Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

On a probabilistic local-global principle for torsion on elliptic curves

par John Cullinan, Meagan Kenney et John Voight

Résumé. Soit m un entier positif et soit E une courbe elliptique sur $\mathbf{Q}$ avec la propriété que $m \mid \#E(\mathbf{F}_p)$ pour un ensemble de densité 1 de nombres premiers p. En nous appuyant sur les travaux de Katz et Harron–Snowden, nous étudions la probabilité que $m \mid \#E(\mathbf{Q})_{\mathrm{tor}}$: nous trouvons qu'elle est non nulle pour tout $m \in \{1, 2, \ldots, 10\} \cup \{12, 16\}$ et nous le calculons exactement quand $m \in \{1, 2, 3, 4, 5, 7\}$. En complément, nous donnons un décompte asymptotique de courbes elliptiques avec une structure de niveau supplémentaire lorsque la courbe modulaire paramétrable résulte du quotient par un groupe sans torsion de genre zéro.

Abstract. Let m be a positive integer and let E be an elliptic curve over $\mathbf{Q}$ with the property that $m \mid \#E(\mathbf{F}_p)$ for a density 1 set of primes p. Building upon work of Katz and Harron–Snowden, we study the probability that $m \mid \#E(\mathbf{Q})_{\mathrm{tor}}$: we find it is nonzero for all $m \in \{1, 2, \ldots, 10\} \cup \{12, 16\}$ and we compute it exactly when $m \in \{1, 2, 3, 4, 5, 7\}$. As a supplement, we give an asymptotic count of elliptic curves with extra level structure when the parametrizing modular curve arises from the quotient by a torsion-free group of genus zero.

1. Introduction

1.1. Motivation. Let E be an elliptic curve over $\mathbf{Q}$ and let $E(\mathbf{Q})_{\mathrm{tor}}$ denote the torsion subgroup of its Mordell–Weil group. If p is a prime of good reduction for E with $p \nmid \#E(\mathbf{Q})_{\mathrm{tor}}$, then we have an injection $E(\mathbf{Q})_{\mathrm{tor}} \hookrightarrow E(\mathbf{F}_p)$; consequently, if $m \mid \#E(\mathbf{Q})_{\mathrm{tor}}$ then $m \mid \#E(\mathbf{F}_p)$ for all but finitely many p. The converse statement holds only *up to isogeny*, by a result of Katz [19, Theorem 2]: if $m \mid \#E(\mathbf{F}_p)$ for a set of primes p of

2000 *Mathematics Subject Classification.* 11G05, 14H52.
Mots-clefs. Elliptic curves, torsion subgroups, arithmetic statistics.
The authors would like to thank Robert Harron and Siman Wong for helpful conversations, Robert Lemke Oliver for comments, and Peter J. Cho, Keunyoung Jeong, Grant Molnar, Carl Pomerance, Edward Schaefer, David Zureick–Brown, and the anonymous referee for their feedback and corrections. Voight was supported by an NSF CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029).

density 1, then there exists an elliptic curve E' over $\mathbf{Q}$ that is isogenous over $\mathbf{Q}$ to E such that $m \mid \#E'(\mathbf{Q})_{\mathrm{tor}}$.

We say E locally has a subgroup of order m if $m \mid \#E(\mathbf{F}_p)$ (equivalently, $m \mid \#E(\mathbf{Q}_p)_{\mathrm{tor}}$) for a set of primes p of density 1. With respect to the property of having a subgroup of order m, the result of Katz is then a local-global principle for *isogeny classes* of elliptic curves. In this paper, we consider a probabilistic refinement for the elliptic curves themselves: if E locally has a subgroup of order m, what is the *probability* that E globally has a subgroup of order m?

1.2. Notation. Every elliptic curve E over $\mathbf{Q}$ is defined by a unique equation of the form $y^2 = f(x) = x^3 + Ax + B$ with $A, B \in \mathbf{Z}$ such that $4A^3 + 27B^2 \neq 0$ and there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$. Let $\mathscr{E}$ be the set of elliptic curves of this form, and define the height of $E \in \mathscr{E}$ by

$$\mathrm{ht}\, E := \max(|4A^3|, |27B^2|). \tag{1.2.1}$$

For $H > 0$, let $\mathscr{E}_{\leq H} := \{E \in \mathscr{E} : \mathrm{ht}\, E \leq H\}$ be the finite set of elliptic curves of height at most H.

For $m \in \mathbf{Z}_{\geq 1}$, let $\mathscr{E}_{m?}$ be the set of $E \in \mathscr{E}$ such that E locally has a subgroup of order m. In this notation, our goal is to study the probability

$$P_m := \lim_{H \to \infty} \frac{\#\{E \in \mathscr{E}_{\leq H} : m \mid \#E(\mathbf{Q})_{\mathrm{tor}}\}}{\#\{E \in \mathscr{E}_{m?} \cap \mathscr{E}_{\leq H}\}} \tag{1.2.2}$$

when this limit exists.

1.3. Results. In view of the theorem of Mazur [23] on rational torsion, we have $\mathscr{E}_{m?}$ nonempty if and only if $m \in \{1, 2, \ldots, 10, 12, 16\}$. Our main result is as follows.

Theorem 1.3.1. *For all $m \in \{1, 2, \ldots, 10, 12, 16\}$, the probability P_m defined in (1.2.2) exists and is nonzero. Moreover, P_m is effectively computable.*

For $m = 1$ we have vacuously $P_m = 1$. For $m = 2$, we again have $P_m = 1$ because if $E \in \mathscr{E}_{2?}$ then its defining cubic polynomial $f(x) \in \mathbf{Z}[x]$ has a root modulo p for a set of primes of density 1, so by the Chebotarev density theorem it has a root in $\mathbf{Q}$. The cases where $m = 3, 4$ require special consideration and will be treated at the end of this section.

For $m \geq 5$ in our list, our proof of Theorem 1.3.1 is carried out in the following way. We show that P_m can be expressed in terms of the number of points of bounded height on a finite list of explicitly given modular curves—reducing to the case where $m = \ell^n$ is a prime power, these curves arise from a careful study of the ℓ-adic Galois representation, refining the above theorem of Katz (see §2.3). We then apply the principle of Lipschitz, counting points in a homogeneously expanding region, to count elliptic

curves by height on these modular curves. Taking the ratio, we then find a positive probability.

To count elliptic curves by height, we establish a general result of potential independent interest: we extend work of Harron–Snowden [17], who provide asymptotics for the number of elliptic curves of bounded height in a universal family, as follows. Let $N \in \mathbf{Z}_{\geq 1}$ and let $G \leq \mathrm{GL}_2(\mathbf{Z}/N)$ be a subgroup with $\det(G) = (\mathbf{Z}/N)^\times$. Let $\pi_N \colon \mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N)$ be the projection map and let

$$\Gamma_G := \pi_N^{-1}(G \cap \mathrm{SL}_2(\mathbf{Z}/N)) \leq \mathrm{SL}_2(\mathbf{Z}). \tag{1.3.2}$$

Let Y_G be the open modular curve obtained by taking the quotient of the upper half-plane by the action of Γ_G. Let $\mathrm{Gal}_{\mathbf{Q}} := \mathrm{Gal}(\mathbf{Q}^{\mathrm{al}} \mid \mathbf{Q})$ and let

$$\overline{\rho}_{E,N} \colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{Aut}(E[N](\mathbf{Q}^{\mathrm{al}})) \simeq \mathrm{GL}_2(\mathbf{Z}/N)$$

be the Galois representation on the N-torsion subgroup of E. We write $\overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \lesssim G$ to mean that the image of $\overline{\rho}_{E,N}$ is conjugate in $\mathrm{GL}_2(\mathbf{Z}/N)$ to a subgroup of G.

Theorem 1.3.3. *Let $G \leq \mathrm{GL}_2(\mathbf{Z}/N)$ be such that $\det G = (\mathbf{Z}/N)^\times$. Suppose that Γ_G is torsion free (in particular, $-1 \notin \Gamma_G$) and that Y_G has genus zero and no irregular cusps. Let*

$$d(G) := \tfrac{1}{2}[\mathrm{PSL}_2(\mathbf{Z}) : \Gamma_G] = \tfrac{1}{4}[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G]. \tag{1.3.4}$$

Then $d(G) \in \mathbf{Z}_{\geq 1}$, and there exists an effectively computable $c(G) \in \mathbf{R}_{\geq 0}$ such that

$$\#\{E \in \mathscr{E}_{\leq H} : \overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \lesssim G\} = c(G)H^{1/d(G)} + O(H^{1/e(G)}) \tag{1.3.5}$$

as $H \to \infty$, where $e(G) = 2d(G)$.

In particular, this theorem applies to the groups G that arise in the proof of Theorem 1.3.1. Moreover, it allows us to count elliptic curves with (marked) torsion of size at least 5; dealing with the remaining few cases separately, we have the following corollary.

Corollary 1.3.6. *For each T in Table 1.3.8, we have*

$$\#\{E \in \mathscr{E}_{\leq H} : E(\mathbf{Q})_{\mathrm{tor}} \simeq T\} = c(T)H^{1/d(T)} + O(H^{1/e(T)}). \tag{1.3.7}$$

In view of Table 1.3.8, the count of curves $E \in \mathscr{E}_{\leq H}$ such that $E(\mathbf{Q})_{\mathrm{tor}}$ merely *contains* a subgroup isomorphic to T has the same asymptotic as the count in (1.3.7).

T	$1/d(T)$	$1/e(T)$	T	$1/d(T)$	$1/e(T)$
$\{0\}$	$5/6$	$1/2$	$\mathbf{Z}/9$, $\mathbf{Z}/10$	$1/18$	$1/36$
$\mathbf{Z}/2$	$1/2$	$1/3$	$\mathbf{Z}/12$	$1/24$	$1/48$
$\mathbf{Z}/3$	$1/3$	$1/4$	$\mathbf{Z}/2 \times \mathbf{Z}/2$	$1/3$	$1/6$
$\mathbf{Z}/4$	$1/4$	$1/6$	$\mathbf{Z}/2 \times \mathbf{Z}/4$	$1/6$	$1/12$
$\mathbf{Z}/5$, $\mathbf{Z}/6$	$1/6$	$1/12$	$\mathbf{Z}/2 \times \mathbf{Z}/6$	$1/12$	$1/24$
$\mathbf{Z}/7$, $\mathbf{Z}/8$	$1/12$	$1/24$	$\mathbf{Z}/2 \times \mathbf{Z}/8$	$1/24$	$1/48$

Table 1.3.8: Asymptotic count of elliptic curves with designated torsion

Harron–Snowden [17, Theorem 1.2] proved that $\#\{E \in \mathscr{E}_{\leq H} : E(\mathbf{Q})_{\mathrm{tor}} \simeq T\} \asymp H^{1/d(T)}$ for the groups T in Table 1.3.8, and gave the power-saving asymptotic with explicit constant [17, Theorem 5.6] for $\#T \leq 3$. Indeed, there has been a recent spate of work on the topic of counting elliptic curves with certain level structure by height [4, 6, 8, 24, 25]; the theorem above provides an asymptotic in cases not handled by these other works.

We follow the strategy of Harron–Snowden in the proof of Theorem 1.3.3, again applying the Principle of Lipschitz. The constant $c(G)$ is given by a product of an area of a compact region in the plane multiplied by a sieving factor that includes certain effectively computable local correction factors. The square-root error term accounts for the boundary of the region. The hypotheses of Theorem 1.3.3 ensure that the moduli problem defined by G is fine, so there is a universal elliptic curve over the associated moduli scheme. (In fact, there are only finitely many torsion-free, genus zero congruence subgroups $\Gamma_G \leq \mathrm{SL}_2(\mathbf{Z})$—a list first compiled by Sebbar [26].)

Remark 1.3.9. Although the above result suffices for our purposes, echoing Harron–Snowden [17, §1.5], it would be desirable to establish a statement generalizing Theorem 1.3.3 to an arbitrary group G with Γ_G of genus zero. See work of Ellenberg–Satriano–Zureick-Brown [14, §4] for a conjecture of Batyrev–Manin–Malle type which predicts an estimate for the number of rational points of bounded height on stacky curves.

Returning to our main result, Theorem 1.3.3 applies directly to the cases $m \geq 5$: tallying degrees $d(G)$, it is then straightforward to prove Theorem 1.3.1. In fact, we show that even before tallying the degrees $d(G)$, we know they are all equal for curves arising from "isogenous" moduli problems, as follows (Theorem 3.2.1).

Theorem 1.3.10. *Let $\varphi\colon E \to E'$ be an isogeny of elliptic curves over $\mathbf{Q}$. Let $N \in \mathbf{Z}_{\geq 1}$, let $G := \overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \leq \mathrm{GL}_2(\mathbf{Z}/N)$ and similarly G' for E'. Then the associated modular curves Y_G and $Y_{G'}$ are isomorphic over $\mathbf{Q}$, and $d(G) = d(G')$.*

The invariance of the index of the adelic Galois representation under isogeny was proven by Greenberg [16, Proposition 2.1.1] using a beautiful but very different argument; we view the isomorphism of modular curves as a refinement.

Finally, carrying this out this strategy with an explicit calculation yields P_5 and P_7 in section 4.

Theorem 1.3.11. *We have* $P_5 = 25/34 \approx 73.5\%$ *and* $P_7 = 4/(4+\sqrt{7}) \approx 60.2\%$.

For $m = 5$ and $m = 7$, and more generally, our investigation reveals that the curves with torsion have *smaller height* relative to their counterparts with just locally a subgroup of order m.

We now return to the remaining values $m = 3, 4$ are interesting in their own right and benefit from direct arguments, so we dig deeper. Consider first the case $m = 3$. We first recall that every elliptic curve $E \in \mathscr{E}_{3?}$ either has a rational 3-torsion point or its quadratic twist by -3 does. With careful attention to local contributions at 3, we find a matching growth rate for the quadratic twists, yielding the following result.

Theorem 1.3.12. *We have* $P_3 = 1/2$.

So Theorem 1.3.12 says that among elliptic curves with $3 \mid \#E(\mathbf{F}_p)$ for almost all p, there are 50-50 odds that $3 \mid \#E(\mathbf{Q})_{\mathrm{tor}}$.

When $m = 4$, the situation is more complicated, due in part to the fact that E can have $4 \mid \#E(\mathbf{Q})_{\mathrm{tor}}$ in two different ways. We first show that having full 2-torsion dominates having a point of order 4 among elliptic curves in $\mathscr{E}_{4?}$ in the following sense.

Proposition 1.3.13. *We have* $E \in \mathscr{E}_{4?}$ *if and only if at least one of the following holds:*

(i) $E(\mathbf{Q})[2] \simeq (\mathbf{Z}/2)^2$, *or*
(ii) E *has a cyclic* 4*-isogeny defined over* $\mathbf{Q}$.

Proposition 1.3.13 can also be rephrased geometrically: if $E \in \mathscr{E}_{4?}$, then since $\mathscr{E}_{4?} \subseteq \mathscr{E}_{2?}$ the elliptic curve E arises from a $\mathbf{Q}$-rational point on the classical modular curve $Y_0(2) = Y_1(2)$, and this point lifts to a $\mathbf{Q}$-rational point under at least one of the natural projection maps $Y(2) \to Y_0(2)$ or $Y_0(4) \to Y_0(2)$, each of degree 2.

The fact that $4 \mid \#E(\mathbf{F}_p)$ for all good odd p in case (ii) can be explained by a governing field that is biquadratic: for half of the good primes we have $E(\mathbf{F}_p)[2] \simeq (\mathbf{Z}/2)^2$ whereas for the complementary half $E(\mathbf{F}_p)$ has an element of order 4. See Proposition 5.1.4 for details.

We then count the number of elliptic curves in case (i) and (ii) with a direct argument: we find they have the same asymptotic rate of growth, with explicit constants. Next, we show that among curves satisfying (ii),

those with $4 \mid \#E(\mathbf{Q})_{\mathrm{tor}}$ are asymptotically negligible. Therefore, P_4 is equal to the probability that E belongs to case (i) among those curves belonging to (i) and (ii), giving the following result.

Theorem 1.3.14. *There exists a constant $c_4 \in \mathbf{R}_{>0}$ such that as $H \to \infty$,*

$$\begin{aligned}\#\{E \in \mathscr{E}_{\leq H} : E \text{ has a cyclic 4-isogeny defined over } \mathbf{Q}\}\\ = c_4 H^{1/3} + O(H^{1/6}).\end{aligned}$$

Moreover, we have $c_4 \approx 0.9574$ and $P_4 \approx 27.2\%$ effectively computable.

The exact value of c_4 is given in Proposition 5.3.10 and for P_4 in Proposition 5.3.12. For both $m = 3, 4$, these theorems match experimental data (Remarks 5.2.6, 5.3.15).

Remark 1.3.15. We choose to normalize our height function including the constants in the discriminant function, following Bhargava–Shankar [3]. Alternatively, one can order the elliptic curves by defining

$$\mathrm{ht}'(E) := \max(|A^3|, |B^2|)$$

(without the scalars $4, 27$). The probability for $m = 3$ is again $1/2$ in this height; see Remark 5.3.17 for the probability for $m = 4$ computed in this way instead.

1.4. Organization. Our paper is organized as follows. In Section 2, we collect relevant facts about Galois representations attached to elliptic curves as a way to reformulate our main question in terms of Galois image, refining work of Katz [19]. With these images in hand, it then becomes a computation with universal curves to obtain the order of growth of curves in $\mathscr{E}_{m?}$ ordered by height. In section 4, we use this to prove our main result for $m \geq 5$ and carry this out explicitly for P_5, P_7. In section 5, we treat the remaining cases $m = 3, 4$ in detail, computing the asymptotics and the relevant constants.

2. Galois representations and divisibility

In this section, we characterize the image of the Galois representation under the condition of local m-divisibility. The main results of this section are Corollary 2.3.13 and Theorem 2.3.14: we bound the degree of an isogeny (guaranteed by the theorem of Katz [19, Theorem 1]) from any elliptic curve E with locally a subgroup of order m to an elliptic curve E' with a subgroup of order m.

2.1. Setup. We reset our notation, working in more generality to start. Let K be a number field with ring of integers $\mathbf{Z}_K$ and algebraic closure K^{al}. Let E be an elliptic curve over K with origin $\infty \in E(K)$. By a prime of K we mean a nonzero prime ideal $\mathfrak{p} \subset \mathbf{Z}_K$, and we write $\mathbf{F}_{\mathfrak{p}} := \mathbf{Z}_K/\mathfrak{p}$ for

the residue field of $\mathfrak{p}$; we say a prime $\mathfrak{p}$ is good (for E) if $\mathfrak{p}$ is prime of good reduction for E.

Let $\ell \in \mathbf{Z}$ be prime and let $T_\ell E := \varprojlim_n E[\ell^n](K^{\mathrm{al}}) \simeq \mathbf{Z}_\ell^2$ be the ℓ-adic Tate module, writing $P = (P_n)_n \in T_\ell E$ with each $P_n \in E[\ell^n](K^{\mathrm{al}})$ satisfying $\ell P_n = P_{n-1}$. The absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$ acts continuously on $T_\ell E$ giving a Galois representation

$$\rho_{E,\ell} \colon \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell E) \simeq \mathrm{GL}_2(\mathbf{Z}_\ell) \tag{2.1.1}$$

with $\det \rho_{E,\ell} : \mathrm{Gal}_K \to \mathbf{Z}_\ell^\times$ equal to the ℓ-adic cyclotomic character. In the above, we follow the convention that matrices act on the left on column vectors.

We write

$$\overline{\rho}_{E,\ell^n} : \mathrm{Gal}_K \to \mathrm{Aut}(E[\ell^n](K^{\mathrm{al}})) \tag{2.1.2}$$

for just the action on $E[\ell^n](K^{\mathrm{al}})$, alternatively obtained as the composition of $\rho_{E,\ell}$ with reduction modulo ℓ^n. We also define $V_\ell E := T_\ell E \otimes \mathbf{Q}_\ell$.

If E' is another elliptic curve over K, by an isogeny $\varphi \colon E \to E'$ we mean an isogeny defined over K. (If we have need to consider isogenies defined over an extension, we will indicate this explicitly.)

For a good prime $\mathfrak{p}$ of K coprime to ℓ, we have

$$\#E(\mathbf{F}_\mathfrak{p}) = \det(1 - \rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})) \tag{2.1.3}$$

where $\mathrm{Frob}_\mathfrak{p}$ is the conjugacy class of the Frobenius automorphism at $\mathfrak{p}$ in Gal_K, and recall that the point counts $\#E(\mathbf{F}_\mathfrak{p})$ are well-defined on the isogeny class of E. Moreover, by the Chebotarev density theorem, the condition $\ell^n \mid \#E(\mathbf{F}_\mathfrak{p})$ for a set of primes $\mathfrak{p}$ of density 1 is equivalent to the group-theoretic condition

$$\det(1 - \rho_{E,\ell}(\sigma)) \equiv 0 \pmod{\ell^n} \tag{2.1.4}$$

for all $\sigma \in \mathrm{Gal}_K$, and further $\ell^n \mid \#E(\mathbf{F}_\mathfrak{p})$ for primes $\mathfrak{p}$ in a set of density 1 if and only if $\ell^n \mid \#E(\mathbf{F}_\mathfrak{p})$ for all but finitely many $\mathfrak{p}$.

2.2. Galois images. Both to motivate what follows and because we will make use of it, we begin with the following lemma.

Definition 2.2.1. *A basis P_1, P_2 for $T_\ell E$ is clean if there exist $r, s \in \mathbf{Z}_{\geq 0}$ such that (in coordinates) $P_{1,r}, P_{2,s}$ generate $E[\ell^\infty](K)$.*

Choosing generators, we see that $T_\ell E$ always has a clean basis. Moreover, if P_1, P_2 is a clean basis, then the integers r, s are unique and $E[\ell^\infty](K) \simeq \mathbf{Z}/\ell^r \times \mathbf{Z}/\ell^s$.

Lemma 2.2.2. *The following statements hold.*

(a) *In a clean basis for $T_\ell E$, we have*

$$\rho_{E,\ell}(\mathrm{Gal}_K) \leq \begin{pmatrix} 1+\ell^r\mathbf{Z}_\ell & \ell^s\mathbf{Z}_\ell \\ \ell^r\mathbf{Z}_\ell & 1+\ell^s\mathbf{Z}_\ell \end{pmatrix} \tag{2.2.3}$$

where by convention $1+\ell^0\mathbf{Z}_\ell := \mathbf{Z}_\ell^\times$.

(b) *If (2.2.3) holds in a basis for $T_\ell E$, then $P_{1,r}, P_{2,s}$ generate a subgroup of $E[\ell^\infty](K)$ isomorphic to $\mathbf{Z}/\ell^r \times \mathbf{Z}/\ell^s$; if moreover equality holds in (2.2.3), then this basis is clean.*

Proof. Straightforward. □

Now let $n \geq 1$, and for integers $0 \leq r, s \leq n$, define the subgroup

$$G_\ell(n;r,s) := \begin{pmatrix} 1+\ell^r\mathbf{Z}_\ell & \ell^s\mathbf{Z}_\ell \\ \ell^{n-s}\mathbf{Z}_\ell & 1+\ell^{n-r}\mathbf{Z}_\ell \end{pmatrix} \leq \mathrm{GL}_2(\mathbf{Z}_\ell) \tag{2.2.4}$$

with the same convention as in (2.2.3). Indeed, the group on the right-hand side of (2.2.3) is $G_\ell(r+s;r,s)$, i.e., corresponds to $n = r+s$. When the prime ℓ is clear, we will drop the subscript and abbreviate $G(n;r,s) = G_\ell(n;r,s)$.

Our motivation for studying these groups is indicated by the following lemma.

Lemma 2.2.5. *If $\rho_{E,\ell}(\mathrm{Gal}_K) \leq G(n;r,s)$ for some $0 \leq r,s \leq n$, then $\ell^n \mid \#E(\mathbf{F}_\mathfrak{p})$ for all but finitely many $\mathfrak{p}$.*

Proof. We see directly that $\det(1-g) \equiv 0 \pmod{\ell^n}$ for all $g \in G(n;r,s)$, so the result follows from (2.1.4). □

Example 2.2.6. If $\ell = 2$, then $G_2(1;0,0) = G_2(1;1,0)$.

Example 2.2.7. Suppose that $\rho_{E,\ell}(\mathrm{Gal}_K) = G(n;r,s)$ as above, with $n \geq 1$.

If $r = n$ and $s = 0$, then $\overline{\rho}_{E,\ell^n} = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ and so if $P_1, P_2 \in E[\ell^n](K^{\mathrm{al}})$ are the nth coordinates of the chosen basis for $T_\ell E$, then $E[\ell^\infty](K) = \langle P_1 \rangle \simeq \mathbf{Z}/\ell^n$.

Similarly, if $r = s = 0$ and $\ell \neq 2$, then $\overline{\rho}_{E,\ell^n} = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$; thus $E[\ell^\infty](K) = \{\infty\}$ and E has a unique cyclic isogeny over K of order ℓ^n whose kernel is generated by P_1.

In both cases, we have $\ell^n \mid \#E(\mathbf{F}_\mathfrak{p})$ for all but finitely many $\mathfrak{p}$.

Interchanging the basis elements made in the identification (2.1.1) gives an isomorphism

$$G(n;r,s) \xrightarrow{\sim} G(n;n-r,n-s) \tag{2.2.8}$$

so without loss of generality we may suppose that $r+s \leq n$ (and still that $0 \leq r,s \leq n$). If $n = r+s$, we have $G(n;r,n-r) \simeq G(n;n-r,r)$.

Lemma 2.2.9. *The following statements hold.*

(a) *The group* $G_\ell(n; r, s)$ *is equal to the preimage of its reduction modulo* $\ell^{\max(r,s,n-s,n-r)}$.
(b) *We have* $\det G_\ell(n; r, s) = 1 + \ell^{\min(r,n-r)}\mathbf{Z}_\ell$.
(c) *We have*

$$[\mathrm{GL}_2(\mathbf{Z}_\ell) : G_\ell(n; r, s)] = \begin{cases} \ell^{2n-3}(\ell^2-1)(\ell-1), & \text{if } \min(r, n-r) \geq 1; \\ \ell^{2n-2}(\ell^2-1), & \text{if } \min(r, n-r) = 0. \end{cases}$$

(d) *If* $\ell^n \geq 5$, *then* $G_\ell(n; r, s) \cap \mathrm{SL}_2(\mathbf{Z})$ *is torsion free.*

Proof. Parts (a) and (b) follow from a direct calculation. For part (c), we reduce modulo n (using (a)) and count the size of the reduction in each coordinate: we find

$$\frac{\phi(\ell^n)}{\phi(\ell^r)}\ell^{n-s}\ell^s\frac{\phi(\ell^n)}{\phi(\ell^{n-r})} = \ell^{3n-2}(\ell-1)^2 \cdot \begin{cases} (\ell^{n-2}(\ell-1)^2)^{-1}, & \text{if } r, n-r \geq 1; \\ (\ell^{n-1}(\ell-1))^{-1}, & \text{if } r = 0, n. \end{cases}$$

Simplifying and noting $\#\mathrm{GL}_2(\mathbf{Z}/\ell^n) = \ell^{4(n-1)}\#\mathrm{GL}_2(\mathbf{Z}/\ell) = \ell^{4n-3}(\ell-1)(\ell^2-1)$, the result follows.

For part (d), as in Lemma 2.2.5 we have $\det(g-1) \equiv 0 \pmod{\ell^n}$ for all $g \in G(n; r, s)$. If $g \in \mathrm{SL}_2(\mathbf{Z})$ is torsion, then its characteristic polynomial matches that of a root of unity of order dividing 6, and if $g \neq 1$ then $\det(g-1) = 1, 2, 3, 4$, a contradiction. □

The groups $G(n; r, s)$ arise from curves isogenous to the ones studied in Lemma 2.2.2, as follows.

Proposition 2.2.10. *Suppose in a (clean) basis for* $T_\ell E$ *that we have*

$$\rho_{E,\ell}(\mathrm{Gal}_K) = G(n; r, n-r).$$

Then the following statements hold.

(a) *Any cyclic subgroup* $C \leq E[\ell^\infty](K^{\mathrm{al}})$ *stable under* Gal_K *in fact has* $C \leq E[\ell^\infty](K)$.
(b) *If* $\varphi\colon E \to E'$ *is a cyclic isogeny with* $\deg\varphi = \ell^k$, *then* $k \leq \max(r, n-r)$. *Moreover, there exists a clean basis for* E' *such that*

$$\rho_{E',\ell}(\mathrm{Gal}_K) = \begin{cases} G(n; r, n-r-k), & \text{only if } k \leq n-r; \\ G(n; n-r, r-k), & \text{only if } k \leq r. \end{cases} \tag{2.2.11}$$

In (2.2.11), we mean that if $r < k \leq n-r$ then the first case must occur, and symmetrically if $n-r < k \leq r$ then the second case must occur; if $k \leq \min(r, n-r)$, then either case can arise. The proof will show that all possibilities do arise.

Proof. We first prove (a). Interchanging basis elements as in (2.2.8), we may suppose without loss of generality that $r \leq n-r$. Let $\#C = \ell^k$. A generator for C is of the form $P = x_1P_{1,k} + x_2P_{2,k}$ with $(x_1 : x_2) \in \mathbf{P}^1(\mathbf{Z}/\ell^k)$.

- If $k \leq r$, then we have full ℓ^k-torsion $E[\ell^k](K^{\mathrm{al}}) = E[\ell^k](K)$ and so certainly (a) holds.
- Suppose $r < k \leq n - r$. Then by hypothesis,
$$\overline{\rho}_{E,\ell^k}(\mathrm{Gal}_K) = \left\{ \begin{pmatrix} 1 + \ell^r a & 0 \\ \ell^r c & 1 \end{pmatrix} : a, c \in \mathbf{Z}/\ell^{k-r} \right\}.$$
Taking $a \in \mathbf{Z}/\ell^{k-r}$, we see that the only stable lines (eigenvectors) in the action on column vectors are generated by elements $(x : 1) \in \mathbf{P}^1(\mathbf{Z}/\ell^k)$ with $\ell^{k-r} \mid x$, so $P = xP_{1,k} + P_{2,k} = (x/\ell^{k-r})P_{1,r} + P_{2,k} \in E[\ell^k](K)$ as desired.
- Finally, if $k > s := n - r$, then $\ell^{k-s}C$ is Galois stable, so $(x_1 : x_2) \equiv (0 : 1) \pmod{\ell^s}$ by the previous case. Applying upper-triangular unipotent matrices in $\overline{\rho}_{E,\ell^k}(\mathrm{Gal}_K)$ then gives a contradiction.

Next, part (b). Lemma 2.2.2(b) and the preceding part (a) imply $k \leq \max(r, n - r)$. We now change convention for convenience, supposing that $n - r \leq r$. Let P_1, P_2 be the given clean basis for $T_\ell E$. As in (a), let $C = \ker \varphi$ be generated by $P = x_1P_{1,k} + x_2P_{2,k}$ with $(x_1 : x_2) \in \mathbf{P}^1(\mathbf{Z}/\ell^k)$. We consider two cases.

First, suppose $x_1 = 0$. Then $(x_1 : x_2) = (0 : 1)$ and C is generated by $P_{2,k}$. A basis for $T_\ell E'$ (in $V_\ell E$) is then given by $P_1, \ell^{-k}P_2$. In this basis, we have

(2.2.12)
$$\rho_{E',\ell}(\mathrm{Gal}_K) = \begin{pmatrix} 1 & 0 \\ 0 & \ell^k \end{pmatrix} G(n; r, n-r) \begin{pmatrix} 1 & 0 \\ 0 & \ell^{-k} \end{pmatrix} = G(n; r, n-r-k)$$

as claimed.

Otherwise, we have $x_1 \neq 0$; then $(x_1 : x_2) = (1 : x)$ for $x \in \mathbf{Z}/\ell^k$; we lift to $x \in \mathbf{Z}_\ell^\times$. Let
$$U := \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}_\ell).$$
Let $Q_i = UP_i$ for $i = 1, 2$, so Q_1, Q_2 is a (no longer necessarily clean) basis for $T_\ell E$ in which $\ker \varphi = \langle Q_{2,k} \rangle$. Nevertheless, we calculate:

(2.2.13)
$$\begin{pmatrix} \ell^k & 0 \\ 0 & 1 \end{pmatrix} U = \begin{pmatrix} \ell^k & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix} = \begin{pmatrix} 0 & \ell^k \\ 1 & x \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & \ell^k \end{pmatrix} = U'A.$$

A basis for $T_\ell E'$ (in $V_\ell E$) is given by $Q_1, \ell^{-k}Q_2$, so the same is true after applying $(U')^{-1} = U'$ which just swaps basis vectors to give $\ell^{-k}Q_2, Q_1$. In this basis, the image of $\rho_{E',\ell}(\mathrm{Gal}_K)$ is
$$U' \begin{pmatrix} \ell^k & 0 \\ 0 & 1 \end{pmatrix} UG(n; r, n-r)U^{-1} \begin{pmatrix} \ell^{-k} & 0 \\ 0 & 1 \end{pmatrix} U' = AG(n; r, n-r)A^{-1}$$

and we then compute:

$$\begin{aligned}(2.2.14)\qquad &\begin{pmatrix}1 & x\\ 0 & \ell^k\end{pmatrix}\begin{pmatrix}1+\ell^r a & \ell^{n-r}b\\ \ell^r c & 1+\ell^{n-r}d\end{pmatrix}\begin{pmatrix}1 & -x\ell^{-k}\\ 0 & \ell^{-k}\end{pmatrix}\\ &=\begin{pmatrix}1+\ell^r(a+cx) & -(a+cx)(x\ell^{r-k})+(b+dx)\ell^{n-r-k}\\ c\ell^{k+r} & 1+d\ell^{n-r}-cx\ell^r\end{pmatrix}.\end{aligned}$$

We are free to reparametrize, replacing $a, b \leftarrow a+cx, b+dx$ to get

$$(2.2.15)\qquad =\begin{pmatrix}1+\ell^r a & b\ell^{n-r-k}-ax\ell^{r-k}\\ c\ell^{k+r} & 1+d\ell^{n-r}-cx\ell^r\end{pmatrix}.$$

Since $n-r \leq r$, then we recognize the group $G(n; r, n-r-k)$. Putting these together gives the result. □

Recall that the ℓ-isogeny graph of E has as vertices the set of curves ℓ-power isogenous to E up to isomorphism and (undirected) edges are ℓ-isogenies. Proposition 2.2.10 provides a description of the ℓ-isogeny graph of E when $\rho_{E,\ell}(\mathrm{Gal}_K) = G(n; r, n-r)$ (depending essentially only on n)—a nontrivial path in the graph is a cyclic ℓ-power isogeny. Here are a few illustrative examples.

Example 2.2.16. Suppose $\rho_{E,\ell}(\mathrm{Gal}_K) = G(n; r, n-r)$ with $n \geq 1$, and without loss of generality suppose $r \leq n-r$.

If $r = 0$, then E has Galois image $G(n; 0, n)$, and the isogeny graph consists of a chain of $n+1$ vertices with Galois images $G(n; 0, n), G(n; 0, n-1), \ldots, G(n; 0, 0)$; the kernels of these isogenies are cyclic subgroups of $E[\ell^\infty](K) \simeq \mathbf{Z}/\ell^n$.

For Galois image $G(2; 1, 1)$ ($n = 2$ and $r = 1$), there are $\ell + 1$ vertices adjacent to E with Galois image $G(2; 1, 0)$.

We conclude this section by a study of curves with Galois image (contained in) $G(n; r, s)$, building on Lemma 2.2.2.

Lemma 2.2.17. *Suppose $\rho_{E,\ell}(\mathrm{Gal}_K) \leq G(n; r, s)$ with $0 \leq r, s, r+s \leq n$, and if $\ell = 2$ suppose that $(r, s) \neq (0, 0)$. Then the following statements hold.*

(a) *If $\rho_{E,\ell}(\mathrm{Gal}_K) = G(n; r, s)$, then $P_{1,r}, P_{2,s}$ generate $E[\ell^\infty](K)$; in particular, we have $E[\ell^\infty](K) \simeq \mathbf{Z}/\ell^r \times \mathbf{Z}/\ell^s$.*

(b) *Suppose $\rho_{E,\ell}(\mathrm{Gal}_K) \leq G(n; r, s)$. Then, for all t such that $s \leq t \leq n-r$, there exists a cyclic ℓ^{t-s} isogeny $E \to E'$ over K such that if P_1, P_2 is a basis for $T_\ell E$, then*

$$\rho_{E',\ell}(\mathrm{Gal}_K) \leq G(n; r, t)$$

in the basis $\ell^{s-t}P_1, P_2$ for $T_\ell E'$ (in $V_\ell E$).

(c) *The elliptic curve E admits a cyclic $\ell^{n-(r+s)}$-isogeny $E \to E'$ over K with $\ell^n \mid \#E'(K)_{\mathrm{tor}}$.*

Proof. We prove (a), and let $P_{1,n}, P_{2,n} \in E[\ell^n](K^{\mathrm{al}})$ be the nth coordinates of the chosen basis for $T_\ell E$, and consider a point $P := x_1 P_{1,n} + x_2 P_{2,n} \in E[\ell^n](K^{\mathrm{al}})$ with $x_1, x_2 \in \mathbf{Z}/\ell^n$. Of course $P \in E[\ell^n](K)$ if and only if $(g-1)(P) \equiv 0 \pmod{\ell^n}$ for all $g \in G(n; r, s)$. If $P \in E[\ell^n](K)$, then taking diagonal matrices shows that $\ell^{n-r} \mid x_1$ and $\ell^r \mid x_2$; since $r + s \leq n$, we have $s \leq n - r$ so $\ell^s \mid x_1$ and similarly $\ell^{n-s} \mid x_2$. Conversely,

$$\begin{pmatrix} \ell^r a & \ell^s b \\ \ell^{n-s} c & \ell^{n-r} d \end{pmatrix} \begin{pmatrix} \ell^{n-r} \\ \ell^{n-s} \end{pmatrix} \equiv 0 \pmod{\ell^n} \tag{2.2.18}$$

so $E[\ell^n](K) = \langle \ell^{n-r} P_1, \ell^{n-s} P_2 \rangle \simeq \mathbf{Z}/\ell^r \times \mathbf{Z}/\ell^s$, proving (a).

Next, part (b). Let $u \in \mathbf{Z}$ satisfy $s \leq u \leq n$. A similar argument in coordinates as in the previous paragraph shows $\ell^u P_{1,n}$ generates a Galois-stable subgroup of $E(K)$. Let $E' := E/\langle \ell^u P_{1,n} \rangle$, so that the quotient map $E \to E'$ defines a cyclic ℓ^{n-u}-isogeny. Conjugating as in (2.2.12) shows that $\rho_{E',\ell}(\mathrm{Gal}_K) = G(n; r, s+n-u)$. Restricting u to range over $r + s \leq u \leq n$, the image $\rho_{E',\ell}(\mathrm{Gal}_K)$ ranges over $G(n; r, t)$ with for $s \leq t \leq n - r$, with $n - u = t - s$.

Finally, for (c), take $t = n - r$ in part (b). □

2.3. Refining the theorem of Katz. In this section, we refine the result of Katz (mentioned in the introduction), which we now recall.

Theorem 2.3.1 (Katz [19])**.** *Let $n \geq 1$. Suppose that $\ell^n \mid \#E(\mathbf{F}_\mathfrak{p})$ for a set of good primes of K of density 1. Then there exists an elliptic curve E' over K that is K-isogenous to E and a $\mathbf{Z}_\ell$-basis of $T_\ell E' \simeq \mathbf{Z}_\ell^2$ such that*

$$\rho_{E',\ell}(\mathrm{Gal}_K) \leq G(n; r, n-r) \tag{2.3.2}$$

for some integer $0 \leq r \leq n$. In particular, $\ell^n \mid \#E'(K)_{\mathrm{tor}}$.

Proof. We briefly review the method of proof for the reader's convenience. (Some details of the argument are explained in the next section.) Let V be a 2-dimensional $\mathbf{Q}_\ell$-vector space and let $G \leq \mathrm{Aut}(V)$ be a compact open subgroup. By an inductive group-theoretic argument, Katz [19, Theorem 1] shows that if

$$\det(1 - g) \equiv 0 \pmod{\ell^n}$$

holds for all $g \in G$, then there exist G-stable lattices $\mathcal{L}' \subseteq \mathcal{L} \subseteq V$ such that the quotient $\mathcal{L}/\mathcal{L}'$ has order ℓ^n and trivial G-action; equivalently, there exists a $\mathbf{Q}_\ell$-basis of V such that $G \leq G(n; r, n-r)$ for some integer $0 \leq r \leq n$.

We then apply the preceding paragraph to elliptic curves [19, Theorem 2]. We take $V = T_\ell E \otimes \mathbf{Q}_\ell$ and $G = \mathrm{Gal}_K$; then $\mathcal{L}' = T_\ell(E')$ for some elliptic curve E' over K that is K-isogenous to E, and

$$\mathcal{L}/\mathcal{L}' \subseteq \ell^{-n}\mathcal{L}'/\mathcal{L}' \simeq \mathcal{L}'/\ell^n\mathcal{L}' \simeq E'[\ell^n] \tag{2.3.3}$$

is a subgroup of K-rational torsion points of E' (see [19, Introduction] for a review of Galois-stable lattices of the Tate module). □

Lemma 2.3.4. *Under the hypotheses of Theorem 2.3.1, the isogeny $\varphi\colon E \to E'$ may be taken to be a cyclic ℓ-power isogeny.*

Proof. Given any isogeny $\varphi\colon E \to E'$, we may factor φ into first an isogeny of ℓ-power degree then an isogeny of degree coprime to ℓ. The latter isogeny preserves the image of $\rho_{E',\ell}$, so we may assume φ has ℓ-power degree. The resulting isogeny factors as a cyclic ℓ-power isogeny followed by multiplication by a power of ℓ, and again the latter preserves the image of $\rho_{E',\ell}$, so the conclusion follows. □

To refine Theorem 2.3.1, we identify the image of $\rho_{E,\ell}$ by following the isogeny guaranteed by Lemma 2.3.4. In general, one can say little more than E is isogenous to E'! The following lemma is the starting point for Katz, as it is for us.

Lemma 2.3.5. *Let k be a field, let V be a k-vector space with $\dim_k V = 2$, and let $G \leq \mathrm{GL}(V)$ be a subgroup. Suppose that $\det(1-g) = 0$ for all $g \in G$. Then there exists a basis of $V \simeq k^2$ such that $G \leq \mathrm{GL}_2(k)$ is contained one of the subgroups*

$$\begin{pmatrix} 1 & k \\ 0 & k^\times \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} k^\times & k \\ 0 & 1 \end{pmatrix}.$$

Proof. See Serre [28, p. I-2, Exercise 1]; when k is perfect, see the proof by Katz [19, Lemma 1, p. 484] using the Brauer–Nesbitt theorem. □

Corollary 2.3.6. *If $\ell \mid \#E(\mathbf{F}_\mathfrak{p})$ for a set of primes of K of density 1, then at least one of the following holds:*

(i) *$E(K)[\ell] \neq \{\infty\}$; or*
(ii) *there is a cyclic ℓ-isogeny $E \to E'$ over K where $E'(K)[\ell] \neq \{\infty\}$.*

Proof. Apply Lemma 2.3.5 with $k = \mathbf{F}_\ell$ and $V = E[\ell]$, and $G = \overline{\rho}_{E,\ell}(\mathrm{Gal}_K)$. For the first subgroup we are in case (i); for the second, the basis P_1, P_2 provided by the lemma gives an ℓ-isogenous curve $E' := E/\langle P_1 \rangle$ over K with the image of $\langle P_2 \rangle$ invariant under G, so we are in case (ii). □

In other words, Corollary 2.3.6 says that when $n = 1$, we may take the isogeny $\varphi\colon E \to E'$ provided by Lemma 2.3.4 to have degree dividing ℓ; in particular, this proves a refinement of Theorem 2.3.1 for $n = 1$.

We now seek to generalize Corollary 2.3.6 to the prime power case $m = \ell^n$. We start by considering the case where the degree of the isogeny $\varphi\colon E \to E'$ provided by Lemma 2.3.4 is large.

Lemma 2.3.7. *Let $\varphi\colon E \to E'$ be a cyclic ℓ^k-isogeny over K such that $\ell^n \mid \#E'(K)_{\mathrm{tor}}$. Suppose that $k \geq n$. Then there is a $\mathbf{Z}_\ell$-basis for $T_\ell E \simeq \mathbf{Z}_\ell^2$ such that*

$$\rho_{E,\ell}(\mathrm{Gal}_K) \leq G(n;r,0) = \begin{pmatrix} 1+\ell^r\mathbf{Z}_\ell & \mathbf{Z}_\ell \\ \ell^n\mathbf{Z}_\ell & 1+\ell^{n-r}\mathbf{Z}_\ell \end{pmatrix} \tag{2.3.8}$$

for some integer $0 \leq r \leq n$. In particular, there exists a cyclic ℓ^{n-r}-isogeny $\psi\colon E \to E''$ such that $\ell^n \mid \#E''(K)_{\mathrm{tor}}$ and $\rho_{E'',\ell}(\mathrm{Gal}_K) \leq G(n;r,n-r)$.

Proof. By hypothesis, there is a cyclic subgroup $C_k \leq E(K^{\mathrm{al}})$ stable under Gal_K of order ℓ^k. Since $k \geq n$, the subgroup $\ell^{k-n}C_k \leq E(K^{\mathrm{al}})$ is also Gal_K-stable and order ℓ^n. Extending to a basis for $E[\ell^n](K^{\mathrm{al}})$, we have

$$G := \overline{\rho}_{E,\ell^n}(\mathrm{Gal}_K) \leq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}. \tag{2.3.9}$$

The containment (2.3.8) is determined by reduction modulo ℓ^n, so equivalently we show

$$G \leq \begin{pmatrix} 1+\ell^r\mathbf{Z}/\ell^n & * \\ 0 & 1+\ell^{n-r}\mathbf{Z}/\ell^n \end{pmatrix} \tag{2.3.10}$$

for some r.

Since $\ell^n \mid \#E'(K)_{\mathrm{tor}}$, as in (2.1.4) we conclude that $\det(1-g) \equiv 0 \pmod{\ell^n}$ for all $g \in G$. Let $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$ be such that $r := \mathrm{ord}_\ell(1-a)$ minimal, so that $0 \leq r \leq n$. Then

$$\det(1-g) = (1-a)(1-d) \equiv 0 \pmod{\ell^n} \tag{2.3.11}$$

gives $d \equiv 1 \pmod{\ell^{n-r}}$, which is a start. To finish, let $g' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in G$ be any element, and let $r' := \mathrm{ord}_\ell(1-a) \geq r$. Then $\mathrm{ord}_\ell(1-d') \geq n-r'$ as in (2.3.11), so if $r' = r$ we are done. So suppose $r' > r$. Consider the determinant condition on gg', which reads

$$\det(1-gg') = (1-aa')(1-dd') \equiv 0 \pmod{\ell^n}. \tag{2.3.12}$$

Then $aa' \equiv a \not\equiv 1 \pmod{\ell^{r+1}}$, so $\mathrm{ord}_\ell(1-aa') = r$, and thus $\mathrm{ord}_\ell(1-dd') \geq n-r$, i.e., $dd' \equiv 1 \pmod{\ell^{n-r}}$. But we already have $d \equiv 1 \pmod{\ell^{n-r}}$, so $d' \equiv 1 \pmod{\ell^{n-r}}$, proving (2.3.10).

The final statement then follows from Lemma 2.2.17(b), with $s = 0$. □

Corollary 2.3.13. *For $m \geq 1$, suppose that $m \mid \#E(\mathbf{F}_\mathfrak{p})$ for a set of primes of K of density 1. Then there exists a cyclic isogeny $\varphi\colon E \to E'$ of degree $d \mid m$ such that $m \mid \#E'(K)_{\mathrm{tor}}$. Moreover, for every $\ell^n \parallel m$, there exists $0 \leq r \leq n$ (depending on ℓ) such that*

$$\rho_{E',\ell}(\mathrm{Gal}_K) \leq G_\ell(n;r,n-r).$$

Proof. For each prime power $\ell^n \parallel m$, apply the theorem of Katz (Theorem 2.3.1), the refinements of Lemmas 2.3.4 and 2.3.7; and then combine these isogenies (taking the sum of the kernels). □

By Corollary 2.3.13, the possible elliptic curves E that locally have a subgroup of order $m = \ell^n$ arise (dually) from cyclic isogenies from curves with ℓ-adic Galois images contained in $G_\ell(n; r, n-r)$ for some r. To conclude, we add the hypothesis that this latter containment is an *equality*; when we calculate probabilities, we will see this fullness condition holds outside of a negligible set.

Theorem 2.3.14. *For $m \geq 1$, suppose that $m \mid \#E(\mathbf{F}_\mathfrak{p})$ for a set of primes of K of density 1, and let $\varphi\colon E \to E'$ be a cyclic ℓ-power isogeny over K such that $\rho_{E',\ell}(\mathrm{Gal}_K) = G(n; r, n-r)$ (in a choice of basis for $T_\ell E'$) for some $0 \leq r \leq n$. Then there exists s with $0 \leq s \leq n$ such that $\rho_{E,\ell}(\mathrm{Gal}_K) = G(n; r, s)$ (in a basis for $T_\ell E$).*

Proof. We have $\deg \varphi = \ell^k$ for some $k \geq 0$. We apply Proposition 2.2.10(b) to the dual isogeny $\varphi^\vee\colon E' \to E$ (with, alas, the roles of E and E' interchanged): we conclude that $\rho_{E,\ell}(\mathrm{Gal}_K) = G(n; r, s)$ with $0 \leq s \leq n-r \leq n$ or $\rho_{E,\ell}(\mathrm{Gal}_K) = G(n; n-r, s')$ with $s' \leq r \leq n$. In the latter case, recalling (2.2.8), we have equivalently $\rho_{E,\ell}(\mathrm{Gal}_K) = G(n; r, s)$ with $0 \leq s = n - s' \leq n$. □

3. Counting elliptic curves

In this section, we count by height elliptic curves parametrized by a modular curve of genus zero uniformized by a torsion free congruence subgroup.

3.1. Moduli of elliptic curves. We quickly set up the necessary theory concerning moduli of elliptic curves.

Let $G \leq \mathrm{GL}_2(\mathbf{Z}/N)$ be a subgroup. If G arises as the image of the mod N Galois representation of an elliptic curve over $\mathbf{Q}$, then its determinant is the cyclotomic character and thus surjective, so we suppose that $\det G = (\mathbf{Z}/N)^\times$. Let $\pi_N\colon \mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N)$ be the projection and as in (1.3.2) let

$$\Gamma_G := \pi_N^{-1}(G \cap \mathrm{SL}_2(\mathbf{Z}/N)) \leq \mathrm{SL}_2(\mathbf{Z}).$$

The group Γ_G is a discrete group acting properly on the upper half-plane $\mathbf{H}^2$, and the quotient $\Gamma_G \backslash \mathbf{H}^2$ can be given the structure of a Riemann surface (compact minus finitely many points). Attached to G is the moduli problem of elliptic curves with G-level structure, as in the following proposition.

Proposition 3.1.1. *Suppose that $\det G = (\mathbf{Z}/N)^\times$. Then there exists an affine, smooth, geometrically integral curve Y_G defined over $\mathbf{Q}$, unique up to isomorphism, with the following properties.*

(i) *There is an isomorphism of Riemann surfaces $\Gamma_G \backslash \mathbf{H}^2 \xrightarrow{\sim} Y_G(\mathbf{C})$.*

(ii) *For every number field K, there is a (functorial) bijection between the set $Y_G(K)$ and the set of K^{al}-isomorphism classes of Gal_K-stable G-equivalence classes of pairs (E,ι), where E is an elliptic curve over K and $\iota\colon E[N](K^{\mathrm{al}}) \to (\mathbf{Z}/N)^2$ is an isomorphism of groups.*

(iii) *For every elliptic curve E over K, there exists ι such that the isomorphism class of (E,ι) lies in $Y_G(K)$ if $\overline{\rho}_{E,N}(\mathrm{Gal}_K) \lesssim G$ is contained in a subgroup conjugate to G; the converse holds if $j(E) \neq 0, 1728$.*

(iv) *If Γ_G is torsion free (in particular $-1 \notin G$), then* (ii) *holds but for K-isomorphism classes, and there is a universal elliptic curve $E_{G,\mathrm{univ}} \to Y_G$, unique up to isomorphism.*

In (iv), in particular, $E_{G,\mathrm{univ}}$ is an elliptic curve over (the affine coordinate ring of) Y_G, and the bijection in (iv) is defined by the map that sends $P \in Y_G(K)$ to the fiber of $E_{G,\mathrm{univ}} \to Y_G$ over P.

Proof. The curve Y_G can be constructed as the quotient of the (connected but geometrically disconnected) modular curve $Y(N)$ defined over $\mathbf{Q}$ by G. For more details, see Deligne–Rapoport [12, Chapters IV, VI] or the tome of Katz–Mazur [20, Chapter 4]; for property (iii), see Baran [2, §4] and Zywina [33, Proposition 3.2]. □

We recall also here the notion of an *irregular cusp* (see e.g., Diamond–Shurman [13, (3.3), p. 75], Shimura [29, §2.1, p. 29]), primarily to show it is only a minor nuisance. Let $\Gamma \leq \mathrm{SL}_2(\mathbf{Z})$ be a subgroup of finite index. If $-1 \in \Gamma$, then every cusp of Γ is regular; so suppose $-1 \notin \Gamma$. Then the stabilizer of the cusp ∞ under Γ is an infinite cyclic group generated by $\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ for some $h \in \mathbf{Z}_{>0}$, and we accordingly say that ∞ is regular or irregular as the sign of this generator is $+$ or $-$. For any cusp s, we choose a matrix $\alpha \in \mathrm{SL}_2(\mathbf{Z})$ such that $\alpha(\infty) = s$ and conjugate the preceding definition.

The groups $G_\ell(n;r,s) \leq \mathrm{GL}_2(\mathbf{Z}_\ell)$ of Section 2 naturally define subgroups $\overline{G}_{\ell^n}(n;r,s) \leq \mathrm{GL}_2(\mathbf{Z}/\ell^n)$ by reduction modulo ℓ^n.

Lemma 3.1.2. *Let ℓ be prime, let $n \geq 1$, and for integers $0 \leq r, s \leq n$ with $r + s \leq n$, let $G = \overline{G}_{\ell^n}(n;r,s) \leq \mathrm{GL}_2(\mathbf{Z}/\ell^n)$ be the reduction modulo ℓ^n of $G_\ell(n;r,s)$. Then the group Γ_G has no irregular cusps except when $\ell^n = 2^2 = 4$ and $rs = 0$.*

Proof. If $\gamma \in \Gamma_G$, then $\gamma = \begin{pmatrix} 1+\ell^r a_0 & \ell^s b_0 \\ \ell^{n-s} c_0 & 1+\ell^{n-r} d_0 \end{pmatrix}$ with $a_0, b_0, c_0, d_0 \in \mathbf{Z}$ and

$$\begin{aligned} \det(\gamma) &= (1+\ell^r a_0)(1+\ell^{n-r} d_0) - \ell^n b_0 c_0 \\ &= 1 + \ell^r a_0 + \ell^{n-r} d_0 + \ell^n (a_0 d_0 - b_0 c_0) = 1, \end{aligned} \tag{3.1.3}$$

so expanding we find

$$\operatorname{tr}(\gamma) = 2 + \ell^r a_0 + \ell^{n-r} d_0 \equiv 2 \pmod{\ell^n}. \tag{3.1.4}$$

Let s be a cusp of Γ_G and $\alpha \in \mathrm{SL}_2(\mathbf{Z})$ be such that $\alpha(\infty) = s$, and consider the group $\alpha^{-1}\Gamma_G\alpha$. Let $\alpha^{-1}\gamma\alpha = \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \alpha^{-1}\Gamma_G\alpha$ generate the stabilizer of ∞. Then $\operatorname{tr}(\alpha^{-1}\gamma\alpha) = \operatorname{tr}(\gamma) = \pm 2 \equiv 2 \pmod{\ell^n}$. Suppose s is irregular. Then $-2 \equiv 2 \pmod{\ell^n}$ so $\ell^n = 2^1, 2^2$. If $\ell^n = 2^1$ then $-1 \in \Gamma_G$ and s is regular by definition. So suppose $\ell^n = 2^2$. We have the cases $(r,s) = (0,0), (1,0), (1,1), (2,0)$. If $r = 1$ then again $-1 \in \Gamma_G$. Otherwise, $(r,s) = (2,0), (0,0)$ then by Example 2.2.7 we see $\Gamma_G = \Gamma_1(4)$, and $1/2$ is indeed an irregular cusp [13, Exercise 3.8.7]. □

Lemma 3.1.5. *We have*

$$\Gamma_{\overline{G}_{\ell^n}(n;r,s)} = \Gamma_{\overline{G}_{\ell^n}(n;r',s)}$$

where $r' := \max(r, n-r)$.

Proof. Looking back at (3.1.3), we see that e.g. if $r \leq n-r$ then $1+\ell^r a_0 \equiv 1 \pmod{\ell^{n-r}}$, so $\ell^{n-r} \mid \ell^r a_0$. □

Lemma 3.1.5 indicates one of the ways in which different moduli problems can have the same underlying uniformizing congruence subgroup.

To complete our setup for our main result (Theorem 3.3.1), we must decide how to count our elliptic curves. Specifically, we need to distinguish between counting elliptic curves E for which *there exists* a rational G-structure, versus counting equivalence classes of pairs (E, ι) of elliptic curves E equipped with rational G-structures ι. Ultimately, we will see that these two counts differ by a simple multiple (on the main term, and with square root error term).

To this end, for an elliptic curve E over $\mathbf{Q}$, let $r_G(E)$ be the number of K^{al}-isomorphism classes of Gal_K-stable G-equivalence classes of pairs (E, ι) as in Proposition 3.1.1(b), equivalently the number of isomorphism classes $[(E, \iota)] \in Y_G(\mathbf{Q})$. Let

$$r(G) := [N_{\mathrm{GL}_2(\mathbf{Z}/N)}(G) : G] \tag{3.1.6}$$

be the index of G in its normalizer in $\mathrm{GL}_2(\mathbf{Z}/N)$. Write

$$\pm G := G\langle -1 \rangle = G \cup -G,$$

so $\pm G = G$ if and only if $-1 \in G$. Then $N_{\mathrm{GL}_2(\mathbf{Z}/N)}(\pm G) = N_{\mathrm{GL}_2(\mathbf{Z}/N)}(G)$, so $r(G) = 2r(\pm G)$ if $-1 \notin G$.

Example 3.1.7. If $G = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$, then $N_{\mathrm{GL}_2(\mathbf{Z}/N)}(G) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ and so $r(G) = \phi(N) = [\Gamma_0(N) : \Gamma_1(N)]$ and $r(\pm G) = \phi(N)/2$ when $N \geq 3$.

Lemma 3.1.8. *Let E be an elliptic curve over $\mathbf{Q}$ with $j(E) \neq \{0, 1728\}$. Then the following statements hold.*

(a) *If $r_G(E) \geq 1$, then $r_G(E) \geq r(\pm G)$.*
(b) *If $r_G(E) > r(\pm G)$, then there exists a proper subgroup $G' < G$ such that $r_{G'}(E) \geq 1$.*

Proof. First, part (a). By the description in Proposition 3.1.1(ii), the group $N_{\mathrm{GL}_2(\mathbf{Z}/N)}(G)$ acts functorially on moduli points (postcomposing after ι), so it acts by automorphisms of Y_G defined over $\mathbf{Q}$. In particular, this group acts on the set of isomorphism classes $[(E, \iota)] \in Y_G(\mathbf{Q})$ that counted by $r_G(E)$. We claim that the stabilizer of this action is $\pm G$. Indeed, let $u \in N_{\mathrm{GL}_2(\mathbf{Z}/N)}(G)$ and suppose that $[(E, \iota)] = [(E, u\iota)]$. Then there exists an automorphism $\alpha \in \mathrm{Aut}(E)$ such that $G\iota = Gu\iota\alpha$. Since $j(E) \neq \{0, 1728\}$ we have $\mathrm{Aut}(E) = \{\pm 1\}$, hence $G\iota = Gu\iota\alpha = Gu\alpha\iota$ so $\pm Gu = \pm G$, i.e., $u \in \pm G$. This proves (a).

We now prove (b). In view of Proposition 3.1.1(iii), we may prove the contrapositive: if the image $\rho_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \lesssim G \leq \mathrm{GL}_2(\mathbf{Z}/N)$ is *onto* G (up to conjugacy), then in fact $r_G(E) = r(\pm G)$. Indeed, let $[(E, \iota)], [(E, \iota')] \in Y_G(\mathbf{Q})$. Then the isomorphisms $\iota, \iota' \colon E(K^{\mathrm{al}})[N] \to (\mathbf{Z}/N)^2$ may be chosen such that the two representations $\rho_{E,N}, \rho'_{E,N} \colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/N)$ are subgroups of G. Let $u := \iota'\iota^{-1} \in \mathrm{GL}_2(\mathbf{Z}/N)$; then the matrix u conjugates the image of $\rho_{E,N}$ into $\rho'_{E,N}$. But since $\rho_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) = G$ by hypothesis and $\rho'_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \leq G$, we must have $u \in N_{\mathrm{GL}_2(\mathbf{Z}/N)}(G)$. Thus $r_G(E) \leq r(\pm G)$, so by (a) equality holds. □

3.2. Isogeny invariance. In this section, having in section 2 understood our probability as a condition relating isogenous elliptic curves, we are led to the following theorem which relates the image of Galois for isogenous curves.

Theorem 3.2.1. *Let $\varphi \colon E \to E'$ be an isogeny of elliptic curves over a number field K. Let $N \in \mathbf{Z}_{\geq 1}$, let $G := \overline{\rho}_{E,N}(\mathrm{Gal}_K) \leq \mathrm{GL}_2(\mathbf{Z}/N)$ and similarly G' for E'. Then the groups $\Gamma_G, \Gamma_{G'} \leq \mathrm{GL}_2(\mathbf{Q})$ are conjugate in $\mathrm{GL}_2(\mathbf{Q})$, the associated modular curves Y_G and $Y_{G'}$ are isomorphic over $\mathbf{Q}$, and*

$$[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G] = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_{G'}].$$

As mentioned in the introduction, the invariance of the index of the p-adic Galois representation under isogeny was already proven by Greenberg [16, Proposition 2.1.1], by a different argument.

Proof. Without loss of generality, we may assume that $\varphi \colon E \to E'$ is given by a cyclic N-isogeny, so that the Galois image G has

$$G \leq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \tag{3.2.2}$$

It follows from this group-theoretic statement that for every elliptic curve A over K whose mod N-Galois image is (conjugate to a) subgroup of G, there is an isogeny $\varphi\colon A \to A'$ (over K, with cyclic kernel of order N generated by the point corresponding basis vector) such that the mod N-Galois image of A' is a subgroup of G'. Moreover, $\det G = \det G'$, since the determinant is the cyclotomic character and so its image only depends on (the roots of unity in) K. Finally, the dual isogeny maps $\varphi^\vee\colon E' \to E$, and similarly maps G' to G. In other words, the moduli problems attached to G and to G' are naturally equivalent, which gives an isomorphism $Y_G \xrightarrow{\sim} Y_{G'}$ of curves over their common field of definition $\mathbf{Q}(\zeta_N)^{\det G} = \mathbf{Q}(\zeta_N)^{\det G'}$.

From (3.2.2) we have

$$[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G] = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(N)][\Gamma_0(N) : \Gamma_G]. \tag{3.2.3}$$

Applying the isogeny φ and swapping basis vectors acts by conjugation by the element $\nu = \begin{pmatrix} 0 & 1 \\ N & 0 \end{pmatrix}$ so that $\nu\Gamma_G\nu^{-1} = \Gamma_{G'}$. Since ν normalizes the group $\Gamma_0(N)$, we have

$$[\Gamma_0(N) : \Gamma_G] = [\nu\Gamma_0(N)\nu^{-1} : \nu\Gamma_G\nu^{-1}] = [\Gamma_0(N) : \Gamma_{G'}]. \tag{3.2.4}$$

Plugging this into (3.2.3) gives the result on indices. □

Remark 3.2.5. We believe that Theorem 3.2.1 should also follow more generally from the natural compatibilities satisfied by Shimura's theory of canonical models [29, §6.7]. The argument above gives a bit more information, namely that $\Gamma_{G'}$ is obtained from Γ_G under conjugation by the Atkin–Lehner involution of $\Gamma_0(N)$.

In the next section, we will prove that for modular curves Y_G such that Γ_G is torsion free of genus zero, the asymptotic point count depends only on the index $[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G]$; together with Theorem 3.2.1 and the theorem of Katz (as refined in the previous section), this provides a concise explanation and ultimately a proof that the probability P_m is positive for $m \geq 5$.

3.3. Asymptotics. In this section, we prove Theorem 1.3.3. We recall notation from section 1.2, and we prove the following weaker version first.

Theorem 3.3.1. *Let $G \leq \mathrm{GL}_2(\mathbf{Z}/N)$ have $\det G = (\mathbf{Z}/N)^\times$, and suppose that Γ_G is torsion free of genus zero and has no irregular cusps. Let*

$$d(G) := \tfrac{1}{2}[\mathrm{PSL}_2(\mathbf{Z}) : \Gamma_G] = \tfrac{1}{4}[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G].$$

Then $d(G) \in 6\mathbf{Z}_{\geq 1}$, and there exists $c(G) \in \mathbf{R}_{\geq 0}$ such that

$$N_G(H) := \#\{E \in \mathscr{E}_{\leq H} : \overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \lesssim G\} = c(G)H^{1/d(G)} + O(H^{1/e(G)})$$

as $H \to \infty$, where $e(G) = 2d(G)$.

As mentioned in the introduction, we follow an approach outlined in Harron–Snowden [17, §5].

Proof. Our proof proceeds in four steps.

Step 1: universal curve. Let Y_G be the curve over $\mathbf{Q}$ given by Proposition 3.1.1. We are given that Γ_G (equivalently Y_G) has genus zero. If $Y_G(\mathbf{Q}) = \emptyset$, then the theorem is trivially true taking $c(G) = 0$. So we may suppose $\#Y_G(\mathbf{Q}) = \infty$, in which case by choosing a coordinate t we have $Y_G = \operatorname{Spec} \mathbf{Q}[t] \smallsetminus S \subseteq \mathbf{A}^1_{\mathbf{Q}} = \operatorname{Spec} \mathbf{Q}[t]$ where $S \subseteq Y_G$ is a finite set of closed points (stable under $\mathrm{Gal}_{\mathbf{Q}}$). Since Γ_G is torsion free, by Proposition 3.1.1(iv), there is a universal curve of the form

$$E_{G,\mathrm{univ}} \colon y^2 = x^3 + f(t)x + g(t) \tag{3.3.2}$$

where $f(t), g(t) \in \mathbf{Q}(t)$ (and regular away from S). In particular, for every elliptic curve E over $\mathbf{Q}$ such that $\overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \lesssim G$, there exists $t_0 \in \mathbf{Q} \smallsetminus S$ such that E is isomorphic to the curve $y^2 = x^3 + f(t_0)x + g(t_0)$.

Repeating carefully the argument of Harron–Snowden [17, Proposition 3.2, second proof of Lemma 3.3] (given under more restrictive hypothesis, but using the fact that Γ_G has no irregular cusps by hypothesis), after minimally clearing denominators we have $f(t), g(t) \in \mathbf{Q}[t]$ with $\gcd(f(t), g(t)) = 1$, and

$$3 \deg f(t) = 2 \deg g(t) = \deg(j) = [\mathrm{PSL}_2(\mathbf{Z}) : \Gamma_G] = 2d(G) \tag{3.3.3}$$

and moreover $12 \mid [\mathrm{PSL}_2(\mathbf{Z}) : \Gamma_G]$. In particular, $d(G) = \frac{1}{2}[\mathrm{PSL}_2(\mathbf{Z}) : \Gamma_G] \in 6\mathbf{Z}_{\geq 1}$. We now homogenize, letting $t = a/b$ and clearing denominators, giving

$$E_{A,B} \colon y^2 = x^3 + A(a,b)x + B(a,b) \tag{3.3.4}$$

with $A(a,b), B(a,b) \in \mathbf{Z}[a,b]$ satisfying

$$\begin{aligned} \deg A(a,b) &= \deg f(t) = \tfrac{2}{3}d(G) \\ \deg B(a,b) &= \deg g(t) = d(G) \end{aligned} \tag{3.3.5}$$

Step 2: principle of Lipschitz. In view of (3.3.4), as a first step we count the number of integer points in the region

$$R(H) := \{(a,b) \in \mathbf{R}^2 : |A(a,b)| \leq (H/4)^{1/3} \text{ and } |B(a,b)| \leq (H/27)^{1/2}\} \tag{3.3.6}$$

as $H \to \infty$.

We claim that the region $R(H)$ is bounded. By the above, the polynomials $f(t), g(t)$ are coprime, so

$$\max(|f(x)|^3, |g(x)|^2) \geq \mu > 0 \tag{3.3.7}$$

is bounded below for all $x \in \mathbf{R}$. From (3.3.5), we have

$$\begin{aligned} |A(a,b)| &= |b^{2d(G)/3} f(a/b)| \\ |B(a,b)| &= |b^{d(G)} g(a/b)| \end{aligned} \tag{3.3.8}$$

we conclude that

$$H \geq \max_{a,b \in \mathbf{R}} (|4A(a,b)^3|, |27B(a,b)^2|) \geq \mu |b^{d(G)}|$$

so b is bounded; a symmetric argument shows that a is bounded.

Being closed and bounded, the region $R(H)$ is compact. Moreover, $R(H)$ has rectifiable boundary (defined by polynomials). By the Principle of Lipschitz [11], the number of integral points in the region (3.3.6) is given by its area up to an error proportional to the length of its boundary.

Conveniently, the region $R(H)$ is *homogeneous* in H: dropping parentheses to write $H^{1/2d(G)} = H^{1/(2d(G))}$, again from (3.3.5) we have

$$H^{1/d(G)} R(1) = R(H). \tag{3.3.9}$$

Indeed, if $(a', b') = (H^{1/2d(G)} a, H^{1/2d(G)} b)$, then from

$$|A(a', b')| = (H^{1/2d(G)})^{2d(G)/3} |A(a,b)| = H^{1/3} |A(a,b)|$$

and similarly with B, we have $(a', b') \in R(H)$ if and only if $(a, b) \in R(1)$.

Therefore,

$$\begin{aligned} \#(R(H) \cap \mathbf{Z}^2) &= \operatorname{area}(R(H)) + O(\operatorname{len}(\operatorname{bd}(R(H)))) \\ &= \operatorname{area}(R(1)) H^{1/d(G)} + O(H^{1/2d(G)}) \end{aligned} \tag{3.3.10}$$

where the exponent on the error term follows from being the arclength of a 2-dimensional compact region with polynomial boundary.

We will use a slight refinement of this estimate which improves the error term, due to Huxley [18] (and applied in our setting by Pomerance–Schaefer [25, §4])—our boundary is defined by nonlinear polynomials, so the error term in (3.3.10) arising from lattice points on the boundary can be improved to $O(H^{1/2d(G)-\delta})$ for some $\delta > 0$.

Step 3: sieving. We now apply a sieve to take care of local conditions: among the lattice points counted in the previous step, we want exactly those with $E \in \mathscr{E}$. We first restrict the count of lattice points, then adjust the constant by finitely many local factors.

First, the points $(a,b) \in \mathbf{Z}^2$ such that $4A(a,b)^3 + 27B(a,b)^2 = 0$ lie on a curve, which by standard estimates is $O(H^{1/2d(G)})$ so applying this condition does not change (3.3.10). Second, for the points $(a,b) \in \mathbf{Z}^2$ such that $p \mid a$ and $p \mid b$, we have overcounted and we need to apply the correction factor $1 - 1/p^2$ for all primes p. We say $(a,b) \in \mathbf{Z}^2$ is groomed if $4A(a,b)^3 + 27B(a,b)^2 \neq 0$ and $\gcd(a,b) = 1$. A standard Möbius sieve

argument (see e.g. Harron-Snowden [17, Proof of Theorem 5.5]) with the improved error term $O(H^{1/2d(G)-\delta})$, together with (3.3.10), gives

$$\begin{aligned}\#\{(a,b) \in R(H) \cap \mathbf{Z}^2 : (a,b) \text{ groomed}\} \\ = \frac{\operatorname{area}(R(1))}{\zeta(2)} H^{1/d(G)} + O(H^{1/2d(G)}).\end{aligned} \tag{3.3.11}$$

We now consider local conditions imposed by minimal models. Suppose that q is a power of a prime p such that $q^4 \mid A(a,b)$ and $q^6 \mid B(a,b)$ with $\gcd(a,b) = 1$. Recall $A(t,1) = f(t)$ and $B(t,1) = g(t)$ are coprime. If $p \nmid b$, then $f(t)$ and $g(t)$ have a common root $a/b \in \mathbf{Z}/q$, so q divides the nonzero resultant $\operatorname{Res}_t(f(t), g(t)) \in \mathbf{Z}$ of $f(t)$ and $g(t)$ with respect to t [9, Chapter 3]; similarly, if $p \nmid a$ then q divides the resultant of $A(1,u) = u^{\deg f} f(1/u)$ and $B(1,u)$. Let m be the least common multiple of these two resultants. Applying the Sun Zu Theorem (CRT), we have shown that if $e \in \mathbf{Z}_{\geq 1}$ satisfies $e^4 \mid A(a,b)$ and $e^6 \mid B(a,b)$, then in fact $e \mid m$.

So let E be an elliptic curve over $\mathbf{Q}$, and suppose E has a G-level structure defined over $\mathbf{Q}$ in the sense of Proposition 3.1.1(iv). By (3.3.4), we have $E\colon y^2 = x^3 + Ax + B$ where $A = A(a,b)$ and $B = B(a,b)$ for some $a, b \in \mathbf{Z}$ with $\gcd(a,b) = 1$ (coming from $t = a/b \in \mathbf{Q}$ in lowest terms). Then there exists a unique integer $e \in \mathbf{Z}_{\geq 1}$ such that the unique representative of E in $\mathscr{E}$ is given by $y^2 = x^3 + A'x + B'$ where $A' = e^{-4}A(a,b) \in \mathbf{Z}$ and $B' = e^{-6}B(a,b) \in \mathbf{Z}$: namely, the largest positive integer e such that $e^{12} \mid \gcd(A(a,b)^3, B(a,b)^2)$. We call e the minimality defect of (a,b). By the previous paragraph, we have $e \mid m$. Moreover,

$$e^{12} \operatorname{ht} E = \max(|4A^3|, |27B^2|)$$

so $(A,B) \in R(e^{12}H)$. Recalling the discussion at the end of section §3.1, let

$$N_G^{\square}(H) := \#\{(E, G\iota) : E \in \mathscr{E}_{\leq H} \text{ and } \overline{\rho}_{E,N}(\operatorname{Gal}_{\mathbf{Q}}) \lesssim_\iota G\}$$

count the number of pairs $(E, G\iota)$ where $E \in \mathscr{E}_{\leq H}$ and $G\iota$ is a $\operatorname{Gal}_{\mathbf{Q}}$-stable G-equivalence class of isomorphism $E[N](K^{\mathrm{al}}) \to (\mathbf{Z}/N)^2$. Running this argument in the other direction, we conclude that the count

$$\begin{aligned}N_G^{\square}(H) = \sum_{e \mid m} \#\{(a,b) \in R(e^{12}H) \cap \mathbf{Z}^2 \\ : (a,b) \text{ groomed, minimality defect } e\}.\end{aligned} \tag{3.3.12}$$

Of course, the condition that (a,b) has minimality defect e is determined by congruence conditions on a and b. Let δ_e be the proportion of integers (congruence classes) satisfying this condition, so $0 \leq \delta_e \leq 1$ and $\sum_{e \mid m} \delta_e = 1$. For each e and each such congruence class, the principle of Lipschitz applies; summing of congruences classes then multiplies the asymptotic by

the factor δ_e. Applying (3.3.11), from (3.3.12) we conclude

$$N_G^{\square}(H) = \frac{\mathrm{area}(R(1))}{\zeta(2)}\left(\sum_{e|m}\delta_e e^{12/d(G)}\right)H^{1/d(G)} + O(H^{1/2d(G)}) \tag{3.3.13}$$

so in particular

$$c^{\square}(G) = \frac{\mathrm{area}(R(1))}{\zeta(2)}\left(\sum_{e|m}\delta_e e^{12/d(G)}\right). \tag{3.3.14}$$

Step 4: automorphisms. Finally, to count the number of curves (rather than curves equipped with level structure), we apply Lemma 3.1.8. For the curves with Galois image exactly G (up to conjugacy) and $j(E) \neq 0, 1728$, we have overcounted by the factor $2r(\pm G) = r(G)$, the additional factor 2 coming from $t = a/b = a'/b' \in \mathbf{Q}$ is in lowest terms if and only if $(a', b') = \pm(a, b)$. The curves with $j(E) = 0, 1728$ have $A = 0$ or $B = 0$, so are negligible (comparing to the length of the boundary). For the remaining curves, suppose that E has $\overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) = G' < G$ a proper subgroup (up to conjugation). If $\Gamma_{G'}$ has genus ≥ 1, then $N_{G'}(H)$ is either finite or grows slower than any power of H (see Serre [27, p. 133]), so in particular is $O(H^{1/d(G)})$. Otherwise, $\Gamma_{G'}$ has genus zero and is still torsion free without irregular cusps. Since $\det G' = \det G = (\mathbf{Z}/N)^{\times}$, we have

$$[G : G'] = [\Gamma_G : \Gamma_{G'}] \in \mathbf{Z}_{\geq 2}$$

so $d(G') \geq 2d(G)$. Applying Step 3 then shows that the count of these curves is negligible.

Thus from (3.3.13) we get that

$$\#\{E \in \mathscr{E}_{\leq H} : \overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \lesssim G\} = c(G)H^{1/d(G)} + O(H^{1/2d(G)}) \tag{3.3.15}$$

where

$$c(G) = \frac{c^{\square}(G)}{r(G)} = \frac{\mathrm{area}(R(1))}{r(G)\zeta(2)}\left(\sum_{e|m}\delta_e e^{12/d(G)}\right) \tag{3.3.16}$$

as claimed. □

Corollary 3.3.17. *With notation as in Theorem 3.3.1, we have*

$$N_G(H) = \#\{E \in \mathscr{E}_{\leq H} : \overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) \sim G\} + O(H^{1/2d(G)}).$$

In other words, counting curves with image contained in G is asymptotic to the count of curves with image equal to G.

Proof. Proven in Step 4 of the proof of Theorem 3.3.1. □

Proposition 3.3.18. *The constant $c(G)$ in Theorem 3.3.1 is effectively computable.*

Proof. We first claim that the universal curve is effectively computable, in the sense that there is a Turing machine (effective procedure) that, given input G, outputs $f(t), g(t) \in \mathbf{Q}(t)$ such that (3.3.2) is universal. We compactify Y_G by adding cusps $X_G := Y_G \cup \Delta$; the set Δ (naturally identified with the set of G-orbits of $\mathbf{P}^1(\mathbf{Z}/N)$) is effectively computable. By Voight–Zureick-Brown [32, Chapter 4], the canonical ring of Y_G is the log canonical ring of X_G; this graded ring has a simple, explicit description [32, §4.2] in terms of $\#\Delta$. Moreover [32, §6.2], the log canonical ring is isomorphic to the graded ring of modular forms of even weight for Γ_G; by linear algebra with q-expansions computed via modular symbols as explained by Assaf [1], we obtain explicit equations for this canonical ring, realizing X_G as a subvariety of weighted projective space. Next, we can effectively determine if $X_G(\mathbf{Q}) = \emptyset$ and, if $X_G(\mathbf{Q}) \neq \emptyset$, compute $P_0 \in X_G(\mathbf{Q})$: briefly, we compute a canonical divisor, embed $X_G \to \mathbf{P}^2$ as a conic, and either find that $X_G(\mathbf{Q}_p) = \emptyset$ for some prime p or we find a point in $X_G(\mathbf{Q})$, after which we may parametrize the entire set $X_G(\mathbf{Q})$ in terms of a parameter t, giving a computable isomorphism between the field of fractions of the log canonical ring and $\mathbf{Q}(t)$. Finally, using linear algebra we recognize the Eisenstein series E_4, E_6 first as elements of the graded ring and then as rational functions in t.

The remaining quantities are also effectively computable. We compute the degree as

$$4d(G) = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G] = [\mathrm{SL}_2(\mathbf{Z}/N) : G \cap \mathrm{SL}_2(\mathbf{Z}/N)]\phi(N).$$

For the constant $c(G)$, we note that the area $\mathrm{area}(R(1))$ can be computed to any desired precision by numerical integration, and $r(G)$ can be determined by finite exhaustion. The integer m is effectively computable as the least common multiple of resultants, and we can find the set of divisors of m and then for each $e \mid m$, compute the proportion δ_e by exhaustive enumeration. □

Remark 3.3.19. Actually, by work of Sebbar [26] there are exactly 33 torsion-free, genus zero subgroups of $\mathrm{PSL}_2(\mathbf{Z})$, all of which lift to torsion-free subgroups of $\mathrm{SL}_2(\mathbf{Z})$ by Kra [22, Theorem, p. 181]. Up to twist, there are only finitely many G that can give each Γ_G, so the set of groups G that satisfy the hypotheses of Theorem 1.3.3 is finite (again, up to twist). So it would be desirable to carry out the proof of Proposition 3.3.18 in every case, and to just compute these constants (keeping track of the effect of the twist)—but such a task lies outside of the motivation and scope of this paper.

Nevertheless, many of the curves in Sebbar's list arise in our analysis, as follows. By (1.3.2) and the natural projection $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{PSL}_2(\mathbf{Z})$, we can

associate to every $G_\ell(n;r,s)$ a subgroup Γ_G of $\mathrm{PSL}_2(\mathbf{Z})$ via

$$G_\ell(n;r,s) \leftrightarrow \Gamma_{\overline{G}_{\ell^n}(n;r,s)},$$

(though of course a given group may not have genus 0). Of the 33 genus zero subgroups of $\mathrm{PSL}_2(\mathbf{Z})$, some can be written as Γ_G with $G = \overline{G}_{\ell^n}(n;r,s)$. In particular, we have

$$\begin{aligned} \Gamma(\ell^n) &= \Gamma_{\overline{G}_{\ell^n}(2n;n,n)} \\ \Gamma_1(\ell^n) &= \Gamma_{\overline{G}_{\ell^n}(n;n,0)} = \Gamma_{\overline{G}_{\ell^n}(n;0,0)} \\ \Gamma_0(4) &= \Gamma_{\overline{G}_4(2;1,0)}, \end{aligned} \tag{3.3.20}$$

with functorial intersections. In this way, the 16 groups

$\Gamma(2)$	$\Gamma(3)$	$\Gamma(4)$	$\Gamma(5)$	$\Gamma_1(5)$	$\Gamma_1(7)$
$\Gamma_1(8)$	$\Gamma_1(9)$	$\Gamma_1(10)$	$\Gamma_1(12)$	$\Gamma_0(4)$	$\Gamma_0(6)$
$\Gamma_0(4)\cap\Gamma(2)$	$\Gamma_1(8)\cap\Gamma(2)$	$\Gamma_0(2)\cap\Gamma(3)$	$\Gamma_0(3)\cap\Gamma(2)$		

in [26] can be each realized as (intersections of) the $\Gamma_{\overline{G}_\ell(n;r,s)}$. Of the remaining 17 torsion-free genus zero groups, 9 can be realized as Γ_H, where H is a *proper* subgroup of some $\overline{G}_\ell(n;r,s)$. The remaining 8 torsion-free genus zero groups

$$\begin{aligned} &\Gamma_0(8),\ \Gamma_0(9),\ \Gamma_0(8)\cap\Gamma(2),\ \Gamma_0(12), \\ &\Gamma_0(16),\ \Gamma_0(18),\ \Gamma_0(16)\cap\Gamma_1(8),\ \Gamma_0(25)\cap\Gamma_1(5) \end{aligned}$$

do not correspond to a $G_\ell(n;r,s)$ (or to an intersection).

We now officially conclude the proof.

Proof of Theorem 1.3.3. Combine Theorem 3.3.1 with Proposition 3.3.18. □

4. The probabilities P_m for $m \geq 5$

In this section, we prove Theorem 1.3.1, and we obtain an explicit result for the cases $m = 5$ and $m = 7$. Although we do not do so, one can apply the arguments of this section to similarly compute P_m for the remaining values of $m \geq 5$.

4.1. Proof of main result. Let $m \in \{1, 2, \ldots, 10, 12, 16\}$. As in section 1.2, we seek to refine our understanding of the subset

$$\mathscr{E}_{m?} := \{E \in \mathscr{E} : m \mid \#E(\mathbf{F}_p) \text{ for a set of primes } p \text{ of density } 1\} \tag{4.1.1}$$

by considering the probability

$$P_m := \lim_{H\to\infty} \frac{\#\{E \in \mathscr{E}_{\leq H} : m \mid \#E(\mathbf{Q})_{\mathrm{tor}}\}}{\#\{E \in \mathscr{E}_{m?} \cap \mathscr{E}_{\leq H}\}}; \tag{4.1.2}$$

in particular, we want to show P_m is defined. (Until we do, we may take P_m to be the lim sup.)

We now proceed to prove Theorem 1.3.1 for $m \geq 5$. Our strategy is as follows. First, building on section 2, we show that 100% of curves in the numerator and denominator of P_m are obtained from curves whose ℓ-adic Galois image in a clean basis is equal to $G_\ell(n; r, s)$ for every $\ell \mid m$ (in particular, the mod m image is the full preimage of the reductions modulo $\ell^n \parallel m$). Second, using Theorem 3.3.1, we give an asymptotic count for these curves; we find a positive proportion, as predicted by Theorem 3.2.1.

Definition 4.1.3. *We say that an elliptic curve E over $\mathbf{Q}$ is m-full if for all $\ell^n \parallel m$, there exist $r, s \in \mathbf{Z}_{\geq 0}$ with $r, s \leq n$ such that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbf{Q}}) = G_\ell(n; r, s)$ (in a basis for $T_\ell(E)$).*

As in (2.2.8), in Definition 4.1.3 we may without loss of generality further suppose that $r + s \leq n$. By Lemma 2.2.5, if E is m-full, then $E \in \mathscr{E}_{m?}$. The following proposition provides a converse sufficient for our purposes.

Proposition 4.1.4. *We have*

$$\#\{E \in \mathscr{E}_{\leq H} : E \text{ is } m\text{-full}\} \sim \#(\mathscr{E}_{m?} \cap \mathscr{E}_{\leq H})$$

as $H \to \infty$.

Proof. Let $E \in \mathscr{E}_{m?}$. By Corollary 2.3.13, there exists a cyclic isogeny $\varphi\colon E \to E'$ of degree $d \mid m$ such that for all $\ell^n \mid m$, we have $\rho_{E',\ell}(\mathrm{Gal}_{\mathbf{Q}}) \leq G_\ell(n; r, n-r)$ for some $0 \leq r \leq n$ (with these quantities depending on ℓ). Moreover, by Theorem 2.3.14, if $\rho_{E',\ell}(\mathrm{Gal}_{\mathbf{Q}}) = G_\ell(n; r, n-r)$ for all $\ell \mid m$ (so equality holds), then E is m-full.

Let $T_m E := \varprojlim_n E[m^n](\mathbf{Q}^{\mathrm{al}}) \simeq \prod_{\ell \mid m} \mathbf{Z}_\ell^2$ be the m-adic Tate module; let

$$\rho_{E,m}\colon \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{Z}_m}(T_m E) \simeq \mathrm{GL}_2(\mathbf{Z}_m) \simeq \prod_{\ell \mid m} \mathrm{GL}_2(\mathbf{Z}_\ell) \tag{4.1.5}$$

be the associated Galois representation, and let $G := \rho_{E,m}(\mathrm{Gal}_{\mathbf{Q}})$ be the image. Repeat this with E' and G'. Let $G'_{\mathrm{full}} := \prod_{\ell \mid m} G_\ell(n; r, n-r)$, so by the first paragraph we have $G' \leq G'_{\mathrm{full}}$. Suppose that $G' < G'_{\mathrm{full}}$ is a strict inequality; we will show the count of the curves E obtained in this way is asymptotically negligible.

We first consider the counts of the target curves E'. We begin by reducing to a finite problem, lifting an argument from Sutherland–Zywina [30, Proof of Proposition 3.6(i)]. The profinite group G'_{full}, as a product of compact ℓ-adic Lie groups, satisfies condition (iv) of a proposition of Serre [27, Proposition, §10.6, p. 148; Example 1, p. 149], so it satisfies condition (ii): its Frattini subgroup $\Phi(G'_{\mathrm{full}})$, the intersection of the maximal closed proper subgroups, is open. Therefore there are only finitely many maximal proper open (so finite index) subgroups of G'_{full}. In particular, G' is contained in (at least) one of these subgroups.

Since $m \geq 5$, the group $\Gamma_{G'_{\mathrm{full}}}$ is torsion free by Lemma 2.2.9(d), and so by Proposition 3.1.1, there exists a curve $Y_{G'_{\mathrm{full}}}$ that is a fine moduli space for G'_{full}. Since $G' < G'_{\mathrm{full}}$, the same holds for G' and moreover we have a map $Y_{G'} \to Y_{G'_{\mathrm{full}}}$. Since $[G'_{\mathrm{full}} : G'] > 1$ and $\det(G') = \det(G'_{\mathrm{full}}) = \mathbf{Z}_m^\times$, we have

$$[G'_{\mathrm{full}} \cap \mathrm{SL}_2(\mathbf{Z}_m) : G' \cap \mathrm{SL}_2(\mathbf{Z}_m)] > 1,$$

and hence $[\Gamma_{G'_{\mathrm{full}}} : \Gamma_{G'}] > 1$. Repeating the argument in Corollary 3.3.17, the asymptotic count of elliptic curves parametrized by $Y_{G'}$ are negligible in comparison to those parametrized by Y_G (the image of $Y_{G'}(\mathbf{Q})$ in $Y_G(\mathbf{Q})$ is thin). Therefore

$$\begin{aligned} &\#\{E' \in \mathscr{E}_{\leq H} : [E'] \in Y_{G'}(\mathbf{Q})\} \\ &\qquad = o(\#\{E' \in \mathscr{E}_{\leq H} : [E'] \in Y_{G'_{\mathrm{full}}}(\mathbf{Q})\}). \end{aligned} \tag{4.1.6}$$

Repeating this argument with G' one of the finitely many maximal proper subgroups and summing, we have

$$\#\{E' \in \mathscr{E}_{\leq H} : G' < G'_{\mathrm{full}}\} = o(\#\{E \in \mathscr{E}_{\leq H} : [(E, \iota)] \in Y_{G'_{\mathrm{full}}}(\mathbf{Q})\}).$$

To finish, we count the curves E. By Theorem 3.2.1, the groups Γ_G is conjugate in $\mathrm{GL}_2(\mathbf{Q})$ to $\Gamma_{G'}$ and have the same underlying modular curve. By Theorem 3.3.1, the asymptotics for the count of such E is the same as that for counting E'; therefore, the result follows from (4.1.6). □

With Proposition 4.1.4 in hand, we just need to count by height the number of m-full elliptic curves by the choices for the groups $G_\ell(n; r, s)$ for $\ell^n \parallel m$ subject to (2.2.8), and then to decide the proportion of which have m-torsion, as follows. We recall the special case $\ell^n = 2^1$ in Example 2.2.6.

Corollary 4.1.7. *For $m \geq 5$, the probability P_m is nonzero for all m.*

Proof. By Proposition 4.1.4, in the denominator of P_m we need to count curves parametrized by groups $G \leq \mathrm{GL}_2(\mathbf{Z}/m)$ isomorphic (via the CRT) to the product $\overline{G}_{\ell^n}(n_\ell; r_\ell, s_\ell)$ (with $0 \leq r_\ell, s_\ell, r_\ell + s_\ell \leq n_\ell$, where $m = \prod \ell^{n_\ell}$, by (2.2.8)), and the numerator consists of the subset of counts with $r_\ell + s_\ell = n_\ell$. By Lemma 2.2.9(d), the groups Γ_G are torsion free. Only groups G with $\det G = (\mathbf{Z}/m)^\times$ and Γ_G of genus zero contribute nonnegligibly. By Theorem 3.3.1, the asymptotic for such a group is determined by $d(G) = \frac{1}{4}[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G]$.

We compute

$$[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G] = [\mathrm{GL}_2(\mathbf{Z}/m) : G] = \prod_{\ell \mid m} [\mathrm{GL}_2(\mathbf{Z}_\ell) : G_\ell(n_\ell; r_\ell, s_\ell)] \tag{4.1.8}$$

since the group is a direct product. But we computed these indices in Lemma 2.2.9: they only depend on whether $\min(r_\ell, n_\ell - r_\ell) \geq 1$ or not; the smallest degree $d(G)$ (from the smallest index, giving the largest asymptotic

$H^{1/d(G)}$) occurs when $\min(r_\ell, n_\ell - r_\ell) \geq 1$ for each ℓ. Whatever the largest asmyptotic, we may always choose $s_\ell = n_\ell - r_\ell$ and by Lemma 2.2.17(a) such curves have m-torsion, hence arise with positive probability. □

For the sake of explicitness, we indicate the rate of growth for each group in Table 4.1.9. By a straightforward calculation in Magma [5], we find Table 4.1.9: the universal elliptic curve for $G_\ell(n; r, n-r)$ is isogenous to $G_\ell(n; r, n-r-k)$ for $k \leq n-r$ and $G_\ell(n; n-r, r-k)$ for $k \leq r$, so we can use universal equations for one to get to all others. A list of all universal polynomials for the m-full groups that occur can be found online [10].

m	G	$d(G)$	torsion
5	all	6	$\{0\}$, $\mathbf{Z}/5$
6	all	6	$\mathbf{Z}/2$, $\mathbf{Z}/6$
7	all	12	$\{0\}$, $\mathbf{Z}/7$
8	$G_2(3; r, 0)$, $r = 1, 2, 3$	12	$\mathbf{Z}/2^r$
8	$G_2(3; r, 1)$, $r = 1, 2$	6	$\mathbf{Z}/2^r \times \mathbf{Z}/2$
9	all	18	$\{0\}$, $\mathbf{Z}/3$, $\mathbf{Z}/9$
10	all	18	$\mathbf{Z}/2$, $\mathbf{Z}/10$
12	$G_2(4; r, 0) \times G_3(1; 0, 0)$, $r = 1, 2$	24	$\mathbf{Z}/2^r$
12	$G_2(4; 1, 1) \times G_3(1; 1, 0)$	12	$\mathbf{Z}/6 \times \mathbf{Z}/2$
16	all	24	$\mathbf{Z}/2^r \times \mathbf{Z}/2$, $r = 0, 1, 2, 3$

Table 4.1.9: Data for modular curves parametrizing m-full elliptic curves

We find that for $m \in \{5, 6, 7, 9, 10, 16\}$, all m-full groups G have the same index $d(G)$; for $m = 8, 12$, we distinguish between two cases.

4.2. Setup to compute P_ℓ for $\ell = 5, 7$. In the remainder of this section, we follow the proof of Corollary 4.1.7 and compute P_ℓ for $\ell = 5, 7$. The main simplification in these cases is that, aside from a negligible subset when $\ell = 5$ (see Lemma 4.3.3), elliptic curves in $\mathscr{E}_{\ell?}$ either have a global point of order ℓ, or are ℓ-isogenous to one that does.

Let $\ell \in \{5, 7\}$. The Tate normal form of an elliptic curve, which gives a universal curve with a rational ℓ-torsion point, has Weierstrass model

$$E(t) : y^2 + (1-c)xy - by = x^3 - bx^2 \tag{4.2.1}$$

with $b, c \in \mathbf{Z}[t]$ explicitly given; the rational point $(0, 0)$ generates a rational subgroup of order ℓ, and accordingly the image of the ℓ-adic Galois representation lies in the group $G_\ell(1; 1, 0)$ as in Example 2.2.7. Applying Vélu's formulas [31, (11)] to the isogeny with kernel generated by $(0, 0)$, one obtains a model:

$$E'(t) : y^2 + (1-c)xy - by = x^3 - bx^2 + dx + e, \tag{4.2.2}$$

for $d, e \in \mathbf{Z}[t]$. The curve $E'(t)$ is the universal elliptic curve for the moduli problem of elliptic curves with ℓ-adic Galois representation contained in $G_\ell(1;0,0)$, just as in Lemma 2.2.17(b) the property that for any nonsingular specialization $t \in \mathbf{Q}$ it locally has a subgroup of order ℓ.

Passing to short Weierstrass form, we write

$$E(t) : y^2 = x^3 + f(t)x + g(t)$$
$$E'(t) : y^2 = x^3 + f'(t)x + g'(t),$$

for explicit polynomials $f(t), f'(t), g(t), g'(t) \in \mathbf{Q}[t]$ given in (4.3.2) below. Let $j(t)$ (resp. $j'(t)$) be the j-function of $E(t)$ (resp. $E'(t)$).

Recall the integer $r(G)$ defined in (3.1.6). As in Example (3.1.7), we find that

$$r(G) = 4, 6 \tag{4.2.3}$$

for $m = 5, 7$, so the ratio of the two cancels in each case.

Writing $t = a/b$ and homogenizing, we finally arrive at two-parameter integral models

$$\begin{aligned} E(a,b) &: y^2 = x^3 + A(a,b)x + B(a,b) \\ E'(a,b) &: y^2 = x^3 + A'(a,b)x + B'(a,b), \end{aligned} \tag{4.2.4}$$

where $A, B \in \mathbf{Z}[a,b]$ and $A', B' \in \mathbf{Z}[a,b]$ are coprime pairs.

We can now count integral curves by height and apply the methods of the previous sections. Before preceding, as a guide to the reader we give an overview of the calculations in both cases here.

The probability P_ℓ will follow from the explicit computation of two growth constants: $c(G_\ell(1;1,0))$ and $c(G_\ell(1;0,0))$, associated to elliptic curves with a rational point of order ℓ, and those that admit a rational ℓ-isogeny (but not a rational point of order ℓ), respectively. Since the main growth terms have the same degree (see Table 4.1.9), we find

$$P_\ell = \frac{c(G_\ell(1;1,0))}{c(G_\ell(1;1,0)) + c(G_\ell(1;0,0))} = \left(1 + \frac{c(G_\ell(1;0,0))}{c(G_\ell(1;1,0))}\right)^{-1}, \tag{4.2.5}$$

where the constants $c(G_\ell(1;1,0))$ and $c(G_\ell(1;0,0))$ are defined in (3.3.13).

To ease notation, we abbreviate

$$c := c(G_\ell(1;1,0))$$
$$c' := c(G_\ell(1;0,0)).$$

We also define the quantities arising in Step 3 of Theorem 3.3.1, namely

$$\begin{aligned} m &:= \operatorname{lcm}\big(\operatorname{Res}_t(f(t), g(t)), \operatorname{Res}_t(\breve{f}(t), \breve{g}(t))\big) \\ m' &:= \operatorname{lcm}\big(\operatorname{Res}_t(f'(t), g'(t)), \operatorname{Res}_t(\breve{f}'(t), \breve{g}'(t))\big), \end{aligned} \tag{4.2.6}$$

where $\breve{h}(t) := t^{\deg h} h(1/t)$ is the reciprocal polynomial of $h(t) \in \mathbf{Q}[t]$, along with the corresponding correction ratios δ_e and δ'_e measuring the proportion of curves with minimality defect e for $e \mid m, m'$, respectively, all as appearing in (3.3.13).

Therefore, to compute P_ℓ we are reduced to computing the ratio

$$\frac{c'}{c} = \frac{\operatorname{area}(R'(1)) \sum_{e|m'} \delta'_e e^{12/d(G)}}{\operatorname{area}(R(1)) \sum_{e|m} \delta_e e^{12/d(G)}}, \tag{4.2.7}$$

where

$$\begin{aligned} R(1) &:= \{(a,b) \in \mathbf{R}^2 : |A(a,b)| \le 4^{-1/3} \text{ and } |B(a,b)| \le 27^{-1/2}\} \\ R'(1) &:= \{(a,b) \in \mathbf{R}^2 : |A'(a,b)| \le 4^{-1/3} \text{ and } |B'(a,b)| \le 27^{-1/2}\}. \end{aligned} \tag{4.2.8}$$

We compute the local corrections by finite search. The ratio of areas has a remarkably simple expression, as follows. By Lemma 3.1.5, we have $\Gamma_{\overline{G}_\ell(1;0,0)} = \Gamma_{\overline{G}_\ell(1;1,0)}$, i.e., the curves $E(t)$ and $E'(t)$ are universal curves over the same base modular curve. Over $\mathbf{Q}(\zeta_\ell)$, the determinant of the mod ℓ Galois representation (the cyclotomic character) becomes trivial, so both of these curves solve the same moduli problem over $\mathbf{Q}(\zeta_\ell)$, and hence over $\mathbf{C}$. Since these two schemes represent the same functor, there is an isomorphism between them. Both have base scheme a Zariski open in $\mathbf{P}^1$ (say with variables t and t', respectively), so there exists a linear fractional transformation ψ such that $t' = \psi(t)$. Postcomposing with the j-function $X \to X(1) = \mathbf{P}^1$, we conclude that there exists a linear fractional transformation ψ such that

$$j(\psi(t)) = j'(t). \tag{4.2.9}$$

In concrete terms, given the j-invariants $j(t)$ and $j'(t)$ we compare zeroes and poles to explicitly compute the linear fractional transformation ψ. By homogenizing t to (a,b) and computing the effect on each variable, we get a change of variables mapping $R(1)$ bijectively onto $R'(1)$. Therefore, the ratio

$$\frac{\operatorname{area}(R'(1))}{\operatorname{area}(R(1))}$$

is the determinant of the change of variables matrix! (In particular, this can be given exactly without needing it for the two areas themselves.)

4.3. The case $\ell = 5$. We now carry out the above strategy for $\ell = 5$. In the Tate normal form (4.2.1), we compute $b = c = t$ (see also García-Selfa–Tornero [15, Thm. 3.1]); applying Vélu's formulas [31, (11)] gives

$$\begin{aligned} d &= -5t^3 - 10t^2 + 5t, \text{ and} \\ e &= -t^5 - 10t^4 + 5t^3 - 15t^2 + t \end{aligned} \tag{4.3.1}$$

in (4.2.2). The Weierstrass coefficients and j-invariants of $E(t)$ and $E'(t)$ are given by

$$\begin{aligned} f(t) &= -27(t^4 - 12t^3 + 14t^2 + 12t + 1) \\ g(t) &= 54(t^6 - 18t^5 + 75t^4 + 75t^2 + 18t + 1) \\ j(t) &= \frac{f(t)^3}{t^5(t^2 - 11t - 1)} \end{aligned}$$

(4.3.2)

$$\begin{aligned} f'(t) &= -27(t^4 + 228t^3 + 494t^2 - 228t + 1) \\ g'(t) &= 54(t^6 - 522t^5 - 10005t^4 - 10005t^2 + 522t + 1) \\ j'(t) &= \frac{f'(t)^3}{t(t^2 - 11t - 1)^5}. \end{aligned}$$

Lemma 4.3.3. *The curve $E'(t_0)$ defined by (4.2.2) has a rational 5-torsion point if and only $t_0 \in \mathbf{Q}^{\times 5}$.*

Proof. The discriminant of $E'(t)$ is $t(t^2 - 11t - 1)^5$, so $t = 0$ is the only rational singular specialization. By explicitly computing the 5-division polynomial of $E'(t)$ using the expressions in (4.3.2), one can show that the 5-torsion field of $E'(t)$ has Galois group F_{20} over $\mathbf{Q}(t)$ and is the splitting field of $x^5 - t$ over $\mathbf{Q}(t)$. For any non-zero specialization $t = t_0$, the mod 5 representation of $E'(t_0)$ is a subgroup of

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

If, in addition, $E'(t_0)$ has a rational 5-torsion point, then the above Galois representation is diagonal, yet must have surjective determinant. Thus, the 5-torsion field of $E'(t_0)$ is $\mathbf{Q}(\zeta_5)$ and so the polynomial $x^5 - t_0$ has a rational root, but does not split; *i.e.* t_0 is a rational 5th power.

Conversely, if $t_0 = s^5$ then the point

$$\begin{aligned} &(s^8 + s^7 + 2s^6 - 2s^5 + 5s^4 - 3s^3 + 2s^2 - s, \\ &\quad s^{12} - s^{11} - s^{10} + s^8 - 10s^7 + 13s^6 - 11s^5 + 5s^4 - 3s^3 + s^2) \end{aligned}$$

is a point of order 5. □

Remark 4.3.4. If $t_0 \in \mathbf{Q}$, then as in Example 2.2.16, the isogeny class to which $E(t_0)$ belongs typically contains only two curves, $E(t_0)$ and $E'(t_0)$, linked by a 5-isogeny, with the two representations in Lemma 2.3.5 (contained in a Borel subgroup); see for example the isogeny class with LMFDB [21] label 38.b. However, if t_0 is a 5th power, then $E'(t_0)$ has a rational 5-torsion point, the mod 5 representation of $E'(t_0)$ is contained in the split Cartan subgroup

$$\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix} \leq \mathrm{GL}_2(\mathbf{F}_5),$$

and $E'(t_0)$ admits two different rational 5-isogenies: for example, 1342.b.

By the classification of possible images of mod 5 and mod 7 representations of Zywina [33, Theorems 1.4, 1.5], this is a "worst case scenario" for the isogeny graph of a curve in $\mathscr{E}_{5?}$. By comparison, for curves in $\mathscr{E}_{7?}$, all isogeny classes contain two curves linked by a 7-isogeny. See the recent preprint Chiloyan–Lozano-Robledo [7] on the classification of isogeny graphs of elliptic curves over $\mathbf{Q}$.

We now compute the all-important change of coordinates $\phi(t)$ in (4.2.9). We write

$$u := (11 + 5\sqrt{5})/2 \approx 11.09 \in \mathbf{R}_{>0}$$

so that u and $-1/u$ are the roots of the quadratic polynomial $t^2 - 11t - 1$. We define the linear fractional transformation

$$\psi(t) := \frac{ut + 1}{t - u}, \tag{4.3.5}$$

mapping $u \to \infty$, $0 \to -1/u$, and $\infty \to u$. It is routine to verify that $j(\psi(t)) = j'(t)$.

Lemma 4.3.6. *With $R(1), R'(1)$ as defined in (4.2.8), we have*

$$\frac{\operatorname{area}(R'(1))}{\operatorname{area}(R(1))} = \frac{1}{5}. \tag{4.3.7}$$

Proof. By the observation following (4.2.9), the ratio of areas is the determinant of the change of variables matrix mapping $R(1)$ bijectively onto $R'(1)$. There is a pleasant, visible symmetry in this case—one which gave this entire project momentum—so we are even more explicit in this case.

Define the angle $\theta := \arctan(2/11)/2$, so that

$$\cos\theta = \frac{1}{5}\sqrt{\frac{25 + 11\sqrt{5}}{2}} \quad \text{and} \quad \sin\theta = \frac{1}{5}\sqrt{\frac{25 - 11\sqrt{5}}{2}}.$$

Direct calculation reveals that

$$\begin{aligned} A'(a\cos\theta - b\sin\theta, a\sin\theta + b\cos\theta) &= A(\sqrt{5}a, -\sqrt{5}b), \\ B'(a\cos\theta - b\sin\theta, a\sin\theta + b\cos\theta) &= B(\sqrt{5}a, -\sqrt{5}b). \end{aligned}$$

In other words, a rotation by θ, followed by a reflection and a scaling of a and b by $\sqrt{5}$ maps $R'(1)$ bijectively onto $R(1)$, as in Figure 4.3.8.

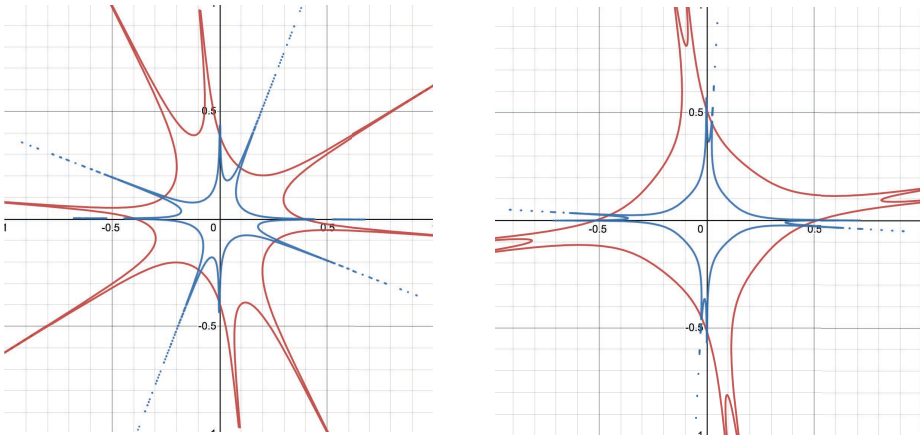

Figure 4.3.8: Symmetry of $R(1)$ and $R'(1)$, $m = 5$

The ratio $\operatorname{area}(R'(1))/\operatorname{area}(R(1)) = 1/5$ follows from the fact that a reflection/rotation is area-preserving and the scaling is by $\sqrt{5}$ in both directions a and b. □

Now we calculate the sieve factor in (4.2.7), which is the last ingredient needed for an exact expression for P_5. Because we will perform a similar sieve for the case P_7, we go into some detail here and then proceed more quickly through this step when $\ell = 7$.

We start by recording the integers m and m' defined in (4.2.6), computed by resultants:

$$m = 2^{16}3^{36}5,$$
$$m' = 2^{16}3^{36}5^{25}.$$

We recall that $d(G_5(1;1,0)) = d(G_5(1;0,0)) = 6$. Thus, the local correction factors for c is

$$\sum_{e|m} \delta_e e^{12/d(G)} = \sum_{e|2^{16}3^{36}5} \delta_e e^2$$

and similar for c'. We now compute the δ_e and δ'_e.

Lemma 4.3.9. *With all notation as above, we have $\delta_1 = 1$ and $\delta_e = 0$ for all other divisors e of m.*

Proof. Let $(a,b) \in \mathbf{Z}^2$. One can easily verify by hand or computer that if $p = 2, 3$, or 5, then

$$p^4 \mid A(a,b) \text{ and } p^6 \mid B(a,b)$$

if and only if $a \equiv b \equiv 0 \pmod{p}$. If $e > 1$ is a possible minimality defect (recall this means that e is the largest positive integer such that $e^{12} \mid$

$\gcd(A(a,b)^3, B(a,b)^2))$, then e is divisible by at least one of 2, 3, or 5 and so by the previous observation (a,b) is not groomed. Thus $\delta_e = 0$. Since $\sum_{e|m} \delta_e = 1$, we have $\delta_e = 1$. □

Corollary 4.3.10. *We have*

$$c = c(G_\ell(1;1,0)) = \frac{\mathrm{area}(R(1))}{\zeta(2)}.$$

Proof. Plug Lemma 4.3.9 and (3.3.16). □

Lemma 4.3.11. *We have $\delta'_e = 0$ for all divisors e of $m'/5^{25}$.*

Proof. A similar calculation as in Lemma 4.3.9 shows that if $p = 2, 3$, then

$$p^4 \mid A'(a,b) \text{ and } p^6 \mid B'(a,b)$$

if and only if $a \equiv b \equiv 0 \pmod{p}$, so the same conclusion holds. □

By Lemma 4.3.11, it only remains to compute δ'_e for $e \mid 5^{25}$.

Lemma 4.3.12. *We have $\delta'_e = 0$ for all $e > 5$, $\delta'_1 = 29/30$, and $\delta'_5 = 1/30$, so that*

$$\sum_{e|5^{25}} \delta'_e e^2 = \frac{29}{30} + \frac{1}{30} \cdot 25 = \frac{9}{5}.$$

Proof. We first show that $\delta'_e = 0$ for $e > 5$. Suppose $e > 5$, so that $e = 5^k$ for $1 \le k \le 25$. Let $(a,b) \in \mathbf{Z}^2$ have minimality defect e, so $e^{12} \mid \gcd(A'(a,b)^3, B'(a,b)^2)$; then $e^{12} \mid A'(a,b)^3$, whence $e^4 \mid A'(a,b)$. Note that e is divisible by 5^2.

Suppose further that $\gcd(a,b) = 1$. We will show that there are no solutions to the congruence

$$A'(a,b) \equiv 0 \pmod{5^6}, \tag{4.3.13}$$

implying that it is impossible for $e^4 \mid A'(a,b)$ unless $\gcd(a,b) \neq 1$, i.e., unless (a,b) is not groomed.

Since $\gcd(a,b) = 1$, either a or b is coprime to 5. By the symmetry of the coefficients of $A'(a,b)$, it suffices to assume b is coprime to 5, and hence invertible modulo 5^6. Multiplying (4.3.13) by $(1/b)^6$, we are left with the congruence

$$f'(t) \equiv 0 \pmod{5^6},$$

to which there are no solutions. As we sketched above, this is enough to conclude that $\delta'_e = 0$ for $e > 5$. It remains to calculate δ'_5, which we can do working modulo 25.

Suppose

$$A'(a,b) \equiv 0 \pmod{5^4} \quad \text{and} \quad B'(a,b) \equiv 0 \pmod{5^6}.$$

If b is invertible modulo 25, then we are left to consider the congruences

$$f'(t) \equiv 0 \pmod{5^4} \quad \text{and} \quad g'(t) \equiv 0 \pmod{5^6}.$$

which happens if and only if $t \equiv 18 \pmod{25}$. Similarly if a is invertible, then we find $t \equiv 7 \pmod{25}$. We also note that 18 and 7 are inverses modulo 25, reflecting the fact that A' and B' are each reciprocal polynomials. This accounts for $1/30$ of the possible ratios $(a : b)$ among groomed (a, b) modulo 25. (Alternatively, working over $\mathbf{P}^1(\mathbf{Z}/25)$, we find that of the 30 rational points, only $[18 : 1] = [1 : 7]$ solve the above congruences.)

Thus, $\delta'_5 = 1/30$, and $\delta'_1 = 1 - 1/30 = 29/30$, and the correction factor of $9/5$ follows. □

Corollary 4.3.14. *The constant c' is given by*

$$c' = \frac{9 \operatorname{area}(R(1))}{5\zeta(2)}.$$

Proof. This follows immediately from Lemmas 4.3.11 and 4.3.12, as in Corollary 4.3.10. □

We finally arrive at the exact value of P_5.

Corollary 4.3.15. *We have $P_5 = 25/34 \approx 73.5\%$.*

Proof. Combining Corollaries 4.3.10 and 4.3.14, together with Lemmas 4.3.6 and 4.3.12, we have

$$\frac{c'}{c} = \frac{\operatorname{area}(R'(1)) \sum_{e|m'} \delta'_e e^2}{\operatorname{area}(R(1))} = \frac{1}{5} \cdot \frac{9}{5} = \frac{9}{25}.$$

By (4.2.5), we have

$$P_5 = \frac{c}{c + c'} = \frac{1}{1 + c'/c} = \frac{1}{1 + 9/25} = \frac{25}{34}.$$ □

Remark 4.3.16. We perform a count of 5-full elliptic curves $E \in \mathscr{E}_{5?} \cap \mathscr{E}_{\leq H}$ in Magma of height $H \leq 10^{36}$, giving 196772 with a global subgroup of order 5 and 70784 with only a local, but not global, subgroup of order 5. These 70784 further decompose as 37944 with $e = 1$ and 32840 with $e = 5$. These proportions are in line with the ones predicted above and altogether give a ratio of

$$196772/(196772 + 70784) \approx 73.5\%,$$

which agrees nicely with our calculations above.

4.4. The Case $\ell = 7$. Repeating the steps in the previous section, we are more brief. The universal models for those curves have Weierstrass data:

$$\begin{aligned}
f(t) &= -27t^8 + 324t^7 - 1134t^6 + 1512t^5 - 945t^4 + 378t^2 - 108t - 27 \\
g(t) &= 54t^{12} - 972t^{11} + 6318t^{10} - 19116t^9 + 30780t^8 - 26244t^7 + 14742t^6 \\
&\quad - 11988t^5 + 9396t^4 - 2484t^3 - 810t^2 + 324t + 54 \\
f'(t) &= -27t^8 - 6156t^7 - 1134t^6 + 46872t^5 - 91665t^4 + 90720t^3 - 44982t^2 \\
&\quad + 6372t - 27 \\
g'(t) &= 54t^{12} - 28188t^{11} - 483570t^{10} + 2049300t^9 - 3833892t^8 + 7104348t^7 \\
&\quad - 13674906t^6 + 17079660t^5 - 11775132t^4 + 4324860t^3 - 790074t^2 \\
&\quad + 27540t + 54.
\end{aligned}$$

As above, we let A, B, A', B' denote the homogenizations of f, g, f', g'.

The j-invariant $j(t)$ of $E(t)$ is given explicitly by

$$j(t) = \frac{(t^2 - t + 1)^3(t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1)^3}{t^7(t-1)^7(t^3 - 8t^2 + 5t + 1)}$$

and so has simple poles at the roots of the polynomial $h(t) := t^3 - 8t^2 + 5t + 1$, and poles of order 7 at $0, 1, \infty$. Similarly, the j-invariant $j'(t)$ of $E'(t)$ has simple poles at 0, 1, ∞ and poles of order 7 at the roots of $h(t)$. The roots of $h(t)$ are real, generate the field $\mathbf{Q}(\zeta_7 + \zeta_7^{-1})$, and we label them according to the ordering $\rho_1 < \rho_2 < \rho_3$. Under the linear fractional transformation

$$\psi(t) = \frac{(\rho_2 - \rho_1)t + (\rho_1 - \rho_2)\rho_3}{(\rho_2 - \rho_3)t + (\rho_1\rho_3 - \rho_1\rho_2)},$$

we have $j(\psi(t)) = j'(t)$. We now proceed exactly as above.

Lemma 4.4.1. *With $R(1), R'(1)$ as defined in (4.2.8), we have*

$$\frac{\operatorname{area}(R'(1))}{\operatorname{area}(R(1))} = \frac{1}{\sqrt{7}}. \tag{4.4.2}$$

Proof. The change of variables $(a, b) \mapsto J(a, b)$ defined by matrix multiplication (on columns)

$$J := \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} \begin{pmatrix} \rho_2 - \rho_1 & \rho_1\rho_3 - \rho_2\rho_3 \\ \rho_2 - \rho_3 & \rho_1\rho_3 - \rho_1\rho_2 \end{pmatrix},$$

and $u = 7^{-3/4}$ maps $R(1)$ bijectively onto $R'(1)$ by checking that

$$A(J(a, b)) = A'(a, b) \text{ and } B(J(a, b)) = B'(a, b).$$

Then

$$|\det(J)| = |u^2(\rho_2 - \rho_3)(\rho_1^2 - \rho_1\rho_2 - \rho_1\rho_3 + \rho_3\rho_2)| = \sqrt{7},$$

which proves the lemma. □

Just like in the case $\ell = 5$ we must compute the local correction factors. We compute $m = -2^{32}3^{72}7$ and $m' = -2^{32}3^{72}7^{49}$ and check that $d(G) = 12$ (so that we sum $\delta_e e^1$ and $\delta'_e e^1$ over the divisors of m and m', respectively).

Lemma 4.4.3. *We have $\delta_e = \delta'_e = 0$ when e is divisible by a power of 2, and $\delta_7 = 0$.*

Proof. Similar to our work in the $\ell = 5$ case, one checks that

$$2^4 \mid A(a,b) \quad \text{and} \quad 2^6 \mid B(a,b)$$

if and only if $a \equiv b \equiv 0 \pmod 2$ and similarly for $A'(a,b)$ and $B'(a,b)$. An analogous calculation gives us the same result for the polynomials $A(a,b)$ and $B(a,b)$ when $p = 7$.

Thus, none of the groomed pairs (a,b) contribute to the correction factor in these cases and by the identical argument to the one in Lemma 4.3.9 we conclude that $\delta_e = \delta'_e = 0$ when e is a power of 2 and that $\delta_7 = 0$, as claimed. □

Lemma 4.4.4. *With all notation as above, we have*

$$\begin{aligned} \delta'_e &= 0 \text{ if } 7^2 \mid e. \\ \delta_e = \delta'_e &= 0 \text{ if } 3^2 \mid e \\ \delta_3 &= 1/4 \\ \delta_1 &= 3/4 \\ \delta'_3 &= 7/32 \\ \delta'_7 &= 3/32 \\ \delta'_{21} &= 1/32 \\ \delta'_1 &= 21/32. \end{aligned}$$

Proof. The reasoning is identical to that in Lemma 4.3.12. Suppose $3^2 \mid e$. Let $(a,b) \in \mathbf{Z}^2$ have minimality defect e, so $e^{12} \mid \gcd(A(a,b)^3, B(a,b)^2)$; then $e^{12} \mid A(a,b)^3$, whence $e^4 \mid A(a,b)$. Since e is divisible by 3^2, we have that $A(a,b) \equiv 0 \pmod{3^8}$.

If, in addition, $\gcd(a,b) = 1$ we can show that there are no solutions to the congruence

$$A(a,b) \equiv 0 \pmod{3^5}, \tag{4.4.5}$$

implying that it is impossible for $e^4 \mid A(a,b)$ unless $\gcd(a,b) \neq 1$, *i.e.* unless (a,b) is not groomed.

Since $\gcd(a,b) = 1$, either a or b is coprime to 3. Moreover, since the coefficients of $A(a,b)$ are not symmetric, we must consider both cases. If b is coprime to 3, then it is invertible modulo 3^5 and so we led to the congruence

$$f(t) \equiv 0 \pmod{3^5},$$

which has no solutions. Similarly, we can invert a to arrive at the congruence

$$t^8 f(1/t) \equiv 0 \pmod{3^5},$$

which also has no solutions. We can repeat this same argument for the polynomial $A'(a,b)$ and again for the polynomial $A'(a,b)$ when e is divisible by 7^2. In all cases we conclude that there are no groomed pairs (a,b) giving rise to divisibility by e^{12} in these cases. This leaves only a handful of cases left to work out: δ_3, δ_3', δ_7', and δ_{21}'. These will, in turn, give us δ_1 and δ_1'.

For δ_3 and δ_3' we work in $\mathbf{P}^1(\mathbf{Z}/3)$ and find

$$A(a,b) \equiv 0 \pmod{3^4} \text{ and } B(a,b) \equiv 0 \pmod{3^6}$$

if and only if

$$[a:b] \equiv [2:1] \equiv [1:2] \pmod{3} \tag{4.4.6}$$

This accounts for 1 of the 4 points of $\mathbf{P}^1(\mathbf{Z}/3)$, hence $\delta_3 = 1/4$. For δ_3', we find the exact conditions as (4.4.6).

Turning to δ_7' we find

$$A'(a,b) \equiv 0 \pmod{7^4} \text{ and } B'(a,b) \equiv 0 \pmod{7^6}$$

if and only if

$$[a:b] \equiv [5:1] \equiv [1:3] \pmod{7}. \tag{4.4.7}$$

This accounts for 1 of the 8 points of $\mathbf{P}^1(\mathbf{Z}/7)$.

For δ_{21}' we use the CRT combined with the proportions at 3 and 7 above. We finally arrive at

$$\begin{aligned} \delta_3' &= \frac{1}{4} \cdot \frac{7}{8} = \frac{7}{32} \\ \delta_7' &= \frac{3}{4} \cdot \frac{1}{8} = \frac{3}{32} \\ \delta_{21}' &= \frac{1}{4} \cdot \frac{1}{8} = \frac{1}{32}. \\ \delta_1' &= 1 - \delta_3' - \delta_7' - \delta_{21}' = \frac{21}{32}. \end{aligned}$$

□

Corollary 4.4.8. *We have*

$$P_7 = 4/(4+\sqrt{7}) \approx 60.2\%$$

Proof. By (4.2.5) and Lemmas 4.4.1, 4.4.3, and 4.4.4, we have

$$P_7 = \frac{c}{c+c'} = \frac{1}{1+c'/c},$$

with

$$\frac{c'}{c} = \frac{1}{\sqrt{7}} \cdot \frac{(21/32) + (7/32)\cdot 3 + (3/32)\cdot 7 + (1/32)\cdot 21}{(3/4) + (1/4)\cdot 3} = \frac{\sqrt{7}}{4},$$

from which the exact value of P_7 follows. □

Remark 4.4.9. Similar to 4.3.16, we perform a count of elliptic curves in Magma of height $H \leq 10^{72}$. We get 1291676 with a global subgroup of order 7 (where 645918 correspond to $e = 1$ and 645758 to $e = 3$). We also get 854432 that locally have a subgroup of order 7, but not globally. These 854432 break down as: 213522 with $e = 1$; 213704 with $e = 3$; 213714 with $e = 7$; and 213492 with $e = 21$. All of these proportions agree nicely with the predictions above, and give a ratio of

$$\frac{1291676}{1291676 + 854432} \approx 60.2\%,$$

which is very good corroborating evidence for Corollary 4.4.8.

5. The probabilities P_3 and P_4

In this section, we compute the values of P_3 and P_4 using similar methods as in the previous section, but without appealing to the general result (in particular, there are non-fine moduli spaces). In the case $m = 3$ we can evaluate P_3 without computing explicit growth constants thanks to a symmetry argument, while for $m = 4$ we express P_4 as a ratio of growth constants given explicitly by an integral.

5.1. Universal models. Here we parametrize curves that locally have a subgroup of order m for $m \in \{3, 4\}$, working in a bit more generality. Let F be a global field with $\operatorname{char} F \neq 2, 3$ and let $E\colon y^2 = f(x) = x^3 + Ax + B$ be an elliptic curve over F. For $d \in F^\times$, let $E_d\colon dy^2 = f(x)$ denote the quadratic twist by d.

Lemma 5.1.1. *Suppose that E locally has a subgroup of order 3, i.e., $3 \mid \#E(\mathbf{F}_\mathfrak{p})$ for a set of primes $\mathfrak{p}$ of F of density 1. Then the following statements hold.*

(a) *Either $E(F)[3] \neq \{\infty\}$ or $E_{-3}(F)[3] \neq \{\infty\}$.*
(b) *There exist $a, b \in F$ and $u \in \{1, -3\}$ such that E is defined by the equation*

$$y^2 = x^3 + u^2(6ab + 27a^4)x + u^3(b^2 - 27a^6).$$

Proof. Let $E \in \mathscr{E}_{3?}$ be given by $y^2 = x^3 + Ax + B$. By Lemma 2.3.5, either $E(F)[3] \neq \{\infty\}$ or E admits a 3-isogeny over F to a curve E' with $E'(F)[3] \neq \{\infty\}$. In either case, E has a rational 3-isogeny and the x-coordinate of a generator of the kernel must be defined over $\mathbf{Q}$. Hence the 3-division polynomial of E has a root $a \in F$.

By Theorem 2.3.14, the semisimplification of the mod 3 Galois representation attached to E has $\overline{\rho}^{\mathrm{ss}}_{E,3} \simeq \mathbf{1} \oplus \epsilon_3$, where ϵ_3 is the mod 3 cyclotomic character. If E has a 3-torsion point then

$$a^3 + Aa + B \in F^{\times 2}$$

so we interpret $F(\mathbf{1}) = F(\sqrt{a^3+Aa+B})$. Since $F(\epsilon_3) = F(\sqrt{-3})$, it follows that

$$F(\epsilon_3) = F(\sqrt{-3(a^3+Aa+B)}).$$

Thus, either E has a rational point of order 3 or its quadratic twist by -3 does, proving (a).

Part (b) is by a routine, universal computation (see e.g. García-Selfa–Tornero [15, §2] for a derivation). □

We now turn to $m = 4$. To set things up, suppose that E has a nontrivial 2-torsion point $T \in E(F)$. Writing $T = (-b, 0)$, we have a model

$$E\colon y^2 = x^3 + Ax + b^3 + Ab. \tag{5.1.2}$$

Lemma 5.1.3. *Let R be a 2-division point of T on E, i.e., $2R = T$. Then the following are equivalent:*

(i) *$x(R) \in F$;*
(ii) *$3b^2 + A \in F^{\times 2}$; and*
(iii) *E admits an F-rational cyclic 4-isogeny whose kernel contains T.*

Proof. The 2-division points of T form a torsor under $E[2]$ and there are two x-coordinates. Computing with the group law on a universal curve, the minimal polynomial of the x-coordinates is exactly

$$x(R)^2 + 2bx(R) - (A + 2b^2).$$

Thus, $x(R) \in F$ if and only if the discriminant $12b^2 + 4A$ is a non-zero square in F, showing (i) $\Leftrightarrow$ (ii).

For (i) $\Rightarrow$ (iii), if there exists R with $x(R) \in F$, then the subgroup $\langle R \rangle = \{0, R, T, 3R\}$ is stable under $\mathrm{Gal}(\overline{F}/F)$ since

$$3R = -R = (x(R), -y(R)).$$

For (iii) $\Rightarrow$ (i), if $\langle R \rangle$ is Galois stable, then for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$ we have $\sigma(R) = \pm R$ so $\sigma(x(R)) = x(R)$, whence $x(R) \in F$. □

Proposition 5.1.4. *The elliptic curve E locally has a subgroup of order 4 if and only if at least one of the following statements hold:*

(i) *$E(F)[2] \simeq (\mathbf{Z}/2)^2$, or*
(ii) *E has a cyclic 4-isogeny defined over F.*

Moreover, in case (ii)*, there exist $a, b \in F$ such that E is defined by*

$$y^2 = x^3 + (a^2 - 3b^2)x + a^2b - 2b^3$$

and the following statements hold:

- *$E(F)[2] \simeq (\mathbf{Z}/2)^2$ if and only if $9b^2 - 4a^2 \in F^{\times 2}$, and*
- *$E(F)[4] \not\subseteq E(F)[2]$ if and only if $2a - 3b \in F^{\times 2}$ or $-2a - 3b \in F^{\times 2}$.*

Proof. An elliptic curve E/F admits a rational cyclic 4-isogeny if and only if it has a Galois-stable cyclic subgroup of order 4; by stability, E has a rational point of order 2 contained in the cyclic group. Then the 2-adic representation of E lies in the group

$$\begin{pmatrix} 1+2\mathbf{Z}_2 & \mathbf{Z}_2 \\ 4\mathbf{Z}_2 & 1+2\mathbf{Z}_2 \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod 4.$$

Clearly, $\det(1-g) \equiv 0 \pmod 4$ for all elements of this group and so E has a local subgroup of order 4. Conversely, if $\det(g-1) \equiv 0 \pmod 4$ for all $g \in \operatorname{im} \rho_{E,2}$, but E does not have full rational 2-torsion, then it will have one point of order 2 defined over F. Then any non-trivial $g \in \operatorname{im} \rho_2$ reduces modulo 2 to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and so can be written in the form

$$\begin{pmatrix} 1+2\alpha & \beta \\ 2\gamma & 1+2\delta \end{pmatrix}, \text{ or } \begin{pmatrix} 1+2\alpha' & 2\beta' \\ 2\gamma' & 1+2\delta' \end{pmatrix},$$

respectively.

In the first case, $\det(1-g) \equiv 0 \pmod 4$ implies $2 \mid \beta\gamma$. But then $2 \mid \gamma$ (or else $E(F)[2] = \mathbf{Z}/2 \times \mathbf{Z}/2$) and so the mod 4 representation on these elements has the shape $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$. If g is of the second form, then multiply by a matrix h of the first form and compute

$$\det(1-gh) \equiv 2(\gamma+\gamma')\beta \pmod 4.$$

Since $2 \mid \gamma$, we must have $2 \mid \beta\gamma'$. And similar to the first case we conclude that $2 \mid \gamma'$. Thus the lower-triangular entry of any element of $\operatorname{im} \rho_{E,2}$ is divisible by 4 and so E admits a rational cyclic 4-isogeny.

Now suppose we are in Case (ii). In light of Lemma 5.1.3, let $a \in F$ be such that $a^2 = 3b^2 + A$, so that

$$E: \ y^2 = x^3 + (a^2 - 3b^2)x + a^2b - 2b^3.$$

Fix square-roots $\sqrt{\pm 2a - 3b} \in F^{\mathrm{al}}$. Then E visibly has two F-rational cyclic 4-isogenies with kernels

$$\langle (a-b, a\sqrt{2a-3b}) \rangle, \text{ and } \langle (-a-b, a\sqrt{-2a-3b}) \rangle,$$

respectively. Doubling either generator results in the marked 2-torsion point T; the other 2-torsion points are then

$$(b/2 \pm \sqrt{9b^2 - 4a^2}/2, 0).$$

The splitting field of the preimages of T under duplication is then a bi-quadratic extension of F with intermediate extensions

$$F(\sqrt{2a-3b}), \ F(\sqrt{-2a-3b}), \ F(\sqrt{9b^2-4a^2}).$$

These quadratic extensions are nontrivial exactly under the conditions stated in Proposition 5.1.4. □

5.2. The Probability P_3. By Lemma 5.1.1, all curves in $\mathscr{E}_{3?}$ either have global point of order 3 or are a quadratic twist by -3 of one that does. These are modeled by the Weierstrass equations

$$y^2 = x^3 + u^2(6ab + 27a^4)x + u^3(b^2 - 27a^6), \tag{5.2.1}$$

where $u = 1$ means the curve has a 3-torsion point and $u = -3$ is its quadratic twist.

Denote by $R_u(H)$ the region (3.3.6) attached to the elliptic curve (5.2.1). Applying the Principle of Lipschitz we see that

$$\operatorname{area} R_u(H) = \operatorname{area} R_u(1)H^{1/3} + O(H^{1/4}). \tag{5.2.2}$$

In particular, observe that

$$\operatorname{area} R_1(1) = 9 \operatorname{area} R_{-3}(1). \tag{5.2.3}$$

Remark 5.2.4. As long as $\#G \geq 5$, we have shown that Lipschitz asymptotics give a growth term of $2/d(G)$ and error of $1/d(G)$. The degrees of the polynomials $A(a, b)$ and $B(a, b)$ are not large enough to ensure these asymptotics when $\#G = 3$ or 4, so we estimate the order of growth of the error term "by hand" (using the results previously obtained by Harron-Snowden).

We are now ready to compute P_3.

Proposition 5.2.5. *We have* $P_3 = 1/2$.

Proof. Appealing to the notation of (4.2.5), we write $c = c(G_3(1; 1, 0))$ and $c' = c(G_3(1; 0, 0))$ and find

$$cH^{1/3} + O(H^{1/4}) \text{ and } c'H^{1/3} + O(H^{1/4})$$

for the number of minimal elliptic curves of height at most H with a global 3-torsion subgroup and the number of quadratic twists, respectively; note the exponents come from the Lipschitz estimate of (5.2.2). It remains to compute c and c' exactly.

For every prime $q \neq 3$, we have

$$q^4 \mid (6ab + 27a^4) \text{ and } q^6 \mid (b^2 - 27a^6)$$

if and only if

$$q^4 \mid 9(6ab + 27a^4) \text{ and } q^6 \mid -27(b^2 - 27a^6).$$

Therefore, sieving out non-minimal equations away from $q = 3$ has no effect on the ratio of the growth constants.

The pairs (a, b) such that

$$3^4 \mid (6ab + 27a^4) \text{ and } 3^6 \mid (b^2 - 27a^6)$$

have $a \equiv 0 \pmod 3$ and $b \equiv 0 \pmod{27}$, which accounts for a proportion of $1/81$ of the pairs.

For the twists, observe that

$$9(6ab + 27a^4) \text{ and } -27(b^2 - 27a^6)$$

are integral if and only if $a, b \in (1/3)\mathbf{Z}$. Among those pairs, similar reasoning shows that $1/81$ yield non-minimal equations.

Taking $a, b \in (1/3)\mathbf{Z}$ scales the area of $R_{-3}(H)$ by 9, whence, by (5.2.3) the number of integral equations parameterizing 3-torsion and local 3-torsion is the same. Sieving out $1/81$ of the pairs from each count does not affect the ratio and so the proportions are equal. □

Remark 5.2.6. We confirm Proposition 5.2.5 experimentally: in a naive way, we compute

$$\frac{\#\{E \in \mathscr{E}_{\leq 10^{12}} : 3 \mid \#E(\mathbf{Q})_{\mathrm{tor}}\}}{\#(\mathscr{E}_{3?} \cap \mathscr{E}_{\leq 10^{12}})} = \frac{3808}{7578} \approx 0.503.$$

5.3. The Probability P_4. The strategy here is similar, but we will need to do more computation to get the growth constants exactly. (The difference between this case and P_3 is that the Weierstrass models of the curves in $\mathscr{E}_4$ are not simply quadratic twists of each other and, moreover, to argue how the shapes of the regions are transformed by cyclic isogenies is at least as difficult as computing the areas by calculus.)

First, we reduce our work by observing from Harron–Snowden [17, Theorem 1.1] that the number of curves up to height H with a rational $\mathbf{Z}/4$-torsion subgroup is $\asymp H^{1/4}$ and curves with full 2-torsion are $\asymp H^{1/3}$. This shows that as $H \to \infty$, curves with full 2-torsion dominate curves with a 4-torsion point in $\mathscr{E}_{4?}$ and so the latter will not contribute to the probability P_4. For completeness, however, we record the quantities $d(\mathbf{Z}/4)$ and $e(\mathbf{Z}/6)$ in the following Proposition and fill in the entry for $\mathbf{Z}/4$ in Table 1.3.8. Because we do not need the growth constant, we are content to sketch a proof.

Proposition 5.3.1. *The number $N_{\mathbf{Z}/4}(H)$ of elliptic curves over $\mathbf{Q}$ of height $\leq H$ with a rational point of order 4 is given by*

$$N_{\mathbf{Z}/4}(H) = cH^{1/4} + O(H^{1/6}),$$

for an explicitly computable constant c.

Proof. By [15, Σ_4, p. 93] elliptic curves over $\mathbf{Q}$ with a rational point of order 4 are parameterized by

$$y^2 = x^3 - 27(16t^2 + 16t + 1)x - 54(64t^3 - 120t^2 - 24t - 1).$$

Homogenizing and clearing denominators across the Weierstrass equation, shows that the number of integral equations is roughly given by the number of integral points in the compact region of $\mathbf{R}^2$ defined by

$$R(H) := \{(a, b) : 4|A(a, b)|^3 \leq H \text{ and } 27|B(a, b)|^2 \leq H\} \tag{5.3.2}$$

where

$$A(a,b) := 27(16a^2 + 16ab^2 + b^4)$$
$$B(a,b) := 54(64a^3 - 120a^2b^2 - 24ab^4 - b^6). \tag{5.3.3}$$

(Here, "roughly" means that $A(a,b)$ and $B(a,b)$ are integral if and only if $(a,b) \in \left(\frac{1}{6}\mathbf{Z}\right) \times \mathbf{Z}$; this can be deduced from congruences. We will not pursue a finer estimate than this because we do not seek an explicit growth constant.)

The compactness of $R(H)$ allows for a Lipschitz analysis. A homogeneity argument with the Weierstrass coefficients (scale a by $H^{1/6}a$ and b by $H^{1/12}b$) shows immediately that $\mathrm{area}(R(H)) = \mathrm{area}(R(1))H^{1/4}$ and $O(\mathrm{len}(\mathrm{bd}(R(H)))) = O(H^{1/6})$. The boundary of $R(H)$ is rectifiable (given by polynomials) and so the area of $R(1)$ is calculable. The constant c is $\mathrm{area}(R(1))$ scaled by $1/r(\mathbf{Z}/4)$ and a sieve factor, both of which are finite calculations. □

For $G = \mathbf{Z}/2 \times \mathbf{Z}/2$, our next goal is to show that the number of isomorphism classes $N_G(H)$ of elliptic curves with global torsion subgroup G of height $\leq H$ is given by

$$N_G(H) = c(G)H^{1/d(G)} + O(H^{1/e(G)}). \tag{5.3.4}$$

Thus, P_4 will be given as a weighted ratio of the constant $c(\mathbf{Z}/2 \times \mathbf{Z}/2)$ and the corresponding constant for curves admitting a cyclic 4-isogeny. We first work out the details for the group $\mathbf{Z}/2 \times \mathbf{Z}/2$ in the following Proposition, which contributes to the data in Table 1.3.8. After this, we count curves admitting a cyclic 4-isogeny in Proposition 5.3.10. From there, it is then a simple matter to fit the pieces together to obtain an exact expression for P_4; this is Corollary 5.3.12.

Proposition 5.3.5. *For $G = \mathbf{Z}/2 \times \mathbf{Z}/2$, we have*

$$c(G) = \frac{121\pi\sqrt{3}\sqrt[3]{2}}{360}$$
$$r(G) = 6$$
$$1/d(G) = 1/3$$
$$1/e(G) = 1/6.$$

Proof. We start with a two-variable model parameterizing elliptic curves with full 2-torsion:

$$y^2 = x^3 - \frac{(a^2 - ab + b^2)}{3}x - \frac{(a+b)(2a-b)(a-2b)}{27}, \tag{5.3.6}$$

identifying the polynomials $A(a,b)$ and $B(a,b)$ as

$$A(a,b) = -(a^2 - ab + b^2)/3$$
$$B(a,b) = -(a+b)(2a-b)(a-2b)/27.$$

It is routine to check that for all $H > 0$ we have the containment

$$\{(a,b) : |4A(a,b)|^3 \leq H\} \subseteq \{(a,b) : |27B(a,b)|^2 \leq H\}.$$

(Briefly, rotate by $\pi/4$ so that it amounts to checking

$$4\left|\frac{a^2}{2} + \frac{b^2}{6}\right|^3 \leq H \Longrightarrow 27\left(\frac{ba^2}{3\sqrt{2}} - \frac{b^3}{27\sqrt{2}}\right)^2 \leq H. \tag{5.3.7}$$

By symmetry and scaling, it suffices to show (5.3.7) holds for $a, b \geq 0$ and $H = 1$, which is easily verified.)

We therefore put

$$R_4(H) = \{(a,b) \in \mathbf{R} \times \mathbf{R} : 4|A(a,b)|^3 \leq H\}. \tag{5.3.8}$$

The constants $c(\mathbf{Z}/2 \times \mathbf{Z}/2)$, $d(\mathbf{Z}/2 \times \mathbf{Z}/2)$, $e(\mathbf{Z}/2 \times \mathbf{Z}/2)$ of the Proposition will follow from asymptotic analysis of the elliptical region defined by (5.3.8).

By the homogeneity of $A(a,b)$ of degree 2, it follows from direct calculation that

$$\text{area}(R_4(H)) = \text{area}(R_4(1))H^{1/3}.$$

By the Principle of Lipschitz applied to the homogeneously expanding compact region $R_4(H)$, we get that the number of integral points in $R_4(H)$ is asymptotically

$$\text{area}(R_4(H)) + O(\text{len}(\text{bd}(R_4(H)))).$$

Therefore, $1/d(\mathbf{Z}/2 \times \mathbf{Z}/2) = 1/3$. The fact that $R_4(H)$ defines an ellipse centered at the origin with boundary equation

$$x^2 - xy + y^2 = 3\left(\frac{H}{4}\right)^{1/3},$$

immediately shows that

$$\text{len}(\text{bd}(R_4(H))) = O(H^{1/6}).$$

It remains to remove singular and sieve out non-minimal equations. The conclusion from the steps will be that $1/e(\mathbf{Z}/2 \times \mathbf{Z}/2) = 1/6$ and an explicit expression for $c(\mathbf{Z}/2 \times \mathbf{Z}/2)$.

The singular equations of the form (5.3.6) have discriminant 0:

$$4A(a,b)^3 + 27B(a,b)^2 = -a^2b^2(a-b)^2 = 0,$$

and by algebraic substitution we see that the number of singular equations up to height H is $O(H^{1/6})$. Therefore, the singular equations can be absorbed into the error term and we can now conclude that $1/e(\mathbf{Z}/2\times\mathbf{Z}/2) = 1/6$.

The points of $R_4(H)$ give a 6-fold overcount of models of the form (5.3.6) because the points

$$\{(a,b),(b,a),(-a,b-a),(b-a,-a),(a-b,-b),(-b,a-b)\}$$

each give rise to the identical Weierstrass equation with height $\leq H$; this shows $r(G) = 6$, as claimed. We also note that if both $A(a,b)$ and $B(a,b)$ are integers, then both a and b are integers, which is routinely verified by congruences, occurs for $1/3$ of all integral pairs $(a,b) \in \mathbf{Z}\times\mathbf{Z}$. Therefore,

$$\frac{\operatorname{area} R_4(1)}{18} \tag{5.3.9}$$

is the growth constant for non-singular, integral equations of the form (5.3.6) of height $\leq H$. It remains to sieve non-minimal equations. We omit the routine computation, which is similar to the ones detailed in Section 4 above, and simply observe that

(a) If $p \neq 3$, then

$$p^4 \mid A(a,b) \text{ and } p^6 \mid B(a,b)$$

if and only if $a \equiv b \equiv 0 \pmod{p^2}$.

(b) If $p = 3$, then

$$3^4 \mid A(a,b) \text{ and } 3^6 \mid B(a,b)$$

if and only if $(a,b) \equiv (0,0)$ or $(9,18)$ or $(18,9) \pmod{27}$.

Thus, if $p \neq 3$ then $1/p^4$ of the equations are non-minimal at p. If $p = 3$, then $1/3^5$ equations are non-minimal. Putting together (5.3.9), this sieve, and the area of the ellipse $R_4(1)$, we see that

$$\frac{c(\mathbf{Z}/2\times\mathbf{Z}/2)}{r(\mathbf{Z}/2\times\mathbf{Z}/2)} = \frac{1}{18}\cdot\left(\frac{1-\frac{1}{3^5}}{1-\frac{1}{3^4}}\right)\frac{\pi\sqrt{3}\sqrt[3]{2}}{\zeta(4)} = \frac{121\pi\sqrt{3}\sqrt[3]{2}}{2160\zeta(4)} \approx 0.355,$$

which completes the proof. □

We now perform the analogous computation for curves admitting a cyclic 4-isogeny.

Proposition 5.3.10. *The number $N(H)$ of elliptic curves over $\mathbf{Q}$ of height $\leq H$ admitting a cyclic 4-isogeny is given by*

$$N(H) = cH^{1/d} + O(H^{1/e}),$$

where

$$\begin{aligned} c &= \frac{\operatorname{area} R_4'(1)}{2\zeta(4)} \approx 0.9574 \\ 1/d &= 1/3 \\ 1/e &= 1/6, \end{aligned}$$

with the exact value of c given in Lemma 5.3.11.

Proof. Appealing to Proposition 5.1.4 we define the region

$$R_4'(H) = \{(a,b) \in \mathbf{R} \times \mathbf{R} : 4|a^2 - 3b^2|^3 \leq H \text{ and } 27|a^2b - 2b^3|^2 \leq H\}$$

parameterizing curves of height $\leq H$ that admit a cyclic 4-isogeny. We follow the same approach as in Proposition 5.3.5 to compute $1/d$, and $1/e$. We separate the calculation of c into a separate lemma following this Proposition.

It follows from homogeneity of $A(a,b)$ and $B(a,b)$ that $\operatorname{area}(R_4'(H)) = \operatorname{area}(R_4'(1))H^{1/3}$ and by applying the Principle of Lipschitz we get $1/d = 1/3$. By inspection on the degrees of $A(a,b)$ and $B(a,b)$, and using the fact that A and B are polynomials (so rectifiable) we see that $\operatorname{len}\operatorname{bd}(R_4'(H)) = O(H^{1/6})$.

Next, we calculate the discriminant

$$4A(a,b)^3 + 27B(a,b)^2 = a^4(4a^2 - 9b^2)$$

and see that the number of singular equations is $O(H^{1/6})$. These singular equations can be absorbed into the Lipschitz error and we conclude that $1/e = 1/6$.

It remains to obtain c. The region $R_4'(1)$ has polynomial boundary and its area can be computed by calculus (see the statement of Lemma 5.3.11 immediately following this proof for an exact value of this area and numerical approximation). We compute that $r(G) = 2$.

It is straightforward to verify that for every prime p, we have $p^4 \mid (a^2 - 3b^2)$ and $p^6 \mid (a^2b - 2b^3)$ if and only if $a \equiv b \equiv 0 \pmod{p^2}$. Sieving, we scale by $\zeta(4)^{-1}$. Altogether, we arrive at the growth constant

$$c = \frac{1}{2} \cdot \frac{1}{\zeta(4)} \operatorname{area}(R_4'(1)) \approx 0.9574$$

as claimed. □

Lemma 5.3.11. *Let $u = 4^{-1/3}, v = 27^{-1/2}$, and define the polynomials $F_\pm \in \mathbf{R}[x]$ by*

$$F_\pm(x) = x^3 \pm ux - v.$$

Let $\alpha_\pm$ denote the unique positive root of $F_\pm$ and set $\beta_\pm = \sqrt{3\alpha_\pm^2 \pm u}$. Where it is defined, let $I(p,q)$ denote the integral

$$I(p,q) = \int_p^q \sqrt{\frac{2y^3+v}{y}}\,\mathrm{d}y.$$

Then we have

$$\begin{aligned}\operatorname{area}(R_4'(1)) &= 4I(\alpha_+,\alpha_-) + 2(\alpha_+\beta_+ - \alpha_-\beta_-) \\ &\quad + \frac{2u}{\sqrt{3}}\log\left(\frac{(\sqrt{3}\alpha_+ + \beta_+)(\sqrt{3}\alpha_- + \beta_-)}{u}\right) \\ &\approx 2.072.\end{aligned}$$

Proof. Straightforward calculation: for a bit more detail, see Pomerance–Schaefer [25, §2], where our area is $2i_4 \approx 2(1.036) \approx 2.072$. □

Corollary 5.3.12. *We have*

$$P_4 = \frac{121\operatorname{area}(R_4(1))}{121\operatorname{area}(R_4(1)) + 1080\operatorname{area}(R_4'(1))} \approx 0.270.$$

Proof. Because both growth rates are $O(H^{1/3})$, we can express P_4 as the following ratio

$$P_4 = \frac{c(\mathbf{Z}/2 \times \mathbf{Z}/2)}{c(\mathbf{Z}/2 \times \mathbf{Z}/2) + c}.$$

The exact value and its approximations follow immediately from Propositions 5.3.5 and 5.3.10. □

Remark 5.3.13. Pomerance–Schaefer [25] count elliptic curves with Galois-stable cyclic subgroups of order 4 and obtain a finer estimate than our Proposition 5.3.10, in the case where they count the number of curves with at least one pair of cyclic subgroups of order 4. In that case they show

$$N(H) = c_1 H^{1/3} + c_2 H^{1/6} + O(H^{0.105}),$$

where their c_1 is exactly our c in Proposition 5.3.10; they also compute the area of the same region that we do in Lemma 5.3.11.

Example 5.3.14. Returning to Example 2.2.16, we have shown that 100% of elliptic curves $E \in \mathscr{E}_{4?}$ are isogenous to an elliptic curve with full 2-torsion (and no further torsion structure); the isogeny class of such curves have isogeny graph which is a tree with three leaves attached to a central root, for example the isogeny class with LMFDB [21] label 350.b.

Remark 5.3.15. We now give some experimental confirmation of Corollary 5.3.12. Enumerating curves in a naive way, among the curves $E \in \mathscr{E}_{4?} \cap \mathscr{E}_{\leq 10^{13}}$ we count:

$E(\mathbf{Q})_{\mathrm{tor}}[2^\infty]$	count
$\mathbf{Z}/2$	20612
$\mathbf{Z}/2 \times \mathbf{Z}/2$	8126
$\mathbf{Z}/2 \times \mathbf{Z}/4$	8
$\mathbf{Z}/4$	1382
$\mathbf{Z}/8$	2

(It appears that the elliptic curve of smallest height with $\#E(\mathbf{Q})_{\mathrm{tor}}[2^\infty] \simeq \mathbf{Z}/2 \times \mathbf{Z}/8$ is the elliptic curve 210.e6 with height $\approx 10^{19.03}$.) The curves with a rational 4-torsion point are, according to the above, a lower-order term—but this is not so totally apparent in the range of our data! So we estimate the probability by

$$\begin{aligned} &\frac{\#\{E \in \mathscr{E}_{\leq 10^{13}} : \#E(\mathbf{Q})_{\mathrm{tor}}[2^\infty] \simeq \mathbf{Z}/2 \times \mathbf{Z}/2\}}{\#\{E \in \mathscr{E}_{4?} \cap \mathscr{E}_{\leq 10^{13}} : \#E(\mathbf{Q})_{\mathrm{tor}}[2^\infty] \leq \mathbf{Z}/2 \times \mathbf{Z}/2\}} \\ &\qquad = \frac{8126}{20612 + 8126} = \frac{8126}{28738} \approx 0.283 \end{aligned} \tag{5.3.16}$$

which matches Corollary 5.3.12 reasonably well.

Remark 5.3.17. Alternatively, one can order the elliptic curves by naive height

$$\mathrm{ht}'(E) := \max(|A^3|, |B^2|)$$

(without the scaling factors $4, 27$) and ask how the explicit probabilities are affected. This does not affect P_3, since the ratio of the areas of the regions $R_1(1)$ and $R_{-3}(1)$ is preserved. However, in the case of P_4, the area of the elliptical region is $2\sqrt{3}\pi$ and the area of the region $R_4'(1)$ is given explicitly by

$$\begin{aligned} 4 \cdot \Bigg(&\frac{(\alpha_+\beta_+ - \alpha_-\beta_-)}{2} + \frac{\log\left((\beta_+ + \sqrt{3}\alpha_+)(\beta_- + \sqrt{3}\alpha_-)\right)}{2\sqrt{3}} \\ &+ I(\alpha_+, \alpha_-)\Bigg) \approx 4.019, \end{aligned}$$

where $\alpha_\pm$ is the real root of $z^3 \pm z - 1$, $\beta_\pm = \sqrt{3\alpha_\pm^2 \pm 1}$, and

$$I(p, q) = \int_p^q \sqrt{\frac{2z^3 + 1}{z}} \mathrm{d}z.$$

No other adjustments to the growth constants are required. Thus, the effect of ordering by ht' versus ht gives $P_4 \approx 0.233$.

References

[1] E. Assaf, *Computing classical modular forms for arbitrary congruence subgroups*, 2021, accepted to Simons Symp.

[2] B. Baran, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130** (2010), no. 12, 2753–2772.

[3] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242.

[4] B. Boggess and S. Sankar, *Counting elliptic curves with a rational N-isogeny for small N*, preprint, 2020, `arXiv:2009.05223`.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (3–4), 1997, 235–265.

[6] P. Bruin and F. Najman, *Counting elliptic curves with prescribed level structures over number fields*, preprint, 2021, `arXiv:2008.05280`.

[7] G. Chiloyan and Á. Lozano-Robledo, *A classification of isogeny-torsion graphs of elliptic curves over* $\mathbf{Q}$, Trans. London Math. Soc. **8** (2021), no. 1, 1–34.

[8] P. Cho and K. Jeong, *Probabilistic behaviors of elliptic curves with torsion points*, preprint, 2020, `arXiv:2005.06862`.

[9] D. A. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, 2nd. ed., Grad. Texts in Math., vol. 185, Springer, New York, 2005.

[10] J. Cullinan and J. Voight, *Universal polynomials for m-full torsion groups*, 2020, [Online; available at http://math.dartmouth.edu/~jvoight/code/compute_universal.m].

[11] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183; Corrigendum, J. London Math. Soc. **39** (1964), 580.

[12] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 349, Springer, Berlin, 1973, 143–316.

[13] F. Diamond and J. Shurman, *A first course in modular forms*, Grad. Texts in Math., vol. 228, Springer-Verlag, New York, 2005.

[14] J. Ellenberg, M. Satriano, and D. Zureick-Brown, *Heights on stacks and a generalized Batyrev–Manin–Malle conjecture*, preprint, 2021, `arXiv:2106.11340v1`.

[15] I. García-Selfa and J. M. Tornero, *A complete Diophantine characterization of the rational torsion of an elliptic curve*, Acta Math. Sin. (Engl. Ser.) **28** (2012), no. 1, 83–96.

[16] R. Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), no. 5, 1167–1196.

[17] R. Harron and A. Snowden, *Counting elliptic curves with prescribed torsion*, J. Reine Angew. Math. **729** (2017), 151–170.

[18] M.N. Huxley, *Exponential sums and lattice points III*, Proc. London Math. Soc. **87** (2003), no. 3, 591–609.

[19] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Inv. Math. **62** (1981), 481–502.

[20] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Math. Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[21] The LMFDB Collaboration, The L-functions and Modular Forms Database, http://www.lmfdb.org, 2020, [Online; accessed 28 June 2020].

[22] I. Kra, *On lifting Kleinian groups to* $\mathrm{SL}(2,\mathbf{C})$, Differential geometry and complex analysis, Springer, Berlin, 1985, 181–193.

[23] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Etudes Sci. Publ. Math., no. 47, 1977, 33–186.

[24] M. Pizzo, C. Pomerance, and J. Voight, *Counting elliptic curves with an isogeny of degree three*, Proc. Amer. Math. Soc. Ser. B **7** (2020), 28–42.

[25] C. Pomerance and E. F. Schaefer, *Elliptic curves with Galois-stable cyclic subgroups of order 4*, Res. Number Theory **7** (2021), no. 2, Paper No. 35.

[26] A. Sebbar, *Classification of torsion-free genus zero congruence groups*, Proc. Amer. Math. Soc. **129** (2001), no. 9, 2517–2527.
[27] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Math., Friedr. Vieweg & Sohn, Braunschweig, 1997.
[28] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Res. Notes Math., vol. 7, A K Peters, Ltd., Wellesley, MA, 1998.
[29] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. of Japan, vol. 11, Kanô Memorial Lectures, 1, Princeton University Press, Princeton, NJ, 1994.
[30] A. V. Sutherland and D. Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra Number Theory **11** (2017), no. 5, 1199–1229.
[31] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.
[32] J. Voight and D. Zureick-Brown, *The canonical ring of a stacky curve*, to appear in Mem. Amer. Math. Soc.
[33] D. Zywina, *Possible indices for the Galois image of elliptic curves over* **Q**, preprint, 2015, `arXiv:1508.07663`.

Department of Mathematics, Bard College, Annandale-On-Hudson, NY 12504, USA
E-mail : `cullinan@bard.edu`
URL: `http://faculty.bard.edu/cullinan/`

Department of Mathematics, University of Minnesota, Minneapolis, MN 55455
E-mail : `kenn0699@umn.edu`

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
E-mail : `jvoight@gmail.com`
URL: `http://www.math.dartmouth.edu/~jvoight/`