A survey on algorithms for computing isogenies on low genus curves

F. Morain

Laboratoire d'Informatique de l'École polytechnique

ANTS8, May 19th, 2008

UNIVERSITY OF
Waterloo

Contents

I. Motivations.

II. Isogenies in theory.

III. Computing modular polynomials.

IV. Computing the isogeny.

V. Conclusions.

Acknowledgments: B. Smith.

I. Motivations

- **Number Theory:**
  - computing algebraic integrals: AGM, etc.
  - classification of curves into isogeny classes (e.g., over a finite field, two curves have the same cardinality).
  - etc.

- **Computational Number Theory:**
  - $g = 1$:
    - First life (1985–1997): crucial role in point counting in Schoof-Elkie-Atkin (SEA), Couveignes, Lercier; still needed for p large; AGM for p small (p-adic methods à la Mestre, Satoh, Kedlaya).
    - Second life (1996–): Kohel, Fouquet/M. (cycles and volcanoes); Couveignes/Henocq, Bröker and Stevenhagen (CM curves using p-adic method).
  - $g \geq 2$: try to extend these previous successes (e.g., modular polynomials).

Motivations (cont'd): cryptologic applications

- $g = 1$ (1999–):
  - speedup for computing $[k]P$ when an "easy" endomorphism is known (Koblitz; Gallant/Lambert/Vanstone + several followers).
  - Special purposes: Smart; Brier & Joye.
  - isogeny graph: $(E_1, E_2) \in \mathscr{E}$ iff E_1 and E_2 are isogenous
    - Galbraith: finding a path between two curves seems difficult;
    - Jao/Miller/Venkatesan: the graph is an expander graph;
    - Galbraith/Hess/Smart: send DL from a hard curve to a weak one;
    - cryptosystems: Teske (hide an easy DLP among harder ones); Rostovtsev/Stolbunov; etc.
    - hash function: Charles/Goren/Lauter use graph of 2-isogenies of supersingular elliptic curves.
- $g \geq 2$:
  - speedups in exponentiations: Kohel/Smith, Takashima, Galbraith/Lin/Scott, etc.
  - $g = 3$: sending DL on $\mathrm{Jac}(H)$ to a weaker one on $\mathrm{Jac}(Q)$ (Smith).

II. Isogenies in theory

Def. An isogeny is a surjective homomorphism of finite kernel between two abelian varieties: $\varphi : \mathscr{A} \to \mathscr{A}'$.

Right away, we will concentrate on jacobians of curves; for simplicity, $g \leq 3$.

Endomorphism: $\mathrm{Jac}' = \mathrm{Jac}$.

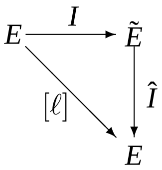
The case $g = 1$

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

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

Thm. (dual isogeny) There is a unique $\hat{I} : \tilde{E} \to E$, $\ell = \deg I$ s.t.

$$(*) \qquad \hat{I} \circ I = [\ell]$$



$\Rightarrow$ I is a factor of $[\ell]$, hence I can provide factors of ψ_ℓ
$\Rightarrow$ key to SEA.

Higher genus

$g = 2$: $\mathrm{Jac}(H)/F \to \mathrm{Jac}(H')$ or $E_1 \times E_2$ (cannot be determined by looking at F only?).

$g = 3$: $\mathrm{Jac}(H)/F \to \mathrm{Jac}(H')$ or $\mathrm{Jac}(C)$ or $E_1 \times E_2 \times E_3$.

If F has suitable properties, then (*) stands also for some ℓ. Typical example is ℓ prime and $F \sim (\mathbb{Z}/\ell\mathbb{Z})^g$.

First examples and illustrations

1. Separable:

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

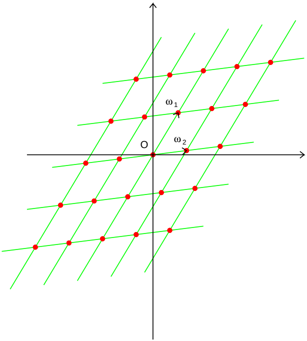
where ψ_k is some division polynomial (i.e., coding the k-torsion). Generalized to division ideals in higher genus.

2. Complex multiplication: $[i](x,y) = (-x, iy)$ on $E : y^2 = x^3 - x$.
Every integer k can be written as $k = k_0 + Ik_1$ where $I^2 \equiv -1 \bmod p$ and $|k_0|, |k_1| \approx \sqrt{p}$
$\Rightarrow$ fast way of evaluating $[k]P$.

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

In the sequel: only separable isogenies.

The classical case: isogenies for curves over $\mathbb{C}$



If $E = \mathbb{C}/L$ and $E' = \mathbb{C}/L'$ and there exists an α s.t. $\alpha L' \subset L$, then E and E' are isogenous.

Modular polynomial: there exists a bivariate polynomial $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$ such that if L/L' is cyclic of index m then

$$\Phi_m(j(L), j(L')) = \Phi_m(j(E), j(E')) = 0.$$

Examples

Ex. $E: Y^2 = X^3 + bX$, $F = \langle (0,0) \rangle$; $\tilde{E}: Y^2 = X^3 - 4bX$,

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

$$\hat{I}(x) = \frac{x^2 - 4\,b}{x},$$

$$\hat{I} \circ I = 2^2[2] = \frac{x^4 - 2\,x^2 b + b^2}{x\,(x^2 + b)}.$$

Later on: how we can effectively compute such formulas.

A typical isogeny pair: $\tilde{E} = \mathbb{C}/(\omega_1/\ell, \omega_2)$ is ℓ-isogenous to $E = \mathbb{C}/(\omega_1, \omega_2)$. Take as finite subgroup:

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

[remember that Weierstrass $\wp$ parametrizes E.]

Complex multiplication

$E = \mathbb{C}/L(1,\tau)$ with quadratic τ in some $\mathbf{K} = \mathbb{Q}(\sqrt{-D})$.

For α an integer in $\mathbf{K}$, Weierstrass $\wp$ gives:

$$\wp(\alpha z) = \frac{N(\wp(z))}{D(\wp(z))}$$

with $\deg(N) = \deg(D) + 1 = \mathrm{Norm}(\alpha)$.

Take $D = 7$ and $E : Y^2 = X^3 - 35X - 98$, $\omega = (-1+\sqrt{-7})/2$:

$$[\omega](x) = \frac{\left(x^2 + (4+\omega)x + 21\,\omega + 7\right)(-1+\omega)}{4x + 16 + 4\,\omega}.$$

CM generalizes to other genera: theory ok, computations doable in genus 2.

Two strategies for building isogenies

Starting from a kernel:

- given $\mathrm{Jac}(C)$ and F, find the module(s) of $\mathrm{Jac}(C') = \mathrm{Jac}(C)/F$, and then C' [this could be non-trivial];
- compute I.

Using modular polynomials: try to mimic the classical case of

- find the roots $\{j'\}$ of $\Phi_\ell(X, j(E)) = 0$;
- for each j', find E' of invariant j';
- compute I.

En route: examine each of these, starting from the (easy) case of $g = 1$.

III. Computing modular polynomials

A) when $g = 1$

Traditionnal modular polynomial: constructed via lattices and curves over $\mathbb{C}$ (plus modular forms and functions).
Remember that

$$j(q) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n q^n.$$

Then $\Phi_\ell^T(X,Y)$ is such that $\Phi_\ell^T(j(q), j(q^\ell))$ vanishes identically.
This polynomial has a lot of properties: symmetrical $\mathbb{Z}[X,Y]$, degree in X and Y is $\ell + 1$ (hence $(\ell+1)^2$ coefficients), etc. and moreover

Thm. [P. Cohen] the height of $\Phi_\ell^T(X,Y)$ is $O((\ell+1)\log \ell)$.
$\Rightarrow$ total size is $\tilde{O}(\ell^3)$.

Example:

$$\Phi_2^T(X,Y) = X^3 + X^2\left(-Y^2 + 1488\,Y - 162000\right) + X\left(1488\,Y^2 + 40773375\,Y + 8748000000\right)$$
$$+Y^3 - 162000\,Y^2 + 8748000000\,Y - 157464000000000.$$

Choosing another modular equation

Why? Always good to have the smallest polynomial so as not to fill the disks too rapidly...

Key point: any function on $\Gamma_0(\ell)$ (or $\Gamma_0(\ell)/\langle w_\ell\rangle$) will do. In particular, if

$$f(q) = q^{-v} + \cdots$$

then there will exist a polynomial $\Phi_\ell[f](X,Y)$ s.t.

$$\Phi_\ell[f](j(q), f(q)) \equiv 0.$$

This polynomial will have $(v+1)(\ell+1)$ coefficients, and height $O(v \log \ell)$, still in $\tilde{O}(\ell^3)$.

Choosing f

Atkin:

- canonical choice $f(q)$ using some power of $\eta(q)/\eta(q^\ell)$ where $\eta(q) = q^{1/24}\prod_{n\geq 1}(1-q^n)$. E.g.

$$\Phi_2^c(J,F) = F^3 + 48F^2 + 768F - JF + 4096.$$

- a difficult method (the laundry method) for finding (conjecturally) the f with smallest v (that can rewritten as θ-functions with characters).

Müller: for (small) integer r, use

$$\frac{T_r(\eta\eta_\ell)}{\eta\eta_\ell}$$

where T_r is the Hecke operator

$$(T_r|f)(\tau) = f(r\tau) + \frac{1}{r}\sum_{k=0}^{r-1} f\left(\frac{\tau+k}{r}\right).$$

Alternatively: one may use some linear algebra on functions obtained via Hecke operators.

Computing $\Phi_\ell[f]$ given f

- **Atkin** (analysis by Elkies): use q-expansion of j and f with $O(v\ell)$ terms, compute power sums of roots of $\Phi_\ell[f]$, write them as polynomials in J and go back to coefficients of $\Phi_\ell[f](X,J)$ via Newton's formulas; use CRT on small primes. $\tilde{O}(\ell^3 \mathsf{M}(p))$; used for $\ell \leq 1000$ fifteen years ago.

- **Charles+Lauter (2005):** compute Φ_ℓ^T modulo p using supersingular invariants mod p, Mestre *méthode des graphes*, ℓ torsion points defined over $\mathbb{F}_{p^{O(\ell)}}$ and interpolation. $\tilde{O}(\ell^4 \mathsf{M}(p))$

- **Enge (2004); Dupont (2004):** use complex floating point evaluation and interpolation. $\tilde{O}(\ell^3)$

Write

$$\Phi_\ell^T(X,J) = X^{\ell+1} + \sum_{u=0}^{\ell} c_u(J) X^u$$

where $c_u(J) \in \mathbb{Z}[J]$, $\deg(c_u(J)) \le \ell+1$. All computations are done using precision $H = O(\ell \log \ell)$.

1. **for** $\ell+1$ values of z_i **do**:

 1.1 Compute floating point approximations to the $\ell+1$ roots $f_r(z_i)$ of $\Phi_\ell[f](X, j(z_i))$ to precision H;

 1.2 Build $\prod_{r=1}^{\ell+1}(X - f_r(z_i)) = X^{\ell+1} + \sum_{u=0}^{\ell} c_u(j(z_i)) X^u$; $O(\mathsf{M}(\ell)\log\ell)$ ops.

2. Perform $\ell+1$ interpolations for the c_u's: $O((\ell+1)\mathsf{M}(\ell)\log\ell)$ ops.

All 1.2 + 2 has cost $O(\ell \mathsf{M}(\ell)(\log\ell)\mathsf{M}(H)) = \tilde{O}(\ell^3)$.

Examples

Data for $T_r(\eta\eta_\ell)/\eta\eta_\ell$ (courtesy Enge)

ℓ	r	H	$\deg(J)$	eval(s)	interp(s)	tot (d)	Mb gz
3011	5	7560	200				368
3079	97	9018	254	7790	640	23	547
3527	13	9894	268	799	1440	3	746
3517	97	10746	290	12400	1110	42	850
4003	13	11408	308	1130	2320	4	1127
5009	5	13349	334	880	3110	3	1819
6029	5	16418	402	1550	6370	7	3251
7001	5	19473	466	2440	11700	13	5182
8009	5	22515	534	3500	20000	22	7905
9029	5	25507	602	5030	33100	35	11460
10079	5	28825	672	7690	56300	61	16152

An algebraic alternative: Charlap/Coley/Robbins

Over some $\mathbf{K}$, write

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

The factor we build is:

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

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

$$\begin{array}{cc} \mathbf{K}[x]/(\psi_\ell(x)) & \\ | & \ell - 1 \\ \mathbf{K}[x]/(M_\sigma(x)) & \\ | & \ell + 1 \\ \mathbf{K}[x] & \end{array}$$

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

CCR (cont'd)

Another modular equation: $M_\sigma(x) = \Phi_\ell(x, j(E))$.
It has the same properties as the traditional one (e.g., factorization patterns) and can be used as is in SEA.
To find $\tilde{A}$ and $\tilde{B}$, we need two more polynomials + some tedious matching of roots.

The first values are:

$$U_3(X) = X^4 + 2AX^2 + 4BX - A^2/3,$$

$$V_3(X) = X^4 + 84AX^3 + 246A^2X^2 + (-63756A^3 - 432000B^2)X$$
$$+576081A^4 + 3888000B^2A,$$

$$W_3(X) = X^4 + 732BX^3 + (171534B^2 + 25088A^3)X^2$$
$$+(11009548B^3 + 1630720BA^3)X - 297493504/27A^6$$
$$-437245479B^4 - 139150592B^2A^3,$$

$$U_5(X) = X^6 + 20AX^4 + 160BX^3 - 80A^2X^2 - 128ABX - 80B^2.$$

B) Modular polynomials when $g = 2$

- **Gaudry + Schost:** the algebraic alternative is generic (Ξ_ℓ)
  - total degree is $d = (\ell^4 - 1)/(\ell - 1)$;
  - number of monomials is $O(\ell^{12})$;
  - can do $\ell = 3$: 50k but a lot of computing time (weblink still active);
  - use its factorization patterns à la Atkin to speedup cardinality computations.

- **The classical modular approach:**
  - Poincaré $\rightarrow$ Siegel (dim $2g$);
  - replace j by $(j_1, j_2, j_3) \Rightarrow$ triplet of modular polynomials, coefficients are rational fractions in j_i's;
  - Dupont (experimental conjectures proven more recently by Bröker+Lauter): stuck at $\ell = 2$ with 26.8 Mbgz (just the beginning of $\ell = 3$); uses evaluation/interpolation again.

C) Modular polynomials when $g = 3$

Gaudry + Schost $\Rightarrow d = (\ell^{2g} - 1)/(\ell - 1)$.

And then: ?????

IV. Computing the isogeny

A) the case $g = 1$: Vélu's formulas

Vélu suggests to use

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

and derives equations for $\tilde{E}$ and I in terms of symmetric functions in the x_Q, the abscissas of points in F. (Plus more properties, like the isogeny is strict.)

How does an isogeny look like?

Extending Vélu, Dewaghe (for $E : Y^2 = X^3 + AX + B$):

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

Fundamental proposition. The isogeny I can be written as

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

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

$$= \ell x - \sigma - 2\sqrt{x^3 + Ax + B} \left(\sqrt{x^3 + Ax + B} \frac{D'(x)}{D(x)} \right)'.$$

Elkies92

1. Compute the h_i's of

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

in $O(\ell^2)$ operations using

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

2. deduce power sums p_i of $D(x)$ in $O(\ell)$ operations using also $\tilde{A}$ and $\tilde{B}$;

3. use fast Newton in $O(\mathsf{M}(\ell))$ to get $D(x)$.

$\Rightarrow$ very fast for small ℓ's.

Bostan/M./Salvy/Schost

Prop. $O(\mathsf{M}(\ell))$ method to get the h_i's given $\tilde{A}$, $\tilde{B}$, σ.

Some ideas: there exists a series $S(x)$ s.t.

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

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

is such that

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

Use fast algorithm for solving this differential equation.

Rem. See *Math. Comp.* paper that includes survey of known methods for isogeny computations.

The case of finite fields of small characteristic

- **Couveignes:** formal groups; Artin-Schreier towers; time $\tilde{O}(\ell^2)$ but bad dependancy on p (see on-going work of L. De Feo).
- **Lercier/Joux** (2006): medium p using p-adic lifting.
- **Lercier/Sirvent** (2008): small p using p-adic lifting + BMSS $\Rightarrow$ complexity of $O(\mathsf{M}(\ell))$ in all cases.

B) The case $g = 2$

Probably not complete list:

- Gaudry+Schost: $\mathrm{Jac}(C) \to E_1 \times E_2$ for a $(2,2)$-isogeny of kernel $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- $\ell = 2$ (AGM): Richelot, Humbert.
- $\ell \geq 3$: Dolgachev/Lehavi; general result for $F = (\mathbb{Z}/\ell\mathbb{Z})^2$; completely explicit for $\ell = 3$; more work needed for $\ell > 3$. Some hope?

C) And for $g = 3$?

Again, lack of general formulas:

- $\ell = 2$ (AGM): Donagi/Livné (+ negative results for $g > 3$); explicit methods by Lehavi + Ritzenthaler.

- Smith (Eurocrypt 2008):
  - $\varphi : \mathrm{Jac}(H) \to \mathrm{Jac}(C)$ where H is hyperelliptic and C smooth plane quartic;
  - intricate construction but relatively simple formulas in the end: uses Recilla's trigonal construction + theorem of Donagi and Livné;
  - works for 18.57% of smooth plane quartics;
  - nice crypto application (DL in $\mathrm{Jac}(C)$ easier than in $\mathrm{Jac}(H)$).

V. Conclusions

- $g = 1$: morally solved.
- $g > 1$:
  - scattered results;
  - curves are not so frequent and/or easy in higher genus;
  - objects are exponentially big: even with sophisticated computer algebra techniques, this sounds difficult.