On The Relationship Between The Discrete Logarithm Problems On Isogenous Elliptic Curves

Steven Galbraith

Royal Holloway and Bedford New College
University of London.

stevenga@dcs.rhbnc.ac.uk

http://www.dcs.rhbnc.ac.uk/~stevenga/ecc.html

Contents

Some Questions and Problems

Let $E/\mathbb{F}_q$ be an elliptic curve and write L for the largest prime factor of the group order $\#E(\mathbb{F}_q)$.

One tends to measure the security of the cryptographic system in terms of the size of the largest prime factor L.

Question: Let E_1 and E_2 be elliptic curves over the same field $\mathbb{F}_q$ such that they both have the same largest prime divisor L of their number of points. Does the discrete logarithm problem have the same difficulty on each curve?

Problem: Let E_1 and E_2 be elliptic curves over $\mathbb{F}_p$ such that $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$. Is there an efficient method to reduce the discrete logarithm problem on $E_1(\mathbb{F}_p)$ to that on $E_2(\mathbb{F}_p)$?

From now on E_1 and E_2 will be non-supersingular and such that $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$.

The Isogeny Theorem

Theorem: (Tate) Let E_1 and E_2 be elliptic curves over $\mathbb{F}_p$ such that $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$. Then there is an isogeny $\phi : E_1 \to E_2$ which is defined over $\mathbb{F}_p$.

An *isogeny* is a morphism of elliptic curves which maps the point at infinity on one curve to the point at infinity on the other. One can prove that an isogeny is always a group homomorphism.

With the notation as in the theorem, an isogeny defined over $\mathbb{F}_p$ induces a group homomorphism $E_1(\mathbb{F}_p) \to E_2(\mathbb{F}_p)$.

All non-zero isogenies have finite kernel. We will be able to restrict to separable isogenies, and so we will call an isogeny whose kernel has size n an n-isogeny.

Isomorphisms

If the elliptic curves E_1 and E_2 have the same j-invariant then they are *isomorphic* and the isomorphism is defined over $\mathbb{F}_p$.

If the curves E_i are written in the form

$$y^2 = x^3 + A_i x + B_i$$

then calculate $u = (A_2/A_1)^{1/4} = (B_2/B_1)^{1/6} \in \mathbb{F}_p$ and the isomorphism is

$$\phi : (x, y) \longmapsto (u^2 x, u^3 y).$$

Therefore, there is a polynomial time translation of the discrete logarithm problem between isomorphic curves with the same number of points.

Endomorphisms And Orders

Define $End(E) = \{$all isogenies mapping $E \to E\}$.

If $E/\mathbb{F}_p$ is ordinary (i.e., not supersingular) then $End(E)$ is an order in an imaginary quadratic field.

An *imaginary quadratic field* is $K = \mathbb{Q}(\sqrt{d})$ where $d < 0$ is square-free integer. The *discriminant* of K is

$$D = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{otherwise.} \end{cases}$$

The *maximal order* in K is

$$\mathcal{O}_K = \mathbb{Z}[(D + \sqrt{D})/2].$$

An *order* in K is a subring of $\mathcal{O}_K$ of the form

$$\mathcal{O} = \mathbb{Z}[c(D + \sqrt{D})/2]$$

where c is a positive number called the *conductor* (or *index*) of the order $\mathcal{O}$. The order $\mathcal{O}$ has discriminant $c^2 D$ and therefore c is uniquely determined by the discriminant of the order $\mathcal{O}$.

Endomorphism Rings Of Elliptic Curves Over Finite Fields

Let $E/\mathbb{F}_p$ be an ordinary elliptic curve with

$$\#E(\mathbb{F}_p) = p + 1 - t$$

(so that t is the trace of the Frobenius endomorphism π).

It is clear that $\mathbb{Z}[\pi] \subseteq End(E)$. This means that $End(E)$ is an order in $\mathbb{Q}(\sqrt{t^2 - 4p})$ which contains the order of discriminant $t^2 - 4p$. In other words, the conductor of $End(E)$ divides the square-part of $t^2 - 4p$.

It is a fact that all isogenies in $End(E)$ are actually defined over $\mathbb{F}_p$.

Relationship Between Class Numbers

The number of elliptic curves over $\mathbb{F}_p$ with endomorphism ring isomorphic to $\mathcal{O}$ is equal to the class number $h_{\mathcal{O}}$ (which is the size of the group $Pic(\mathcal{O})$).

The class number of an order $\mathcal{O}$ of conductor c in a field K is related to the class number of the field K by the formula

$$h_{\mathcal{O}} = h_K c[\mathcal{O}_K^* : \mathcal{O}^*] \prod_{p|c} \left(1 - (\frac{K}{p})p^{-1}\right).$$

Theorem: The number of isomorphism classes of elliptic curves in an isogeny class is $O(\sqrt{p})$.

Handling The Conductor

Theorem: Let $\phi : E_1 \to E_2$ be an isogeny and suppose a prime l divides the index $[End(E_1) : End(E_2)]$ (or vice versa). Then the degree of ϕ is divisible by l.

Theorem: Let E be an elliptic curve over $\mathbb{F}_p$ having endomorphism ring $\mathcal{O}$ where $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$. Let l be a prime number. The following list classifies the possibilities for the l-isogenies defined over $\mathbb{F}_p$.

- If $l \not| [\mathcal{O}_K : \mathcal{O}]$ then there are $1 + \left(\frac{D}{l}\right)$ l-isogenies to elliptic curves with endomorphism ring $\mathcal{O}$.
- If $l | [\mathcal{O}_K : \mathcal{O}]$ then there is one l-isogeny up to an elliptic curve.
- If $l \not| [\mathcal{O} : \mathbb{Z}[\pi]]$ then there are no l-isogenies down.
- If $l | [\mathcal{O} : \mathbb{Z}[\pi]]$ and $l | [\mathcal{O}_K : \mathcal{O}]$ then there are a total of l l-isogenies down.
- If $l | [\mathcal{O} : \mathbb{Z}[\pi]]$ and $l \not| [\mathcal{O}_K : \mathcal{O}]$ then there are $l - \left(\frac{D}{l}\right)$ l-isogenies down.

We need to be able to find isogenies between elliptic curves. This is achieved using modular curves.

Let $\Phi_l(x, y)$ be the standard modular equation for $X_0(l)$. Let $E/\mathbb{F}_p$ be an elliptic curve. Then the elliptic curves E' such that there is an l-isogeny over $\mathbb{F}_p$ from E to E' are those whose j-invariants are the roots of $\Phi_l(j(E), y) \pmod p$.

Work of Elkies and Vélu

Let $E: y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_p$ and let j' be a root of $\Phi_l(j(E), y) \pmod{p}$. Elkies has shown how to compute a polynomial $\psi(x)$ whose roots are the x-coordinates of the points in the kernel of the l-isogeny from E to a curve E' with $j(E') = j'$.

Vélu has shown how to construct an equation for E' and explicit equations for the isogeny $E \to E'$ from the polynomial $\psi(x)$ above.

Strategy Of The Method

Tate's theorem shows that there is some N-isogeny from E_1 to E_2. Rather than finding this isogeny we will find a chain

$$E_1 \simeq E_0' \xrightarrow{\varphi_1} E_1' \xrightarrow{\varphi_2} E_2' \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} E_n' \simeq E_2$$

of isogenies of prime degree.

The first phase of the method is to move from the elliptic curves E_i to elliptic curves whose endomorphism ring is the maximal order. We do this using Kohel's algorithm.

The second phase of the method is to find a chain of prime degree isogenies between these two elliptic curves.

The method is given in 4 stages.

Compute the conductor c of the order $\mathbb{Z}[\pi]$. This is the largest integer such that

$$(t^2 - 4p)/c^2 \equiv 0, 1 \pmod 4.$$

Choose a set of primes

$$\mathcal{L} := \left\{ \text{primes } l : (l, c) = 1, \left(\frac{D}{l}\right) = 1 \text{ and } l < 6(\ln|D|)^2 \right\}.$$

These primes will (assuming the GRH) generate the ideal class group of the field K.

Compute the modular equations $\Phi_l(x, y)$ modulo p for each $l \in \mathcal{L}$ and each $l|c$.

For each curve E_i, find a chain of isogenies from E_i to an elliptic curve E_i' whose endomorphism ring is the maximal order. Set j_1 and j_2 to be the j-invariants of these new curves E_1' and E_2'.

This is done using Kohel's algorithm:

For each prime $l|c$ construct the tree of l-isogenies containing a given j-invariant. An elliptic curve E is "on the floor" at l (which means that the power of l dividing the index $[\mathcal{O}_K : End(E)]$ is the full power of l dividing c) if and only if there is exactly one l-isogeny from E.

Determining which l-isogenies lead downwards allows us to select the unique chain of l-isogenies up to an elliptic curve E' such that

$$l \nmid [\mathcal{O}_K : End(E')].$$

Starting from j_1, construct a (graph-theoretic) tree, whose vertices are labelled as j-invariants and whose edges (labelled by l) correspond to isogenies of prime degree l.

Initially, the tree consists of the vertex labelled j_1 and has no edges.

Choose primes $l \in \mathcal{L}$ at random and, for each vertex j in the tree, find the roots of $\Phi_l(j, y) \pmod{p}$. For each root, determine whether it appears already in the tree. If not then add a vertex corresponding to it and add an edge (labelled l) between it and the vertex j.

Once j_2 appears as a vertex in the tree, find the path connecting j_1 to j_2.

Add this chain of l-isogenies to those already found in Stage 1 (it will usually be necessary to take some isomorphisms to make the chains match up).

Use the theory of Elkies and Vélu to construct the explicit polynomial form of each l-isogeny.

At this stage, instances of the discrete logarithm problem on the curve E_1 may be translated to instances on E_2.

Complexity

We assume unit cost for operations in the field $\mathbb{F}_p$. Initially, we will express the complexity in terms of both h_K and c.

Stage 0: Computing a modular equation $\Phi_l(x, y)$ modulo p requires time $O(l^3)$ and space $O(l^2)$. Thus, computing the modular equations for $l \in \mathcal{L}$ requires polynomial time and space. Dealing with the primes $l|c$ requires $O(c^3)$ time and $O(c^2)$ space.

Stage 1: Finding roots of $\Phi_l(j, y) \pmod p$ can be performed in $O(l^2)$ operations in $\mathbb{F}_p$. This stage therefore requires $O(c^3)$ time and $O(\ln c)$ space.

Stage 2: The tree will have size h_K and, in the worst case, $O(h_K)$ iterations will be needed to construct the full tree. This stage therefore takes time $O(h_K^2(\ln p)^4)$. The chain of isogenies has length $O(h_K)$.

Complexity Continued

Stage 3: Searching through a tree of h_K vertices takes time $O(h_K)$. The length of the total chain of prime degree isogenies is $O(h_K + \ln c)$. The methods of Elkies and Vélu for finding explicit equtions for a given n-isogeny take time $O(n^3)$ and storage $O(n^2)$. For the primes $l \in \mathcal{L}$ this is polynomial time. For the primes $l|c$ this is $O(c^3)$ time and $O(c^2)$ space.

For the worst case analysis we must take c and h_K to be $O(p^{1/2})$. The total complexity is therefore $O(p^{3/2})$ time and $O(p)$ space.

If c is $O(\ln p)$-smooth and if h_K is $O(\ln p)$ then the method becomes polynomial time.

We have been very cautious in the above analysis. It seems plausible to assume the following:

Assumption: It is possible to construct the tree of isogenies so that there is a path between any two vertices of length $O(\ln h_K)$.

In this case the chain of isogenies has length polynomial in the prime p.

In the case when c is $O(\ln p)$-smooth then evaluation of the chain of isogenies, once it has been constructed, can be performed in polynomial time.

Conclusions

The questions posed in the introduction have not been fully answered.

We have seen that for elliptic curves such as those generated by the CM method, the discrete logarithm problems have the same complexity. Note that this does not indicate that such curves are any stronger or weaker than random curves.

For elliptic curves chosen at random, which have the same number of points, it is not clear whether discrete logarithms on some of them are easier than on others.

David Kohel has pointed out that we are asking for isogenies between the 1-dimensional group schemes E. A topic for further research would be to find isogenies between the 0-dimensional group schemes $E[\pi - 1, L]$.