Banff, November 8th, 2005; SEA++ in C++)

Plan

I. Motivation.

II. Classical results.

III. d-admissible curves.

IV. Modifying the SEA algorithm.

V. Implementation.

VI. Conclusions.

I. Motivation

General goal: find $\mathscr{E}/\mathbb{F}_q$ for which evaluating $[m]P$ can be done faster than double-and-add.

Idea: $\#\mathscr{E} = N$ with endomorphism ψ. Write $m = a + b\lambda_\psi \bmod N$, with $\|a\|, \|b\| \sim 1/2 \log_2 N$. Then

$$[m]P = [a]P \oplus [b]\psi(P)$$

$+$ multi-exponentiation algorithm $=$ fast evaluation of $[m]P$.

Classes of curves:

- Gallant-Lambert-Vanstone: CM with tiny discriminant (e.g., $\psi(x,y) = (-x, iy)$);
- Galbraith-Lin-Scott: view $\mathscr{E}/\mathbb{F}_p$ over $\mathbb{F}_{p^2}$ (twist + p-power Frobenius).
- Smith: reduction of $\mathbb{Q}$-curves modulo inert primes (isogeny + p-power Frobenius).

General setting for Smith curves

This talk: $q = p^2$, p large, $\mathscr{E} : Y^2 = X^3 + AX + B$ with A, B in $\mathbb{F}_q$.

Goal: compute $\#\mathscr{E}$ as fast as possible for lots of $\mathscr{E}$ (statistics, good parameters, twist secure curves, etc.).

$\Rightarrow$ use Schoof's algorithm for computing $\#\mathscr{E}$

. . . *but we can do better!*

We suppose $\mathscr{E}$ is ordinary (i.e., not supersingular).

II. Classical results

Frobenius:

$$\begin{array}{rccc} \pi_q : & \overline{\mathbb{K}} & \to & \overline{\mathbb{K}} \\ & x & \mapsto & x^q \end{array}$$

Extension to $\mathscr{E}$:

$$\begin{array}{rccc} \pi_q : & \mathscr{E}(\overline{\mathbb{K}}) & \to & \mathscr{E}(\overline{\mathbb{K}}) \\ & (X,Y) & \mapsto & (X^q, Y^q) \end{array}$$

Thm. The minimal polynomial of π_q is $\chi_\pi(T) = T^2 - tT + q$, $|t| \leq 2\sqrt{q}$ and $\#\mathscr{E} = \chi_\pi(1)$.

Also: little Frobenius

$$\begin{array}{rccc} \sigma : & \overline{\mathbb{K}} & \to & \overline{\mathbb{K}} \\ & x & \mapsto & x^p \end{array}$$

extended to $\pi_p((x,y)) = (x^p, y^p)$ and

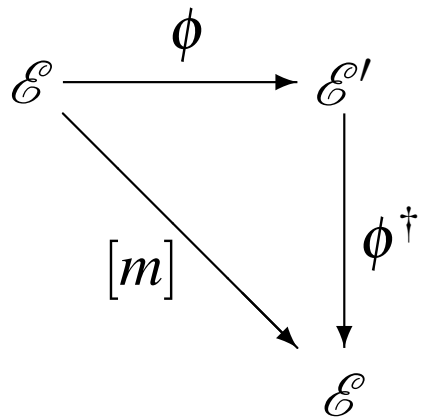
$$\mathscr{E} : Y^2 = X^3 + AX + B, \quad {}^\sigma\mathscr{E} : Y^2 = X^3 + {}^\sigma A X + {}^\sigma B.$$

Isogenies

Def. $\phi : \mathscr{E} \to \mathscr{E}'$, $\phi(O_{\mathscr{E}}) = O_{\mathscr{E}'}$; induces a morphism of groups.

Ex. $[k]$; Frobenius.

Thm. (dual isogeny) There is a unique $\phi^\dagger : \mathscr{E}' \to \mathscr{E}$, $\phi^\dagger \circ \phi = [m]_{\mathscr{E}}$, $\phi \circ \phi^\dagger = [m]_{\mathscr{E}'}$, $m = \deg\phi$.



Isogenies and subgroups

Thm. If F is a finite subgroup of $\mathscr{E}$, there exists ϕ and $\mathscr{E}'$ s.t.

$$\phi : \mathscr{E} \to \mathscr{E}' = \mathscr{E}/F, \quad \ker(\phi) = F.$$

All isogenies are built this way.

Vélu's formulas:

$$\phi(X,Y) = \left(\frac{G(X)}{H(X)^2}, \frac{J(X,Y)}{H(X)^3} \right),$$

$$H(X) = \prod (X - x_F),\ \deg(H) = (\deg\phi - 1)/2$$

(case $\deg\phi$ odd.)

Algorithms: Elkies, Atkin (+Bostan/M./Salvy/Schost); Couveignes (formal groups, Artin Schreier towers – see De Feo *et al.* – this ANTS); Lercier ($p = 2$); Lercier/Sirvent (p-adic methods, see very recent Lairez/Vaccon).

A fundamental construction

Modular polynomial: there exists $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$ s.t. $\mathscr{E}$ and $\mathscr{E}'$ are m-isogenous over $\mathbb{K}$ only if $\Phi_m(j(\mathscr{E}),j(\mathscr{E}')) = 0$.

Let's ignore rationality questions

Key property: finding isogenous curves is equivalent to finding roots of $\Phi_\ell(X,j(\mathscr{E}))$.

A lot was written on how to compute modular polynomials with various properties.

III. d-admissible curves

Three actors:

- degree d isogeny $\vartheta : \mathscr{E} \to \mathscr{E}'$
- dual $\vartheta^\dagger : \mathscr{E}' \to \mathscr{E}$
- Little Frobenius: every isogeny $\vartheta : \mathscr{E} \to \mathscr{E}'$ has a Galois conjugate isogeny ${}^\sigma\vartheta : {}^\sigma\mathscr{E} \to {}^\sigma\mathscr{E}'$ obtained by raising coefficients of ϑ to p-th power.

Def. Assume $p \nmid d$; $\mathscr{E}/\mathbb{F}_{p^2}$ is d-admissible if it is equipped with a d-isogeny

$$\phi : \mathscr{E} \longrightarrow {}^\sigma\mathscr{E} \quad \text{such that} \quad {}^\sigma\phi = \varepsilon\phi^\dagger \quad \text{where} \quad \varepsilon = \pm 1 \ .$$

Prop. Composing $\pi_p : \mathscr{E} \to {}^\sigma\mathscr{E}$ with ${}^\sigma\phi : {}^\sigma\mathscr{E} \to \mathscr{E}$, we obtain the associated endomorphism

$$\psi := {}^\sigma\phi \circ \pi_p \in \mathrm{End}(\mathscr{E})$$

of degree dp.

A typical example: reduction of $\mathbb{Q}$-curve

Hasegawa family for $d = 2$: Δ squarefree integer, for $s \in \mathbb{Q}$:
$\widetilde{\mathscr{E}} : y^2 = x^3 - 6(5 - 3s\sqrt{\Delta})x + 8(7 - 9s\sqrt{\Delta})$.
Let τ be the involution of $\mathbb{Q}(\sqrt{\Delta})$; there is a 2-isogeny
$\widetilde{\phi} : \widetilde{\mathscr{E}} \to {}^{\tau}\widetilde{\mathscr{E}}$ over $\mathbb{Q}(\sqrt{\Delta}, \sqrt{-2})$ with kernel polynomial $x - 4$.

Let p be a prime > 3, s.t. p is inert in $\mathbb{Q}(\sqrt{\Delta})$, and extend τ to the image of σ in $\mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta}, \sqrt{-2}), \mathbb{Q})$; then ${}^{\tau}\widetilde{\phi} = \varepsilon\widetilde{\phi}^{\dagger}$, where $\varepsilon = -(-2/p)$.
Reducing $\widetilde{\mathscr{E}}$ (and $\widetilde{\phi}$) mod p, we get a d-admissible curve $\mathscr{E}/\mathbb{F}_{p^2}$ with associated endomorphism

$$\psi : (x, y) \longmapsto \left(\frac{x^p(x^p - 4) + 18(1 - s\sqrt{\Delta})}{-2(x^p - 4)} \right.,$$

$$\left. \frac{y^p}{\sqrt{-2}^p} \left(\frac{(x^p - 4)^2 - 18(1 - s\sqrt{\Delta})}{-2(x^p - 4)^2} \right) \right).$$

IV. Modifying the SEA algorithm.

Def. (torsion points) For $k \in \mathbb{N}$, $\mathscr{E}[k] = \{P \in \mathscr{E}(\overline{\mathbb{K}}), [k]P = O_{\mathscr{E}}\}$.

Division polynomials: (for $\mathscr{E} : y^2 = x^3 + Ax + B$)

$$[k](X,Y) = \left(\frac{\phi_k(X,Y)}{\Psi_k(X,Y)^2}, \frac{\omega_k(X,Y)}{\Psi_k(X,Y)^3} \right)$$

$$\phi_k = X\Psi_k^2 - \Psi_{k+1}\Psi_{k-1}$$

$$4Y\omega_k = \Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2$$

$$\phi_k, \Psi_{2k+1}, \Psi_{2k}/(2Y), \omega_{2k+1}/Y, \omega_{2k} \in \mathbb{Z}[A,B,X]$$

Classical:

- make them univariate $f_k(X)$ (degree $O(k^2)$);
- design binary forms of recurrence $O(\log k)$ operations.

Schoof's algorithm (1985)

The fundamental idea: let ℓ be prime to p. Then π_q restricted to $\mathscr{E}[\ell]$ satisfies

$$\pi_q{}^2 - t\pi_q + q \equiv 0 \bmod \ell$$

so we can find $t_\ell \equiv t \bmod \ell$ such that

$$(X^{q^2}, Y^{q^2}) \oplus [q](X,Y) = [t_\ell](X^q, Y^q)$$

in $\mathbb{K}[X,Y]/(\mathscr{E}, f_\ell(X))$ and use CRT once $\prod \ell > 4\sqrt{q}$ ($\Rightarrow \ell = O(\log q)$).

Thm. Schoof's algorithm is deterministic polynomial with (bit)-complexity $O((\log q)^8)$, asymptotically $\tilde{O}((\log q)^5)$.

Pb. $\deg(f_\ell) = O(\ell^2)$.

Elkies (ca. 1989)

Consider

$$\pi_q{}^2 - t\pi_q + q = 0, \quad \Delta = t^2 - 4q.$$

If $(\Delta/\ell) = +1$ (*Elkies prime*), then over $\mathbb{F}_\ell$,

$$\mathrm{Mat}(\pi_q) \simeq \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

$\Leftrightarrow \exists F, \pi_q(F) = F \Leftrightarrow F$ is a cyclic subgroup of order ℓ

$\Rightarrow \mathscr{E}$ is ℓ-isogenous to $\mathscr{E}' = \mathscr{E}/F$.

$\Rightarrow f_\ell$ has a factor of degree $(\ell-1)/2$.

SEA algorithm

for prime ℓ **until** $\prod_{\ell \text{ good}} \ell > 4\sqrt{q}$ **do**

1. determine type of ℓ:
   1.1 compute $f(X) = \Phi_\ell(X, j(\mathscr{E}))$;
   1.2 find the roots of f over $\mathbb{K}$ using $\gcd(X^q - X, f)$;
   1.3 if none, use next ℓ;

2. let j_0 be one of the roots:
   2.1 build $\mathscr{E}' = \mathscr{E}/F$ corresponding to j_0; deduce $g_\ell \mid f_\ell$;
   2.2 find $\lambda_\pi \bmod \ell$ s.t. $\pi_q(X,Y) = [\lambda_\pi](X,Y) \bmod (\mathscr{E}, g_\ell)$,
   2.3 compute $t = \lambda_\pi + q/\lambda_\pi \bmod \ell$;

Complexity: for ℓ, $O((\log q) \cdot \mathrm{M}(\ell \log q))$; total $O((\log q) \cdot (\log q) \cdot \mathrm{M}((\log q)^2) = \tilde{O}((\log q)^4)$ probabilistic (half the primes are good).

Back to d-admissible curves

Remember: $\mathscr{E}$ d-admissible curve over $\mathbb{F}_{p^2}$, with separable d-isogeny $\phi : \mathscr{E} \to {}^{\sigma}\mathscr{E}$ (satisfying ${}^{\sigma}\phi = \varepsilon\phi^{\dagger}$ with $\varepsilon = \pm 1$), and associated endomorphism $\psi = {}^{\sigma}\phi \circ \pi_p$.

Thm.

$$r\psi = p + \varepsilon\pi_{p^2} \quad \text{in} \quad \mathrm{End}(\mathscr{E})$$

$$\chi_{\psi}(T) = T^2 - rdT + dp \ ,$$

where r is an integer satisfying

$$dr^2 = 2p + \varepsilon t_{\mathscr{E}}, \quad |r| \leq 2\sqrt{p/d} \ .$$

Key idea: use ψ instead of π, i.e., compute r instead of t.

Modified SEA

for prime ℓ **until** $\prod_{\ell \text{ good}} \ell > 4\sqrt{p/d}$ **do**

1. determine type of ℓ:
   1.1 compute $f(X) = \Phi_\ell(X, j(\mathscr{E}))$;
   1.2 find the roots of f over $\mathbb{K}$ using $\gcd(X^q - X, f)$;
   1.3 if none, use next ℓ;

2. let j_0 be one of the roots:
   2.1 build $\mathscr{E}' = \mathscr{E}/F$ corresponding to j_0; deduce $g_\ell \mid f_\ell$;
   2.2 find $\lambda_\psi \bmod \ell$ s.t. $\psi(X,Y) = [\lambda_\psi](X,Y) \bmod (\mathscr{E}, g_\ell)$;
   2.3 $r = \lambda_\psi/d + p/\lambda_\psi \bmod \ell$; $t = \varepsilon(dr^2 - 2p)$.

Complexity: for ℓ, $O((\log q) \cdot \mathsf{M}(\ell \log q))$; total $O((\log p) \cdot (\log q) \cdot \mathsf{M}((\log p)(\log q)) = \tilde{O}((\log p)^2 (\log q)^2) = \tilde{O}((\log q)^4)$.

But in real life, $p = \sqrt{q}\ldots$ $\Rightarrow$ hope for a speedup of 4.

V. Implementation

Almost all tricks from classical SEA can be transfered *mutatis mutandis*:

- classical algorithms on polynomials (modular composition, etc.);
- algorithms for eigenvalues, isogeny cycles;
- volcanic primes;
- Atkin primes: sort and match (or chinese and match), using $dr^2 = 2p + \varepsilon t$;
- early abort.

Polynomial arithmetic

C++ NTL 9.10.0 (with gcc 6.1.0)
Intel Xeon platform (E5520 CPU at 2.27GHz).

$p_{128} := 314159265358979323846264338327950288459$,

$p_{255} := 31415926535897932384626433832795028841971693993751058209749445923078164062$

ℓ	$X^q \bmod \Phi_\ell$	$X^p \bmod \Phi_\ell + X^p \circ X^p$
p_{128}		
101	0.47	$0.23 + 0.04$
173	0.88	$0.43 + 0.11$
p_{255}		
101	1.40	$0.69 + 0.07$
173	2.80	$1.38 + 0.18$

Benchmarks

$1 \leq s \leq 100$, Elkies primes only (+Atkin primes); average values

	SEA	Modified SEA
p_{128}		
max. ℓ	208 (136)	113 (66)
X^q time	13.10 (6.42)	5.19 (2.74)
Total time	30.12 (18.44, 2.14)	10.45 (4.81, 0.21)
p_{255}		
max. ℓ	394 (326)	208 (153)
X^q time	112.38 (75.62)	34.43 (19.78)
Total time	230.24 (188.14, 2.93)	62.41 (40.02, 0.76)

Twist-secure curves:

$p = p_{255}$ and $s = 269$ yields $(2q', 2q'')$ in 2773 sec (with early abort and fancy speedups).

VI. Conclusions

A volcanic remark:

$$\Delta_\psi = d(dr^2 - 4p) \qquad \text{and} \qquad \Delta_{\pi_q} = t_{\mathscr{E}}^2 - 4p^2 = r^2\Delta_\psi \ ,$$

so $|r|$ is the conductor of $\mathbb{Z}[\pi_q]$ in $\mathbb{Z}[\psi]$: that is,

$$\mathbb{Z}[\pi_q] \subset \mathbb{Z}[\psi] \subseteq \mathrm{End}(\mathscr{E}) \qquad \text{with} \qquad [\mathbb{Z}[\psi] : \mathbb{Z}[\pi_q]] = |r| \ .$$

- all primes $\ell \mid r$ are volcanic;
- we can build curves with $\ell \mid r$ for prescribed ℓ.

Guess: this contruction might yield further applications.

SEA over $\mathbb{F}_{p^n}$: still some algorithmic problems to be solved.

SEA you sooner