

# Fast algorithms for computing isogenies between elliptic curves

A. Bostan, F. Morain, B. Salvy, É. Schost

Laboratoire d'Informatique de l'École polytechnique



Séminaire Algo, May 29th, 2006

1/39

## Motivations

- original one: SEA;
- later: Kohel, Galbraith, Fouquet/FM (volcanoes);
- more recently: Galbraith/Hess/Smart; Smart; Jao/Miller/Venkatesan; Teske; Rostovtsev/Stolbunov.

### Bibliography:

- **green book** (Blake Seroussi Smart). Don't forget to read the original papers, when available. . .
- Gathen & Gerhard, etc.

2/39

## Plan

- I. Elliptic curves and isogenies.
- II. Fast series computations.
- III. Computing the Weierstrass  $\wp$ -function.
- IV. Previous algorithms for computing isogenies.
- V. Our fast variant.
- VI. Benchmarks.

3/39

## I. Elliptic curves and isogenies

$$E : y^2 = x^3 + Ax + B \text{ over } \mathbf{K}, \text{char}(\mathbf{K}) \notin \{2, 3\}.$$

**Def.** (torsion points) For  $n \in \mathbb{N}$ ,  $E[n] = \{P \in E(\overline{\mathbf{K}}), [n]P = O_E\}$ .

### Division polynomials:

$$[n](x, y) = \left( \frac{\phi_n(x, y)}{\psi_n(x, y)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3} \right)$$

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$

$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$$

In  $\mathbf{K}[x, y]/(y^2 - (x^3 + Ax + B))$ , one has:

$$\psi_{2m+1}(x, y) = f_{2m+1}(x), \quad \psi_{2m} = 2yf_{2m}(x)$$

for some  $f_m(x) \in \mathbf{K}[A, B, x]$ .

4/39

$$f_n(x) = \begin{cases} \psi_n(x, y) & \text{for } n \text{ odd} \\ \psi_n(x, y)/(2y) & \text{for } n \text{ even} \end{cases}$$

$$f_{-1} = -1, \quad f_0 = 0, \quad f_1 = 1, \quad f_2 = 1$$

$$f_3(x, y) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$f_4(x, y) = x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3$$

$$f_{2n} = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2)$$

$$f_{2n+1} = \begin{cases} f_{n+2}f_n^3 - f_{n+1}^3f_{n-1}(16y^4) & \text{if } n \text{ is odd} \\ (16y^4)f_{n+2}f_n^3 - f_{n+1}^3f_{n-1} & \text{otherwise.} \end{cases}$$

$$\deg(f_n(x)) = \begin{cases} (n^2 - 1)/2 & \text{if } n \text{ is odd} \\ (n^2 - 4)/2 & \text{otherwise.} \end{cases}$$

**Thm.**  $P = (x, y) \in E[\ell] \iff [2]P = O_E$  or  $f_\ell(x) = 0$ .

5/39

## How does an isogeny look like?

Extending Vélú, Dewaghe. Let

$$D(x) = \prod_{Q \in F^*} (x - x_Q) = x^{\ell-1} - \sigma x^{\ell-2} + \dots$$

where  $\sigma = \sum_{Q \in F^*} x_Q$ .

**Rem.** When  $\ell$  is odd,  $D(x) = g(x)^2$ .

**Fundamental proposition.** The isogeny  $I$  can be written as

$$I(x, y) = \left( \frac{N(x)}{D(x)}, y \left( \frac{N(x)}{D(x)} \right)' \right),$$

$$\begin{aligned} \frac{N(x)}{D(x)} &= \ell x - \sigma - (3x^2 + A) \frac{D'(x)}{D(x)} - 2(x^3 + Ax + B) \left( \frac{D'(x)}{D(x)} \right)' \\ &= \ell x - \sigma - 2\sqrt{x^3 + Ax + B} \left( \sqrt{x^3 + Ax + B} \frac{D'(x)}{D(x)} \right)' \end{aligned}$$

7/39

## Isogenies

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

**First examples**

1. Separable:

$$[k](x, y) = \left( \frac{\phi_k}{\psi_k^2}, \frac{\omega_k}{\psi_k^3} \right)$$

2. Complex multiplication:  $[i](x, y) = (-x, iy)$  on  $E : y^2 = x^3 - x$ .

3. Inseparable:  $\varphi(x, y) = (x^p, y^p)$ ,  $\mathbf{K} = \mathbb{F}_p$ .

**In the sequel: only separable isogenies.**

**Thm.** If  $F$  is a finite subgroup of  $E(\bar{\mathbf{K}})$ , then there exists  $\phi$  and  $\tilde{E}$  s.t.

$$\phi : E \rightarrow \tilde{E} = E/F, \quad \ker(\phi) = F.$$

6/39

## Proof of the fundamental proposition

Vélú gives:

$$x_{I(P)} = x_P + \sum_{Q \in F^*} (x_{P+Q} - x_Q).$$

Injecting the group law:

$$I_x(x) = x + \sum_{Q \in F^*} \left( \frac{3x_Q^2 + A}{x - x_Q} + 2 \frac{x_Q^3 + Ax_Q + B}{(x - x_Q)^2} \right),$$

which can be rewritten as

$$I_x(x) = x + \sum_{Q \in F^*} \left( x - x_Q - \frac{3x^2 + A}{x - x_Q} + 2 \frac{x^3 + Ax + B}{(x - x_Q)^2} \right).$$

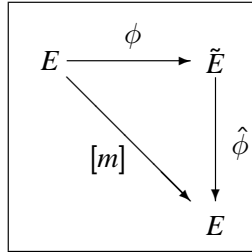
Finish using

$$\sum_{Q \in F^*} \frac{1}{x - x_Q} = \frac{D'(x)}{D(x)}, \quad \sum_{Q \in F^*} \frac{1}{(x - x_Q)^2} = - \left( \frac{D'(x)}{D(x)} \right)' \quad \square$$

8/39

## Dual isogeny

**Thm. (dual isogeny)** There is a unique  $\hat{\phi} : \tilde{E} \rightarrow E$ ,  $\hat{\phi} \circ \phi = [m]$ ,  $m = \deg \phi$ .



**Application to SEA:**  $D$  will be a divisor of  $\psi_m^2$  (resp.  $g \mid f_\ell$ ).

9/39

## Last but not least: Elliptic curves over $\mathbb{C}$

When  $\mathbf{K} = \mathbb{C}$ ,  $E = \mathbb{C}/L = \mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z})$ ,  $E : y^2 = x^3 + Ax + B$  can be parametrized using the Weierstrass function:

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

where  $c_1 = -A/5$ ,  $c_2 = -B/7$ .

**Useful remark:** if  $E$  and  $\tilde{E}$  are  $\ell$ -isogenous, then

$$\tilde{\wp} = \frac{N}{D} \circ \wp.$$

**Fact.** The curve  $\tilde{E} = \mathbb{C}/(\omega_1/\ell, \omega_2)$  is  $\ell$ -isogenous to  $E$ . The associated kernel is:

$$F = \{O_E\} \cup \left\{ \left( \wp(r\omega_1/\ell), \frac{1}{2}\wp'(r\omega_1/\ell) \right), 1 \leq r \leq \ell - 1 \right\}.$$

10/39

## Facts: the Galois point of view

We can put it this way: rewrite

$$f_\ell(X) = \prod_{1 \leq r, s \leq \ell-1} (X - \wp((r\omega_1 + s\omega_2)/\ell)).$$

The factor we build is:

$$D(x) = \prod_{1 \leq r \leq \ell-1} (X - \wp(r\omega_1/\ell))$$

and all its coefficients are in  $\mathbf{K}[\sigma]$  where  $\sigma = \sum_r \wp(r\omega_1/\ell)$ .

$$\begin{array}{c} \mathbf{K}[x]/(f_\ell(x)) \\ | \\ \mathbf{K}[x]/(M_\sigma(x)) \\ | \\ \mathbf{K}[x] \end{array} \quad \begin{array}{l} \ell - 1 \\ \ell + 1 \end{array}$$

If  $\sigma$  is rational over  $\mathbf{K}$ , then  $D(x)$  will have rational coefficients.

**Modular equation:**  $M_\sigma(x) = \Phi_\ell(x, j(E))$ .

11/39

## Application to SEA

**Key point of Elkies:** find prime  $\ell$  for which there exists a rational  $\ell$ -isogeny from  $E$  (detected via modular polynomials  $\Phi_\ell(X, Y)$ ; happens with proba  $1/2$ ). Then  $g(x) \mid f_\ell(x)$  with  $\deg(g) = (\ell - 1)/2$ .

**Black box:** imagine we have a way to compute  $(\tilde{E}, \sigma)$  given  $\mathbf{K}$ ,  $E$ ,  $\ell$ , (some)  $\Phi_\ell$ .

In brief, over  $\mathbb{F}_p$  ( $p \gg \ell$ ), do as if we were over  $\mathbb{C}$ , use modular equations to build  $\tilde{E}$  and  $\sigma$ .

(see FM's 1994/03/07 talk...)

In the remaining part of the talk: compute  $D(x)$  as fast as possible.

12/39

## Examples

**Ex 1.**  $E : y^2 = x^3 + bx, F = \langle (0, 0) \rangle;$

$$\tilde{E} : y^2 = x^3 - 4bx,$$

$$\phi : (x, y) \mapsto \left( \frac{x^3 + bx}{x^2}, y \frac{x^2 - b}{x^2} \right).$$

**A curiosity:**  $E : y^2 = x^3 + x + 3$  defined over  $\mathbb{F}_{1009}$ ;  $E$  is 6-isogenous to

$$\tilde{E} : y^2 = x^3 + 830x + 82$$

and  $\sigma = 739$  (formulas for prime  $\ell$  valid here too!!!) for which

$$\frac{N(x)}{D(x)} = \frac{x^6 + 270x^5 + 325x^4 + 566x^3 + 382x^2 + 555x + 203}{x^5 + 270x^4 + 289x^3 + 659x^2 + 533x + 399}.$$

The denominator factors as

$$(x - 66)(x - 23)^2(x - 818)^2.$$

$x = 66$  is the abscissa of a point of 2-torsion;

$23$  is the abscissa of a point of 3-torsion;

$818$  is the abscissa of a primitive point of 6-torsion.

13/39

## II. Fast series computations

**Fundamental references:** Brent and Kung; Gathen & Gerhard.  
Classical stuff: the **multiplication time** function  $M$  satisfies the following classical super-linearity inequalities for all  $n$  and  $n'$ :

$$\frac{M(n)}{n} \leq \frac{M(n')}{n'} \quad \text{if } n \leq n' \quad \text{and} \quad M(nn') \leq n^2 M(n'),$$

which implies:

$$M(1) + M(2) + M(4) + \dots + M(2^i) \leq 2M(2^i).$$

$\Rightarrow$  all algorithms based on Newton's iteration below have complexity in  $O(M(n))$ .

14/39

**Easy facts:** given a series  $A(z) = a_0 + a_1z + \dots + O(z^n)$ , computing  $\int A(z) dz$  or  $A'(z)$  is possible in  $O(n)$ .

**Less easy facts:** computing  $A(z)B(z)$ ,  $1/A(z)$ ,  $\log A(z)$ ,  $\exp(A(z))$  may be computed in  $O(M(n))$ ; use Newton when needed. Idem for recovering a polynomial  $f$  of degree  $n$  from its first  $n$  power sums  $p_1, \dots, p_n$  (Schönhage), since

$$z^n f\left(\frac{1}{z}\right) = \exp_{n+1}\left(-\sum_{i=1}^n \frac{p_i}{i} z^i\right).$$

**First order linear differential equation:** with  $R(0) = r_0$ , one solves  $R'(z) + F(z)R(z) \equiv G(z) \pmod{z^n}$  as:

$$H(z) = \exp\left(\int_0^z F(u) du\right), R(z) = \left(\frac{1}{H(z)}\right) \left(r_0 + \int_0^z G(u)H(u) du\right)$$

in time  $O(M(n))$ .

15/39

## Application: expanding $\wp$

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

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

With

$$A = -5c_1, B = -7c_2$$

then  $(\wp(z), \wp'(z)/2)$  is a point on  $E : y^2 = x^3 + Ax + B$ .

By exploiting  $\wp'' = 6\wp^2 + 2A$ , one gets for  $k \geq 3$ :

$$c_k = \frac{3}{(k-2)(2k+3)} \sum_{h=1}^{k-2} c_h c_{k-1-h}$$

**Cost:** computing  $\wp$  to order  $n$  costs  $O(n^2)$ .

16/39

## An $O(M(d))$ method for $\wp$

**First idea:** (sketch) put  $\wp(z) = Q(z)/z^2$ , which gives

$$z^2 Q'^2 - 4zQQ' - 4Q^3 + 4Q^2 - 4Az^4Q - 4Bz^6 = 0. \quad (1)$$

$$Q_0(z) = 1 - \frac{A}{5}z^4 - \frac{B}{7}z^6$$

is a solution of (1) at order  $s = 8$ . With  $Q(z) = Q_0 + z^8R(z)$ :

$$R'(z) + F(z)R(z) \equiv G(z) \pmod{z^8}$$

where:

$$F(z) = 5 \frac{6Bz^6 + 7Az^4 + 63}{(10Bz^6 + 7Az^4 + 35)z}$$

$$G(z) = \frac{1}{175} \frac{105A^2Bz^6 + 49A^3z^4 + 125B^2z^4 + 525ABz^2 + 735A^2}{(10Bz^6 + 7Az^4 + 35)z}$$

$$R(z) = \frac{1}{75}A^2 + \frac{3}{385}ABz^2 + \left(\frac{1}{637}B^2 - \frac{2}{4875}A^3\right)z^4 - \frac{2}{5775}A^2Bz^6.$$

17/39

**Second (better) approach:** Define

$$Q(z) = \frac{1}{\wp(z)} \in z^2 + z^6\mathbf{K}[[z^2]] \quad \text{and} \quad R(z) = \sqrt{Q(z)} \in z + z^5\mathbf{K}[[z^2]].$$

The differential equation satisfied by  $R$  is

$$R'(z)^2 = BR(z)^6 + AR(z)^4 + 1.$$

First terms:

$$R(z) = z + \frac{A}{10}z^5 + \frac{B}{14}z^7 + O(z^8) = z \left( 1 + \frac{A}{10}z^4 + \frac{B}{14}z^6 + O(z^7) \right).$$

**Algorithm:**

1. Compute  $R(z) \pmod{z^{2n+4}}$  using linearization;
2. Compute  $Q(z) = R(z)^2 \pmod{z^{2n+5}}$ ;
3. Compute  $\wp(z) = 1/Q(z) \pmod{z^{2n+1}}$ .

**Thm.** The first  $n$  coefficients of the expansion of  $\wp$  can be computed in  $O(M(n))$  field operations.

18/39

## Benchmarks

NTL C++ library on an AMD 64 Processor 3400+ (2.4GHz).

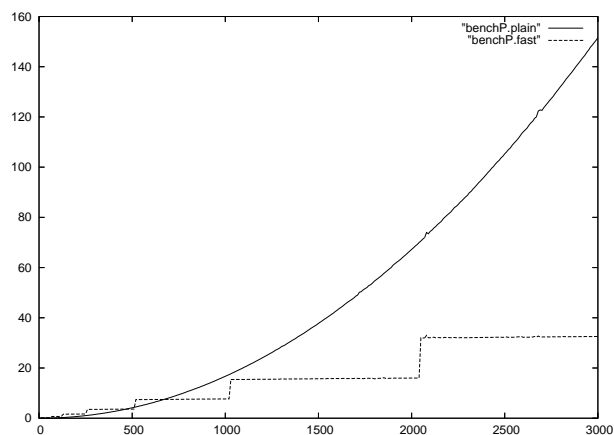


Figure: Timings for computing  $\wp$  on  $E : y^2 = x^3 + 4589x + 91128$  over

$\mathbb{F}_{10^{2004+4683}}$

19/39

## IV. Previous algorithms for computing isogenies

**Elementary remark:**

$$\frac{N}{D} \circ \frac{\hat{N}}{\hat{D}} = \frac{\phi_\ell}{\psi_\ell^2}$$

but all methods to solve this require factoring  $\psi_\ell$ , which is just too costly. . .

**Remember:** if  $E$  and  $\tilde{E}$  are  $\ell$ -isogenous, then

$$\tilde{\wp} = \frac{N}{D} \circ \wp.$$

Indeterminate coefficients, linear system  $\Rightarrow O(\ell^\omega)$ ,  $2 \leq \omega \leq 3$ .

Use

$$\frac{N}{D} = \tilde{\wp} \circ \wp^{-1},$$

but modular composition is too costly ( $O(M(\ell)\sqrt{\ell} + \ell^{\frac{\omega+1}{2}})$  or  $O(M(\ell)\sqrt{\ell \log \ell})$ ).

20/39

## A) Stark's method (1972)

INPUT:  $E$  and  $\tilde{E}$  related via an  $\ell$ -isogeny [ $\sigma$  not required]

OUTPUT:  $I(x) = N(x)/D(x)$ .

ALGORITHM: develop  $\tilde{\wp}(z)$  as a continued fraction in  $\wp(z)$ .

1. First write  $\wp(z) = \wp(Z)$  with  $Z = z^2$ ;  $T := \tilde{\wp}(Z) + O(Z^\ell)$ ;
2.  $n := 1$ ;  $q_0 := 1$ ;  $q_1 := 0$ ;
3. **while**  $\deg(q_n) < \ell - 1$  **do**  
 {inv:  $T(Z) = t_{-r}Z^{-r} + \dots + t_0 + t_1Z + \dots + O(Z^{\ell - \deg q_n - r - 1})$ }  
  - 3.1  $n := n + 1$ ;  $a_n := 0$ ;
  - 3.2 **while**  $r \geq 1$  **do**  
 $a_n := a_n + t_{-r}z^r$ ;  
 $T := T - t_{-r}\wp^r = t_{-s}Z^{-s} + \dots$ ;  
 $r := s$
  - 3.3  $q_n := a_n q_{n-1} + q_{n-2}$ ;
  - 3.4  $T := 1/T$ ;
4. Return  $D := q_n$ .

**Cost:**  $O(\ell M(\ell)) + O(M(\ell))$ .

21/39

$$E : y^2 = x^3 + x + 1 \pmod{503}, \tilde{E} : \tilde{y}^2 = \tilde{x}^3 + 463\tilde{x} + 478 \pmod{503}, \ell = 11.$$

$$\wp(z) = z^{-2} + 201z^2 + 431z^4 + 389z^6 + 260z^8 + O(z^{10}),$$

$$\tilde{\wp} = z^{-2} + 8z^2 + 291z^4 + 189z^6 + 452z^8 + O(z^{10}).$$

$$n = 0 : \tilde{\wp} = \wp + 310z^2 + 363z^4 + 303z^6 + 192z^8 + O(z^{10}),$$

$$\begin{aligned} & 1/(310z^2 + 363z^4 + 303z^6 + 192z^8 + O(z^{10})) \\ &= 86z^{-2} + 266 + 419z^2 + 22z^4 + 427z^6 + O(z^8) \\ &= 86\wp + 266 + \dots \end{aligned}$$

etc. Finally:

$$I(x) = \frac{x^{11} + 335x^{10} + 288x^9 + 161x^8 + 221x^7 + 288x^6 + 110x^5 + 112x^4 + 434x^3 + 125x^2 + 291x + 260}{x^{10} + 335x^9 + 481x^8 + 69x^7 + 382x^6 + 150x^5 + 221x^4 + 92x^3 + 324x^2 + 366x + 4}$$

and denominators factors as:

$$(x + 488)^2 (x + 128)^2 (x + 103)^2 (x + 99)^2 (x + 104)^2.$$

22/39

## B) Atkin

By integrating some formula involving  $\zeta(z) = -\int \wp$ , one gets:

$$D(\wp(z)) = z^{2-2\ell} \exp(F(z))$$

where

$$F(z) = -\sigma z^2 + 2 \left( \sum_{k=1}^{\infty} (\ell c_k - \tilde{c}_k) \frac{z^{2k+2}}{(2k+1)(2k+2)} \right).$$

1. Compute the series  $P_i(Z) = \wp(Z)^i$  at order  $\ell - 1$ , for  $1 \leq i \leq \ell - 1$ ;
2. Compute  $G(Z) = \exp_\ell(F(Z)) = \exp(F(Z)) \pmod{Z^\ell}$ ;
3.  $T := G$ ;  $D := 0$ ;
4. **for**  $i := \ell - 1$  **downto** 0 **do**  
 {at this point,  $T = tZ^{-i} + \dots$ }  
  - 4.1  $D := D + tz^i$ ;
  - 4.2  $T := T - tP_i$ .

**Cost:**  $O(\ell^2) + O(\ell M(\ell))$ .

**Pb:** rather huge constants. We need  $\sigma$ .

23/39

**A better algorithm:** rewrite

$$D\left(\frac{1}{x}\right) = \mathcal{I}^{2-2\ell} ((\exp \circ F) \circ \mathcal{I}), \quad (2)$$

with  $\mathcal{I}(x) = \wp^{-1}(1/x)$ , where  $\wp^{-1}$  is the functional inverse of  $\wp$ , where

$$\mathcal{I}'(x)^2 = \frac{1}{4x(1 + Ax^2 + Bx^3)} \quad \text{or} \quad \mathcal{I}'(x) = \frac{1}{2\sqrt{x}} \frac{1}{\sqrt{1 + Ax^2 + Bx^3}}$$

$\mathcal{I}(x) = x^{\frac{1}{2}} \sum_{i \geq 0} \frac{a_i}{2i+1} x^i$ , with

$$a_0 = 1, \quad a_1 = 0, \quad a_2 = -\frac{A}{2},$$

$$a_{i+1} = \frac{Ba_{i-2} - 2Bia_{i-2} - 2Aia_{i-1}}{2i+2} \quad \text{for } i \geq 2.$$

24/39

## C) Elkies92 (case $D = g^2$ )

$$\frac{d^{2k} \wp(z)}{dz^{2k}} = \mu_k(k+1)\wp^{k+1} + \dots + \mu_k(0)$$

**Cost:** computing all coefficients up to  $k = d$  costs  $O(d^2)$  but with very small constants.

**Idea:** compute  $p_k = \sum_r \wp(r\omega_1/\ell)^k$  via:

$$(2k)!(\tilde{c}_k - c_k) = 2(\mu_k(0)p_0 + \dots + \mu_k(k+1)p_{k+1})$$

for  $1 \leq k \leq d$ . In particular:

$$A - \tilde{A} = 5(6p_2 + 2Ap_0), \quad B - \tilde{B} = 7(10p_3 + 6Ap_1 + 4Bp_0).$$

Once all  $p_k$  are known, use Newton's formulas; by Schönage, this costs  $O(M(d))$ .

**Total cost:**  $O(d^2)$  but with very small constants (again!).

25/39

26/39

AtkinModComp:

1. Compute  $G(Z) = \exp_\ell(F(Z))$ ;
2. Compute  $\mathcal{I}(x)$ ;
3. Compute  $G(\mathcal{I})$  by modular composition (which is possible since  $G$  is in  $\mathbf{K}[[Z]] = \mathbf{K}[[x^2]]$ );
4. Deduce  $D$  using Equation (2).

**Cost:** dominated by the composition of the series  $G = \exp \circ F$  and  $\mathcal{I}$ , which can be done in  $O(M(\ell)\sqrt{\ell} + \ell^{\frac{\omega+1}{2}})$  or  $O(M(\ell)\sqrt{\ell \log \ell})$  operations in  $\mathbf{K}$ .

25/39

26/39

## D) Elkies98

Start from

$$\frac{N(x)}{D(x)} = \tilde{\wp} \circ \wp^{-1}(x)$$

and apply the chain rule to get:

$$(x^3 + Ax + B) \left( \frac{N(x)}{D(x)} \right)' = \left( \frac{N(x)}{D(x)} \right)^3 + \tilde{A} \left( \frac{N(x)}{D(x)} \right) + \tilde{B}.$$

A second differentiation leads to

$$(3x^2 + A) \left( \frac{N(x)}{D(x)} \right)' + 2(x^3 + Ax + B) \left( \frac{N(x)}{D(x)} \right)'' = 3 \left( \frac{N(x)}{D(x)} \right)^2 + \tilde{A}.$$

27/39

Writing

$$\frac{N(x)}{D(x)} = x + \sum_{i \geq 1} \frac{h_i}{x^i}$$

and identifying coefficients of  $x^{-i}$ ,  $i \geq 1$ , one deduces

$$h_1 = \frac{A - \tilde{A}}{5} \quad \text{and} \quad h_2 = \frac{B - \tilde{B}}{7},$$

and for all  $k \geq 3$ :

$$h_k = \frac{3}{(k-2)(2k+3)} \sum_{i=1}^{k-2} h_i h_{k-1-i} - \frac{2k-3}{2k+3} A h_{k-2} - \frac{2(k-3)}{2k+3} B h_{k-3}.$$

$\Rightarrow h_3, \dots, h_{\ell-2}$  using  $O(\ell^2)$  operations in  $\mathbf{K}$ .

Expanding at infinity the right-hand side of Vélú's formulas, one connects the power sums  $p_1 = \sigma, p_2, \dots$  of  $D(x)$  to the coefficients  $h_i$  for  $i \geq 1$ :

$$h_i = (2i+1)p_{i+1} + (2i-1)Ap_{i-1} + (2i-2)Bp_{i-2}.$$

$\Rightarrow O(\ell)$  operations.

**Total complexity:**  $O(\ell^2)$ .

27/39

28/39

## V. Our fast variant

**Idea:** improve on the computation of the  $h_i$ 's in Elkies98.

**Remember:**  $R(z) = 1/\sqrt{\wp(z)}$  and  $\tilde{R}(z) = 1/\sqrt{\tilde{\wp}(z)}$ .

There exists  $S$  s.t.  $\tilde{R} = S \circ R$  from which

$$\frac{N(x)}{D(x)} = \frac{1}{S\left(\frac{1}{\sqrt{x}}\right)^2}.$$

$$S(x) = x + \frac{\tilde{A} - A}{10}x^5 + \frac{\tilde{B} - B}{14}x^7 + O(x^9) \in x + x^3\mathbf{K}[[x^2]]$$

is such that

$$(Bx^6 + Ax^4 + 1)S'(x)^2 = 1 + \tilde{A}S(x)^4 + \tilde{B}S(x)^6.$$

29/39

## We can do without $\sigma$

(1') Compute  $C(x) = (Bx^6 + Ax^4 + 1)^{-1} \bmod x^{8\ell-5} \in \mathbf{K}[[x]]$ ;

(2') Compute  $S(x) \bmod x^{8\ell-4}$  and deduce  $T(x) \bmod x^{4\ell-2}$ ;

(3') Compute  $U(x) = 1/T(x)^2 \bmod x^{4\ell-2}$ ;

(4') Reconstruct the rational function  $U(x)$ ;

(5') Return  $N(x)/D(x) = xU(1/x)$ .

Using fast rational reconstruction, Step (4') can be performed in  $O(M(\ell) \log \ell)$  operations in  $\mathbf{K}$ .

31/39

Write:

$$S(x) = xT(x^2) \quad \text{and} \quad U(x) = \frac{1}{T(x)^2} \in 1 + x^2\mathbf{K}[[x]]$$

so that

$$\frac{N(x)}{D(x)} = xU\left(\frac{1}{x}\right).$$

We assume  $\sigma$  is known:

1. Compute  $C(x) = (Bx^6 + Ax^4 + 1)^{-1} \bmod x^{2\ell-1} \in \mathbf{K}[[x]]$ ;
2. Compute  $S(x) \bmod x^{2\ell}$  as usual and deduce  $T(x) \bmod x^\ell$ ;
3. Compute  $U(x) = 1/T(x)^2 \bmod x^\ell$ ;
4. Compute the coefficients  $h_1, \dots, h_{\ell-2}$  of  $N(x)/D(x)$ , using  $N(x)/D(x) = xU(1/x)$ ;
5. Compute the power sums  $p_2, \dots, p_{\ell-1}$  of  $D(x)$ , using the linear recurrence;
6. Recover  $D(x)$  from its power sums;
7. Deduce  $N(x)$ .

**Cost:** Steps (1) and (5) have cost  $O(\ell)$ . Steps (2), (3), (6) and (7) can be performed in  $O(M(\ell))$  operations, and Step (4) requires no operation.  $\Rightarrow O(M(\ell))$ .

30/39

## Remarks

1. In the case of odd  $\ell$ , we can compute  $g(x)$  instead of  $D(x)$ , *mutatis mutandis*.
2. There is a fastAtkin method, which is actually the same fastElkies when looking up the details.

32/39

## VI. Benchmarks

The first series of timings concerns the computation of isogenies over a small field,  $\mathbf{K} = \mathbb{F}_{10^{19}+51}$ , for the curve  $E : y^2 = x^3 + 4589x + 91128$ .

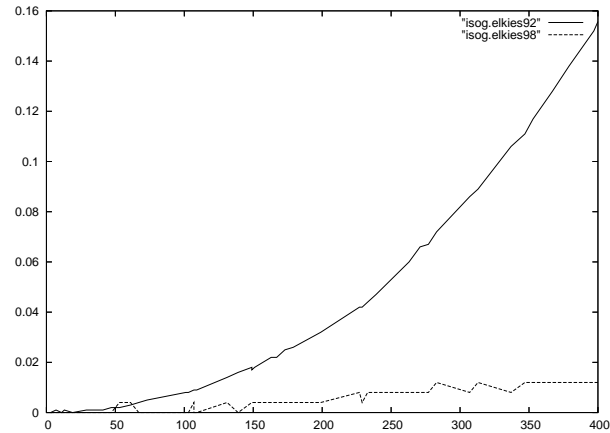


Figure: Elkies1992 vs. Elkies1998.

33/39

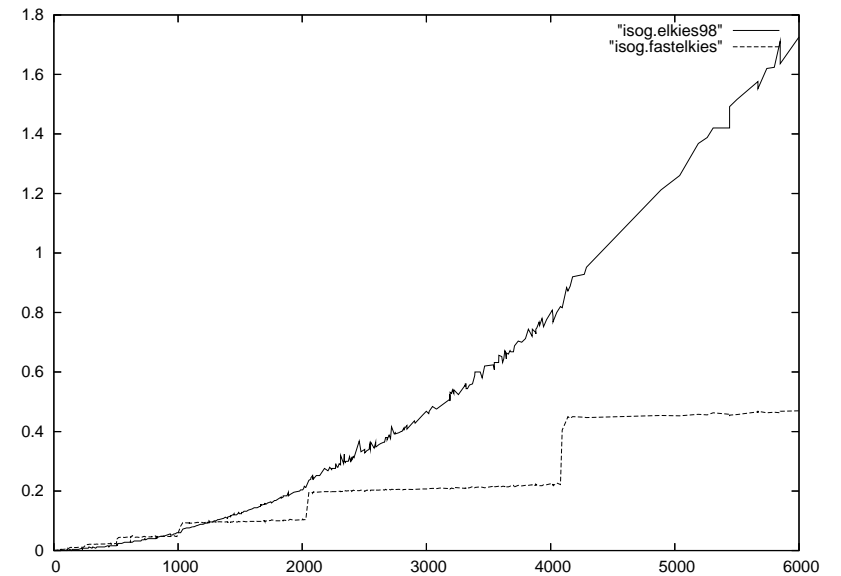


Figure: Elkies1998 vs. fastElkies.

34/39

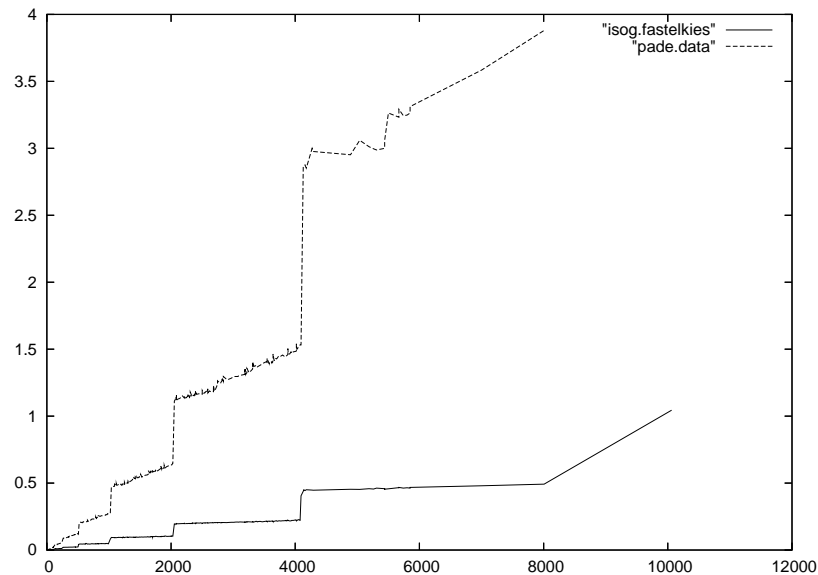


Figure: FastElkies vs. FastElkies'

35/39

Computing  $\ell$ -isogenies for the curve  $E : y^2 = x^3 + Ax + B$  where

$$A = \lfloor 10^{1990} \pi \rfloor = 31415926 \dots 58133904,$$

$$B = \lfloor 10^{1990} e \rfloor = 27182818 \dots 94787610,$$

over  $\mathbb{F}_{10^{2004}+4683}$ .

$\ell$	Computing $\wp$ and $\tilde{\wp}$			Recovering $g$	
	order	quadratic	fast	quadratic	fast
1013	511	8.6	7.0	4.2	1.1
2039	1024	34.6	29.9	17.4	2.5
3019	1514	75.7	30.3	38.2	5.1
4001	2005	132.7	31	66.9	5.5
5021	2515	209.3	64.4	106.2	11.2

36/39

$\ell$	$\wp, \tilde{\wp}$	Inverses		$q_n$
		quadratic	fast	
1013	See Table	23542	1222.7	28.0
2039		??	5113.4	116.9
3019		??	12182	258
4001		??	20388	418.6
5021		??	38910	663.1

Table: Stark's algorithm

$\ell$	$\wp, \tilde{\wp}$	Algorithm Aktin1992			
		exponential naive	fast	$\wp^k$	$g$
1013	See Table	88.4	1.2	72.3	4.4
2039		370.1	4.9	304.9	17.7
3019		955.9	5.1	755.8	38.9
4001		1503	5.2	1218.9	67.6
5021		3180	10.8	2506.4	108.7

$\ell$	$\wp, \tilde{\wp}$	Algorithm AtkinModComp				
		$\exp(F)$	$\mathcal{I}^{1-\ell}$	modular composition		$g$
				ModComp1	ModComp2	
1013	See Table	1.2	2.7	14.3	35.6	0.2
2039		2.5	6.6	45.8	111.9	0.4
3019		5.1	10.4	95.3	241	0.7
4001		5.2	11.6	143.2	338	0.9
5021		10.9	20.9	240	642	1.4

$\ell$	$\wp, \tilde{\wp}$	Elkies1992		
		$\mu$	$p_i$	$g$
1013	See Table	10.4	4.4	See Table
2039		49.1	17.9	
3019		130.6	38.9	
4001		263	68.4	
5021		496.5	106.6	

$\ell$	Elkies1998 and fastElkies			
	$h_i$		$p_i$	$g$
	quadratic	fast		
1013	4.4	4.5	0.05	See Table
2039	17.3	9.6	0.1	
3019	38.0	19.5	0.16	
4001	67.2	20.0	0.21	
5021	105.0	40.7	0.27	

## Conclusions

**Cryptographic sizes:** Elkies98 the best algorithm by far ( $\ell \leq 300$ ).

**What's left to be done?** the case  $p$  small, not for SEA.

Fast versions required for

- Couveignes I (formal groups)?
- Lercier ( $p = 2$ )?
- Couveignes II (Artin-Schreier towers)?

**Maybe:** use a  $p$ -adic approach à la Joux/Lercier (2006).