ELLIPTIC CURVES OVER FINITE FIELDS AND RAMANUJAN GRAPHS ON TWO VERTICES

Daniel Vallières
Department of Mathematics and Statistics, California State University Chico, Chico, California
dvallieres@csuchico.edu

Received: 7/17/23, Accepted: 12/21/23, Published: 1/2/24

Abstract

Let p be an odd prime and let $q = p^a$, where $a = 1$ or $a = 2$. We show that there is a one-to-one correspondence between $\mathbb{F}_q$-isogeny classes of elliptic curves C over $\mathbb{F}_q$ satisfying $|C(\mathbb{F}_q)| \in 4\mathbb{Z}$ and $(q+1)$-regular Ramanujan graphs on two vertices. The correspondence is obtained by matching the Hasse-Weil zeta function of the elliptic curves with the Ihara zeta function of the Ramanujan graphs using the Honda-Tate theorem.

1. Introduction

Let q be a positive integer and let X be a finite connected $(q+1)$-regular graph. The adjacency matrix A of X is symmetric and hence diagonalizable with real eigenvalues. It is known (see [14, Proposition 7.2]) that the eigenvalues λ of A satisfy $|\lambda| \leq q+1$ and that $q+1$ is an eigenvalue with multiplicity one. Letting

$$\lambda(X) = \max\{|\lambda| \, : \, \lambda \neq q+1\},$$

recall that the graph X is called a *Ramanujan graph* if $\lambda(X) \leq 2\sqrt{q}$ (see for instance [5, Definition 1.1]).

In [3], Ihara introduced what is now known as the *Ihara zeta function* of a graph and showed that they are rational functions. He pointed out that these zeta functions may or may not satisfy an analogue of the Riemann hypothesis and he gave examples in [2]. For connections with modular curves, see for instance [11]. The original situation considered by Ihara was in the context of a cocompact discrete torsion-free subgroup Γ of $\mathrm{PGL}(2, \mathbb{Q}_p)$ acting on a certain tree Y associated to $\mathrm{PGL}(2, \mathbb{Q}_p)/\mathrm{PGL}(2, \mathbb{Z}_p)$ and generalizations thereof. The quotient $X = \Gamma \backslash Y$ is a finite graph, and Serre suggested in [9] that the Ihara zeta function could be interpreted in terms of X only. This was explicitly done by Sunada in [12].

DOI: 10.5281/zenodo.10450973

It turns out that a finite connected $(q+1)$-regular graph X is a Ramanujan graph if and only if the Ihara zeta function associated to X satisfies an analogue of the Riemann hypothesis (see [14, Theorem 7.4]). It follows that in the situation where q is a power of a rational prime, one can associate a collection of Weil q-numbers to Ramanujan graphs, where we recall that a *Weil q-number* is an algebraic integer α satisfying

$$|\psi(\alpha)| = q^{1/2},$$

for all embeddings $\psi : \mathbb{Q}(\alpha) \to \mathbb{C}$.

Now, the Honda-Tate theorem (see [8] for instance) gives a classification of isogeny classes of abelian varieties over finite fields precisely in terms of conjugacy classes of Weil q-numbers. So one may expect a connection between (some) abelian varieties over finite fields and (some) $(q+1)$-regular Ramanujan graphs in the situation where q is a power of a rational prime.

Our goal here is to explore this connection in the simplest possible situation. Since the adjacency matrix of a connected $(q+1)$-regular graph with one vertex has a single eigenvalue, namely $q+1$, the first interesting case to look at is the case of connected $(q+1)$-regular graphs on two vertices. Given two nonnegative integers l and m satisfying $2l + m = q + 1$, we let $X(l, m)$ be the $(q+1)$-regular graph that consists of two vertices joined by m undirected edges and with l undirected loops at each of the vertices. The purpose of this note is to show the following theorem.

Theorem A (Theorem 8)**.** *Let $q = p^a$, where p is an odd prime number and a is an integer satisfying $a = 1$ or $a = 2$. Let Ω be the set of $\mathbb{F}_q$-isogeny classes of elliptic curves C over $\mathbb{F}_q$ for which $|C(\mathbb{F}_q)| \in 4\mathbb{Z}$, and let $\mathcal{R}$ be the set of connected $(q+1)$-regular Ramanujan graphs on two vertices. The map $\Omega \to \mathcal{R}$ defined via $[C] \mapsto X(l, m)$, where*

$$l = \frac{q+1}{2} - \frac{|C(\mathbb{F}_q)|}{4} \text{ and } m = \frac{|C(\mathbb{F}_q)|}{2},$$

is a one-to-one correspondence between Ω and $\mathcal{R}$.

Note that by the Hasse bound, l is a positive integer. The integer m is also a positive integer, since $C(\mathbb{F}_q) \neq \varnothing$ and is necessarily even because we are assuming that $|C(\mathbb{F}_q)| \in 4\mathbb{Z}$. Our approach to proving this theorem is to establish a correspondence between the Hasse-Weil zeta functions of elliptic curves whose isogeny classes are in Ω and the Ihara zeta functions of the graphs in $\mathcal{R}$ suitably modified to take into account some discrepancy factors. The correspondence then simply follows from the Honda-Tate theorem which gives in particular a classification of $\mathbb{F}_q$-isogeny classes of elliptic curves defined over $\mathbb{F}_q$. In the situation where $q = p^a$ for some odd prime p and an arbitrary positive integer a, one can obtain a similar correspondence if one restricts to ordinary elliptic curves and exclude a few graphs from $\mathcal{R}$. See Theorem 9 for the precise statement. The case where $p = 2$ is formulated in Theorem 10.

The paper is organized as follows. We gather several known results in Section 2. We collect what we need from graph theory in Section 2.1 and what we need from the theory of abelian varieties over finite fields in Section 2.2. We remind the reader about basic graph terminology in Section 2.1.1, about the Ihara zeta function of a graph in Section 2.1.2, about regular Ramanujan graphs in Section 2.1.3, and we specialize everything to the simple situation of graphs with only two vertices in Section 2.1.4. In Section 2.2.1, we gather together the results we need from the theory of abelian varieties over finite fields, we remind the reader about the Honda-Tate theory in Section 2.2.2, and also about the Hasse-Weil zeta function of curves over finite fields in Section 2.2.3. Then, we formulate and prove our main result in Section 3.

2. Preliminaries

2.1. Graphs

2.1.1. Basic Notation and Terminology

Recall that a *graph* X in the sense of [9] (see also [13]) consists of a collection of *vertices* V_X, a collection of *directed edges* $\mathbf{E}_X$, an *inversion map* $\mathbf{E}_X \to \mathbf{E}_X$ denoted by $e \mapsto \bar{e}$ and an *incidence map* $\mathrm{inc} : \mathbf{E}_X \to V_X \times V_X$ denoted by $e \mapsto \mathrm{inc}(e) = (o(e), t(e))$ satisfying $\bar{e} \neq e$, $\bar{\bar{e}} = e$ and $o(\bar{e}) = t(e)$ for all $e \in \mathbf{E}_X$. Identifying e with $\bar{e}$ gives the set of *undirected edges* which will be denoted by E_X. Note that loops and multiple edges are allowed. Throughout this paper, by a graph we will always mean a finite graph. In other words, we always assume that both V_X and $\mathbf{E}_X$ are finite sets. Given $v \in V_X$, one defines

$$\mathbf{E}_{X,v} = \{e \in \mathbf{E}_X \mid o(e) = v\},$$

and the *valency* (also known as the index, the degree, etc) of v is defined to be $\mathrm{val}(v) = |\mathbf{E}_{X,v}|$. A graph X is called *k-regular* for some positive integer k if $\mathrm{val}(v) = k$ for all $v \in V_X$.

Let us introduce a labeling of the vertices of X, say $V_X = \{v_1, \ldots, v_r\}$. The *adjacency matrix* of X is the $r \times r$ matrix $A = (a_{ij})$, where a_{ij} is the number of directed edges between v_i and v_j for $i = 1, \ldots, r$. The *valence (or degree) matrix* of X is the diagonal $r \times r$ matrix $D = (d_{ij})$, where $d_{ii} = \mathrm{val}(v_i)$ for $i = 1, \ldots, r$.

A *path* c in a graph X consists of a sequence of directed edges $c = e_1 \cdot \ldots \cdot e_n$ satisfying $t(e_i) = o(e_{i+1})$ for $i = 1, \ldots, n-1$. We let $o(c) = o(e_1)$ and $t(c) = t(e_n)$. A graph X is called *connected* if for every two distinct vertices $v_1, v_2 \in V_X$, there exists a path c satisfying $o(c) = v_1$ and $t(c) = v_2$.

A path c is called *closed* if $o(c) = t(c)$. The concatenation of two paths c_1 and c_2 satisfying $t(c_1) = o(c_2)$ will be denoted by $c_1 \cdot c_2$. Using concatenation, closed

paths can be raised to positive integers. In other words, if c is a closed path and m is a positive integer, then c^m will mean c concatenated with itself m times.

The *length* of a path $c = e_1 \cdot \ldots \cdot e_n$ is defined to be n and is denoted by $\text{len}(c)$. The path c is called a *geodesic* if $e_i \neq \bar{e}_{i+1}$ for all $i = 1, \ldots, n-1$. In other words, a geodesic is a path that has no backtracks. If c is a closed geodesic for which $e_1 \neq \bar{e}_n$, then c will be called a *reduced* closed path. Reduced closed paths are precisely the closed paths with neither backtracks nor tails. If $c = e_1 \cdot \ldots \cdot e_n$ is a reduced closed path and k is an integer satisfying $0 \leq k \leq n-1$, then the k-shift of c is the reduced closed path

$$c^{(k)} = e_{k+1} \cdot \ldots e_n \cdot e_1 \cdot \ldots \cdot e_k.$$

If c_1 and c_2 are two reduced closed paths of the same length n, then the relation $c_1 \sim c_2$ if $c_1^{(k)} = c_2$ for some k satisfying $0 \leq k \leq n-1$ is an equivalence relation. An equivalence class $[c]$ is called a *cycle* and the cycle is called *primitive* or *prime* if c is not of the form c_0^m for some reduced closed path c_0 and some integer $m > 1$. Prime cycles will typically be denoted by a symbol such as $\mathfrak{c}$. Note that if $\mathfrak{c} = [c]$ is a prime cycle, then its length $\text{len}(\mathfrak{c}) := \text{len}(c)$ is well-defined and does not depend on the choice of a representative c.

One can associate two homology groups $H_0(X, \mathbb{Z})$ and $H_1(X, \mathbb{Z})$ to any graph. See [13, Section 4]. The *Euler characteristic* of a graph X is defined to be

$$\chi(X) = \text{rank}_{\mathbb{Z}} H_0(X, \mathbb{Z}) - \text{rank}_{\mathbb{Z}} H_1(X, \mathbb{Z}).$$

If X is connected, then [13, Section 4.4] shows that

$$\chi(X) = |V_X| - |E_X|.$$

2.1.2. Ihara Zeta Function

Our main references for this subsection are [14] and [4]. Let X be a connected graph satisfying $\text{val}(v) \geq 2$ for all $v \in V_X$. Its *Ihara zeta function* is defined to be

$$\zeta_X(u) = \prod_{\mathfrak{c}} (1 - u^{\text{len}(\mathfrak{c})})^{-1},$$

where the product is taken over all prime cycles in the graph X. This product can be shown to converge when u is small enough (see [4] and [14, Theorem 8.1]). From now on, given a positive integer k, let $N_k(X)$ be the number of reduced closed paths of length k in X. Then, [14, page 29] shows that

$$\zeta_X(u) = \exp\left(\sum_{k=1}^{\infty} N_k(X) \frac{u^k}{k} \right). \tag{1}$$

Furthermore, there is another useful expression for the Ihara zeta function which we record in the following theorem (see [4]).

Theorem 1 (Ihara determinant formula)**.** *With the notation as above, one has*

$$\zeta_X(u)^{-1} = (1-u^2)^{-\chi(X)}\det(I - Au + (D-I)u^2) \in \mathbb{Z}[u],$$

where I is the identity matrix, A the adjacency matrix of X, and D the valency matrix of X.

From now on, we let

$$h_X(u) = \det(I - Au + (D-I)u^2) \in \mathbb{Z}[u].$$

2.1.3. Regular Ramanujan Graphs

Let q be an integer satisfying $q \geq 2$ and let X be a connected $(q+1)$-regular graph. Let $\mathrm{Spec}(X)$ be the collection of the eigenvalues of the adjacency matrix A of X. It is known that $\mathrm{Spec}(X) \subseteq [-(q+1), q+1]$ and that $q+1$ is an eigenvalue with multiplicity 1 (see for instance [14, Proposition 7.2]). Let

$$\lambda(X) = \max\{|\lambda| \,:\, \lambda \neq q+1\}.$$

Recall that a connected $(q+1)$-regular graph is called a *Ramanujan graph* if $\lambda(X) \leq 2\sqrt{q}$. (We remark that some authors relax this definition to include bipartite graphs that is graphs for which $-(q+1)$ is an eigenvalue.)

Note that from Theorem 1, one has

$$\zeta_X(u)^{-1} = (1-u^2)^{-\chi(X)}(1-(q+1)u+qu^2)\cdot P_X(u),$$

where

$$P_X(u) = \frac{h_X(u)}{(1-u)(1-qu)} = 1 + a_1u + \ldots + q^{r-1}u^{2r-2} \in \mathbb{Z}[u], \tag{2}$$

so that in particular, $P_X(u)$ has constant coefficient 1, leading coefficient q^{r-1} and degree $2r-2$. Furthermore,

$$P_X(u) = \prod_{\lambda \neq q+1} (1 - \lambda u + qu^2),$$

where the product is over all eigenvalues in $\mathrm{Spec}(X)$ different than $q+1$. Consider the function

$$Q_X(s) = \zeta_X(q^{-s})^{-1}$$

of a complex variable s. The zeros of

$$(1-q^{-2s})^{-\chi(X)}(1-(q+1)q^{-s}+q^{1-2s})$$

are all on either the line $\mathrm{Re}(s) = 0$ or the line $\mathrm{Re}(s) = 1$. We will refer to those zeros as the *trivial* zeros of $Q_X(s)$. The other zeros, namely the zeros of

$$P_X(q^{-s}) = \prod_{\lambda \neq q+1} (1 - \lambda q^{-s} + q^{1-2s}),$$

will be referred to as the *non-trivial* zeros of $Q_X(s)$. The proof of the following theorem can be found in [14, Theorem 7.4].

Theorem 2. *Assume that $q \geq 2$ and let X be a connected $(q+1)$-regular graph for which $|V_X| \geq 2$. The graph X is a Ramanujan graph if and only if all the non-trivial zeros of $Q_X(s)$ are on the line $\mathrm{Re}(s) = 1/2$.*

Assume now that q is a power of a rational prime p, say $q = p^a$ for some positive integer a. Recall that an algebraic integer α is called a *Weil q-number* if

$$|\psi(\alpha)| = q^{1/2},$$

for all embeddings $\psi : \mathbb{Q}(\alpha) \to \mathbb{C}$ (see for instance [8, Definition 1.1]). It is known that if α is a Weil q-number, then the number field $\mathbb{Q}(\alpha)$ is either totally real or a CM-field (see [8, Proposition 2.2]).

Proposition 1. *Assume as above that $q = p^a$ for some rational prime p and some positive integer a. If X is a connected $(q+1)$-regular Ramanujan graph, write*

$$P_X(u) = \prod_{i=1}^{2r-2} (1 - \alpha_i u),$$

for some $\alpha_i \in \mathbb{C}$. Then, α_i is a Weil q-number for all $i = 1, \ldots, 2r-2$.

Proof. Consider the reciprocal polynomial $P_X^*(u) = u^{2r-2} P_X(1/u)$. By Equation (2), we have that

$$P_X^*(u) = \prod_{i=1}^{2r-2} (u - \alpha_i)$$

is a monic polynomial with integer coefficients. It follows that the α_i are algebraic integers. If $\psi : \mathbb{Q}(\alpha_i) \to \mathbb{C}$ is any embedding, then $P_X^*(\psi(\alpha_i)) = 0$ and thus $\psi(\alpha_i) = \alpha_j$ for some $j = 1, \ldots, 2r-2$. But Theorem 2 implies that $|\alpha_k| = \sqrt{q}$ for all $k = 1, \ldots, 2r-2$ and the result follows. □

2.1.4. Graphs on Two Vertices

We shall denote by $X(l_1, m, l_2)$ the graph on two vertices v_1, v_2 for which there are l_i undirected loops at v_i for $i = 1, 2$ and m undirected edges between v_1 and v_2. One has

$$\mathrm{val}(v_i) = 2l_i + m,$$

for $i = 1, 2$. A graph $X(l_1, m, l_2)$ is regular if and only if $l_1 = l_2$ in which case it will be denoted simply by $X(l, m)$. The graph $X(l, m)$ is $(2l + m)$-regular. The graph $X(l, m)$ is disconnected if and only if $m = 0$ and bipartite if and only if $l = 0$.

Let $q \geq 2$ be an integer and let m, l be positive integer such that $q+1 = 2l+m$. The adjacency matrix A of $X(l,m)$ is

$$A = \begin{pmatrix} 2l & m \\ m & 2l \end{pmatrix}$$

and its characteristic polynomial is

$$\chi_A(t) = t^2 - 4lt + 4l^2 - m^2 = (t-(2l-m))(t-(q+1)).$$

Thus, the Ihara zeta function of $X = X(l,m)$ is given by

$$\zeta_X(u)^{-1} = (1-u^2)^{-\chi(X)}(1-(q+1)u+qu^2)P_X(u),$$

where

$$P_X(u) = 1-(2l-m)u+qu^2 \in \mathbb{Z}[u]. \tag{3}$$

2.2. Abelian Varieties over Finite Fields

2.2.1. Basic Notation, Terminology and Results

All the facts and results in Section 2.2.1 can be found in [6]. Let $q = p^a$ where p is a rational prime and a is a positive integer. Recall that an *abelian variety* over a finite field $\mathbb{F}_q$ is a geometrically irreducible projective algebraic group over $\mathbb{F}_q$. It is known that an abelian variety is a commutative algebraic group and is necessarily non-singular. An abelian variety A over $\mathbb{F}_q$ is called $\mathbb{F}_q$-*simple* if its only abelian subvarieties over $\mathbb{F}_q$ are 0 and A.

Let A, B be abelian varieties over $\mathbb{F}_q$. A $\mathbb{F}_q$-morphism of abelian varieties $A \to B$ is called a $\mathbb{F}_q$-*isogeny* if it is surjective and has finite kernel. This defines an equivalence relation on the collection of abelian varieties over $\mathbb{F}_q$. We shall write $A \sim B$ if A and B are $\mathbb{F}_q$-isogenous. Any abelian abelian variety over $\mathbb{F}_q$ is $\mathbb{F}_q$-isogenous to a product of $\mathbb{F}_q$-simple abelian varieties and this decomposition is unique up to $\mathbb{F}_q$-isogeny.

If A is an abelian variety over $\mathbb{F}_q$, then we denote the ring of $\mathbb{F}_q$-endomorphisms of A by $\mathrm{End}_{\mathbb{F}_q}(A)$ and we let

$$D = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{\mathbb{F}_q}(A). \tag{4}$$

If A is $\mathbb{F}_q$-simple, then D is a finite dimensional division algebra over $\mathbb{Q}$. The ring $\mathrm{End}_{\mathbb{F}_q}(A)$ is without $\mathbb{Z}$-torsion and therefore we have an inclusion

$$\mathrm{End}_{\mathbb{F}_q}(A) \hookrightarrow D.$$

Let now ℓ be another rational prime satisfying $\ell \neq p$. For a positive integer k, let $A[\ell^k](\overline{\mathbb{F}}_q)$ be the kernel of the multiplication-by-ℓ^k map on the $\overline{\mathbb{F}}_q$-rational points $A(\overline{\mathbb{F}}_q)$, and consider the Tate module

$$T_\ell A = \varprojlim_{k \geq 1} A[\ell^k](\overline{\mathbb{F}}_q).$$

It is known to be a free $\mathbb{Z}_\ell$-module of rank $2 \cdot \dim(A)$. Consider also the $\mathbb{Q}_\ell$-vector space

$$V_\ell A = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell A.$$

If we denote by $\pi_A \in \mathrm{End}_{\mathbb{F}_q}(A)$ the Frobenius endomorphism, then we let $f_A(u)$ denote the characteristic polynomial of π_A acting on $V_\ell A$. It is known to have the form

$$f_A(u) = u^{2\cdot\dim(A)} + \ldots + q^{\dim(A)} \in \mathbb{Z}[u].$$

We also let

$$L_A(u) = u^{2\cdot\dim(A)} f_A(1/u) = 1 + \cdots + q^{\dim(A)} u^{2\cdot\dim(A)} \in \mathbb{Z}[u] \tag{5}$$

be the reciprocal polynomial of $f_A(u)$.

If A is an abelian variety over $\mathbb{F}_q$ that is $\mathbb{F}_q$-simple, then its Frobenius endomorphism π_A is in the center of $\mathrm{End}_{\mathbb{F}_q}(A)$ and since D is a division algebra over $\mathbb{Q}$, π_A is an algebraic integer and $\mathbb{Q}(\pi_A)$ is a number field. Furthermore, the Riemann hypothesis for abelian varieties over finite fields (see [6, Theorem 1.1]) implies that π_A is a Weil q-number. In this case, we let $L = \mathbb{Q}(\pi_A)$ which is either a totally real number field or a CM-field.

2.2.2. The Honda-Tate Theorem

First, we have the following theorem whose proof can be found in [8, Theorem 5.3].

Theorem 3 (Tate)**.** *Two abelian varieties A and B defined over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogenous if and only if*

$$f_A(u) = f_B(u).$$

Further, if the abelian variety is simple, then we have the following result (see [8, Theorem 5.3] and [8, Theorem 5.4]).

Theorem 4 (Tate)**.** *Let A be a simple abelian variety over $\mathbb{F}_q$, let $L = \mathbb{Q}(\pi_A)$ be as above, and let D be the division algebra over $\mathbb{Q}$ defined in Equation (4) above.*

1. *The center of D is L.*
2. *One has*
$$f_A(u) = m_A(u)^d,$$
where $d = \sqrt{[D : L]} \in \mathbb{Z}$ and $m_A(u)$ is the minimal polynomial of π_A.
3. *One has*
$$2 \cdot \dim(A) = [L : \mathbb{Q}] \cdot \sqrt{[D : L]}.$$

4. *The central simple L-algebra D does not split at every real place of L, does split at every finite place not above p, and for a discrete valuation v lying above p, the Hasse invariant of D at v is given by*

$$\mathrm{inv}_v(D) \equiv \frac{v(\pi_A)}{v(q)} \cdot [L_v : \mathbb{Q}_p] \pmod{\mathbb{Z}},$$

where L_v is the local field obtained from L by completing at v. Moreover

$$\mathrm{inv}_v(D) + \mathrm{inv}_{v\circ\rho}(D) \equiv 0 \pmod{\mathbb{Z}},$$

where ρ is the complex conjugation on the CM-field L. (If L is totally real, then ρ is the trivial automorphism.)

Remark 1. If A is a simple abelian variety over $\mathbb{F}_q$, then we know by Theorem 4 that $f_A(u) = m_A(u)^d$, where $d = \sqrt{[D : L]}$. The number d can be calculated as follows (see [8, Facts 17.4]). It is the least common multiple of the denominators of the Hasse invariants $\mathrm{inv}_v(D)$ written as quotients with coprime numerator and denominator, where v runs over all the places of L.

Recall that two Weil q-numbers $\alpha, \beta \in \overline{\mathbb{Q}}$ are *conjugates* of one another if there exists $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\alpha^\sigma = \beta$. In this case, we write $\alpha \sim \beta$, and this defines an equivalence relation on the collection of Weil q-numbers. The following result can be found in [8, Theorem 1.2].

Theorem 5 (Honda-Tate)**.** *Fix a finite field $\mathbb{F}_q$. The assignment $A \mapsto \pi_A$ induces a bijection between the $\mathbb{F}_q$-isogeny classes of simple abelian varieties defined over $\mathbb{F}_q$ and the conjugacy classes of Weil q-numbers.*

As a consequence of Theorems 3, 4 and 5, one has the following precise description of isogeny classes of elliptic curves over finite fields. Fix again a finite field $\mathbb{F}_q$ and write $q = p^a$ for some rational prime p and some positive integer a. By Theorem 3, two elliptic curves C_1 and C_2 defined over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogenous if and only if $f_{C_1}(u) = f_{C_2}(u)$. Given an elliptic curve C over $\mathbb{F}_q$, write

$$f_C(u) = u^2 - \beta u + q,$$

for some $\beta \in \mathbb{Z}$. In this way, one associates to every $\mathbb{F}_q$-isogeny class of elliptic curves over $\mathbb{F}_q$ a rational integer $\beta \in \mathbb{Z}$. This correspondence is well-defined and injective by Theorem 3. It remains to describe the possible β which is the content of the following theorem (see [15, Theorem 4.1]).

Theorem 6. *The $\mathbb{F}_q$-isogeny classes of elliptic curves defined over $\mathbb{F}_q$ are in one-to-one correspondence with the rational integers β satisfying $|\beta| \leq 2\sqrt{q}$ and one of the following conditions:*

1. $(\beta, p) = 1$,
2. *If a is even:* $\beta = \pm 2\sqrt{q}$,
3. *If a is even and* $p \not\equiv 1 \pmod 3$*:* $\beta = \pm\sqrt{q}$,
4. *If a is odd and* $p = 2$ *or* 3*:* $\beta = \pm p^{\frac{a+1}{2}}$,
5. *If either* (i) *a is odd or* (ii) *a is even and* $p \not\equiv 1 \pmod 4$*:* $\beta = 0$.

2.2.3. Hasse-Weil Zeta Functions of Curves

Let C be a geometrically irreducible non-singular projective algebraic curve defined over a finite field $\mathbb{F}_q$. Its *Hasse-Weil zeta function* is defined to be

$$Z_C(u) = \exp\left(\sum_{k=1}^{\infty} |C(\mathbb{F}_{q^k})| \frac{u^k}{k}\right). \tag{6}$$

The Hasse-Weil zeta function satisfies several properties and we record the ones we shall need in the following theorem (see for instance [7, Theorem 3.2] and [7, Theorem 3.3]).

Theorem 7 (Weil)**.** *One has*

$$Z_C(u) = \frac{L_C(u)}{(1-u)(1-qu)},$$

for some polynomial $L_C(u) \in \mathbb{Z}[u]$. The constant coefficient of $L_C(u)$ is 1, its leading coefficient is q^g and the degree of $L_C(u)$ is $2g$, where g is the genus of the curve C. Moreover, if one writes

$$L_C(u) = \prod_{i=1}^{2g} (1 - \alpha_i u),$$

for some $\alpha_i \in \mathbb{C}$, then one has

$$|\alpha_i| = \sqrt{q},$$

for all $i = 1, \ldots, 2g$.

Remark 2. Let C be a geometrically irreducible non-singular projective algebraic curve defined over a finite field $\mathbb{F}_q$ of genus g and consider its Jacobian variety J which is an abelian variety over $\mathbb{F}_q$ of dimension g. Then, one has $L_J(u) = L_C(u)$ (see for instance [6, Corollary 11.4]). Furthermore, if C is an elliptic curve over $\mathbb{F}_q$, then $C = J$ (see [6, page 86]). So the notation for the L-polynomial of an elliptic curve is consistent with Equation (5).

We have the following well known corollaries which we will use later.

Corollary 1. *Let C be an elliptic curve defined over $\mathbb{F}_q$. If one writes*

$$L_C(u) = 1 - \beta u + qu^2,$$

for some $\beta \in \mathbb{Z}$, then

$$\beta = q + 1 - |C(\mathbb{F}_q)|.$$

Proof. From Theorem 7, one has

$$L_C(u) = (1-u)(1-qu)Z_C(u). \tag{7}$$

Write $L_C(u) = (1-\alpha_1 u)(1-\alpha_2 u)$ for some $\alpha_1, \alpha_2 \in \mathbb{C}$ necessarily satisfying $\beta = \alpha_1 + \alpha_2$. Applying the logarithm to Equation (7) leads to the equality of power series

$$-\sum_{k=1}^{\infty}(\alpha_1^k + \alpha_2^k)\frac{u^k}{k} = \sum_{k=1}^{\infty}(|C(\mathbb{F}_{q^k})| - 1 - q^k)\frac{u^k}{k}.$$

Thus, if $k = 1$ we have $\beta = q + 1 - |C(\mathbb{F}_q)|$. □

Corollary 2. *Two elliptic curves C_1 and C_2 defined over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogenous if and only if*

$$|C_1(\mathbb{F}_q)| = |C_2(\mathbb{F}_q)|.$$

Proof. This follows from Corollary 1 combined with Theorem 3 and Remark 2. □

3. Elliptic Curves over Finite Fields and Ramanujan Graphs on Two Vertices

Let us start with the following observation.

Proposition 2. *Let p be a rational prime and let $q = p^a$ for some positive integer a. Assume that X is a connected $(q+1)$-regular Ramanujan graph and that C is a geometrically irreducible non-singular projective algebraic curve over $\mathbb{F}_q$ for which*

$$P_X(u) = L_C(u).$$

Then, one has

$$\chi(X)((-1)^{k+1} - 1) - N_k(X) + 1 + q^k = |C(\mathbb{F}_{q^k})| - 1 - q^k,$$

for all positive integer k.

Proof. On one hand, it follows from Theorem 7 that

$$L_C(u) = (1-u)(1-qu)Z_C(u). \tag{8}$$

On the other hand, it follows from Theorem 1 that

$$P_X(u) = (1-u)^{\chi(X)}(1+u)^{\chi(X)}(1-u)^{-1}(1-qu)^{-1}\zeta_X(u)^{-1}. \tag{9}$$

If $P_X(u) = L_C(u)$, then taking the logarithm of both Equations (8) and (9), and using Equations (6) and (1), lead to the equality of power series

$$\sum_{k=1}^{\infty} \left(\chi(X)((-1)^{k+1}-1) - N_k(X) + 1 + q^k\right) \frac{u^k}{k} = \sum_{k=1}^{\infty} \left(|C(\mathbb{F}_{q^k})| - 1 - q^k\right) \frac{u^k}{k},$$

from which the result follows. □

For instance, if $q = p^a$ with p an odd prime, C is a geometrically irreducible non-singular projective curve of genus zero over $\mathbb{F}_q$ such as $\mathbb{P}^1$ over $\mathbb{F}_q$, and X is the bouquet graph with $(q+1)/2$ loops, then one has

$$P_X(u) = 1 = L_C(u),$$

and thus counting points on a curve of genus zero over $\mathbb{F}_q$ amounts to counting the number of reduced closed paths in X via Proposition 2. The next case to study is the case of graphs on two vertices and this leads to the following theorem which is Theorem A from the introduction.

Theorem 8. *Let $q = p^a$, where p is an odd prime and $a = 1$ or $a = 2$. Let Ω be the set of $\mathbb{F}_q$-isogeny classes of elliptic curves C over $\mathbb{F}_q$ for which $|C(\mathbb{F}_q)| \in 4\mathbb{Z}$, and let $\mathcal{R}$ be the set of connected $(q+1)$-regular Ramanujan graphs on two vertices. The map $\phi : \Omega \to \mathcal{R}$ defined via $[C] \mapsto \phi([C]) = X(l,m)$, where*

$$l = \frac{q+1}{2} - \frac{|C(\mathbb{F}_q)|}{4} \text{ and } m = \frac{|C(\mathbb{F}_q)|}{2},$$

is a one-to-one correspondence.

Proof. First, note that by Corollary 2, two elliptic curves C_1 and C_2 defined over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogenous if and only if $|C_1(\mathbb{F}_q)| = |C_2(\mathbb{F}_q)|$. This shows that ϕ is well-defined and does not depend on the choice of the representative of the isogeny class provided we show that the corresponding graph $X = X(l,m) = \phi([C])$ is a Ramanujan graph. The first thing to note is that the number of reduced closed paths of length one is $N_1(X) = 4l$. Thus, we have

$$N_1(X) - q - 1 = q + 1 - |C(\mathbb{F}_q)|. \tag{10}$$

Consider the polynomial $P_X(u) = 1 - \lambda u + qu^2$ from Equation (3), where

$$\lambda = 2l - m = N_1(X) - q - 1$$

is the unique eigenvalue in $\mathrm{Spec}(X)$ different than $q+1$. On the other hand, consider the L-polynomial of C, namely $L_C(u) = 1 - \beta u + qu^2$ where

$$\beta = q + 1 - |C(\mathbb{F}_q)|$$

by Corollary 1. Thus, it follows from Equation (10) that

$$L_C(u) = P_X(u). \tag{11}$$

The Hasse bound for C implies, in turn, that X is a Ramanujan graph. The fact that the map ϕ is injective follows from Theorem 3.

Let now $X = X(l, m)$ be a $(q+1)$-regular graph on two vertices and assume that it is a Ramanujan graph. In order to show the surjectivity of ϕ, remembering that $N_1(X) = 4l$, we have to find an elliptic curve C over $\mathbb{F}_q$ that satisfies

$$|C(\mathbb{F}_q)| = 2(q+1) - N_1(X). \tag{12}$$

Consider the polynomial $P_X(u) = 1 - \lambda u + qu^2$ from Equation (3) above, where $\lambda = 2l - m \in \mathbb{Z}$. Note that if $(\lambda, p) = 1$, then this is case (1) of Theorem 6. Since

$$\lambda = q + 1 - 2m,$$

one has $(\lambda, p) \neq 1$ if and only if

$$2m \equiv 1 \pmod{p}.$$

Note also that $m = q+1-2l$ is even. Since we are assuming that X is a Ramanujan graph, we necessarily have

$$q + 1 - 2\sqrt{q} \leq 2m \leq q + 1 + 2\sqrt{q}.$$

Thus, if $a = 1$, we have that $(\lambda, p) \neq 1$ if and only if

$$2m = 1 + p \text{ and } p \equiv 3 \pmod{4},$$

in which case $\lambda = 0$. This is case (5) of Theorem 6. If $a = 2$, then we have that $(\lambda, p) \neq 1$ if and only if

$$2m = (p-2)p + 1, p^2 + 1, (p+2)p + 1.$$

Since $2m$ is divisible by four, $2m \neq p^2 + 1$. Thus, $\lambda = \pm 2p$ and this is case (2) of Theorem 6. Thus, if $a = 1$ or 2, there exists an elliptic curve C over $\mathbb{F}_q$ for which

$$L_C(u) = P_X(u).$$

Proposition 2 implies, in particular for $k = 1$, that we have

$$-N_1(X) + 1 + q = |C(\mathbb{F}_q)| - 1 - q,$$

which is exactly the equality (12) we needed to obtain in order to show the surjectivity of ϕ. □

If $q = p^a$ for some odd prime p and some integer $a \geq 3$, then not every $(q+1)$-regular Ramanujan graph on two vertices corresponds to an elliptic curve over $\mathbb{F}_q$. For instance, if $p = 5$ and $a = 3$, so that $q = 5^3$, then consider the graph $X = X(l, m)$, where

$$l = 34 \text{ and } m = 58.$$

The graph X is 126-regular, and

$$P_X(u) = 1 - 10u + 125u^2.$$

Since $10 \leq 10 \cdot \sqrt{5}$, we have that X is a Ramanujan graph. But Theorem 6 shows that there is no elliptic curve C defined over $\mathbb{F}_q$ for which $L_C(u) = P_X(u)$. The multiplicative inverses of the roots of $P_X(u)$ are

$$\alpha_1 = 5 + 10i \text{ and } \alpha_2 = 5 - 10i,$$

which are both Weil q-numbers that are conjugate to one another. Therefore, by Theorem 5 there exists a simple abelian variety over $\mathbb{F}_q$, say A, corresponding to the conjugacy class of α_1. Note that $\mathfrak{p}_1 = (1 + 2i)$ and $\mathfrak{p}_2 = (1 - 2i)$ are the two distinct prime ideals of $\mathbb{Q}(i)$ lying above the split prime 5. Therefore, in $\mathbb{Q}(i)$ we have the prime ideal factorization

$$(\alpha_1) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2.$$

Thus, the non-trivial Hasse invariants of $D = \mathrm{End}^0(A)$ are given by

$$\mathrm{inv}_{\mathfrak{p}_1}(D) \equiv \frac{2}{3} \pmod{\mathbb{Z}} \text{ and } \mathrm{inv}_{\mathfrak{p}_2}(D) \equiv \frac{1}{3} \pmod{\mathbb{Z}}.$$

It follows from Theorem 4 and Remark 1 that $\dim(A) = 3$ and that

$$L_A(u) = P_X(u)^3.$$

On the other hand, if we exclude the supersingular elliptic curves and the Ramanujan graphs $X(l, m)$ on two vertices for which $2m \equiv 1 \pmod{p}$, then we have the following theorem.

Theorem 9. *Let $q = p^a$, where p is an odd prime number and a is an arbitrary positive integer. Let Ω_o be the set of $\mathbb{F}_q$-isogeny classes of ordinary elliptic curves C over $\mathbb{F}_q$ for which $|C(\mathbb{F}_q)| \in 4\mathbb{Z}$, and let $\mathcal{R}_1$ be the set of connected $(q+1)$-regular*

Ramanujan graphs $X(l, m)$ on two vertices for which $2m \not\equiv 1 \pmod{p}$. The map $\phi : \Omega_o \to \mathcal{R}_1$ defined via $[C] \mapsto \phi([C]) = X(l, m)$, where

$$l = \frac{q+1}{2} - \frac{|C(\mathbb{F}_q)|}{4} \text{ and } m = \frac{|C(\mathbb{F}_q)|}{2},$$

is a one-to-one correspondence.

Proof. It suffices to recall that an elliptic curve C over $\mathbb{F}_q$ is supersingular if and only if $(\beta, p) \neq 1$ (see [10, page 154]). The proof is then identical to the one for Theorem 8. □

In [1], it was shown that any elliptic curve C defined over a finite field $\mathbb{F}_q$ (where $q = p^a$ for an odd prime p) satisfying $|C(\mathbb{F}_q)| \in 4\mathbb{Z}$ is $\mathbb{F}_q$-isogenous to a Legendre elliptic curve with one possible exception. Recall that a Legendre elliptic curve C over $\mathbb{F}_q$ is the projective closure of an affine curve given by an equation of the form

$$y^2 = x(x-1)(x-\delta)$$

for some $\delta \in \mathbb{F}_q \setminus \{0, 1\}$. For instance, if we take $q = 3$ and the elliptic curve C corresponding to the affine curve

$$y^2 = x(x-1)(x-2)$$

over $\mathbb{F}_3$, then we have $|C(\mathbb{F}_3)| = 4$. Thus, the corresponding graph X is

and counting points in $C(\mathbb{F}_{3^k})$ essentially amounts to counting reduced closed paths of length k on X via Proposition 2.

The situation when $p = 2$ can be studied similarly. The precise statement is the following one and the proof is identical to the one for Theorem 8.

Theorem 10. *Let $q = 2^a$ where a is any positive integer. Let Ω be the set of $\mathbb{F}_q$-isogeny classes of elliptic curves C over $\mathbb{F}_q$ for which $|C(\mathbb{F}_q)| \equiv 2 \pmod{4}$, and let $\mathcal{R}$ be the set of connected $(q+1)$-regular Ramanujan graphs on two vertices. The map $\phi : \Omega \to \mathcal{R}$ defined via $[C] \mapsto \phi([C]) = X(l, m)$, where*

$$l = \frac{q+1}{2} - \frac{|C(\mathbb{F}_q)|}{4} \text{ and } m = \frac{|C(\mathbb{F}_q)|}{2},$$

is a one-to-one correspondence.

Note that an elliptic curve over $\mathbb{F}_{2^a}$ satisfying $|C(\mathbb{F}_{2^a})| \equiv 2 \pmod 4$ is necessarily ordinary.

Let us end this paper with the following example involving a graph with more than two vertices. Let $q = 2$, and consider $X = K_4$, the complete graph on four vertices. The graph X is 3-regular and $\mathrm{Spec}(X) = \{3, -1, -1, -1\}$; thus,

$$P_X(u) = (1 + u + 2u^2)^3,$$

and X is a 3-regular Ramanujan graph. Theorem 6 implies the existence of an elliptic curve C over $\mathbb{F}_2$ for which

$$L_C(u) = 1 + u + 2u^2.$$

Letting A be the non-simple abelian variety $A = C^3$ over $\mathbb{F}_2$, one has

$$P_X(u) = L_A(u).$$

We point out that A cannot be the Jacobian variety of a curve C over $\mathbb{F}_2$. Indeed, if this were the case, then by Remark 2 we would have

$$L_C(u) = L_A(u) = (1 - \alpha_1 u)^3 (1 - \alpha_2 u)^3,$$

where

$$\alpha_1, \alpha_2 = \frac{-1 \pm \sqrt{-7}}{2}.$$

Thus, we would have

$$Z_C(u)(1 - u)(1 - 2u) = (1 - \alpha_1 u)^3 (1 - \alpha_2 u)^3.$$

Applying the logarithm to both sides and equating the coefficients would give

$$|C(\mathbb{F}_{2^k})| = 1 + 2^k - 3(\alpha_1^k + \alpha_2^k),$$

which, in turn, would lead to

$$|C(\mathbb{F}_2)| = 6, |C(\mathbb{F}_4)| = 14, \text{and } |C(\mathbb{F}_8)| = -6, \ldots$$

But this is impossible.

Acknowledgement. The author is grateful to the Max Planck Institute for Mathematics in Bonn for its hospitality and financial support.

References

[1] R. Auer and J. Top, Legendre elliptic curves over finite fields, *J. Number Theory* **95** (2002), no. 2, 303-312.

[2] Y. Ihara, Discrete subgroups of PL(2, $k_{\wp}$), in *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, Amer. Math. Soc., Providence, RI, 1966.

[3] Y. Ihara, On discrete subgroups of the two by two projective linear group over $\mathfrak{p}$-adic fields, *J. Math. Soc. Japan* **18** (1966), 219-235.

[4] M. Kotani and T. Sunada, Zeta functions of finite graphs, *J. Math. Sci. Univ. Tokyo* **7** (2000), no. 1, 7-25.

[5] A. Lubotzky, R. Phillips, and P. Sarnak, Ramanujan graphs, *Combinatorica* **8** (1988), no. 3, 261-277.

[6] J. S. Milne, *Abelian Varieties (v2.00)*, 2008. Available at `www.jmilne.org/math/`

[7] C. Moreno, *Algebraic Curves over Finite Fields*, Cambridge University Press, Cambridge, 1991.

[8] F. Oort, Abelian varieties over finite fields, in *Higher-Dimensional Geometry over Finite Fields*, IOS, Amsterdam, 2008.

[9] J.-P. Serre, *Arbres, Amalgames,* SL_2, Société Mathématique de France, Paris, 1977.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Dordrecht, 2009.

[11] K. Sugiyama, Zeta functions of Ramanujan graphs and modular forms, *Comment. Math. Univ. St. Pauli* **66** (2017), no. 1-2, 29-43.

[12] T. Sunada, L-functions in geometry and some applications, in *Curvature and Topology of Riemannian Manifolds (Katata, 1985)*, Springer, Berlin, 1986.

[13] T. Sunada, *Topological Crystallography*, Springer, Tokyo, 2013.

[14] A. Terras, *Zeta Functions of Graphs*, Cambridge University Press, Cambridge, 2011.

[15] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. Éc. Norm. Supér. (4)* **2** (1969), 521-560.