REPORTS@SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

Random walks on supersingular isogeny graphs

*Enric Florit Zacarías
Universitat de Barcelona.
efz1005@gmail.com

∗Corresponding author

Resum *(CAT)*

Aquest article dona una visió general de les corbes el·líptiques supersingulars i dels seus grafs d'isogènies. Els grafs d'isogènies han guanyat atenció durant els darrers quinze anys gràcies a les seves aplicacions per construir protocols criptogràfics resistents a atacs quàntics. El seu estudi involucra parlar de corbes el·líptiques, d'àlgebres de quaternions i de passeigs aleatoris sobre grafs (quasi) regulars. En aquest text, donem les eines necessàries per establir la propietat de Ramanujan, que connecta corbes supersingulars en característica p amb formes modulars de nivell p. A mode d'aplicació, expliquem la funció de hash de Charles, Lauter i Goren.

Abstract *(ENG)*

We survey several aspects of supersingular elliptic curves and their isogeny graphs. Isogeny graphs have obtained attention for the last fifteen years due to their uses in quantum-resistant cryptographic protocols. Studying them involves looking at elliptic curves, quaternion algebras, and random walks on (almost) regular graphs, among other topics. In particular, we give the tools necessary to state the Ramanujan property, connecting supersingular curves in characteristic p with modular forms of level p. We also explain the hash function of Charles, Lauter and Goren as an example of application.

Keywords: *isogenies, Ramanujan graphs, random walks.*
MSC (2020): *Primary 14H52, 05C48. Secondary 11F11.*
Received: *July 31, 2021.*
Accepted: *September 22, 2021.*

Acknowledgement

The author has been partially supported by a Màster+UB grant at the IMUB.

1. Introduction

The main goal of this article is to give an overview of the following result.

Theorem 1.1. *All isogeny graphs of supersingular elliptic curves are Ramanujan.*

Supersingular elliptic curves have received an increasing amount of attention due to their applications in postquantum cryptography. While classical elliptic curve cryptography relied on the group structure of elliptic curves over finite fields, isogeny-based cryptography uses morphisms between curves to work with large, random-looking graphs. The Ramanujan property is often cited when introducing supersingular cryptographic protocols, although it is usually not fully explained. This article is an attempt to present the main ingredients that go into this property.

The structure of isogeny graphs has been studied at large by Hecke, Eichler, Pizer, Mestre and Kohel, among others (see e.g. [11, 12, 8, 9]). Here we concentrate on the supersingular case, which in turn requires looking at quaternion algebras and modular forms. The combinatorial properties of Ramanujan graphs are stated more naturally in terms of random walks on Markov chains, so we also use that language.

To illustrate the extent to which the Ramanujan property applies to cryptography, we give the construction of the hash function of Charles, Lauter and Goren [2]. The CLG hash function can be applied to any graph that is a good expander, that is, such that any random walk reaches any vertex with uniform distribution fairly quickly. Ramanujan graphs such as supersingular isogeny graphs are optimal expanders.

The text is organised as follows. We first review the necessary facts about elliptic curves, a complete treatment is found in [13, Chs. II, III and V]. We then define isogeny graphs and their random walks. Afterwards we give background on modular forms and Hecke operators – the reader is invited to consult [3] and [4, Chs. 1 and 5] for further details. We then sketch the proof of the Ramanujan property. The final section is dedicated to the CLG hash function.

2. Elliptic curves

Definition 2.1. Let K be a field. An elliptic curve $E_{/K}$ is a genus one smooth projective curve defined over K together with a K-rational point, denoted by $\infty \in E(K)$.

By the Riemann–Roch theorem [13, Th. II.5.4, Prop. III.3.1], any elliptic curve $E_{/K}$ has an affine Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The corresponding K-rational point appears as the unique point at infinity $\infty = [0 : 1 : 0]$. If $\operatorname{char} K$ is different from 2 and 3, a change of variables puts E in short Weierstrass form,

$$E : y^2 = x^3 + Ax + B$$

with $A, B \in K$. The smoothness condition amounts to the discriminant $\Delta_E = 4A^3 + 27B^2$ being different from zero. Given a field L containing K, one can define an abelian group structure on $E(L)$, given by algebraic morphisms and such that ∞ is the identity. This makes E a one-dimensional instance of an abelian variety.

An important quantity associated to E is its j-invariant,

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Two elliptic curves are isomorphic over $\bar{K}$ (as algebraic varieties and as groups) if and only if their j-invariants are equal. Sometimes special care has to be taken, since the isomorphism could be defined over a (finite) extension of the base field.

Definition 2.2. A non-constant morphism of curves $\phi\colon E_1 \to E_2$ mapping ∞_{E_1} to ∞_{E_2} is called an *isogeny*. The degree of ϕ, $\deg\phi$, is defined to be the degree of the extension of fields $K(E_1)/\phi^*K(E_2)$. The isogeny ϕ is called separable or (purely) inseparable according to the nature of this extension.

The theory of curves implies that any isogeny $\phi\colon E_1 \to E_2$ has to be surjective. Moreover, being a map of abelian varieties, ϕ induces a group homomorphism $E_1(\bar{K}) \to E_2(\bar{K})$. Since the dimensions of E_1 and E_2 are equal, the kernel of ϕ is a finite group. One has

$$\deg\phi = \#\ker\phi$$

if and only if ϕ is a separable isogeny. Conversely, we have the following result.

Theorem 2.3 ([13, Thm. III.4.12])**.** *Let E be an elliptic curve over K, and let G be a finite subgroup of E. Then, there exist an elliptic curve E' and a separable isogeny $\phi\colon E \to E'$, both unique up to isomorphism, such that $\ker\phi = G$. Moreover, ϕ is defined over the smallest extension L of K such that $G^\sigma \subset G$ for every $\sigma \in \mathrm{Gal}(\bar{K}/L)$.*

This theorem is made effective by the formulas of Vélu [14] which compute ϕ in time and space linear in the size of G. A recent development [1] lowers the complexity to $O(\sqrt{\#G})$ operations and yields an actual speedup when $\#G$ is large enough.

When K is a finite field $\mathbb{F}_q$ for some prime power $q = p^r$, the group $E(\bar{\mathbb{F}}_q)$ consists entirely of torsion points. On the other hand, $\mathrm{End}(E)$, the ring of isogenies $\phi\colon E \to E$ with addition and composition, is always a ring of characteristic zero. This is due to the injection $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ given by mapping an integer n to the multiplication-by-n map,

$$\begin{aligned}[n]\colon E &\to E\\ P &\mapsto P + \overset{|n|}{\cdots} + P.\end{aligned}$$

Proposition 2.4 ([13, Cor. 6.4])**.** *Let E be an elliptic curve and let n be a nonzero integer.*

(i) $\deg[n] = n^2$.

(ii) If $\mathrm{char}\,K = 0$ *or* $\mathrm{char}\,K = p > 0$ *with* $p \nmid n$*, then*

$$E[n] := \ker[n] \cong (\mathbb{Z}/n\mathbb{Z})^2.$$

(iii) If $\mathrm{char}\,K = p > 0$*, then either* $E[p^r] = \{0\}$ *or* $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ *for all* $r \geq 1$.

Therefore $[p] \in \mathrm{End}(E_{/\mathbb{F}_p})$ is the first example of an inseparable isogeny, while for $p \nmid n$, $[n]$ is the unique separable isogeny with kernel $E[n]$ given by Theorem 2.3. If $G \subset E$ is a finite cyclic subgroup of order n, and $\phi\colon E \to E' = E/G$ is its quotient isogeny, then the isogeny $\psi\colon E' \to E'/\phi(E[n])$ satisfies that $\psi \circ \phi$ has kernel $E[n]$, so $E'/\phi(E[n]) \cong E$ and $\psi \circ \phi \cong [n]$. This motivates the following definition-result.

Proposition 2.5 ([13, Thm. 6.1])**.** *Let $\phi\colon E_1 \to E_2$ be an isogeny. Then there exists an isogeny $\hat{\phi}\colon E_2 \to E_1$ called the dual isogeny, such that*

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg \phi].$$

Example 2.6. Given a curve $E_{/\mathbb{F}_q} : y^2 = x^3 + Ax + B$, there is a curve $E^{(p)}_{/\mathbb{F}_q} : y^2 = x^3 + A^p x + B^p$. The curve E and its p-power $E^{(p)}$ are related by the Frobenius isogeny $\pi\colon (x, y) \mapsto (x^p, y^p)$. This is a purely inseparable isogeny, so its kernel is trivial. In fact, all inseparable isogenies factor as a power of π composed with a separable isogeny. We have $\deg \pi = p$, so that $\hat{\pi} \circ \pi = [p]$.

It is important to establish the group of automorphisms of E, namely, the group of isogenies of degree 1. This is always a finite group, which we denote by $\mathrm{Aut}(E)$.

Proposition 2.7 ([13, §III.10])**.** *Let E be an elliptic curve defined over K, with either $\mathrm{char}\, K = 0$ or $\mathrm{char}\, K = p \geq 5$.*

(i) If $j(E) = 0$, then $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$.

(ii) If $j(E) = 1728$, then $\mathrm{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$.

(iii) Otherwise, $\mathrm{Aut}(E) = \langle [-1] \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Let B be a finite-dimensional algebra over $\mathbb{Q}$. We say a subring of B is an order if its rank as a $\mathbb{Z}$-module is finite and equal to the dimension of B. In a quadratic field $\mathbb{Q}(\sqrt{D})$ there is a unique maximal order. Meanwhile, in a quaternion algebra

$$B = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}, \quad i^2, j^2 \in \mathbb{Q}^\times, \quad ij = -ji,$$

there are multiple maximal orders. The endomorphism ring of an elliptic curve defined over a finite field can be classified as follows [13, Thm. V.3.1].

Theorem 2.8. *Let $E_{/\mathbb{F}_q}$ be an elliptic curve. The endomorphism ring of E is either*

(i) An order in an imaginary quadratic field, or

(ii) An order in the unique definite quaternion algebra over $\mathbb{Q}$ ramified at p and ∞.

We call (i) the ordinary case, while (ii) is called the supersingular case. The supersingular case can be characterized in several ways [13, Thm. V.3.1].

Theorem 2.9. *Let $E_{/\mathbb{F}_q}$ be an elliptic curve. For each integer $r \geq 1$, let $\pi_r \colon E \to E^{(p^r)}$, $\hat{\pi}_r \colon E^{(p^r)} \to E$ be the p^r-power Frobenius and its dual. The following are equivalent:*

(i) $E[p^r] = 0$ *for one (all)* $r \geq 1$.

(ii) $\hat{\pi}_r$ *is purely inseparable for one (all)* $r \geq 1$.

(iii) The map $[p] \colon E \to E$ *is purely inseparable and* $j(E) \in \mathbb{F}_{p^2}$.

(iv) $\mathrm{End}(E)$ *is an order in a quaternion algebra.*

The third condition implies that there is a finite number of isomorphism classes of supersingular elliptic curves. It is possible to give the actual number of classes [13, §V.5].

Theorem 2.10. *There are* $\left[\frac{p}{12}\right] + \varepsilon_p$ *isomorphism classes of supersingular elliptic curves over* $\bar{\mathbb{F}}_p$*, where* $\varepsilon_p = 0, 1, 1$ *or* 2 *depending on whether* $p \equiv 1, 5, 7$ *or* $11 \bmod 12$.

Lemma 2.11 ([13, Exs. V.4.4, V.4.5])**.**

(i) The curve $E_{/\mathbb{F}_p} : y^2 = x^3 + x$ *(which has* $j(E) = 1728$*) is supersingular if and only if* $p \equiv 3 \bmod 4$.

(ii) The curve $E_{/\mathbb{F}_p} : y^2 = x^3 + 1$ *(which has* $j(E) = 0$*) is supersingular if and only if* $p \equiv 2 \bmod 3$.

2.1 The Deuring correspondence

Let E be a supersingular elliptic curve defined over a finite field $\mathbb{F}_q$. Let $O = \mathrm{End}(E)$ and $B = O \otimes \mathbb{Q} = \mathrm{End}^0(E)$. We fix a "base" curve E_0 with its corresponding endomorphism ring O_0. The Deuring correspondence is the following functorial equivalence:

$$\left\{ \begin{array}{c} \text{Supersingular elliptic curves} \\ \text{over } \mathbb{F}_q \text{ with isogenies} \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} \text{Invertible left } O_0\text{-modules, with} \\ \text{nonzero left } O_0\text{-module homomorphisms} \end{array} \right\}.$$

We follow [15, Ch. 12]. Given a nonzero left ideal $I \subset O$, we want to assign it a curve E_I and an isogeny $\phi_I \colon E \to E_I$. If I contains a separable isogeny $\alpha \colon E \to E$, then we can define $E[I] = \{P \in E \mid P \in \ker \beta \ \forall \beta \in I\}$, and assign the isogeny $\phi_I \colon E \to E_I = E/E[I]$. If all isogenies in I are separable, we can write $I = P^r I'$, where $P = (\pi)$ is the ideal generated by the p-Frobenius, and I' contains a separable isogeny. We then have the isogeny $\phi_I \colon E \to E^{(p^r)} \to E_I$, where $E_I = E^{(p^r)}/E^{(p^r)}[I']$.

The correspondence also works in the opposite way: given an isogeny $\phi \colon E \to E'$, there exists a left ideal I of O and an isomorphism $\rho \colon E_I \to E'$ such that $\phi = \rho\phi_I$.

If we let I be a left ideal for $O_0 = \mathrm{End}(E_0)$, and consider $\mathrm{Hom}(E_I, E_0)$ (which is a left $\mathrm{End}(E_0)$-ideal), then the morphism $\mathrm{Hom}(E_I, E_0) \to I$ given by $\psi \mapsto \psi\phi_I$ is an isomorphism of left O_0-ideals. The full correspondence is summarized by the following result [15, Th. 42.3.2].

Theorem 2.12. *The association* $E \mapsto \mathrm{Hom}(E, E_0)$ *is functorial and defines an equivalence between the category of supersingular elliptic curves over* $\mathbb{F}_q$ *with isogenies, and the category of invertible left* O_0*-modules with left* O_0*-module homomorphisms.*

Further details on quaternion ideals in relation to isogenies can be found in Voight's book and in the articles by Kohel [8, 9].

3. Isogeny graphs

Definition 3.1. Let $p \geq 5$ and ℓ be two different primes. The supersingular ℓ-isogeny graph, denoted $\Gamma(\ell; p)$, is the directed multigraph defined as follows:

- The vertices are isomorphism classes of supersingular elliptic curves defined over $\bar{\mathbb{F}}_p$. If E is such a curve, $[E]$ denotes its corresponding vertex.
- The edges $[E_1] \to [E_2]$ are given by (separable) isogenies $E_1 \to E_2$ of degree ℓ. These are identified in the following way: fixing the curve E_1, two isogenies $\phi\colon E_1 \to E_2$, $\psi\colon E_1 \to E_3$ are equivalent if $\ker\phi = \ker\psi$ (and so $E_2 \cong E_3$).

We consider all our isogenies to be defined over $\bar{\mathbb{F}}_p$. The degree of the vertices of this graph is given by the following fact about finite abelian groups.

Lemma 3.2. *Let ℓ be a prime. The group $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ has $\ell + 1$ cyclic subgroups of order ℓ.* □

The definition says $\Gamma(\ell; p)$ is a directed graph, and by the lemma, it has regular out-degree equal to $\ell+1$. However, Proposition 2.7 and Lemma 2.11 tell us that all vertices in $\Gamma(\ell; p)$ have the same automorphism group whenever $p \equiv 1 \bmod 12$. This is the only phenomenon that can make the graph non-undirected. Indeed, if we take two elliptic curves E_1 and E_2, and we let $w(E_1, E_2)$ and $w(E_2, E_1)$ be the number of ℓ-isogenies from E_1 to E_2 and viceversa, we have

$$\frac{\#\operatorname{Aut}(E_1)}{\#\operatorname{Aut}(E_2)} = \frac{w(E_2, E_1)}{w(E_1, E_2)}. \tag{1}$$

Hence $\Gamma(\ell; p)$ is an $(\ell + 1)$-regular undirected graph if and only if $p \equiv 1 \bmod 12$.

To go deeper into the combinatorial structure of isogeny graphs we need to study random walks. Let $G = (V, E)$ be a directed graph, with a finite set of vertices V and a finite collection of directed edges E. We allow for loops and multiple edges, that is, given two (possibly equal) vertices u and v, there can be two different edges $e_1, e_2 \in E$ from u to v. We assume that for each edge $u \to v$ there is at least one edge $v \to u$, and such that we can reach the whole graph from any single vertex (in particular, G is strongly connected). Given a vertex $u \in V$, we define $\deg u$ to be the number of edges coming out of u. If v is another vertex, we let $w(u, v)$ be the number of edges from u to v.

Definition 3.3. Given any $u_0 \in V$, a random walk on G is a sequence of vertices $u_0, u_1, \ldots, u_n, \ldots$, such that

$$P(u_{i+1} = v \mid u_i = u) = \frac{w(u, v)}{\deg u}.$$

This means that, at each step in the walk, we choose our next step to be a vertex neighboring our current position in the graph. Since the state at any given time determines the probabilities for the next state, this is an example of a discrete-time Markov chain.

We want to give a probability distribution ϕ on V that is "stationary" with respect to the random walk. This will mean that, if we sample a vertex u_0 according to ϕ and we take a random walk starting at u_0, we will obtain at each step a vertex that will also be sampled according to ϕ. Moreover, we will have convergence to ϕ independently of our starting distribution. We first need an additional hypothesis on G.

Definition 3.4. Let $u \in V$ be any vertex. The period of u is the greatest common divisor of the lengths of all paths on G starting and ending at u. The period of G is the greatest common divisor of the periods of all vertices. We say G is aperiodic if its period is equal to 1.

Let us assume that G is aperiodic, undirected, and regular of degree d. If we let M be the adjacency matrix of M, then each column of M sums to d. More importantly, if we let $W = \frac{1}{d}M$, and we let $\psi \in \mathbb{R}^{|V|}$ be a vector with positive entries adding to 1, then the multiplication $W\psi$ yields another vector with positive entries adding to 1. The matrix W representing the random walk is called a stochastic matrix. This procedure is equivalent to performing a step in the random walk of G after sampling a vertex according with the distribution on V given by ψ.

This motivates the result that follows, whose proof is found in [7, Sec. 3]. The matrix W is symmetric, so its eigenvalues are real and can be ordered as

$$1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_n > -1.$$

We let $\lambda_\star = \max\{|\lambda_2|, |\lambda_n|\}$.

Proposition 3.5. *Let $G = (V, E)$ be a connected, aperiodic undirected graph (possibly with loops and multiple edges). Let $u_0 \in V$, and let $u_0, u_1, \ldots, u_n, \ldots$ be a random walk as defined above. Then, for all positive integers n and all vertices $v \in V$ we have*

$$\left| P(u_n = v) - \frac{1}{|V|} \right| \leq \lambda_\star^n.$$

In particular, $\phi(u) = 1/|V|$ is the stationary distribution of the random walk on G.

We now consider a family $\{G_n\}_n$ of d-regular graphs with growing number of vertices. A theorem of Alon and Boppana ([7, Th. 2.7]) says that

$$\liminf_n \lambda_\star(G_n) \geq \frac{2\sqrt{d-1}}{d}.$$

Definition 3.6. A graph G is said to be Ramanujan if $\lambda_\star(G) \leq 2\sqrt{d-1}/d$.

When G is not a regular graph, a similar result can be proven, with stationary distribution given by $\phi(u) = \deg u/(2|V|)$. Directed graphs require a more careful treatment (even with our strong connectivity hypothesis), as they are very close to general Markov chains. Luckily, the isogeny graphs $\Gamma(\ell; p)$ satisfy the nice symmetry property of equation (1). This allows us to give the next result, which generalizes well to abelian varieties (see [5] for further details).

Theorem 3.7. *Consider the graph $\Gamma(\ell; p)$, a starting elliptic curve E_0, and a random walk $E_0, E_1, \ldots, E_n, \ldots$ The stationary distribution is given by $\phi = \tilde{\phi}/\left(\sum_E \tilde{\phi}(E)\right)$, where $\tilde{\phi}(E) = 1/\#\operatorname{Aut}(E)$. Given a positive integer n and any supersingular elliptic curve E,*

$$|P(E_n \cong E) - \phi(E)| \leq \lambda_\star^n \sqrt{\frac{\#\operatorname{Aut}(E)}{\#\operatorname{Aut}(E_0)}}.$$

In the particular case that $p \equiv 1 \bmod 12$ we recover Proposition 3.5.

Proof. The stationary distribution equals ϕ because of the equation (1). For the convergence statement, see [10, Th. 12.3] or [5, Th. 1]. □

An interesting related result is [6, Th. 1], which states the convergence to the same distribution for the graph $\Gamma(\{\ell_1, \dots, \ell_r\}; p)$ of isogenies of several degrees.

We remark that we still have not shown that $\Gamma(\ell; p)$ is a connected graph. The theory of random walks still works, which is why we have omitted this consideration: one can simply apply the results to each connected component of the graph. However, one can indeed show that $\Gamma(\ell; p)$ *is* connected. This will be an immediate consequence of the Ramanujan property: if $\lambda_\star(\Gamma(\ell; p))$ is bounded by $2\sqrt{\ell}/(\ell+1)$, then the random walk matrix has a unique eigenvalue equal to 1. A standard fact in algebraic graph theory then says that $\Gamma(\ell; p)$ has to be connected. Likewise, the aperiodic property of the graphs also follows from the Ramanujan property: another bit of algebraic graph theory says that a graph is non-bipartite if and only if $\lambda_\star(\Gamma(\ell; p)) < 1$. For a strongly connected graph, being aperiodic is equivalent to being non-bipartite.

4. Modular forms and the Ramanujan–Petersson conjecture

Let N be a positive integer. We consider the group of integer matrices

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ N \mid c,\ ad - bc = 1 \right\}.$$

In words, $\Gamma_0(N)$ consists of integer matrices with determinant 1 whose reduction modulo N is upper triangular. It is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, the group of 2-by-2 integer matrices with determinant 1. These matrices act on the complex upper-half plane $\mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ by means of the Möbius transformation,

$$\tau \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Definition 4.1. Let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function, and let N and k be positive integers. We say f is a modular form of weight k and level N if

(i) For all matrices $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, $f(\gamma\tau) = (c\tau + d)^k f(\tau)$, and

(ii) For all matrices $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the transformed function $f(\gamma\tau)(c\tau+d)^{-k}$ is bounded when $\mathrm{Im}(\tau) \to \infty$.

We denote by $M_k(\Gamma_0(N))$ the $\mathbb{C}$-vector space of modular forms of weight k with respect to $\Gamma_0(N)$.

Modular forms can seem somewhat complicated after giving this definition. However, a prominent feature of the theory is that we can work with them using Fourier expansions. For all levels $N \geq 1$, the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is in $\Gamma_0(N)$, the symmetry of $f \in M_k(\Gamma_0(N))$ implies $f(\tau + 1) = f(\tau)$ for all $z \in \mathcal{H}$. From the fact that f is holomorphic and bounded at infinity, we have a Fourier expansion of the form

$$f(\tau) = \sum_{n \geq 0} a_n(f) e^{2\pi i n \tau}.$$

By letting $q = e^{2\pi i\tau}$, we can rewrite this as the *q-expansion* $f(q) = \sum_{n\geq 0} a_n(f)q^n$. If the Fourier expansion of $f(\gamma\tau)(c\tau + d)^{-k}$ starts with $a_0 = 0$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we say f is a cusp form. The subspace of cusp forms is denoted by $S_k(\Gamma_0(N))$. Both $M_k(\Gamma_0(N))$ and $S_k(\Gamma_0(N))$ have finite dimension; see [4, Thms. 3.5.1 and 3.6.1].

We need a few facts about the case of level 1. When the weight k is odd, since the matrix $-\mathrm{Id}_2$ is in $\mathrm{SL}_2(\mathbb{Z})$ we have $f(\tau) = (-1)^k f(\tau)$ for all $\tau \in \mathcal{H}$, so there are no nonzero modular forms of odd weight. When $k \geq 4$ is even, an example of level 1 form is given by the Eisenstein series

$$G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m\tau + n)^k}$$

which is seen to converge uniformly on compact sets. Showing the invariance under $\mathrm{SL}_2(\mathbb{Z})$ is then a simple exercise, done by reordering of the series. This can however not be done in weight 2. In fact, we have $M_2(\Gamma_0(1)) = \{0\}$. A proof can be found in [3, Thm. 5.3].

From now on we restrict to the case of weight $k = 2$. To help study the structure of the spaces $M_2(\Gamma_0(N))$, one defines a series of linear operators $T_\ell \colon M_2(\Gamma_0(N)) \to M_2(\Gamma_0(N))$ for each prime ℓ, called the Hecke operators. These operators preserve the subspace of cusp forms. They commute pairwise, and for all $\ell \nmid N$, they are self-adjoint with respect to a certain inner product – called the Petersson scalar product – which is defined as follows: given two cusp forms f and g of level 2,

$$\langle f, g\rangle = \int_{\mathcal{H}/\Gamma_0(N)} f(\tau)\overline{g(\tau)}\, dx\, dy.$$

By the spectral theorem, the space $S_2(\Gamma_0(N))$ has a basis of simultaneous eigenvectors (called eigenforms) for all Hecke operators T_ℓ with $\ell \nmid N$. The effect of each T_ℓ on the q-expansion of $f(q) = \sum_n a_n q^n$ is given by the formulas

$$T_\ell(f) = \begin{cases} \sum_{\ell|n} a_n q^{n/\ell} + \ell \sum a_n q^{\ell n}, & \text{if } \ell \nmid N, \\ \sum_{\ell|n} a_n q^{n/\ell}, & \text{if } \ell \mid N. \end{cases} \tag{2}$$

From equation (2), if $f(q) = \sum_{n\geq 1} a_n(f)q^n$ is a simultaneous Hecke eigenform such that $a_1(f) = 1$ (this is called a normalized eigenform), then we have $T_\ell(f) = a_\ell(f)f$, so that the Fourier coefficient $a_\ell(f)$ is the eigenvalue of f at ℓ.

At this point, one usually defines a subspace of $S_2(\Gamma_0(N))$ consisting of all forms coming from levels M dividing N: the space of old forms $S_2^{\mathrm{old}}(\Gamma_0(N))$. The space of new forms S_2^{new} is then defined as the orthogonal of S_2^{old} with respect to $\langle\cdot,\cdot\rangle$. Since we are only interested in weight 2 and prime level p, and there are no forms of weight 2 and level 1, we have $S_2(\Gamma_0(p)) = S_2^{\mathrm{new}}(\Gamma_0(p))$. It can be seen that this space has a basis of simultaneous eigenforms for *all* Hecke operators.

What we shall do below is to relate the space of cusp forms of level p, together with its structure as a *Hecke module*, with the adjacency matrices of the graphs $\{\Gamma(\ell; p)\}_\ell$. To that effect, we need the following bound on the Hecke eigenvalues.

Theorem 4.2 (Ramanujan–Petersson conjecture, proven by Deligne)**.** *Let $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ be a normalized Hecke eigenform with Fourier expansion*

$$f(q) = \sum_{n>0} a_n(f)q^n.$$

Then for any prime ℓ we have the inequality $|a_\ell(f)| \leq 2\sqrt{\ell}$.

5. Isogeny graphs are Ramanujan

Let p be a prime. We define a formal group $M_p = \bigoplus_E \mathbb{Z}[E]$, where E ranges over the set of isomorphism classes of supersingular elliptic curves over $\bar{\mathbb{F}}_p$. We let $\alpha_E = \#\operatorname{Aut}(E)/2$. The space M_p has a scalar product defined by $\langle E, E\rangle = \alpha_E$, $\langle E, E'\rangle = 0$ for $E \ncong E'$, and extended linearly.

We give M_p a structure of Hecke module as follows. For each prime $\ell \neq p$, we define the ℓth Hecke operator by

$$T_\ell[E] = \sum_{C_\ell} [E/C_\ell],$$

where C_ℓ runs over all order-ℓ cyclic subgroups of E, and E/C_ℓ is the image of the unique separable isogeny with kernel C_ℓ. These operators commute for $\ell_1, \ell_2 \neq p$. Other operators which we do not need can be defined [11]. The connection of M_p with our isogeny graphs is clear: the adjacency matrix of $\Gamma(\ell; p)$ is the matrix of the operator T_ℓ in the basis $\{[E]\}_E$ of M_p.

We let $\mathrm{Eis} = \sum \frac{1}{\alpha_E}[E] \in M_p \otimes \mathbb{Q}$ and let

$$M_p^0 = \left\{ \sum x_E[E] \;\middle|\; \sum x_E = 0 \right\}$$

be the subspace orthogonal to Eis. We have $T_\ell \,\mathrm{Eis} = (\ell+1)\,\mathrm{Eis}$ for all primes ℓ.

Theorem 5.1. *There is an isomorphism of Hecke modules*

$$M_p^0 \otimes \mathbb{C} \cong S_2(\Gamma_0(p)).$$

Sketch of proof. The isomorphism is constructed in two steps. The first one involves the Deuring correspondence. After fixing a base curve E_0, the functor $E \mapsto \operatorname{Hom}(E, E_0)$ takes a supersingular elliptic curve over $\bar{\mathbb{F}}_p$ to a left $\operatorname{End}(E_0)$-ideal. One then builds an analog module of left ideals for the order $\operatorname{End}(E_0)$, $N = \bigoplus_I \mathbb{Z} \cdot [I]$. This module has an inner product $\langle \cdot, \cdot \rangle$ and an action of Hecke operators

$$T_\ell([I]) = \sum_{\substack{\phi\colon I \to J \\ J/\phi(I) \cong (\mathbb{Z}/\ell\mathbb{Z})^2}} [J].$$

Now there is a Hecke-bilinear pairing $\Theta\colon N \times N \to M_2(\Gamma_0(N))$. To define it, we first define a collection of operators A_n on M_p in terms of the operators T_ℓ, and such that $A_\ell = T_\ell$ for all primes ℓ. Then Θ is defined by

$$\Theta([I],[J]) = 1 + 2\sum_{n=1}^{\infty} \langle A_n([I]), [J]\rangle q^n$$

and extended bilinearly to $N \times N$. This pairing takes $N \times N^0$ and $N^0 \times N$ to the space of cusp forms. For all $\ell \neq p$ one has

$$T_\ell(\Theta([I],[J])) = \Theta(T_\ell([I]),[J]) = \Theta([I], T_\ell([J]))$$

and then the proof is concluded by showing that $\Theta(-, v)\colon N \to M_2(\Gamma_0(p))$ is an isomorphism of Hecke modules for an appropriate $v \in N$ (see [8, Cor. 4]). □

Corollary 5.2. *The second largest eigenvalue of the graph $\Gamma(\ell; p)$ is bounded by $2\sqrt{\ell}$. In particular, for $p \equiv 1 \bmod 12$ the supersingular isogeny graph $\Gamma(\ell; p)$ is an $(\ell+1)$-regular Ramanujan graph.*

Proof. The matrix of the Hecke operator T_ℓ on M_p is the adjacency matrix of $\Gamma(\ell; p)$. It has largest eigenvalue $\lambda_1 = \ell + 1$ corresponding to the constant vector $\mathbf{1}$. The remaining eigenvalues satisfy the Ramanujan–Petersson bound for normalized eigenforms in $S_2(\Gamma_0(N))$, so that the second largest eigenvalue of the random walk matrix satisfies $\lambda_\star \leq 2\sqrt{\ell}/(\ell+1)$. This is the definition of Ramanujan graph whenever the graph is regular and undirected, which is the case whenever $p \equiv 1 \bmod 12$. □

Together with Theorem 3.7, this gives a bound on the diameter of $\Gamma(\ell; p)$ which is logarithmic in p. This has the following arithmetic formulation.

Theorem 5.3. *Let E_1 and E_2 be two supersingular elliptic curves over $\bar{\mathbb{F}}_p$. For any prime $\ell \neq p$, there exists a separable isogeny $\phi\colon E_1 \to E_2$ of degree $\ell^{O(\log p)}$.* □

6. Hash functions from isogeny graphs

We fix a prime number ℓ. Consider the set $\{0, 1, \dots, \ell-1\}^* = \bigsqcup_{n\geq 1}\{0, 1, \dots, \ell-1\}^n$ of strings of arbitrary length, representing information codified in base ℓ. For example, the case $\ell = 2$ corresponds to arbitrary-length binary strings. Given a finite set S, a hash function consists of a map $h : \{0, \dots, \ell-1\}^* \to S$.

A cryptographic hash function usually requires additional properties, for instance, it asks that the image of h is "uniformly distributed" in some sense. Using Theorem 3.7 and the fact that $\Gamma(\ell; p)$ is a Ramanujan graph, we shall build a hash function with the property that for a fixed m large enough, the image of $h\colon \{0, 1, \dots, \ell-1\}^m \to S$ is uniformly distributed.

We follow the construction of Charles, Lauter and Goren [2]. The set S shall consist of the isomorphism classes of supersingular elliptic curves. For the setup, we pick two such elliptic curves E_{-1}, E_0 which are connected by an isogeny of degree ℓ, $\phi_{-1}\colon E_{-1} \to E_0$. Then there are ℓ isogenies of degree ℓ from E_0 which are different from the dual $\hat{\phi}_{-1}$. We label them $\phi_0^{(0)}, \dots, \phi_0^{(\ell-1)}$. Given a string

$$b = b_0 \cdots b_{m-1} \in \{0, 1, \dots, \ell-1\}^m,$$

we define recursively a path in $\Gamma(\ell; p)$ by taking a step in the graph according to b_i. The path starts by $\phi_0^{(b_0)} : E_0 \to E_1$. Recursively, after taking an isogeny $E_{i-1} \to E_i$ we label the ℓ isogenies from E_i different from $\hat{\phi}_{i-1}$ as $\phi_i^{(0)}, \dots, \phi_i^{(\ell-1)}$, and take a further step by using $\phi_i^{(b_i)}$.

After m steps, we will arrive at a supersingular elliptic curve E_m. The hash of b can then be defined to be this curve (in the set of supersingular elliptic curves, which achieves a uniform distribution after sufficiently many steps). Usually, one takes the j-invariant of the curve, as it depends only on its isomorphism class.

The CLG hash function has two additional properties: collision resistance and preimage resistance. These are due to the lack of short loops in $\Gamma(\ell; p)$ for suitable p. Additional details can be found in [2].

References

[1] D.J. Bernstein, L. De Feo, A. Leroux, B. Smith, Faster computation of isogenies of large prime degree, in: *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, The Open

Book Series **4**, Mathematical Science Publishers, Berkeley, CA, 2020, 39–55.

[2] D.X. Charles, K.E. Lauter, E.Z. Goren, "Cryptographic hash functions from expander graphs", *J. Cryptology* **22**(1) (2009), 93–113.

[3] K. Conrad, "Modular forms (draft, CTNT 2016)", `https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/CTNTmodularforms.pdf`.

[4] F. Diamond, J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics **228**, Springer-Verlag, New York, 2005.

[5] E. Florit, B. Smith, "Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph", Preprint (2021), `https://arxiv.org/abs/2101.00919`.

[6] S.D. Galbraith, C. Petit, J. Silva, "Identification protocols and signature schemes based on supersingular isogeny problems", *J. Cryptology* **33**(1) (2020), 130–175.

[7] S. Hoory, N. Linial, A. Wigderson, "Expander graphs and their applications", *Bull. Amer. Math. Soc. (N.S.)* **43**(4) (2006), 439–561.

[8] D.R. Kohel, Computing modular curves via quaternions, in: *Fourth CANT Conference: Number Theory and Cryptography*, University of Sydney, Dec. 3, 1997.

[9] D. R. Kohel, Hecke module structure of quaternions, in: *Class field theory—its centenary and prospect* (Tokyo, 1998), Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001, 177–195.

[10] D.A. Levin, Y. Peres, E.L. Wilmer, *Markov chains and mixing times*, With a chapter by James G. Propp and David B. Wilson, American Mathematical Society, Providence, RI, 2009.

[11] J.-F. Mestre, La méthode des graphes. Exemples et applications, in: *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields* (Katata, 1986), Nagoya Univ., Nagoya, 1986, 217–242.

[12] A.K. Pizer, "Ramanujan graphs and Hecke operators", *Bull. Amer. Math. Soc. (N.S.)* **23**(1) (1990), 127–137.

[13] J.H. Silverman, *The arithmetic of elliptic curves*, Second edition, Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009.

[14] J. Vélu, "Isogénies entre courbes elliptiques", *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241.

[15] J. Voight, *Quaternion algebras*, Graduate Texts in Mathematics **288**, Springer, Cham, 2021.