On computing isogenies of unknown degree

Luca de Feo

On computing isogenies of unknown degree

Luca De Feo

July 26, 2010

Abstract

We present an extension to Couveignes algorithm that, given two elliptic curves E and E', permits to compute all isogenies of degrees up to a certain bound N in time $\tilde{O}(N^2)$.

It is well known that two curves having the same number of points over a finite field are isogenous, however this doesn't say anything on the degree of the isogeny connecting them. Given two elliptic curves E and E' defined over $\mathbb{F}_q$ and having the same number of points, we want to find the smallest degree isogeny between them.

The simplest solution is to take any algorithm computing a fixed degree isogeny and try all the degrees until an isogeny is found. If ℓ is the degree of the smallest isogeny, this of course adds a factor ℓ to the complexity of any polynomial time algorithm.

Couveignes' algorithm [1], however, can be easily adapted to solve this problem at no additional cost. This short paper is not self-contained: we make references to the variants and improvements to Couveignes' algorithm given in [2].

Observe that in Couveignes' algorithm, apart for the choice of k, the computation of $E[p^k]$ and the polynomial interpolation step do not depend at all on ℓ. The degree of the isogeny only comes into play in the last part of the Cauchy interpolation, that is the rational function reconstruction. We study more in detail this last step.

Rational Function Reconstruction Rational function reconstruction takes as input a degree n polynomial T, a polynomial A of degree less than n and a target degree $m \leqslant n$ and outputs the unique rational function such that

$$A \equiv \frac{R}{V} \bmod T$$

and $\deg R < m$, $\deg V \leqslant n - m$. This is done by computing a Bezout relation $AV + TU = R$ with the expected degrees via an XGCD algorithm. If a classical XGCD algorithm is used, one simply computes all the lines

$$\begin{aligned} R_0 &= T, & U_0 &= 1, & V_0 &= 0, \\ R_1 &= A, & U_1 &= 0, & V_1 &= 1, \\ R_{i-1} &= Q_i R_i + R_{i+1}, & U_{i+1} &= U_{i-1} - Q_i U_i, & V_{i+1} &= V_{i-1} - Q_i V_i \end{aligned} \tag{1}$$

and stops as soon as a remainder R_{i+1} with $\deg R_{i+1} < m$ is found. If a fast XGCD algorithm as [3, Algo. 11.4] is used, one directly aims at the two lines

$$\begin{aligned} R_{h-2} &= Q_{h-1}R_{j-1} + R_h \\ R_{h-1} &= Q_h R_h + R_{h+1} \end{aligned} \tag{2}$$

such that $\deg R_{h+1} < m \leqslant \deg R_h$ without computing the intermediate lines.

When looking for an ℓ-isogeny, one simply sets $m = \ell+1$. Observe that if the algorithm doesn't return a rational fraction $\frac{R}{V}$ with $\deg R = \ell$ and $\deg V = \ell-1$, then no such fraction congruent to A modulo T exists.

If ℓ is not *a priori* known, we can still use the fact that a separable isogeny with cyclic kernel must have $\deg R = \deg V + 1$. In fact if we suppose $R = R_i$ and $V = V_i$, then

$$\begin{aligned} \deg T &= \deg V_{i+1} + \deg R_i, \\ \deg R_i - \deg V_i &= \deg R_{i-1} - \deg V_{i+1} \end{aligned}$$

implies

$$\deg T + 1 = \deg R_{i-1} + \deg R_i\ .$$

Hence, if A is congruent to an ℓ-isogeny with $\ell = \left\lfloor \frac{\deg T}{2} \right\rfloor - t$ for some $t \geqslant 0$, then

$$\deg R_{i-1} = \left\lceil \frac{\deg T}{2} \right\rceil + t + 1 > \left\lfloor \frac{\deg T}{2} \right\rfloor - t = \deg R_i\ . \tag{3}$$

Thus we can recover any isogeny having degree less than $\left\lfloor \frac{\deg T}{2} \right\rfloor$ using either a classical or a fast XGCD algorithm setting $m = \left\lceil \frac{\deg T}{2} \right\rceil + 1$.

Recognising an isogeny Once we have a rational fraction with the required degree, we have to test if it really is an isogeny. In order to understand how often we have to make this test, we introduce some more terminology. Let $n_i = \deg R_i$, we call $(n_0, \ldots, n_r)$ the *degree sequence* of A and T; a degree sequence is said *normal* if $n_i = n_{i+1} + 1$ for any i.

Proposition 1. *Let $f, g \in \mathbb{F}_q[X]$ be uniformly chosen random polynomials of respective degrees $n_0 > n_1 > 0$ and let $(n_0, n_1, \ldots, n_r)$ be their degree sequence. For $0 \leqslant i < n_1$ define the binary random variables $X_i = 1 \Leftrightarrow i \in (n_0, n_1, \ldots, n_r)$, then the X_i are independent random variables and* $\mathrm{Prob}(X_i = 0) = \frac{1}{q}$.

Proof. Pairs of polynomials f, g are in bijection with the GCD-sequence $(R_r, Q_r, \ldots, Q_1)$ constituted by their GCD and the quotients of the GCD algorithm. To each such sequence is associated a degree sequence

$$(n_0, n_1, \ldots, n_r) = \left(\deg R_r + \sum_{i=1}^{r} \deg Q_i, \ldots, \deg R_r + \sum_{i=1}^{1} \deg Q_i, \deg R_r \right)\ ,$$

thus for any given degree sequence there are

$$(q-1)q^{n_0-n_1}\cdot(q-1)q^{n_1-n_2}\cdot\dots\cdot(q-1)q^{n_r}=(q-1)^{r+1}q^{n_0}$$

GCD-sequences.

Let I and O be two disjoints subsets of $\{X_i\}$, the number of GCD-sequences such that $X\in I\Rightarrow X=1$ and $X\in O\Rightarrow X=0$,

$$\sum_{s=0}^{n_1-\#I-\#O}\binom{n_1-\#I-\#O}{s}(q-1)^{s+2+\#I}q^{n_0}=(q-1)^{2+\#I}q^{n_0}q^{n_1-\#I-\#O}\;.$$

There are $(q-1)^2q^{n_0}q^{n_1}$ pairs of polynomials of degrees n_0,n_1, thus

$$\mathrm{Prob}\big(\{X=1\mid X\in I\},\{X=0\mid X\in O\}\big)=\left(\frac{q-1}{q}\right)^{\#I}\left(\frac{1}{q}\right)^{\#O}\;.\qquad(4)$$

The claim follows. □

Degree sequences associated to isogenies are in general not normal, in fact if $\ell\leqslant\left\lfloor\frac{\deg T}{2}\right\rfloor-t$, equation (3) shows that there must be at least a gap of degree $2c$ in the degree sequence. Heuristically, we can expect that if the polynomial A doesn't correspond to an isogeny, then A and T act like random polynomials, thus, by the proposition above, the probability that A looks like an isogeny of degree $\ell\leqslant\left\lfloor\frac{\deg T}{2}\right\rfloor-t$ is less than $\frac{1}{q^{2t}}$.

Therefore, by choosing an appropriate $t\in O(\log_q p^k)$, our variant can find any isogeny of degree less than $\frac{p^k-1}{4}-t$ at the same cost of one run of Couveignes' algorithm.

No other method for computing isogenies is known to have a similar generalisation. This makes Couveignes' algorithm a rather surprising exception and we wonder whether this simple idea can find interesting applications.

References

[1] J.-M. Couveignes. Computing ℓ-isogenies using the p-torsion. in *ANTS'II*, 59–65. Springer, 1996.

[2] L. De Feo. Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic, To appear in *Journal of Number Theory*, 2010.

[3] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.