The DLP on Elliptic Curves with the same order

Marios Magioladitis

Forschungsseminar WS2007/2008

Institute of Experimental Mathematics (IEM)
University of Duisburg-Essen

January 2008

Forschungsseminar Wintersemester 2007/2008.
Organisation: Gabor Wiese.

Lecture **The DLP on Elliptic Curves with the same order** was given on the 15th of January 2008 in the Institute of Experimental Mathematics (IEM).

I would like to thank Andrey Timofeev for his help.

Marios Magioladitis
Homepage: http://www.exp-math.uni-essen.de/~magiolad
E-mail: magiolad@iem.uni-due.de

References

[JMV] D. Jao, St. Miller, R. Venkatesan, *Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?*
[Smith] B. Smith, *Isogenies and the Discrete Logarithm Problem on Jacobians of Genus 3 Hyperelliptic Curves*
[Kohel] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, University of California, Berkeley, 1996 (Ph.D. thesis).
[Iwaniec] H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics, vol. 17, AMS, Providence, RI, 1997.

Chapter 1

Setting the problem

In the following p will always be a prime number and q a power of p.

Definition 1.1. *Let K be a field and let E_1 and E_2 be two elliptic curves over K. We say that E_1 and E_2 are isogenous if there exists a non-trivial algebraic group homomorphism $\phi : E_1 \to E_2$. We say that this ϕ is an isogeny.*

Definition 1.2. *If ϕ is an isogeny the degree of the ϕ is defined as $\deg(\phi) := \# \ker(\phi)$.*

Theorem 1.3. *(Tate) Let E_1 and E_2 be two elliptic curves over F_q.*

$$E_1 \textit{ and } E_2 \textit{ are isogenous } \Leftrightarrow |E_1| = |E_2|.$$

Question: If we conider two isogenous elliptic curves, is there any difference in security? Is any difference in the DLP?

Answer: No. (Assuming GRH and that the curves have the same endomorphism ring over $\bar{\mathbb{F}}_q$).

The requirement for the curves to have the same endomorphism ring is technical. All known polynomial time techniques for constructing equal order curves produce only curves with nearly equal endomorphism ring.

Question: Can we extend this result for curves of genus 2?

Answer: Hopefully we can.

Question: Can we extend this result for curves of genus 3?

Answer: No.

There are two classes of curves of genus 3: hyperelliptic and non-hyperlleptic. A hyperelliptic curve cannot be isomorphic to a non-hyperlleptic.

- Gaudry, Thomé, Thériault and Diem showed that the DLP in Jacobians of hyperelliptic curves of genus 3 over $\mathbb{F}_q$ may be solved in $\tilde{O}(q^{4/3})$ group operations.
- Diem's index calculus algorithm can solve the DLP in Jacobians of non-hyperelliptic curves of genus 3 over $\mathbb{F}_q$ in $\tilde{O}(q)$ group operations.

As a result, the security of non-hyperelliptic curves of genus 3 is considered to be lower than that of hyperelliptic. In order to extend the work for elliptic curves to curves with genus 3 is better to restrict ourselves in hyperlliptic curves.

Definition 1.4. *An order $\mathcal{O}$ in a field K is a subset of K s.t.*

(i) *$\mathcal{O}$ is a subring of K containing* 1,

(ii) *$\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module,*

(iii) *$\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.*

Remark 1.5. *We call $\mathcal{O}_K$ the maximal order of K, since it contains any order of K. The index $f = [\mathcal{O}_K : \mathcal{O}]$ is called the conductor of the order $\mathcal{O}$. The discriminant D of $\mathcal{O}$ is equal to $D := f^2 d_K$, where d_K is the discriminant of K.*

Remark 1.6. *Let $\mathcal{O}$ be an order in a quadratic field K.*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K.$$

Definition 1.7. *Let E be an elliptic curve over $\mathbb{F}_q$. An endomorphism of E is an isogeny $E \to E$.*

We define $\mathrm{End}\,(\mathrm{E}) = \{\eta : \mathrm{E} \to \mathrm{E} \mid \eta \text{ endomorphism}\} \cup \{0\}$ *to be the ring of endomorphisms of E.*

Theorem 1.8. *(Deuring, 1941)* $\mathrm{End}\,(\mathrm{E})$ *is isomorphic to an order to the quaternion algebra or to an order in an imaginary quadrartic field. In the first case we say E is supersingular and in the second case we say E is ordinary.*

Let $S_{N,q}$ be the set of all elliptic curves over $\mathbb{F}_q$, up to isomorphism, that have order N over $\mathbb{F}_q$.

Two elliptic curves E_1 and E_2 defined over $\mathbb{F}_q$ are said to belong in the same isomorphism class if $E_1, E_2 \in S_{N,q}$ for some N.

Curves in the same isomorphism class are either all supersingular or all ordinary. Let $E_1, E_2 \in S_{N,q}$. We say that E_1 and E_2 have the same level if $\mathrm{End}\,(\mathrm{E}_1) = \mathrm{End}\,(\mathrm{E}_2)$.

In the following we'll prove the following:

Corollary 1.9. *(Assuming GRH) The DLP on elliptic curves is random reducible in the following sense: Given any algorithm A that solves DLP on some fixed positive proportion of curves in a fixed level, then DLP can probabilistically solved on any given curve in the same level with* $\mathrm{polylog}\,(q)$ *expected queries to A with random inputs.*

Method to prove the corollary: Use elements of graph theory. Introduce the "isogeny graph" and do random walks on it.

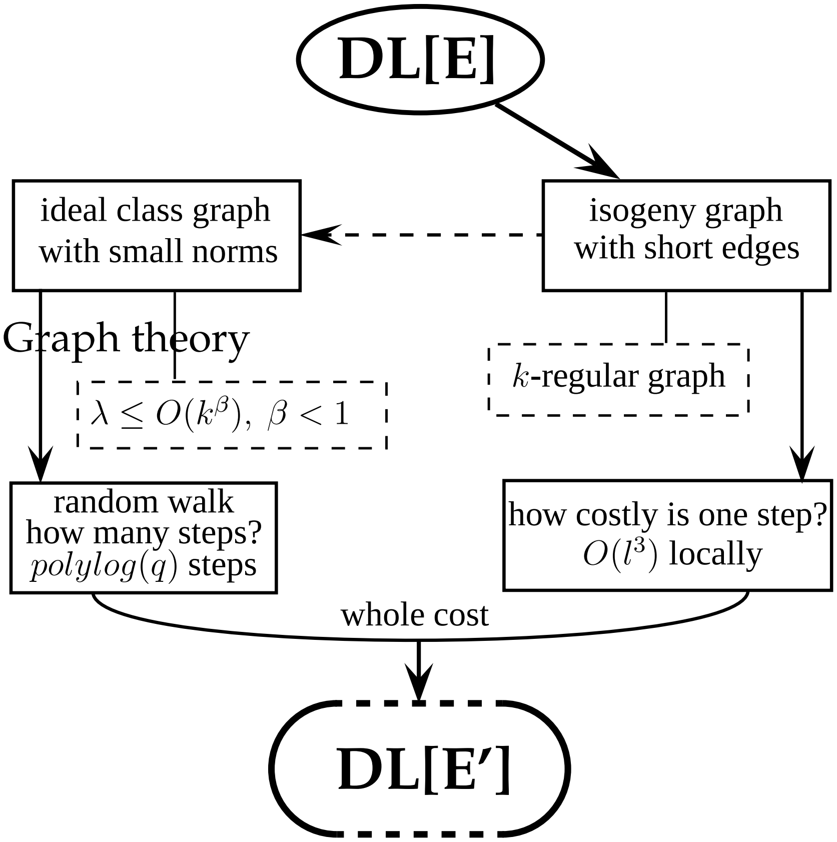
DL[E]
ideal class graph with small norms
isogeny graph with short edges
Graph theory
k-regular graph
$\lambda \leq O(k^{\beta}),\ \beta < 1$
random walk how many steps? $polylog(q)$ steps
how costly is one step? $O(l^3)$ locally
whole cost
DL[E′]

Figure 1.1: Sketch of proof

Chapter 2

Isogenies of CM curves

Definition 2.1. *Let E an elliptic curve defined over $\mathbb{F}_q$ and K the field containing* $\mathrm{End}\,(\mathrm{E})$*. The field K is called the CM field of E we write c_E of the conductor of* $\mathrm{End}\,(\mathrm{E})$ *and c_π for the conductor of $\mathbb{Z}[\pi]$.*

From now on, we assume that we are in the ordinary case.

The following theorem describes the structure of elliptic curves within an isogeny class from the point of view of their endomorphism ring.

Theorem 2.2. *Let E_1 and E_2 be ordinary isogenous elliptic curves defined over $\mathbb{F}_q$. Let K denote the imaginary quadratic field containing* $\mathrm{End}\,(\mathrm{E}_1)$ *and $\mathcal{O}_K$ its maximal order.*

1. $\mathbb{Z}[\pi] \subseteq \mathrm{End}\,(\mathrm{E}_1), \mathrm{End}\,(\mathrm{E}_2) \subseteq \mathcal{O}_\mathrm{K}$.

2. $\mathrm{End}\,(\mathrm{E}_2) \subset \mathrm{K}$

3. *The following are equivalent:*

   (a) $\mathrm{End}\,(\mathrm{E}_1) = \mathrm{End}\,(\mathrm{E}_2)$,

   (b) $\exists \phi, \psi : E_1 \to E_2$ *isogenies over $\mathbb{F}_q$ of relatively prime degree,*

   (c) $[\mathcal{O}_K : \mathrm{End}\,(E_1)] = [\mathcal{O}_K : \mathrm{End}\,(E_2)]$ *(i.e. $c_{E_1} = c_{E_2}$),*

   (d) $[\mathrm{End}\,(\mathrm{E}_1) : \mathbb{Z}[\pi]] = [\mathrm{End}\,(\mathrm{E}_2) : \mathbb{Z}[\pi]]$.

4. *Let $\phi : E_1 \to E_2$ be an isogeny of prime degree l, defined over $\mathbb{F}_q$. Then* $\mathrm{End}\,(\mathrm{E}_1) \subseteq \mathrm{End}\,(\mathrm{E}_2)$ *or* $\mathrm{End}\,(\mathrm{E}_2) \subseteq \mathrm{End}\,(\mathrm{E}_1)$*, and the index of the smaller in the larger divides l.*

5. *Let l prime that divides exactly one of c_{E_1} and c_{E_2}. Then, for every isogeny $\phi : E_1 \to E_2$ defined over $\mathbb{F}_q$ we have that $l \mid |\phi|$.*

Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$. Let π be the Frobenius endomorphism relative to $\mathbb{F}_q$. The following are equivalent:

1. $\mathbb{Q} \subset \mathrm{End}\,(\mathrm{E}) \subset \mathbb{C}$.
2. $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}, \forall r > 0$.
3. The dual of the Frobenius endomorphism is separable.
4. $(\mathrm{Tr}\,(\pi), q) = 1$.

For the following we denote: $\mathcal{O} = \mathrm{End}\,(\mathrm{E}), \mathcal{O}' = \mathrm{End}\,(\mathrm{E}'), \mathcal{O}_\mathrm{l} = \mathcal{O} \otimes \mathbb{Z}_\mathrm{l}$ and $\mathbb{Z}[\pi]_l = \mathbb{Z}[\pi] \otimes \mathbb{Z}_l$.

Proposition 2.3. *Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ with endomorphism ring $\mathcal{O}$ of discriminant D. Let l be a prime, and let $(\frac{D}{l})$ be the Legendre symbol.*

1. *$\mathcal{O}_l$ maximal $\Rightarrow \exists(\frac{D}{l}) + 1$ isogenies of degree l to curves with endomorphism ring isomorphic to $\mathcal{O}$.*
2. *$\mathcal{O}_l$ nonmaximal $\Rightarrow \nexists$ isogenies of degree l with endomorphism ring $\mathcal{O}$.*
3. *If there exist more than $(\frac{D}{l}) + 1$ isogenies of degree l, up to isomorphism, then all isogenies of degree l are defined over $\mathbb{F}_q$, and up to isomorphism of the pairs (E, E') are exactly*

$$\left(l - (\frac{D}{l})\right)[\mathcal{O}^* : \mathcal{O}'^*]^{-1}$$

elliptic curves E' and isogenies $E \to E'$ of degree l s.t. $\mathcal{O}'$ is properly contained in $\mathcal{O}$.

Proof. Proposition 23 of [Kohel]. □

Computing the endomorphism ring

We consider an elliptic curve E over a field K. Let c_π be the conductor of $\mathbb{Z}[\pi]$.

We know that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\pi - \alpha}{c_\pi}\right],$$

where α is known.

We can compute the order of the curve in polynomial time (for example using Schoof's algorithm). We obtain the trace of Frobenius t by the formula $t = q + 1 - \#E(\mathbb{F}_q)$ and afterwards the discriminant $t^2 - 4q$. Since $c_\pi d_K^2 = t^2 - 4q$, c_π can be computed deterministically.

We remind that

$$c_\pi = c_E[\mathrm{End}\,(\mathrm{E}) : \mathbb{Z}[\pi]].$$

In the case that $End(E) = \mathcal{O}_K$ (i.e. $c_E = 1$) we are done. We can use a theorem of Kohel to determine the isomorphic type of the endomorphism expicitly in every case.

Theorem 2.4. *There exists a deterministic algorithm that given an ellict curve E over the field $\mathbb{F}_q$, computes the isomorphism type of the endomorphism ring E. If GRH holds, for any $\epsilon > 0$ the algorithm runs in time $O(q^{1/3+\epsilon})$.*

Proof. Theorem 24 of [Kohel]. □

Chapter 3

Properties of isogenies of elliptic curves

We say that an isogeny $\phi : E_1 \to E_2$ of prime degree l defined over $\mathbb{F}_q$ is

-"**down**" if $[\mathrm{End}\,(E_1) : \mathrm{End}\,(E_2)] = l$
-"**up**" if $[\mathrm{End}\,(E_2) : \mathrm{End}\,(E_1)] = l$
-"**horizontal**" if $\mathrm{End}\,(E_1) = \mathrm{End}\,(E_2)$.

The following theorem classifies the number of degree l isogenies of each type:

Theorem 3.1. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$, with endomorphism ring* $\mathrm{End}\,(\mathrm{E})$ *of discriminant D. Let l be a prime different than p.*

- Assume $l \not| c_E$. There are exactly $1 + (\frac{D}{l})$ horizontal isogenies $E \to E'$ of degree l.

a. $l \not| c_\pi \Rightarrow$ no other isogenies of degree l over $\mathbb{F}_q$.

b. $l | c_\pi \Rightarrow \exists l - (\frac{D}{l})$ down isogenies of degree l.

- Assume $l | c_E$. There is one up isogeny of degree l.

a. $l \not| \frac{c_\pi}{c_E} \Rightarrow$ no other isogenies of degree l over $\mathbb{F}_q$.

b. $l | \frac{c_\pi}{c_E} \Rightarrow \exists l$ down isogenies of degree l.

Proof. Section 4.2 of [Kohel]. □

Case	Type	Subcase	Type
$l \nmid c_E$	$1 + (\frac{D}{l}) \rightarrow$	$l \nmid c_\pi$	
		$l \vert c_\pi$	$l - (\frac{D}{l}) \downarrow$
$l \vert c_E$	$1 \uparrow$	$l \nmid \frac{c_\pi}{c_E}$	
		$l \vert \frac{c_\pi}{c_E}$	$l \downarrow$

Table 3.1: Number and type of isogenies $E \rightarrow E'$ of degree l over $\mathbb{F}_q$.

An isogeny graph is a graph whose nodes consist of all elements in $S_{N,q}$ belonging to a fixed level.

Note that an horizontal isogeny always goes between two curves of the same level; likewise, an up isogeny enlarges the size of the endomoprhism ring and a down isogeny reduces its size.

Since there are fewer elliptic curves at higher levels than at lower levels, the collection of isogeny graphs, under the level interpretation, as a "pyramid" or a "volcano", with up isogenies ascending the structure and down isogenies descending.

Definition 3.2. *Let E_1, E_2 be two elliptic curves. We define two isogenies $\phi, \phi' : E_1 \rightarrow E_2$ to be be equivalent if there exists an automorphism $\alpha \in \mathrm{Aut}\,(\mathrm{E}_2)$ s.t. $\phi' = \alpha\phi$.*

Defining the isogeny graphs for small degree

Let now $\mathcal{O}$ to be the common endomorphism ring for all elliptic curves in a $S_{N,q}$ for some fixed N and q.

We denote $\mathcal{G}$ the regular graph whose:
-vertices are elements in $S_{N,q}$
-edges are equivalence classes of horizontal isogenies defined over $\mathbb{F}_q$ of prime degree $\leq (\log q)^{2+\delta}$, for a fixed constant $\delta > 0$.

Remark 3.3.

1. *We choose this degree bound because it must be small enough to permit isogenies to be computed, but large enough to allow the graph to be connected and to have the rapid mixing properties we 'll need later.*
2. *It is proven that a constant $\delta > 0$ that satisfies all the requirements exists, provided that we restrict the isogenies to a single level.*

By standard facts from Complex Multiplication Theory, each invertible ideal $\mathfrak{a} \subset \mathcal{O}$ produces an elliptic curve $\mathbb{C}/\mathfrak{a}$ definied over the ring class field L of $\mathcal{O}$. ($\mathbb{Q} \subset L \subset \mathbb{C}$).

The curve $\mathbb{C}/\mathfrak{a}$ has complex multiplication by $\mathcal{O}$, and two different ideals yield isomorphic curves if and only if they belong to the same ideal class.

Each invertible ideal $\mathfrak{b} \subset \mathcal{O}$ defines an isogeny $\mathbb{C}/\mathfrak{a} \rightarrow \mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1}$, and the degree of this isogeny is $N(\mathfrak{b})$.

Morover, it can be proved that for any prime ideal $\mathfrak{P}$ in L lying over p, the reductions $\mod \mathfrak{P}$ of the above elliptic curves and isogenies are defined over $\mathbb{F}_q$, and every elliptic curves and every horizontal isogeny in $\mathcal{G}$ arises in this way.

We conclude, that the isogeny graph $\mathcal{G}$ is isomorphic to the corresponging graph $\mathcal{H}$ whose

-nodes are elliptic curves $\mathbb{C}/\mathfrak{a}$ with CM by $\mathcal{O}$

-edges are complex analytic isogenies represented by ideals $\mathfrak{b} \subset \mathcal{O}$ of prime norm $\leq (\log q)^{2+\delta}$, for a fixed constant $\delta > 0$.

This isomorphism preserves the degrees of isogenies, in the sense that the degree of any isogeny in $\mathcal{G}$ is equal to the norm of its corresponding ideal $\mathfrak{b}$ in $\mathcal{H}$.

We can now create one more isomorphic graph to the above. The graph $\mathcal{H}$ has an alternate description as a Cayley graph $\mathcal{H}'$ on the ideal class group $\mathrm{Cl}\,(\mathcal{O})$ of $\mathcal{O}$. Indeed,

- each node of $\mathcal{H}'$ is an ideal class of $\mathcal{O}$,

- two ideal classes $[\mathfrak{a}_1], [\mathfrak{a}_2]$ are connected by an edge $\Leftrightarrow$ exists prime ideal $\mathfrak{b}$ with $N(\mathfrak{b}) \leq (\log q)^{2+\delta}$ s.t. $[\mathfrak{a}_1\mathfrak{b}] = [\mathfrak{a}_2]$.

Therefore,

$$\mathcal{G} \xrightarrow{\sim} \mathcal{H} \xrightarrow{\sim} \mathcal{H}'$$

Remark 3.4. *For ordinary curves we have that*

$$\mathrm{End}\,(\mathrm{E}_1) = \mathrm{End}\,(\mathrm{E}_2) \Rightarrow \mathrm{Aut}\,(\mathrm{E}_1) = \mathrm{Aut}\,(\mathrm{E}_2), \forall \mathrm{E}_1, \mathrm{E}_2 \in \mathrm{S}_{\mathrm{N,q}}.$$

Hence, the isogeny graph $\mathcal{G}$ is a symmetric graph and we can regard it as undirected.

Chapter 4

Eigenvalues of adjacency matrices of isogeny graphs

Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a finite graph with h vertices. We let $\mathcal{G}$ to be a k-regular graph, i.e. exactly k edges meet at each vertice.

Given a labeling of the vertices $\mathcal{V} = \{v_1, ..., v_h\}$ the adjacency matrix of $\mathcal{G}$ is the symmetric $h \times h$ matrix $A = [A_{ij}]$, where $A_{ij} = \#$of vertices between v_i and v_j

We can identify functions on $\mathcal{V}$ with vectors in $\mathbb{R}^h$ and think of A as a self-adjoint operation on $L^2(\mathcal{V})$. All the eigenvalues of A satisfy the bound $|\lambda| \leq k$.

Constant vectors are eigenfunctions of A with eigenvalue k. This is called the trivial eigenvalue.

A k-regular graph $\mathcal{G}$ is called a Ramanujan graph if all non-constant eigenvectors have eigenvalues $|\lambda| \leq 2\sqrt{k-1}$ for any nontrivial eigenvalue which is not equal $-k$ (the latter happens if and only if the graph is bipartite).

A "nearly Ramanujan" graph is a graph that all nontrivial eigenvalues of its adjacency matrix satify $O(k^\beta), \beta < 1$.

Proposition 4.1. *Let $\mathcal{G}$ be a k-regular graph on h vertices. Suppose that the eigenvalue λ of any nonconstant eigenvector satisfies the bound $|\lambda| \leq c$ for some $c < k$. Let S be any subset of the vertices of $\mathcal{G}$, and x be any vertex in $\mathcal{G}$. Then a random walk of any length at least $\frac{\log 2h/|S|^{1/2}}{\log k/c}$ starting from x will land in S with probability at least $\frac{|S|}{2h}$.*

Proof. Proposition 3.1 of [JMV]. □

If our isogeny graph is a k-regular graph, for some k, and has the properties of "nearly Ramanujan" graph we can get our result from the last proposition.

Problem: The isogeny graph has $O(\sqrt{q})$ vertices and this makes it too large to be stored.

Solution: We don't consider all the isogenies. We compute the graph locally.

There is a way, given an elliptic curve E and a prime number l to efficiently compute any curve E' which is connected to E with an isogeny of degree l.

Step 1: We find the j-invariants of E' be solving the modular polynomial relation $\Phi_l(j(E), j(E')) = 0$. This can be done in $O(l^3)$ field operations.

Step 2: We obtain the isogenies themselves by using an algorithm of Foquet and Morain.

Now we have to do a little work in the $\mathcal{H}$ graph. We recall that in this graph the elliptic curves are represented by ideal classes in an order $\mathcal{O}$ of a quadratic field K. We recall that these isogenies have prime degree $\leq m$, where $m = (\log q)^{2+\delta}, \delta > 0$.

We recall that, the $\mathcal{H}$ graph has one node for each ideal class of $\mathcal{O}$. So the total number of nodes in the graph $\mathcal{G}$ is the ideal class number of $\mathcal{O}$. We denote the ideal class representatives with $\{\alpha_1, ..., \alpha_h\}$.

For the following we denote $D = disc(\mathcal{O})$.

Proving that the non-trivial eigenvalues are properly bounded

The isomorphism between $\mathcal{G}$ and $\mathcal{H}$ implies that the generating function for degree n isogenies between the vertices α_i and α_j of $\mathcal{G}$ is given by

$$\sum_{n=1}^{\infty} M_{\alpha_i,\alpha_j}(n) q^n := \frac{1}{e} \sum_{z \in \alpha_i^{-1}\alpha_j} q^{N(z)/N(\alpha_i^{-1}\alpha_j)},$$

where e is the number of units in $\mathcal{O}$ ($e = 2$ for $D > 4$).

The righthand side sum depends only in the ideal class of the fractional ideal $\alpha_i^{-1}\alpha_j$ and in fact is a θ-series, which we can denote as $\theta_{\alpha_i^{-1}\alpha_j}(q)$.

Hence, we have that

$$\sum_{n=1}^{\infty} M_{\alpha_i,\alpha_j}(n) q^n = \frac{1}{e} \theta_{\alpha_i^{-1}\alpha_j}(q)$$

Theorem 4.2. *The sum above is a holomorphic modular form of weight* 1 *for* $\Gamma_0(D)$ *of* $SL(2,\mathbb{Z})$*, of nebentype* $\left(\frac{D}{\cdot}\right)$.

Proof. Theorem 10.9 of [Iwaniec]. □

We consider the simpler graph on $V = \{a_1, ..., a_h\}$ whose edges represent isogenies of degree exactly equal to n.

The adjacency matrix of this graph is the $h \times h$ matrix

$$M(n) = \left[M_{\alpha_i,\alpha_j}(n)\right]_{\{1\leq i,j\leq h\}}$$

We can do diagonilization to these adjacency matrices for all n's at once to get the eigenvalues.

In order to do this we define the matrix

$$A_q = \sum_{n\geq 1} M(n)q^n,$$

for any value $q < 1$ (where the sum converges absolutely).

Hence, we have that

$$A_q = \left[\sum_{n\geq 1} M_{\alpha_i,\alpha_j}(n)q^n\right] = \left[\frac{1}{e}\theta_{\alpha_i^{-1}\alpha_j}(q)\right],$$

where $1 \leq i, j \leq h$.

Let $\chi = \begin{bmatrix} \chi(a_1) \\ \vdots \\ \chi(a_h) \end{bmatrix}$ to be a character of $\mathrm{Cl}\,(\mathcal{O})$, then the i-th entry of the vector $A_q\chi$, computed by matrix multiplication is

$$(A_q\chi)(\alpha_i) = \frac{1}{e}\sum_{j=1}^{h} \theta_{\alpha_i^{-1}\alpha_j}(q)\chi(\alpha_j),$$

i.e. (by reindexing $\alpha_j \mapsto \alpha_i\alpha_j$)

$$(A_q\chi)(\alpha_i) = \frac{1}{e}\left(\sum_{j=1}^{h} \chi(\alpha_j)\theta_{\alpha_j}(q)\right)\chi(\alpha_i).$$

i.e.

$$(eA_q)\begin{bmatrix}\chi(a_1)\\ \vdots\\ \chi(a_h)\end{bmatrix} = \left(\sum_{\alpha_j\in \mathrm{Cl}\,(\mathcal{O})}\chi(\alpha_j)\theta_{\alpha_j}(q)\right)\begin{bmatrix}\chi(a_1)\\ \vdots\\ \chi(a_h)\end{bmatrix}.$$

i.e.

$$(eA_q)\chi = \left(\sum_{\alpha_j\in \mathrm{Cl}\,(\mathcal{O})}\chi(\alpha_j)\theta_{\alpha_j}(q)\right)\chi.$$

Hence, χ is an eigenvector of the matrix eA_q with eigenvalue equal to the sum of θ-functions enclosed in parentheses (called the Hecke θ-function).

We denote

$$\theta_\chi(q) = \sum_{\alpha_j\in \mathrm{Cl}\,(\mathcal{O})}\chi(\alpha_j)\theta_{\alpha_j}(q).$$

The L-functions of these Hecke characters can be written as

$$L(s,\chi) = \sum_{\mathfrak{a}\subset K}\chi(\mathfrak{a})(N\mathfrak{a})^{-s}$$

By setting

$$a_n(\chi) = \sum_{\mathfrak{a}\subset K, N\mathfrak{a}=n}\chi(\mathfrak{a})$$

we can write

$$L(s,\chi) = \sum_{n=1}^{\infty} a_n(\chi)n^{-s}.$$

Claim: $a_n(\chi)$ is the eigenvalue of $eM(n)$ for the eigenvector formed by the character χ as above.

Indeed,

$$A_q\chi = \sum_{n\geq 1} M(n)\chi q^n$$

i.e.

$$\left(e \sum_{n \geq 1} M(n) \chi q^n \right) (a_i) = \theta_\chi(q)(a_i).$$

By isolating the coefficient of q^n, we have that

$$eM(n)\chi = a_n(\chi)$$

Our isogeny graph is a superposition of the graphs $M(n)$, where n is a prime bounded by $m = (\log q)^{2+\delta}$ for some fixed $\delta > 0$.

We recall that is graph is isomorph to a graph on the elliptic curves represented by ideal classes in an order $\mathcal{O}$ of $K = \mathbb{Q}(\sqrt{d})$, whose edges are isogenies of prime degree $\leq m$.

The characters χ of $\mathrm{Cl}\,(\mathcal{O})$ are the common eigenvalues of the adjacency matrices $\{M(p) \mid p \leq m\}$ of these graphs. So their eigenvalues are

$$\lambda_\chi = \frac{1}{e} \sum_{p \leq m} a_p(\chi)$$

i.e.

$$\lambda_\chi = \frac{1}{e} \sum_{p \leq m} \left(\sum_{\mathfrak{a} \subset K, N\mathfrak{a} = p} \chi(\mathfrak{a}) \right).$$

We have a bound for the eigenvalues if we assume the GRH.

Lemma 4.3. *Let $D < 0$ and let $\mathcal{O}$ be the quadratic order with* $\mathrm{disc}\,(\mathcal{O}) = \mathrm{D}$. *If χ is a nontrivial character of* $\mathrm{Cl}\,(\mathcal{O})$, *then the GRH for $L(s, \chi)$ implies that the sum is bounded by $O(m^{1/2} \log |mD|)$ with an absolute implied constant.*

Proof. Lemma 4.1 of [JMV]. The proof assumes the GRH for the L-functions. It uses a result of Iwaniec to obtain the bound. □

Proving that the isogeny graph is k-regular

To prove that the isogeny graph is k-regular for some k we consider the special eigenvalue λ_{triv}.

When χ is the trivial character λ_{triv} equals the degree of the regular graph $\mathcal{G}$.

Since roughly half of rational primes p split in K, and those which do, split into two ideals of norm p we have that

$$\lambda_{triv} \sim \frac{1}{e}\pi(m) \sim \frac{m}{e\log m},$$

by the prime number theorem.

This eigenvalue is always the largest in absolute value, because $|\chi(\mathfrak{a})|$ always equals 1 when χ is the trivial character.

Proving that the isogeny graphs are nearly Ramanujan graphs

We have to prove that $\lambda_\chi = O(\lambda_{triv}^{\beta})$, for some $\beta < 1, \forall$ non-trivial eigenvalue.

There are only finitely many levels for q less than any given bound, so it suffices to prove it for q large.

By Lemma 4.3 we have that λ_χ is bounded by $O(m^{1/2}\log|mD|)$ with an absolute implied constant. On the other hand $|D| \leq 4q, \lambda_{triv} \sim \frac{m}{e\log m}, m = (\log q)^{2+\delta}, \delta > 0$. These imply that

$$\lambda_\chi = O(\lambda_{triv}^{\beta}),$$

for any $\beta > \frac{1}{2} + \frac{1}{\delta+2}$.

This proves that our graphs are nearly Ramanujan graphs.

Now we can state a theorem

Theorem 4.4. *(Assuming GRH) Let E be an elliptic curve of order N over $\mathbb{F}_q$. There exists a polynomial $P(x)$, independent of N and q, s.t. for $m = P(\log q)$ the isogeny graph $\mathcal{G}$ on each level is a nearly Ramanujan graph and any random walk on $\mathcal{G}$ will reach a subset of size h with probability at least $\frac{h}{2|\mathcal{G}|}$ after* polylog (q) *steps.*

Completing the proof of Theorem 4.4 and corollary 1.9

The last bound and Proposition 4.1 imply the random walk assertion of Theorem 4.4 and complete its proof.

The Theorem shows that a random walk from any fixed curve E, by using isogenies, probabilistically reaches the proportion where the algorithm succeeds, in at most polylog (q) steps. Since every step is a low degree isogeny, their composition can be computed in polylog (q) steps. This provides the random polynomial time reduction of DLOG along isogenous curves in the random walk, and hence from E to a curve for which the algorithm succeds. This completes the proof for the Corollary as well.