Eyal Z. GOREN et Payman L KASSAEI

p-adic Dynamics of Hecke Operators on Modular Curves

p-adic Dynamics of Hecke Operators on Modular Curves

par Eyal Z. GOREN et Payman L KASSAEI

RÉSUMÉ. Cet article se penche sur la dynamique p-adique des opérateurs de Hecke d'indice premier à p agissant sur les points des courbes modulaires dans les cas de bonne réduction ordinaire et supersingulière. Une attention particulière est accordée à la dynamique des points CM. Dans le cas de réduction ordinaire, nous exploitons les coordonnées de Serre–Tate, alors que dans le cas de réduction supersingulière nous utilisons un paramètre sur l'espace de déformations de l'unique groupe formel de hauteur 2 sur $\overline{\mathbb{F}}_p$ et le morphisme de périodes de Gross–Hopkins.

ABSTRACT. In this paper we study the p-adic dynamics of prime-to-p Hecke operators on the set of points of modular curves in both cases of good ordinary and supersingular reduction. We pay special attention to the dynamics on the set of CM points. In the case of ordinary reduction we employ the Serre–Tate coordinates, while in the case of supersingular reduction we use a parameter on the deformation space of the unique formal group of height 2 over $\overline{\mathbb{F}}_p$, and take advantage of the Gross–Hopkins period map.

1. Introduction

In this paper we study the dynamics of Hecke operators on the modular curves $X_1(N)$ in the p-adic topology. The motivation for this paper initially came from a desire to understand the impact of this dynamics on the study of the canonical subgroup over Shimura varieties, as part of the continuation of our work [14]. While studying this problem, we realized that even in the simplest case of Shimura varieties, the modular curves, there are significant challenges. Our work on this specific setting is the content of this paper; the techniques introduced here will be useful in studying much more general situations that we hope to discuss in future work.

There are other motivations to study this problem. Let R be the maximal order of a finite field extension of $\mathbb{Q}_p$. Let κ denote the residue field of R. Let X be a Shimura variety of PEL type with a smooth integral model over R, over which the action of the prime-to-p Hecke algebra extends. The

action on the special fibre X_κ has been studied extensively by Chai and Oort, as part of Oort's philosophy of foliations on Shimura varieties of PEL type [5, 7, 24]. From our perspective, the work of Chai and Oort is a "mod p shadow" of the p-adic dynamics of Hecke operators.

Secondly, Clozel and Ullmo [8, 9] have studied dynamics of the Hecke operators over the complex numbers in connection with the André–Oort conjecture, bringing in tools from measure theory and ergodic theory. Our work resonates well with theirs as our main interest lies in the action of Hecke operators on special subvarieties, albeit in the p-adic topology. In particular, in this paper we pay special attention to the action of Hecke operators on CM points. More than that, somewhat serendipitously, after non-trivial reductions, including via the Gross–Hopkins period morphism, our analysis uses results on random walks on groups and ergodic theory.

When this work was essentially completed, we learned of interesting work on the same topic by Herrero–Menares–Rivera-Letelier [19]; see also the forthcoming [18]. The points of view taken in our respective works are different, and the results fit well together to shed light on complementary aspects of the theory. While we are interested in the distribution of the set of points in a Hecke orbit in the p-adic topology, [18] considers the convergence of a sequence of Hecke orbits to the Gauss point of the affine Berkovich line. Unlike our work, [19] considers only modular curves of level 1, but it is believed that their results hold in more general levels. See also the recent preprint [11].

We now briefly discuss the contents of this paper. Our main interest is in the action of the prime-to-p Hecke operators on CM points (points on the modular curve that correspond to CM elliptic curves) regarded as the special Shimura subvarieties of the modular curve $X_1(N)$. We denote a point of $X_1(N)(\mathbb{C}_p)$ by $x = (E_x, P_x)$, where E_x is an elliptic curve and P_x a point of order N of it. We simplify the analysis by looking at the action of the (iterations of) a single Hecke operator T_ℓ, where $\ell \neq p$ is a prime. A key point of our approach is to use reduction mod p to propel results from characteristic p to characteristic 0. The analysis breaks naturally into two cases: (i) ordinary reduction and (ii) supersingular reduction. That is, we distinguish between the case where the elliptic curve E_x has good ordinary reduction, and the case where it has supersingular reduction. The case of bad reduction is not important to us as our main interest is in CM points; these always have (potentially) good reduction. That being said, the methods in the ordinary case can easily be applied to the case of bad reduction.

Ordinary reduction. The locus of ordinary reduction in the modular curve $X_1(N)$ can be partitioned into a union of residue discs which are shuffled around via the Hecke operator T_ℓ in a way that can be fully

understood using the theory of ℓ-isogeny volcanoes. In fact, the centre of these discs, i.e., the *canonical lifts*, are moved around exactly according to the ℓ-isogeny volcano. Consequently, to study the dynamics of T_ℓ acting on a point x of ordinary reduction, one needs to understand the returns of the orbit to the residue disc D containing x. It transpires that this question can be reduced to the dynamics of a *single* automorphism of the disc, induced by a particular endomorphism f of $\overline{E}$, the reduction of E_x. At this point, we switch gears and, by means of Serre–Tate theory, view the residue disc as the rigid-analytic generic fiber of the formal scheme that is the universal deformation space of $\overline{E}$. As such, the disc has a natural parameter t, where the canonical lift corresponds to $t = 0$. We prove (Theorem 4.1.2), using [21], that the action of f on the disc is given by

$$t \mapsto (1+t)^{\bar{f}/f} - 1,$$

where f and its complex conjugate $\bar{f}$ are viewed as elements of $\mathbb{Z}_p^\times$ via their action on the p-adic Tate module of $\overline{E}$. This provides a very clear picture of the orbits and their closures and allows us to completely determine the dynamics of T_ℓ on the CM points in D, which turn out to be periodic points for the action of f; see Section 4, in particular, Propositions 4.2.2, 4.2.3, 4.3.1, 4.4.1.

Throughout our discussion in Sections 2–4 of the action of Hecke operators on elliptic curves E with ordinary reduction $\overline{E}$, we assume that

$(\star)$ $\qquad\qquad\qquad\qquad \mathrm{End}^0(E) \not\cong \mathbb{Q}(i), \mathbb{Q}(\rho),$

where $i^2 = -1, \rho^2 + \rho + 1 = 0$. This guarantees that for any elliptic curve $\overline{E}'$ isogenous to $\overline{E}$, we have $\mathrm{Aut}(\overline{E}') = \{\pm 1\}$. This assumption is made for simplicity only; the methods extend to the general case.

Supersingular reduction. Once more, our analysis begins in characteristic p, where we introduce a class of directed graphs $\Lambda_\ell(N)$ that we call "supersingular graphs". These graphs are defined in a way that encodes the action of T_ℓ on the supersingular points in $X_1(N)(\overline{\mathbb{F}}_p)$. Roughly speaking, vertices of $\Lambda_\ell(N)$ correspond to supersingular points of $X_1(N)(\overline{\mathbb{F}}_p)$, and edges to isogenies of degree ℓ. They are directed graphs of outgoing degree $\ell + 1$, and usually of ingoing degree $\ell + 1$ as well. They serve as level $\Gamma_1(N)$ analogues of the (graphs defined by the) Brandt matrix $B(\ell)$.

Again, the finitely many residue discs of supersingular reduction in $X_1(N)$ move under the iterations of T_ℓ according to walks in the graph $\Lambda_\ell(N)$. However, the returns under T_ℓ to a particular supersingular disc turns out to be much more complicated than in the ordinary case. Fixing a supersingular residue disc $D \subset X_1(N)(\mathbb{C}_p)$ specializing to a supersingular elliptic curve $(\overline{E}, \overline{P})$ in characteristic p, the branches of the iterations of T_ℓ

that return to D generate a subgroup $\mathscr{H}_N \subset (\mathrm{End}(\overline{E}) \otimes \mathbb{Z}_p)^\times =: \mathscr{R}^\times$, $\mathscr{R}$ being the maximal order in the unique non-split quaternion algebra over $\mathbb{Q}_p$. The nature of the groups $\mathscr{H}_N$ is not entirely clear. We prove several results about these groups and, in particular, show that they have an abundance of mutually non-commuting elements; enough so that they are dense in GL_2 relative to the Zariski topology, under the inclusion $\mathscr{R}^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_q)$, where $q = p^2$, and $\mathbb{Q}_q = W(\mathbb{F}_q)[p^{-1}]$.

To study the action of the highly complicated non-abelian group $\mathscr{H}_N$ on D, we once again interpret D as the rigid-analytic space associated to a universal deformation space, this time of a 1-dimensional formal group of height 2. This allows us to use the work of Gross–Hopkins [20] and Lubin–Tate [22]. Using the equivariant Gross–Hopkins period morphism $\Phi : D \to \mathbb{P}^1$, we may study of the action of $\mathscr{H}_N$ on D via the action of Möbius transformations on $\mathbb{P}^1$. We define open discs $J \subset D, U \subset \mathbb{P}^1$ such that Φ restricts to an isomorphism $J \to U$. We show that all CM points of discriminant prime to p lie in $J(W(\mathbb{F}_q))$, which is in bijection with $U(W(\mathbb{F}_q))$, the open unit disc in $W(\mathbb{F}_q)$. The key point now is that we are able to obtain a very explicit description of the p-adic closure $\mathbb{H}_N$ of $\mathscr{H}_N$ in $\mathscr{R}^\times$. We equip $\mathbb{H}_N$ with a measure coming from the action of T_ℓ. We translate our questions about the Hecke orbit of a CM point $x \in D$ under T_ℓ to questions about stationary measures for the action of $\mathbb{H}_N$. Using the description of $\mathbb{H}_N$ and the work of Benoist–Quint [2], we conclude that there is a unique stationary probability measure (namely, a measure fixed under the action of $\mathbb{H}_N$), independent of x and N, whose support is $J(W(\mathbb{F}_q))$. See Theorems 5.10.4–5.10.7.

2. The ℓ-isogeny graph: the ordinary case

Before defining the various ℓ-isogeny graphs of elliptic curves, we recall some definitions from graph theory.

2.1. Graph theory terminology. Let Λ be a directed graph. We will call a directed edge, $v \to w$, an *arrow*. A *walk* in Λ is a sequence of arrows $v_i \xrightarrow{e_i} w_i$ for $i = 1, \ldots, d$, where $w_i = v_{i+1}$ for $i = 1, \ldots, d-1$. This walk is called a closed walk if $v_1 = w_d$. We allow the empty walk and consider it a closed walk. If ω_1, ω_2 are walks in Λ such that the end point of ω_1 is the starting point of ω_2, we denote $\omega_2 \circ \omega_1$ the walk obtained by traversing ω_1 followed by ω_2. If v is a vertex in Λ, we define $\Omega(\Lambda, v)$ to be the monoid of closed walks in Λ starting and ending at v under $\circ$. We often write $\omega_2 \omega_1$ for $\omega_2 \circ \omega_1$.

If ω is a closed walk in Λ starting at v_1 and traversing, in order, vertices $v_1, v_2, \ldots, v_d = v_1$, we can view ω as a closed walk in $\Omega(\Lambda, v_i)$ for all $1 \le i \le d$. We will often abuse notation and denote all these walks by the same notation if the starting point of the walk is understood.

A *path* is a walk in which vertices do not repeat (and so a path is necessarily open). In a *cycle*, vertices do not repeat, except that the last vertex is equal to the first (and so a cycle is closed).

An undirected graph is called *regular* if every vertex has the same degree. Every loop, i.e., an edge between a vertex and itself, contributes one to the degree at the vertex. A directed graph is called *regular of degree r* if the in-degree and the out-degree of each vertex equal r. An arrow of the form $v \to v$ contributes one to both the in-degree and the out-degree. A directed graph is called *connected* if given any two vertices x, y, there is a walk starting from x and ending in y.

Let ℓ be a positive integer. An infinite connected undirected graph Σ is called an *ℓ-volcano* if there is a surjective function $b \colon \Sigma^V \to \mathbb{N}$ (where Σ^V is the set of vertices) such that

(1) Σ is $(\ell + 1)$-regular,
(2) $b^{-1}(0)$ with its induced subgraph structure (called the *rim*) is a regular graph of degree at most 2,
(3) for $i > 0$, each vertex in $b^{-1}(i)$ is connected to a unique vertex in $b^{-1}(i - 1)$ and to ℓ vertices in $b^{-1}(i + 1)$.

2.2. Definition of the ordinary ℓ-isogeny graphs. Let $p \neq \ell$ be primes. Let $N \geq 1$ be an integer such that $(N, p\ell) = 1$. In the following we will study the ℓ-isogeny graph of $\underline{E} = (E, P)$, consisting of an ordinary elliptic curve E over $\overline{\mathbb{F}}_p$ with a point P of order N on it (cf. [30] in the case $N = 1$). Recall our standing assumption:

$$(\star) \qquad\qquad \mathrm{End}^0(E) \not\cong \mathbb{Q}(i), \mathbb{Q}(\rho).$$

For two such objects, $\underline{E}_1 = (E_1, P_1)$ and $\underline{E}_2 = (E_2, P_2)$, we write

$$\underline{E}_1 \overset{\ell}{\sim} \underline{E}_2$$

if there is an isogeny $\lambda \colon E_1 \to E_2$ of degree a power of ℓ such that $\lambda(P_1) = P_2$. This defines an equivalence relation on the set of isomorphism classes of all such pairs (to see the symmetry, let $\alpha(N)$ denote the order of ℓ in $(\mathbb{Z}/N\mathbb{Z})^\times$. Then $\deg(\lambda)^{\alpha(N)-1}\lambda^\vee \colon \underline{E}_2 \to \underline{E}_1$ takes P_2 to P_1).

We define a directed graph $\Lambda_\ell(\underline{E}, N)$ as follows. The set of vertices $\Lambda_\ell(\underline{E}, N)^V$ is the set of isomorphism classes of all pairs $\underline{E}_1 = (E_1, P_1)$ over $\overline{\mathbb{F}}_p$ that satisfy $\underline{E}_1 \overset{\ell}{\sim} \underline{E}$. We define an arrow between two such isomorphism classes $[(E_1, P_1)]$, $[(E_2, P_2)]$ to be an isogeny $\lambda \colon (E_1, P_1) \to (E_2, P_2)$ of degree ℓ, where we identify two such isogenies up to isomorphism. In other words, arrows corresponding to isogenies $\lambda \colon (E_1, P_1) \to (E_2, P_2)$ and

$\lambda' \colon (E_1', P_1') \to (E_2', P_2')$ are identified if there is a commutative diagram

$$
\begin{array}{ccc}
(E_1, P_1) & \xrightarrow{\;\lambda\;} & (E_2, P_2) \\
{\scriptstyle f_1} \downarrow & & \downarrow {\scriptstyle f_2} \\
(E_1', P_1') & \xrightarrow{\;\lambda'\;} & (E_2', P_2')
\end{array}
$$

where f_1, f_2 are isomorphisms. Note that $\Lambda_\ell(\underline{E}, N)$ is a connected directed graph. Also, due to our assumption on $\mathrm{Aut}(E)$, when $N > 2$, once we fix representatives (E_1, P_1) and (E_2, P_2) above, an arrow between the corresponding vertices determines a unique isogeny of degree ℓ from (E_1, P_1) to (E_2, P_2). When $N \le 2$, this isogeny is only defined up to sign. We further define

$$
\Lambda_\ell^{\mathrm{ord}}(N) = \coprod_{\underline{E} \text{ ordinary}} \Lambda_\ell(\underline{E}, N),
$$

where $\underline{E}$ runs over all representatives $\underline{E} = (E, P)$ modulo the equivalence relation $\overset{\ell}{\sim}$.

Let $K = \mathrm{End}^0(E)$ be the algebra of rational endomorphisms of E, which is a quadratic imaginary field of discriminant $\Delta = \Delta(E)$ ($\Delta \ne -3, -4$). We denote the order of conductor c in K by R_c. If $\underline{E} \overset{\ell}{\sim} \underline{E}_1$ then $\mathrm{End}(E_1)$ is an order in K of conductor

$$
\mathfrak{f}(E_1) = \ell^r m,
$$

where $(m, p\ell) = 1$, and $r \ge 0$. Note that m is an invariant of the equivalence classes under $\overset{\ell}{\sim}$. The discriminant $\mathfrak{d}(E_1)$ of $\mathrm{End}(E_1)$ satisfies $\mathfrak{d}(E_1) = \mathfrak{f}(E_1)^2 \Delta(E_1)$. We can define a level function

$$
b_N \colon \Lambda_\ell(\underline{E}, N)^V \to \mathbb{N}
$$

by setting $b_N([\underline{E}_1]) = r$.

2.3. The isogeny associated to a walk. Let ω be a walk

$$
[\underline{E}_0] \overset{\lambda_1}{\to} [\underline{E}_1] \overset{\lambda_2}{\to} \ldots \overset{\lambda_d}{\to} [\underline{E}_d]
$$

in $\Lambda_\ell(\underline{E}, N)$. Note that if $N > 2$ we can think of each λ_i as an isogeny of degree ℓ from $\underline{E}_{i-1}$ to $\underline{E}_i$; if $N \le 2$, these isogenies are only defined up to sign. We define

$$
\widetilde{\omega} := \lambda_d \circ \cdots \circ \lambda_2 \circ \lambda_1
$$

which is an ℓ^d-isogeny from E_0 to E_d sending P_0 to P_d, defined only up to sign if $N \le 2$. In particular, if $\omega \in \Omega(\Lambda_\ell(\underline{E}, N), [\underline{E}])$ then $\widetilde{\omega}$ is an element of $\mathrm{End}(E)$ of degree ℓ^d fixing P.

2.4. Properties of the ℓ-isogeny graphs. When $N = 1$, the directed graph $\Lambda_\ell(E, 1)$ has the property that for every arrow $[E_1] \to [E_2]$ corresponding to an ℓ-isogeny $\lambda\colon E_1 \to E_2$, there is a corresponding arrow $[E_2] \to [E_1]$ given by the dual isogeny $\lambda^\vee\colon E_2 \to E_1$. Identifying these corresponding arrows, we obtain an *undirected* graph denoted $\Lambda_\ell^{\mathrm{ud}}(E, 1)$. Our convention is that if $[E_1] = [E_2]$, and if $\lambda^\vee \neq \pm\lambda$, then the resulting loop is counted with multiplicity two in $\Lambda_\ell^{\mathrm{ud}}(E, 1)$; otherwise, it is counted with multiplicity 1. The function b_1 defined above descends to $b_1\colon \Lambda_\ell^{\mathrm{ud}}(E, 1) \to \mathbb{N}$.

For a set S of endomorphisms of E (and in particular for a prime ideal L of $\mathrm{End}(E)$) we let $E[S] = \cap_{s \in S} \mathrm{Ker}(s)$. The following proposition about the structure of the graph $\Lambda_\ell^{\mathrm{ud}}(E, 1)$ is known (cf. [30]).

Proposition 2.4.1. *Let E be an ordinary elliptic curve over $\overline{\mathbb{F}}_p$ for which we have $\mathrm{End}^0(E) \not\cong \mathbb{Q}(i), \mathbb{Q}(\rho)$ and $\mathfrak{f}(E) = \ell^r m$.*

(1) *The graph $\Lambda_\ell^{\mathrm{ud}}(E, 1)$ is an ℓ-volcano with respect to the level function b_1. The rim is a regular graph of degree $1 + (\frac{\Delta(E)}{\ell})$, the vertices of which are exactly those vertices of $\Lambda_\ell^{\mathrm{ud}}(E, 1)$ that have CM by R_m. (Here $(\frac{\Delta(E)}{\ell})$ is the Kronecker symbol.)*

(2) *Let $L|\ell$ be a prime ideal of R_m. Let $a = \mathrm{ord}_{cl(R_m)}(L)$; in particular, we have $L^a = (f)$ for $f \in R_m$. If ℓ is inert in R_m, then the rim consists of a single vertex and has no edges. If ℓ is ramified in R_m but L is not principal, then the rim consists of two vertices $[E_1]$ and $[E_1/E_1[L]]$ with exactly one edge between them (the class of the natural projection $E_1 \to E_1/E_1[L]$). In all other cases, the rim consists of a cycle of length a given by*

$$[E_1] - [E_1/E_1[L]] - \cdots - [E_1/E_1[L^a]] = [E_1]$$

(using the isomorphism $E_1/E_1[L^a] \to E$ induced by f).

(3) *The cardinality of $b_1^{-1}(i)$ equals*

$$|b_1^{-1}(i)| = \begin{cases} \mathrm{ord}_{cl(R_m)}(L) & i = 0, \; L|\ell \text{ a prime ideal of } R_m, \\ (\ell - (\frac{\Delta(E)}{\ell}))\ell^{i-1}\, \mathrm{ord}_{cl(R_m)}(L) & i \geq 1. \end{cases}$$

If $[E'] \xrightarrow{\lambda} [E'']$ is an arrow in $\Lambda_\ell(E, 1)$, we denote $[E''] \xrightarrow{\lambda^\vee} [E']$ the arrow obtained via the dual isogeny. Similarly, we define for a walk ω from $[E']$ to $[E'']$, a walk $\omega^\vee$ in the reverse direction.

We define two particular walks in $\Lambda_\ell(E, 1)$ as follows. If ℓ is inert in R_m, we define $\omega_{rim}^+ = \omega_{rim}^-$ to be the empty walk. If $\ell = L^2$ is ramified in R_m we define $\omega_{rim}^+ = \omega_{rim}^-$ to be the unique closed walk in the rim (up to the choice of starting point; see Remark 2.4.2 below). It is a loop if L is principal and of length 2 if it is not. If ℓ is split, there are two distinct cycles in $\Lambda_\ell(E, 1)$ traversing the rim of $\Lambda_\ell^{\mathrm{ud}}(E, 1)$, one in each possible direction. Let us call

them ω_{rim}^+ and ω_{rim}^-. We denote $f_{rim}^+, f_{rim}^- \in R_m$ the isogenies associated to ω_{rim}^+ and ω_{rim}^-, respectively (with the usual sign ambiguity).

Remark 2.4.2. As explained at the beginning of this section, we are using the same notation, $\omega_{rim}^\pm$, to denote the several walks that start and end at any vertex along the rim. This shall not cause confusion as it is always understood what starting point is considered. Regardless of the starting point of ω_{rim}^+, f_{rim}^+ will be the same element of R_m under the natural identifications of the endomorphism rings of the elliptic curves on the rim.

Consider the homotopy equivalence relation defined on the set of walks in $\Lambda_\ell(E, 1)$ generated by relations

$$\omega_2 \omega_1 \sim_h \omega_2 \omega^\vee \omega \omega_1,$$

where ω_1, ω_2 are two walks such that the endpoint of ω_1 is the starting point of ω_2 (call it $[E_1]$), and ω is a walk starting at $[E_1]$. It is easy to see that Proposition 2.4.1 implies the following.

Corollary 2.4.3. *Every element in* $\Omega(\Lambda_\ell(E, 1), [E_1])$ *is equivalent under* $\sim_h$ *to a closed walk of the form*

$$\omega^\vee (\omega_{rim}^\pm)^n \omega,$$

where ω *is a path from* $[E_1]$ *to the rim of the graph, and* n *is a non-negative integer.*

Consider the map of directed graphs

$$\pi_N \colon \Lambda_\ell(\underline{E}, N) \to \Lambda_\ell(E, 1)$$

which sends a vertex $[(E_1, P_1)]$ to $[E_1]$, and an arrow $[(E_1, P_1)] \xrightarrow{\lambda} [(E_2, P_2)]$ to $[E_1] \xrightarrow{\lambda} [E_2]$. Note that for any N, and any vertex $[\underline{E}_1] \in \Lambda_\ell(\underline{E}, N)^V$, the arrows starting in $[\underline{E}_1]$ are in natural bijection with subgroups of order ℓ of E_1 and so π_N is a *covering map* of directed graphs. As such, many properties of $\Lambda_\ell(\underline{E}, N)$ can be deduced from the corresponding properties of $\Lambda_\ell(E, 1)$. For example, since the action of the operator T_ℓ on a point $[\underline{E}_1]$ can be described by $[\underline{E}_1] \mapsto \sum_{[\underline{E}_1] \to [\underline{E}_1']} [\underline{E}_1']$ (sum over arrows in $\Lambda_\ell^{ord}(N)$), the action of T_ℓ on $[\underline{E}_1] = [(E_1, P_1)]$ and $[E_1]$ are easily related.

3. The Hecke correspondence T_ℓ on ordinary elliptic curves

3.1. T_ℓ in characteristic 0. For what follows, the reader may consult [6] for a general introduction to deformation theory of abelian varieties and p-divisible groups, and [21] for the case of ordinary abelian varieties. In addition, the reference [10] provides a good introduction to rigid-analytic geometry, while the construction of the generic fibre of a formal scheme appears in [4].

Recall that $p \neq \ell$ are primes, and N is an integer coprime to $p\ell$. Let E be an ordinary elliptic curve defined over $\overline{\mathbb{F}}_p$. Assume that $\mathrm{Aut}(E) = \{\pm 1\}$. Let $\widetilde{D}(E) \cong \mathrm{Spf}(W(\overline{\mathbb{F}}_p)[[x]])$ be the deformation space of E defined over $W(\overline{\mathbb{F}}_p)$; it pro-represents the functor of deformations of E to local artinian rings $(R, \mathfrak{m}_R)$ with a given isomorphism $R/\mathfrak{m}_R \cong \overline{\mathbb{F}}_p$. Let $D(E) = \widetilde{D}(E)_{rig}$ denote the associated rigid-analytic space; it is isomorphic to the open unit disc over $W(\overline{\mathbb{F}}_p)[1/p]$. For an elliptic curve $\widetilde{E}$ lifting E, we define $D(\widetilde{E}) = D(E)$.

The same construction can be done for a pair $\underline{E} = (E, P)$, where E is as above, and P is a point of order N on E. Let $\widetilde{D}(\underline{E})$ denote the formal deformation space of $\underline{E}$ over $W(\overline{\mathbb{F}}_p)$, and let $D(\underline{E})$ be the associated rigid-analytic space. For $\widetilde{\underline{E}}$ lifting $\underline{E}$, we set $D(\widetilde{\underline{E}}) = D(\underline{E})$.

Since $E[N]$ is an étale group scheme over $\overline{\mathbb{F}}_p$, the forgetful map provides an isomorphism between the deformation space of $\underline{E}$ and E. Hence, the rigid-analytic forgetful map

$$\pi_N \colon D(\underline{E}) \to D(E)$$

is an isomorphism too.

When $N \geq 4$, the moduli of pairs $(\widetilde{E}, \widetilde{P})$ where $\widetilde{E}$ is an elliptic curve of good reduction over an $W(\overline{\mathbb{F}}_p)[1/p]$-algebra is represented by the (noncuspidal part) of the rigid-analytic modular curve $X_1(N)$. Let $X_1(N)_{\overline{\mathbb{F}}_p}$ be the corresponding modular curve over $\overline{\mathbb{F}}_p$. Let $\mathrm{sp} : X_1(N) \to X_1(N)_{\overline{\mathbb{F}}_p}$ denote the specialization map. Then, for any $\widetilde{\underline{E}} = (\widetilde{E}, \widetilde{P})$ of reduction $\underline{E} = (E, P)$, we have $D(\widetilde{\underline{E}}) = D(\underline{E}) = \mathrm{sp}^{-1}([\underline{E}])$, where $[\underline{E}]$ denotes the isomorphism class of $\underline{E}$ viewed as a point on $X_1(N)_{\overline{\mathbb{F}}_p}$.

When $N < 4$, there may be points $\underline{E} = (E, P)$ with a nontrivial automorphism group and the moduli space is no longer representable. We could still define coarse moduli spaces $X_1(N)$, $X_1(N)_{\overline{\mathbb{F}}_p}$, and a specialization map $\mathrm{sp} : X_1(N) \to X_1(N)_{\overline{\mathbb{F}}_p}$. In this case, we have $\mathrm{sp}^{-1}([\underline{E}]) = D(\underline{E})/\mathrm{Aut}(\underline{E})$.

We are interested in the p-adic dynamics of T_ℓ on the ordinary good reduction part of $X_1(N)$, or, to be more precise, on the set of $\mathbb{C}_p$-points of $\sqcup_{\underline{E}} D(\underline{E})$, where $\underline{E}$ runs over the isomorphism classes of ordinary elliptic curves over $\overline{\mathbb{F}}_p$ equipped with a point of order N. If $n > 0$ is an integer, the correspondence T_ℓ^n acts on $X_1(N)$ via the formula

$$T_\ell^n([(\widetilde{E}, \widetilde{P})]) = \sum_C \mu_C[(\widetilde{E}/C, P \bmod C)],$$

where C runs over all subgroups of $\widetilde{E}$ of order ℓ^n, $[(\widetilde{E}, \widetilde{P})]$ denotes the isomorphism class of $(\widetilde{E}, \widetilde{P})$, and μ_C are positive multiplicities that can be explicitly calculated.

3.2. Automorphisms of residue discs. Let $\alpha(N)$ be the order of ℓ in the group $(\mathbb{Z}/N\mathbb{Z})^\times$. Recall our standing assumption $(\star)$.

Lemma 3.2.1. *Let* $\lambda\colon \underline{E}_1 = (E_1, P_1) \to (E_2, P_2) = \underline{E}_2$ *be an* ℓ^n*-isogeny of elliptic curves over* $\overline{\mathbb{F}}_p$ *sending* P_1 *to* P_2*. There is a unique rigid-analytic isomorphism,*

$$\lambda^*\colon D(\underline{E}_1) \to D(\underline{E}_2),$$

such that for all $x = [(\widetilde{E}_1, \widetilde{P}_1)] \in D(\underline{E}_1)$*, we have* $\lambda^*(x) = [(\widetilde{E}_1/C, \widetilde{P}_1 \bmod C)]$*, where* C *is the unique subgroup of* $\widetilde{E}_1$ *lifting* $\mathrm{Ker}(\lambda)$*. The inverse of* λ^* *is given by* $(\deg(\lambda)^{\alpha(N)-1}\lambda^\vee)^*$*. If* $\underline{E}_1 = \underline{E}_2$ *and* $\lambda \in \mathbb{Z}$ *then* $\lambda^* = \mathrm{id}$*. For* $\lambda_1\colon \underline{E}_1 \to \underline{E}_2$*, and* $\lambda_2\colon \underline{E}_2 \to \underline{E}_3$ *we have* $(\lambda_2 \circ \lambda_1)^* = \lambda_2^* \circ \lambda_1^*$*.*

Proof. We claim there is a unique family of subgroup schemes $\widetilde{C}$ of order ℓ^n of the universal family of elliptic curves over $D(\underline{E}_1)$ with the following property: its specialization at every point $(\widetilde{E}_1, \widetilde{P}_1) \in D(\underline{E}_1)$ is a subgroup of $\widetilde{E}_1$ reducing to $\mathrm{Ker}(\lambda)$ in E_1. The morphism λ^* is then defined via dividing the universal family of elliptic curves on $D(\underline{E}_1)$ by the subgroup $\widetilde{C}$. More precisely, let $(\mathcal{E}_1, \mathcal{P}_1)$ be a formal deformation of (E_1, P_1) to a local artinian ring $(R, \mathfrak{m}_R)$ with a given isomorphism $R/\mathfrak{m}_R \cong \overline{\mathbb{F}}_p$. This data includes an isomorphism $\epsilon : \mathcal{E}_1 \otimes R/\mathfrak{m}_R \overset{\sim}{\to} E_1$ sending $\mathcal{P}_1$ to P_1. Since $(\ell, p) = 1$, $\mathrm{Ker}(\lambda)$ is an étale subgroup scheme of E_1, and hence it lifts uniquely to a subgroup $\mathcal{C}$ of the deformation $\mathcal{E}_1$. We define

$$\lambda^*(\mathcal{E}_1, \mathcal{P}_1) = (\mathcal{E}_1/\mathcal{C}, \mathcal{P}_1 \bmod \mathcal{C}),$$

where the right side is viewed as a formal deformation of (E_2, P_2) via the isomorphism

$$(\mathcal{E}_1/\mathcal{C}) \otimes R/\mathfrak{m}_R \overset{\epsilon}{\to} E_1/\mathrm{Ker}(\lambda) \to E_2,$$

where $E_1/\mathrm{Ker}(\lambda) \to E_2$ is the isomorphism induced by λ. This defines a morphism of the formal deformation spaces $\widetilde{\lambda}^* : \widetilde{D}(\underline{E}_1) \to \widetilde{D}(\underline{E}_2)$. The desired map is the rigid-analytic morphism λ^* associated to $\widetilde{\lambda}^*$. The uniqueness follows from the uniqueness of the lift of $\mathrm{Ker}(\lambda)$. The other statements follow easily from the construction and its uniqueness. $\qquad\square$

Let $\underline{E} = (E, P)$ be an ordinary elliptic curve over $\overline{\mathbb{F}}_p$ along with a point of order N. Let $\mathrm{End}_{\ell^\infty}(\underline{E})$ denote the monoid of ℓ-power isogenies of E fixing P. The above construction gives a monoid homomorphism

$$* : \mathrm{End}_{\ell^\infty}(\underline{E}) \to \mathrm{Aut}(D(\underline{E})).$$

sending λ to λ^*.

Proposition 3.2.2. *The kernel of* $*$ *is precisely* $\mathbb{Z} \cap \mathrm{End}_{\ell^\infty}(\underline{E})$*.*

Proof. Let $\lambda \in \mathrm{End}_{\ell^\infty}(\underline{E})$ such that $\lambda^* = 1$. From the construction of λ^* that means that for any lift $\widetilde{E}$ with its unique subgroup $\widetilde{C}$ lifting $C := \mathrm{Ker}(\lambda)$, we have $\widetilde{E}/C \cong \widetilde{E}$ and so that $\widetilde{E}$ has an endomorphism of degree $\sharp C$. As most lifts have only $\mathbb{Z}$ as endomorphisms, for some lift $\widetilde{E}$ we most have $\widetilde{C} = \mathrm{Ker}(\ell^n)$ and so $\lambda = \pm\ell^n$. The converse proceeds the same way. $\quad\square$

Using the above construction, we have a homomorphism of monoids (that we still denote $*$ hoping no confusion will arise)

$$* : \Omega(\Lambda_\ell(\underline{E}, N), \underline{E}) \to \mathrm{Aut}(D(\underline{E})),$$

sending ω to $\omega^* := \widetilde{\omega}^*$, where $\widetilde{\omega}$ is the isogeny associated to ω. Note that even when the isogeny $\widetilde{\omega}$ may only be defined up to sign, $\widetilde{\omega}^*$ is uniquely defined. More generally, if ω is a walk in $\Lambda(\underline{E}, N)$ of length d from $[\underline{E}_0]$ to $[\underline{E}_d]$, then ω^* can be similarly defined to be an isomorphism

$$(3.1) \qquad\qquad \omega^* : D(\underline{E}_0) \to D(\underline{E}_d).$$

induced by the walk ω. For two walks ω_1, ω_2 such that the endpoint of ω_1 is the starting point of ω_2, we have $(\omega_2 \circ \omega_1)^* = \omega_2^* \circ \omega_1^*$.

Proposition 3.2.3. *The image of $* : \Omega(\Lambda_\ell(\underline{E}, N), \underline{E}) \to \mathrm{Aut}(D(\underline{E}))$ is a cyclic group.*

Proof. Note that this image is a subgroup of the image of

$$* : \Omega(\Lambda_\ell(E, 1), [E]) \to \mathrm{Aut}(D(E)).$$

We prove that the image of the latter is cyclic. Note that for a walk ω_1 in $\Lambda_\ell(E, 1)$, we have $(\omega_1^\vee)^* = (\omega_1^*)^{-1}$. Consequently ω^* depends only on the class of ω under the equivalence relation $\sim_h$. Thus, applying Corollary 2.4.3, it follows that the image of $*$ is generated by an automorphism conjugate to $(\omega_{rim}^+)^*$. $\qquad\qquad\square$

Finally, we define

$$f : \Omega(\Lambda_\ell(E, 1), [E]) \to \mathbb{Z}_p^\times, \quad \omega \mapsto f_\omega,$$

where f_ω is the image of $\widetilde{\omega}$ under the map $\mathrm{End}(E) \to \mathrm{End}(T_p E) \cong \mathbb{Z}_p$. When $N \leq 2$, f_ω is defined only up to sign. We denote by $\bar{f}_\omega$ the image of $\overline{\widetilde{\omega}}$ in $\mathbb{Z}_p^\times$, where the bar sign denotes complex conjugation in $\mathrm{End}(E)$.

3.3. T_ℓ via walks. Let $n > 0$ be an integer. Let $\mathrm{Walk}(n, [\underline{E}])$ be the set of all walks of length n in $\Lambda_\ell(\underline{E}, N)$ starting at $\underline{E}$. For $\omega \in \mathrm{Walk}(n, [\underline{E}])$, let $[\underline{E}_\omega]$ denote its endpoint. The action of T_ℓ^n on the vertices of $\Lambda_\ell(\underline{E}, N)$ is then none other than $T_\ell^n([\underline{E}]) = \sum_{\omega \in \mathrm{Walk}(n, [\underline{E}])} [\underline{E}_\omega]$.

Proposition 3.3.1. *The correspondence T_ℓ^n on the residue disc $D(\underline{E})$ decomposes as a sum of rigid-analytic functions. More explicitly,*

$$T_\ell^n = \sum_{\omega \in \mathrm{Walk}(n, [\underline{E}])} \widetilde{\omega}^*,$$

where $\widetilde{\omega}^* : D(\underline{E}) \to D(\underline{E}_\omega)$ is the isomorphism defined in (3.1).

Proof. Proceeding by induction on n, it suffices to check the case $n = 1$. In this case, for any point $(\widetilde{E}, \widetilde{P})$ in $D(\underline{E})$ we have

$$T_\ell(\widetilde{E}, \widetilde{P}) = \sum_{C \subset \widetilde{E}} (\widetilde{E}/C, \widetilde{P} \bmod C),$$

where the summation is over all subgroups C of $\widetilde{E}$ of order ℓ (that correspond bijectively under reduction with the subgroups of $\underline{E}$ of order ℓ). On the other hand, the last sum is precisely $\sum_{\omega \in \mathrm{Walk}(1,[\underline{E}])} \widetilde{\omega}^*(\widetilde{E}, \widetilde{P})$, by Lemma 3.2.1. □

4. Dynamics of T_ℓ on ordinary points

4.1. Proposition 3.3.1 shows that the flow of the disc $D(\underline{E})$ under the iteration of T_ℓ is exactly like the flow of $\underline{E} \in \Lambda_\ell(\underline{E}, N)^V$ under the iteration of T_ℓ. The mass of $T_\ell^n(\underline{E})$ escapes to infinity. More precisely, we have the following proposition.

Proposition 4.1.1. *For $[\underline{E}] \in \Lambda_\ell(\underline{E}, N)^V$ and a positive integer n, define the probability measure*

$$\delta_n = \delta_{n,[\underline{E}]} = \frac{1}{\sharp \, \mathrm{Walk}(n, [\underline{E}])} \sum_{\omega \in \mathrm{Walk}(n,[\underline{E}])} \delta_{[\underline{E}_\omega]},$$

where $\delta_{[\underline{E}_\omega]}$ is the Dirac measure on $\Lambda_\ell(\underline{E}, N)^V$ concentrated at $[\underline{E}_\omega]$. Then, for any compactly supported function $f \colon \Lambda_\ell(\underline{E}, N)^V \to \mathbb{C}$, we have

$$\int f \mathrm{d}\delta_n \to 0 \quad \text{as } n \to \infty.$$

Proof. As π_N is a covering map that commutes with T_ℓ, it is enough to prove the statement for $N = 1$. In this case, we may further reduce the question to the ℓ-volcano $\Lambda_\ell(E, 1)$, where it follows from standard techniques of random walks; see, for example, [26, 31]. □

Therefore, the further study of the dynamics of T_ℓ on $D(\underline{E})$ is reduced to the study of the dynamics of branches of T_ℓ^n that bring the disc back to itself, or, equivalently, the branches corresponding to the closed walks of $\Lambda_\ell(\underline{E}, N)$. Let ω be a closed walk starting and ending at $[\underline{E}]$. Let $\overline{\omega}$ denote its image in $\Lambda_\ell(E, 1)$. It is clear from the definitions that we have a commutative diagram

$$
\begin{array}{ccc}
D(\underline{E}) & \xrightarrow{\omega^*} & D(\underline{E}) \\
{\cong}\downarrow{\scriptstyle \pi_N} & & {\cong}\downarrow{\scriptstyle \pi_N} \\
D(E) & \xrightarrow{\overline{\omega}^*} & D(E)
\end{array}
$$

This shows that the dynamics of ω^* on $D(\underline{E})$ is equivalent to the dynamics of $\overline{\omega}^*$ on $D(E)$. In view of Proposition 3.2.3, understanding the dynamics

of such functions boils down to understanding the dynamics of a single function on the open unit disc; that of the automorphism of $D(E)$ induced by ω_{rim}^{+}. In the following, for a closed walk ω in $\Lambda_\ell(E, 1)$, we explicitly calculate ω^* on $D(E)$ in terms of a coordinate on it.

Theorem 4.1.2. *There is a choice of local parameter t on $D(E)$ such that for any $\omega \in \Omega(\Lambda_\ell(E, 1), [E])$, the automorphism $\omega^* : D(E) \to D(E)$ is given by the map*

$$t \mapsto (1 + t)^{\bar{f}_\omega / f_\omega} - 1$$

where $f_\omega \in \mathbb{Z}_p^\times$ is defined in Section 3.2. Such a map is an isometry of the disc.

The theorem follows from the following Lemma.

Lemma 4.1.3. *Let κ be a field of characteristic p, and $(\bar{A}, \mu_{\bar{A}})$ be a principally polarized ordinary abelian scheme of dimension g over κ. Fix an isomorphism $T_p \bar{A} \cong \mathbb{Z}_p^g$. Let*

$$f : \bar{A} \to \bar{A}$$

be an isogeny of degree n prime to p, and $f^\dagger$ denote the image of f under the Rosati involution induced by $\mu_{\bar{A}}$. Let $M(f^{-1}) = (f_{ij})_{i,j} \in \mathrm{GL}_g(\mathbb{Z}_p)$ (respectively, $M(f^\dagger) = (g_{ij})_{i,j}$) denote the matrix of the automorphism on $T_p \bar{A} \cong \mathbb{Z}_p^g$ induced by f^{-1} (respectively, $f^\dagger$). Let f denote the automorphism of the deformation space D of $(\bar{A}, \mu_{\bar{A}})$ induced by $f : \bar{A} \to \bar{A}$. There is an isomorphism $D \cong \mathrm{Spf}[[t_{ij}]]_{i,j}$ under which the automorphism f takes the shape

$$f^*(t_{ij}) = \prod_{1 \le r,s \le g} (1 + t_{rs})^{f_{ri} g_{sj}} - 1 \qquad 1 \le i, j \le g.$$

Proof. Let $\mathcal{C}_\kappa$ denote the category of local Artin rings $(R, \mathfrak{m}_R)$ such that $R/\mathfrak{m}_R = \kappa$. By Serre–Tate's theory of deformation of ordinary abelian varieties, deformations of $\bar{A}$ over R are in correspondence with the elements of $\mathrm{Hom}_{\mathbb{Z}_p}(T_p \bar{A} \otimes_{\mathbb{Z}_p} T_p \bar{A}^\vee, \widehat{\mathbb{G}}_m(R))$, where $\widehat{\mathbb{G}}_m$ denotes the multiplicative formal group over R. We briefly recall (following [21]) how a bilinear form $\eta_A \in \mathrm{Hom}_{\mathbb{Z}_p}(T_p \bar{A} \otimes_{\mathbb{Z}_p} T_p \bar{A}^\vee, \widehat{\mathbb{G}}_m(R))$ is associated to a deformation A of $\bar{A}$ over $R \in \mathcal{C}_\kappa$. By Serre–Tate's theory of deformation of abelian varieties [21] (See also [23, Appendix]), to give a deformation $\bar{A}$ over R is equivalent to give a deformation $A[p^\infty]$ of $\bar{A}[p^\infty]$ over R. This, in turn, is equivalent to giving an extension

$$0 \to \widehat{A} \to A[p^\infty] \to T_p \bar{A} \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p / \mathbb{Z}_p) \to 0,$$

where $\widehat{A}$, the formal group of A, is isomorphic to the unique toroidal formal group lifting $\widehat{\bar{A}}$. Every such extension is the push-out of the canonical

extension

$$0 \to T_p\overline{A} \to T_p\overline{A} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to T_p\overline{A} \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p) \to 0$$

by a unique map

$$\phi_A : T_p\overline{A} \to \widehat{A}(R)$$

defined as follows. Choose N such that $\mathfrak{m}_R^{N+1} = 0$, and note that $\widehat{A}(R)$ is killed by p^N, as $p \in \mathfrak{m}_R$. Let $x = (x_n)$ be an element of $T_p\overline{A}$. Pick $n \geq N$, and let $\widetilde{x}_n$ be an arbitrary lift of $x_n \in \overline{A}(\overline{\mathbb{F}}_p)$ to $A(R)$. We define $\phi_A(x) = p^n\widetilde{x}_n$ which is easily seen to be independent of the choice of $n \geq N$. The definition is independent of the choice of $\widetilde{x}_n$, as any two choices differ by an element on $\widehat{A}(R)$ which is killed by p^N. Also, $\phi_A(x)$ lies in $\widehat{A}(R)$ since its reduction mod $\mathfrak{m}_R$ is zero by construction. Finally, we use the Weil pairing to identify $\widehat{A}(R)$ with $\mathrm{Hom}(T_p\overline{A}^\vee, \widehat{\mathbb{G}}_m(R))$ (this identification is valid over κ, and can be lifted to R since $\widehat{A}$ is of multiplicative type). This re-interprets $\phi_A : T_p\overline{A} \to \widehat{A}(R)$ as a bilinear form

$$\eta_A \in \mathrm{Hom}_{\mathbb{Z}_p}(T_p\overline{A} \otimes_{\mathbb{Z}_p} T_p\overline{A}^\vee, \widehat{\mathbb{G}}_m(R)).$$

First we claim the following general statement. Let $\delta : A_1 \to A_2$ be a prime-to-p isogeny of principally polarized ordinary abelian schemes over $R \in \mathcal{C}_\kappa$, and $\delta : \overline{A}_1 \to \overline{A}_2$ be its reduction. Then the following diagram

$$
\begin{array}{ccc}
T_p\overline{A}_1 \otimes_{\mathbb{Z}_p} T_p\overline{A}_1^\vee & \xrightarrow{\eta_{A_1}} & \widehat{\mathbb{G}}_m(R) \\
\Big\downarrow{\scriptstyle \delta\otimes(\delta^\vee)^{-1}} & & \Big\| \\
T_p\overline{A}_2 \otimes_{\mathbb{Z}_p} T_p\overline{A}_2^\vee & \xrightarrow{\eta_{A_2}} & \widehat{\mathbb{G}}_m(R)
\end{array}
$$

is commutative. The commutativity follows from the commutativity of the following diagram (which itself follows from the construction):

$$
\begin{array}{ccccc}
T_p\overline{A}_1 & \xrightarrow{\phi_{A_1}} & \widehat{A}_1(R) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_p}(T_p\overline{A}_1^\vee, \widehat{\mathbb{G}}_m(R)) \\
\Big\downarrow{\scriptstyle \delta} & & \Big\downarrow{\scriptstyle \delta} & & \Big\downarrow{\scriptstyle (\delta^\vee)^*} \\
T_p\overline{A}_2 & \xrightarrow{\phi_{A_2}} & \widehat{A}_2(R) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_p}(T_p\overline{A}_2^\vee, \widehat{\mathbb{G}}_m(R))
\end{array}
$$

Going back to the proof, let $\overline{C}$ denote the kernel of the isogeny f, and $\pi : \overline{A} \to \overline{A}/\overline{C}$ be the canonical projection. There is a unique isomorphism $\lambda : \overline{A}/\overline{C} \xrightarrow{\sim} \overline{A}$ such that $f = \lambda \circ \pi$. Let (A, C) be a deformation of $(\overline{A}, \overline{C})$ to $R \in \mathcal{C}_\kappa$, which implies that A/C is a deformation of $\overline{A}/\overline{C} \cong \overline{A}$ to R. By the above discussion, to deformations $A, A/C$ of $\overline{A}$, we can associate bilinear

forms

$$\eta_A \in \mathrm{Hom}_{\mathbb{Z}_p}(T_p\overline{A} \otimes_{\mathbb{Z}_p} T_p\overline{A}^\vee, \widehat{\mathbb{G}}_m(R))$$

$$\eta_{A/C} \in \mathrm{Hom}(T_p(\overline{A}/\overline{C}) \otimes_{\mathbb{Z}_p} T_p((\overline{A}/\overline{C})^\vee), \widehat{\mathbb{G}}_m(R)).$$

Define $\eta'_{A/C} := \eta_{A/C} \circ \underline{\lambda}^{-1}$, where

$$\underline{\lambda} : T_p(\overline{A}/\overline{C}) \otimes_{\mathbb{Z}_p} T_p(\overline{A}/\overline{C})^\vee \to T_p\overline{A} \otimes_{\mathbb{Z}_p} T_p\overline{A}^\vee$$

is given by $\lambda \otimes (\lambda^\vee)^{-1}$. Similarly, define $\underline{\pi} = \pi \otimes (\pi^\vee)^{-1}$. From the above discussion, it follows that the following diagram is commutative:

$$
\begin{array}{ccc}
T_p\overline{A} \otimes_{\mathbb{Z}_p} T_p\overline{A}^\vee & \xrightarrow{\;\eta'_{A/C}\;} & \widehat{\mathbb{G}}_m(R) \\
{\scriptstyle\underline{\lambda}}\big\uparrow & & \big\| \\
T_p(\overline{A}/\overline{C}) \otimes_{\mathbb{Z}_p} T_p((\overline{A}/\overline{C})^\vee) & \xrightarrow{\;\eta_{A/C}\;} & \widehat{\mathbb{G}}_m(R) \\
{\scriptstyle\underline{\pi}}\big\uparrow & & \big\| \\
T_p\overline{A} \otimes_{\mathbb{Z}_p} T_p\overline{A}^\vee & \xrightarrow{\;\eta_A\;} & \widehat{\mathbb{G}}_m(R)
\end{array}
$$

Let $\{v_i\}_i$ be the standard basis for $T_p\overline{A}$ under our fixed isomorphism $T_p\overline{A} \cong \mathbb{Z}_p^g$, and let $\{w_i = \mu_{\overline{A}}(v_i)\}_i$ be the corresponding basis for $T_p\overline{A}^\vee$. Let $M(f^{-1}) = (f_{ij}) \in \mathrm{GL}_g(\mathbb{Z}_p)$ be the matrix of inverse of the map induced by f on $T_p\overline{A}$ in this basis. Let $f^\dagger = \mu_{\overline{A}}^{-1} \overline{f} \mu_{\overline{A}}$ denote the image of f under the Rosati involution associated to $\mu_{\overline{A}}$. Let $M^\vee(f^\vee)$ denote the matrix, with respect to $\{w_i\}$, of the map induced map by $f^\vee$ on $T_p\overline{A}^\vee$. This matrix can be calculated as follows. We have

$$f^\vee(w_i) = \mu_{\overline{A}}(\mu_{\overline{A}}^{-1} f^\vee \mu_{\overline{A}})(v_i) = \mu_{\overline{A}}(f^\dagger(v_i)),$$

which shows that $M^\vee(f^\vee) = M(f^\dagger) = (g_{ij})^{-1}$. There is an isomorphism $D \cong \mathrm{Spf}[[t_{ij}]]$, where for any deformation A over any $R \in \mathcal{C}_\kappa$ we have $1 + t_{ij}(A) = \eta_A(v_i \otimes w_j)$. To calculate $f^*(t_{ij})$, we use the above diagram to write

$$\eta'_A(v_i \otimes w_j) = \eta_A(f^{-1}(v_i) \otimes f^\vee(w_j))$$

$$= \eta_A\left(\sum_r f_{ri}v_r \otimes \sum_s g_{sj}w_s\right) = \prod_{r,s} \eta_A(v_r \otimes w_s)^{f_{ri}g_{sj}}$$

which proves the statement of the lemma. $\qquad\square$

4.2. Periodic points: canonical and quasi-canonical lifts. Let E be an ordinary elliptic curve over $\overline{\mathbb{F}}_p$. Then $\operatorname{End}(E)$ is isomorphic to an order of a prime-to-p conductor $\mathfrak{f}(E)$ in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free negative integer. There is a unique (up to isomorphism) elliptic curve $\widetilde{E}_{can}$ over $W(\overline{\mathbb{F}}_p)$ lifting E such that the natural reduction map

$$\operatorname{End}(\widetilde{E}_{can}) \to \operatorname{End}(E)$$

is an isomorphism. This elliptic curve is called the *canonical lift* of E. A lift $\widetilde{E}$ of $E/\overline{\mathbb{F}}_p$ is called *quasi-canonical* if the image of the reduction map $\operatorname{End}(\widetilde{E}) \to \operatorname{End}(E)$ is an order in $\operatorname{End}(E)$; its conductor is necessarily of the form $p^a \mathfrak{f}(E)$ for some $a \geq 0$. The case $a = 0$ corresponds to the canonical lift.

Let $\underline{E} = (E, P)$ consist of an ordinary elliptic curve E over $\overline{\mathbb{F}}_p$ and a point P of order N on E. We say $\underline{\widetilde{E}} = (\widetilde{E}, \widetilde{P})$ is a (quasi-) canonical lift of $\underline{E}$ if $\widetilde{E}$ is a (quasi-) canonical lift of E. Since $(p, N) = 1$, the point P can be uniquely lifted, and hence there is a unique canonical lift of $\underline{E}$ which we denote by $\underline{\widetilde{E}}_{can}$. We write $\widetilde{D}(\underline{E}) \cong \operatorname{Spf}(W(\overline{\mathbb{F}}_p)[[t]])$, where t is the Serre–Tate coordinate on $\widetilde{D}(\underline{E})$. We prove the following.

Proposition 4.2.1. *Let notation be as above.*

    (1) *We have $t(\underline{\widetilde{E}}_{can}) = 0$.*

    (2) *$\underline{\widetilde{E}}$ is a quasi-canonical lift of $\underline{E}$ of conductor $p^a \mathfrak{f}(E)$ if and only if $1 + t(\underline{\widetilde{E}})$ is a primitive p^a-th root of unity.*

In other words, $D(\underline{E})$ is isomorphic to the open unit disc around 1, the canonical lift corresponds to 1, and the other quasi-canonical lifts correspond to the nontrivial p-power roots of unity.

Proof. We will use the Serre–Tate theory of local moduli of ordinary abelian varieties. We refer to the proof of Lemma 4.1.3 for a summary of their construction and for notation. First we recall the following fact (see [21]). Let A_1 and A_2 be abelian varieties over $\overline{\mathbb{F}}_p$, and $\widetilde{A}_1, \widetilde{A}_2$, respective lifts corresponding to pairings $\eta_{\widetilde{A}_1}, \eta_{\widetilde{A}_2}$. Let $\delta \colon A_1 \to A_2$ be a morphism. Then δ lifts to a morphism $\widetilde{\delta} \colon \widetilde{A}_1 \to \widetilde{A}_2$ if and only if for all $v \in T_p A_1, w \in T_p A_2^\vee$ we have

$$\eta_{\widetilde{A}_1}(\delta(v), w) = \eta_{\widetilde{A}_2}(v, \delta^\vee(w)).$$

We will apply this with $A_1 = A_2 = E$. Consider E with its canonical polarization and hence a canonical isomorphism $T_p E \xrightarrow{\sim} T_p E^\vee$. Under this identification, for any $\delta \in \operatorname{End}(E)$, the dual isogeny $\delta^\vee \in \operatorname{End}(E^\vee)$ is identified with $\bar{\delta} \in \operatorname{End}(E)$. Let v be a basis element in $T_p E$. This provides us with the Serre–Tate isomorphism

$$\widetilde{D}(\underline{E}) \cong \widetilde{D}(E) \cong \operatorname{Spf}(W(\overline{\mathbb{F}}_p)[[t]]),$$

where for any lift $(\widetilde{E})$ of $(\underline{E})$, we have $1 + t(\widetilde{E}) = \eta_{\tilde{E}}(v, v)$.

In our notation, $\mathrm{End}^0(E) = K = \mathbb{Q}(\sqrt{d})$, d square-free. If $d \equiv 2, 3$ (mod 4) let $\gamma = \sqrt{d}$, and if $d \equiv 1$ (mod 4) let $\gamma = (1 + \sqrt{d})/2$. Thus, $\mathcal{O}_K = \mathbb{Z} + \gamma\mathbb{Z}$. The lift $\widetilde{E}$ is a quasi-canonical lift of $\underline{E}$ of conductor dividing $p^a \mathfrak{f}(E)$ in K if and only if $\alpha = p^a \mathfrak{f}(E)\gamma$ can be lifted from $\mathrm{End}(E)$ to $\mathrm{End}(\widetilde{E})$. This is equivalent to having $\eta_{\tilde{E}}(\alpha v, v) = \eta_{\tilde{E}}(v, \overline{\alpha}v) = \eta_{\tilde{E}}(\overline{\alpha}v, v)$, which is equivalent to

$$\eta_{\tilde{E}}(v, v)^{\alpha - \overline{\alpha}} = (1 + t(\widetilde{E}))^{\alpha - \overline{\alpha}} = 1.$$

If $d \equiv 2, 3$ (mod 4), we have $(1 + t(\widetilde{E}))^{\alpha - \overline{\alpha}} = (1 + t(\widetilde{E}))^{2p^a \mathfrak{f}(E)\sqrt{d}}$; if $d \equiv 1$ (mod 4), we have $(1 + t(\widetilde{E}))^{\alpha - \overline{\alpha}} = (1 + t(\widetilde{E}))^{p^a \mathfrak{f}(E)\sqrt{d}}$.

If $p \neq 2$, taking into account that p splits in K, we find that $2\mathfrak{f}(E)\sqrt{4d}$, respectively $\mathfrak{f}(E)\sqrt{d}$, are p-adic units, and so $(1 + t(\widetilde{E}))^{\alpha - \overline{\alpha}} = 1$ if and only if $(1 + t(\widetilde{E}))^{p^a} = 1$. If $p = 2$, then since p splits in K, we must have $d \equiv 1$ (mod 4) and, again, $(1 + t(\widetilde{E}))^{\alpha - \overline{\alpha}} = 1$ if and only if $(1 + t(\widetilde{E}))^{p^a} = 1$.

This proves the second part of the Proposition. For the first part, simply put $a = 0$, to obtain $1 + t(\widetilde{E}_{can}) = 1$. $\qquad \square$

Let $\mathrm{ord} = \mathrm{ord}_p$ denote the p-adic valuation on $\overline{\mathbb{Q}}_p$, normalized so that $\mathrm{ord}(p) = 1$.

Proposition 4.2.2. *Let $\omega \in \Omega(\Lambda_\ell(\underline{E}, N), [\underline{E}])$ be such that $\omega^* \in \mathrm{Aut}(D(\underline{E}))$ is nontrivial. Consider the dynamics of $\{(\omega^*)^n\}_{n \geq 1}$ on $D(\underline{E})$. The following hold:*

(1) *Every pre-periodic point in $D(\underline{E})$ is periodic.*
(2) *Let $m > 0$ be an integer. The index $[\mathcal{O}_K : \mathbb{Z}[\widetilde{\omega}^m]] < \infty$ unless, possibly, when $K = \mathbb{Q}(\sqrt{-\ell})$. If $K = \mathbb{Q}(\sqrt{-\ell})$ then $\widetilde{\omega} = \pm(-\ell)^{b/2}$ for some odd positive integer b, and $[\mathcal{O}_K : \mathbb{Z}[\widetilde{\omega}^m]] = \infty$ if and only if m is even.*
(3) *Assume that $[\mathcal{O}_K : \mathbb{Z}[\widetilde{\omega}^m]] < \infty$, then the periodic points in $D(\underline{E})$ of order dividing m are exactly the quasi-canonical points of $D(\underline{E})$ of conductor dividing $[\mathcal{O}_K : \mathbb{Z}[\widetilde{\omega}^m]]$. In terms of the Serre–Tate coordinate t, these correspond to points $\widetilde{\underline{E}} \in D(\underline{E})$ for which $(1 + t(\widetilde{E}))^{p^a} = 1$, where $a = \mathrm{ord}_p([\mathrm{End}(E) : \mathbb{Z}[\widetilde{\omega}^m]])$.*
(4) *If $[\mathcal{O}_K : \mathbb{Z}[\widetilde{\omega}^m]] = \infty$ any point is a periodic point of order dividing m.*

Proof. First, note that all pre-periodic points are periodic simply because $\omega^* \in \mathrm{Aut}(D(\underline{E}))$. To prove claim (2) note that $\widetilde{\omega}$ is a non-integer integral element of K (thus generating K over $\mathbb{Q}$) whose norm is ℓ^n for some $n > 0$. If $[\mathcal{O}_K : \mathbb{Z}[\widetilde{\omega}^m]] = \infty$ then $\widetilde{\omega}^m = \pm\ell^{mn/2}$. This implies that the discriminant of K divides $-4\ell^n$ and so the discriminant of K, which is not -3 or -4,

must be equal to $-\ell$ or -4ℓ if ℓ is odd, and -8 if $\ell = 2$. This implies that $K = \mathbb{Q}(\sqrt{-\ell})$. The rest of (2) is clear.

Let $\underline{\widetilde{E}} = (\widetilde{E}, \widetilde{P}) \in D(\underline{E})$. It follows from the construction of ω^* that $(\omega^*)^m(\underline{\widetilde{E}}) = \underline{\widetilde{E}}$ if and only if $\widetilde{\omega}^m \in \operatorname{End}(E)$ can be lifted to an endo-morphism of $\widetilde{E}$. If $\widetilde{\omega}^m$ is not an integer, this is equivalent to $\underline{\widetilde{E}}$ being a quasi-canonical lift with endomorphism ring containing $\mathbb{Z}[\widetilde{\omega}^m] \subset \operatorname{End}(E)$, i.e., $\underline{\widetilde{E}}$ being a quasi-canonical lift of conductor dividing $[\mathcal{O}_K : \mathbb{Z}[\widetilde{\omega}^m]]$. In terms of the Serre–Tate coordinate, we have already seen in the proof of Proposition 4.2.1 that $(1 + t(\underline{\widetilde{E}}))^{p^a} = 1$ if and only if $\widetilde{E}$ is a quasi-canonical lift of conductor dividing $p^a \mathfrak{f}(E)$. If $\widetilde{\omega}^m$ is an integer then every point is m-periodic. The rest follows immediately. $\square$

Corollary 4.2.3. *The T_ℓ-forward orbit of any CM point $\underline{\widetilde{E}}$ with ordinary reduction and conductor $p^a \mathfrak{f}(\underline{\widetilde{E}})$ is a discrete set, intersecting each residue disc at a finite set contained in the p^a-roots of unity (relative to the Serre–Tate coordinate). The prime-to-ℓ part of the conductor of the endomorphism ring in such an orbit is an invariant.*

4.3. Closure of orbits and CM.

Proposition 4.3.1. *Let $\underline{E} = (E, P)$ be an elliptic curve of ordinary reduc-tion over $\mathbb{C}_p$. Let $K = \operatorname{End}^0(E)$.*

  (1) *If K is a CM field, the orbit of $\underline{E}$ under T_ℓ is a discrete set consist-ing only of elliptic curves with the same endomorphism algebra K. Consequently, any point in the closure of the orbit of $\underline{E}$ has CM by an order whose conductor differs from that of $\operatorname{End}(E)$ only at ℓ.*
  (2) *If $K = \mathbb{Q}$, no point in the closure of the orbit of $\underline{E}$ under T_ℓ has CM.*

Proof. Corollary 4.2.3 contains (1), since p-power roots of unity form a discrete set of the unit disc. Consider then the case $K = \mathbb{Q}$. Suppose that there is a CM point $\underline{E}_0$ in the closure of the orbit of $\underline{E}$. Let $F = \operatorname{End}^0(E_0)$ and let p^a be the p-part of the conductor of $\operatorname{End}(E_0)$ in F.

We claim that $F = \operatorname{End}^0(\overline{E})$ where $\overline{E}$ is the reduction of E modulo the maximal ideal of $\mathbb{C}_p$. Indeed, since $\underline{E}_0$ is in the closure of the orbit of $\underline{E}$ there is an ℓ-isogeny, $\underline{E} \to \underline{E}_1$, where $\underline{E}_1$ is in the residue disc $D(\underline{E}_0)$, and so $F = \operatorname{End}^0(\overline{E}_0) = \operatorname{End}^0(\overline{E}_1) = \operatorname{End}^0(\overline{E})$.

Let S be the set of all CM points that are quasi-canonical lifts of $\overline{E}$, with conductor whose p-part is p^a. They and $\underline{E}$ belong to the same residue disc $D(\underline{E})$. Let

$$\operatorname{dist}(\underline{E}, S) = \{\operatorname{dist}(\underline{E}, s) : s \in S\},$$

where we view here the residue disc as a subset of $\mathbb{C}_p$ by means of a Serre–Tate coordinate, $\underline{E}$ and s are elements of $\mathbb{C}_p$, and the distance is the p-adic metric. Note that $\operatorname{dist}(S)$ is a finite set of *positive* real numbers.

Now, let f be an ℓ-isogeny $\underline{E} \to \underline{E}'$ such that $\underline{E}' \in D(\underline{E}_0)$. The induced isomorphism of residue discs $f^*: D(\underline{E}) \to D(\underline{E}_0)$ is an *isometry*.[1] Thus, $\mathrm{dist}(\underline{E}, S) = \mathrm{dist}(\underline{E}', f^*(S))$. Moreover, by a counting argument, $f^*(S)$ consists of *all* quasi-canonical lifts in $D(\underline{E}_0)$ with p part of the conductor being p^a. Thus, $\underline{E}_0 \in f^*(S)$ and we find that $\mathrm{dist}(\underline{E}', \underline{E}_0)$ is bounded from below regardless of f. This is a contradiction. □

4.4. Dynamics of $t \mapsto (1+t)^\lambda - 1$. As we have seen, the action of the Hecke operator T_ℓ on points of ordinary reduction reduces, essentially, to the study of an automorphism of the open disc of radius 1, which is of the form $t \mapsto \omega^*(t) = (1+t)^{\bar{f}_\omega / f_\omega} - 1$. Therefore, we now direct our attention to automorphisms of the disc of the form

$$t \mapsto h(t) := (1+t)^\lambda - 1, \quad \lambda \in \mathbb{Z}_p^\times.$$

Recall that $(1+t)^\lambda = \sum_{n \geq 0} \binom{\lambda}{n} t^n$, where $\binom{\lambda}{n} = \frac{\lambda(\lambda-1)\dots(\lambda-n+1)}{n!}$.

The nature of the orbit $\{h^n(x) : n \in \mathbb{Z}\}$ is best understood through a sequence of reductions that while providing a complete picture also convince the reader that formulating a quantitive answer in the general case is too messy.

Thus, let F be a finite extension of $\mathbb{Q}_p$ with a residue field of degree p^f and ramification index e. Let $\mathfrak{m}_F$ be the maximal ideal of F. Define for $n \geq 1$,

$$U_n = 1 + \mathfrak{m}_F^n \subset \mathcal{O}_F^\times.$$

We have a decomposition:

$$\mathcal{O}_F^\times = \mu_{p^f - 1} \times U_1.$$

We change coordinate so that the centre is 1, and so our map in the new coordinate (still called t) is simply

$$t \mapsto h(t) = t^\lambda.$$

Let $x \in \mathcal{O}_F^\times$; since x should reduce to 1, we take $x \in U_1$. The group U_1 has a non-canonical decomposition

$$U_1 = \mu_{p^a} \times U',$$

where U' is isomorphic as a $\mathbb{Z}_p$-module to $\mathbb{Z}_p^g$, $g = [F : \mathbb{Q}_p]$. The action of h respects this decomposition and we see that at the expense of passing from λ to λ^{p^a} (which will result in decomposing the orbit into a union of finitely many translated-orbits for λ^{p^a}),

- *We may reduce to the case $x \in U'$.*

---

[1] Any automorphism of the open unit disc defined over a discretely valued field extension of $\mathbb{Q}_p$ is an isometry.

Choose an $n_0 > \frac{e}{p-1}$ and a sufficiently large n_1. The homomorphism

$$U' \to U_{n_0}, \qquad x \mapsto x^{p^{n_1}},$$

is a homeomorphism from U' into an open subgroup of finite index of U_{n_0} that commutes with h. To stress, it is injective. Thus, we accept the next reduction:

- *We may reduce to the case $x \in U_{n_0}$.*

Now, the logarithm function, $\log(t) = \sum_{n \geq 1} (-1)^{n-1} \frac{t^n}{n}$, converges on U_1. If $n > \frac{e}{p-1}$, then

$$\log : U_n \xrightarrow{\sim} \mathfrak{m}_F^n$$

is an isometry whose inverse is given by $\exp(t) = \sum_{n \geq 1} \frac{t^n}{n!}$. That explains our interest in assuming that $x \in U_{n_0}$. Thus, by applying the logarithm, the orbit $\{x^{\lambda^n} : n \in \mathbb{Z}\}$ is transformed into the orbit

$$\{\log(x) \cdot \lambda^n : n \in \mathbb{Z}\} = \log(x) \cdot \{\lambda^n : n \in \mathbb{Z}\}.$$

And so we accept the next reduction.

- *The essential information about the orbit of $h(x)$ is contained in the properties of the subset of $\mathbb{Z}_p^\times$ given by $\{\lambda^n : n \in \mathbb{Z}\}$.*

This last question is uniform. It doesn't know about x or F. Unfortunately, also here we run into similar book-keeping issues, and so once again we satisfy ourselves with a reduction that comes from the decomposition $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$.

- *We may reduce to the case $\lambda \in (1 + p\mathbb{Z}_p)$.*

Finally, by applying the logarithm, we find that

- *The set $\{\lambda^n : n \in \mathbb{Z}\}$ in $1 + p\mathbb{Z}_p$ is mapped bijectively to the set $\log(\lambda) \cdot \mathbb{Z}$ in $p\mathbb{Z}_p$, whose closure is a disc in $p\mathbb{Z}_p$ of radius $p^{-\operatorname{ord}(\lambda-1)}$, centred at $\log(\lambda)$.*

Without getting bogged down in the details, we can conclude the following:

Proposition 4.4.1. *Assume that x is not a root of unity.*

(1) *The closure of the orbit of any point x under ω^* is equal to a finite disjoint union of sets, each homeomorphic to $\mathbb{Z}_p$.*

(2) *In contrast to the case of a CM point, where the orbit is countable and discrete, the closure of the orbit of x under iterations of T_ℓ is of cardinality $2^{\aleph_0}$.*

5. The ℓ-isogeny graph: the supersingular case

5.1. Some notation. Recall our choice of a fixed prime number p. In the following, E, E_1, and so on, will typically denote supersingular elliptic curves in characteristic p. We denote $\operatorname{Frob}_E : E \to E^{(p)}$ the Frobenius

isogeny; occasionally we denote it φ for simplicity of notation. We denote $B = B_{p,\infty}$ the quaternion algebra over $\mathbb{Q}$ ramified precisely at p and ∞ and denote $\mathscr{B}$ its p-adic completion $B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_p$; $\mathcal{R}$ will denote a maximal order of $B_{p,\infty}$ and $\mathscr{R}$ its p-adic completion. The order $\mathcal{R}$ is not unique but $\mathscr{R}$ is. Let $q = p^2$ and $\mathbb{F}_q$ a field of cardinality q in a fixed algebraic closure $\overline{\mathbb{F}}_p$. Denote $\mathbb{Q}_q = W(\mathbb{F}_q)[p^{-1}]$. When we talk about $\overline{\mathbb{Q}}_p$ we have in mind an algebraic closure containing $W(\overline{\mathbb{F}}_p)$ and $\mathbb{C}_p$ denotes its completion.

5.2. Definition of supersingular graphs. As in the ordinary case, in addition to the fixed prime p, we now fix a prime ℓ, and a positive integer N, such that $p \neq \ell$, $(N, p\ell) = 1$. Although some of the results below apply to the case $\ell = 2$, some of the literature we are using necessitates assuming ℓ is odd and so we assume that from this point on. Recall that $\alpha(N)$ denotes the order of ℓ in the group $\mathbb{Z}/N\mathbb{Z}^\times$.

Definition 5.2.1. A pair (N, p) is called *rigid* if for every supersingular elliptic curve E, and $P \in E[N]$ of order N, we have $\mathrm{Aut}(E, P) = \{1\}$. It is called *solid* if $\mathrm{Aut}(E, P) \subseteq \{\pm 1\}$. If p is clear from the context, we shall simply say N is rigid, or solid.

The classification of automorphism groups of elliptic curves (see [28, III, Section 10]) implies:

Lemma 5.2.2. *If (N, p) is rigid it is solid. Further:*
  (1) *If $N = 1$, then (N, p) is never rigid and is solid iff $p \equiv 1 \pmod{12}$.*
  (2) *If $N = 2$, then (N, p) is never rigid and is solid iff $p \equiv 1 \pmod 4$.*
  (3) *If $N = 3$, then (N, p) is solid iff $p \equiv 1 \pmod 3$. If it is solid then it is rigid.*
  (4) *If $N > 3$, then (N, p) is rigid.*

To define supersingular graphs in a very concrete way, we make use of the following.

Lemma 5.2.3. *Every supersingular elliptic curve has a model E over $\mathbb{F}_{p^2}$ such that $\mathrm{Frob}_E^2 = p$, unique up to $\mathbb{F}_{p^2}$-isomorphisms.*

Proof. [2] Let $\varphi = \mathrm{Frob}_E$. This Lemma is well-known for $\varphi^2 = -p$; cf. Serre [27, p. 284], [1, Lemma 3.20]. The variant $\varphi^2 = p$ is obtained for $p > 2$ by a quadratic twist. Even for $p = 2$ we can pass from $\varphi^2 = -p$ to $\varphi^2 = p$, but this time by twisting by the element of $H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_p/\mathbb{F}_q}, \mathrm{Aut}(E))$ that sends Frobenius to i, an automorphism of order 4 of E. $\qquad\square$

We fix such elliptic curves as representatives for the $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves. Given N, we extend this choice to a choice of representatives (E, P) for the $\overline{\mathbb{F}}_p$-isomorphism classes of pairs

---

[2]We have learned of this nice fact from a post of Bjorn Poonen on Mathoverflow.

(E_1, P_1), where E_1 is supersingular and P_1 is a point of E_1 of order N. There is no canonical way to choose the points P, and so we make an arbitrary choice once and for all, and call the set of representatives $Rep(N)$. For a representative E, the number of representatives $(E, P) \in Rep(N)$ is the number of orbits of $\operatorname{Aut}(E)$ acting on the points of order N in E.

We now define the *supersingular graph* $\Lambda_\ell(N)$ *of level N*. The set of vertices $\Lambda_\ell(N)^V$ of $\Lambda_\ell(N)$ is the set $\operatorname{Rep}(N)$ we have fixed above. The construction is such that $\Lambda_\ell(N)$ will be a directed graph, whose arrows are labeled, and we describe its arrows in two equivalent ways.

(1) For every vertex (E, P), and a cyclic subgroup C of E of order ℓ, draw an arrow from the vertex (E, P) to the unique representative (E_1, P_1) of $(E/C, P \bmod C)$. Let $\pi_C \colon E \to E/C$ be the canonical map, and let $\alpha \colon E/C \to E_1$ be an isomorphism such that $\alpha(\pi_C(P)) = P_1$. Note the morphism $\lambda = \alpha \circ \pi_C \colon (E, P) \to (E_1, P_1)$. It is unique up to composition with elements of $\operatorname{Aut}(E_1, P_1)$. An arrow is marked with the set of *labels*

$$\operatorname{Aut}(E_1, P_1) \circ \lambda.$$

Every element of $\operatorname{Aut}(E_1, P_1) \circ \lambda$ will be called a label of the arrow.

(2) Let (E, P) and (E_1, P_1) be representatives in $\operatorname{Rep}(N)$, i.e., vertices of $\Lambda_\ell(N)$. The set of degree ℓ isogenies $\lambda \colon (E, P) \to (E_1, P_1)$, if non-empty, has a natural action of $\operatorname{Aut}(E_1, P_1)$, and we associate to every orbit $\operatorname{Aut}(E_1, P_1) \circ \lambda$ of this action an arrow from (E, P) to (E_1, P_1), together with the set of labels $\operatorname{Aut}(E_1, P_1) \circ \lambda$.

In our second definition, every arrow corresponds to a unique subgroup C of E of order ℓ, which is the kernel of any isogeny in its set of labels $\operatorname{Aut}(E_1, P_1) \circ \lambda$. Note that there is a unique isomorphism $\alpha \colon E/C \to E_1$ making the diagram below commutative:

$$
\begin{array}{ccc}
E & \xrightarrow{\ \lambda\ } & E_1 \\
& \searrow{\scriptstyle \pi_C} \quad \nearrow{\scriptstyle \alpha} & \\
& E/C &
\end{array}
$$
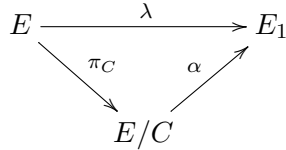
It follows that the point $P_1 = \lambda(P)$ is equal to $\alpha(\pi_C(P))$ and so the two constructions of the arrows in the graph are the same.

Remark 5.2.4. Note that there is no obvious way to make the graphs $\Lambda_\ell(N)$ undirected; the natural idea of identifying an isogeny λ with its dual $\lambda^\vee$ fails in general because $\lambda^\vee$ and λ^{-1} differ by multiplication by ℓ, which acts non-trivially on points of order N (unless $\ell \equiv 1 \pmod{N}$).

Even in the case $N = 1$ there is a problem as the graphs are typically non-symmetric. The number of arrows from E_1 to E_2 is $\operatorname{Aut}(E_1)/\operatorname{Aut}(E_2)$ times the number of arrows from E_2 to E_1. The adjacency matrix of $\Lambda_\ell(1)$

is the ℓ-th Brandt matrix. See [15], in particular Proposition 2.7. Finally, we remark that in general the graphs may contain loops and multiple arrows.

5.3. Properties of supersingular graphs. The graphs $\Lambda_\ell(N)$ need not be simple in general, however we do have the following proposition.

Proposition 5.3.1. *If $N > 4\ell^2$ the graph $\Lambda_\ell(N)$ is simple, i.e., contains no loops or multiple edges; moreover, every arrow has a unique label in this case. The girth of the graph $\Lambda_\ell(N)$ is at least $\log_\ell(N/4)$.*

Proof. The statement about the girth implies the one about the loops. Suppose that the girth is r. Then, we can find a representative (E, P) and a $\gamma \in \operatorname{End}(E)$ such that the $\deg(\gamma) = \ell^r$ and $\gamma(P) = P$. Therefore, $N | \sharp \operatorname{Ker}(\gamma - 1) = \deg(\gamma - 1)$. Thinking about γ as a complex number of modulus $\ell^{r/2}$ we have $\deg(\gamma - 1) = |\gamma - 1|^2 \leq (|\gamma| + 1)^2 \leq (2|\gamma|)^2 = 4\ell^r$, which gives $N \leq 4\ell^r$.

Suppose we have two distinct arrows $f, g \colon (E_1, P_1) \to (E_2, P_2)$. Then $g^{-1} \circ f$ is a rational endomorphism of (E_1, P_1), and $\gamma := \ell g^{-1} \circ f = g^\vee \circ f$ is an endomorphism of E_1 of degree ℓ^2 such that $\gamma(P_1) = \ell P_1$. Consequently, $N | \sharp \operatorname{Ker}(\gamma - \ell) = |\gamma - \ell|^2 \leq 4\ell^2$. Thus, if $N > 4\ell^2$ there are no multiple edges, and by Lemma 5.2.2 no multiple labels. $\square$

We note that there is a natural map

$$\pi_N : \Lambda_\ell(N) \to \Lambda_\ell(1), \qquad (E, P) \mapsto E,$$

taking an arrow with label $\lambda \colon (E_1, P_1) \to (E_2, P_2)$ to the arrow $\lambda \colon E_1 \to E_2$.

The construction of the graphs $\Lambda_\ell(N)$ is motivated by the study of the Hecke operator T_ℓ; the directed walks of length r in $\Lambda_\ell(N)$ that begin at (E, P) describe the image of the point $(E, P) \in X_1(N)(\overline{\mathbb{F}}_p)$ under T_ℓ^r, including multiplicities. With this in mind, we make a further study of these graphs. We first prove a technical lemma about translating isogenies to walks.

Lemma 5.3.2. *Let $\underline{E} = (E, P)$ be a vertex of $\Lambda_\ell(N)$. Let $\lambda : \underline{E} \to \underline{E}'$ be an isogeny of degree ℓ^r. Let $\underline{E}'' \in Rep(N)$, and $\epsilon : \underline{E}' \to \underline{E}''$ be an isomorphism. Then there is a walk of length r in $\Lambda_\ell(N)$,*

$$\underline{E} = \underline{E}_0 \xrightarrow{\lambda_1} \underline{E}_1 \xrightarrow{\lambda_2} \cdots \xrightarrow{\lambda_{r-1}} \underline{E}_{r-1} \xrightarrow{\lambda_r} \underline{E}_r = \underline{E}'',$$

where each λ_i is a label for the corresponding arrow, and $\epsilon^{-1} \lambda_r \ldots \lambda_2 \lambda_1 = \lambda$.

Proof. Let $C_r = \operatorname{Ker}(\lambda)$. Factorize λ as $(E, P) \to (E/C_r, P \bmod C_r) \overset{\delta}{\cong} \underline{E}'$, and let

$$0 = C_0 \subsetneq C_1 \subsetneq C_2 \subsetneq \cdots \subsetneq C_r = \operatorname{Ker}(\lambda)$$

be a filtration by subgroups with cyclic quotients of order ℓ. For each $0 <$
$i < r$, let ϵ_i be an isomorphism

$$\epsilon_i \colon (E/C_i, P \bmod C_i) \cong \underline{E}_i,$$

where $\underline{E}_i \in \mathrm{Rep}(N)$, such that $\epsilon_0 = \mathrm{id}$, $\underline{E}_r = \underline{E}''$, and $\epsilon_r = \epsilon\delta$. Let
$\rho_i \colon E/C_{i-1} \to E/C_i$ be the canonical morphism. Since C_r is the kernel
of λ, we have $\lambda = \delta\rho_n \ldots \rho_1$. This yields a factorization

$$\epsilon\lambda = (\epsilon_r \circ \rho_r \circ \epsilon_{r-1}^{-1}) \circ \cdots \circ (\epsilon_2 \circ \rho_2 \circ \epsilon_1^{-1}) \circ (\epsilon_1 \circ \rho_1 \circ \epsilon_0^{-1}).$$

Note that each $\lambda_i := \epsilon_i \circ \rho_n \circ \epsilon_{i-1}^{-1}$ is a label for an arrow in the graph $\Lambda_\ell(N)$
from $\underline{E}_{i-1}$ to $\underline{E}_i$. This provides a walk of length r starting at $\underline{E}$, ending at
$\underline{E}''$, such that $\epsilon^{-1}\lambda_r \ldots \lambda_2\lambda_1 = \lambda$. $\qquad\square$

Theorem 5.3.3. *The graphs $\Lambda_\ell(N)$ have the following properties.*
   (1) *$\Lambda_\ell(N)$ is a connected, directed graph of fixed out-degree $\ell + 1$.*
   (2) *The graph $\Lambda_\ell(N)$ is not bipartite.*
   (3) *If N is rigid, every vertex in $\Lambda_\ell(N)$ has in-degree $\ell + 1$ as well.*

Proof. The fact that $\Lambda_\ell(N)$ is a directed graph and every vertex has out-
degree $\ell + 1$ follows from the construction and the description of arrows by
means of cyclic subgroups of order ℓ.

Let G be the algebraic group over $\mathbb{Q}$ whose $\mathbb{Q}$-points are

$$B_{p,\infty}^1 = \{x \in B_{p,\infty} : \mathrm{Nm}(x) = 1\};$$

it is a form of SL_2 and hence G is semi-simple, almost simple, and simply
connected. Fix two pairs $(E, P_1), (E, P_2)$ in $\mathrm{Rep}(N)$. We identify $B_{p,\infty}$ with
$\mathrm{End}^0(E)$ and that gives us a maximal order $\mathcal{R}$ that corresponds to $\mathrm{End}(E)$.
The group $G(\mathbb{Q})$ is then the group of rational endomorphisms of E of norm
1. We choose a symplectic basis for the Tate modules $T_u(E)$ for every prime
$u \neq p$. The action of $G(\mathbb{Z}_u)$ on $T_u(E)$ induces an isomorphism $G(\mathbb{Z}_u) \cong$
$\mathrm{SL}_2(\mathbb{Z}_u)$.

Using strong approximation for G relative to the place ℓ, we can find an
element y of $G(\mathbb{Q})$ that is very close, except possibly at ℓ, to the element

$$x \in G(\mathbb{A}_\mathbb{Q}^f), \qquad x = (x_u)_u = \begin{cases} 1 & u \nmid N, \\ x_u & u \mid N, \end{cases}$$

where the elements $x_u, u \mid N$, are chosen to be in $\mathrm{SL}_2(\mathbb{Z}_u)$ and such that
$\prod_{u \mid N} x_u \pmod{N} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ takes P_1 to P_2.

The element y is thus integral, except possibly at ℓ, and $\mathrm{Nm}(y) = 1$.
Replacing y by $\ell^{\alpha(N)m}y$ for a suitable positive integer m, we have proven the
existence of an isogeny $f \colon (E, P_1) \to (E, P_2)$ of degree a power of ℓ. Using
Lemma 5.3.2, we can factor f as a composition of cyclic isogenies of degree ℓ
and we thus find that (E, P_1) is connected to (E, P_2) in $\Lambda_\ell(N)$. Combined
with the well-known fact that $\Lambda_\ell(1)$ is connected (namely, between any two

supersingular elliptic curves over $\overline{\mathbb{F}}_p$ there is some isogeny of degree a power of ℓ – see below), one concludes that $\Lambda_\ell(N)$ is connected as well. In fact, we have proven that for all E, and for all P_1, P_2 of order N on E, there is a walk of even length from (E, P_1) to (E, P_2).

We now prove that $\Lambda_\ell(N)$ is not bipartite. We first consider the case $N = 1$. It is enough to prove that there is a closed walk of odd length in $\Lambda(1)$. By Lemma 5.3.2, this is equivalent to proving that there is an elliptic curve E with an endomorphism of degree ℓ^r, where r is a positive odd integer. Let E be an arbitrary supersingular elliptic curve, and consider the quadratic form in 4 variables and discriminant p^2,

$$\deg \colon \operatorname{End}(E) \cong \mathcal{R} \to \mathbb{Z}.$$

We need to prove that deg represents an integer of the form ℓ^r, for some r a positive odd integer. We show that it represents every large enough positive integer prime to p. We will use the fact that the Integral Hasse Principle for a quadratic form on a rank 4 lattice holds for large enough integers that are relatively prime to the discriminant of the quadratic form of the lattice. Since ℓ is prime to p, our desired result follows if we prove that the quadratic form deg represents every integer locally. The quadratic form deg is positive definite at infinity. At a finite place $v \neq p$, we have an isomorphism $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_v \cong M_2(\mathbb{Z}_v)$ via which norm corresponds to the determinant, and every v-adic integer can be represented as a determinant. At prime p, we have $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathscr{R}$ which has a model

$$\left\{ \begin{pmatrix} a & pb^\sigma \\ b & a^\sigma \end{pmatrix} : a, b \in W(\mathbb{F}_{p^2}) \right\},$$

and where the degree map associates to the above matrix its determinant $aa^\sigma - pbb^\sigma$. By local class field theory, the norm map $W(\mathbb{F}_{p^2})^\times \to \mathbb{Z}_p^\times$ is surjective. Therefore, all elements of $\mathbb{Z}_p$ of even valuation are norms of the form aa^σ, and all those with odd valuations are norms of the form $-pbb^\sigma$. This ends the proof that $\Lambda_\ell(1)$ is not bipartite.

Next we prove the result for general N. We show again that $\Lambda_\ell(N)$ has a closed walk of odd length. Let (E, P) be a vertex. Let $\gamma : E \to E$ be an isogeny of degree ℓ^r with r odd as in the previous paragraph. By Lemma 5.3.2, this isogeny provides us with a walk of odd length from (E, P) to (E, P'), where $(E, P') \in Rep(N)$ is isomorphic to $(E, \gamma(P))$. In proving the connectivity of the graph, we have shown that there is a walk of even length from (E, P') to (E, P). Composing these walks, we obtain a closed walk of odd length starting and ending at (E, P). This proves that $\Lambda_\ell(N)$ is not bipartite.

We now prove part (3). Suppose that (N, p) is rigid. By counting, it is enough to show that every vertex (E, P) has in-degree at least $\ell + 1$. Let $C_1, \ldots, C_{\ell+1}$ be the subgroups of order ℓ of E and $\pi_i : E \to E/C_i$ the

canonical morphism. Consider the diagrams

$$(E, \ell^{\alpha(N)-1}P) \xrightarrow{\pi_i} (E/C_i, \ell^{\alpha(N)-1}P \bmod C_i) \xrightarrow{\pi_i^\vee} (E, \ell^{\alpha(N)}P) = (E, P).$$

Then, replacing $(E/C_i, \ell^{\alpha(N)-1}P \bmod C_i)$ by the corresponding representative $(E/C_i, \ell^{\alpha(N)-1}P \bmod C_i)^r$ and adjusting $\pi_i^\vee$ by the unique implied ℓ-isogeny $\pi_i^{\vee,r}$, we find $\ell + 1$ arrows leading into (E, P):

$$(E/C_i, \ell^{\alpha(N)-1}P \bmod C_i)^r \xrightarrow{\pi_i^{\vee,r}} (E, P).$$

We claim that these are distinct arrows. If for some i, j we get the same arrow then we have $(E/C_i, \ell^{\alpha(N)-1}P \bmod C_i) \cong (E/C_j, \ell^{\alpha(N)-1}P \bmod C_j)$ *and*, under this (unique) isomorphism, $\pi_i^\vee = \pi_j^\vee$. But then $\pi_i = \pi_j$ and so $C_i = C_j$. □

5.4. From walks to endomorphisms. We now introduce some additional constructions. In addition to fixing p, ℓ, N, fix now an object $\underline{E} = (E, P)$, where E is a supersingular elliptic curve, and P is a point on E of order N. Let $\mathcal{R} = \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$.

Recall that if h is an arrow from $\underline{E}_1 = (E_1, P_1)$ to $\underline{E}_2 = (E_2, P_2)$ in $\Lambda_\ell(N)$, then h is an orbit under the action of $\mathrm{Aut}(\underline{E}_2)$ on the set of degree ℓ isogenies from E_1 to E_2 that take P_1 to P_2. Elements in this orbit were called labels for h. By a *labeled walk* in the graph $\Lambda_\ell(N)$ we mean a walk with a choice of label for each arrow in the walk. For two closed labeled walks ω_1 and ω_2 based at $\underline{E}$, their composition $\omega_2 \circ \omega_1$ is the labeled walk obtained by traversing ω_1 followed by ω_2. We allow the empty walk and its set of labels is, per definition, $\mathrm{Aut}(\underline{E})$. We introduce the following notation:

- $\Omega(\Lambda_\ell(N), \underline{E})$ denotes the monoid of closed labeled walks in $\Lambda_\ell(N)$ starting at $\underline{E}$.
- Given $\omega \in \Omega(\Lambda_\ell(N), \underline{E})$, by composing the labels of the arrows occurring in ω, we get an endomorphism $\widetilde{\omega} \in \mathcal{R}$; as $\widetilde{\omega}$ has norm a power of ℓ, we have $\widetilde{\omega} \in \mathscr{R}^\times$.
- We denote by $\mathscr{H}_N^+(\underline{E})$ the monoid in $\mathscr{R}^\times$ obtained as the image of $\Omega(\Lambda_\ell(N), \underline{E})$. By Lemma 5.3.2, $\mathscr{H}_N^+(\underline{E})$ consists of those endomorphisms f of E of degree a non-negative power of ℓ such that $f(P) = P$. Let $\mathscr{H}_N(\underline{E})$ be the subgroup of $\mathscr{R}^\times$ generated by $\mathscr{H}_N^+(\underline{E})$. Note that $\ell^{\alpha(N)} \in \mathscr{H}_N(\underline{E})$.
- We denote by $\mathscr{G}_N(\underline{E})$ the subgroup of $\mathrm{PGL}_2(\mathbb{Q}_q)$ that is the image of $\mathscr{H}_N(\underline{E})$ under the composition $\mathscr{B}^\times \to \mathrm{GL}_2(\mathbb{Q}_q) \to \mathrm{PGL}_2(\mathbb{Q}_q)$. The map $\mathscr{B}^\times \to \mathrm{GL}_2(\mathbb{Q}_q)$ is chosen so that the image of $\mathscr{R}$ is

$$\left\{ \begin{pmatrix} a & pb^\sigma \\ b & a^\sigma \end{pmatrix} : a, b \in W(\mathbb{F}_q) \right\},$$

where σ is the Frobenius automorphism. For $\omega \in \Omega(\Lambda_\ell(N), \underline{E})$, we denote the image of $\widetilde{\omega}$ in $\mathscr{G}_N(\underline{E})$ by $\widetilde{\omega}$ again.

Lemma 5.4.1. *$\mathscr{H}_N(\underline{E})$ is the group of rational endomorphisms of E of the form $f = f_1/\ell^t$ such that $f_1 \in \mathrm{End}(E), \deg(f_1) = \ell^r, r, t \in \mathbb{N}$, and $f(P) = P$.*

Proof. One inclusion is clear: using that for any isogeny g, we have $g^{-1} = g^\vee / \deg(g)$, it follows that the elements of $\mathscr{H}_N(\underline{E})$ have the desired property. For the other, note that for f with the above property, $g := \ell^{\alpha(N)t} f$ is an endomorphism satisfying $g(P) = P$ and thus belongs to $\mathscr{H}_N^+(\underline{E})$. The result now follows since $\ell^{\alpha(N)}$ is in $\mathscr{H}_N^+(\underline{E})$. $\qquad\square$

From this point on, we fix $\underline{E} = (E, P)$ in $Rep(N)$ and simplify the notation by dropping $\underline{E}$ from the notation: $\mathscr{H}_N = \mathscr{H}_N(\underline{E})$, $\mathscr{G}_N = \mathscr{G}_N(\underline{E})$, $\Omega(\Lambda_\ell(N)) = \Omega(\Lambda_\ell(N), \underline{E})$.

It follows easily from the definitions that the following diagram is commutative and its arrows are homomorphisms that have the indicated properties.

$$
\begin{array}{ccc}
\Omega(\Lambda_\ell(N)) \longrightarrow \mathscr{H}_N \twoheadrightarrow \mathscr{G}_N \\
\Big\downarrow{\scriptstyle \pi_N} \qquad \Big\uparrow \qquad \Big\uparrow \\
\Omega(\Lambda_\ell(1)) \longrightarrow \mathscr{H}_1 \twoheadrightarrow \mathscr{G}_1
\end{array}
$$

If $p \equiv 1 \pmod{12}$, then the pair $(1, p)$ is solid, in the sense of Definition 5.2.1. In particular, $f \mapsto f^\vee$ defines a one-one correspondence between $\mathrm{Hom}(E, E')$ and $\mathrm{Hom}(E', E)$, for any two supersingular elliptic curves E, E'. Therefore, we can, just as in the ordinary case, define an undirected graph $\Lambda_\ell^{\mathrm{ud}}(1)$ by identifying an arrow corresponding to f with the reverse arrow corresponding to $f^\vee$. Note that when f is an endomorphism of E of degree ℓ, and $f \neq \pm f^\vee$, the corresponding loop in $\Lambda_\ell^{\mathrm{ud}}(1)$ is considered with multiplicity 2.

Let $H(4\ell)$ denote the Hurwitz class number of positive definite primitive quadratic forms of discriminant -4ℓ, see [15].

Proposition 5.4.2. *The following hold:*

(1) *The group $\mathscr{H}_N$ (resp., $\mathscr{G}_N$) is a finitely-generated finite-index subgroup of $\mathscr{H}_1$ (resp., $\mathscr{G}_1$).*

(2) *The groups $\mathscr{G}_N$ are highly non-commutative. To be precise:*

    (a) *The groups $\mathscr{H}_N$ and $\mathscr{G}_N$ have arbitrarily large subsets of pairwise non-commuting elements.*

    (b) *Let $p \equiv 1 \pmod{12}$. Let $\gamma(\ell) = \frac{1}{2} H(4\ell)$. Then the fundamental group $\pi_1(\Lambda_\ell(1), E)$ is a free group of rank $1 + \frac{\gamma(\ell)}{2} + \frac{(\ell-1) \cdot (p-1)}{24}$.*

Furthermore, there are elements $\mathscr{C}_1, \ldots, \mathscr{C}_{\gamma(\ell)}$ that are part of a basis of $\pi_1(\Lambda_\ell(1), E)$ such that

$$\mathscr{G}_1 \cong \pi_1(\Lambda_\ell(1), E)/\langle\!\langle \mathscr{C}_1^2, \ldots, \mathscr{C}_{\gamma(\ell)}^2 \rangle\!\rangle,$$

where $\langle\!\langle \mathscr{C}_1^2, \ldots, \mathscr{C}_{\gamma(\ell)}^2 \rangle\!\rangle$ denotes the minimal normal subgroup containing $\mathscr{C}_1^2, \ldots, \mathscr{C}_{\gamma(\ell)}^2$. Consequently, $\mathscr{G}_1$ has a quotient that is a free group of rank $1 - \frac{\gamma(\ell)}{2} + \frac{(\ell-1)\cdot(p-1)}{24}$.

Proof. To show that the groups $\mathscr{G}_N$ are finitely generated, we will produce a finite set of generators. First, we prove a lemma.

Lemma 5.4.3. *Let $\underline{E}_1 = (E_1, P_1)$ and $\underline{E}_2 = (E_2, P_2)$ be vertices of $\Lambda_\ell(N)$. Let $\lambda \colon \underline{E}_1 \to \underline{E}_2$ be an isogeny of degree ℓ^m for some $m > 0$. There is an isogeny*

$$\eta_\lambda \colon \underline{E}_2 \to \underline{E}_1$$

of degree $\ell^a \leq \ell^{m+2(\alpha(N)-1)}$ such that $\lambda \circ \eta_\lambda$ is multiplication by a power of ℓ. In particular, for every labeled walk ω from $\underline{E}_1$ to $\underline{E}_2$ of length m, there is a labeled walk η_ω from $\underline{E}_2$ to $\underline{E}_1$ of length $a \leq m + 2(\alpha(N)-1)$ such that $\widetilde{\omega} \circ \widetilde{\eta_\omega} \in \mathscr{G}_N$ is the identity.

Proof. Define $\eta_\lambda := \ell^x \lambda^\vee$, where x is the smallest non-negative integer for which we have $\alpha(N)|(m + x)$. We have $\deg(\eta_\lambda) = \ell^{m+2x} \leq \ell^{m+2(\alpha(N)-1)}$. We also have $\eta_\lambda \circ \lambda = \ell^{x+m}$, and $\eta_\lambda(P_2) = \ell^x(\lambda^\vee(P_2)) = \ell^{m+x}P_1 = P_1$, as desired. $\qquad\square$

We now prove the finite generation of $\mathscr{G}_N = \mathscr{H}_G(\underline{E})$, and deduce the finite generation of $\mathscr{H}_N$. Let $v(N)$ denote the number of vertices in $\Lambda_\ell(N)$. We prove that the finite set

$$Gen = \{\widetilde{\omega} : \omega \in \Omega(\Lambda_\ell(N), \underline{E}) \text{ of length } \leq 2\alpha(N) + 2v(N) - 3\}$$

generates $\mathscr{G}_N$. Let $\omega \in \Omega(\Lambda_\ell(N), \underline{E})$ be a closed labeled walk comprised of vertices $E_1 = E, E_2, \ldots, E_n, E_{n+1} = E$, with labeled arrows h_i from E_i to E_{i+1}. For each $2 \leq i \leq n$, let ω_i denote a labeled walk from E_1 to E_i of length at most $v(N) - 1$ (these exist since $\Lambda_\ell(N)$ is connected). Then, $\widetilde{\omega} = \widetilde{h}_n \ldots \widetilde{h}_1$ can be written as a product

$$\widetilde{\omega} = (\widetilde{h_n \omega_n})(\widetilde{\eta_{\omega_n} h_{n-1} \omega_{n-1}}) \ldots (\widetilde{\eta_{\omega_3} h_2 \omega_2})(\widetilde{\eta_{\omega_2} h_1}),$$

in which each factor is in Gen. This proves that $\mathscr{G}_N$ is finitely generated. As the kernel of $\mathscr{H}_N \to \mathscr{G}_N$ is finitely generated, also $\mathscr{H}_N$ is finitely generated. (The kernel is generated by $\ell^{\alpha(N)}$ and $-\ell^{\beta(N)}$, where $\beta(N)$ is the least non-negative integer such that $\ell^{\beta(N)} \equiv -1 \pmod{N}$; if no such $\beta(N)$ exists, the kernel is generated by $\ell^{\alpha(N)}$ alone.)

Denote by $\mathscr{H}_N^1$ the subgroup of $\mathscr{H}_1$ composed of elements whose action on the N-torsion points of E is trivial. Then, $\mathscr{H}_1 \supseteq \mathscr{H}_N \supseteq \mathscr{H}_N^1$, and to

prove $\mathscr{H}_N$ is of finite index in $\mathscr{H}_1$, it is enough to show that $\mathscr{H}_N^1$ is of finite index in $\mathscr{H}_1$. But, $\mathscr{H}_1/\mathscr{H}_N^1 \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and the assertion follows.

Next, we prove that $\mathscr{H}_N$ has an arbitrarily large subset of pairwise non-commuting elements. Let n be a positive integer. Let $\mathcal{R} = \mathrm{End}(E)$, and let $d_1, \ldots, d_n$ be large enough distinct primes such that ℓ is split and p is inert in each of the fields $K_i = \mathbb{Q}(\sqrt{-d_i})$. By [13, Theorem 1.4] and the discussion preceding it, each field K_i has an optimal embedding $K_i \to B_{p,\infty}$ relative to $\mathcal{R}$; that is, the image of $\mathcal{O}_{K_i}$ is contained in $\mathcal{R}$. The images of the fields K_i do not commute.

As ℓ is split, in each field K_i, we have a decomposition into primes ideals $\ell\mathcal{O}_{K_i} = \mathscr{L}_{i,1}\mathscr{L}_{i,2}$. Let r be an integer divisible by the class numbers of $K_1, \ldots, K_n$ and let $s_N = \sharp\, \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then, $\mathscr{L}_i^r = (t_i)$, and $\tau_i := t_i^{s_N}$ have the following properties:

   (i) $\tau_i \in \mathcal{R}$;
   (ii) $K_i = \mathbb{Q}(\tau_i)$, and hence τ_i and τ_j do not commute for $i \neq j$;
   (iii) $\tau_i \in \mathscr{H}_N$ as $t_i \in \mathscr{H}_1$ and t_i acts by an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $E[N]$.

This provides us with n pairwise non-commuting elements of $\mathscr{H}_N$. In addition, since commutators have trace 0 and the kernel of $\mathscr{H}_N \to \mathscr{G}_N$ consists of non-zero scalars, the images of the τ_i do not commute in $\mathscr{G}_N$ either.

Finally, we assume $p \equiv 1 \pmod{12}$, and consider the graph $\Lambda_\ell^{\mathrm{ud}}(1)$, which has $(p-1)/12$ vertices. The fundamental group $\pi_1(\Lambda_\ell^{\mathrm{ud}}(1), E)$ can be described the following way. Let $\Lambda_\ell^{\mathrm{en}}(1)$ be the ("enlarged") graph with the same vertices as $\Lambda_\ell^{\mathrm{ud}}(1)$, but for every edge e in $\Lambda_\ell^{\mathrm{ud}}(1)$ introduce two corresponding edges $e^\epsilon, \epsilon \in \{+, -\}$ in $\Lambda_\ell^{\mathrm{en}}(1)$, thereby getting a directed connected graph. Introduce an equivalence relation on the set $\Omega(\Lambda_\ell^{\mathrm{en}}(1), E)$ of closed directed walks as the one generated by basic equivalences

$$\omega_1\omega_2 \sim \omega_1 e^\epsilon e^{-\epsilon}\omega_2.$$

The corresponding set of equivalence classes forms a group, naturally isomorphic to $\pi_1(\Lambda_\ell^{\mathrm{ud}}(1), E)$. Note that we have graph morphisms

$$\Lambda_\ell^{\mathrm{en}}(1) \to \Lambda_\ell(1) \to \Lambda_\ell^{\mathrm{ud}}(1).$$

In fact, the morphism $\Lambda_\ell^{\mathrm{en}}(1) \to \Lambda_\ell(1)$ is a bijection on vertices and all edges except for *self-dual edges*, namely, edges that correspond to loops with labels $\pm\lambda$ such that $\pm\lambda = \pm\lambda^\vee$ (i.e., the loops of multiplicity 1 in $\Lambda_\ell^{\mathrm{ud}}(1)$). There is a natural map

$$\Omega(\Lambda_\ell^{\mathrm{en}}(1), E) \to \mathscr{G}_1.$$

Indeed, each edge e^ϵ inherits a set of labels $\pm\lambda$ from $\Lambda_\ell(1)$, and so for each walk we can associate the composition of the labels that gives a well defined element in $\mathscr{G}_1$. Equivalent elements of $\Omega(\Lambda_\ell^{\mathrm{en}}(1), E)$ have the same image.

We note that if e^ϵ corresponds to a self-dual loop in $\Lambda_\ell(1)$ then we get $(e^\epsilon)^2 = 1$ in $\mathscr{G}_1$.

To every loop c_i of multiplicity 1 in $\Lambda_\ell(1)$, we associate an element $\mathscr{C}_i$ of $\pi_1(\Lambda_\ell^{\mathrm{ud}}(1), E)$ by taking a path ω_i from E to the vertex of the loop c_i, and letting $\mathscr{C}_i = \omega_i^\vee c_i \omega_i$. We get a well-defined homomorphism

$$\pi_1(\Lambda_\ell(1), E)/\langle\!\langle \mathscr{C}_1^2, \ldots, \mathscr{C}_{\gamma(\ell)}^2 \rangle\!\rangle \to \mathscr{G}_1.$$

It is easy to check using Lemma 5.3.2 that this is a surjective homomorphism. The injectivity is equivalent to checking that a composition of ℓ-isogenies $f_n \circ \cdots \circ f_1$ is, up to a sign, multiplication by a power of ℓ if and only if it is composed of nested pairs of ℓ-isogenies $\pm\lambda \circ \lambda^\vee$. To see this last statement, consider a composition of ℓ-isogenies $f_n \circ \cdots \circ f_1$ which is equal to $\ell^{n/2}$, say

$$E = E_0 \xrightarrow{f_1} E_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} E_n \ .$$

Let $i+1$ be the minimal integer such that ℓ divides $f_{i+1} \circ \cdots \circ f_1$. That is, $\mathrm{Ker}(f_{i+1} \circ \cdots \circ f_1) \cong \mathbb{Z}/\ell^i\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and, under this isomorphism, $\mathrm{Ker}(f_j \circ \cdots \circ f_1) = \mathbb{Z}/\ell^j\mathbb{Z} \times \{0\}$ for $j \leq i$. It follows that $\mathrm{Ker}(f_{i+1} \circ f_i) \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, which implies that $E_{i+1} \cong E_{i-1}$ and $f_{i+1} \circ f_i$ is equal to the multiplication-by-ℓ map up to an automorphism of E_{i+1}, namely, up to ± 1 due to our assumption on p. Therefore, $f_{i+1} = \pm f_i^\vee$.

A label of a self-dual loop at a vertex E' corresponds to an embedding $\mathbb{Z}[\sqrt{-\ell}] \hookrightarrow \mathrm{End}(E')$. By [15, Section 1], there are $H(4\ell)$ such embeddings. Therefore the number of self-dual loops of $\Lambda_\ell^{\mathrm{ud}}(1)$ is $\gamma(\ell)$. Hence, the group $\pi_1(\Lambda_\ell^{\mathrm{ud}}(1), E)$ is a free group of rank $1 + \frac{\gamma(\ell)}{2} + \frac{(\ell-1)\cdot(p-1)}{24}$ and so $\mathscr{G}_1$ has a quotient that is a free group of rank $1 - \frac{\gamma(\ell)}{2} + \frac{(\ell-1)\cdot(p-1)}{24}$. $\qquad\square$

5.5. The closure of $\mathscr{H}_N^+$, $\mathscr{H}_N$ and $\mathscr{G}_N$. Our purpose is to determine the p-adic and Zariski closures of the monoid $\mathscr{H}_N^+$ in $\mathscr{R}^\times$, and the same for $\mathscr{G}_N$. We will use $\mathbb{H}, \mathbb{G}$, etc. to denote p-adic closures and H, G, etc. to denote Zariski closures.

We introduce the following submonoid of $\mathscr{H}_N^+$:

$$\mathscr{H}_N^{1,+} = \{f \in \mathrm{End}(E) : f \equiv 1 \pmod N, \deg(f) \in \langle \ell^{\alpha(N)} \rangle\},$$

and let $\mathscr{H}_N^1$ be the minimal group containing $\mathscr{H}_N^{1,+}$ (it already appeared in the proof of Proposition 5.4.2). Denote by $\mathbb{H}_N^+, \mathbb{H}_N^{1,+}$ the p-adic closure of $\mathscr{H}_N^+$ and $\mathscr{H}_N^{1,+}$ in $\mathscr{R}^\times$, respectively. Let $\mathscr{L}_N$ be the p-adic closure of $\langle \ell^{\alpha(N)} \rangle$ in $\mathscr{R}^\times$. Note that $\mathscr{L}_N$ is also the p-adic closure of $\{\ell^{r\alpha(N)} : r = 1, 2, 3, \ldots\}$

Proposition 5.5.1. $\mathbb{H}_N^{1,+} = \{x \in \mathscr{R}^\times : \mathrm{Nm}(x) \in \mathscr{L}_N\}$.

Proof. Let $A = \{x \in \mathscr{R}^\times : \mathrm{Nm}(x) \in \mathscr{L}_N\}$. Clearly, $\mathscr{H}_N^{1,+} \subset A$. Since A is a compact group, also $\mathbb{H}_N^{1,+} \subseteq A$.

For the reverse inclusion we will use Theorem 1.2 of [25]. Write $\mathcal{R} = \mathrm{End}(E) \subset B_{p,\infty}$ and identify $\mathcal{R}$ with $\mathbb{Z}^4$ so that $1 = (1,0,0,0)$; let Q be the positive definite quadratic form corresponding to the norm of $B_{p,\infty}$. Then $\mathscr{R} = \mathbb{Z}_p^4$. Let $\underline{\alpha} = (\alpha_1, \ldots, \alpha_4) \in A$. We need to show that for all $M \geq 0$, $\exists\,(\beta_1, \ldots, \beta_4) \in \mathbb{Z}^4$ such that:

- $Q(\beta_1, \ldots, \beta_4) = \ell^{r\alpha(N)}$ for $r > 0$ such that $\ell^{r\alpha(N)} \equiv \mathrm{Nm}(\underline{\alpha}) \pmod{p^M}$,
- $(\beta_1, \ldots, \beta_4) \equiv (1,0,0,0) \pmod{N}$, and
- $(\beta_1, \ldots, \beta_4) \equiv (\alpha_1, \ldots, \alpha_4) \pmod{p^M}$.

Note that there are always arbitrary large r satisfying the congruence in the first condition. For convenience we take $M \geq 2$.

Let $m = Np^M$ and let $(\lambda_1, \ldots, \lambda_4) \in (\mathbb{Z}/m\mathbb{Z})^4$ correspond to the above last two congruence conditions. By the result cited above, to get a solution (for $r \gg_M 0$), it suffices to show that for every prime u there is a $(x_1, \ldots, x_4) \in \mathbb{Z}_u^4$ such that $Q(x_1, \ldots, x_4) = \ell^{r\alpha(N)}$ and $(x_1, \ldots, x_4) \equiv (\lambda_1, \ldots, \lambda_4) \pmod{u^{\mathrm{ord}_u(m)}}$.

For $u \nmid m$, there is no congruence condition, $(\mathbb{Z}_u^4, Q) \cong (M_2(\mathbb{Z}_u), \det)$, and the matrix $\left(\begin{smallmatrix} 1 & \\ & \ell^{r\alpha(N)} \end{smallmatrix}\right)$ is a solution. For $u \mid N$, we still have $(\mathbb{Z}_u^4, Q) \cong (M_2(\mathbb{Z}_u), \det)$, and the matrix $\left(\begin{smallmatrix} 1 & \\ & \ell^{r\alpha(N)} \end{smallmatrix}\right)$ is still a solution because it satisfies the congruence condition $\left(\begin{smallmatrix} 1 & \\ & \ell^{r\alpha(N)} \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right) \bmod u^{\mathrm{ord}_u(m)}$.

For $u = p$ we want a solution in $\mathbb{Z}_p^4$ that is congruent to $(\alpha_1, \ldots, \alpha_4)$ $\pmod{p^M}$. We have now $(\mathscr{R}, Q) \cong \left(\left\{\left(\begin{smallmatrix} a & pb^\sigma \\ b & a^\sigma \end{smallmatrix}\right) : a, b \in W(\mathbb{F}_q)\right\}, \det\right)$. The element $\underline{\alpha}$ satisfies the congruence condition, is represented by a matrix $\left(\begin{smallmatrix} a_1 & pb_1^\sigma \\ b_1 & a_1^\sigma \end{smallmatrix}\right)$, and has determinant $\mathrm{Nm}(\underline{\alpha})$ that is congruent to $\ell^{r\alpha(N)}$ modulo p^M. We want to find $\tilde{a}_1$ such that $\tilde{a}_1 \equiv a_1 \pmod{p^M}$ and $\det\left(\begin{smallmatrix} \tilde{a}_1 & pb_1^\sigma \\ b_1 & \tilde{a}_1^\sigma \end{smallmatrix}\right) = \ell^{r\alpha(N)}$.

We claim that the norm map

$$a_1 + p^M W(\mathbb{F}_q) \to \mathrm{Nm}(a_1) + p^M \mathbb{Z}_p$$

is surjective. As a_1 is a unit, $a_1 + p^M W(\mathbb{F}_q) = a_1(1 + p^M W(\mathbb{F}_q))$ and it is enough to prove that Nm is a surjection $1 + p^M W(\mathbb{F}_q) \to 1 + p^M \mathbb{Z}_p$.

Applying the logarithm to both sides, we reduce to showing that the trace map $tr = tr_{W(\mathbb{F}_q)/\mathbb{Z}_p} \colon p^{M+1} W(\mathbb{F}_q) \to p^{M+1} \mathbb{Z}_p$ is surjective; this is easily verified. Finally, since $\ell^{r\alpha(N)} + pb_1 b_1^\sigma \in \mathrm{Nm}(a_1) + p^M \mathbb{Z}_p$, there is an $\tilde{a}_1 \in a_1 + p^M W(\mathbb{F}_q)$ whose norm is $\ell^{r\alpha(N)} + pb_1 b_1^\sigma$. $\qquad\square$

Corollary 5.5.2. $\mathbb{H}_N^{1;+}$ *is a group, equal to the p-adic closure of $\mathscr{H}_N^1$. Denote it henceforth by $\mathbb{H}_N^1$. The quotient group $\mathscr{R}^\times / \mathbb{H}_N^1$ is a finite group isomorphic to $\mathbb{Z}_p^\times / \mathscr{L}_N$.*

We have inclusions $\mathbb{H}_1 = \mathbb{H}_1^1 \supseteq \mathbb{H}_N^+ \supseteq \mathbb{H}_N^1$, and so $\mathbb{H}_N^+ / \mathbb{H}_N^1$ is a finite monoid contained in the group $\mathbb{H}_1 / \mathbb{H}_N^1$, hence a group itself.

Corollary 5.5.3. $\mathbb{H}_N^+$ *is a group, equal to the p-adic closure of* $\mathscr{H}_N$. *Denote it henceforth by* $\mathbb{H}_N$. *We have that* $\mathbb{H}_N/\mathbb{H}_N^1$ *is a cyclic subgroup of the group* $\mathscr{L}_1/\mathscr{L}_N \cong \mathbb{Z}/\alpha(N)\mathbb{Z}$.

Let $\Pi \colon \mathrm{GL}_2(\mathbb{Q}_q) \to \mathrm{PGL}_2(\mathbb{Q}_q)$ be the natural projection map. We are interested in the image of $\mathbb{H}_N$ under Π. Denote

$$\mathrm{sat}(\mathbb{H}_N) = \mathbb{Z}_p^\times \mathbb{H}_N = \Pi^{-1}\Pi(\mathbb{H}_N) \cap \mathscr{R}^\times.$$

The group $\mathrm{sat}(\mathbb{H}_N)$ is closed, hence $\Pi(\mathbb{H}_N)$ is closed in $\mathrm{PGL}_2(\mathbb{Q}_q)$ and equal to $\mathbb{G}_N$.

Proposition 5.5.4. *We have*

$$\mathrm{sat}(\mathbb{H}_N) = \mathscr{R}_\square^\times := \left\{ \begin{pmatrix} a & pb^\sigma \\ b & a^\sigma \end{pmatrix} \in \mathscr{R}^\times : aa^\sigma - pbb^\sigma \in (\mathbb{Z}_p^\times)^2 \cdot \langle \ell \rangle \right\}.$$

Thus, $\mathrm{sat}(\mathbb{H}_N)$ *has index at most* 2 *in* $\mathscr{R}^\times$ *if p is odd, and index at most* 4 *if* $p = 2$; *further,* $\mathrm{sat}(\mathbb{H}_N) = \mathscr{R}^\times$ *if and only if p is odd and* ℓ *is not a square modulo p.*

Proof. We first examine $\mathrm{sat}(\mathbb{H}_N^1)$. As $\mathscr{R}^\times/\mathbb{H}_N^1 \cong \mathbb{Z}_p^\times/\mathscr{L}_N$ via the determinant map, we find that $\mathscr{R}^\times/\mathrm{sat}(\mathbb{H}_N^1)$ is isomorphic to $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2\langle \ell^{\alpha(N)}\rangle$. Since the graph $\Lambda_\ell(N)$ is not bipartite (Theorem 5.3.3), there is an element in $\mathscr{H}_N^+$ whose degree is an odd power of ℓ. Consequently, $\mathscr{R}^\times/\mathrm{sat}(\mathbb{H}_N) \cong \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2\langle \ell \rangle$ and, in fact, $\mathrm{sat}(\mathbb{H}_N)$ is precisely the elements in $\mathscr{R}^\times$ whose determinant lies in $(\mathbb{Z}_p^\times)^2\langle \ell \rangle$. $\qquad\square$

Corollary 5.5.5. *We have* $\mathbb{G}_N = \Pi(\mathscr{R}_\square^\times)$, *which is independent of* N.

Proposition 5.5.6. *Let* H_N, G_N *be, respectively, the Zariski closures of* $\mathscr{H}_N$, $\mathscr{G}_N$ *in* $\mathrm{GL}_2(\mathbb{Q}_q)$, $\mathrm{PGL}_2(\mathbb{Q}_q)$. *Then* $H_N = \mathrm{GL}_2(\mathbb{Q}_q)$ *and* $G_N = \mathrm{PGL}_2(\mathbb{Q}_q)$.

Proof. As $H_N \supseteq \mathbb{H}_N, G_N \supseteq \mathbb{G}_N$, our assertion is quite clear from the description of algebraic subgroups of GL_2 and PGL_2 over an algebraic closure. For example, the proof of Proposition 5.4.2 shows that we can find arbitrarily large subsets of pairwise non-commuting elements of $\mathscr{H}_N$ lying in the connected component H_N^0 of H_N. Indeed, if $h = [H_N : H_N^0]$, we may replace in the proof the elements τ_i by τ_i^h that are mutually non-commuting, semi-simple, and have semi-simple commutators (every element of $\mathscr{B}^\times$ is semi-simple). It is also easy to arrange for a commutator to be non-central. From this it is easy to deduce that $H_N^0 = \mathrm{GL}_2$ or SL_2. On the other hand, we have elements of determinant $\ell^{\alpha(N)m}, m \in \mathbb{Z}$, in H_N. It follows that $H_N = \mathrm{GL}_2$ and $G_N = \mathrm{PGL}_2(\mathbb{Q}_q)$. $\qquad\square$

5.6. Dynamics implications - I. At this point we want to explain the implication of our results thus far for the study of the dynamics of the Hecke operator T_ℓ. Let $\underline{E} = (E, P)$ be an elliptic curve over $\mathbb{C}_p$ with good supersingular reduction, thought of as a point on $X_1(N)(\mathbb{C}_p)$ for N rigid. Let $D(\underline{E})$ be its residue disc. As we have seen (the arguments proving Lemma 3.2.1 apply), the correspondence $T_\ell^n|_{D(\underline{E})}$ decomposes into a sum of rigid-analytic isomorphisms between residue discs. If $T_\ell^n(\underline{E}) = \sum_i [\underline{E}_i]$ (with repetitions allowed) then

$$T_\ell^n|_{D(\underline{E})} = \sum_i f_i,$$

where each $f_i \colon D(\underline{E}) \to D(\underline{E}_i)$ is an isometry. Further, the discs $D(\underline{E}_i)$ are recognized by the mod p reductions $\overline{\underline{E}}_i$, which are supersingular curves too. Thus, as in the ordinary case, the movement of the residue discs follows the dynamics of the Hecke orbit of $\overline{\underline{E}}$, which is described by walks in the finite supersingular graph $\Lambda_\ell(N)$.

Enumerate the vertices of the $(\ell + 1)$-regular directed graph $\Lambda_\ell(N)$ as $\{v_1, \ldots, v_{\nu(N)}\}$, and let T denote the normalized adjacency matrix, so that $(\ell+1)T_{ij}$ is the number of edges from v_i to v_j. By Theorem 5.3.3, the matrix T is bi-stochastic and can be viewed as a time-homogenous irreducible Markov chain. As $\Lambda_\ell(N)$ is not bipartite, every eigenvalue of T, besides 1, has modulus smaller than 1. Thus, any initial probability distribution on $\Lambda_\ell(N)^V$ converges exponentially fast to the unique probability distribution $\frac{1}{\nu(N)} \sum_i \delta_{v_i}$, where δ_{v_i} is the Dirac distribution supported on v_i. (For $N = 2$ everything goes through the same; for $N = 1$ most of the considerations go through, but the limit measure need not be the one we have specified. For example, if $p = 11$ and $\ell = 5$, then T is $\frac{1}{6} \cdot \left(\begin{smallmatrix} 3 & 3 \\ 2 & 4 \end{smallmatrix}\right)$ and the stationary distribution is $\left(\begin{smallmatrix} 2/5 \\ 3/5 \end{smallmatrix}\right)$.)

With these considerations, to understand further the action of T_ℓ^n we may restrict our attention to a single disc. That is, we need to study the action of the monoid $\mathscr{H}_N^+(\underline{E})$ on the residue disc $D(\underline{E})$. This residue disc may be viewed as the generic rigid-analytic fibre $(\widetilde{D}(\overline{\underline{E}}))_{rig}$ of the formal scheme $\widetilde{D}(\overline{\underline{E}})$ that is the formal deformation space of the elliptic curve $\overline{\underline{E}}$; equivalently, by Serre–Tate and étaleness, of the p-divisible group $\overline{E}[p^\infty]$; equivalently, by Tate, of the formal group $\widehat{\overline{E}}$. The group $\mathscr{R}^\times$, and hence $\mathscr{H}_N$, can thus be interpreted as automorphism groups of $\widehat{\overline{E}}$. The work of Gross–Hopkins, which is our next topic, will allow us to consider instead the action of $\mathscr{H}_N$, that factors through $\mathscr{G}_N$, on $\mathbb{P}^1_{\mathbb{Q}_q}$. The methods we shall use will rely on the p-adic and Zariski closures of $\mathscr{G}_N$. As the groups $\mathbb{G}_N, G_N$ are well-understood by Corollary 5.5.5 and Proposition 5.5.6, this will prove to be a powerful technique.

We can view the formal deformation space $\widetilde{D}(\overline{E})$ as representing the functor $\mathscr{F}$ on complete local Noetherian $W(\mathbb{F}_q)$-algebras R with residue field k,

(5.1) $\qquad\qquad \mathscr{F}: \quad R \mapsto \mathscr{F}(R) = \{(\mathscr{E}, \varphi)\}/\text{isom.},$

where $\mathscr{E}$ is a p-divisible group over $\mathrm{Spec}(R)$, and $\varphi\colon \mathscr{E} \otimes_R k \to E[p^\infty] \otimes_{\mathbb{F}_q} k$ is an isomorphism. The group $\mathrm{Aut}(E[p^\infty])$, of which $\mathscr{H}_N$ is a subgroup, acts on the universal deformation space via its action on the functor: $\gamma \in \mathrm{Aut}(E[p^\infty])$ acts by

$$(\mathscr{E}, \varphi) \mapsto (\mathscr{E}, \gamma \circ \varphi).$$

Since the p-divisible group of $\overline{E}$ is connected, by a result of Tate, the functor of deformations of the formal group of $\overline{E}$ is equivalent to the function $\mathscr{F}$.

For $N = 1$ one uses the following diagram. Choose an auxiliary rigid N, and use the diagram:

$$
\begin{array}{ccc}
D(\underline{E}) & = & (\widetilde{D}(\overline{E}))_{rig} \\
\downarrow & & \quad\Big\downarrow{\scriptstyle \mathscr{H}_N^+ -\text{equivar.}}{\cong} \\
D(E) & = & (\widetilde{D}(\overline{E}))_{rig} \\
\downarrow & & \downarrow \\
D(E)/\mathrm{Aut}(\overline{E}) & = & (\widetilde{D}(\overline{E}))_{rig}/\mathrm{Aut}(\overline{E})
\end{array}
$$

We remark that the action of $\mathrm{Aut}(\overline{E})$ is non-trivial only when $\mathrm{Aut}(\overline{E}) \supsetneq \{\pm 1\}$, and this only happens at $j = 0, 1728$, if these are supersingular at all.

5.7. The work of Gross and Hopkins. In this section we review some of the work of Gross and Hopkins [20], specializing to cases of particular interest to us.

5.7.1. *The ideal disc.* Gross and Hopkins study one-dimensional connected p-divisible groups through one dimensional formal groups. In [20, p. 31] they construct a very particular universal typical formal group F of height n over the ring $\mathbb{Z}_p[\![u_1, \ldots, u_{n-1}]\!]$. The case that would interest us most is $n = 2$. Let $\overline{F}_0$ denote the reduction of F modulo the maximal ideal of $\mathbb{Z}_p[\![u_1, \ldots, u_{n-1}]\!]$; it is a formal group of dimension 1 and height n over $\mathbb{F}_p$, and, as in [20], we let F_0 be the specialization of F to a formal group over $\mathbb{Z}_p$ obtained by specializing all the u_i to 0. We denote $\overline{F} = \overline{F}_0 \otimes_{\mathbb{F}_p} \mathbb{F}_{p^n}$. (Note that our notation differs a little from [20].)

Consider the functor $\mathscr{F}^\star$ on the category of complete local noetherian $W(\mathbb{F}_{p^n})$-algebras $(R, \mathfrak{m}_R)$ with $p \in \mathfrak{m}_R$, $k_R := R/\mathfrak{m}_R$, given by

(5.2) $\ R \mapsto \mathscr{F}^\star(R)$

$$= \{G/R \text{ a formal group law } G \otimes_R k_R = \overline{F} \otimes_{\mathbb{F}_{p^n}} k_R\}/\star\text{-isom.}$$

Here, we say that G/R and G'/R are $\star$-*isomorphic* if there is an isomorphism $G \xrightarrow{\sim} G'$ over R, which reduces to the identity modulo $\mathfrak{m}_R$. This functor is representable by $W(\mathbb{F}_{p^n})[\![u_1, \ldots, u_{n-1}]\!]$, and $F \otimes_{\mathbb{Z}_p} W(\mathbb{F}_{p^n})$ is a universal object over it [20, p. 45].

Let $A_n = W(\mathbb{F}_{p^n})$; it is an unramified extension of $\mathbb{Q}_p$ of degree n that contains all $p^n - 1$ roots of unity. From the specific definition of F given in [20], it follows that $F_0 \otimes_{\mathbb{Z}_p} A_n$ has an action of A_n such that $[\zeta](x) = \zeta \cdot x$ for $\zeta \in \mu_{p^n-1}$. This induces an action of A_n on $\overline{F}$, making it into a formal A_n-module of height 1, with an induced embedding $j_n \colon A_n \to \mathrm{End}(\overline{F})$. The image of j_n along with the Frobenius morphism φ generate $\mathrm{End}(\overline{F})$. Indeed, we have

$$\mathrm{End}(\overline{F} \otimes_{\mathbb{F}_{p^n}} \overline{\mathbb{F}}_p) = \mathrm{End}(\overline{F}) = A_n \oplus A_n\varphi \oplus \cdots \oplus A_n\varphi^{n-1},$$

with $\varphi^n = p$, and $\varphi a = a^\sigma \varphi$, for $a \in A_n$, where σ denotes the Frobenius automorphism of A_n. The centre of $\mathrm{End}(\overline{F})$ is $\mathbb{Z}_p$. Note that every element b of $\mathrm{End}(\overline{F})$, being an endomorphism of a 1-dimensional formal group, is given by a power series $b(x) \in \mathbb{F}_{p^n}[\![x]\!]$.

5.7.2. The action of $\mathrm{Aut}(\bar{F})$ on $\mathrm{Spf}\, A_n[\![u_1, \ldots, u_{n-1}]\!]$. From the above discussion it follows that

$$\mathscr{A}_n := \mathrm{Aut}(\overline{F}) = A_n^\times \oplus A_n\varphi \oplus \cdots \oplus A_n\varphi^{n-1},$$

and its center is $\mathbb{Z}_p^\times$. The action of $\mathscr{A}_n$ on $\mathrm{Spf}\, A_n[\![u_1, \ldots, u_{n-1}]\!]$ is already described in [22] as follows: Given $b \in \mathscr{A}_n$, represented by the power series $b(x) \in \mathbb{F}_{p^n}[\![x]\!]$, let $b^{-1}(x)$ be the inverse of $b(x)$ relative to composition (so that $b(b^{-1}(x)) = x$, etc.) and lift $b^{-1}(x)$ to a power series $h(x) \in A_n[\![x]\!]$ in an arbitrary way. Given the universal formal group law F over $A_n[\![u_1, \ldots, u_{n-1}]\!]$, there is a unique group law F' over $A_n[\![u_1, \ldots, u_{n-1}]\!]$ such that

$$F'(h(x), h(y)) = h(F(x, y)).$$

Note that $F \xrightarrow{\sim} F'$ over the ring $A_n[\![u_1, \ldots, u_{n-1}]\!]$ via the map h, but this isomorphism is not a $\star$-isomorphism. By the universal property of F, there exists a unique automorphism $\beta(b)$ of $A_n[\![u_1, \ldots, u_{n-1}]\!]$ over A_n such that

$$\beta(b)F \underset{\star}{\simeq} F'.$$

(The notation $\beta(b)F$ means specializing F by applying the $\beta(b)$ to its coefficients.) The automorphism $\beta(b)$ depends only on b and not on the choice of h, since for varying h the formal group laws F' are all $\star$-isomorphic.

Here we have described the global action, but the action on points on the universal deformation space $A_n[\![u_1, \ldots, u_{n-1}]\!]$, namely on specializations of F through homomorphisms $A_n[\![u_1, \ldots, u_{n-1}]\!] \to R$, is virtually the same.

This describes the action of $\mathscr{A}_n$ via the $\star$-isomorphism model. If we consider the equivalent functor classifying $(G/R, \psi)$ a formal group law with

$\psi\colon G \otimes_R k_R \xrightarrow{\cong} \overline{F} \otimes_{\mathbb{F}_p} k_R$, up to isomorphism, we have a natural action of $\mathscr{A}_n$, where $b \in \mathscr{A}_n$ acts on $(G/R, \psi)$ by taking it to $(G/R, b \circ \psi)$. The following proposition is an easy exercise.

Proposition 5.7.1. *The two actions of $\mathscr{A}_n$ on the universal deformation space $A_n[\![u_1, \dots, u_{n-1}]\!]$ are the same.*

We thus get a homomorphism β, with kernel $\mathbb{Z}_p^\times$,

$$\beta\colon \mathscr{A}_n \longrightarrow \operatorname{Aut}_{A_n}(A_n[\![u_1, \dots, u_{n-1}]\!]).$$

It induces an action of $\mathscr{A}_n$ on the formal scheme $\widetilde{X} = \operatorname{Spf}(A_n[\![u_1, \dots, u_{n-1}]\!])$ and on the associated rigid space

$$X = \widetilde{X}_{rig} = (\operatorname{Spf}(A_n[\![u_1, \dots, u_{n-1}]\!]))_{rig}.$$

In [20, Proposition 14.13] we find that if R is a complete local noetherian A_n-algebra, and $x \in \widetilde{X}(R)$ with corresponding formal group law F_x, then the orbit of x under $\mathscr{A}_n$ is

$$\operatorname{Orb}(x) = \{y \in \widetilde{X}(R)\colon F_x \cong F_y \text{ over } R\}$$

(note that this is, of course, an isomorphism and not a $\star$-isomorphism) and

$$\operatorname{Stab}(x) = \operatorname{Aut}(F_x).$$

5.8. Canonical and quasi-canonical lifts: the supersingular case.
Now, we consider the case $n = 2$. Our main interest in this section is in points $x \in X$ that have a large endomorphism ring. They are tightly linked to dynamical aspects of the action of $\operatorname{Aut}(\overline{F})$ on X, and a fortiori to the action of $\mathscr{H}_N$ on X, as we shall see. But we initially consider the larger picture, which is the action of $\operatorname{Aut}(\overline{F})$. We consider points $x \in X$ such that

$$\operatorname{End}(F_x) \supsetneq \mathbb{Z}_p.$$

In this case, $\operatorname{End}(F_x)$ is an order in a quadratic field extension of $\mathbb{Q}_p$. Up to isomorphism there are finitely many such fields; they are in bijection with the non-identity elements of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. Fix models $\{K_i\} = \{K_1, \dots, K_r\}$ for these fields, and for $K \in \{K_i\}$ denote the ring of integers by $\mathcal{O}_K$. Let $\{1, \gamma_K\}$ be the automorphism group of $K/\mathbb{Q}_p$.

5.8.1. We first classify $x \in X$ according to the isomorphism class K_i of the field $K_x := \operatorname{End}^0(F_x)$.

Fix then $K \in \{K_i\}$ and consider points x such that $K_x \cong K$. We have then

$$\operatorname{End}(F_x) \cong \mathcal{O}_{K,s_x} := \mathbb{Z}_p + p^{s_x}\mathcal{O}_K,$$

and we call the non-negative integer s_x the *level*, or *conductor*, of x. Choose an isomorphism $\iota_x\colon \mathcal{O}_{K,s_x} \to \operatorname{End}(F_x)$. It is unique up to composition with

γ_K; when we want to refer to the pair of embeddings we shall write $\iota_x^\pm$. The map ι_x induces an embedding

$$\bar{\iota}_x \colon \mathcal{O}_{K,s_x} \hookrightarrow \mathrm{End}(\overline{F}) \cong \mathscr{R}.$$

As the order $\mathscr{R}$ consists of all integral elements of $\mathscr{B}$, the embedding $\bar{\iota}_x$ extends uniquely to an embedding $\bar{\iota} \colon \mathcal{O}_K \hookrightarrow \mathrm{End}(\overline{F})$. Thus, any embedding $\bar{\iota}_x$ comes from an "optimal embedding".

Given $d \in \mathscr{R}^\times \setminus \mathbb{Z}_p^\times$, it will be convenient to denote $\mathcal{O}_{K,s(d)}$ the order isomorphic to $\mathbb{Z}_p[d]$, and denote ι_d its embedding into $\mathrm{End}(\overline{F})$.

5.8.2. Fix an embedding $\bar{\iota} \colon \mathcal{O}_K \to \mathrm{End}(\overline{F})$. Let $QC(\bar{\iota}, K, s)$ be the set of points x of X such that $K_x \cong K$, $s_x = s$ and ι_x extends to $\bar{\iota}$. These are the quasi-canonical lifts relative to $\bar{\iota}$ of level s. Let $qc(K, s) = \sharp QC(\bar{\iota}, K, s)$ (it is independent of $\bar{\iota}$). Gross [16] gives the following formula:

$$(5.3) \qquad qc(K, s) = \begin{cases} 1 & \text{if } s = 0, \\ (p+1)p^{s-1} & s > 0, K \text{ unramified}, \\ p^s & s > 0, K \text{ ramified}. \end{cases}$$

Caution. Note that what Gross calls a quasi-canonical lift x of level s is a point of $QC(\bar{\iota}, K, s)$ if s is even, and a point of $QC(\varphi\bar{\iota}\varphi^{-1}, K, s)$ if s is odd, where $\varphi \colon \overline{F} \to \overline{F}$ is Frobenius. Nonetheless, the result about $qc(K, s)$ quoted from [16] is valid, as $\varphi\bar{\iota}\varphi^{-1}$ is an embedding $\mathcal{O}_K \to \mathscr{R}$ as well.

5.8.3. The sets of points we have defined enjoy an action of $\mathscr{B}^\times$ coming from conjugating the embedding $\bar{\iota}$. An element $\gamma \in \mathscr{B}^\times$ induces, for any K and s, a bijection

$$QC(\bar{\iota}, K, s) \xrightarrow{\sim} QC(\gamma\bar{\iota}\gamma^{-1}, K, s).$$

We are interested in the action of $\mathscr{R}^\times = \mathrm{Aut}(\overline{F})$. Consider the surjective homomorphism $\nu := \mathrm{ord} \circ \mathrm{Nm} : \mathscr{B}^\times \to \mathbb{Z}$, where Nm is the reduced norm and ord is p-adic valuation. In the model $\left\{ \left(\begin{smallmatrix} a & pb^\sigma \\ b & a^\sigma \end{smallmatrix} \right) \right\}$, $\nu = \mathrm{ord} \circ \det$ and so we see that $\mathscr{R}^\times = \mathrm{Ker}(\nu)$ and $\mathscr{B}^\times/\mathscr{R}^\times \cong \mathbb{Z}$. As by Skolem–Noether $\mathscr{B}^\times$ acts transitively on the set of embeddings $\bar{\iota} \colon K \to \mathscr{B}$ (they are all optimal), the orbits of $\mathscr{R}^\times$ on the set of these embeddings are in bijection with $\mathscr{B}^\times/\mathscr{R}^\times \cdot \mathrm{Cent}_{\mathscr{B}^\times}(\bar{\iota}(K)) = \mathscr{B}^\times/\mathscr{R}^\times \cdot \bar{\iota}(K^\times)$. As $\nu|_K = \mathrm{ord} \circ \mathrm{Nm}_{K/\mathbb{Q}_p}$ we find that the $\mathscr{R}^\times$-orbits in the set of optimal embeddings $\mathcal{O}_K \to \mathscr{R}$ are in bijection with $\mathbb{Z}/\mathrm{ord}(\mathrm{Nm}(K^\times))$. Therefore:

- If $K/\mathbb{Q}_p$ is ramified, $\mathrm{Aut}(\overline{F})$ acts transitively on the set of embeddings $\bar{\iota} \colon \mathcal{O}_K \to \mathscr{R}$. In this action, the centralizer $\mathrm{Cent}(\bar{\iota})$ is $\bar{\iota}(K^\times)$ and the normalizer satisfies $\mathrm{Norm}(\bar{\iota})/\mathrm{Cent}(\bar{\iota}) \cong \{1, \gamma_K\}$, where the non-trivial class indeed induces γ_K by its conjugation action. We remark that this persists also when we take the normalizer and centralizer in $\mathscr{R}^\times$.

- If $K/\mathbb{Q}_p$ is unramified, there are two orbits for the action of $\mathscr{R}^\times$ on the set of embeddings $\bar{\iota}\colon \mathcal{O}_K \to \mathscr{R}$. Again, we have $\mathrm{Norm}(\bar{\iota})/\mathrm{Cent}(\bar{\iota}) \cong \{1, \gamma_K\}$, but if we take the normalizer and centralizer in $\mathscr{R}^\times$, we have $\mathrm{Norm}(\bar{\iota}) \cap \mathscr{R}^\times / \mathrm{Cent}(\bar{\iota}) \cap \mathscr{R}^\times \cong \{1\}$. To see that, consider the standard inclusion $K \to \mathscr{B}$ given by $a \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & a^\sigma \end{smallmatrix}\right)$, where the normalizer is generated over the centralizer by $\varphi = \left(\begin{smallmatrix} 0 & p \\ 1 & 0 \end{smallmatrix}\right)$ (a non-integral element). The two $\mathscr{R}^\times$ orbits are thus distinguished by the induced action on the tangent space of $\overline{F}$. Note, however, that even in this case, $\mathrm{Aut}(\overline{F})$ acts transitively on the subrings of $\mathscr{B}$ that are isomorphic to $\mathcal{O}_K$.

5.8.4. Consider now $b \in \mathscr{R}^\times$ and the automorphism $\beta(b)$ of X induced by it. If $b \in \mathbb{Z}_p^\times$ then $\beta(b)$ is the identity map, and conversely. We are interested in the periodic points $\mathrm{Per}(b)$ of $\beta(b)$ (in particular in the fixed points $\mathrm{Fix}(b)$), and so we may assume $b \notin \mathbb{Z}_p^\times$.

- If b has finite order in $\mathscr{R}^\times/\mathbb{Z}_p^\times$, then $\mathrm{Per}(b) = X$.
- If b has infinite order in $\mathscr{R}^\times/\mathbb{Z}_p^\times$ and $x \in X$ is a periodic point of length r, say, then x is a fixed point of $\beta(b^r)$. Note that there are two embeddings associated to b^r,

$$\bar{\iota}_{b^r}^\pm \colon \mathcal{O}_{K,s} \to \mathscr{B},$$

where $K \in \{K_i\}$ is the unique field isomorphic to $\mathbb{Q}_p(b^r) = \mathbb{Q}_p(b)$ and $s = s(b^r)$ is the level. We therefore next direct our attention to fixed points.

5.8.5. Let $d \in \mathscr{R}^\times, d \notin \mathbb{Z}_p^\times$. As noted $\mathrm{Fix}(\beta(d)) = \{x : d \in \mathrm{End}(F_x)\}$. If so, $\mathrm{End}(F_x)$ is an order of conductor $s_x \leq s(d)$. Furthermore, the associated pair of embeddings $\iota_x^\pm \colon \mathcal{O}_{K_x, s_x} \to \mathrm{End}(\overline{F})$ extend $\bar{\iota}_d^\pm$. Let K be the representative isomorphic to $\mathbb{Q}_p[d]$. Then,

$$
\begin{aligned}
\mathrm{Fix}(d) &= \bigcup_{s \leq s(d)} QC(\bar{\iota}_d^\pm, K, s) \\
&= \bigcup_{s \leq s(d)} \{x \in X : K_x \cong \mathbb{Q}_p[d], s_x = s, \bar{\iota}_x^\pm = \bar{\iota}_d^\pm\}.
\end{aligned}
$$
(5.4)

We return to periodic points for $\beta(b)$, assuming b is of infinite order in $\mathscr{R}^\times/\mathbb{Z}_p^\times$. It's an easy exercise that $\sup\{s(b^r) : r \geq 1\} = \infty$. Let K be the representative isomorphic to $\mathbb{Q}_p[b]$. Then,

$$
\begin{aligned}
\mathrm{Per}(b) &= \bigcup_{r \geq 1} \mathrm{Fix}(b^r) \\
&= \bigcup_{s \geq 0} QC(\bar{\iota}_b^\pm, K, s) \\
&= \{x \in X : K_x \cong K, \bar{\iota}_x^\pm = \bar{\iota}_b^\pm\}
\end{aligned}
$$
(5.5)

(the abuse of notation $\bar{\iota}_b = \bar{\iota}_{b^r}$ is justified). Some information about the location of the periodic points can be found in [16, 20].

5.8.6. We can draw some immediate conclusions concerning the action of $\mathscr{H}_N$ on X. For one, for every element b of $\mathscr{H}_N$, viewed as a branch of the Hecke operator T_ℓ^n for some n, the fixed and periodic points of $\beta(b)$ are given by Sections 5.8.4–5.8.5. In addition, in contrast to the ordinary case:

Corollary 5.8.1. *The elements of $\mathscr{A}_2 = \mathscr{R}^\times$ do not have a common fixed point. In fact there is no finite subset of X that is stable under $\mathscr{H}_N$.*

Proof. The first statement follows easily, since we may pick integral elements b_1, b_2, generating distinct quadratic extensions inside $\mathscr{B}$. Then $\mathrm{Fix}(b_1) \cap \mathrm{Fix}(b_2) = \emptyset$. In fact, as in the proof of Proposition 5.4.2, we can choose $b_i \in \mathscr{H}_N$ such that $b_i^{n_i} \notin \mathbb{Z}_p^\times$, for all $n_i > 0$.

As to the second statement, if S is a finite set stable under $\mathscr{H}_N$, then, for suitable $n_i > 0$, we have $S \subseteq \mathrm{Fix}(b_i^{n_i}), i = 1, 2$. But, we still have $\mathrm{Fix}(b_1^{n_1}) \cap \mathrm{Fix}(b_2^{n_2}) = \emptyset$. Thus, $S = \emptyset$. □

5.9. The Gross–Hopkins period map. We specialize the results of Gross–Hopkins to the case $n = 2$. Recall our notation from Section 5.1: $q = p^2$, $\mathbb{Q}_q$ is the quadratic unramified extension of $\mathbb{Q}_p$.

In their paper [20] Gross and Hopkins construct a period map

$$\Phi \colon X \to \mathbb{P}^1$$

of rigid-analytic spaces over $\mathbb{Q}_p$ with the following properties ([20, in particular Lemma 19.3 and Corollary 23.15]):

(1) Φ is a morphism of rigid spaces that is étale and surjective.
(2) Φ is equivariant for the action of $\mathscr{A}_2$, where $\mathscr{A}_2 = \{ \left(\begin{smallmatrix} a & pb^\sigma \\ b & a^\sigma \end{smallmatrix} \right) \colon a \in W(\mathbb{F}_q)^\times, b \in W(\mathbb{F}_q) \} \subset \mathrm{GL}_2(\mathbb{Q}_q)$, acting through Möbius transformations on $\mathbb{P}^1$.
(3) Furthermore, Φ restricts to a rigid-analytic isomorphism

$$J \colon = \{x \in X \colon \mathrm{ord}(x) \geq 1/2\} \overset{\sim}{\longrightarrow} U \colon = \{w \colon \mathrm{ord}(w) \geq 1/2\} \subset \mathbb{P}^1_{(w_0 \colon w_1)}$$

In particular, the map Φ induces a bijection between the $\mathbb{Q}_{p^2}$ points of J and U. Under this map the point 0, corresponding to the formal group F_0, is mapped to the point $w = 0 = (1 : 0)$ (sic!), where $w = w_1/w_0$. Furthermore, both J and U are $\mathscr{A}_2$-invariant.

5.9.1. *Reduction to the ideal disc.* Above we have discussed the work of Gross–Hopkins that relates to the deformation of a very particular formal group that we denoted $\overline{F}$. To connect it with our main subject, let E be a supersingular elliptic curve defined over a finite extension k of $\mathbb{F}_q$, and P a point of order N on E. Then E has a unique model E_1 over

$\mathbb{F}_q$ whose Frobenius endomorphism φ satisfies $\varphi^2 = p$ (Lemma 5.2.3). Using [17, Proposition 24.2.9], we find that the formal group $\widehat{E}_1$ is isomorphic to $\overline{F}$ over $\mathbb{F}_q$, as the property $\varphi^2 = p$ holds for $\overline{F}$ as well. Fix such an isomorphism. Then the universal deformation spaces of $\underline{E} = (E, P)$ and $\overline{F}$ become isomorphic after base change to $W(k)$. We remark that the functor $\mathscr{F}^\star$ in (5.2) (in the case $n = 2$) is naturally equivalent to $\mathscr{F}$ in (5.1) (see [22, Proposition 3.3] and that allows us to use [20, 22]).

The associated rigid space $X_{\underline{E}} = D(\underline{E})$ inherits an action of $\mathscr{A}_2$ and an equivariant period map $\Phi \colon X_{\underline{E}} \to \mathbb{P}^1$ over $W(k)[p^{-1}]$, as well as a base point 0 corresponding to the unique A_2-formal module (none other than F_0) lifting $\widehat{E}$.

Lemma 5.9.1. *Let K be a quadratic imaginary field in which p is either inert or ramified. Let $E/\overline{\mathbb{Q}}_p$ be an elliptic curve with CM by an order of K of conductor prime to p. Then $\mathbb{Q}_p(j(E))$ is a finite extension of $\mathbb{Q}_p$ of ramification index at most 2. In fact, if p is inert in K, $\mathbb{Q}_p(j(E))$ is at most a quadratic unramified extension of $\mathbb{Q}_p$, while if p is ramified in K, $\mathbb{Q}_p(j(E))$ has degree dividing 4 over $\mathbb{Q}_p$.*

Proof. Assume that E has CM by $R_\mathfrak{f}$, the order of conductor $\mathfrak{f} \in \mathbb{Z}_{\geq 1}$ in $\mathcal{O}_K$. Let $K(\mathfrak{f})$ denote the ring class field of conductor $\mathfrak{f}$ over K. Let V denote the set of all finite places of K, and for $v \in V$, denote by O_v (resp., K_v) the completion of $\mathcal{O}_K$ (resp., K) at v. Let $\pi_v \colon \mathcal{O}_v^\times \to (\mathcal{O}_v/\mathfrak{f}\mathcal{O}_v)^\times$ be the natural projection. Under the isomorphism of class field theory, $K(\mathfrak{f})$ corresponds to the subgroup $K^\times W \subset \mathbb{A}_K^\times$, where W is given by $W = \Pi_{v \in V} W_v$, and W_v is defined as

$$W_v = \begin{cases} \pi_v^{-1}((\mathbb{Z}/\mathfrak{f}\mathbb{Z})^\times) & v | \mathfrak{f}, \\ \mathcal{O}_{K,v}^\times & v \nmid \mathfrak{f}. \end{cases}$$

Let $\mathfrak{p}$ denote the unique prime of K above p, and choose a prime $\widetilde{\mathfrak{p}}$ of $K(\mathfrak{f})$ above $\mathfrak{p}$. By class field theory, the local field $K(\mathfrak{f})_{\widetilde{\mathfrak{p}}}$ corresponds to the subgroup $K^\times W \cap K_\mathfrak{p} \subset K_\mathfrak{p}^\times$. Let us denote by $\mathrm{Pic}(R_\mathfrak{f})$ the ideal class group of $R_\mathfrak{f}$. Let a denote the order of $[\mathfrak{p}]$ in $\mathrm{Pic}(R_\mathfrak{f})$. Then

$$K^\times W \cap K_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^\times \varpi_\mathfrak{p}^{a\mathbb{Z}},$$

where $\varpi_\mathfrak{p}$ is a choice of a uniformizer in $\mathcal{O}_\mathfrak{p}$. In particular, we find that $K(\mathfrak{f})_{\widetilde{\mathfrak{p}}}$ is an unramified extension of degree a over $K_\mathfrak{p}$. By the theory of complex multiplication we have $K(j(E)) = K(\mathfrak{f})$. Hence, it is enough to show that $K(\mathfrak{f})_{\widetilde{\mathfrak{p}}}$ satisfies the conditions stated in the lemma. If p is inert in K, then $K_\mathfrak{p} = \mathbb{Q}_{p^2}$ and $a = 1$. If p is ramified in K, then $K_\mathfrak{p}$ is a quadratic ramified extension of $\mathbb{Q}_p$ and $a \leq 2$. This proves the lemma. $\square$

Corollary 5.9.2. *All CM points of conductor prime to p in the residue disc $D(\underline{E})$ lie in $J(\mathbb{Q}_q)$.*

5.10. Dynamics implications - II: Ideas from ergodic theory. By Corollary 5.9.2, all CM points of discriminant prime to p in $D(\underline{E})$ lie in the set J defined above. Clearly, if we wish to understand the action of $\mathscr{A}_2$ on J (and in particular on such CM points) we may as well study the action of $\mathscr{A}_2$ on U. More precisely, we are interested in the action of $\mathscr{H}_N$ on J and we may reduce it to the very explicitly described action of $\mathscr{G}_N$ on U (see Corollary 5.5.5).

This is a fortunate setting, achieved at the price of restricting our attention to "mildly ramified" CM points that lie in a particular small disc within $D(\underline{E})$. The general case is more complex and indeed the map Φ is given by a complex formula ([20, (25.6), (25.7)]) that makes it hard to translate results for $\mathbb{P}^1$ to results for $D(\underline{E})$.

5.10.1. *Minimal sets.* Let $\mathbb{K}$ be a field extension of $\mathbb{Q}_q$. We denote by $J(\mathbb{K})$, $U(\mathbb{K})$, etc., points of J, U, etc., with coordinates in $\mathbb{K}$. Recall that $\mathbb{H}_N$ is the closure of $\mathscr{H}_N$ and of $\mathscr{H}_N^+$ in $\mathscr{R}^\times = \mathscr{A}_2$. The groups $\mathbb{H}_N$, $\mathrm{sat}(\mathbb{H}_N)$, $\mathbb{G}_N$ are the same in their action on $\mathbb{P}^1(\mathbb{K})$, and in fact act by isometries on $U(\mathbb{K})$. This follows from the identity $\gamma x - \gamma y = \frac{(x-y)(aa^\sigma - pbb^\sigma)}{(bx+a^\sigma)(by+a^\sigma)}$, for $\gamma = \left(\begin{smallmatrix} a & pb^\sigma \\ b & a^\sigma \end{smallmatrix}\right)$.

An $\mathbb{H}_N$-*minimal set* of $\mathbb{P}^1(\mathbb{K})$ is an $\mathbb{H}_N$-invariant non-empty closed set that is minimal relative to these properties.

Proposition 5.10.1. *The $\mathbb{H}_N$-minimal sets S are the sets of the form $\mathbb{H}_N \cdot f$, for some $f \in \mathbb{P}^1(\mathbb{K})$. Furthermore, $\mathbb{H}_N \cdot f = \overline{\mathscr{H}_N^+ \cdot f}$.*

Proof. First note that for any f we have that $\mathbb{H}_N \cdot f$ is closed (in fact, compact) because $\mathbb{H}_N$ is compact and the action of $\mathrm{GL}_2(\mathbb{K})$ on $\mathbb{P}^1(\mathbb{K})$ is continuous. If S is minimal, pick any $f \in S$, then $\mathbb{H}_N \cdot f \subseteq S$ is closed and $\mathbb{H}_N$-invariant, hence equal to S. Conversely, consider a set $\mathbb{H}_N \cdot f$ for some $f \in \mathbb{P}^1(\mathbb{K})$. As an $\mathbb{H}_N$-minimal subset contained in $\mathbb{H}_N \cdot f$ contains an element of the form γf for some $\gamma \in \mathbb{H}_N$ and so it also contains $\mathbb{H}_N \cdot \gamma f = \mathbb{H}_N \cdot f$.

To prove the rest, one proves that $\overline{\mathscr{H}_N^+ \cdot f} = \overline{\mathscr{H}_N^+} \cdot f = \mathbb{H}_N \cdot f$: On the one hand, $\overline{\mathscr{H}_N^+} \cdot f$ is closed and contains $\mathscr{H}_N^+ \cdot f$, hence also its closure. On the other hand, let $\gamma_i \in \mathscr{H}_N^+, \gamma_i \to \gamma$, then also $\gamma_i \cdot f \to \gamma \cdot f$. This shows that $\overline{\mathscr{H}_N^+} \cdot f \subseteq \overline{\mathscr{H}_N^+ \cdot f}$. $\qquad\square$

5.10.2. *Measures.* Our proof in Proposition 5.4.2 that $\mathscr{G}_N$ is finitely generated in fact supplied us with a set of $t = t(N)$ elements,

$$\Gamma = \{\gamma_1, \ldots, \gamma_t\},$$

in $\mathscr{H}_N^+$ that generate the image of $\mathscr{H}_N^+$ in $\mathrm{PGL}_2(\mathbb{Q}_q)$ as a monoid. We include the identity among them. Note that there is no canonical choice of such elements, though we chose the generators to be the set of all elements

of $\mathscr{H}_N^+$ obtained from closed labeled walks of explicitly bounded length. Let $\mu = \mu(N, \Gamma)$ be the atomic measure of $\mathrm{GL}_2(\mathbb{Q}_q)$ supported on Γ. Namely,

$$\mu = \frac{1}{t} \sum_{i=1}^{t} \delta_{\gamma_i}.$$

The following lemma is clear.

Lemma 5.10.2. *The group* $\mathbb{H}_N$ *is the minimal closed monoid of* $\mathrm{GL}_2(\mathbb{Q}_q)$ *(in the p-adic topology) containing the support of* μ. *To underline that, denote it in the sequel* $\mathbb{H}_{N,\mu}$.

We use the work of Benoist and Quint [2]; see also the references [3, 12] for general background material. In particular, [2] implies the following:

Theorem 5.10.3. *The map* $\nu \mapsto \mathrm{Supp}(\nu)$ *is a bijection*

$$\{\mu\text{-ergodic probability measures on } U(\mathbb{K})\}$$

$$\Leftrightarrow \{\mathbb{H}_{N,\mu}\text{-minimal subsets of } U(\mathbb{K})\}.$$

Corollary 5.10.4. *There is a unique* $\mathbb{H}_{N,\mu}$-*ergodic measure* $\nu(\mu)$ *on* $U(\mathbb{Q}_q)$, *hence a unique* $\mathbb{H}_{N,\mu}$-*stationary probability measure. Its support is* $U(\mathbb{Q}_q)$.

Proof. The μ-ergodic measures on $U(\mathbb{Q}_q)$ are in one-one correspondence with $\mathbb{H}_{N,\mu}$-minimal sets. We claim that $\mathscr{R}_\square^\times$ acts transitively on $U(\mathbb{Q}_q)$: given $x \in U(\mathbb{Q}_q)$, for any $a \in W(\mathbb{F}_q)^\times$ the matrix $\left(\begin{smallmatrix} a & p\ (xa)^\sigma \\ xa & a^\sigma \end{smallmatrix}\right)$ takes $(1,0)$ to x and has determinant $aa^\sigma(1 - pxx^\sigma)$ which for an appropriate choice of a lies in $(\mathbb{Z}_p^\times)^2\langle \ell \rangle$. That is, it belongs to $\mathscr{R}_\square^\times$.

As $\mathscr{R}_\square^\times$ acts transitively on $U(\mathbb{Q}_q)$ we can write $U(\mathbb{Q}_q) = \mathscr{R}_\square^\times/B$, where B is the stabilizer of $(1,0)$ in $\mathscr{R}_\square^\times$ and it contains $\mathbb{Z}_p^\times$. Thus, by Proposition 5.10.1, the minimal orbits are in bijection with

$$\mathbb{H}_{N,\mu}\backslash\mathscr{R}_\square^\times/B = \mathrm{sat}(\mathbb{H}_{N,\mu})\backslash\mathscr{R}_\square^\times/B,$$

which is a singleton. The ergodic measures are the extremal points of the convex closed set of probability measures on the compact metric space $U(\mathbb{Q}_q)$ and the Krein–Milman theorem (see e.g., [29, Chapter 8]) then provides the uniqueness of the $\mathbb{H}_{N,\mu}$-stationary probability measure. $\qquad \square$

By Proposition 5.5.6 the Zariski closure H_N of $\mathscr{H}_N^+$ is $\mathrm{GL}_2(\mathbb{Q}_q)$, and is in particular reductive. We may therefore apply the results of Benoist and Quint [2] and conclude the following.

Theorem 5.10.5. *For every* $x \in U(\mathbb{K})$ *the measure*

$$(5.6) \qquad\qquad \nu_x = \lim_{n \to \infty} \frac{1}{n+1} \sum_{k=0}^{n} \mu^{*k} * \delta_x$$

exists and is a μ-*stationary measure, depending continuously on* x. *Thus, if* $x \in U(\mathbb{Q}_q)$, $\nu_x = \nu(\mu)$ *and is independent of* x.

Note that $\sum_{k=0}^{n} \mu^{*k} * \delta_x$ is nothing but the images of x (counted with multiplicities) under the composition of up to n automorphisms of the form $\gamma_1^{-1}, \ldots, \gamma_t^{-1}$. This theorem is the measure-theoretic manifestation that the orbit of x is "well-distributed" in the closure of its orbit. Note that while the measure depends on Γ, the support of the measure, i.e. $\mathbb{H}_{N,\mu} \cdot x$, does not. Thus, whatever "branches" of the Hecke operator T_ℓ we choose, the orbit is well-distributed in its closure that is independent of N.

While the theorem above can viewed as a non-commutative analogue of the weak law of large numbers, the next result is the analogue of the strong law of large numbers.

Theorem 5.10.6. *For every* $x \in U(\mathbb{K})$*, for almost all sequences* $\gamma = (\gamma_{i_n})_{n=1}^{\infty}$*,* $\gamma_{i_n} \in \{\gamma_1, \ldots, \gamma_t\}$*, the measure*

$$(5.7) \qquad \nu_{x,\gamma} = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \delta_{\gamma_{i_n}^{-1}\ldots\gamma_{i_1}^{-1}x}$$

exists and is a μ-stationary μ-ergodic probability measure. Furthermore,

$$\nu_x = \int \nu_{x,\gamma}\, \mathrm{d}\gamma.$$

In particular, if $x \in U(\mathbb{Q}_q)$

$$\nu_{x,\gamma} = \nu_x = \nu(\mu).$$

Finally, we recall the implications for CM points.

Theorem 5.10.7. *Let* $x = \underline{E} = (E, P)$ *be a CM point of supersingular reduction on* $X_1(N)$*,* $N \geq 3$*, such that* $\mathrm{End}(E)$ *has discriminant prime to* p*. Let* $\mathscr{H}_N^+ = \mathscr{H}_N^+(\underline{E})$ *denote the set of branches of the iterations of the Hecke operator* T_ℓ *returning to the residue disc* $D = D(\underline{E})$*. Let* $\mathbb{H}_{N,\mu}$ *be its p-adic closure equipped with the probability measure μ relative to the generators* $\{\gamma_1, \ldots, \gamma_t\}$ *as defined above.*

There is a unique $\mathbb{H}_{N,\mu}$*-invariant (ergodic) probability measure* $\nu(\mu)$ *on* $J(\mathbb{Q}_q)$*, and we have*

$$(5.8) \qquad \nu(\mu) = \lim_{n\to\infty} \frac{1}{n+1} \sum_{k=0}^{n} \mu^{*k} * \delta_x$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \delta_{\gamma_{i_n}^{-1}\ldots\gamma_{i_1}^{-1}x},$$

for almost all sequences $\gamma = (\gamma_{i_n})_{n=1}^{\infty}$*,* $\gamma_{i_n} \in \{\gamma_1, \ldots, \gamma_t\}$*.*

and the London Mathematical society through its Research Grant is grate-
fully acknowledged. We thank the referees for excellent suggestions that
allowed us to strengthen our results in the supersingular case and improve
the overall presentation.

References

[1] M. H. Baker, E. González-Jiménez, J. González & B. Poonen, "Finiteness results for modular curves of genus at least 2", *Am. J. Math.* **127** (2005), no. 6, p. 1325-1387.

[2] Y. Benoist & J.-F. Quint, "Random walks on projective spaces", *Compos. Math.* **150** (2014), no. 9, p. 1579-1606.

[3] ———, *Random walks on reductive groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., vol. 62, Springer, 2016.

[4] P. Berthelot, "Cohomologie rigide et cohomologie rigide à supports propres. Première partie", prépublication IRMAR 96-03, 89 pages, available from `https://perso.univ-rennes1.fr/pierre.berthelot/`, 1996.

[5] C.-L. Chai, "Hecke orbits as Shimura varieties in positive characteristic", in *Proceedings of the international Congress of Mathematicians. Vol. II*, European Mathematical Society, 2006, p. 295-312.

[6] C.-L. Chai & F. Oort, "Moduli of abelian varieties and *p*-divisible groups", in *Arithmetic geometry*, Clay Mathematics Proceedings, vol. 8, American Mathematical Society, 2009, p. 441-536.

[7] ———, "Monodromy and irreducibility of leaves", *Ann. Math.* **173** (2011), no. 3, p. 1359-1396.

[8] L. Clozel & E. Ullmo, "Équidistribution de sous-variétés spéciales", *Ann. Math.* **161** (2005), no. 3, p. 1571-1588.

[9] ———, ":Équidistribution adélique des tores et équidistribution des points CM", *Doc. Math.* **Extra Vol.** (2006), p. 233-260.

[10] B. Conrad, "Several approaches to non-Archimedean geometry", in *p-adic geometry*, University Lecture Series, vol. 45, American Mathematical Society, 2008, p. 9-63.

[11] D. Disegni, "*p*-adic equidistribution of CM points", `https://arxiv.org/abs/1904.07743`, 2019.

[12] M. Einsiedler & T. Ward, *Ergodic theory with a view towards number theory*, Graduate Texts in Mathematics, vol. 259, Springer, 2011.

[13] N. Elkies, K. Ono & T. Yang, "Reduction of CM elliptic curves and modular function congruences", *Int. Math. Res. Not.* **2005** (2005), no. 44, p. 2695-2707.

[14] E. Z. Goren & P. L. Kassaei, "Canonical subgroups over Hilbert modular varieties", *J. Reine Angew. Math.* **670** (2012), p. 1-63.

[15] B. H. Gross, "Heights and the special values of *L*-series", in *Number theory (Montreal, Quebec, 1985)*, CMS Conference Proceedings, vol. 7, American Mathematical Society, 1985, p. 115-187.

[16] ———, "On canonical and quasicanonical liftings", *Invent. Math.* **84** (1986), no. 2, p. 321-326.

[17] M. Hazewinkel, *Formal groups and applications*, AMS Chelsea Publishing, 2012, corrected reprint of the 1978 original.

[18] S. Herrero, R. Menares & J. Rivera-Letelier, "*p*-adic distribution of CM points and Hecke orbits. II. Linnik equidistribution on the supersingular locus", to appear.

[19] ———, "*p*-adic distribution of CM points and Hecke orbits. I: Convergence towards the Gauss point", *Algebra Number Theory* **14** (2020), no. 5, p. 1239-1290.

[20] M. J. Hopkins & B. H. Gross, "Equivariant vector bundles on the Lubin-Tate moduli space", in *Topology and representation theory (Evanston, IL, 1992)*, Contemporary Mathematics, vol. 158, American Mathematical Society, 1992, p. 23-88.

[21] N. Katz, "Serre–Tate local moduli", in *Algebraic surfaces (Orsay, 1976–78)*, Lecture Notes in Mathematics, vol. 868, Springer, 1981, p. 1976-78.

[22] J. LUBIN & J. TATE, "Formal moduli for one-parameter formal Lie groups", *Bull. Soc. Math. Fr.* **94** (1966), p. 49-59.

[23] W. MESSING, *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, vol. 264, Springer, 1972.

[24] F. OORT, "Foliations in moduli spaces of abelian varieties and dimension of leaves", in *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. II*, Progress in Mathematics, vol. 270, Birkhäuser, 2009, p. 465-501.

[25] N. T. SARDARI, "Optimal strong approximation for quadratic forms", *Duke Math. J.* **168** (2019), no. 10, p. 1887-1927.

[26] S. SAWYER, "Isotropic random walks in a tree", *Z. Wahrscheinlichkeitstheor. Verw. Geb.* **42** (1978), no. 4, p. 279-292.

[27] J.-P. SERRE, "Two letters on quaternions and modular forms (mod p)", *Isr. J. Math.* **95** (1996), p. 281-299.

[28] J. H. SILVERMAN, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009.

[29] B. SIMON, *Convexity. An analytic viewpoint*, Cambridge Tracts in Mathematics, vol. 187, Cambridge University Press, 2011.

[30] A. V. SUTHERLAND, "Isogeny volcanoes", in *ANTS X–Proceedings of the Tenth Algorithmic Number Theory Symposium*, The Open Book Series, vol. 1, Mathematical Sciences Publishers, 2013, p. 507-530.

[31] W. WOESS, *Random walks on infinite graphs and groups*, Cambridge Tracts in Mathematics, vol. 138, Cambridge University Press, 2000.

Eyal Z. GOREN
Department of Mathematics and Statistics
McGill University
805 Sherbrooke St. W.
Montreal H3A 0B9, QC, Canada
E-mail: eyal.goren@mcgill.ca
URL: https://www.math.mcgill.ca/goren/

Payman L KASSAEI
Department of Mathematics
King's College London
Strand, London WC2R 2LS, United Kingdom
E-mail: payman.kassaei@kcl.ac.uk
URL: https://nms.kcl.ac.uk/payman.kassaei/