Evaluating large degree isogenies in subexponential time

David Jao and Vladimir Soukharev

University of Waterloo

July 19, 2010

Outline

1. Preliminaries
   - Isogenies
   - Examples of isogenies
   - Previous algorithms
2. Our algorithm
   - Background: Bröker-Charles-Lauter algorithm
   - Generalizing BCL to arbitrary curves
3. Example

Isogenies

- Let E and E' be elliptic curves over F.
- An *isogeny* $\phi\colon E \to E'$ is an algebraic morphism

$$\phi(x,y) = \left(\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)}\right)$$

  satisfying $\phi(\infty) = \infty$.
- Equivalently, an isogeny is an algebraic morphism which is a group homomorphism.
- The *degree* of an isogeny is its degree as an algebraic map.
- The *endomorphism ring* $\mathrm{End}(E)$ is the set of isogenies from $E(\bar{F})$ to itself. This set forms a ring under composition.

Examples

Example (Scalar multiplication)

- Let $E : y^2 = x^3 + ax + b$.
- For $n \in \mathbb{Z}$, define $[n]\colon E \to E$ by $[n](P) = nP$. Then $[n]$ is an isogeny.
- When $n = 2$,

$$[2](x, y) = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, \frac{(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b - a)y}{8(x^3 + ax + b)^2} \right)$$

- The degree of $[n]$ is n^2.
- The cardinality of $\ker([n])$ is also n^2.

Examples

Example (Frobenius map)

- Let $F = \mathbb{F}_q$ be a finite field.
- Define $\pi\colon E \to E$ by
$$\pi(x, y) = (x^q, y^q).$$
- π is an algebraic map and a group homomorphism, hence an isogeny.
- $\deg(\pi) = q$, but $\#\ker(\pi) = 1$.

The reason for this strange behavior is because π is *inseparable*.

Examples

Example (Dual isogenies)

- Let $F = \mathbb{F}_{109}$.
- Let $E_1\colon y^2 = x^3 + 2x + 2$ and $E_2\colon y^2 = x^3 + 34x + 45$. An isogeny $\phi\colon E_1 \to E_2$ (of degree 3) is given by

$$\phi(x, y) = \left(\frac{x^3 + 20x^2 + 50x + 6}{x^2 + 20x + 100}, \frac{(x^3 + 30x^2 + 23x + 52)y}{x^3 + 30x^2 + 82x + 19}\right).$$

- There exists an isogeny $\hat{\phi}\colon E_2 \to E_1$, given by

$$\hat{\phi}(x, y) = \left(\frac{x^3 + 49x^2 + 46x + 104}{9x^2 + 5x + 34}, \frac{(x^3 + 19x^2 + 66x + 47)y}{27x^3 + 77x^2 + 88x + 101}\right),$$

  satisfying $\phi \circ \hat{\phi} = [3]$ and $\hat{\phi} \circ \phi = [3]$.
- $\hat{\phi}$ is the *dual isogeny* of ϕ and vice-versa.

Examples

Example (Complex multiplication)

- Let $E\colon y^2 = x^3 - x$ be defined over F.
- Let $i \in F$ be a square root of -1.
- Define

$$\phi(x, y) = (-x, iy).$$

- Then $\phi \circ \phi = [-1]$, and we have an inclusion $\mathbb{Z}[i] \hookrightarrow \operatorname{End}(E)$.

Overview

- Isogenies between elliptic curves over finite fields have many applications in cryptography and number theory.
- For many of these applications, it is necessary to evaluate large degree isogenies explicitly. Large means $\ell \gtrapprox 2^{100}$.
- $[n]\colon E \to E$ is easy to evaluate using double-and-add.
- Inseparable isogenies (i.e., Frobenius maps) are easy to evaluate: compute x^q using square-and-multiply.
- Linear combinations and compositions of easy to evaluate isogenies (scalar multiplication, frobenius map, complex multiplication by a small discriminant, small degree isogenies) are easy to evaluate.
- All other large degree isogenies are infeasible to evaluate via any obvious algorithms.

Ordinary curves

Theorem

Let E be an elliptic curve defined over a finite field. As a $\mathbb{Z}$-module, $\dim_{\mathbb{Z}} \operatorname{End}(E)$ is equal to either 2 or 4.

Definition

An elliptic curve E over a finite field is *supersingular* if $\dim_{\mathbb{Z}} \operatorname{End}(E) = 4$, and *ordinary* otherwise.

- Ordinary curves are more secure for cryptography.
- Isogenous curves are always either both ordinary, or both supersingular.
- For the rest of this talk, we assume all curves are ordinary.

Useful facts

Theorem (Tate)

For any two curves E_1 and E_2 defined over $\mathbb{F}_q$, there exists an isogeny from E_1 to E_2 over $\mathbb{F}_q$ if and only if $t(E_1) = t(E_2)$ (equivalently, if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$).

Remark: The trace of E can be computed in polynomial time (Schoof).

More useful facts

Let $\phi\colon E \to E'$ be a separable isogeny.

- $E' \cong E/\ker\phi$.
- $\ker\phi$ is an ideal of $\mathrm{End}(E)$.
- Up to isomorphism, the ideal $\ker\phi$ uniquely determines ϕ.

Horizontal isogenies

Definition

- An isogeny which maps between E and E', such that $\mathrm{End}(E) = \mathrm{End}(E')$ is called a horizontal isogeny.

Theorem

- *There is a 1-1 correspondence between horizontal isogenies* $\phi\colon E \to E'$ *and proper ideals* $\mathfrak{I}_\phi \subset \mathrm{End}(E)$.
- $\mathfrak{I}_{\phi\circ\psi} = \mathfrak{I}_\phi \mathfrak{I}_\psi$.
- $\deg \phi$ *equals the norm of* $\mathfrak{I}_\phi$.

The old, slow way

Let $E\colon y^2 = x^3 + ax + b$, and let $\mathfrak{I}_\phi = \mathfrak{L} \subset \mathrm{End}(E)$ be a non-inert prime ideal of norm ℓ. (Note: ℓ is prime.)

- Denote by $\Phi_\ell(X, Y)$ the *classical modular polynomial* of level ℓ.
- Solve $\Phi_\ell(j(E), Y) = 0$ for Y. Let h be a solution.
- Set

$$
\begin{aligned}
s &= -\frac{18b}{\ell a} \frac{\frac{\partial \Phi}{\partial X}(j(E), h)}{\frac{\partial \Phi}{\partial Y}(j(E), h)} j(E) \in \mathbb{F}_q \\
a' &= -\frac{1}{48} \frac{s^2}{h(h-1728)} \in \mathbb{F}_q \\
b' &= -\frac{1}{864} \frac{s^3}{h^2(h-1728)} \in \mathbb{F}_q
\end{aligned}
$$

- Then the equation for E' is $y^2 = x^3 + a'x + b'$.
- The equation for ϕ is also known (and is even more complicated).

Classical modular polynomials

$$\begin{aligned}
\Phi_2(X,Y) = {} & X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY + 8748000000X + Y^3 - 162000Y^2 \\
& + 8748000000Y - 157464000000000 \\
\Phi_3(X,Y) = {} & X^4 - X^3Y^3 + 2232X^3Y^2 - 1069956X^3Y + 36864000X^3 + 2232X^2Y^3 + 2587918086X^2Y^2 \\
& + 8900222976000X^2Y + 452984832000000X^2 - 1069956XY^3 + 8900222976000XY^2 - 770845966336000000XY \\
& + 1855425871872000000000X + Y^4 + 36864000Y^3 + 452984832000000Y^2 + 1855425871872000000000Y \\
\Phi_5(X,Y) = {} & X^6 - X^5Y^5 + 3720X^5Y^4 - 4550940X^5Y^3 + 2028551200X^5Y^2 - 246683410950X^5Y + 1963211489280X^5 \\
& + 3720X^4Y^5 + 1665999364600X^4Y^4 + 107878928185336800X^4Y^3 + 383083609779811215375X^4Y^2 \\
& + 128541798906828816384000X^4Y + 1284733132841424456253440X^4 - 4550940X^3Y^5 \\
& + 107878928185336800X^3Y^4 - 441206965512914835246100X^3Y^3 + 26898488858380731577417728000X^3Y^2 \\
& - 192457934618928299655108231168000X^3Y + 280244777828439527804321565297868800X^3 + 2028551200X^2Y^5 \\
& + 383083609779811215375X^2Y^4 + 26898488858380731577417728000X^2Y^3 \\
& + 5110941777552418083110765199360000X^2Y^2 + 36554736583949629295706472332656640000X^2Y \\
& + 6692500042627997708487149415015068467200X^2 - 246683410950XY^5 + 128541798906828816384000XY^4 \\
& - 192457934618928299655108231168000XY^3 + 36554736583949629295706472332656640000XY^2 \\
& - 264073457076620596259715790247978782949376XY + 53274330803424425450420160273356509151232000X \\
& + Y^6 + 1963211489280Y^5 + 1284733132841424456253440Y^4 + 280244777828439527804321565297868800Y^3 \\
& + 6692500042627997708487149415015068467200Y^2 + 53274330803424425450420160273356509151232000Y \\
& + 141359947154721358697753474691071362751004672000
\end{aligned}$$

Computing modular polynomials

- Clearly, computing $\Phi_\ell(X, Y)$ is infeasible for large ℓ.
- Theoretical complexity: $O(\ell^{3+\varepsilon})$
- World record over $\mathbb{Z}$: $\ell \approx 10000$ (Enge, 2007)
- World record over $\mathbb{Z}_p$: $\ell \approx 20000$ (Bröker, Lauter, Sutherland, 2010)
- Our goal: $\ell \gtrapprox 2^{100}$

Outline

1. Preliminaries
   - Isogenies
   - Examples of isogenies
   - Previous algorithms
2. Our algorithm
   - Background: Bröker-Charles-Lauter algorithm
   - Generalizing BCL to arbitrary curves
3. Example

BCL algorithm

- Let E be an elliptic curve
- Let $\mathfrak{L}$ be a (proper) split prime ideal of $\mathrm{End}(E) \cong \mathcal{O}_\Delta$.
- Let ℓ be the norm of $\mathfrak{L}$.
- Goal: Evaluate the normalized horizontal isogeny $\phi_\ell \colon E \to E/\mathfrak{L}$.
- Note: $\mathfrak{L}\bar{\mathfrak{L}} = (\ell)$.
- Obtain the factorization of $\mathfrak{L}$ in the class group, $[\mathfrak{L}] = [\mathfrak{p}_1]^{e_1}[\mathfrak{p}_2]^{e_2} \cdots [\mathfrak{p}_n]^{e_n}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are split prime ideals of small norm generating $\mathrm{Cl}(\mathcal{O}_\Delta)$.
- Compute $(a) = \mathfrak{L}\bar{\mathfrak{p}}_1^{e_1}\bar{\mathfrak{p}}_2^{e_2} \cdots \bar{\mathfrak{p}}_n^{e_n} = \mathrm{Norm}(\mathfrak{p}_1)^{e_1} * \mathrm{Norm}(\mathfrak{p}_2)^{e_2} * \cdots * \mathrm{Norm}(\mathfrak{p}_n)^{e_n}(\alpha)$.
- Obtain $\mathfrak{L} = (\alpha)\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_n^{e_n}$, where $\alpha = a/m$.

BCL algorithm (cont'd)

- Let $\phi_c = \phi_{p_1}^{e_1}\phi_{p_2}^{e_2}\cdots\phi_{p_n}^{e_n}\colon E \to E_c$, where $E_c = E/E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_n^{e_n}]$.
- Evaluate $\phi_c(P) \in E_c$ using old techniques recursively.
- Let $\alpha = (u + v\pi_q)/(zm)$, and using those values compute the isomorphism $\eta\colon E_c \to E'$, where $\eta^*(\omega_{E'}) = (u/zm)\omega_{E_c}$.
- Compute $Q = \eta(\phi_c(P))$.
- Compute $r = x((zm)^{-1}(u + v\pi_q)(Q))^{|\mathcal{O}_\Delta^*|/2}$.

Drawbacks of BCL algorithm

- BCL algorithm scales very well as ℓ grows large, but not very well as $|\Delta|$ grows large.
- Bröker-Charles-Lauter do not give any runtime analysis of the ideal factorization step other than to say that it is polynomial time in $|\Delta|$.
- Only works well with small discriminant curves (eg. pairing-friendly curves).

Idea of our algorithm

- Our algorithm uses techniques similar to BCL, but we speed up the algorithm by factoring $\mathfrak{L}$ in a more efficient manner.
- We use ideas from the subexponential class group discrete log algorithm by Hafner and McCurley to factor $[\mathfrak{L}]$.

Factoring ideals

Our method for evaluating isogenies is based on factoring prime ideals. Given a prime ideal $\mathfrak{L} \subset \mathrm{End}(E)$:

- Choose an upper bound N.
- For each split prime $p_i < N$, let $\mathfrak{p}_i$ be a prime ideal of norm p_i.
- Choose *sparse* exponents $e_i < (N/p_i)^2$ at random until

  $$\mathrm{Reduce}(\mathfrak{L}\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_n^{e_n})$$

  factors completely into a product of the prime ideals $\mathfrak{p}_i$, where the number of nonzero exponents in the resulting factorization is small since the ideal is reduced.
- The above exponent bounds come from [Bisson-Sutherland 09].
- We used their bounds to take advantage of their runtime analysis, but many other choices of bounds also work.

Factoring ideals (cont'd)

- Write
$$\mathrm{Reduce}(\mathfrak{L}\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_n^{e_n}) = \mathfrak{p}_1^{f_1}\mathfrak{p}_2^{f_2}\cdots\mathfrak{p}_n^{f_n}$$
- Then
$$[\mathfrak{L}] = [\mathfrak{p}_1]^{f_1-e_1}[\mathfrak{p}_2]^{f_2-e_2}\cdots[\mathfrak{p}_n]^{f_n-e_n}$$
- Hence
$$\mathfrak{L} = (\alpha)\mathfrak{p}_1^{f_1-e_1}\mathfrak{p}_2^{f_2-e_2}\cdots\mathfrak{p}_n^{f_n-e_n}$$
for some principal fractional ideal (α).
- Evaluate the isogenies corresponding to $(\alpha), \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ to obtain the isogeny corresponding to $\mathfrak{L}$.

Complexity of the algorithm

Definition (Subexponential time complexity)

For $0 < \alpha < 1$, define

$$L_n(\alpha, c) = O(\exp((c + o(1))(\log n)^\alpha (\log\log n)^{1-\alpha})).$$

Theorem

Under the Generalized Riemann Hypothesis and additional heuristics, the optimal value for the bound N is $L_q(\frac{1}{2}, \frac{1}{2\sqrt{3}})$, and the expected time complexity of the overall algorithm is

$$\log(\ell) L_q(\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}).$$

Outline

An example

- $p = 564538252084441556247016902735257$
- $E : y^2 = x^3 + 321094768129147601892514872825668x + 430782315140218274262276694323197$ over $\mathbb{F}_p$
- $\ell = 28226912604222077812350845136775 3$
- $\mathrm{End}(E) = \mathcal{O}_d$ where $d = -1662463135200311258479604622103147$ (n.b. this order is maximal)
- $\mathfrak{L} = (282269126042220778123508451367753, 2w + 1051376607341231209053104894724 70)$ where $w = \frac{1+\sqrt{d}}{2}$
- $P = (97339010987059066523156133908935, 149670372846169285760682371978898)$

Then, using Sutherland's `smoothrelation` program, we obtain

$$\mathfrak{L} = \left(\frac{\beta}{m}\right)\bar{\mathfrak{p}}_7^{72}\bar{\mathfrak{p}}_{13}^{100}\bar{\mathfrak{p}}_{23}^{14}\bar{\mathfrak{p}}_{47}^{2}\bar{\mathfrak{p}}_{73}^{2}\bar{\mathfrak{p}}_{103}\mathfrak{p}_{179}\mathfrak{p}_{191}$$

Resulting curve E' and values of m, β and $\phi(P)$

$$m = 7^{72} 13^{100} 23^{14} 47^{2} 73^{2} 103^{1} 179^{1} 191^{1}$$

$$\begin{aligned}\beta = {} & 33839476010201212678153099318918935556774403746141370474 92\backslash \\ & 98715122260417314622648471444260197118494483544222058008848 37 \\ & - 1713152334033312180094376774440754045496152167352278262491\backslash \\ & 5890140971672388272394276444760757048909796 85 \cdot w\end{aligned}$$

Then $E' = y^2 = x^3 + 840812629621647700320334943079 76x + 50692858542723838730751004194 4828$ and $\phi(P) = (45068965671865226880353686849 6211, \pm 34560869787118983929267473456 7941)$.

References

- J. Hafner and K. McCurley. A rigorous subexponential algorithm for computation of class groups. J. Amer. Math. Soc., 2(4):837–850, 1989.
- R. Bröker, D. Charles, and K. Lauter. Evaluating large degree isogenies and applications to pairing based cryptography. In Pairing' 08: Proceedings of the 2nd international conference on Pairing-Based Cryptography, pages 100–112, Berlin, Heidelberg, 2008. Springer-Verlag.
- S. D. Galbraith, F. Hess, and N. P. Smart. Extending the GHS Weil descent attack. In Advances in cryptology—EUROCRYPT 2002 (Amsterdam), volume 2332 of Lecture Notes in Comput. Sci., pages 29–44. Springer, Berlin, 2002.
- G. Bisson and A. Sutherland, Computing the endomorphism ring of an ordinary elliptic curve over a finite field, J. Num. Thy. 2009