

# JOURNAL

de Théorie des Nombres  
de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*


Nathanaël MUNIER et Ari SHNIDMAN

**Sandpile groups of supersingular isogeny graphs**

Tome 35, n° 3 (2023), p. 751-774.

<https://doi.org/10.5802/jtnb.1262>

© Les auteurs, 2023.

 Cet article est mis à disposition selon les termes de la licence  
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.  
<http://creativecommons.org/licenses/by-nd/4.0/fr/>



*Le Journal de Théorie des Nombres de Bordeaux est membre du  
Centre Mersenne pour l'édition scientifique ouverte*

<http://www.centre-mersenne.org/>

e-ISSN : 2118-8572

# Sandpile groups of supersingular isogeny graphs

par NATHANAËL MUNIER et ARI SHNIDMAN

RÉSUMÉ. Soient  $p$  et  $q$  deux nombres premiers distincts, et soit  $X_{p,q}$  le graphe  $(q+1)$ -régulier dont les nœuds sont les courbes elliptiques supersingulières sur  $\overline{\mathbb{F}}_p$  et dont les arêtes sont les  $q$ -isogénies. Pour une valeur de  $p$  fixée, la distribution des sous-groupes de  $\ell$ -Sylow du groupe jacobien de  $X_{p,q}$  est donnée pour  $q \rightarrow \infty$ . Nous constatons que cette distribution ne correspond pas à l’heuristique de Cohen–Lenstra dans ce contexte. La preuve que nous donnons utilise des représentations de Galois reliées à des courbes modulaires. Comme corollaire, nous donnons une borne supérieure sur la probabilité que le groupe jacobien soit cyclique, que nous conjecturons être optimale.

ABSTRACT. Let  $p$  and  $q$  be distinct primes, and let  $X_{p,q}$  be the  $(q+1)$ -regular graph whose nodes are supersingular elliptic curves over  $\overline{\mathbb{F}}_p$  and whose edges are  $q$ -isogenies. For fixed  $p$ , we compute the distribution of the  $\ell$ -Sylow subgroup of the sandpile group (i.e. Jacobian) of  $X_{p,q}$  as  $q \rightarrow \infty$ . We find that the distribution disagrees with the Cohen–Lenstra heuristic in this context. Our proof is via Galois representations attached to modular curves. As a corollary, we give an upper bound on the probability that the Jacobian is cyclic, which we conjecture to be sharp.

## 1. Introduction

Attached to any finite undirected graph  $X$  is a finite abelian group  $J(X)$ , called the Jacobian or sandpile group of  $X$ .<sup>1</sup> One may think of  $J(X)$  as the class group of the graph, in analogy with the divisor class group of an algebraic curve or the ideal class group of a number field.

For any prime number  $\ell$ , let  $J(X)[\ell^\infty]$  denote the subgroup of elements killed by some power of  $\ell$ . As with the Cohen–Lenstra heuristics for ideal class groups [3], we can ask about the distribution of the finite abelian  $\ell$ -group  $J(X)[\ell^\infty]$ , as  $X$  varies over a countable family of graphs.<sup>2</sup> Recently, Wood [17] has verified a Cohen–Lenstra-type heuristic for Erdős–Rényi

---

Manuscrit reçu le 21 mai 2022, accepté le 21 janvier 2023.

2020 *Mathematics Subject Classification*. 05C48, 11R29.

*Mots-clefs*. Graphs, Jacobians, isogenies, modular curves.

The second author was supported by the Israel Science Foundation (grant No. 2301/20).

<sup>1</sup>Other names for it are the critical group and the divisor class group. See Section 2 for the definition.

<sup>2</sup>For the families we consider, the size of  $J(X)$  grows, so we cannot make sense of the analogous question for the entire group  $J(X)$ .

random graphs, and Mészáros proved analogous results for random regular graphs [9].

In this paper, we compute these distributions for certain families of Ramanujan graphs, namely supersingular isogeny graphs. To define these graphs, let  $p$  and  $q$  be distinct prime numbers, and assume  $p \equiv 1 \pmod{12}$ , for simplicity. Let  $X_p$  be the set of isomorphism classes of supersingular elliptic curves  $E$  over  $\overline{\mathbb{F}}_p$ , a set of size  $n := (p - 1)/12$ . See [16, §5.4] for background on supersingular elliptic curves. Each  $E \in X_p$  contains  $q + 1$  distinct subgroups of order  $q$ , and hence admits  $q + 1$  degree  $q$  isogenies  $\phi : E \rightarrow E'$ , up to isomorphism. Moreover, each  $q$ -isogeny  $E \rightarrow E'$  admits a dual  $q$ -isogeny  $E' \rightarrow E$  in the opposite direction. Let  $X_{p,q}$  denote the undirected  $(q + 1)$ -regular graph whose vertex set is  $X_p$  and whose edges correspond to  $q$ -isogenies. Set  $J_{p,q} := J(X_{p,q})$ .

Our main results determine the distribution of the finite abelian groups  $J_{p,q}[\ell^\infty]$ , when  $p$  and  $\ell$  are fixed and  $q \rightarrow \infty$ . Thus, the number of vertices is fixed, while the degree of the graph goes to infinity. Our proof makes use of the link between the graphs  $X_{p,q}$  and the Galois representation attached to the modular curve  $X_0(p)$ , as we shall explain. It would also be interesting to consider families where  $q$  is fixed and  $p \rightarrow \infty$ , but this would require different methods.

**1.1. Results.** When  $p$  is fixed, the groups  $J_{p,q}$  carry an extra structure which heavily influences their distribution. Namely, they are each modules for a certain ring  $\mathbb{T}$ , called the Hecke algebra. To define  $\mathbb{T}$ , let  $L_q$  be the Laplacian of  $X_{p,q}$ , viewed as a linear operator on the space of functions  $\text{Hom}(X_p, \mathbb{Z})$ . Note that as  $q$  varies, the operators  $L_q$  act on the same space of functions. Crucially, they commute with each other. Define the submodule of degree-zero functions

$$M = \left\{ f \in \text{Hom}(X_p, \mathbb{Z}) : \sum_{E \in X_p} f(E) = 0 \right\},$$

on which  $L_q$  acts as well. Then  $\mathbb{T}$  is the commutative subring of  $\text{End}_{\mathbb{Z}}(M)$  generated by the endomorphisms  $L_q$ . It is known to be semisimple and of rank  $n - 1 = \text{rk}_{\mathbb{Z}} M$  as a  $\mathbb{Z}$ -module, which means that  $M$  is rank 1 (not necessarily free) as a  $\mathbb{T}$ -module. The Jacobian  $J_{p,q}$  is then a module for the Hecke algebra  $\mathbb{T}$ . In fact,  $J_{p,q}$  is essentially the cokernel  $M/L_q M$ . More precisely, for  $\ell \nmid n$ , we have

$$(1.1) \quad J_{p,q}[\ell^\infty] \simeq M_\ell / L_q M_\ell,$$

where  $M_\ell = M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$  (see Proposition 3.3). Given this, one might naively guess that the groups  $J_{p,q}[\ell^\infty]$  should be distributed as a random  $\mathbb{T}$ -module of the form  $\mathbb{T}_\ell / a \mathbb{T}_\ell$ , where  $\mathbb{T}_\ell = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$  and  $a \in \mathbb{T}_\ell$  is sampled according to

Haar measure. However, this turns out to be incorrect, because it ignores the particular form of the elements  $L_q$ .

By definition  $L_q = q + 1 - T_q$ , where  $T_q \in \mathbb{T}$  is the image of the adjacency matrix of  $X_{p,q}$ , thought of as an element of  $\text{End}_{\mathbb{Z}} \text{Hom}(X_p, \mathbb{Z})$ . Thus  $L_q$  is (formally) the determinant of  $x - 1$  acting on the free rank two  $\mathbb{T}$ -module  $\mathbb{T}[x]/(x^2 - T_q x + q)$ . This rank two module arises naturally in the context of Hashimoto's edge-adjacency operator, whose characteristic polynomial computes the zeta function of the graph. This suggests a different model for the groups  $J_{p,q}[\ell^\infty]$ , namely as random cokernels  $\mathbb{T}_\ell / \det(g - 1)\mathbb{T}_\ell$ , where  $g$  is sampled from the group

$$\mathbb{G}_\ell := \{g \in \text{GL}_2(\mathbb{T}_\ell) : \det(g) \in \mathbb{Z}_\ell^\times\},$$

endowed with its  $\ell$ -adic topology and its probability Haar measure.

Our first result states that for all but finitely many primes  $\ell$ , this is indeed the correct distribution. For an arbitrary  $\mathbb{T}$ -module  $G$ , define

$$\mathbb{P}(J_{p,q}[\ell^\infty] \simeq G) := \lim_{X \rightarrow \infty} \frac{\#\{q < X : J_{p,q}[\ell^\infty] \simeq G\}}{\#\{q < X\}},$$

which is the probability that  $J_{p,q}[\ell^\infty]$  is isomorphic to  $G$  as  $\mathbb{T}$ -modules (or  $\mathbb{T}_\ell$ -modules). Let  $\text{Disc}(\mathbb{T}) \in \mathbb{Z}$  be the discriminant of the ring  $\mathbb{T}$ .

**Theorem 1.1.** *Fix a prime  $\ell$  not dividing  $6n \text{Disc}(\mathbb{T})$ , and let  $G$  be a finite  $\mathbb{T}_\ell$ -module. Let  $\mu$  be the Haar probability measure on the group  $\mathbb{G}_\ell$ . Then*

$$\mathbb{P}(J_{p,q}[\ell^\infty] \simeq G) = \mu(g \in \mathbb{G}_\ell : \mathbb{T}_\ell / \det(g - 1)\mathbb{T}_\ell \simeq G).$$

Before discussing the proof of Theorem 1.1, we address the natural follow-up question: what is the distribution in Theorem 1.1, in concrete terms? The first thing to observe is that the distribution behaves differently depending on the  $\ell$ -adic valuation of  $q - 1$ . Indeed, the cokernel  $\mathbb{T}_\ell / \det(g - 1)\mathbb{T}_\ell$  measures the  $\ell$ -adic distance from 1 to the two eigenvalues of  $g$ . If  $\det g$  (which we imagine is  $q$ ) is itself  $\ell$ -adically close to 1, then both of the eigenvalues can be close to 1, whereas if  $\det g$  is not close to 1, then at most one eigenvalue can be close to 1.

With this phenomenon in mind, we only give an explicit formula for the distribution as  $q$  varies through primes  $q \not\equiv 1 \pmod{\ell}$ ; the case of  $q \equiv 1 \pmod{\ell}$  is more complicated. We may write  $\mathbb{T}_\ell \simeq \bigoplus_{i=1}^t \mathcal{O}_i$ , where each  $\mathcal{O}_i$  is a finite free ring extension of  $\mathbb{Z}_\ell$  of degree  $d_i$ . Since  $\ell$  does not divide the discriminant of  $\mathbb{T}$ , each  $\mathcal{O}_i$  is a discrete valuation ring with maximal ideal  $\ell\mathcal{O}_i$  and residue field  $\mathcal{O}_i/\ell\mathcal{O}_i$  of size  $\ell^{d_i}$ . The following result computes the probability  $\mathbb{P}(J_{p,q}[\ell^\infty] \simeq G)$  in Theorem 1.1, in terms of the integers  $d_1, \dots, d_t$ . Since  $M_\ell$  is a rank one  $\mathbb{T}_\ell$ -module, this probability is 0 unless  $G$  is isomorphic to  $G_{\mathbf{k}} := \bigoplus_{i=1}^t \mathcal{O}_i / \ell^{k_i} \mathcal{O}_i$ , for some tuple  $\mathbf{k} = (k_i) \in \mathbb{Z}_{\geq 0}^t$ .

**Theorem 1.2.** *Assume  $\ell$  does not divide  $6n \operatorname{Disc}(\mathbb{T})$ . Let  $\delta_{ij}$  be Kronecker’s delta function. As  $q \rightarrow \infty$  varying through primes  $q \not\equiv 1 \pmod{\ell}$ , we have*

$$\mathbb{P}(J_{p,q}[\ell^\infty] \simeq G_{\mathbf{k}}) = \frac{1}{\#G_{\mathbf{k}}} \prod_{i=1}^t \left(1 - \frac{1}{\ell^{d_i} - 1}\right)^{\delta_{0k_i}}.$$

Note that  $G_{\mathbf{k}} \simeq \bigoplus_{i=1}^t (\mathbb{Z}/\ell^{k_i}\mathbb{Z})^{d_i}$ , as abstract abelian groups. Thus, one can easily determine from Theorem 1.2 the explicit distribution of the abstract abelian groups  $J_{p,q}[\ell^\infty]$ . To compute  $\mathbb{T}_\ell$  (which amounts to computing the integers  $d_i$ ), one can use Sage or Magma. See Section 6 for some worked out examples.

It is interesting to compare the distribution in Theorem 1.2 with a naive Cohen–Lenstra-type heuristic. As explained in [2], because the Jacobian of a graph  $X$  is naturally endowed with a perfect symmetric bilinear form, the Cohen–Lenstra heuristic in the setting of sandpile groups predicts that for each finite abelian group  $G$ ,

$$\mathbb{P}(J(X) \simeq G) \propto \frac{\#\{\text{perfect symmetric bilinear } G \times G \rightarrow \mathbb{C}^\times\}}{\#G \# \operatorname{Aut}(G)}.$$

This is what Wood proves in the context of Erdős–Rényi random graphs. In our case,  $J_{p,q}$  is a rank one  $\mathbb{T}$ -module, and the number of perfect  $\mathbb{T}$ -linear pairings of a rank one  $\mathbb{T}$ -module is equal to the size of its automorphism group. Thus the naive Cohen–Lenstra heuristic would predict

$$\mathbb{P}(J_{p,q} \simeq G_{\mathbf{k}}) \propto \frac{1}{\#G_{\mathbf{k}}},$$

which also agrees with the naive guess that  $J(X_{p,q})[\ell^\infty]$  is modeled by the groups  $\mathbb{T}_\ell/a\mathbb{T}_\ell$  for  $a \in \mathbb{T}_\ell$ . This is nearly what we find in Theorem 1.2, except there is an extra factor of  $1 - \frac{1}{\ell^{d_i} - 1}$  for each trivial component of  $G_{\mathbf{k}}$  (i.e. for each  $i$  such that  $k_i = 0$ ). We see that for Jacobians of supersingular isogeny graphs, there is a slight and unexpected bias towards  $\mathbb{T}$ -modules with non-trivial components.

For any fixed  $t \geq 0$ , one can give explicit formulas for the distribution of the groups  $J_{p,q}$  as  $q \rightarrow \infty$  varies through primes such that  $v_\ell(q - 1) = k$ , but these formulas seem quite complicated for  $k > 0$ . This is somewhat analogous to the complications that arise in the Cohen–Lenstra–Martinet heuristics when the ground field contains  $\ell$ -th roots of unity [6].

One statistical quantity which we found accessible without any restriction on  $q$ , is the probability that  $J_{p,q}[\ell^\infty]$  is cyclic.

**Theorem 1.3.** *Let  $\ell$  be a prime not dividing  $6n \operatorname{Disc}(\mathbb{T})$ . Recall  $\mathbb{T}_\ell \simeq \bigoplus_{i=1}^t \mathcal{O}_i$ , with each  $\mathcal{O}_i$  unramified over  $\mathbb{Z}_\ell$  of degree  $d_i$ . Let  $t_1$  be the number of factors with  $d_i = 1$ . Then the probability that  $J_{p,q}[\ell^\infty]$  is a cyclic abelian*

group is

$$\frac{\ell - 2 + t_1}{\ell - 1} \prod_{i=1}^t \left(1 - \frac{1}{\ell^{d_i} - 1}\right) + \left(\frac{\ell^2 + (t_1 - 1)\ell - 1}{\ell^3 - 2\ell^2 + 1}\right) \prod_{i=1}^t \left(1 - \frac{\ell^{d_i}}{\ell^{2d_i} - 1}\right).$$

As a function of  $\ell$ , this expression is  $1 - O(\ell^{-2})$ , with implied constant depending only on  $p$ .

We can prove similar results for the subgroup  $J_{p,q}[L^\infty]$ , where  $L$  is any squarefree integer coprime to  $6n \text{Disc}(\mathbb{T})$ . We find that the  $\ell$ -Sylow subgroups are independent of each other, as one might expect (see Theorem 5.13). Taking  $L \rightarrow \infty$ , we deduce the following upper bound on the proportion of primes  $p$  for which  $J_{p,q}$  is cyclic.

**Theorem 1.4.** *Let  $S = \prod_{\ell|6n \text{Disc}(\mathbb{T})} \ell$  and let  $J_{p,q}[1/S]$  be the prime-to- $S$  part of  $J_{p,q}$ . Then as  $q \rightarrow \infty$ , the probability that  $J_{p,q}[1/S]$  is cyclic is at most  $\prod_{\ell \notin S} E(\ell) > 0$ , where the Euler factor  $E(\ell)$  equals*

$$\frac{\ell - 2 + t_1(\ell)}{\ell - 1} \prod_{i=1}^{t(\ell)} \left(1 - \frac{1}{\ell^{d_i} - 1}\right) + \left(\frac{\ell^2 + (t_1(\ell) - 1)\ell - 1}{\ell^3 - 2\ell^2 + 1}\right) \prod_{i=1}^{t(\ell)} \left(1 - \frac{\ell^{d_i}}{\ell^{2d_i} - 1}\right),$$

$t(\ell)$  is the number of factors in  $\mathbb{T}_\ell$ , and where  $t_1(\ell)$  is the number of degree one factors of  $\mathbb{T}_\ell$ . In particular, the Euler product  $\prod_{\ell \notin S} E(\ell)$  is also an upper bound for the probability that  $J_{p,q}$  is cyclic.

We conjecture that this upper bound is also the correct lower bound, which would imply that a positive proportion of the groups  $J_{p,q}[1/S]$  are cyclic.

**1.2. Proofs.** The first step in the proof of Theorem 1.1 is to identify a rank two  $\mathbb{T}_\ell$ -module  $V_\ell$ , which does not depend on  $q$ , and operators  $g_q \in \text{End}_{\mathbb{T}_\ell}(V_\ell)$  such that  $J_{p,q}[\ell^\infty] \simeq \mathbb{T}_\ell / \det(g_q - 1)\mathbb{T}_\ell$ .

To find  $V_\ell$ , we use the deep connection between supersingular isogeny graphs and Galois representations that are familiar in number theory. Indeed, the algebra  $\mathbb{T}$  is also known to act by correspondences on the modular curve  $X_0(p)$ ; see e.g. [5]. Moreover, there is a  $(\mathbb{T} \otimes \mathbb{Q})$ -linear isomorphism between  $M \otimes \mathbb{Q}$  and the space  $S_2(\Gamma_0(p), \mathbb{Q})$  of weight two cusp forms of level  $\Gamma_0(p)$ , which may be viewed as the space of regular differentials on  $X_0(p)$ . This is proved either by using the Jacquet–Langlands correspondence or via theta series as in [5]. Let  $J_0(p)$  be the Jacobian of  $X_0(p)$ , an abelian variety of dimension  $n - 1$ . Then the Tate module

$$V_\ell = \varprojlim J_0(p)[\ell^k]$$

is free of rank two over  $\mathbb{T}_\ell$  and admits an action  $\rho_\ell : G_{\mathbb{Q}} \rightarrow \text{Aut}_{\mathbb{T}_\ell}(V_\ell)$  by the absolute Galois group  $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . In conjunction with (1.1) and

the  $\mathbb{T}$ -module isomorphism  $M \otimes \mathbb{Q} \simeq S_2(\Gamma_0(p), \mathbb{Q})$ , the Eichler–Shimura relation [15] implies that for  $\ell \nmid pN$ , we have

$$(1.2) \quad J_{p,q}[\ell^\infty] \simeq \mathbb{T}_\ell / \det(\rho_\ell(\text{Frob}_q) - 1)\mathbb{T}_\ell,$$

where  $\text{Frob}_q$  is a choice of Frobenius automorphism at  $p$  (see Proposition 3.6). Thus  $V_\ell$  is the sought after  $\mathbb{T}_\ell$ -module. The elements  $\rho_\ell(\text{Frob}_q)$  lie in  $\mathbb{G}_\ell$  because the determinant of  $\rho_\ell$  is the cyclotomic character, and hence  $\det(\rho_\ell(\text{Frob}_q)) = q$ . As an aside, it was observed in [7, §4.3] that for  $\ell \nmid n$ , we have

$$\#J_{p,q}[\ell^\infty] = \#J_0(p)(\mathbb{F}_q)[\ell^\infty],$$

which is a weaker version of (1.2). In fact, one deduces from (1.2) that the groups  $J_{p,q}[\ell^\infty]$  and  $J_0(p)(\mathbb{F}_p)[\ell^\infty]$  are *not* isomorphic in general, despite having the same cardinality.

To prove that the Frobenius cokernels  $\mu$ -equidistribute, we need two more ingredients. The first is the fact that  $\rho_\ell$  maps  $G_\mathbb{Q}$  surjectively onto  $\mathbb{G}_\ell$ . General results for Galois representation attached to modular curves imply that this surjectivity holds for all but finitely many  $\ell$ . To get precise control of the allowed values of  $\ell$ , we use Ribet’s strong result in the case where the level  $p$  is prime [12], which proves surjectivity for all  $\ell \nmid n \text{ Disc}(\mathbb{T})$ . The second ingredient in our proof is Chebotarev’s density theorem.

The proofs of Theorems 1.2–1.4 amount to some rather elaborate  $\ell$ -adic computations which seem to magically simplify at the end. The core of the computation involves determining the number matrices in  $\text{GL}_2(\mathcal{O}/\ell^i)$  having eigenvalue 1, which we expect will have other applications. It would be interesting to compute the full distribution including primes  $q \equiv 1 \pmod{\ell}$ , but our approach gives unruly intermediate formulas in that case.

**1.3. Remarks and further directions.** For  $\ell \mid n \text{ Disc}(\mathbb{T})$ , the distribution of the groups  $J_{p,q}[\ell^\infty]$  may very well differ from those in Theorems 1.1 and 1.2. For example, if there is a mod  $\ell$  congruence between two newforms of level  $p$ , then  $\ell$  will divide  $\text{Disc}(\mathbb{T})$  and the distribution will not agree with Theorem 1.2. In that case, the distribution could conceivably agree with the abstract distribution in Theorem 1.1, but Ribet’s results no longer apply, so we are not sure.

It is natural to wonder about the distribution of the groups  $J_{p,q}[\ell^\infty]$  with  $q$  fixed and  $p \rightarrow \infty$ . The authors are not sure what the distribution should be in this case. What is needed is an  $\ell$ -adic version of the results of Serre [14] and Conrey–Duke–Farmer [4], but controlling the  $\ell$ -adic norms of the terms in the trace formula seems difficult.

If  $C/\mathbb{Q}_p$  is a semistable curve, then the Jacobian of the component graph of a minimal regular model of  $C$  over  $\mathbb{Z}_p$  is isomorphic to the component group of the special fiber of the Néron model of its Jacobian variety. Let  $X^{pq}/\mathbb{Q}_q$  be the quaternionic Shimura curve over  $\mathbb{Q}_q$  parameterizing abelian

surfaces admitting a subring of endomorphisms isomorphic to the quaternion order of discriminant  $pq$ . Ribet has shown that the component graph  $\mathcal{X}^{p,q}$  of  $X^{pq}/\mathbb{Q}_q$  is a double cover of the graph  $X_{p,q}$ ; see [11, 4.4] and [1, §4]. It follows that  $J_{p,q}$  is a quotient of  $J(\mathcal{X}^{p,q})$ , and hence our results shed light on the group structure of these component groups. It would be interesting to determine the exact structure of the groups  $J(\mathcal{X}^{p,q})$  via a closer study of this double cover.

### 2. Jacobians of graphs

Let  $X$  be a finite undirected graph with vertex set  $V(X)$  and edge set  $E(X)$ . Self-loops and multi-edges are allowed. The Jacobian of  $X$  is defined in terms of the group of divisors on  $G$

$$\text{Div}(X) = \left\{ \sum_{v \in V(X)} a_v v : a_v \in \mathbb{Z} \right\},$$

which is the free abelian group on the set  $V(X)$ . We may of course identify  $\text{Div}(X)$  with the group  $\text{Hom}(V(X), \mathbb{Z})$  from the introduction.

The *degree* of a divisor  $\sum a_v v$  is the integer  $\sum a_v$ . We write  $\text{Div}^0(X) \subset \text{Div}(X)$  for the subgroup of degree 0 divisors. Each function  $f : V(X) \rightarrow \mathbb{Z}$  determines a *principal divisor*

$$\text{div}(f) = \sum_v \sum_{e=vw \in E(X)} (f(v) - f(w))v.$$

Two divisors  $D, D' \in \text{Div}(X)$  are *linearly equivalent* if their difference is principal, or, in other words, if  $D - D' = \text{div}(f)$  for some function  $f$ . Principal divisors have degree 0, so equivalent divisors have the same degree.

**Definition 2.1.** The *Jacobian*  $J(X)$  is the group of linear equivalence classes in  $\text{Div}^0(X)$ , i.e. the quotient of  $\text{Div}^0(X)$  by the subgroup of principal divisors.

**Remark 2.2.** The group of all functions  $f : V(X) \rightarrow \mathbb{Z}$  is generated by the indicator functions  $\delta_v(w) = \delta_{vw}$ , for each  $v \in V(X)$ . The linear equivalence relation is therefore generated by the relations  $\sum_{e=vw} (v-w)$ , one for each  $v$ .

### 3. Jacobians of supersingular isogeny graphs

Recall that  $p \equiv 1 \pmod{12}$  is a prime and  $X_p$  is the set of supersingular elliptic curves over  $\overline{\mathbb{F}}_p$ . Let  $q$  be any prime different from  $p$ , and let  $X = X_{p,q}$  be the supersingular  $q$ -isogeny graph with vertex set  $X_p$ . Then  $G$  is a  $(q+1)$ -regular graph on  $n := (p-1)/12$  vertices.

The  $\mathbb{Z}$ -module  $\text{Div}(X)$  is free of rank  $n$ , with basis given by the  $n$  supersingular elliptic curves  $E \in X_p$ . The Hecke operator  $T_q : \text{Div}(X) \rightarrow \text{Div}(X)$  sends  $E$  to  $\sum_{E' \sim E} E'$ , where the sum is over every edge  $E' \sim E$  in  $X_{p,q}$ .



**Example 3.1.** When  $p = 37$ , there are three supersingular elliptic curves, with  $j$ -invariants 8 and the roots  $\alpha$  and  $\bar{\alpha}$  of  $x^2 - 6x - 6 \in \mathbb{F}_{37}[x]$ . For  $q = 2$ , we compute in Sage that

- $T_2 E_8 = E_8 + E_\alpha + E_{\bar{\alpha}}$ ,
- $T_2 E_\alpha = E_8 + 0E_\alpha + 2E_{\bar{\alpha}}$ , and
- $T_2 E_{\bar{\alpha}} = E_8 + 2E_\alpha + 0E_{\bar{\alpha}}$ .

The Hecke operator  $T_2$  is degree 3, since the graph  $X_{37,2}$  is 3-regular.

In general,  $T_q$  sends divisors of degree  $n$  to divisors of degree  $(q + 1)n$ . In particular, it preserves the subgroup  $\text{Div}^0(X)$ . The latter sits in an exact sequence

$$(3.1) \quad 0 \rightarrow \text{Div}^0(X) \longrightarrow \text{Div}(X) \xrightarrow{\text{deg}} \mathbb{Z} \rightarrow 0,$$

of abelian groups. For varying primes  $q$ , the operators  $T_q \in \text{End}_{\mathbb{Z}} \text{Div}(X)$  commute with each other. They therefore generate a commutative algebra  $\tilde{\mathbb{T}}$ , called the Hecke algebra, which is semisimple and free of rank  $n$  as a  $\mathbb{Z}$ -module [5]. Then (3.1) is an exact sequence of  $\tilde{\mathbb{T}}$ -modules, with  $T_q$  acting on  $\mathbb{Z}$  by multiplication by  $q + 1$ . Let  $\mathbb{T}$  be the subalgebra of  $\text{End}_{\mathbb{Z}} \text{Div}^0(X)$  generated by the action of the  $T_q$ . Then  $\mathbb{T}$  is a quotient of  $\tilde{\mathbb{T}}$  and has rank  $n - 1$ .

**Lemma 3.2.** *There is an isomorphism of  $\mathbb{T}$ -modules  $J_{p,q} \simeq \text{Div}^0(X)/(q + 1 - T_q) \text{Div}(X)$ .*

*Proof.* From the definitions, the subgroup of principal divisors is precisely  $(q + 1 - T_q) \text{Div}(X)$ . □

The degree map  $\text{Div}(X) \rightarrow \mathbb{Z}$  does not quite admit a  $\tilde{\mathbb{T}}$ -module section, but there is a map  $\mathbb{Z} \rightarrow \text{Div}(X)$  sending 1 to  $\Delta := \sum_{E \in X_p} E$ . The subgroup  $\text{Div}^0(X) \oplus \mathbb{Z}\Delta$  has index  $n$  inside  $\text{Div}(X)$ , with cokernel isomorphic to  $\mathbb{Z}/n\mathbb{Z}$ .

**Proposition 3.3.** *We have  $\#J_{p,q} = \frac{1}{n} \det(q + 1 - T_q | \text{Div}^0(X))$ . More precisely, there is an isomorphism of  $\mathbb{T}$ -modules*

$$J_{p,q} \simeq \text{coker}(q + 1 - T_q | \text{Div}^0(X)) / \langle (q + 1 - T_q)(E) \rangle,$$

for any choice of  $E \in X_p$ .

*Proof.* This follows from applying the snake lemma to the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Div}^0(X) \oplus \mathbb{Z}\Delta & \longrightarrow & \text{Div}(X) & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Div}^0(X) & \longrightarrow & \text{Div}^0(X) & \longrightarrow & 0 \longrightarrow 0 \end{array}$$

whose vertical maps are  $q + 1 - T_q$ . □

Since  $\mathbb{T}$  and  $\text{Div}^0(X)$  are free of rank  $n - 1$  as  $\mathbb{Z}$ -modules, the group  $\text{Div}^0(X)$  is a torsion-free rank one  $\mathbb{T}$ -module, though not necessarily free. For any prime  $\ell$ , let  $\mathbb{T}_\ell = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$  and  $\text{Div}^0(X)_\ell = \text{Div}^0(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ . The  $\mathbb{Q}_\ell$ -algebra  $\mathbb{T}_\ell \otimes \mathbb{Q} = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$  is a finite product  $\bigoplus_{i=1}^t K_i$  of finite field extensions of  $\mathbb{Q}_\ell$ . Assume from now on that  $\ell$  does not divide the discriminant of  $\mathbb{T}$ . Then each  $K_i$  is unramified of degree  $d_i \geq 1$  over  $\mathbb{Q}_\ell$ , and

$$\mathbb{T}_\ell \simeq \bigoplus_{i=1}^t \mathcal{O}_i,$$

where  $\mathcal{O}_i$  is the integral closure of  $\mathbb{Z}_\ell$  in  $K_i$ .

**Proposition 3.4.** *If  $\ell$  does not divide  $n \text{Disc}(\mathbb{T})$ , then*

$$J_{p,q}[\ell^\infty] \simeq \bigoplus_{i=1}^t \mathcal{O}_i / (q + 1 - T_q) \mathcal{O}_i,$$

where we view  $T_q$  in  $\mathcal{O}_i$  via the projection  $\mathbb{T}_\ell \rightarrow \mathcal{O}_i$ .

*Proof.* Since  $\mathbb{T}_\ell$  is a product of discrete valuation rings, any rank one torsion-free module is free. After identifying  $\text{Div}^0(X)_\ell$  with  $\mathbb{T}_\ell$ , the action of  $T_q$  is by left-multiplication. Since  $T_q$  acts  $\mathbb{T}_\ell$ -linearly, it sends  $\mathcal{O}_i$  to  $\mathcal{O}_i$  and the result follows from Proposition 3.3 (since we also assume  $\ell \nmid n$ ).  $\square$

As explained in the introduction, we can realize the group  $J_{p,q}[\ell^\infty]$  as  $\mathbb{T}_\ell / \det(g_q - 1) \mathbb{T}_\ell$  for some  $\mathbb{T}_\ell$ -linear map  $g_q$  on a rank two  $\mathbb{T}_\ell$ -module  $V_{\ell,q}$ . However, the module we constructed was somewhat contrived, and in particular, depended on  $q$ . To prove Theorem 1.1 we will find a *single* rank two  $\mathbb{T}_\ell$ -model  $V_\ell$  and an operator  $g_q$  on it (for each prime  $q$ ) with the same properties.

We must first recall the connection to modular forms. It is known that the algebra  $\mathbb{T}$  is isomorphic to the Hecke algebra acting on the space of weight two cusp forms  $S_2(\Gamma_0(p), \mathbb{Z})$  with integer coefficients [5, Thm. 3.1]. It follows that there is a bijection between the maximal ideals  $\lambda_i$  of  $\mathbb{T}_\ell$  and pairs  $(f, \lambda)$ , where  $f = \sum a_n(f)q^n$  runs through a set of representatives for the  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -orbits of newforms in  $S_2(\Gamma_0(p), \overline{\mathbb{Q}})$ , and  $\lambda$  runs through the prime ideals in  $\mathcal{O}_f$  above  $\ell$ , where  $\mathcal{O}_f$  is the ring of integers of the number field generated by the coefficients  $a_n(f)$ . Since we assume  $\ell \nmid \text{Disc}(\mathbb{T})$ , the ring  $\mathcal{O}_i$  is isomorphic to the completion  $\mathcal{O}_{f,\lambda}$  of  $\mathcal{O}_f$  at  $\lambda$ . Thus

$$\mathbb{T}_\ell \simeq \bigoplus_{(f,\lambda)} \mathcal{O}_{f,\lambda},$$

where the sum is understood to be over the pairs  $(f, \lambda)$  as before.

The following description of  $J_{p,q}[\ell^\infty]$  in terms of modular forms gives a convenient way to compute this group using any software which computes newforms and their Fourier coefficients.

**Proposition 3.5.** *If  $\ell$  does not divide  $n \operatorname{Disc}(\mathbb{T})$ , then*

$$J_{p,q}[\ell^\infty] \simeq \bigoplus_{(f,\lambda)} \mathcal{O}_{f,\lambda}/(q+1-a_q(f))\mathcal{O}_{f,\lambda},$$

where we view  $a_q(f)$  in  $\mathcal{O}_{f,\lambda}$  via the projection  $\mathbb{T}_\ell \rightarrow \mathcal{O}_{f,\lambda}$ .

*Proof.* We use the fact that  $\operatorname{Div}^0(X)_\ell$  is isomorphic as  $\mathbb{T}_\ell$ -module to  $S_2(\Gamma_0, \mathbb{Z}_\ell)$  [5]. In fact, they are both free of rank 1, under the assumptions on  $\ell$ . Multiplication by  $T_q$  on  $\mathcal{O}_{f,\lambda}$  is given by multiplication by  $a_p(f_i)$ , since  $f$  is a newform, and so the same must be true for the action of  $T_q$  on  $\mathcal{O}_i$ . Thus, the result follows from Proposition 3.4.  $\square$

Let  $X_0(p)$  be the modular curve parameterizing elliptic curves with a cyclic subgroup of order  $p$ . This is a smooth projective algebraic curve over  $\mathbb{Q}$ . Let  $J_0(p)$  be its Jacobian, an abelian variety over  $\mathbb{Q}$  of dimension equal to the genus of  $X_0(p)$ , which is  $g = n - 1$ . For each  $k$ , let  $J_0(p)[\ell^k]$  denote the group of  $\ell^k$ -torsion points in  $J_0(p)$ , which is a finite  $G_{\mathbb{Q}}$ -module, isomorphic as a group to  $(\mathbb{Z}/\ell^k\mathbb{Z})^{2g}$ . These  $G_{\mathbb{Q}}$ -modules form an inverse system under the multiplication-by- $\ell$  maps. Let  $V_\ell = \varprojlim_k J_0(p)[\ell^k]$  be the inverse limit.<sup>3</sup> Then  $V_\ell$  is free of rank  $2g$  over  $\mathbb{Z}_\ell$  and carries a  $\mathbb{Z}_\ell$ -linear action of  $G_{\mathbb{Q}}$ .

The Tate module  $V_\ell$  has even more structure. The Hecke algebra  $\mathbb{T}$  acts by correspondences on the curve  $X_0(p)$ , and hence acts by endomorphisms on  $J_0(p)$ . It is known that  $\mathbb{T} = \operatorname{End}(J_0(p))$ , since  $p$  is prime [8], but we will only use the containment  $\mathbb{T} \subset \operatorname{End}(J_0(p))$ . It follows that  $V_\ell$  is a rank two  $\mathbb{T}_\ell$ -module. If  $\ell \nmid \operatorname{Disc}(\mathbb{T})$  or if  $\ell > 2$ , then Mazur showed that  $V_\ell$  is moreover a free  $\mathbb{T}_\ell$ -module [8, II.15-17]. Thus, the  $G_{\mathbb{Q}}$ -action can be thought of as a representation

$$\rho_\ell : G_{\mathbb{Q}} \longrightarrow \operatorname{Aut}_{\mathbb{T}_\ell}(V_\ell)$$

or

$$\rho_\ell : G_{\mathbb{Q}} \longrightarrow \operatorname{GL}_2(\mathbb{T}_\ell),$$

if either  $\ell \nmid \operatorname{Disc}(\mathbb{T})$  or  $\ell > 2$ . The Galois representation  $V_\ell$  is unramified at all primes  $p \nmid N\ell$ , so that the action of an arithmetic Frobenius element  $\operatorname{Frob}_q \in G_{\mathbb{Q}}$  is well-defined.

**Proposition 3.6.** *For  $\ell \nmid n \cdot \operatorname{Disc}(\mathbb{T})p$ , there is an isomorphism of  $\mathbb{T}_\ell$ -modules*

$$J_{p,q}[\ell^\infty] \simeq \mathbb{T}_\ell / \det(\rho_\ell(\operatorname{Frob}_q) - 1)\mathbb{T}_\ell$$

where  $\operatorname{Frob}_q \in G_{\mathbb{Q}}$  is a Frobenius element for  $q$ .

*Proof.* If  $\lambda$  is a maximal ideal in  $\mathbb{T}$  and  $k \geq 1$ , let  $J_0(p)[\lambda^k]$  denote the  $G_{\mathbb{Q}}$ -module of points in  $J_0(p)(\overline{\mathbb{Q}})$  killed by all elements in the ideal  $\lambda^k$ .

---

<sup>3</sup>In the literature,  $V_\ell$  is more often written as  $T_\ell$  or  $T_\ell J_0(p)$ , but we have already used up this notation.

Define  $V_\lambda = \lim_k J_0(p)[\lambda^k]$ , the  $\lambda$ -adic Tate module of  $J_0(p)$ . Then we have a decomposition of  $G_{\mathbb{Q}}$ -representations:

$$V_\ell = \bigoplus_{(f,\lambda)} V_\lambda,$$

where  $(f, \lambda)$  varies over orbits of newforms  $f$  and prime ideals  $\lambda$  in  $\mathcal{O}_f$  lying above  $\ell$ , as before. It is known that  $V_\lambda$  is free of rank two over  $\mathcal{O}_i \simeq \mathcal{O}_{f,\lambda}$ , and the determinant of  $V_\lambda$  is the cyclotomic character  $\chi$ . By the Eichler–Shimura relation [15], the action of a Frobenius element  $\text{Frob}_q \in G_{\mathbb{Q}}$  on  $V_\lambda$  has trace equal to  $T_q \in \mathcal{O}_i$ . Now,  $T_q$  acts by  $a_q(f)$  on  $V_\lambda$  and  $\chi(\text{Frob}_q) = q$ . Thus, the characteristic polynomial of  $\text{Frob}_q$  on the rank two  $\mathcal{O}_i$ -module  $V_\lambda$  is  $x^2 - a_q(f)x + q$ . We find that  $\det(\rho_\ell(\text{Frob}_q) - 1) = q + 1 - a_q(f)$ . The result now follows from Proposition 3.5 and summing over all  $(f, \lambda)$ .  $\square$

It is interesting to compare Proposition 3.6 with the following result of Hashimoto [7, 4.3].

**Theorem 3.7.** *Let  $X_0(p)$  be the modular curve of level  $\Gamma_0(p)$  and let  $J_0(p)$  be its Jacobian. Then*

$$n \cdot \#J_{p,q} = \#J_0(p)(\mathbb{F}_q)$$

Let us sketch an alternative proof of this theorem. If  $A$  is an abelian variety over  $\mathbb{F}_q$ , then  $\#A(\mathbb{F}_q) = \det(\text{Fr} - 1)$  where  $\text{Fr}$  is the action of the geometric Frobenius on the  $\ell$ -adic Tate-module of  $A$  [10]. Moreover, if  $A$  is the reduction of an abelian variety  $\tilde{A}$  over  $\mathbb{Q}$ , then this action agrees with the action of  $\text{Frob}_q$  on the  $\ell$ -adic Tate module of  $\tilde{A}$ . Thus, the theorem follows from Propositions 3.3 and 3.6, and some additional care to treat the primes  $\ell \mid n \text{Disc}(\mathbb{T})$ .

Note that  $J_0(p)(\mathbb{F}_q)$  always contains a point of order  $n = (p - 1)/12$ , namely the reduction  $D$  of the cuspidal divisor  $(0) - (\infty)$  on the modular curve. Theorem 3.7 says that the finite abelian groups  $J_{p,q}$  and  $J_0(p)(\mathbb{F}_q)/\langle D \rangle$  have the same cardinality. However, these two groups are not isomorphic in general as the former is a rank 1  $\mathbb{T}$ -module whereas the latter is not. In any case, note that  $X_{p,q}$  describes  $q$ -isogenies of (super-singular) elliptic curves in characteristic  $p$ , whereas  $X_0(p)(\mathbb{F}_q)$  describes  $p$ -isogenies of elliptic curves in characteristic  $q$ . Thus, Hashimoto’s formula can be viewed as a kind of reciprocity law between their Jacobians.

### 4. Proof of Theorem 1.1

Let  $L_q = q + 1 - T_q \in \mathbb{T}_\ell$  be the Laplacian operator for the graph  $X_{p,q}$ . As in the proof of Proposition 3.6, we have

$$L_q = \det(\rho_\ell(\text{Frob}_q) - 1).$$

Recall that  $\mathbb{T}_\ell \simeq \bigoplus_{i=1}^t \mathcal{O}_i$ , where each  $\mathcal{O}_i$  is a discrete valuation ring. Let

$$v : (\mathbb{T}_\ell \otimes \mathbb{Q})^\times \rightarrow \bigoplus_{i=1}^t \mathbb{Z}$$

be the homomorphism which is the discrete valuation on each factor. By Proposition 3.6, the group  $J_{p,q}[\ell^\infty]$  depends only on the tuple  $v(L_q)$ . Indeed,

$$J_{p,q}[\ell^\infty] \simeq \bigoplus_{i=1}^t \mathcal{O}_i / \ell^{k_i} \mathcal{O}_i,$$

where  $v(L_q) = (k_i)_{i=1}^t$ .

Now let  $G$  be the finite  $\mathbb{T}_\ell$ -module in the Theorem. Recall that

$$\mathbb{P}(J_{p,q}[\ell^\infty] \simeq G) = \lim_{X \rightarrow \infty} \frac{\#\{p < X : J_{p,q}[\ell^\infty] \simeq G\}}{\#\{p < X\}},$$

and  $\mathbb{P}(J_{p,q}[\ell^\infty] \simeq G) = 0$  unless  $G = \bigoplus_{i=1}^t \mathcal{O}_i / \ell^{k_i} \mathcal{O}_i$ , for some  $\mathbf{k} = (k_i) \in \mathbb{Z}_{\geq 0}^t$ . So we assume  $G = G_{\mathbf{k}}$ , for some such  $\mathbf{k}$ .

Consider the ideal  $I_{\mathbf{k}} = \{a \in \mathbb{T}_\ell : v(a) \geq \mathbf{k}\}$  in  $\mathbb{T}_\ell$ . By Proposition 3.6, there is an isomorphism  $J_{p,q}[\ell^\infty] \simeq G$  if and only if the image of  $\rho_\ell(\text{Frob}_q)$  in  $\text{GL}_2(\mathbb{T}_\ell / I_{\mathbf{k}})$  has 1 as an eigenvalue and the image of  $\rho_\ell(\text{Frob}_q)$  in  $\text{GL}_2(\mathbb{T}_\ell / I_{\mathbf{w}})$  does not have 1 as an eigenvalue for any  $\mathbf{w} > \mathbf{k}$ . In particular, we can detect whether  $J_{p,q}[\ell^\infty] \simeq G$  from the image of  $\rho_\ell(\text{Frob}_q)$  in  $\text{GL}_2(\mathbb{T}_\ell / I_{\mathbf{k}+\mathbf{1}})$ , where  $\mathbf{k} + \mathbf{1} = (k_i + 1)_{i=1}^t$ .

A result of Ribet [12] states that if  $\ell \nmid 6n \text{Disc}(\mathbb{T})$ , then the image of the Galois representation  $\rho_\ell : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{T}_\ell)$  is precisely the group

$$\mathbb{G}_\ell := \{g \in \text{GL}_2(\mathbb{T}_\ell) : \det(g) \in \mathbb{Z}_\ell^\times\}$$

from the introduction. Hence the image of  $\rho_\ell(G_{\mathbb{Q}})$  in  $\text{GL}_2(\mathbb{T}_\ell / I_{\mathbf{k}+\mathbf{1}})$  is

$$\mathbb{G}_\ell(\mathbf{k} + \mathbf{1}) := \{g \in \text{GL}_2(\mathbb{T}_\ell / I_{\mathbf{k}+\mathbf{1}}) : \det(g) \in \mathbb{Z}_\ell^\times(\mathbf{k} + \mathbf{1})\},$$

where  $\mathbb{Z}_\ell^\times(\mathbf{k} + \mathbf{1})$  is the image of  $\mathbb{Z}_\ell^\times \rightarrow \mathbb{T}_\ell^\times \rightarrow (\mathbb{T}_\ell / I_{\mathbf{k}+\mathbf{1}})^\times$ . Let  $L$  be the finite Galois extension of  $\mathbb{Q}$  which is the fixed field of the kernel of  $\rho_\ell : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{T}_\ell / I_{\mathbf{k}+\mathbf{1}})$ . Thus  $\text{Gal}(L/\mathbb{Q}) \simeq \mathbb{G}_\ell(\mathbf{k} + \mathbf{1})$ . Applying the Chebotarev density theorem to  $L/\mathbb{Q}$ , we find that  $\mathbb{P}(J_{p,q}[\ell^\infty] \simeq G)$  is equal to the proportion of elements of the finite group  $\mathbb{G}_\ell(\mathbf{k} + \mathbf{1})$  whose reduction in  $\text{GL}_2(\mathbb{T}_\ell / I_{\mathbf{k}})$  has 1 as an eigenvalue, but whose reduction in  $\text{GL}_2(\mathbb{T}_\ell / I_{\mathbf{w}})$  does not have 1 as an eigenvalue, for all tuples  $\mathbf{k} < \mathbf{w} < \mathbf{k} + \mathbf{1}$ . By definition of the Haar measure on  $\mathbb{G}_\ell$ , this is equal to the probability that a random  $g \in \mathbb{G}_\ell$  satisfies  $\mathbb{T}_\ell / \det(g - 1)\mathbb{T}_\ell \simeq G$ , as desired.

### 5. Computing the distribution

In this section we prove Theorems 1.2, 1.3, and 1.4. Fix a prime  $\ell$  and integer  $d \geq 1$ , and let  $\lambda = \ell^d$ . Let  $\mathcal{O}$  be the (unique) degree  $d$  unramified cyclic extension of  $\mathbb{Z}_\ell$ . Thus,  $\mathcal{O}$  is a discrete valuation ring containing  $\mathbb{Z}_\ell$ ,

with maximal ideal  $\mathfrak{m} = \ell\mathcal{O}$  and with residue field  $\mathcal{O}/\mathfrak{m}$  isomorphic to the finite field  $\mathbb{F}_\lambda$ . The maximal ideal of  $\mathbb{Z}_\ell$  is  $\ell\mathbb{Z}_\ell$ , so that its residue field  $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell \simeq \mathbb{F}_\ell$  is naturally a subfield of  $\mathcal{O}/\mathfrak{m} \simeq \mathbb{F}_\lambda$ . For any  $k \geq 1$ , we have an inclusion of rings  $\mathbb{Z}_\ell/\ell^k \hookrightarrow \mathcal{O}/\mathfrak{m}^k$ . For  $D \in \mathcal{O}/\mathfrak{m}^k$ , define

$$N(k, D) = \#\{g \in \text{GL}_2(\mathcal{O}/\mathfrak{m}^k) : \det(g - 1) = 0 \text{ and } \det(g) = D\}.$$

**Proposition 5.1.** *Fix  $k \geq 1$  and  $D \in (\mathbb{Z}_\ell/\ell^k\mathbb{Z}_\ell)^\times$ . If  $v(1 - D) = 0$ , then*

$$N(k, D) = \lambda^{2k-1}(\lambda + 1).$$

*Proof.* For this proof, we abuse the usual notation slightly and consider the “reduced valuation”

$$v : \mathcal{O}/\mathfrak{m}^k \rightarrow \{0, 1, \dots, k\}$$

defined by the formula  $\pi^{-1}((a)) = \mathfrak{m}^{v(a)}$ , where  $\pi : \mathcal{O} \rightarrow \mathcal{O}/\mathfrak{m}^k$  is the reduction map and  $(a)$  is the ideal generated by  $a$ .

We wish to compute the number

$$N(k, D) = \#\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathcal{O}/\mathfrak{m}^k) : ad - bc = D \text{ and } 1 - a - d + D = 0 \right\}.$$

Now, if  $a$  is fixed, then  $d$  is determined by the formula  $d = 1 - a + D$ . Note that  $ad - D = (1 - a)(a - D)$ . Thus

$$N(k, D) = \sum_{a \in \mathcal{O}/\mathfrak{m}^k} \sum_{\substack{b \in \mathcal{O}/\mathfrak{m}^k \\ vbf(b) \leq v((1-a)(a-D))}} \sum_{\substack{c \in \mathcal{O}/\mathfrak{m}^k \\ bc = (1-a)(a-D)}} 1$$

**Lemma 5.2.** *If  $b, M \in \mathcal{O}/\mathfrak{m}^k$  satisfy  $v(b) \leq v(M)$  then the number of elements  $c \in \mathcal{O}/\mathfrak{m}^k$  such that  $bc = M$  is  $\lambda^{v(b)}$ .*

*Proof.* If  $M = 0$ , then  $c$  satisfies  $bc = 0$  if and only if  $v(c) \geq k - v(b)$ , and there are  $\lambda^{k-(k-v(b))} = \lambda^{v(b)}$  such elements. If  $M \neq 0$ , then  $c$  must have valuation  $v(M) - v(b)$ , and there are  $\lambda^{k-v(M)+v(b)-1}(\lambda - 1)$  such elements. Multiplying such elements by  $b$ , we are equally likely to obtain any element of valuation  $v(M)$ . Thus, after dividing by the  $\lambda^{k-v(M)-1}(\lambda - 1)$  elements of valuation  $v(M)$ , we find that  $\lambda^{v(b)}$  elements  $c$  satisfy  $bc = M$ .  $\square$

By the Lemma, we have

$$(5.1) \quad N(k, D) = \sum_{a \in \mathcal{O}/\mathfrak{m}^k} \sum_{\substack{b \in \mathcal{O}/\mathfrak{m}^k \\ vbf(b) \leq v((1-a)(a-D))}} \lambda^{v(b)}.$$

Since  $v(1 - D) = 0$ , we can have  $v(1 - a) > 0$  and we can also have  $v(a - D) > 0$  but never both. Moreover,  $(1 - a)(a - D) = 0$  if and only if

$a = 1$  or  $a = D$ . Thus, we compute

$$\begin{aligned}
 N(k, D) &= \sum_{j=1}^k \#\{a : v(1 - a) = j\} \sum_{i=0}^j \#\{b : v(b) = i\} \lambda^i \\
 &\quad + \sum_{j=1}^k \#\{a : v(a - D) = j\} \sum_{i=0}^j \#\{b : v(b) = i\} \lambda^i + \lambda^{2k-2}(\lambda - 2)(\lambda - 1).
 \end{aligned}$$

**Lemma 5.3.** *We have*

$$\#\{b : v(b) = i\} \lambda^i = \begin{cases} \lambda^{k-1}(\lambda - 1) & \text{if } i < k \\ \lambda^k & \text{if } i = k. \end{cases}$$

*Proof.* Indeed, the number of  $b \in \mathcal{O}/\mathfrak{m}^k$  of valuation  $i$  is  $\lambda^{k-1-i}(\lambda - 1)$  if  $i < k$  and 1 if  $i = k$ . □

Separating the contributions from  $a = 1$  and  $a = D$ , we have:

$$N(k, D) = 2(k + 1)\lambda^k - 2k\lambda^{k-1} + \lambda^{2k-2}(\lambda - 2)(\lambda - 1) + A$$

where  $A$  is equal to

$$\begin{aligned}
 &\sum_{j=1}^{k-1} \#\{a : v(1 - a) = j\} (j + 1) \lambda^{k-1} (\lambda - 1) \\
 &\quad + \sum_{j=1}^{k-1} \#\{a : v(a - D) = j\} (j + 1) \lambda^{k-1} (\lambda - 1).
 \end{aligned}$$

Using Lemma 5.3, we compute

$$A = 2\lambda^{2k-1}(\lambda - 1)^2 \sum_{j=2}^k \frac{j}{\lambda^j}.$$

Combining the formula

$$\sum_{i=0}^n i a^i = \frac{a - a^{n+1}}{(1 - a)^2} - \frac{na^{n+1}}{1 - a},$$

we eventually find that

$$A = 2\lambda^{2k} - 2\lambda^k - 2(\lambda - 1)k\lambda^{k-1} - 2(\lambda - 1)^2\lambda^{2k-2}.$$

Thus,

$$\begin{aligned} N(k, D) &= 2(k + 1)\lambda^k - 2k\lambda^{k-1} + \lambda^{2k-2}(\lambda - 2)(\lambda - 1) + 2\lambda^{2k} \\ &\quad - 2\lambda^k - 2(\lambda - 1)k\lambda^{k-1} - 2(\lambda - 1)^2\lambda^{2k-2} \\ &= \lambda^{2k} + \lambda^{2k-1} \\ &= \lambda^{2k-1}(\lambda + 1), \end{aligned}$$

as desired. □

For any  $D \in \mathcal{O}/\mathfrak{m}^{k+1}$ , define the set

$$\mathcal{M}(k, D) = \{g \in \text{GL}_2(\mathcal{O}/\mathfrak{m}^{k+1}) : v(\det(g - 1)) = k \text{ and } \det(g) = D\}$$

and let  $M(k, D) = \#\mathcal{M}(k, D)$ .

**Proposition 5.4.** *Fix  $k \geq 0$  and  $D \in (\mathcal{O}/\mathfrak{m}^{k+1})^\times$ . If  $v(1 - D) = 0$ , then*

$$M(k, D) = \begin{cases} \lambda(\lambda - 2)(\lambda + 1) & \text{if } k = 0 \\ \lambda^{2k+1}(\lambda - 1)(\lambda + 1) & \text{if } k > 0 \end{cases}$$

*Proof.* First assume  $k = 0$ . Then  $M(0, D)$  is the number of  $g \in \text{GL}_2(\mathbb{F}_\lambda)$  of determinant  $D$  such that  $\det(g - 1) \neq 0$ . Now, the number of  $g$  with determinant equal to  $D$  is

$$\frac{\#\text{GL}_2(\mathbb{F}_\lambda)}{\lambda - 1} = (\lambda + 1)\lambda(\lambda - 1).$$

Thus,  $M(0, D) = (\lambda + 1)\lambda(\lambda - 1) - N(1, D)$ , and by Proposition 5.1, this is

$$(\lambda - 1)\lambda(\lambda + 1) - \lambda(\lambda + 1) = \lambda(\lambda + 1)(\lambda - 2).$$

Now assume  $k \geq 1$ . Let  $\pi : \text{GL}_2(\mathcal{O}/\mathfrak{m}^{k+1}) \rightarrow \text{GL}_2(\mathcal{O}/\mathfrak{m}^k)$ . Recall that  $N(k, \pi(D))$  is the cardinality of the set

$$\mathcal{N}(k, \pi(D)) = \{h \in \text{GL}_2(\mathcal{O}/\mathfrak{m}^k) : \det(h) = \pi(D) \text{ and } \det(h - 1) = 0\}.$$

Then  $\pi$  sends  $\mathcal{M}(k, D)$  to  $\mathcal{N}(k, \pi(D))$ . Conversely, given  $h \in \mathcal{N}(k, \pi(D))$ , there is at least one  $g \in \pi^{-1}(h)$  with  $\det(g) = D$ . Any other element of  $\pi^{-1}(h)$  has the form  $g + \ell^k M$  for some matrix  $M$ . The determinant of  $g + \ell^k M$  is equal to

$$\begin{aligned} (a + \ell^k m_1)(d + \ell^k m_4) - (b + \ell^k m_2)(c + \ell^k m_3) \\ = \det(g) + \ell^k(am_4 + dm_1 - cm_2 - bm_3) \end{aligned}$$

and hence equals  $D = \det(g)$  if and only if  $M$  lies in the kernel of a certain non-zero linear functional  $\text{Mat}_2(\mathbb{F}_\lambda) \rightarrow \mathbb{F}_\lambda$ . There are therefore  $\lambda^3$  pre-images  $g' \in \pi^{-1}(h)$  with  $\det(g') = D$ . Not all of them satisfy  $v(\det(g - 1)) = k$ , but we have

$$M(k, D) = \lambda^3 N(k, \pi(D)) - N(k + 1, D).$$



By Proposition 5.1, we have

$$\begin{aligned} M(k, D) &= \lambda^{2k+2}(\lambda + 1) - \lambda^{2(k+1)-1}(\lambda + 1) \\ &= \lambda^{2k+1}(\lambda(\lambda + 1) - \lambda - 1) \\ &= \lambda^{2k+1}(\lambda - 1)(\lambda + 1), \end{aligned}$$

as claimed. □

Now let  $\mathbf{k} = (k_i) \in \mathbb{Z}_{\geq 0}^t$ . Let  $\mathbb{T}_\ell = \bigoplus_{i=1}^t \mathcal{O}_i$ , where each  $\mathcal{O}_i$  is a finite unramified extension of  $\mathbb{Z}_\ell$  of degree  $d_i \geq 1$ . The residue field  $\mathcal{O}_i/\mathfrak{m}_i$  of  $\mathcal{O}_i$  is isomorphic to  $\mathbb{F}_{\lambda_i}$ , where  $\lambda_i = \ell^{d_i}$ . Recall that  $\mathbf{k}$  determines a finite  $\ell$ -primary  $\mathbb{T}_\ell$ -module  $G_{\mathbf{k}} = \bigoplus_{i=1}^t \mathcal{O}_i/\ell^{k_i}$ . If  $g \in \mathbb{G}_\ell$ , then  $\mathbb{T}_\ell/\det(g - 1)\mathbb{T}_\ell \simeq G_{\mathbf{k}}$  if and only if  $v(\det(g - 1)) = \mathbf{k}$ , where here  $v : \mathbb{T}_\ell \rightarrow \mathbb{Z}^t$  is the combined valuation from Section 4.

Recall the ideals  $I_{\mathbf{k}+1}$  and the sets  $\mathbb{Z}_\ell^\times(\mathbf{k} + 1)$ . Having fixed  $\mathbf{k}$  for the time being, we will abuse notation and write  $v : \mathbb{T}_\ell/I_{\mathbf{k}+1} \rightarrow \prod_{i=1}^t \{0, 1, \dots, k_i + 1\}$  for the “combined reduced valuation”. Let  $k = \max_i k_i$ , and observe that we may view  $\mathbb{Z}_\ell/\ell^{k+1}\mathbb{Z}_\ell$  as a subring of  $\mathbb{T}_\ell/I_{\mathbf{k}+1}$ . Define  $\mathbb{Z}_\ell^\diamond(\mathbf{k} + 1)$  to be the subset of elements  $D$  of this subring such that  $v(D(1 - D)) = 0$ . Now define

$$M(\mathbf{k}) = \#\{g \in \text{GL}_2(\mathbb{T}_\ell/I_{\mathbf{k}+1}) : \det(g) \in \mathbb{Z}_\ell^\diamond(\mathbf{k} + 1) \text{ and } v(\det(g - 1)) = \mathbf{k}\}.$$

**Proposition 5.5.** *Let  $\delta_{ij} \in \{0, 1\}$  be Kronecker’s delta. Then*

$$M(\mathbf{k}) = \ell^k(\ell - 2) \prod_{i=1}^t \lambda_i^{2k_i+1}(\lambda_i - 1 - \delta_{0k_i})(\lambda_i + 1).$$

*Proof.* Recall that we view  $\mathbb{Z}_\ell/\ell^{k+1}\mathbb{Z}_\ell$  as a subring of  $\mathbb{T}_\ell/I_{\mathbf{k}+1}$  in the natural way. We have

$$M(\mathbf{k}) = \sum_{D \in \mathbb{Z}_\ell^\diamond(\mathbf{k}+1)} M(\mathbf{k}, D)$$

where

$$M(\mathbf{k}, D) = \#\{g \in \text{GL}_2(\mathbb{T}_\ell/I_{\mathbf{k}+1}) : \det(g) = D \text{ and } v(\det(g - 1)) = \mathbf{k}\}.$$

On the other hand,

$$M(\mathbf{k}, D) = \prod_{i=1}^t M(k_i, D_i),$$

where  $D_i$  is the image of  $D$  in  $\mathbb{Z}_\ell/\ell^{k_i+1}$  and

$$M(k_i, D_i) = \#\{g \in \text{GL}_2(\mathcal{O}_i/\mathfrak{m}_i^{k_i+1}) : \det(g) = D_i \text{ and } v_i(\det(g - 1)) = k_i\}.$$

By Proposition 5.4, we have

$$M(\mathbf{k}, D) = \prod_{i=1}^t \lambda_i^{2k_i+1} (\lambda_i - 1 - \delta_{0k_i}) (\lambda_i + 1),$$

where  $\lambda_i = \#\mathcal{O}_i/\mathfrak{m}_i$ . Thus,

$$\begin{aligned} M(\mathbf{k}) &= \sum_{D \in \mathbb{Z}_\ell^\diamond(\mathbf{k}+1)} M(\mathbf{k}, D) \\ &= \ell^k (\ell - 2) \prod_{i=1}^t \lambda_i^{2k_i+1} (\lambda_i - 1 - \delta_{0k_i}) (\lambda_i + 1). \end{aligned}$$

as claimed. □

Let  $\mathbb{G}'_\ell = \{g \in \mathbb{G}_\ell : \det(g) - 1 \in \mathbb{Z}_\ell^\times\}$ .

**Theorem 5.6.** Fix  $\mathbf{k} \in \mathbb{Z}_{\geq 0}^t$  and let  $\delta_i = 1$  if  $k_i = 0$  and  $\delta_i = 0$  if  $k_i > 0$ . Then the proportion of  $g \in \mathbb{G}'_\ell$  such that  $\mathbb{T}_\ell / \det(g - 1)\mathbb{T}_\ell \simeq G_{\mathbf{k}}$  is

$$\prod_{i=1}^t \lambda_i^{-k_i} \left(1 - \frac{1}{\lambda_i - 1}\right)^{\delta_i} = \frac{1}{\#G_{\mathbf{k}}} \prod_{i=1}^t \left(1 - \frac{1}{\lambda_i - 1}\right)^{\delta_i}.$$

**Remark 5.7.** The distribution above is a product of  $t$  independent probability distributions, since

$$\sum_{k=0}^\infty \lambda^{-k} \left(1 - \frac{1}{\lambda - 1}\right)^{\delta_{0k}} = 1 - \frac{1}{\lambda - 1} + \frac{1}{1 - 1/\lambda} - 1 = 1.$$

*Proof.* Define  $\mathbb{G}'_\ell(\mathbf{k} + 1) := \{g \in \text{GL}_2(\mathbb{T}_\ell/I_{\mathbf{k}+1}) : \det(g) \in \mathbb{Z}_\ell^\diamond(\mathbf{k} + 1)\}$ . Then

$$\begin{aligned} \#\mathbb{G}'_\ell(\mathbf{k} + 1) &= \#\mathbb{Z}_\ell^\diamond(\mathbf{k} + 1) \cdot \#\ker(\text{GL}_2(\mathbb{T}_\ell/I_{\mathbf{k}+1}) \rightarrow (\mathbb{T}_\ell/I_{\mathbf{k}+1})^\times) \\ &= \ell^k (\ell - 2) \prod_{i=1}^t \#\ker(\text{GL}_2(\mathcal{O}_i/\mathfrak{m}_i^{k_i+1}) \rightarrow (\mathcal{O}_i/\mathfrak{m}_i^{k_i+1})^\times) \\ &= \ell^k (\ell - 2) \prod_{i=1}^t \lambda_i^{4k_i} \frac{(\lambda_i^2 - 1)(\lambda_i^2 - \lambda_i)}{\lambda_i^{k_i} (\lambda_i - 1)} \\ &= \ell^k (\ell - 2) \prod_{i=1}^t \lambda_i^{3k_i+1} (\lambda_i^2 - 1). \end{aligned}$$

Thus, by Proposition 5.5, the proportion of  $g \in \mathbb{G}'_\ell$  giving rise to  $G_{\mathbf{k}}$  is

$$\prod_{i=1}^t \frac{\lambda_i^{2k_i+1} (\lambda_i - 1 - \delta_{0k_i})}{\lambda_i^{3k_i+1} (\lambda_i - 1)} = \prod_{i=1}^t \lambda_i^{-k_i} \left(1 - \frac{1}{\lambda_i - 1}\right)^{\delta_i}. \quad \square$$

*Proof of Theorem 1.2.* The result follows from combining Theorem 5.6 with (the proof of) Theorem 1.1. Indeed, restricting to primes  $q \not\equiv 1 \pmod{\ell}$  amounts to restricting to the subgroup  $\mathbb{G}'_\ell \subset G_\ell$ . □

Now we apply Theorem 1.2 to the understand how often  $J_{p,q}[\ell]$  is cyclic. Fix a prime  $\ell \nmid 6n \text{ Disc}(\mathbb{T})$ .

**Corollary 5.8.** *As  $q \rightarrow \infty$  through primes  $q \not\equiv 1 \pmod{\ell}$ , we have*

$$\mathbb{P}(J_{p,q}[\ell^\infty] = 0) = \prod_{i=1}^t \left(1 - \frac{1}{\lambda_i - 1}\right).$$

**Corollary 5.9.** *As  $q \rightarrow \infty$  through primes  $q \not\equiv 1 \pmod{\ell}$ , the probability that  $J_{p,q}[\ell^\infty]$  is a cyclic abelian group is*

$$\left(1 + \frac{t_1}{\ell - 2}\right) \prod_{i=1}^t \left(1 - \frac{1}{\lambda_i - 1}\right),$$

where  $t_1$  is the number of  $\mathcal{O}_i$  which are isomorphic to  $\mathbb{Z}_\ell$  (i.e. with  $d_i = 1$ ).

*Proof.* The  $\mathcal{O}_i$ -component of  $J_{p,q}[\ell^\infty]$  can only be non-trivial and cyclic if  $d_i = 1$ , or in other words  $\lambda_i = \ell$ . Indeed,  $\mathcal{O}_i/\mathfrak{m} \simeq \mathbb{F}_{\lambda_i}$  is isomorphic to  $(\mathbb{Z}/\ell)^{d_i}$  as an abelian group. Let us index the factors  $\mathcal{O}_i$  so that  $d_i = 1$  for  $1 \leq i \leq t_1$ . Then the probability that  $J_{p,q}[\ell^\infty]$  is cyclic is

$$\begin{aligned} & \prod_{i=1}^t \frac{\lambda_i - 2}{\lambda_i - 1} + \sum_{i=1}^{t_1} \frac{1}{\ell - 1} \prod_{j \neq i}^t \frac{\lambda_j - 2}{\lambda_j - 1} \\ &= \kappa + \sum_{i=1}^{t_1} \kappa \cdot \frac{\ell - 1}{\ell - 2} \cdot \frac{1}{\ell - 1} = \kappa + \frac{t_1}{\ell - 2} \kappa = \left(1 + \frac{t_1}{\ell - 2}\right) \kappa, \end{aligned}$$

where  $\kappa = \prod_{i=1}^t \frac{\lambda_i - 2}{\lambda_i - 1}$ . □

What about analogues of the results for  $q \equiv 1 \pmod{\ell}$ ? In principle one can write a closed formula for the distribution of  $J_{p,q}[\ell^\infty]$  (as in Theorem 5.6) as  $q \rightarrow \infty$  varies through primes such that  $v_\ell(p - 1) = k > 0$ , for any fixed  $k$ , but the formulas seemed very complicated to us. For our purposes, we will be happy to simply give analogues of Corollaries 5.8 and 5.9.

**Proposition 5.10.** *As  $q \rightarrow \infty$  through  $q \equiv 1 \pmod{\ell}$ , the probability that  $J_{p,q}[\ell^\infty] = 0$  is*

$$\prod_{i=1}^t \left(1 - \frac{\lambda_i}{\lambda_i^2 - 1}\right).$$

*Proof.* First let  $\mathcal{O} = \mathcal{O}_i$  and  $\lambda = \lambda_i$ . Then the number of  $M \in \text{GL}_2(\mathcal{O}/\mathfrak{m})$  with  $\det(M) = 1$  and  $\det(M - 1) = 0$  is  $(\lambda - 1)^2 + (\lambda - 1) + \lambda = \lambda^2$ , by (5.1). The total number of  $M$  with determinant 1 is

$$\frac{\#\text{GL}_2(\mathbb{F}_\lambda)}{\#\mathbb{F}_\lambda^\times} = \frac{(\lambda^2 - 1)(\lambda^2 - \lambda)}{\lambda - 1} = \lambda(\lambda - 1)(\lambda + 1)$$

Thus the probability that such an  $M$  has  $\det(M - 1) \neq 0$  is  $1 - \frac{\lambda}{\lambda^2 - 1}$ . The proposition now follows by taking the product over all  $i$ .  $\square$

**Proposition 5.11.** *As  $q \rightarrow \infty$  through  $q \equiv 1 \pmod{\ell}$ , the probability that  $J_{p,q}[\ell^\infty]$  is cyclic is*

$$\left(1 + \frac{t_1 \ell}{\ell^2 - \ell - 1}\right) \prod_{i=1}^t \left(1 - \frac{\lambda_i}{\lambda_i^2 - 1}\right)$$

*Proof.* The probability is

$$\begin{aligned} & \prod_{i=1}^t \frac{\lambda_i^2 - \lambda_i - 1}{\lambda_i^2 - 1} + \sum_{i=1}^{t_1} \frac{\ell}{\ell^2 - 1} \prod_{j \neq i} \frac{\lambda_j^2 - \lambda_j - 1}{\lambda_j^2 - 1} \\ &= \kappa + \sum_{i=1}^{t_1} \kappa \cdot \frac{\ell^2 - 1}{\ell^2 - \ell - 1} \cdot \frac{\ell}{\ell^2 - 1} = \kappa + \frac{t_1 \ell}{\ell^2 - \ell - 1} \kappa = \left(1 + \frac{t_1 \ell}{\ell^2 - \ell - 1}\right) \kappa, \end{aligned}$$

where  $\kappa = \prod_{i=1}^t \frac{\lambda_i^2 - \lambda_i - 1}{\lambda_i^2 - 1}$ .  $\square$

Putting together Corollary 5.9 and Proposition 5.11, we obtain the following, which is Theorem 1.3.

**Corollary 5.12.** *As  $q \rightarrow \infty$ , the probability that  $J_{p,q}[\ell^\infty]$  is cyclic is*

$$\frac{\ell - 2 + t_1}{\ell - 1} \prod_{i=1}^t \left(1 - \frac{1}{\lambda_i - 1}\right) + \left(\frac{\ell^2 + (t_1 - 1)\ell - 1}{\ell^3 - 2\ell^2 + 1}\right) \prod_{i=1}^t \left(1 - \frac{\lambda_i}{\lambda_i^2 - 1}\right).$$

As  $\ell \rightarrow \infty$ , this is  $1 - O(\ell^{-2})$ , with the implied constant depending only on  $p$ .

*Proof.* Call the desired probability  $P$ . Then by Dirichlet’s theorem on primes in arithmetic progressions, we have  $P = (1 - \frac{1}{\ell-1})P_A + \frac{1}{\ell-1}P_B$ , where  $P_A$  and  $P_B$  are the probabilities computed in Corollary 5.9 and 5.11, respectively. This gives the claimed formula. To estimate the first term, we may ignore the factors with  $\lambda_i = \ell^{d_i} > \ell$ . Taking  $x = \ell - 1$ , we compute

$$P_A \approx \left(1 + \frac{t_1}{x - 1}\right) \left(1 - \frac{1}{x}\right)^{t_1} = 1 + O(x^{-2}) = 1 + O(\ell^{-2}).$$

Thus

$$P = \left(1 - \frac{1}{\ell - 1}\right) + O(\ell^{-2}) + \frac{1}{\ell - 1} (1 + O(\ell^{-1})) = 1 + O(\ell^{-2}),$$

as desired.  $\square$

Since  $\prod_{\ell}(1 - O(\ell^{-2})) > 0$ , this gives an explicit positive upper bound on the proportion of primes  $p$  such that  $J_{p,q}$  is cyclic. It also suggests that a positive proportion of the groups  $J_{p,q}$  are cyclic, but we cannot deduce this from our results. We at least have the following, which is Theorem 1.4.

**Theorem 5.13.** *Let  $S$  be the set of primes dividing  $6n \text{Disc}(\mathbb{T})$ . The probability that  $\bigoplus_{\ell \notin S} J_{p,q}[\ell^\infty]$  is cyclic is at most*

$$\prod_{\ell \notin S} \left( \frac{\ell - 2 + t_1(\ell)}{\ell - 1} \prod_{i=1}^{t(\ell)} \left( 1 - \frac{1}{\lambda_i - 1} \right) + \left( \frac{\ell^2 + (t_1(\ell) - 1)\ell - 1}{\ell^3 - 2\ell^2 + 1} \right) \prod_{i=1}^{t(\ell)} \left( 1 - \frac{\lambda_i}{\lambda_i^2 - 1} \right) \right),$$

where  $t(\ell)$  is the number of factors in  $\mathbb{T}_\ell$  and  $t_1(\ell)$  is the number of degree one factors of  $\mathbb{T}_\ell$ . In particular, the above Euler product is also an upper bound on the probability that  $J_{p,q}$  is cyclic.

*Proof.* Technically speaking, this does not follow from the previous results. However, Ribet’s results apply not just to a single prime, but to any set of primes not contained in  $S$  [12]. This shows that for any finite set of primes  $\ell_1, \dots, \ell_m$  not in  $S$ , the distributions of the groups  $J_{p,q}[\ell_i^\infty]$  are independent of each other. Taking a limit as  $m \rightarrow \infty$  leads to the desired upper bound.  $\square$

In fact, Ribet’s result applies even to infinite sets of primes not contained in  $S$ . This suggests that with some extra work one might be able to prove a uniformity estimate and hence prove:

**Conjecture 5.14.** The probability that  $\bigoplus_{\ell \notin S} J_{p,q}[\ell^\infty]$  is cyclic is positive and equal to

$$\prod_{\ell \notin S} \left( \frac{\ell - 2 + t_1(\ell)}{\ell - 1} \prod_{i=1}^{t(\ell)} \left( 1 - \frac{1}{\lambda_i - 1} \right) + \left( \frac{\ell^2 + (t_1(\ell) - 1)\ell - 1}{\ell^3 - 2\ell^2 + 1} \right) \prod_{i=1}^{t(\ell)} \left( 1 - \frac{\lambda_i}{\lambda_i^2 - 1} \right) \right).$$

### 6. Examples

We make our results completely explicit for the two smallest values of  $p$ . One may do similar computations for any value of  $p$ , after computing the Hecke algebra  $\mathbb{T}$  in Sage or magma.

**6.1. Case  $p = 37$ .** In this case  $\#X_p = n = (37 - 1)/12 = 3$  and hence  $\dim S_2(\Gamma_0(37)) = 2$ . The two newforms  $f_1$  and  $f_2$  of level 37 have rational coefficients. It follows that  $\mathbb{T}$  is a subring of  $\mathbb{Z} \times \mathbb{Z}$ , and by a discriminant computation in SageMath [13], we find that it has index two (coming from the congruence  $f_1 \equiv f_2 \pmod{2}$ ). Thus  $\mathbb{T}_\ell = \mathbb{Z}_\ell \times \mathbb{Z}_\ell$  for  $\ell > 2$ . By Theorem 5.6, if  $\ell > 3$  is fixed and the primes  $q \not\equiv 1 \pmod{\ell}$  go to  $\infty$ , the probability that  $J_{37}(q)[\ell^\infty] \simeq \mathbb{Z}/\ell^{k_1} \times \mathbb{Z}/\ell^{k_2}$  (as a  $\mathbb{T}_\ell$ -module) is

$$(6.1) \quad \frac{1}{\ell^{k_1+k_2}} \left( \frac{\ell - 2}{\ell - 1} \right)^{\delta_{0k_1}} \left( \frac{\ell - 2}{\ell - 1} \right)^{\delta_{0k_2}}.$$

In particular, for fixed  $\ell$  and for  $q \not\equiv 1 \pmod{\ell}$  going to  $\infty$ , we have

$$\mathbb{P}(J_{37}(q)[\ell^\infty] = 0) = \left( \frac{\ell - 2}{\ell - 1} \right)^2.$$

To determine the distribution of the underlying abelian groups (ignoring the  $\mathbb{T}_\ell$ -module structure), treat the two factors as unordered. For example, the probability that  $J_{37}(q)[\ell^\infty] \simeq \mathbb{Z}/\ell \times \mathbb{Z}/\ell^2$  as abelian groups is

$$\mathbb{P}\left(J_{37}(q)[\ell^\infty] \simeq \mathbb{Z}/\ell \times \mathbb{Z}/\ell^2\right) + \mathbb{P}\left(J_{37}(q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2 \times \mathbb{Z}/\ell\right) = 2 \cdot \frac{1}{\ell^3}.$$

**Example 6.1.** The  $(i, j)$  entry of the following matrix is the number of primes  $q \not\equiv 1 \pmod{5}$  less than 14000712 with  $J_{37}(q)[5^\infty] \simeq \mathbb{Z}/5^{i-1} \times \mathbb{Z}/5^{j-1}$  (as abelian groups), with  $i \leq j$ .

$$\begin{pmatrix} 409362 & 218950 & 43483 & 8787 & 1829 & 359 & 69 & 12 & 1 & 0 \\ 0 & 29077 & 11591 & 2239 & 456 & 103 & 22 & 7 & 2 & 0 \\ 0 & 0 & 1132 & 465 & 92 & 15 & 4 & 1 & 0 & 0 \\ 0 & 0 & 0 & 45 & 20 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We see that the group  $\mathbb{Z}/5 \times \mathbb{Z}/25$ , say, shows up a proportion of  $\frac{11591}{728129} \approx .015919$  of the time, compared to the true asymptotic proportion  $\frac{2}{5^3} = .016$ .

For any  $\ell > 3$ , Corollary 5.12 says that the proportion of  $q$  for which  $J_{37}(q)[\ell^\infty]$  is cyclic is

$$1 - \frac{(\ell + 2)(\ell^2 - \ell - 1)}{(\ell - 1)^3(\ell + 1)^2}.$$

If we restrict to  $q \not\equiv 1 \pmod{\ell}$ , then by Corollary 5.12 this proportion is

$$\left(1 + \frac{2}{\ell - 2}\right) \left(\frac{\ell - 2}{\ell - 1}\right)^2 = \frac{\ell(\ell - 2)}{(\ell - 1)^2}.$$

For example, when  $\ell = 5$ , this is  $\frac{15}{16} = .9375$ , which can be compared with the proportion  $.937817\dots$  computed from the data in the matrix above. If we allow primes up to 19000853, then this proportion becomes  $.937752\dots$ , consistent with the convergence to  $.9375$ .

Conjecture 5.14 says that the probability that  $J_{37}(q)[1/6]$  is cyclic is

$$\prod_{\ell > 3} \left(1 - \frac{(\ell + 2)(\ell^2 - \ell - 1)}{(\ell - 1)^3(\ell + 1)^2}\right) = .885\dots$$

**6.2. Case  $p = 61$ .** We have  $n = (61 - 1)/12 = 5$ , so  $\dim S_2(\Gamma_0(61)) = 4$ . There are two  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -orbits of newforms  $f_1$  and  $f_2$ . The fields generated by their Fourier coefficients are  $\mathbb{Q}$  and  $K = \mathbb{Q}[x]/(x^3 - 30x - 2)$ , respectively. The latter is a cubic field of discriminant  $148 = 2^2 \cdot 37$ . Sage reports that the Hecke algebra  $\mathbb{T}$  has discriminant  $2^4 \cdot 37$  and hence is index two in the maximal order  $\mathbb{Z} \times \mathcal{O}_K$ . The non-maximality of  $\mathbb{T}$  comes from the congruence  $f_1 \equiv f_2 \pmod{\lambda}$ , where  $\lambda$  is the unique prime of  $K$  above 2.

Thus, for any fixed  $\ell \notin \{2, 5, 37\}$ , we have

$$\mathbb{T}_\ell \simeq \mathbb{Z}_\ell \times \bigoplus_{\lambda|\ell} \mathcal{O}_\lambda,$$

where the sum is over the primes  $\lambda$  of  $\mathcal{O}_K$  above  $\ell$  and  $\mathcal{O}_\lambda$  is the completion of  $\mathcal{O}_K$  at  $\lambda$ . Note that  $\mathcal{O}_\lambda$  is unramified of degree  $f_\lambda$ , where  $f_\lambda$  is the residual degree:  $\mathcal{O}_K/\lambda \simeq \mathbb{F}_{\ell^{f_\lambda}}$ . The residual degrees are either  $(1, 1, 1)$ ,  $(1, 2)$ , or  $(3)$ , depending on how  $\ell$  splits in  $\mathcal{O}_K$ . By Chebotarev’s density theorem, the proportion of primes  $\ell$  with the given splitting type is  $1/6$ ,  $1/2$ , and  $1/3$ , respectively.

For example, the prime 13 splits as  $\mathfrak{l}_1\mathfrak{l}_2$  in  $\mathcal{O}_K$ , with  $\mathfrak{l}_i$  having norm  $13^i$ . Thus,  $\lambda_1 = \lambda_2 = 13$  and  $\lambda_3 = 13^2$ , and

$$J_{61}(q)[13^\infty] \simeq (\mathbb{Z}/13^a) \times (\mathbb{Z}/13^b) \times (\mathbb{Z}/13^c)^2$$

for integers  $a, b, c \geq 0$ . For primes  $q \not\equiv 1 \pmod{13}$ , the probability for the tuple  $(a, b, c)$  can be read off of Theorem 1.2. For example, the probability that  $J_{61}(q)[13^\infty] \simeq (\mathbb{Z}/13)^3$ , as abelian groups, is

$$2 \cdot \frac{1}{13} \frac{11}{12} \frac{1}{13^2} \approx .000834,$$

corresponding to the two tuples  $(1, 0, 1)$  and  $(0, 1, 1)$ . In Table 6.1, we compare the asymptotic proportions with the observed proportion for the first 62772 primes  $q \not\equiv 1 \pmod{13}$ .

TABLE 6.1. Distribution of the group  $J_{61}(q)[13^\infty] \simeq \prod_{i=1}^4 (\mathbb{Z}/13^{a_i})$ , for  $q \not\equiv 1 \pmod{13}$

$(a_1, a_2, a_3, a_4)$	Limiting proportion	Observed proportion ( $q \leq 861997$ )
$(0, 0, 0, 0)$	$20207/24192 \approx .83527$	$\approx .8356$
$(0, 0, 0, 1)$	$1837/13104 \approx .1401$	$\approx .1398$
$(0, 0, 1, 1)$	$1849/170352 \approx .01085$	$\approx .01096$
$(0, 0, 0, 2)$	$1837/170352 \approx .01078$	$\approx .01067$
$(0, 0, 1, 2)$	$167/184548 \approx .0009049$	$\approx .0009239$
$(0, 1, 1, 1)$	$11/13182 \approx .00083447$	$\approx .000860$
$(0, 0, 0, 3)$	$1837/2214576 \approx .0008295$	$\approx .0008283$

The shape of the Euler factor in Corollary 5.12 depends on the splitting type of  $\ell$  in  $\mathbb{Z} \times \mathcal{O}_K$ . For the types  $(1, 1, 1, 1)$ ,  $(1, 1, 2)$ , and  $(1, 3)$  we compute

the following Euler factors:

$$f_1(\ell) = 1 - \frac{6\ell^7 - 2\ell^6 - 43\ell^5 + 17\ell^4 + 92\ell^3 - 2\ell^2 - 79\ell - 34}{(\ell - 1)^5(\ell + 1)^4}$$

$$f_2(\ell) = 1 - \frac{(\ell + 1)^3(2\ell^7 - 5\ell^5 - 3\ell^4 + 4\ell^2 + 7\ell + 2)}{(\ell - 1)^4(\ell^2 + 1)}$$

$$f_3(\ell) = 1 - \frac{\ell^4 - \ell^3 + \ell - 2}{(\ell - 1)^2(\ell + 1)(\ell^2 - \ell + 1)(\ell^2 + \ell + 1)}$$

Since  $2 \cdot 3 \cdot 5 \cdot 37 = 1110$ , Conjecture 5.14 predicts that  $J_{61}(q)[1/1110]$  is cyclic with probability

$$\prod_{\ell \in \mathcal{O}_K = \lambda_1 \lambda_2 \lambda_3} f_1(\ell) \prod_{\ell \in \mathcal{O}_K = \lambda_1 \lambda_2} f_2(\ell) \prod_{\ell \in \mathcal{O}_K = (\ell)} f_3(\ell) = .9544 \dots$$

For primes  $q$  up to 861997, we found the proportion to be  $\frac{65325}{68492} \approx .9537$ .

**Acknowledgments.** The authors thank Amitay Kamber and Guy Sapire, as well as Ori Parzanchevski for a helpful conversation about Hashimoto’s edge-adjacency operator. The first author visited the Hebrew University of Jerusalem virtually as part of an internship via the Erasmus program and ENS Rennes.

### References

- [1] L. AMORÓS, A. IEZZI, K. LAUTER, C. MARTINDALE & J. SOTÁKOVÁ, “Explicit connections between supersingular isogeny graphs and Bruhat–Tits trees”, *Cryptology ePrint Archive*, Report 2021/372, 2021, <https://ia.cr/2021/372>.
- [2] J. CLANCY, T. LEAKE & S. PAYNE, “A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs”, *Exp. Math.* **24** (2015), no. 1, p. 1-7.
- [3] H. COHEN & H. W. LENSTRA, JR, “Heuristics on class groups of number fields”, in *Number theory, Noordwijkerhout 1983*, Lecture Notes in Mathematics, vol. 1068, Springer, 1984, p. 33-62.
- [4] J. B. CONREY, W. DUKE & D. W. FARMER, “The distribution of the eigenvalues of Hecke operators”, *Acta Arith.* **78** (1997), no. 4, p. 405-409.
- [5] M. EMERTON, “Supersingular elliptic curves, theta series and weight two modular forms”, *J. Am. Math. Soc.* **15** (2002), no. 3, p. 671-714.
- [6] D. GARTON, “Random matrices, the Cohen–Lenstra heuristics, and roots of unity”, *Algebra Number Theory* **9** (2015), no. 1, p. 149-171.
- [7] W.-C. W. LI, *Zeta and L-functions in number theory and combinatorics*, CBMS Regional Conference Series in Mathematics, vol. 129, American Mathematical Society, 2019, published for the Conference Board of the Mathematical Sciences, vii+95 pages.
- [8] B. MAZUR, “Modular curves and the Eisenstein ideal”, *Publ. Math., Inst. Hautes Étud. Sci.* (1977), no. 47, p. 33-186, with an appendix by Mazur and M. Rapoport.
- [9] A. MÉSZÁROS, “The distribution of sandpile groups of random regular graphs”, *Trans. Am. Math. Soc.* **373** (2020), no. 9, p. 6529-6594.
- [10] D. MUMFORD, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Tata Institute of Fundamental Research; Hindustan Book Agency, 2008, with appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition, xii+263 pages.
- [11] K. A. RIBET, “On modular representations of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  arising from modular forms”, *Invent. Math.* **100** (1990), no. 2, p. 431-476.



- [12] ———, “Images of semistable Galois representations”, in *Olga Taussky-Todd: In memoriam. Special issue of the Pacific Journal of Mathematics*, International Press, 1997, p. 277-297.
- [13] THE SAGE DEVELOPERS, *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020, <https://www.sagemath.org>.
- [14] J.-P. SERRE, “Répartition asymptotique des valeurs propres de l’opérateur de Hecke  $T_p$ ”, *J. Am. Math. Soc.* **10** (1997), no. 1, p. 75-102.
- [15] G. SHIMURA, “Correspondances modulaires et les fonctions  $\zeta$  de courbes algébriques”, *J. Math. Soc. Japan* **10** (1958), p. 1-28.
- [16] J. H. SILVERMAN, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 1986, xii+400 pages.
- [17] M. M. WOOD, “The distribution of sandpile groups of random graphs”, *J. Am. Math. Soc.* **30** (2017), no. 4, p. 915-958.

Nathanaël MUNIER  
Institut de Mathématiques de Toulouse 1 R.3  
Université Paul Sabatier  
118 Rte de Narbonne  
31400 Toulouse, France  
*E-mail*: [nathanael.munier@ens-rennes.fr](mailto:nathanael.munier@ens-rennes.fr)

Ari SHNIDMAN  
Einstein Institute of Mathematics  
The Hebrew University of Jerusalem  
Edmund J. Safra Campus  
Jerusalem 9190401, Israel  
*E-mail*: [ari.shnidman@gmail.com](mailto:ari.shnidman@gmail.com)