ECC'98

September 16, 1998

Isogeny computations and point counting on elliptic curves

F. Morain

http://www.lix.polytechnique.fr/Labo/Francois.Morain/

Plan

I. Motivations: SEA, Kohel, Galbraith.

II. Elliptic curves.

III. Counting points on elliptic curves over finite fields.

IV. Isogenies.

V. The case p small.

VI. Conclusion.

II. Elliptic curves over $\mathbb{K}$

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

$$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4, c_6 = b_2^3 + 36b_2b_4 - 216b_6,$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0$$

$$j(E) = \frac{c_4^3}{\Delta}$$

$E(\mathbb{K})$, tangent-and-chord ($\oplus$)

m**-torsion**: $E[m] = \{P \in \overline{\mathbb{K}}, [m]P = O_E\}$ can be described by $f_m(X)$ s.t.
$P = (x, y) \in E[m] \leftrightarrow f_m(x) = 0$;
$\deg(f_m) = O(m^2)$.

$E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ when $(m, \mathrm{char}(\mathbb{K})) = 1$

III. Counting points on elliptic curves over finite fields

$$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^n}$$

Th. $\phi : (X, Y) \mapsto (X^q, Y^q)$ satisfies

$$\pi^2 - c\pi + q = 0$$

$$\#E(\mathbb{K}) = q + 1 - c, |c| \leq 2\sqrt{q}$$

Caveat: we do not consider supersingular curves, for which $c \equiv 0 \bmod p$ and c can have at most 6 precise values.

Schoof's algorithm: ϕ restricted to $E[\ell]$ satisfies:

$$\pi^2 - c\pi + q \equiv 0 \bmod \ell$$

so we can find $c_\ell \equiv c \bmod \ell$ such that

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

in $\mathbb{K}[X, Y]/(E, f_\ell(X))$ and use CRT once $\prod \ell > 4\sqrt{q}$. Yields a $O(\log^8 q)$ **deterministic algorithm**.

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

Isogenies

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

Prop. $\phi \neq$ cte:

$$\begin{array}{rccc} \tilde{\phi} : & \mathbb{K}(E^*) & \hookrightarrow & \mathbb{K}(E) \\ & f & \mapsto & f \circ \phi \end{array}$$

$$\deg\phi = [\mathbb{K}(E) : \tilde{\phi}(\mathbb{K}(E^*))] < \infty$$

Rem. (in)separability.

Thm. There is a unique $\hat{\phi} : E^* \to E$, $\hat{\phi} \circ \phi = [m]$, $m = \deg\phi$.

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[dr, "{[m]}"'] & E^* \arrow[d, "\hat{\phi}"] \\ & E \end{tikzcd}$$

Examples

1.

$$[k](X,Y) = \left(\frac{A_k}{\psi_k^2}, \frac{B_k}{\psi_k^3}\right)$$

$$\deg_s[k] = k^2$$

2. $[i](X,Y) = (-X, iY)$ on $E : Y^2 = X^3 - X$,
$\deg[i] = 1 = \mathrm{Norm}(i)$.

3. $\pi(X,Y) = (X^q, Y^q), \mathbb{K} = \mathbb{F}_q, \deg_i \pi = q$.

4.

$$\begin{tikzcd}
E \arrow[r, "\sigma"] \arrow[dr, "{[p]}"'] & E^p \arrow[d, "\hat{\sigma}"] \\
& E
\end{tikzcd}$$

$$[p](X,Y) = (\hat{\sigma}_x(X^p, Y^p), \dots) = (\hat{\sigma}_x(X,Y)^p, \dots).$$

“Quotienting” E

Thm. If F is a finite subgroup of E, then there exists ϕ and E^* s.t.

$$\phi : E \to E^* = E/F, \quad \ker(\phi) = F.$$

Ex. $E : y^2 = x^3 + ax^2 + bx$, $F =< (0,0) >$;

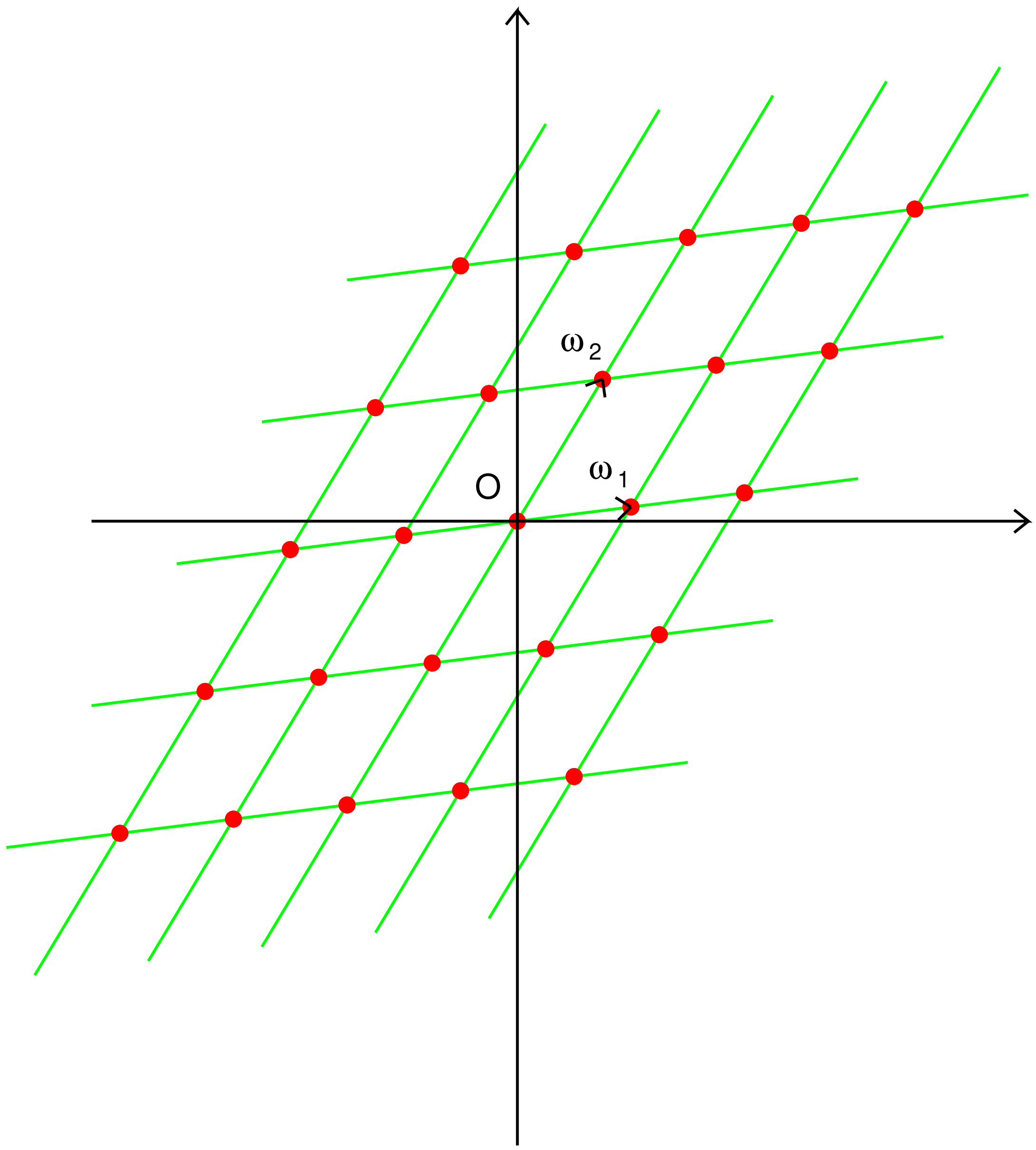
$$E^* : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X,$$

$$\phi : (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right).$$

More generally: Vélu’s formulas give

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

(case $\deg \phi$ odd.)



ω 2
ω 1
O

The case $\mathbb{K} = \mathbb{C}$

$$E = \mathbb{C}/L(\omega_1, \omega_2)$$

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) = \frac{1}{z^2} + \sum_{k=1}^{\infty} G_{2k}(L) z^{2k}$$

$$g_2(L) = 60 G_4(L), g_3 = 140 G_6(L)$$

$(\wp(z), \wp'(z))$ is a point on $E : y^2 = 4x^3 - g_2 x - g_3$.

Case $L(1, \tau)$:

$$\Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2, \quad j(\tau) = 12^3 g_2(\tau)^3 / \Delta(\tau).$$

Isogenies over $\mathbb{C}$

$$E : \mathbb{C}/L(\omega_1, \omega_2) \leftrightarrow g_2, g_3$$

Isogenous lattice: $L(\omega_1/\ell, \omega_2) \rightsquigarrow E^*$ which is ℓ-isogenous to E.

$$\ker(\phi) = \{(\wp(r\omega_1/\ell), \frac{1}{2}\wp'()), 1 \leq r < \ell\} \cup \{O_E\}.$$

$$\phi_x = \frac{\cdots}{\prod(X - \wp(r\omega_1/\ell))} = \frac{\cdots}{\prod'(X - \wp(r\omega_1/\ell))^2}.$$

$H(X)$ can be computed via $\sum_r \wp(r\omega_1/\ell)^k$ which live in $1/(2k+1)!\mathbb{Z}[g_2, g_3]$ (using q developments, modular forms, etc.)

Application to point counting

Suppose F is a subgroup of order ℓ of E:

$$\begin{tikzcd} E \arrow[r, "I"] \arrow[dr, "{[\ell]}"'] & E^* \arrow[d, "\hat{I}"] \\ & E \end{tikzcd}$$

$$I(X,Y) = (\frac{G}{H^2}, \ldots), \deg(H) = (\ell - 1)/2$$

$\ker(I) \subset E[\ell] \Rightarrow H(X) \mid f_\ell(X)$ in $\mathbb{K}[X]$.

Schoof's algorithm on a degree $O(\ell)$ polynomial.

Pb. When does such an F exist over $\mathbb{K}$?

Elkies's idea

Consider $\pi : (X,Y) \mapsto (X^q, Y^q)$ and its restriction π_ℓ to $E[\ell]$:

$$\pi_\ell^2 - t\pi_\ell + q = 0,$$

$$\Delta = t^2 - 4q.$$

If $\left(\frac{\Delta}{\ell}\right) = +1$, then

$$\mathrm{Mat}(\pi_\ell) \simeq \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \Leftrightarrow \exists F, \pi(F) = F \Leftrightarrow F$$

is a cyclic subgroup of order ℓ, defined over $\mathbb{K}$.

Clon. If $\left(\frac{\Delta}{\ell}\right) = +1$, f_ℓ has a factor of degree $(\ell - 1)/2$.

Pb. How do we know that $\left(\frac{\Delta}{\ell}\right) = +1$?

Modular polynomials

Thm. $\exists \Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ s.t. E and E^* are ℓ-isogenous over $\mathbb{K}$ iff $\Phi_\ell(j(E), j(E^*)) = 0$.

Thm.

$$\Phi_\ell(X, j(E)) = \begin{cases} (1)(1)(r) \cdots (r) & \text{if } \left(\frac{\Delta}{\ell}\right) = +1, \\ (r) \cdots (r) & \text{if } \left(\frac{\Delta}{\ell}\right) = -1, \end{cases}$$

Clon. $\left(\frac{\Delta}{\ell}\right) = +1$ **iff** $\Phi_\ell(X, j(E))$ **has two distinct roots over** $\mathbb{K}$.

Elkies's algorithm

repeat

1. factor $\Phi_\ell(X, j(E))$ over $\mathbb{K}$.
2. if type = $(1)(1)(r)\cdots(r)$:

   2.1 build E^*;

   2.2 build I;

   2.3 find $t \bmod \ell$;

until $\prod_{\ell \text{ good}} \ell > 4\sqrt{q}$.

Thm. $O(\log^6 q)$ probabilistic.

Pbs. Solve 2.1 and 2.2:

1. $p \gg \ell$: Elkies, Atkin;
2. $p = 2$: Couveignes, Lercier;
3. other cases.

Elkies's algorithm: the case p large

If $\mathbb{K} = \mathbb{C}$, then $E = \mathbb{C}/L(\omega_1, \omega_2)$ and $E^* = \mathbb{C}/(\omega_1/\ell, \omega_2)$.

- One can build Ψ_m using series operations: Φ^c, Φ^*, Φ^Θ (Atkin), Φ^M (Müller), for $\ell \leq 1000$.
- One can find the equation of E^* using rational formulas.
- $F = \{O_E\} \cup \{(\wp(r\omega_1/\ell), \frac{1}{2}\wp'(r\omega_1/\ell)), 1 \leq r \leq \ell - 1\}$.
- Use recurrence relations for the denominator of I or Stark's algorithm: develop $\wp^*(z) = G(\wp(z))/H(\wp(z))^2$.
- Computing I takes $O(\ell)$ steps and uses $O(\ell)$ memory.
- We need about ℓ coefficients of $\wp$ and $\wp^*$. The method works as well when $p > 0$, provided $p > 3$ and $p \gg \ell$.
- Very efficient in practice: p with 500 decimal digits.

V. The case p small

Pb: p small (say 2), two ℓ isogenous curves E and E^* are given, we look for $I(X) = G(X)/H(X)^2$.

A) CouveignesI.

B) Lercier.

C) CouveignesII.

Formal group

$$t = -X/Y, s = -1/Y$$

$$F(t,s) := t^3 + a_1 ts + a_2 t^2 s + a_3 s^2 + a_4 ts^2 + a_6 s^3 - s = 0.$$

$$s = \mathcal{S}(t) = t^3 + a_1\, t^4 + (a_1^2 + a_2)t^5 + O(t^6).$$

$$Y = -\frac{1}{s} = -t^{-3} + a_1 t^{-2} + a_2 t^{-1} + a_3 + (a_1 a_3 + a_4)t + O(t^2)$$

$$X = \frac{t}{s} = -tY = t^{-2} - a_1 t^{-1} - a_2 - a_3 t - (a_1 a_3 + a_4)t^2 + O(t^3)$$

$$Z = \frac{1}{X} = t^2 + a_1 t^3 + (a_1^2 + a_2)t^4 + O(t^5)$$

$$t_3 = F_a(t_1, t_2) = t_1 + t_2 - a_1 t_1 t_2 - a_2(t_1^2 t_2 + t_1 t_2^2)$$

$$-(2a_3 t_1^3 t_2 - (a_1 a_2 - 3a_3)t_1^2 t_2^2 + 2a_3 t_1 t_2^3) + \dots$$

$$[2]t_1 = 2\, t_1 - a_1\, t_1^2 - 2\, a_2\, t_1^3 + (a_1\, a_2 - 7\, a_3)\, t_1^4 + \cdots$$

Th. $[p](t) = \Psi_{p,E}(t)^p = c_p(E)t^p + O(t^p)$.

Th. $\mathrm{Norm}_{\mathbb{K}/\mathbb{F}_p} \equiv \mathrm{Tr}_{\mathbb{K}/\mathbb{F}_p}(\phi) \bmod p$.

Csq. we can assume $c_p(E) = c_p(E^*)$.

Ex. $c_2([a_1, a_2, a_3, a_4, a_6]) = a_1$, $c_3([a_2, a_6]) = a_2$.

CouveignesI

$$\begin{aligned} E: \quad Y^2 + a_1XY + a_3Y &= X^3 + a_2X^2 + a_4X + a_6, \\ E^*: \quad Y^2 + a_1^*XY + a_3^*Y &= X^3 + a_2^*X^2 + a_4^*X + a_6^*, \end{aligned}$$

$$\begin{array}{rccc} I: & E & \longrightarrow & E^* \\ & (X,Y) & \longmapsto & \left(\dfrac{G(X)}{H^2(X)}, \dfrac{J(X,Y)}{H^3(X)}\right), \end{array}$$

where $\deg(G) = \ell$, $\deg(H) = (\ell - 1)/2$.

$$I : X \mapsto X^* = I(X) = \frac{G(X)}{H(X)^2}$$

$$X \mapsto 1/Z$$

$$\hat{I} : Z \mapsto Z^* = \hat{I}(Z) = Z\frac{\hat{H}^2(Z)}{\hat{G}(Z)}$$

with $\hat{G}(Z) = Z^\ell G(1/Z)$, $\hat{H}(Z) = Z^{(\ell-1)/2}H(Z)$.

$$\hat{I}(Z) = \sum_{k=0}^{\infty} \alpha_k Z^k \leftrightarrow \hat{I}(Z(t)) = \sum_k \alpha_k Z(t)^k = Z^*(t)$$

is completely characterized by $\alpha_0, \alpha_2, \ldots, \alpha_{2\ell-1}$ (Berlekamp-Massey).

Couveignes's idea: find a series that looks like an isogeny and then check whether it comes from a fraction the denominator of which has degree ℓ.

Morphisms of formal groups

$$\begin{array}{rrcl}\mathcal{E}: & t^3+a_1ts+a_2t^2s+a_3s^2+a_4ts^2+a_6s^3-s & = & 0,\\ \mathcal{E}^*: & t^3+a_1^*ts+a_2^*t^2s+a_3^*s^2+a_4^*ts^2+a_6^*s^3-s & = & 0.\end{array}$$

$\forall\, P_1=(t_1(\tau),s_1(\tau))$ and $P_2=(t_2(\tau),s_2(\tau))$ of $\mathcal{E}$:

$$\mathcal{M}(P_1\oplus P_2)=\mathcal{M}(P_1)\oplus\mathcal{M}(P_2)$$

$$\mathcal{U}(t)=\sum_{i\geq 1}u_it^i,$$

$$\mathcal{M}(t(\tau),s(\tau))=(\mathcal{U}(t(\tau)),\mathcal{S}^*(\mathcal{U}(t(\tau))))$$

$$\mathcal{U}(t_1\oplus t_2(\tau))=\mathcal{U}(t_1(\tau))\oplus\mathcal{U}(t_2(\tau)).$$

Th. The set of morphisms from $\mathcal{E}$ to $\mathcal{E}^*$ is a $\mathbb{Z}_p$-module of rank 1.

Process: find any non-trivial morphism $\mathcal{U}$ and then look for some p-adic N s.t. $\mathcal{W}=[N]\circ\mathcal{U}$ comes from an isogeny.

Rem. since 2ℓ terms of $\hat{I}(Z)$ are needed, and since $Z=s/t=t^2+O(t^3)$, we need $\mathcal{L}=4\ell$ terms of $\mathcal{W}$.

Finding morphisms

Assume $u_1, \ldots, u_{i-1}$ are known.

1st case: $i \neq p^k$:

$$\mathcal{U}(\tau \oplus A\tau) = \mathcal{U}(\tau) \oplus \mathcal{U}(A\tau)$$

$$\tau \oplus A\tau = (1 + A)\tau + O(\tau^2)$$

$$\mathcal{U}(\tau \oplus A\tau) = \sum_{k=1}^{\infty} u_k((1 + A)\tau + O(\tau^2))^k$$

u_i appears as $(1 + A)^i u_i +$ terms depending only on $u_1, u_2, \ldots, u_{i-1}$

$$\mathcal{U}(\tau) \oplus \mathcal{U}(A\tau) = \mathcal{U}(\tau) + \mathcal{U}(A\tau) + P(\mathcal{U}(\tau), \mathcal{U}(A\tau))$$

u_i appears as $(1 + A^i)u_i +$ terms depending only on $u_1, u_2, \ldots, u_{i-1}$

$$u_i\left((1 + A)^i - 1 - A^i\right) + e_i(A, u_1 \ldots, u_{i-1}) = 0,$$

If $(1 + A)^i \neq 1 + A^i$, we get u_i.

2nd case: $i = p^k$

$$\mathcal{U}([p]\tau) = [p]^*(\mathcal{U}(\tau))$$

$$\tilde{\mathcal{U}}(t) = \sum_{k=1}^{\infty} \tilde{u}_k t^k, \tilde{u}_k = \sqrt[p]{u_k}$$

$$\tilde{\mathcal{U}}(\tau) \circ \Psi(\tau) = \Psi^*(\tau) \circ \mathcal{U}(\tau)$$

$$\sqrt[p]{c^*} u_i - c^{p^{e-1}} \tilde{u}_i + f_i(\tilde{u}_1, \ldots, \tilde{u}_{i-1}) = 0,$$

$$\eta = c^{(p^e-1)/(p-1)}$$

$$\left(\frac{u_i}{\eta}\right) - \left(\frac{u_i}{\eta}\right)^p = f_i'.$$

Ex. $cu_1^p = u_1 c^* \Rightarrow u_1^p = u_1$

Prop. Let $p^r < \mathcal{L} < p^{r+1}$. There are at most p^{r+1} distinct series. Moreover $u_1 \neq 0$. There are $p^r(p-1)$ (truncated) morphisms.

Enumerating all morphisms

$$\mathcal{W} = [N] \circ \mathcal{U}$$

$$N = \sum_{i=0}^{\infty} n_i p^i$$

$$p^r < \mathcal{L} < p^{r+1}$$

$$[N] \circ \mathcal{U} = \bigoplus_{i=0}^{r} [n_i] \circ ([p^i] \circ \mathcal{U}) \oplus \sum_{i>r} [n_i] \circ ([p^i] \circ \mathcal{U}).$$

$\rightarrow$ it is enough to test $[N] \circ \mathcal{U}$ for $N < p^{r+1}$ and $n_0 \neq 0$.

Rem. $[p^{r+1} - N] \circ \mathcal{U} = [-N] \circ \mathcal{U} + O(t^{p^{r+1}}) \rightarrow$ consider only $N < p^{r+1}/2$ and N prime to p.

The algorithm in brief

procedure ComputeIsogeny($\ell, \mathcal{E}, \mathcal{E}^*$)

1. compute a generator $\mathcal{U}$ of the set of morphisms between $\mathcal{E}$ and $\mathcal{E}^*$;
2. **for** $N = 1$ to $p^{r+1}/2$ and N prime to p **do**
   (a) compute
   $$(\mathcal{M}(t), \mathcal{S}^*(\mathcal{M}(t))) = [N] \circ (\mathcal{U}(t), \mathcal{S}(\mathcal{U}(t)));$$
   (b) if $\mathcal{M}$ comes from an isogeny then stop.

Th. Couveignes's algorithm takes time $O(\ell^3)$ and space $O(\ell^2)$.

See Lercier & Morain, *Math. Comp.*, to appear.

An example

$$\mathbb{K} = \mathbb{F}_{2^{11}} = \mathbb{F}_2[T]/(T^{11} + T^2 + 1)$$

$$E : Y^2 + XY = X^3 + a, E^* : Y^2 + XY = X^3 + b$$

$$a = T^4 + T^2 + T = \overline{22},$$

$$b = T^{10}+T^9+T^6+T^5+T^4+T^3+T^2+T+1 = \overline{1663}$$

$$\ell = 5$$

$$I(X) = \frac{G(X)}{H(X)^2}$$

where $\deg(G(X)) = 5, \deg(H(X)) = 2$.

$$A = \overline{2}$$

$$(\mathcal{U}(t), \mathcal{S}(\mathcal{U}(t))) = (t + O(t^2), t^3 + O(t^4)).$$

u_2: $\mathcal{U}([2]t) = [2]^*(\mathcal{U}(t))$ leads to

$$\sqrt{u_2}^2 + \sqrt{u_2} = 0.$$

We take $u_2 = 0$.

u_3: $\mathcal{U}(t \oplus At) = \mathcal{U}(t) \oplus \mathcal{U}(At)$ which yields the unique value $u_3 = 0$.

$$\sqrt{u_4}^2 + \sqrt{u_4} + \overline{1194} = 0.$$

and we take $u_4 = \overline{1820}$.

$$\ldots$$

$$\mathcal{U}(t) = t + \overline{1820}t^4 + \overline{1820}t^5 + \overline{1641}t^7 + \overline{1280}t^8 + \overline{873}t^9 + \overline{783}t^{10}$$
$$+ \overline{1746}t^{11} + \overline{360}t^{12} + \overline{884}t^{13} + \overline{1082}t^{14} + \overline{987}t^{15} + \overline{522}t^{16}$$
$$+ \overline{1556}t^{17} + \overline{1365}t^{18} + \overline{171}t^{19} + \overline{702}t^{20} + \overline{62}t^{21} + O(t^{22}),$$

and

$$\mathcal{S}(\mathcal{U}(t)) = t^3 + t^4 + t^5 + \overline{1821}t^6 + \overline{1821}t^7 + \overline{1821}t^8 + \overline{1662}t^9 + \overline{541}t^{10}$$
$$+ \overline{872}t^{11} + \overline{678}t^{12} + \overline{260}t^{13} + \overline{193}t^{14} + \overline{1407}t^{15} + \overline{868}t^{16}$$
$$+ \overline{1370}t^{17} + \overline{126}t^{18} + \overline{1244}t^{19} + \overline{1295}t^{20} + \overline{606}t^{21} + \overline{1473}t^{22} + \overline{791}t^{23} + O(t^{24}).$$

$$[11] \circ \mathcal{U}(t) = t + t^2 + t^3 + \overline{1820}t^4 + \overline{1820}t^5 + \overline{1820}t^6 + \overline{373}t^7 + \overline{1140}t^8$$

$$+\overline{1140}t^9+\overline{260}t^{10}+\overline{1231}t^{11}+\overline{1205}t^{12}+\overline{1291}t^{13}+\overline{305}t^{14}$$

$$+\overline{175}t^{15}+\overline{480}t^{16}+\overline{113}t^{17}+\overline{1536}t^{18}+\overline{1205}t^{19}+\overline{274}t^{20}+\overline{1337}t^{21}+O(t^{22}),$$

Berlekamp-Massey:

$$I(X(t)) = \frac{X^5(t) + \overline{1641}X^3(t) + \overline{419}X(t)}{(X^2(t) + \overline{1821}X(t) + \overline{1958})^2}$$

$$G(X) = X(X^4 + \overline{1641}X^2 + \overline{419}),$$

$$H(X) = X^2 + \overline{1821}X + \overline{1958}.$$

B) Lercier's algorithm

Motivation: CouveignesI too slow, too much memory involved (huge series computations).

$$p = 2, E : Y^2 + XY = X^3 + a, E^* : Y^2 + XY = X^3 + b$$

Prop. $I(X) = G(X)/H(X)^2$,
$G = X(H^2 + H'(XH)')$.

Proof: Use Vélu's formulas. $\Box$

Coro. $G(X) = XL(X)^2$.

$$\alpha = \sqrt[4]{a}, \beta = \sqrt[4]{b}, d = (\ell - 1)/2$$

Prop. $L(X) = \lambda X^d H(\sqrt{a}/X)$ where
$\lambda = \sqrt{\beta/\alpha}\alpha^{-d}$.

Proof: The only point of order 2 on E (resp. E^*) is $P = (0, \sqrt{a})$ (resp. $P^* = (0, \sqrt{b})$):

$$P \oplus M = (0, \sqrt{a}) \oplus (X, Y) = (\sqrt{a}/X, \dots)$$

$$I(P \oplus M) = P^* \oplus I(M). \Box$$

Prop. Let $\hat{L}(X)$ (resp. $\hat{H}(X)$) denotes the polynomial $\sqrt{L(X^2)}$ (resp. $\sqrt{H(X^2)}$). Then

(*) $X^d\hat{H}(X+\sqrt{a}/X) = H(X)L(X)$;

(**)
$(X+\alpha)X^d\hat{L}(X+\sqrt{a}/X) = XL(X)^2+\beta H(X)^2$.

Proof: Use $I([2]M) = [2]I(M)$. □

$$L(X) = \sum_{i=0}^{d} p_i^2 X^i, H(X) = \sum_{i=0}^{d} q_i^2 X^i$$

Coro.

(i) $p_d = q_d$.

(ii) For all i, one has $q_i = \lambda\alpha^{-i}p_{d-i}$.

(iii) $p_d^4 + p_d = 0$ (*hint:* use $(**)$).

Prop. Take $p_d = q_d = 1$. Then

$$p_{d-1} = \alpha+\beta, p_{d-2} = p_{d-1}^4 + \alpha p_{d-1} + d\alpha^2,$$

$$p_0^4 = \alpha^{2d} + \alpha^{2d-1}p_{d-1}.$$

$+$ cf. Bluher.

Idea: solve the polynomial system coming from $(**)$, in a clever way, using $(*)$. Can be improved using Vélu's formulas.

Analysis: heuristically, time is $O(\ell^3)$ with a much better constant; space is $O(\ell)$.

In practice: considerably faster than Couveignes's first algorithm: 400 times faster for computing isogenies for $\mathbb{K} = \mathbb{F}_{2^{300}}$, resulting in a speed-up of 5 on the total running time for the complete SEA algorithm.

$\mathbb{F}_{2^{155}}$	86 sec
$\mathbb{F}_{2^{196}}$	308 sec
$\mathbb{F}_{2^{300}}$	2851 sec

(Alpha 266 MHz)

The same example again

$$I(X) = \frac{G(X)}{H(X)^2} = \frac{XL^2(X)}{H(X)^2},$$

with $\deg(L(X)) = 2$ and $\deg(H(X)) = 2$.

$$\alpha = \sqrt[4]{a} = \overline{571}, \beta = \sqrt[4]{b} = \overline{859}$$

$$L(X) = \sum_{i=0}^{d} p_i^2 X^i$$

$$p_0 = \sqrt[4]{\alpha^{2d} + \alpha^{2d-1} p_{d-1}} = \overline{1519},$$

$$p_1 = \alpha + \beta = \overline{352},$$

$$p_2 = \overline{1}.$$

$$L(X) = X^2 + \overline{1194}X + \overline{1746}$$

$$H(X) = X^2 + \overline{1821}X + \overline{1958}.$$

Very important remark: This case is completely misleading!!!

C) CouveignesII

Prop.

$$\begin{tikzcd} E \arrow[r, "\pi"] \arrow[dr, "{[p]}"'] & E^p \arrow[d, "\hat{I}"] \\ & E \end{tikzcd}$$

$$[p](X,Y) = (F_p(X)^p, G_p(X,Y)^p)$$

Coro.

$$f_{p^i}(X) = \tilde{f}_{p^i}^{p^i}, \deg \tilde{f}_{p^i} = d_i = p^{i-1}(p-1)/2 \text{ or } 2^{i-1}$$

Assumption: $\tilde{f}_{p^k}(X)$ has all its roots over $\mathbb{K}$.

Idea: I sends the p^k-torsion of E on the p^k-torsion of E^*:

$$I([m]P) = [m]P^*$$

$$I(x_m) = x_m^*$$

Let $A(X)$ s.t. $A(x_m) = x_m^*$ for all m, $1 \leq m \leq d_k$.

Then

$$I(X) \equiv A(X) \bmod \tilde{f}_{p^k}(X)$$

If $d_k > 2\ell$, recover H via the euclidean algorithm:

$$\begin{aligned}
\tilde{f}_{p^k}(X) &= q_1(X)A(X) + r_1(X), \deg(r_1) < \deg(A),\\
A(X) &= q_2(X)r_1(X) + r_2(X),\\
\cdots &= \cdots\\
r_i(X) &= q_{i+2}(X)r_{i+1}(X) + r_{i+2}(X), i \geq 1
\end{aligned}$$

$$u_{-1} = 1, v_{-1} = 0, u_0 = 0, v_0 = 1$$

$$u_{i+2}(X) = u_i(X) - q_{i+2}(X)u_{i+1}(X),$$

$$v_{i+2}(X) = v_i(X) - q_{i+2}(X)v_{i+1}(X),$$

$$r_i(X) = \tilde{f}_{p^k}(X)u_i(X) + A(X)v_i(X)$$

When $\deg(v_i) = \ell - 1$, one has

$$A(X)v_i(X) \equiv r_i(X) \bmod \tilde{f}_{p^k}(X)$$

and if v_i is a square, we let $H = v_i^2$.

Rem. In general, the p^k-division is not rational and the interpolation part must be done with some care.

Prop. Complexity should be time $O(\ell^{2+\epsilon})$, space $O(\ell)$.

Prop. Artin-Schreier approach of Couveignes: $O(n\mathcal{M}(\ell))$.

Again, the same example

$$E : Y^2 + XY = X^3 + \overline{22}, E^* : Y^2 + XY = X^3 + \overline{1663}$$

$$k = 2 + \lceil \log_2 \ell \rceil = 5, d_k = 2^{5-1} > 2 \times 5$$

$$P = [\overline{355}, \overline{735}, \overline{1}], P^* = [\overline{632}, \overline{974}, \overline{1}]$$

m	1	2	3	4	5	6	7	8
x_m	$\overline{355}$	$\overline{498}$	$\overline{1954}$	$\overline{1182}$	$\overline{59}$	$\overline{1210}$	$\overline{1059}$	$\overline{571}$
m	9	10	11	12	13	14	15	16
x_m	$\overline{471}$	$\overline{1735}$	$\overline{1491}$	$\overline{2011}$	$\overline{1734}$	$\overline{1943}$	$\overline{1980}$	$\overline{0}$

m	1	2	3	4	5	6	7	8
x_m^*	$\overline{632}$	$\overline{759}$	$\overline{1151}$	$\overline{1769}$	$\overline{1898}$	$\overline{1949}$	$\overline{828}$	$\overline{859}$
m	9	10	11	12	13	14	15	16
x_m^*	$\overline{882}$	$\overline{1370}$	$\overline{1814}$	$\overline{695}$	$\overline{459}$	$\overline{94}$	$\overline{183}$	$\overline{0}$

Lagrange's formulas:

$$A(X) = \overline{1488}X^{15} + \overline{1726}X^{14} + \overline{1429}X^{13} + \overline{326}X^{12} + \overline{1934}X^{11}$$

$$+\overline{607}X^{10} + \overline{1661}X^9 + \overline{998}X^8 + \overline{760}X^7 + \overline{1460}X^6$$

$$+\overline{1070}X^5 + \overline{1580}X^4 + \overline{768}X^3 + \overline{1530}X^2 + \overline{1447}X.$$

Using Euclid's algorithm, we find

$$v_2 = \overline{1207}X^4 + \overline{1934}X^2 + \overline{1396} = C(X^2 + \overline{1821}X + \overline{1958})^2.$$

Conclusion

- $p \gg \ell$: one fast algorithm.
- $p = 2$: three algorithms, isogeny computations are no longer a limitation of the Schoof-Elkies-Atkin algorithm (cf. Lercier's 2^{1663} record).
- p small: combination of the algorithms, take the best part of each of them, cf. Lercier's thesis.
- CouveignesII: what is the impact of fast polynomial operations?
- $n \approx \log p$????