RIMS Kôkyûroku Bessatsu
B66 (2017), 195–211

The Ihara zeta functions of a Ramanujan graph

By

Ken-ichi Sugiyama[*]

Abstract

We will discuss the relationship between Ihara's zeta functions of Ramanujan graphs and Hasse-Weil's congruent congruent zeta functions of modular curves. The residue of the Hasse-Weil's congruent zeta functions at $t = 1$ will be described by the number of supersingular points and the complexity of the associated graphs.

§ 1. Introduction

The aim of this report is to study the relationship between the Ihara zeta functions of a connected Ramanujan graphs and the Hasse-Weil zeta functions of smooth proper curves defined over a finite field.

Shortly a graph is a one dimensional simplicial complex. In this paper we will only treat graphs oriented in both directions. The informations of a graph G are encoded in the adjacency matrix A, which describes how edges and vertices are connected. Although graphs are geometric objects they are intimately related to number theory. In fact let $\mathcal{P}(G)$ be the set of reduced and tail-less primitive closed paths of G i.e. the set of closed path without backtracking and not around more than once. We call two elements of $\mathcal{P}(G)$ are *equivalent* if one is a shift of the other and let $\mathfrak{P}(G)$ denote the set of equivalent classes of $\mathcal{P}(G)$. The length of a closed path (= the number of edges contained in the path) only depends on the equivalent class and we have a function

$$l : \mathfrak{P}(G) \to \mathbb{Z}.$$

Received June 15, 2016. Revised November 17, 2016.
2010 Mathematics Subject Classification(s): 05C30, 05C38, 05C50, 11G18, 11G20, 11M38, 11M99, 14G10.
Key Words: *Ramanujan graphs, the Ihara zeta function, modular curves, the Hasse-Weil zeta function.*

[*] Department of Mathematics, Faculty of Science, Rikkyo University, Toshima-ku, Tokyo, 171-8501, Japan.
e-mail: `kensugiyama@rikkyo.ac.jp`

Now the zeta function of G is defined as

$$Z(G;t) = \prod_{[c]\in\mathfrak{P}(G)} \frac{1}{1-t^{l([c])}} \tag{1.1}$$

(See **Section 2** for these materials and the facts concerning graphs). The function is originally defined by Ihara and called *the Ihara zeta function.* It is studied by various mathematicians (we only refer [11], [12], [14], [15], [16], [13], [29] but there are much more). One of the most remarkable properties is that $Z(G;t)$ is a rational function;

$$Z(G;t) = \frac{(1-t^2)^{\chi(G)}}{\det[1-At+Qt^2]}. \tag{1.2}$$

Here Q is a diagonal matrix whose entry at the vertex x is $d(x)-1$ where $d(x)$ is the number of edges exiting from x and $\chi(G)$ denotes the Euler characteristic of G. In this paper we assume that G is connected and d-regular i.e. $d(x) = d$ for any vertex x. Then d is an eigenvalue of A of multiplicity one. Moreover it is known that an eigenvalue λ of A satisfies $|\lambda| \leq d$ and that $-d$ is an eigenvalue of A if and only if G is bipartite. If $|\lambda| \leq 2\sqrt{d-1}$ is satisfied for an eigenvalue λ of A other than $\pm d$, then the graph is called *Ramanujan.* The zeta function of a Ramanujan graph has similar properties as the the Hasse-Weil congruent zeta function, which we will now recall.

Let C be a smooth proper curve defined over a finite field $\mathbb{F}_q$ of characteristic p. The q-th power Frobenius $F = Fr_q$ acts on the set of closed points $C(\overline{\mathbb{F}}_q) := \mathrm{Hom}_{\mathbb{F}_q}(\mathrm{Spec}(\overline{\mathbb{F}}_q), C)$ by the obvious way and $|C|$ denotes the orbit space. The degree of a closed point x is defined to be the extension degree of the residue field $k(x)$ over $\mathbb{F}_q$ and it descends to the map

$$\deg : |C| \to \mathbb{Z}.$$

Now the Hasse-Weil zeta function $W(C;t)$ of C is defined as

$$W(C;t) = \prod_{x\in|C|} \frac{1}{1-t^{\deg(x)}} = \exp(\sum_{n=1}^{\infty} \frac{|C(\mathbb{F}_{q^n})|}{n} t^n), \tag{1.3}$$

where $C(\mathbb{F}_{q^n})$ is the set of $\mathbb{F}_{q^n}$-rational points which is identified with the set of fixed poitns $C(\overline{\mathbb{F}}_q)^{F^n}$. *A priori* this is only a formal power series but it is a rational function by the Grothendieck-Lefschetz trace formula ([5]). In fact for a prime $l(\neq p)$ let $H^i_{et}(\overline{C}, \mathbb{Z}_l)$ denote the l-adic étale cohomology, where $\overline{C}$ is the base change C over the $\overline{\mathbb{F}}_q$. It is a free $\mathbb{Z}_l$-module whose rank is the twice of the genus of C. It has the action of F and

$$W(C;t) = \frac{\det(1-Ft \mid H^1_{et}(\overline{C}, \mathbb{Z}_l))}{(1-t)(1-qt)}. \tag{1.4}$$

Now observe that (1.1) and (1.3) are quite similar if one corresponds $\mathcal{P}(G)$ and $\mathfrak{P}(G)$ to $C(\overline{\mathbb{F}}_q)$ and $|C|$, respectively. Hence it will be natural to expect that there should be relation between (1.2) and (1.4). But there are obvious constraints. In fact by the solution of the Weil conjecture, the eigenvalue of F on $H^1_{et}(\overline{C}, \mathbb{Z}_l)$ are algebraic integers of modulus $\sqrt{q}$ ([4]). The corresponding condition of A is that the associated graph is connected $(q+1)$-regular Ramanujan not bipartite. After these consideration our question is whether there is a pair (G, C) of a Ramanujan graph and a curve defined over $\mathbb{F}_q$ so that

$$\frac{\det[1 - At + Qt^2]}{(1-t)(1-qt)} = \det(1 - Ft \,|\, H^1_{et}(\overline{C}, \mathbb{Z}_l)) = (1-t)(1-qt)W(C;t),$$

or equivalently

$$\frac{1}{W(C;t)} = \frac{(1-t)^2(1-qt)^2}{(1-t^2)^{\chi(G)}} Z(G;t). \tag{1.5}$$

These relations between the zeta function of graphs and the Hasse-Weil congruent zeta function are pointed out by Ihara ([17]) and after that there are several ways to construct Ramanujan graphs ([20], [21], [23]). Our construction is based on the way of Mestre and Oesterlé, which is sketched in [23]. Here is a summary of our construction. Let us fix a prime N and take another prime p. The Hecke operator T_p naturally acts on the free abelian group generated by supersingular elliptic curves over $\overline{\mathbb{F}}_N$. The representation matrix is called *a Brandt matrix* and will be denoted by $B(p)$. Taking adjacency matrix of a graph gives a bijective correspondence between the set of graphs and the set of matrices satisfying certain conditions. The Brandt matrix is a candidate of an adjacency matrix of our graph but unfortunately not in general since it does not satisfy the necessary conditions to be an adjacency matrix of a graph. However, if $N-1$ is divisible by 12, $B(p)$ becomes an adjacency matrix of a Ramanujan graph $G_N(p)$.

Theorem 1.1. *Let N be a prime such that $N-1$ is divisible by 12 and we set*

$$n = \frac{N-1}{12}.$$

Then

1.

$$W(X_0(N)_{\mathbb{F}_p}, t) Z(G_N(p), t) = \frac{1}{(1-t)^2(1-pt)^2(1-t^2)^{\frac{n(p-1)}{2}}}.$$

2.

$$\lim_{t \to 1} (t-1) W(X_0(N)_{\mathbb{F}_p}, t) = \frac{n\tau(G_N(p))}{p-1}.$$

Here $\tau(G_N(p))$ is the complexity of $G_N(p)$ which is defined to be the number of spanning trees in $G_N(p)$ (see §2).

The assertion (2) of the theorem may be compared to *the class number formula*, but we do not know how $\tau(G_N(p))$ can be interpreted as a K-theoretical object. Let $S_2(\Gamma_0(N))$ be the space of cusp forms of weight 2 for the Hecke congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$. Then the dimension of $S_2(\Gamma_0(N))$ is $n-1$ and we can take normalized Hecke eigenforms $\{f_1, \cdots, f_{n-1}\}$ as its basis. Let

$$f_i = \sum_{n=1}^{\infty} a_n(f_i) q^n, \quad q = e^{2\pi i z} \quad (\mathrm{Im}\, z > 0)$$

be the Fourier expansion which satisfies $a_1(f_i) = 1$ by definition. The classical Kirchhoff formula which is used to derive (2) of **Theorem 1.1** and the Eichler-Shimura relation will imply the following congruence.

Theorem 1.2. *Let $p(\neq N)$ be a prime such that $1+p$ is a multiple of $n = \frac{N-1}{12}$. Then the product of p-th coefficients $\mu_N(p) := \prod_{i=1}^{n-1} a_p(f_i)$ is divisible by n.*

We have listed the results of numerical experiments for $N = 37$, 61, 73 in the last section. **Theorem 1.2** immediately yields the following corollary.

Corollary 1.3. *Let r be a prime divisor of n. Then there is a normalized Hecke eigenform $f = \sum_{n=1}^{\infty} a_n(f) q^n \in S_2(\Gamma_0(N))$ satisfying*

$$|\{p \textit{ is a prime} : a_p(f) \equiv 0 \,(\mathrm{mod}\, r), \quad p \equiv -1 \,(\mathrm{mod}\, n)\}| = \infty$$

Acknowledgements. The author thanks Prof. Noro who has kindly informed us of the results of numerical experiments, and Prof. Geisser for his careful reading the manuscript. He also appreciates Prof. Aoki's comments and valuable suggestions.

§ 2. The Ihara zeta function of a graph

In this section we recall basic facts of the Ihara zeta function of a graph. The basic references are [2], [29] and [31].

A (finite) graph G consists of a finite set of vertices $V(G)$ and a finite set of oriented edges $E(G)$, which satisfy the following property. There are *the end point maps*,

$$\partial_0, \quad \partial_1 : E(G) \to V(G),$$

and *an orientation resersal*,

$$J : E(G) \to V(G), \quad J^2 = \text{identity},$$

such that $\partial_i \circ J = \partial_{1-i}\,(i = 0, 1)$. The quotient $E(G)/J$ is called *the set of geometric edges* and is denoted by $GE(G)$. We regard an element of $GE(G)$ as an unoriented edge.

For $x \in V(G)$ we set

$$E_j(x) = \{e \in E(G) \,|\, \partial_j(e) = x\}, \quad j = 0, 1.$$

Thus $JE_j(x) = E_{1-j}(x)$. Intuitively $E_0(x)$ (resp. $E_1(x)$) is the set of edges starting from (resp. arriving at) x. The *degree* of x, $d(x)$, is defined by

$$d(x) = |E_0(x)| = |E_1(x)|.$$

$E(G)$ is naturally divided into two classes, *loops* and *passes.* An edge $e \in E(G)$ is called *a loop* if $\partial_0(e) = \partial_1(e)$ and is called *a pass* otherwise. Let $\rho(x)$ and $p(x)$ be the number of loops and passes starting from x, respectively. Note that, because of the involution J, if we replace "starting" by "arriving" these number does not change. By definition, it is clear that

$$d(x) = 2\rho(x) + p(x).$$

We call G *k-regular* if $d(x) = k$ for all $x \in V(G)$. If $V(G)$ is a disjoint union of two subsets $V_+(G)$ and $V_-(G)$ and every edge connects points $P_+ \in V_+(G)$ and $P_- \in V_-(G)$, we mention that G is *bipartite.*

A path of length m is a sequence $c = (e_1, \cdots, e_m)$ of edges such that $\partial_0(e_i) = \partial_1(e_{i-1})$ for all $1 < i \leq m$ and the path is *reduced* if $e_i \neq J(e_{i-1})$ for all $2 \leq i \leq m$. The path is *closed* if $\partial_0(e_1) = \partial_1(e_m)$ and the closed path has *no tail* if $e_m \neq J(e_1)$. A closed path of length one is called *a loop.* Two closed paths are *equivalent* if one is obtained from the other by a cyclic shift of the edges. Let $C(G)$ be the set of reduced and tail-less closed paths of G and $\mathfrak{C}(G)$ the collection of its equivalence classes. Since the length is depend on the equivalence class the length function descends to the map;

$$l : \mathfrak{C}(G) \to \mathbb{N}, \quad l([c]) = l(c),$$

where $[c]$ is the class determined by c. We define a reduced and tail-less closed path c to be primitive if it is not obtained by going $r(\geq 2)$ times some another closed path. Let $\mathfrak{P}(G)$ be the subset of $\mathfrak{C}(G)$ consisting of the classes of primitive closed paths (which are reduced and tail-less by definition). Now the Ihara zeta function of G is defined to be

$$Z(G; t) = \prod_{[c] \in \mathfrak{P}(G)} \frac{1}{1 - t^{l([c])}}.$$

For a finite set X, $\mathbb{Z}^X$ denotes the set of $\mathbb{Z}$-valued function on X which is a free abelian group generated by X. We set $q(x) := d(x) - 1$ and define endomorphism Q and A of $\mathbb{Z}^{V(G)}$ as

$$Q : \mathbb{Z}^{V(G)} \to \mathbb{Z}^{V(G)}, \quad Q(x) = q(x)x \ (x \in V(G)),$$

and

$$A(x) = \sum_{e \in E(G), \partial_0(e) = x} \partial_1(e), \quad x \in \mathbb{Z}^{V(G)}.$$

Note that because of the involution J,

$$A(x) = \sum_{e \in E(G), \partial_1(e) = x} \partial_0(e).$$

The operator A will be called *adjacency operator.* We sometimes identify it with the representing matrix with respect to the basis $\{x\}_{x \in V(G)}$. Thus the xy-entry of A_{xy} is the number of edges starting from x and arriving at y. The orientation reversing involution J implies

$$A_{xy} = A_{yx}.$$

Note that $A_{xx} = 2\rho(x)$ and $p(x) = \sum_{y \neq x} A_{yx}$.

Connecting distinct vertices x and y by A_{xy}-edges and drawing $\frac{1}{2}A_{xx}$-loops at x, the adjacency matrix A determines a 1-dimensional unoriented simplicial complex. We call it *the geometric realization* of G, and denote it by G again. We say that G is connected if its the geometric realization is. The Euler characteristic $\chi(G)$ is equal to $|V(G)| - |GE(G)|$, hence if G is connected, the fundamental group is a free group of rank $1 - |V(G)| + |GE(G)|$. *A tree* is defined to be a graph which is connected and simply connected. A tree T contained in G satisfying $V(T) = V(G)$ is called *a spanning tree* of G. Intuitively a spanning tree is a maximal tree in G. Let $\tau(G)$ denote the number of spanning trees of G and we call $\tau(G)$ the *complexity* of G. For a later purpose, we summarize the relationship between a graph and its adjacency matrix.

Proposition 2.1. *Let $A = (a_{ij})_{1 \leq i,j \leq m}$ be an $m \times m$-matrix satisfying the following conditions.*

1. *The entries $\{a_{ij}\}_{ij}$ are non-negative integers and satisfy*

$$a_{ij} = a_{ji}, \quad \forall i \, and \, j.$$

2. *a_{ii} is even for every i.*

Then there is a unique graph G whose adjacency matrix is A. Moreover, G is k-regular if and only if one of the following conditions holds :

1.

$$\sum_{i=1}^{m} a_{ij} = k, \quad \forall j$$

2.

$$\sum_{j=1}^{m} a_{ij} = k, \quad \forall i.$$

Proposition 2.2. *([30]* **Proposition 2.2***) Let G be a k-regular graph with m vertices. Then the Euler characteristic $\chi(G)$ satisfies*

$$\chi(G) = \frac{m(2-k)}{2}.$$

In the following, a graph G is always assumed to be *connected.* Here is the Ihara's formula for the zeta function.

Fact 2.3. *([2],[13],[16],[29])*

$$Z(G;t) = \frac{(1-t^2)^{\chi(G)}}{\det[1 - At + Qt^2]}.$$

Proposition 2.2 and **Fact 2.3** yield the following result.

Proposition 2.4. *Let G be a k-regular graph with m vertices. Then*

$$Z(G;t) = \frac{(1-t^2)^{\frac{m(2-k)}{2}}}{\det[1 - At + Qt^2]}.$$

Let $E_0(G) \subset E(G)$ be a section of the natural projection $E(G) \to GE(G)$, which is identified the set of oriented edges for a certain orientation. Let

$$\partial : \mathbb{Z}^{E_0(G)} \to \mathbb{Z}^{V(G)}$$

be the boundary map and ∂^t the dual. Then *the Laplacian* Δ of G is defined to be $\Delta = \partial\partial^t$. It is known that ([31], [13]),

$$\Delta = 1 - A + Q. \tag{2.1}$$

Here is the relationship between the complexity and the Laplacian.

Fact 2.5. *(The Kirchhoff law, [3]* **Theorem 6.3***) Let $\{0, \alpha_1, \cdots, \alpha_{n-1}\}$ be the eigenvalues of Δ. Then*

$$\tau(G) = \frac{\alpha_1 \cdots \alpha_{n-1}}{n}.$$

Let G' be the graph obtained by deleting all loops of G. By the equation (2.1) we see that the Laplacian of G and G' are same, and **Fact 2.5** implies

$$\tau(G) = \tau(G').$$

One may also observe this fact by inspection. Here is an example.

Example 2.6. Let G and G' be graphs with vertices $\{[1],[2],[3],[4]\}$ and whose shape are described by the following adjacency matrices A and A', respectively. The (i,j)-entry is the number of geometric edges connecting vertices $[i]$ and $[j]$.

1.
$$A = \begin{pmatrix} 2\,1\,0\,1 \\ 1\,0\,3\,0 \\ 0\,3\,0\,1 \\ 1\,0\,1\,2 \end{pmatrix}, \quad Q = \begin{pmatrix} 3\,0\,0\,0 \\ 0\,3\,0\,0 \\ 0\,0\,3\,0 \\ 0\,0\,0\,3 \end{pmatrix}$$

2.
$$A' = \begin{pmatrix} 0\,1\,0\,1 \\ 1\,0\,3\,0 \\ 0\,3\,0\,1 \\ 1\,0\,1\,0 \end{pmatrix}, \quad Q' = \begin{pmatrix} 1\,0\,0\,0 \\ 0\,3\,0\,0 \\ 0\,0\,3\,0 \\ 0\,0\,0\,1 \end{pmatrix}$$

Then G is a 4-regular graph which has loops at the vertices [1] and [4] and G' is obtained by deleting these loops from G. The equation (2.1) shows that the corresponding Laplacians Δ and Δ' are equal. In fact

$$\Delta = \Delta' = \begin{pmatrix} 2 & -1 & 0 & -1 \\ -1 & 4 & -3 & 0 \\ 0 & -3 & 4 & -1 \\ -1 & 0 & -1 & 2 \end{pmatrix}.$$

The eigenvalues of this matrix are $\{0, 2, 5+\sqrt{5}, 5-\sqrt{5}\}$, and Kirchhoff law tells us

$$\tau(G) = \tau(G') = \frac{2(5+\sqrt{5})(5-\sqrt{5})}{4} = 10.$$

Drawing a picture, one can immediately verify this.

Since we have assumed that G is connected, 0 is an eigenvalue of Δ with multiplicity one. Hence if G is a regular graph of degree k, the above observation shows that k is an eigenvalue of A with multiplicity one. It is known that

$$|\lambda| \le k \quad \text{for any eigenvalue } \lambda \text{ of } A$$

that $-k$ is an eigenvalue of A if and only if G is bipartite ([31], **Chapter 3**).

Definition 2.7. We say that G is Ramanujan if for all eigenvalues λ of A that $|\lambda| \neq k$ satisfy

$$|\lambda| \leq 2\sqrt{k-1}.$$

§ 3. Ramanujan graphs

In this section we will explain some ways to construct a Ramanujan graph.

Let G be a group. A subset S is called *symmetric* if the inverse of any element $s \in S$ is also contained in S. Then *the Cayley graph* $C(G, S)$ is a graph whose vertices are the elements of G and $x, y \in G$ are connected if $y = sx$ for a certain $s \in S$. If d is the cardinality of S, $C(G, S)$ is d-regular.

§ 3.1. A trivial example

Fact 3.1. *([31]* **Chapter 3, Theorem 2***) Let S be a symmetric subset of $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \cdots, n-1\}$. Then the eigenvalues of the adjacency matrix of the Cayley graph $C(\mathbb{Z}/n\mathbb{Z}, S)$ are*

$$\{\sum_{s \in S} \exp(-\frac{2\pi iks}{n})\}_{k=0,1,\cdots,n-1}.$$

Take $S = \{1, -1\}$ as a symmetric set . Then $C(\mathbb{Z}/n\mathbb{Z}, S)$ is the regular n-gon and the adjacency matrix is

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Fact 3.1 shows that the eigenvalues of A are

$$\{2\cos(\frac{2\pi k}{n})\}_{k=0,1,\cdots,n-1}$$

and $C(\mathbb{Z}/n\mathbb{Z}, \{\pm 1\})$ is a connected Ramanujan graph. Note that it is bipartite if and only if n is even.

§ 3.2. The construction due to Li ([20])

Let p be an odd prime. Consider the norm map

$$N : \mathbb{F}_{p^2}^{\times} \to \mathbb{F}_p^{\times}, \quad N(x) = x \cdot x^p$$

and let S be the kernel, namely

$$S = \{x \in \mathbb{F}_{p^2} \,|\, x^{p+1} = 1\}.$$

Take $G = \mathbb{F}_{p^2}$ (an additive group) and then S is symmetric subset of $(p+1)$-elements. Let us consider the Cayley graph $C(\mathbb{F}_{p^2}, S)$, which is regular of degree $p+1$. In order to describe the property it is convenient to identify the adjacency matrix with the linear operator A on the function space $L(\mathbb{F}_{p^2}) := \{f : \mathbb{F}_{p^2} \to \mathbb{C}\}$ which is defined to be

$$(Af)(x) := \sum_{s\in S} f(x+s). \quad f \in L(\mathbb{F}_{p^2}).$$

By [31] pp.74-pp.75,

$$\psi_k(x) := \exp(\frac{2\pi i \mathrm{Tr}(kx)}{p}) \quad (k \in \mathbb{F}_{p^2})$$

is an eigenfunction of A of the eigenvalue

$$\lambda_k := \sum_{x\in\mathbb{F}_{p^2}^{\times}, N(x)=N(k)} \exp(\frac{2\pi i \mathrm{Tr}(x)}{p}), \quad k \neq 0,$$

and

$$\lambda_0 = p + 1.$$

Here Tr is the trace

$$\mathrm{Tr}(x) := x + x^p.$$

Note that $\lambda_k (k \neq 0)$ is the Kloosterman sum and Deligne has shown (see [6] pp.219 and pp.220 (7.2.5)) that

$$|\lambda_k| \leq 2\sqrt{p}, \quad k \neq 0.$$

Hence $C(\mathbb{F}_{p^2}, S)$ is a connected Ramanujan graph which is not bipartite.

§ 3.3. The construction due to Lubotzky-Phillips-Sarnak ([21], [32])

Let p and q be distinct primes congruent 1 mod 4. Then -1 is a quadratic residue mod q and there is an integer i such that

$$i^2 \equiv -1 \,(\mathrm{mod}\ q).$$

Let us consider the equation

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p. \tag{3.1}$$

By a well-known theorem due to Jacobi it has $8(p+1)$ integer solutions and let $a = (a_0, a_1, a_2, a_3)$ be one of them. Then one finds that only one a_i is odd and remains are even. Hence the number of the solutions with $a_0 > 0$ and odd is $p+1$ and let Σ denote the collection of such solutions. To $a = (a_0, a_1, a_2, a_3) \in \Sigma$ we associate a matrix in $\mathrm{PGL}_2(\mathbb{F}_q)$,

$$\hat{a} = \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix},$$

and set

$$S := \{\hat{a} \,|\, a \in \Sigma\} \subset \mathrm{PGL}_2(\mathbb{F}_q).$$

It is symmetric and we form a Cayley graph $X^{p,q} := C(\mathrm{PGL}_2(\mathbb{F}_q), S)$. This is $(p+1)$-regular graph whose number of vertices is $q(q^2-1)$. Since the determinant of $\hat{a}$ is p, $X^{p,q}$ is not connected if $(\frac{p}{q}) = 1$ (i.e. $p \in (\mathbb{F}_q^\times)^2$). In fact let us divide the set of vertices $V(X^{p,q})$ into $V_+ := \{g \in \mathrm{PGL}_2(\mathbb{F}_q) \,|\, \det(g) \in (\mathbb{F}_q^\times)^2\}$ and $V_- := \{g \in \mathrm{PGL}_2(\mathbb{F}_q) \,|\, \det(g) \notin (\mathbb{F}_q^\times)^2\}$. If $(\frac{p}{q}) = 1$ any elements of S never connect V_+ and V_- since $\det(\hat{a})$ $(\hat{a} \in S)$ is a quadratic residue mod q. Hence if $(\frac{p}{q}) = 1$ we replace $\mathrm{PGL}_2(\mathbb{F}_q)$ by the subgroup $\mathrm{PSL}_2(\mathbb{F}_q)$ of index 2 and define $Y^{p,q} = C(\mathrm{PSL}_2(\mathbb{F}_q), S)$. Then both $X^{p,q}$ (if $(\frac{p}{q}) = -1$) and $Y^{p,q}$ (if $(\frac{p}{q}) = 1$) are connected regular graphs of degree $p+1$. Lubotzky, Phillips and Sarnak have shown that $X^{p,q}$ (resp. $Y^{p,q}$) is bipartite (resp. not bipartite) Ramanujan graph ([21] **Theorem 4.1**). The proof is based on the harmonic analysis on the algebraic group $G = \mathbb{H}^\times / Z(\mathbb{H}^\times)$ where $\mathbb{H}^\times$ is the set of invertible elements of the Hamilton quaternion $\mathbb{H}$ and Z denotes the center.

§ 4. The Ramanujan graph of a modular curve

§ 4.1. The Brandt matrix

In this subsection we will recall the theory of Brandt matrices after [9]. Let N be a prime, and let B be the quaternion algebra over $\mathbb{Q}$ ramified at two places N and ∞. Let R be a fixed maximal order in B and $\{I_1, \cdots, I_n\}$ be the set of left R-ideals representing the distinct ideal classes. We call n *the class number* of B and it is computed by N as shown in the following **Table 1** ([9]**Table 1.3**). We choose $I_1 = R$. For $1 \le i \le n$, R_i denotes the right order of I_i, and let w_i the order of $R_i^\times / \{\pm 1\}$. The product

$$W = \prod_{i=1}^{n} w_i \tag{4.1}$$

is independent of the choice of R and is equal to the exact denominator of $\frac{N-1}{12}$ ([9], p.117). Eichler's mass formula states that

$$\sum_{i=1}^{n} \frac{1}{w_i} = \frac{N-1}{12}.$$

N	n
2	1
3	1
$\equiv 5(12)$	$(N+7)/12$
$\equiv 7(12)$	$(N+5)/12$
$\equiv 11(12)$	$(N+13)/12$
$\equiv 1(12)$	$(N-1)/12$

Table 1. The table of the class number

Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_N$. There are n distinct isomorphism classes $\{E_1, \cdots, E_n\}$ of supersingular elliptic curves over $\mathbb{F}$ such that $\mathrm{End}(E_i) \simeq R_i$. Let p be a prime distinct from N, and let $\mathrm{Hom}(E_i,\, E_j)(p)$ denote the set of homomorphisms from E_i to E_j of degree p. The (i, j)-entry of the Brandt matrix $B(p)$ is defined to be

$$b_{ij} = \frac{1}{2w_j} |\mathrm{Hom}(E_i,\, E_j)(p)|. \tag{4.2}$$

Since $\mathrm{Hom}(E_i,\, E_j)(p)$ has a faithful action of $R_j^\times$ from the right, b_{ij} is a non-negative integer. In fact b_{ij} equals to the number of subgroup C of order p in E_i such that $E_i/C \simeq E_j$ ([9] **Proposition 2.3**).

Now we assume that $N-1$ is divisible 12. Since $\frac{N-1}{12}$ is an integer $W = \prod_{i=1}^n w_i = 1$ and $w_i = 1$ for all i. Hence by Eichler's mass formula

$$n = \frac{N-1}{12}. \tag{4.3}$$

Fact 4.1. *([25]* **Proposition 4.6***, see also [30]* **Proposition 3.1***) Let N be a prime such that $N-1$ is divisible by 12. Then the Brandt matrix $B(p) = (b_{ij})_{1 \le i,j \le n}$ $(p \neq N)$ satisfies the following.*

1. *Every entry is a non-negative integer and $B(p)$ is symmetric;*

$$b_{ij} = b_{ji}.$$

2. *The diagonal entires $\{b_{ii}\}_i$ are even for all i.*

3. *For any $i = 1, \cdots, n$,*

$$\sum_{j=1}^n b_{ij} = p + 1.$$

By **Proposition 2.1** $B(p)$ determines a $(p+1)$-regular graph, which will be denoted by $G_N(p)$. Here is a remark. If $\frac{N-1}{12}$ is not an integer, then $w_i > 1$ for certain i. This implies that $B(p)$ is not symmetric and the assumption of **Proposition 2.1** is not satisfied.

§ 4.2. The construction of a Ramanujan graph

We will explain an outline of our construction of Ramanujan graphs. See [30] for details. Our results are based on the idea of Mestre and Oésterle ([23]) but we adopt a slightly different viewpoint.

Our idea is to relate $G_N(p)$ and the space of modular forms. Let N be a prime and $S_2(\Gamma_0(N))$ the space of cusp forms of weight 2 for the Hecke's congruence subgroup

$$\Gamma_0(N) := \{\begin{pmatrix} a\, b \\ c\, d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \quad c \equiv 0 \,(\mathrm{mod}\, N)\}.$$

Let $Y_0(N)$ be the modular curve which parametrizes isomorphism classes of a pair $\mathbf{E} = (E, \Gamma_N)$ of an elliptic curve E and a cyclic subgroup Γ_N of order N of E. It is a smooth curve defined over $\mathbb{Q}$, and the set of $\mathbb{C}$-valued points is the quotient of the upper half plane by $\Gamma_0(N)$. The compactification $X_0(N)$ of $Y_0(N)$ has the canonical model over $\mathbb{Z}$ which has been studied by [7] and [19] in detail. Then $S_2(\Gamma_0(N))$ is identified with the space of holomorphic 1-forms $H^0(X_0(N), \Omega)$, and in particular with the tangent space $\mathrm{Tan}J_0(N)$ at the origin of the Jacobian variety $J_0(N)$ of $X_0(N)$.

For a prime p different from N, $X_0(N)$ furnishes the p-th Hecke operator defined by

$$T_p(E, \Gamma_N) := \sum_C (E/C, (\Gamma_N + C)/C), \tag{4.4}$$

where C runs through all cyclic subgroups of E of order p. By functoriality, T_p acts on $J_0(N)$ and in turn on $\mathrm{Tan}J_0(N)$, and the action coincides with the usual action on $S_2(\Gamma_0(N))$ (see [28]) under identification. We define the Hecke algebra as $\mathbb{T} := \mathbb{Q}[\{T_p\}_{p \neq N}]$, which is a commutative subring of $\mathrm{End}J_0(N)$. Let $\mathcal{J}_0(N)$ be the Neron model of $J_0(N)$ over $\mathbb{Z}$. It is known that the connected components of the reduction of $\mathcal{J}_0(N)$ at N are tori. Following [26], we will describe its character group. $X_0(N)_{\mathbb{F}_N}$ has two irreducible components C_F and C_V, which are isomorphic to the projective line $\mathbb{P}^1 = X_0(1)$. Over C_F (resp. C_V), Γ_N is the kernel of the Frobenius F (resp. the Verschiebung V), and they intersect at supersingular points $\Sigma_N = \{E_1, \cdots, E_n\}$ as ordinary double points. Consider the homomorphism

$$\partial : \oplus_{E_i \in \Sigma_N} \mathbb{Z}E_i \to \mathbb{Z}C_F \oplus \mathbb{Z}C_V, \quad \partial(E_i) = C_F - C_V.$$

The image of ∂ is a free abelian group of rank one generated by $\delta := C_F - C_V$. X being the kernel of ∂, we have the exact sequence

$$0 \to X \to \oplus_{E_i \in \Sigma_N} \mathbb{Z} E_i \overset{\partial}{\to} \mathbb{Z}\delta \to 0. \tag{4.5}$$

It is straightforward to check that

$$X = \{ \sum_{E_i \in \Sigma_N} a_i \cdot E_i \,|\, a_i \in \mathbb{Z}, \sum_{i=1}^{n} a_i = 0 \},$$

and by [26]**Proposition 3.1**, X is the character group of the connected component of the reduction $\mathcal{J}_0(N)_{\mathbb{F}_N}$ at N. In particular we see that

$$\dim J_0(N) = \dim S_2(\Gamma_0(N)) = \dim X \otimes \mathbb{Q} = n - 1.$$

Let p be a prime with $p \neq N$. Then T_p operates on $\oplus_{E_i \in \Sigma_N} \mathbb{Z} E_i$ by (4.4). Note that $\Gamma_N = 0$, since E_i is supersingular and we may write (4.4) as

$$T_p(E_i) := \sum_{C} E_i / C. \tag{4.6}$$

A simple computation shows that

$$T_p(C_F) = (p+1)C_F, \quad T_p(C_V) = (p+1)C_V, \quad T_p(\delta) = (p+1)\delta. \tag{4.7}$$

and X is preserved by T_p. Remember that X is the character group of $\mathcal{J}_0(N)_{\mathbb{F}_N}$ and this action of T_p on X is nothing but the action which is induced by T_p on $\mathcal{J}_0(N)_{\mathbb{F}_N}$. Here is a relationship between T_p and the Brandt matrix. By [9]**Proposition 4.4**,

$$T_p E_i = \sum_{j=1}^{n} b_{ij} E_j, \tag{4.8}$$

hence $B(p)$ is the representation matrix of T_p. Using the multiplicity one theorem ([1]) we show the following result, which is the main point of our construction.

Proposition 4.2. *([30]* **Proposition 3.2***) $X \otimes \mathbb{C}$ and $S_2(\Gamma_0(N))$ are isomorphic as $\mathbb{T}$-modules.*

Hence **Proposition 4.2** together with (4.5), (4.7) and (4.8) implies that

$$\begin{aligned} \det[1 - B(p)t + pt^2] &= \det[1 - T_p t + pt^2 \,|\, X \otimes \mathbb{C}] \cdot \det[1 - T_p t + pt^2 \,|\, \mathbb{C}\delta] \\ &= \det[1 - T_p t + pt^2 \,|\, S_2(\Gamma_0(N))](1-t)(1-pt). \end{aligned}$$

Now use Eichler-Shimura relation ([6][27]) and we see that the characteristic polynomial of the geometric Frobenius Fr_p is computed by the Brandt matrix,

$$\det[1 - B(p)t + pt^2] = \det(1 - p_l(Fr_p)t \,|\, H^1_{et}(X_0(N)_{\overline{\mathbb{F}}_p}, \mathbb{Z}_l)(1-t)(1-pt). \tag{4.9}$$

By the Weil conjecture, (4.9) implies that $G_N(p)$ is a connected $(p+1)$-regular Ramanujan graph that is not bipartite. Now (1) of **Theorem 1.1** is an immediate consequence of **Proposition 2.4** and (4.9). Also (2) of **Theorem 1.1** can be shown without difficulty (see [30] **Theorem 3.1**).

§ 5. Numerical tables

1. Take $N = 37$. Then $n = 3$, and the dimension of $J_0(37)$ is two. Hence there are two cuspidal Hecke eigenform $f_{37,a}$ and $f_{37,b}$. Let p be a prime such that $p+1$ is a multiple of 3. **Theorem 1.2** says that, for such a prime p, $\mu_{37}(p)$ is a multiple of 3. Here are some calculations.

p	5	11	17	23	29	41	47
$a_p(f_{37,a})$	-2	-5	0	2	6	-9	-9
$a_p(f_{37,b})$	0	3	6	6	-6	-9	3
$\mu_{37}(p)$	0	-15	0	12	36	81	-27

2. Take $N = 61$. Then $n = 5$ and the dimension of $J_0(61)$ is 4. Hence there are four cuspidal Hecke eigenform f_{61a} and $\{f_{61b,(i)}\}_{i=1,2,3}$. Here $f_{61,a}$ is defined over $\mathbb{Q}$ and $\{f_{61b,(i)}\}_{i=1,2,3}$ are defined over K, where K is the decomposition field of $x^3 - x^2 - 3x + 1 = 0$. Let p be a prime such that $p+1$ is a multiple of 5. By **Theorem 1.2**, for such a prime p, $\mu_{61}(p)$ is a multiple of 5.

p	19	29	59	79	89
$a_p(f_{61a})$	4	-6	9	3	-4
$a_p(f_{61b,(i)})$	$3\gamma_i - 7$	$-\gamma_i^2 + 2\gamma_i + 3$	$-\gamma_i^2 - 3\gamma_i + 13$	$-4\gamma_i^2 - \gamma_i + 14$	$4\gamma_i^2 - 2\gamma_i - 10$
$\mu_{37}(p)$	80	120	2925	-1875	320

Here $\{\gamma_1, \gamma_2, \gamma_3\}$ are the distinct solutions of $x^3 - x^2 - 3x + 1 = 0$.

3. Take $N = 73$. Then $n = 6$ and the dimension of $J_0(73)$ is 5. Hence there are five cuspidal Hecke eigenform $f_{73,a}$, $f^{\pm}_{73,b}$ and $f^{\pm}_{73,c}$. Although $f_{73,a}$ is defined over $\mathbb{Q}$, $f^{\pm}_{73,b}$ and $f^{\pm}_{73,c}$ are defined over $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{13})$, respectively. Here ± denotes the conjugate over $\mathbb{Q}$. Let p be a prime such that $p+1$ is a multiple of 6. **Theorem 1.2** predicts that, for such a prime p, $\mu_{73}(p)$ is a multiple of 6.

p	5	11	17	23	29	41	47	53
$a_p(f_{73,a})$	2	-2	2	4	2	6	6	10
$a_p(f^{\pm}_{73,b})$	α	$-\alpha-3$	$-6\alpha-9$	$\alpha-6$	$-4\alpha-3$	$4\alpha+6$	-4$\alpha-9$	$8\alpha+15$
$a_p(f^{\pm}_{73,c})$	$-\beta$	$\beta+3$	$2\beta-3$	$\beta+6$	$-4\beta+3$	-6	9	$4\beta-3$
$\mu_{73}(p)$	-6	-18	810	8580	1122	720	396	36210

In the table α and β are the solutions of

$$\alpha^2 + 3\alpha + 1 = 0, \quad \beta^2 - \beta - 3 = 0.$$

References

[1] Atkin, A.-O.-L. and Lehner, J., Hecke operators on $\Gamma_0(m)$, *Math. Ann.*, **185** (1970),134–160.

[2] Bass, B., The Ihara-Selberg zeta functions of a tree lattice, *Intern. J. Math.*, **3** (1992), 717–797.

[3] Biggs, N., Algebraic Graph Theory, *Cambridge Tracts in Math.* **vol. 67**, Cambridge Univ. Press, 1974.

[4] Deligne, P., La conjecture de Weil : I, *Publ. de IHES,* **43**(1974), 273–307.

[5] Deligne, P., Cohomologie étale SGA4 1/2, *Lecture Notes in Mathematics* **569**, Springer, 1976.

[6] Deligne, P., Formes modulaires et représentation de l-adiques, *Sém. Bourbaki 355, Lecture Notes in Mathematics* **179**, Springer, 1971, 139–172.

[7] Deligne, P. and Rapoport, M., Les schémas de modules de courbes elliptiques, *Modular Functions of One Variable II, Lecture Notes in Mathematics* **349**, Springer, 1975, 143–316.

[8] Eichler, M., Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruernzzetafunktion, *Arch. Math.* **5** (1954), 355–366.

[9] Gross, B.-H., Heights and the special values of L-series, *C.M.S. Conf. Proc.* **7**(1987), 115–187.

[10] Grothendieck, A., SGA 7 I, Exposé IX *Lecture Notes in Math.* **288**(1972), 313–523, 1972.

[11] Hashimoto, K., On zeta and L-functions of finite graphs, *Intern. J. Math.* **1**(1990), 381–396.

[12] Hashimoto, K., Zeta functions of finite graphs and representations of p-adic groups, *Adv. Stud. in Pure Math.* **15**(1991), 211–280.

[13] Hoffman, J. -W., Remarks on the zeta function of a graph, *Proc. Fourth Inter. Conf. Dynam. Sys. and Diff. Eq.* (2003), 413–422.

[14] Ihara, Y., Discrete subgroups of PSL$(2, k_{\mathfrak{P}})$, *Proc. Sympos. in Pure Math. IX, Boulder, Colo.* (1965), 272–278.

[15] Ihara, Y., Algebraic curves mod $\mathfrak{P}$ and arithmetic groups, *Proc. Sympos. in Pure Math. IX, Boulder, Colo.* (1965), 265–271.

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

[17] Ihara, Y., Hecke Polynomials as congruence ζ functions in elliptic modular case, *Ann. of Math.* **85 (2)**(1967), 267–295.

[18] Ihara, Y., Shimura curves over finite fields and their rational points, *Contemp. Math.* **245**(1999), 15–23.

[19] Katz, N. and Mazur, B., Arithmetic Moduli of Elliptic Curves, *Ann. of Math. Stud.*, **108**, Princeton, 1995.

[20] Li, W., Character sums and abelian Ramanujan graphs, *J. Number Theory* **41**(1992), 199–217.

[21] Lubotzky, A., Phillips, P., Sarnak, P., Ramanujan graphs, *Combinatorics* **8(3)**(1988), 261–277.

[22] Margulis, G., Explicit group theoretic construction of combinatorial schemes an their application to the design of expanders and concentrators, *J. Prob.of Info. Trans.* (1988), 39–46.

[23] Mestre, J.-F., La méthode des graphes. Examples et applications, *Proc. Int. Conf. on class numbers and fund. units of algebraic number fields*, Katata, Japan, (1986), 217–242.

[24] Murty, M.-R., Ramanujan graphs, *J. Ramanujan Math. Soc.* **18** (2001), 1–20.

[25] Pizer, A.-K., Ramanujan graphs, Computational perspectives on number theory (Chicago, H. 1995), *AMS/IP Stud. Adv. Math.* **7**(1998), 159–178.

[26] Ribet, K.-A., On modular representations of Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Inventiones Math.*, **100**(1990), 421–476.

[27] Shimura, G., Construction of class fields and zeta functions of algebraic curves, *Annals of Math.*, **85**(1967), 58–159.

[28] Shimura, G., Introduction to the Arithmetic Theory of Automorphic Functions, *Publ. of Math. Soc. Japan*, **11**, Princeton, 1971,

[29] Stark, H.-M. and Terras, A., Zeta functions of finite graphs and coverings, *Adv. Math.*, **121**(1996), 124–165.

[30] Sugiyama, K., The zeta function of a Ramanujan graph, *to appear in Comm. Math. Univ. St. Pauli.*

[31] Terras, A., Fourier Analysis on Finite Groups and Applications, *London Math. Soc. Student Texts* **vol. 43**, Cambridge Univ. Press, 1999.

[32] Valette, A., Graphes de Ramanujan et applications, *Sém. Bourbaki 1996-97*, **n° 829**, Astérisque (1997), 247–276.

[33] Vignéras, M.-F., Arithmétique des algébre de quaternions, *Lecture Notes in Math.*, **800**, Springer, 1980.