ON A PROBABILISTIC LOCAL-GLOBAL PRINCIPLE FOR TORSION ON ELLIPTIC CURVES

JOHN CULLINAN, MEAGAN KENNEY, AND JOHN VOIGHT

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 is torsion free of genus zero.

CONTENTS

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 [10, Theorem 2]: if $m \mid \#E(\mathbf{F}_p)$ for a set of primes p of 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 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 $\mathscr{E}_{\leq H} := \{E \in \mathscr{E} : \operatorname{ht} E \leq H\}$ 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 [14] 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.*

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 $\mathbf{Q}$.

At the other extreme, 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 Lipshitz, counting points in a homogeneously expanding region, to count elliptic curves by height on these modular curves, giving a positive probability.

To count elliptic curves by height, we establish a general result of potential independent interest: we extend work of Harron–Snowden [9], 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

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

We consider $\Gamma_G \leq \mathrm{PSL}_2(\mathbf{Z})$ in the natural way, and let X_G the associated modular curve. 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 X_G has genus zero and no irregular cusps. Let*

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

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

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

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.

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 1.3.4: Asymptotic count of elliptic curves with designated torsion

Corollary 1.3.5. *For each T in Table 1.3.4, we have*

$$\#\{E \in \mathscr{E}_{\leq H} : E(\mathbf{Q})_{\mathrm{tor}} \simeq T\} = c(T)H^{1/d(T)} + O(H^{1/e(T)}). \tag{1.3.6}$$

By Table 1.3.4, the count of curves $E \in \mathscr{E}_{\leq H}$ such that $E(\mathbf{Q})_{\mathrm{tor}}$ contains a subgroup isomorphic to T has the same asymptotic.

Harron–Snowden [9, 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 1.3.4, and gave the power-saving asymptotic [9, Theorem 5.6] for $\#T \leq 3$. We follow their strategy 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 [17].)

Remark 1.3.7. Although this result suffices for our purposes, echoing Harron–Snowden [9, §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.

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. Moreover, carrying this out with explicit details allows us to compute P_5 and P_7 in section 4.

Theorem 1.3.8. *We have $P_5 = 125/164 \approx 76\%$ and $P_7 = 49\sqrt{7}/(49\sqrt{7} + 52) \approx 71\%$.*

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 1.3.9. *We have $P_3 = 1/2$.*

In other words, among elliptic curves with $3 \mid \#E(\mathbf{F}_p)$ for almost all p, the odds are fifty-fifty 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 1.3.10. *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 1.3.10 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 1.3.11. *There exists an effectively computable constant $c_4 \in \mathbf{R}_{>0}$ such that as $H \to \infty$,*

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

Moreover, we have $c_4 \approx 0.9572$ and $P_4 \approx 27.2\%$.

The exact value of c_4 is given in Proposition 5.3.9 and for P_4 in Proposition 5.3.11. For both $m = 3, 4$, these theorems match experimental data (Remarks 5.2.5, 5.3.14).

Remark 1.3.12. Alternatively, one can order the elliptic curves by defining

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

(without the scaling factors $4, 27$). We probability for $m = 3$ is again $1/2$ in this height; see Remark 5.3.16 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 [10]. 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 $m \ge 5$ 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.

1.5. **Acknowledgements.** The authors would like to thank Robert Harron and Siman Wong for helpful conversations, Robert Lemke Oliver for comments, and Carl Pomerance and Edward Schaefer for their feedback and corrections. Voight was supported by an NSF CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029).

2. Galois representations and divisibility

In this section, we characterize the image of Galois 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 [10, 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. The absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{al}} \,|\, K)$ acts continuously on the Tate module $T_\ell E := E[\ell^\infty](K^{\mathrm{al}}) \simeq \mathbf{Z}_\ell^2$ 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. *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 $1+\ell^0\mathbf{Z}_\ell := \mathbf{Z}_\ell^\times$.

Conversely, 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 $\mathbf{Z}/\ell^r \times \mathbf{Z}/\ell^s$.

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

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

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 may further suppose $r \geq s = n - r$.

Lemma 2.2.9. *The following statements hold.*

(a) *The group $G_\ell(n; r, s)$ is 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*

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

(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 $\#\operatorname{GL}_2(\mathbf{Z}/\ell^n) = \ell^{4(n-1)}\#\operatorname{GL}_2(\mathbf{Z}/\ell) = \ell^{4n-3}(\ell-1)(\ell^2-1)$, 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 $g \in \operatorname{SL}_2(\mathbf{Z})$ is torsion, then its characteristic polynomial matches that of a root of unity of order dividing 6, and if $g \neq 1$ then $\det(g-1) = 3, \pm 4$, a contradiction. □

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

Proposition 2.2.10. *Suppose in a clean basis for $T_\ell E$ that $\rho_{E,\ell}(\operatorname{Gal}_K) = G(n;r,n-r)$. Then the following statements hold.*

(a) *Any 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*

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

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 $\#C = \ell^k$. If $k \leq r$, then $E[\ell^k](K^{\mathrm{al}}) = E[\ell^k](K)$ and so the result holds. Suppose $r < k \leq s$. Then a generator for C is of the form $x_1P_{1,k} + x_2P_{2,k}$ with $(x_1 : x_2) \in \mathbf{P}^1(\mathbf{Z}/\ell^k)$. By hypothesis,

$$\overline{\rho}_{E,\ell^k}(\operatorname{Gal}_K) = \left\{ \begin{pmatrix} 1+\ell^r a & 0 \\ \ell^r c & 1 \end{pmatrix} : a, c \in \mathbf{Z}/\ell^{k-r} \right\}.$$

This group stabilizes $\infty \in \mathbf{P}^1(\mathbf{Z}/\ell^k)$ and acts transitively on its (affine) complement, so there are no other stable lines (eigenvectors) in its action on column vectors; thus we must have $C = \langle P_{2,k} \rangle$. Finally, if $k > s := n-r$, then $\ell^{k-s}C$ is Galois stable, so C is generated by $P := x_1P_{1,k} + x_2P_{2,k}$ with $(x_1 : x_2) \equiv (0 : 1) \pmod{\ell^s}$. Taking diagonal matrices in $\overline{\rho}_{E,\ell^k}(\operatorname{Gal}_K)$ then gives a contradiction.

Next, part (b). Lemma 2.2.2 and (a) imply $k \leq \max(r, n-r)$. Let P_1, P_2 be the given clean basis for $T_\ell E$. We claim we can reduce to the case where $\ker\varphi$ is generated by $P_{1,k}$ or $P_{2,k}$ (in coordinates). Indeed, let C be the largest cyclic subgroup of $E[\ell^\infty](K)$ containing $\ker\varphi$; then $\#C = r$ or $\#C = n-r$. Interchanging basis elements, we may suppose that $\#C = r$. Let Q_1 be a generator of C; then $\ker\varphi = \langle \ell^{r-k}Q_1 \rangle$. Lift to a clean basis of $T_\ell E$; by Lemma 2.2.2, in this (conjugate) basis we have $\rho_{E,\ell}(\operatorname{Gal}_K) \leq G(n;r,n-r)$ so by hypothesis and counting equality again holds.

So we may suppose $\ker\varphi$ is generated by $P_{1,k}$ or $P_{2,k}$, with respectively $k \leq r$ or $k \leq n-r$, and $E' \simeq E/\ker\varphi$. Then a basis for $T_\ell E'$ (in $V_\ell E$) is given by $\ell^{-k}P_1, P_2$ or $P_1, \ell^{-k}P_2$,

respectively. In the first case, we have

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

Applying (2.2.8) converts $G(n;r,n-r+k)$ to $G(n;n-r,r-k)$. In the second case, we find $\rho_{E',\ell}(\mathrm{Gal}_K) = G(n;r,n-r-k)$. 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 2.2.13. 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) $G(n;r,s)$.

Lemma 2.2.14. *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 $\rho_{E,\ell}(\mathrm{Gal}_K) \leq G(n;r,s)$, then $P_{1,r}, P_{2,s}$ generate a subgroup of $E[\ell^\infty](K)$ isomorphic to $\mathbf{Z}/\ell^r \times \mathbf{Z}/\ell^s$.*

(b) *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 $E[\ell^\infty](K) \simeq \mathbf{Z}/\ell^r \times \mathbf{Z}/\ell^s$.*

(c) *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*

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

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

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

Proof. Part (a) is again straightforward, using that $r+s \leq n$.

We next prove (b), 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,

$$\begin{pmatrix} \ell^r a & \ell^s b \\ \ell^{n-s} c & \ell^{n-r} d \end{pmatrix} \begin{pmatrix} \ell^{n-r} \\ \ell^{n-s} \end{pmatrix} \equiv 0 \pmod{\ell^n} \tag{2.2.15}$$

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 (b).

Next, part (c). 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 (d), take $t = n-r$ in part (c). □

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 [10])**.** *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 [10, 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 $G = G(n; r, n-r)$ for some integer $0 \leq r \leq n$.

We then apply the preceding paragraph to elliptic curves [10, 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'. □

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 [18, p. I-2, Exercise 1]; when k is perfect, see the proof by Katz [10, 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 2.2.14(c), 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 $T_\ell E$).*

Recalling (2.2.8), we may equivalently replace the conclusion with image $G(n; r, s)$ with $0 \leq s \leq n-r$ or $G(n; r', n-r)$ with $0 \leq r' = n - s \leq r$.

Proof. We have $\deg \varphi = \ell^k$ for some $k \geq 0$, and by Lemma 2.3.7 we may suppose that $k \leq n$. The dual isogeny $\varphi^\vee\colon E' \to E$ is then described by Proposition 2.2.10(b), giving the result. □

3. Counting elliptic curves

In this section, we count 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; we need only the special case where the moduli problems are fine, so the stackiness is kept to a minimum.

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

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

We make the nontrivial hypothesis that Γ_G is torsion free: in particular, $-1 \notin G$. Then Γ_G is a discrete group acting freely and faithfully on the upper half-plane $\mathbf{H}^2$, and the quotient $\Gamma_G \backslash \mathbf{H}^2$ has a canonical structure of a Riemann surface (compact minus finitely many points).

Attached to G is the fine moduli problem of elliptic curves with G-level structure, as in the following proposition.

Proposition 3.1.1. *Suppose* $\det G = (\mathbf{Z}/N)^\times$ *and* Γ_G *is torsion free. Then there exists a unique affine, smooth, geometrically integral curve* Y_G *defined over* $\mathbf{Q}$*, 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 isomorphism classes of* Gal_K*-stable* G*-orbits of pairs* (E, ι)*, where* E *is an elliptic curve over* K *and* $\iota\colon (\mathbf{Z}/N)^2_K \simeq E[N]$ *is an isomorphism of group schemes over* K*.*

(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 and only if* $\overline{\rho}_{E,N}(\mathrm{Gal}_K) \lesssim G$ *is contained in a subgroup conjugate to* G*.*

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 [6, §4] or the tome of Katz–Mazur [11]; for property (iii), see Baran [3, §4]. □

By Yoneda's lemma, whenever we have an inclusion $G \leq G' \leq \mathrm{GL}_2(\mathbf{Z}/N)$, there is a forgetful map from G'-level structure to G-level structure, and a corresponding map $Y_{G'} \to Y_G$ over $\mathbf{Q}$. Since the curve Y_G solves a moduli problem, there is a universal elliptic curve $\phi_G\colon E_{G,\mathrm{univ}} \to Y_G$, unique up to isomorphism: in particular, $E_{G,\mathrm{univ}}$ is an elliptic curve over (the coordinate ring of) Y_G, and the bijection in (ii) is defined by the map that sends $P \in Y_G(K)$ to the fiber of ϕ_G over P.

Remark 3.1.2. We do not require the smooth compactification and its moduli interpretation as generalized elliptic curves.

We recall also here the notion of an *irregular cusp* (see e.g., Diamond–Shurman [7, (3.3), p. 75], Shimura [19, §2.1, p. 29]). Let $\Gamma \leq \mathrm{SL}_2(\mathbf{Z})$. 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 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 3.1.3. *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

$$\begin{aligned} \det(\gamma) &= (1 + \ell^r a_0)(1 + \ell^{n-r} d_0) - \ell^n b_0 c_0 \\ &= 1 + \ell^r a_0 + \ell^{n-r} d_0 + \ell^n (a_0 d_0 - b_0 c_0) = 1, \end{aligned} \tag{3.1.4}$$

so expanding we find

$$\operatorname{tr}(\gamma) = 2 + \ell^r a_0 + \ell^{n-r} d_0 \equiv 2 \pmod{\ell^n}. \tag{3.1.5}$$

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 [7, Exercise 3.8.7]. □

Lemma 3.1.6. *We have*

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

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

Proof. Looking back at (3.1.4), we see that e.g. if $r \leq n - r$ then $1 + \ell^r a_0 \equiv 1 \pmod{\ell^{n-r}}$, so $\ell^{n-r} \mid \ell^r a_0$. □

The content of Lemma 3.1.6 will be to indicate one of the ways in which different moduli problems can have the same underlying uniformizing congruence subgroup.

3.2. **Asymptotics.** In this section, we prove Theorem 1.3.3. We prove the following weaker version first.

Theorem 3.2.1. *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*

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

Then there exists $c(G) \in \mathbf{R}_{\geq 0}$ *such that*

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

as $H \to \infty$.

As explained in the introduction, we follow an approach outlined in Harron–Snowden [9].

Proof. Our proof proceeds in three 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 $\mathrm{Gal}_{\mathbf{Q}}$). The universal curve has the form

$$E_{G,\mathrm{univ}} \colon y^2 = x^3 + f(t)x + g(t) \tag{3.2.2}$$

where $f(t), g(t) \in \mathbf{Q}(t)$: 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 [9, 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

$$3 \deg f(t) = 2 \deg g(t) = \deg(j) = [\mathrm{PSL}_2(\mathbf{Z}) : \Gamma_G] = d(G) \tag{3.2.3}$$

with moreover $12 \mid d(G)$. We now homogenize, letting $t = a/b$ and clearing denominators, giving

$$E_{A,B} \colon y^2 = x^3 + A(a,b)x + B(a,b) \tag{3.2.4}$$

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

The map $\mathbf{A}^1 \to \mathbf{A}^2$ defined by $t \mapsto (f(t), g(t))$ is nonconstant and therefore has image a curve, and the map has some degree $r(G) \geq 1$; consequently away from finitely many points, the map is $r(G)$-to-1. Since $E_{A,B}$ is obtained from homogenization of (3.2.2), we conclude that the map $(a,b) \mapsto E_{A,B}$ with $\gcd(a,b) = 1$ is also $r(G)$-to-1.

Step 2: principle of Lipschitz. Let E be an elliptic curve over $\mathbf{Q}$ defined by $E \colon y^2 = x^3 + Ax + B$ with $E \in \mathscr{E}$ is an elliptic curve over $\mathbf{Q}$ that has a G-level structure defined over $\mathbf{Q}$. By (3.2.4), there exist $a, b \in \mathbf{Z}$ such that $A = A(a,b)$ and $B = B(a,b)$. Therefore, to count the subset of $Y_G(\mathbf{Q})$ represented by a pair (E, ι) with $E \in \mathscr{E}_{\leq H}$, we need to count the number of integer points in the region

$$R(H) := \{(a,b) \in \mathbf{R}^2 : |A(a,b)| \leq (H/4)^{1/3} \text{ and } |B(a,b)| \leq (H/27)^{1/2}\} \subset \mathbf{R}^2 \tag{3.2.5}$$

subject to the conditions

(N1) $4A(a,b)^3 + 27B(a,b)^2 \neq 0$, and
(N2) there does not exist a prime p such that $p^4 \mid A(a,b)$ and $p^6 \mid B(a,b)$.

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

$$\max_{x \in \mathbf{R}} (|f(x)|^3, |g(x)|^2) \geq c > 0 \tag{3.2.6}$$

is bounded below. Since

$$\begin{aligned} |A(a,b)| &= |b^{d(G)/3} f(a/b)| \\ |B(a,b)| &= |b^{d(G)/2} g(a/b)| \end{aligned} \tag{3.2.7}$$

we conclude that

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

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

Therefore the region $R(H)$ is compact, because it is closed and bounded, and has rectifiable boundary (defined by polynomials). By the Principle of Lipschitz [5], the number of integral points in the region (3.2.5) 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: since $\deg A(a,b) = \deg f(t) = \frac{1}{3} d(G)$ and $\deg B(a,b) = \deg g(t) = \frac{1}{2} d(G)$ by (3.2.3), we have

$$H^{1/d(G)} R(1) = R(H). \tag{3.2.8}$$

Therefore, the count of elliptic curves (ignoring overcounting and conditions (N1)–(N2)) is thus

$$\frac{\mathrm{area}(R(H))}{r(G)} + O(\mathrm{len}(\mathrm{bd}(R(H)))) = \frac{\mathrm{area}(R(1))}{r(G)} H^{2/d(G)} + O(H^{1/d(G)}) \tag{3.2.9}$$

where $r(G) \in \mathbf{Z}_{\geq 1}$ is defined at the end of Step 1.

The points (a, b) such that $4A(a, b)^3 + 27B(a, b)^2 = 0$ lie on a curve, which by standard estimates is $O(H^{1/d(G)})$, so applying condition (N1) does not change (3.2.9).

Step 3: sieving. To conclude, we apply the condition (N2) by a standard sieve, taking care of local conditions.

We have $\deg A \geq 4$ and similarly $\deg B \geq 6$ by (3.2.3). Since $\gcd(f(t), g(t)) = 1$, the (weighted homogeneous) ideal $I := \langle A(a, b), B(a, b)\rangle \subseteq \mathbf{Z}[a, b]$ has codimension 2, so is supported above a set S of finitely many primes. Therefore, for all $p \notin S$, the ideal I is supported on the irrelevant ideal, and therefore $p^4 \mid A(a, b)$ and $p^6 \mid A(a, b)$ for $a, b \in \mathbf{Z}$ if and only if $p \mid a$ and $p \mid b$. For such primes, we have overcounted and need to multiply by the correction factor $1 - 1/p^2$. For the remaining primes $p \in S$, there are two possibilities for a correction factor.

Either $p^4 \mid A(a, b)$ and $p^6 \mid A(a, b)$ for $a, b \in \mathbf{Z}$ if and only if $p \mid a$ and $p \mid b$ (just like for $p \notin S$), and we define

$$\delta_p := \frac{1}{p^{12}} \#\{a, b \in \mathbf{Z}/p^6 : A(a, b) \equiv 0 \pmod{p^4} \text{ and } B(a, b) \equiv 0 \pmod{p^6}\}; \tag{3.2.10}$$

we have overcounted and need to multiply by the factor $1 - \delta_p$. Or, it may happen that $p^4 \mid A(a, b)$ and $p^6 \mid A(a, b)$, but one of a or b is not divisible by p. In that case, it is still a finite calculation to sieve the non-minimal equations, but the sample space for the δ_p may be larger, once a and b are appropriately scaled (see Proposition 4.3.11 and 4.4.3 for examples of carrying this out in practice).

A standard Möbius sieve argument then gives

$$c(G) = \operatorname{area}(R(1))\zeta(2)^{-1} \prod_{p \in S} \frac{1 - p^{-2}}{1 - \delta_p}. \tag{3.2.11}$$

Combining Steps 1–3, we conclude the proof. □

Corollary 3.2.12. *With notation as in Theorem 3.2.1, we have*

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

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

Proof. Suppose that E has $\overline{\rho}_{E,N}(\mathrm{Gal}_{\mathbf{Q}}) = G' < G$ up to conjugation a proper subgroup. If $\Gamma_{G'}$ has genus ≥ 1, then $N_{G'}(H)$ is either finite or grows slower than any power of H, 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 Theorem 3.2.1 then gives the result. □

Proposition 3.2.13. *The constant $c(G)$ in Theorem 3.2.1 is effectively computable.*

Proof. We first claim that the universal curve is effectively computable, in the sense that there is a Turing machine that, given input G, outputs $f(t), g(t) \in \mathbf{Q}(t)$ such that (3.2.2) 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

[23, Chapter 4], the canonical ring of Y_G is the log canonical ring of X_G; this graded ring has a simple, explicit description [23, §4.2] in terms of $\#\Delta$. Moreover [23, §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 [2], 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. The degree is easy to compute as $d(G) = [\mathrm{PSL}_2(\mathbf{Z}/N) : G]$. For the constant $c(G)$, we note that the area $\mathrm{area}(R(1))$ can be computed to any desired precision by numerical integration. To compute the set S of bad primes in step 3, we use Gröbner basis techniques, or just compute S as the set of primes dividing the resultant of $A(a,1), B(a,1)$ or $A(1,b), B(1,b)$. For the primes $p \in S$, the quantity δ_p can be computed by exhaustive enumeration. □

Remark 3.2.14. Actually, by work of Sebbar [17] 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 [13, 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 3.2.13 in every case, and to just compute these constants (keeping track of the effect of the twist)—such a task lies outside of the motivation and scope of this paper.

However, 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 $(\mathrm{P})\,\mathrm{SL}_2(\mathbf{Z})$, some can be written as Γ_G with $G = \overline{G}_{\ell^n}(n; r, s)$. In particular, we have

$$\begin{aligned} \Gamma(\ell^n) &= \Gamma_{\overline{G}_\ell(2n;n,n)} \\ \Gamma_1(\ell^n) &= \Gamma_{\overline{G}_\ell(n;n,0)} = \Gamma_{\overline{G}_\ell(n;0,0)} \\ \Gamma_0(4) &= \Gamma_{\overline{G}_2(2;1,0)}, \end{aligned} \tag{3.2.15}$$

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 [17] 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

$$\Gamma_0(8),\ \Gamma_0(9),\ \Gamma_0(8) \cap \Gamma(2),\ \Gamma_0(12),\ \Gamma_0(16),\ \Gamma_0(18),\ \Gamma_0(16) \cap \Gamma_1(8),\ \Gamma_0(25) \cap \Gamma_1(5)$$

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 3.2.1 with Proposition 3.2.13. □

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 $m = 7$. One can apply the arguments of this section to compute P_m for any $m \geq 5$.

4.1. **Proof of main result.** Let $m \in \{1, 2, \ldots, 10, 12, 16\}$. As in the introduction, we consider the set $\mathscr{E}$ of elliptic curves E over $\mathbf{Q}$ of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbf{Z}$ satisfying:

- $4A^3 + 27B^2 \neq 0$, and
- There is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

We define the height of $E \in \mathscr{E}$ by

$$\operatorname{ht} E := \max(|4A^3|, |27B^2|) \tag{4.1.1}$$

and for $H > 0$, let $\mathscr{E}_{\leq H} := \{E \in \mathscr{E} : \operatorname{ht} E \leq H\}$.

We seek to refine our understanding of the subset

$$\mathscr{E}_{m?} := \{E \in \mathscr{E} : m \mid \#E(\mathbf{F}_p) \text{ for a set of primes } p \text{ of density } 1\} \tag{4.1.2}$$

by considering the probability

$$P_m := \lim_{H \to \infty} \frac{\#\{E \in \mathscr{E}_{\leq H} : m \mid \#E(\mathbf{Q})_{\mathrm{tor}}\}}{\#\{E \in \mathscr{E}_{m?} \cap \mathscr{E}_{\leq H}\}}; \tag{4.1.3}$$

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 the principle of Lipschitz, we give an asymptotic count for these curves, and find a positive proportion.

Definition 4.1.4. *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 4.1.4 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 4.1.5. *We have*

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

as $H \to \infty$.

In other words, we can replace the denominator in the probability P_m by the count of m-full curves by height.

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 $\rho_{E',\ell}(\mathrm{Gal}_{\mathbf{Q}}) \le G_\ell(n; r, n-r)$ for some $0 \le r \le n$. 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. We show that the curves that are not m-full are asymptotically negligible.

A subgroup $G' \le \mathrm{GL}_2(\mathbf{Z}_m) \simeq \prod_{\ell \mid m} \mathrm{GL}_2(\mathbf{Z}_\ell)$ of finite index is relevant if the following conditions hold:

(a) $\det(G') = \prod_{\ell \mid m} \mathbf{Z}_\ell^\times$, and
(b) for every $\ell^n \parallel m$, there exists $0 \le r \le n$ such that the projection of G' to $\mathrm{GL}_2(\mathbf{Z}_\ell)$ is contained in $G_\ell(n; r, n-r)$.

We say that G' is minimally relevant if G' is relevant and there exists ℓ such that the containment in (b) is *proper*. There are only finitely many minimally relevant subgroups up to conjugacy, and each is a direct product $G' = \prod_{\ell \mid m} G'_\ell$ of the full preimages G'_ℓ of its projections onto $\mathrm{GL}_2(\mathbf{Z}_\ell)$.

Let G' be a minimally relevant subgroup; then G' is strictly contained in a relevant subgroup G which is a direct product of groups $G_\ell(n; r, n-r)$, defined by conditions modulo m by Lemma 2.2.9(a) and CRT. Let $\Gamma_G := \pi_m^{-1}(G \cap \mathrm{SL}_2(\mathbf{Z}/m)) \le \mathrm{SL}_2(\mathbf{Z})$ be the group attached to G. Since $m \ge 5$, the group Γ_G is torsion free (see Lemma 2.2.9(d)), and so by Proposition 3.1.1, there exists a curve Y_G that is a fine moduli space for G. Since $G' \le G$, the same holds for G', and we have a map $Y_{G'} \to Y_G$. Actually, since the containment $G' < G$ is proper and $\det(G') = \det(G) = \mathbf{Z}_m^\times$, the containment $\Gamma_{G'} < \Gamma_G$ is proper, so the map $Y_{G'} \to Y_G$ is a map of degree $[G : G'] = [\Gamma_G : \Gamma_{G'}] > 1$. Repeating the argument in Corollary 3.2.12, the curves parametrized by $Y_{G'}$ are negligible in comparison to those parametrized by Y_G (the image of $X_{G'}(\mathbf{Q})$ in $X_G(\mathbf{Q})$ is thin, see Serre [20, Chapter 10]), and

$$\#\{E \in \mathscr{E}_{\le H} : (E, \varphi) \in X_{G'}(\mathbf{Q})\} = o(\#\{E \in \mathscr{E}_{\le H} : (E, \varphi) \in X_G(\mathbf{Q})\}). \tag{4.1.6}$$

Adding up over the finitely many possibilities for G', we have shown that

$$\#\{E \in \mathscr{E}_{\le H} : E \text{ is } \textit{not } m\text{-full}\} = o(\#\{E \in \mathscr{E}_{\le H} : E \text{ is } m\text{-full}\}) \tag{4.1.7}$$

and the result follows. □

With Proposition 4.1.5 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 degenerate case $\ell^n = 2^1$ in Example 2.2.6.

Corollary 4.1.8. *For $m \ge 5$, the probability P_m is nonzero for all m.*

Proof. By Proposition 4.1.5, in the denominator of P_m we need to count curves parametrized by groups $G \le \mathrm{GL}_2(\mathbf{Z}/m)$ isomorphic (via the CRT) to the product $\overline{G}_{\ell^n}(n_\ell; r_\ell, s_\ell)$ (with $0 \le r_\ell, s_\ell, r_\ell + s_\ell \le n_\ell$, by (2.2.8)), and the numerator consists of the subset of counts with $r + s = n$. 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 3.2.1, the asymptotic for such a group is determined by $d(G) = \frac{1}{2}[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G]$. We compute

$$d(G) = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_G] = [\mathrm{GL}_2(\mathbf{Z}/m) : G] = \prod_{\ell \mid m} [\mathrm{GL}_2(\mathbf{Z}_\ell) : G_\ell(n_\ell; r_\ell, s_\ell)] \tag{4.1.9}$$

since the group is a direct product. But we computed these indices in Lemma 2.2.9: they only depend on whether $\min(r_\ell, n_\ell - r_\ell) = 0$ or not; the smallest degree $d(G)$ (from the smallest index, giving the largest asymptotic $H^{1/d(G)}$) occurs when $\min(r_\ell, n_\ell - r_\ell) = 0$ for each ℓ, and this case occurs whenever there is *cyclic* m-torsion (so as long as $m \neq 16$). Whatever the largest asmyptotic, we may always choose $s_\ell = n_\ell - r_\ell$ and by Lemma 2.2.14(b) such curves have m-torsion, and so such curves arise with positive probability. □

For the sake of explicitness, we indicate the rate of growth for each group. By a straightforward calculation in Magma, we find Table 4.1.10: by (2.2.12), 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.

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	$\mathbf{Z}/2^r\mathbf{Z}$
8	$G_2(3; r, 1)$, $r = 1, 2$	6	$\mathbf{Z}/2^r\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$
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	$\mathbf{Z}/2^r\mathbf{Z}$
12	$G_2(4; 1, 1) \times G_3(1; 1, 0)$	12	$\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$
16	all	24	$\mathbf{Z}/2^r \times \mathbf{Z}/2$, $r = 0, 1, 2, 3$

Table 4.1.10: 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.

Remark 4.1.11. In following sections we will work with explicit universal polynomials for certain m-full groups (specifically, when $m = 3, 4, 5, 7$). A list of all universal polynomials for the m-full groups that occur can be found online [4].

4.2. **Setup to compute P_m for $m = 5, 7$.** In the remainder of this section, we follow the proof of Corollary 4.1.8 and compute P_m for $m = 5, 7$. The main simplification in these cases is that, aside from a negligible subset when $m = 5$ (see Lemma 4.3.3), elliptic curves in $\mathscr{E}_{m?}$ either have a global point of order m, or are m-isogenous to one that does.

Let $m = \ell \in \{5, 7\}$. 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 [22, (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 2.2.14(c) 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 $f, f', g, g' \in \mathbf{Q}[t]$. Let $j(t)$ (resp. $j'(t)$) be the j-function of $E(t)$ (resp. $E'(t)$).

In Step 1 of Theorem 3.2.1 we require that the map $t \to (f(t), g(t))$ is 1-to-1 except possibly at a finite number of points (similarly for $(f'(t), g'(t))$). In the next sections we list the explicit polynomials f, f', g, g'. For each $m \in \{5, 7\}$ we find the mappings are 1-to-1. Indeed, in every case the determinant factors as

$$f(t)g(s) - f(s)g(t) = (s - t)F(s, t),$$

where $F(s, t) = 0$ defines an irreducible curve of genus at least 2, which has finitely many points by Faltings' theorem. This similarly holds for the map $t \to (f'(t), g'(t))$.

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

$$\begin{aligned} E(a,b) &: y^2 = x^3 + A(a,b)x + B(a,b) \\ E'(a,b) &: y^2 = x^3 + A'(a,b)x + B'(a,b), \end{aligned} \tag{4.2.3}$$

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, we give a quick overview of the calculations in both cases here.

Let $c = c(G_\ell(1;1,0))$ and $c' = c(G_\ell(1;0,0))$ as defined in (3.2.11). The finite set S appearing in the definition of c is the set of primes supported on $\mathrm{Res}(f(t), g(t))$, and the same for S' and c'. In fact, we will see that $S = S' = \{2, 3, \ell\}$. Since the main growth terms have the same degree (see Table 4.1.10), we find

$$P_\ell = \frac{c}{c + c'} = \frac{1}{1 + c'/c} \tag{4.2.4}$$

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

$$\frac{c'}{c} = \frac{\mathrm{area}(R'(1))}{\mathrm{area}(R(1))} \prod_{q \in \{2,3,\ell\}} \frac{1 - \delta_q}{1 - \delta'_q}, \tag{4.2.5}$$

where

$$\begin{aligned} R(1) &:= \{(a,b) \in \mathbf{R}^2 : |A(a,b)| \le (1/4)^{1/3} \text{ and } |B(a,b)| \le (1/27)^{1/2}\} \subset \mathbf{R}^2 \\ R'(1) &:= \{(a,b) \in \mathbf{R}^2 : |A'(a,b)| \le (1/4)^{1/3} \text{ and } |B'(a,b)| \le (1/27)^{1/2}\} \subset \mathbf{R}^2 . \end{aligned} \tag{4.2.6}$$

We compute the local corrections δ_q, δ'_q by finite search. The ratio of areas has a remarkably simple expression, as follows. By Lemma 3.1.6, 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! It follows that there is a linear fractional transformation $\varphi(t) \in \mathbf{Q}(\zeta_\ell)(t)$ such that

$$j(\varphi(t)) = j'(t). \tag{4.2.7}$$

By an easy explicit computation of φ, we get a change of variables mapping $R(1)$ bijectively onto $R'(1)$. Therefore, the ratio

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

is the determinant of the change of variables matrix.

4.3. **The case $m = 5$.** We now carry out the above strategy for $m = \ell = 5$. In the Tate normal form (4.2.1), we compute $b = c = t$ (see e.g. García-Selfa–Tornero [8, Thm. 3.1]); applying Vélu's formulas [22, (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

$$\begin{aligned} f(t) &= -27(t^4 - 12t^3 + 14t^2 + 12t + 1) \\ g(t) &= 54(t^6 - 18t^5 + 75t^4 + 75t^2 + 18t + 1) \\ j(t) &= \frac{f(t)^3}{t^5(t^2 - 11t - 1)} \\ f'(t) &= -27(t^4 + 228t^3 + 494t^2 - 228t + 1) \\ g'(t) &= 54(t^6 - 522t^5 - 10005t^4 - 10005t^2 + 522t + 1) \\ j'(t) &= \frac{f'(t)^3}{t(t^2 - 11t - 1)^5}. \end{aligned} \tag{4.3.2}$$

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. 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

$$(s^8 + s^7 + 2s^6 - 2s^5 + 5s^4 - 3s^3 + 2s^2 - s, s^{12} - s^{11} - s^{10} + s^8 - 10s^7 + 13s^6 - 11s^5 + 5s^4 - 3s^3 + s^2)$$

is a point of order 5. □

Remark 4.3.4. If $t_0 \in \mathbf{Q}$, then as in Example 2.2.13, 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 [12] 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 $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right) \leq \mathrm{GL}_2(\mathbf{F}_5)$, 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 [24, Thms. 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 [1] on the classification of isogeny graphs of elliptic curves over $\mathbf{Q}$.

We now compute the all-important change of coordinates $\phi(t)$ in (4.2.7). We write $u := (11+5\sqrt{5})/2 \in \mathbf{R}_{>0}$ so that u and $-1/u$ are the roots of the quadratic polynomial $t^2-11t-1$ and define the linear fractional transformation

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

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

Lemma 4.3.6. *With $R(1), R'(1)$ as defined in (4.2.6), we have*

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

Proof. By the observation following (4.2.7), the ratio $\frac{\mathrm{area}(R'(1))}{\mathrm{area}(R(1))}$ 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, so we are extra-explicit.

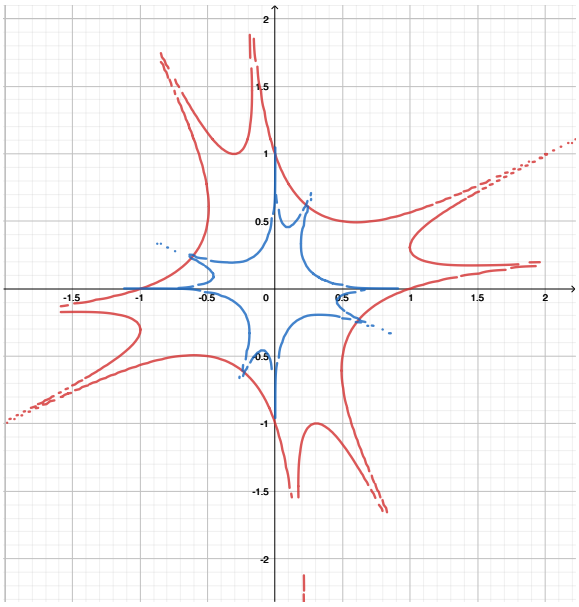
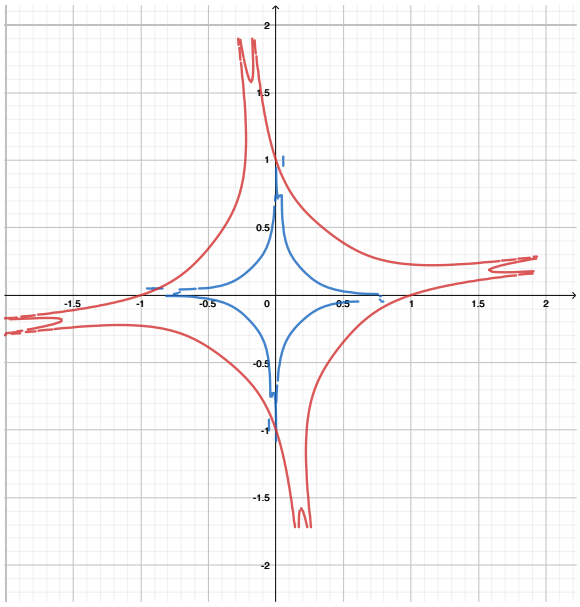
Define the angle $\theta := \arctan(2/11)/2$, so that

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

Direct calculation reveals that

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

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 $R(1)$:

The ratio $\frac{\text{area}(R'(1))}{\text{area}(R(1))} = \frac{1}{5}$ 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 (4.2.5), which is the last ingredient needed for an exact expression for P_5. Because we will perform a similar sieve for the case $m = 7$, and because the counting is slightly nontrivial, we go into some detail here. We will then be able to proceed more quickly through this step when $m = 7$.

The ideal $I = \langle A(a,b), B(a,b)\rangle \subseteq \mathbf{Z}[a,b]$ of Step 3 of Theorem 3.2.1 is supported above a finite set S of prime numbers. Recapping our argument from Step 3, for all $p \notin S$, we have $p^4 \mid A(a,b)$ and $p^6 \mid B(a,b)$ if and only if $p \mid a$ and $p \mid b$. At these primes we have overcounted and adjust by multiplying by the local zeta-factor $1-1/p^2$. For $p \in S$, it may be the case that $p^4 \mid A(a,b)$ and $p^6 \mid B(a,b)$, but either p does not divide a or p does not divide b and simply dividing the coefficients by p^4 and p^6, respectively, produces a non-integral Weierstrass equation. We need a finer sieve.

Given the polynomials $A(a,b)$ and $B(a,b)$ we compute the saturation of the ideal I at (a,b). The result is an integer D such that if $(a,b) \not\equiv (0,0) \pmod{p}$ and $M \mid A(a,b)$ and $M \mid B(a,b)$, then $M \mid D$. We perform these computations for both the elliptic curves E and E' and record the results in the following Lemma.

Lemma 4.3.8. *Let $A(a,b)$ and $B(a,b)$ (resp. $A'(a,b)$, $B'(a,b)$) be the homogenizations of the polynomials $f(t)$ and $g(t)$ (resp. $f'(t)$, $g'(t)$) of (4.3.2), respectively. Then, the saturation of the ideal I (resp. I') at (a,b) is given by the integer $D = 2^5 3^5 5$ (resp. $D' = 2^5 3^5 5^{10}$).*

Proof. Routine computation in Magma. □

By Lemma 4.3.8, we need only investigate the primes 2, 3 and 5. The following lemma dispenses with most of the cases easily.

Lemma 4.3.9. *For $q \in \{2,3,5\}$, we have:*

(4.3.10)

q	δ_q	δ'_q
2	1/4	1/4
3	1/9	1/9
5	1/25	

Proof. We easily verify by hand or finite calculation that

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

if and only if $a \equiv b \equiv 0 \pmod{q}$ for $q = 2,3,5$, and that

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

if and only if $a \equiv b \equiv 0 \pmod{q}$ for $q = 2,3$. Therefore, $\delta_q = 1/q^2$, as indicated in the table. □

Lemma 4.3.11. *We have $\delta'_5 = 5/13$.*

Proof. We computed $D' = 2^5 3^5 5^{10}$, and so we can factor a 5^4 or a 5^8 from A'. Let us first consider a factor 5^4, since in the course of this analysis we will see that the 5^8 is irrelevant. We need to consider $(a,b) \in (1/5)\mathbf{Z} \times (1/5)\mathbf{Z}$. Since we can multiply by 5, we just need to count $n_1 = \#S_1$, where

$$S_1 := \{(a,b) \in \mathbf{Z}/5^{12} \times \mathbf{Z}/5^{12} : 5^4 \mid A'(a,b) \text{ and } 5^6 \mid B'(a,b)\} \tag{4.3.12}$$

since this is equivalent to $A(a/5,b/5), B(a/5,b/5) \in \mathbf{Z}$, and then count $n_2 = \#S_2$, where

$$S_2 := \{(a,b) \in \mathbf{Z}/5^{12} \times \mathbf{Z}/5^{12} : 5^8 \mid A'(a,b) \text{ and } 5^{12} \mid B'(a,b)\} \tag{4.3.13}$$

since these are the overcounts. We will then have

$$\delta_3 = n_2/n_1. \tag{4.3.14}$$

To reduce the size of the sample space, we observe that each set S_i can be written as the disjoint union

$$S_i = S_{i,00} \cup S'_i, \tag{4.3.15}$$

where

$$\begin{aligned} S_{i,00} &:= \{(a,b) \in S_i : a \equiv b \equiv 0 \pmod{5}\}, \text{ and} \\ S'_i &:= \{(a,b) \in S_i : a \not\equiv 0 \pmod{5} \text{ or } b \not\equiv 0 \pmod{5}\}. \end{aligned} \tag{4.3.16}$$

We therefore have $n_i = \#S_{i,00} + \#S'_i = 5^{22} + \#S'_i$, and so it remains to calculate $\#S'_i$.

If $(a,b) \in S'_i$ then $(ua,ub) \in S'_i$ for all $u \in (\mathbf{Z}/5^{12})^\times$. Scaling, we see

$$\#S'_i = \phi(5^{12}) \left(\#\{(a,1) \in S'_i\} + \#\{(1,b) \in S'_i\}\right). \tag{4.3.17}$$

We compute $\#\{(a,1) \in S'_i\} = 5^{10}, 0$ and $\#\{(1,b) \in S'_i\} = 5^{10}, 0$ for $i = 1,2$ by counting roots of a univariate polynomial, giving

$$n_1 = 5^{21}13, \; n_2 = 5^{22},$$

and so $\delta_5 = 5/13$, as claimed. □

We finally arrive at the exact value of P_5.

Corollary 4.3.18. *We have $P_5 = 125/164 \approx 76.22\%$.*

Proof. By (4.2.4), we have

$$P_5 = \frac{c}{c+c'} = \frac{1}{1+c'/c},$$

and by (4.2.5) we have

$$\frac{c'}{c} = \frac{\text{area}(R'(1))}{\text{area}(R(1))} \prod_{q\in\{2,3,5\}} \frac{1-\delta_q}{1-\delta'_q}.$$

Apply Lemmas 4.3.6, 4.3.9, and 4.3.11 to get

$$\frac{c'}{c} = \frac{1}{5} \cdot \frac{24}{25(1-5/13)},$$

from which the exact value of P_5 follows. □

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:

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

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

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

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

Lemma 4.4.1. *With $R(1), R'(1)$ as defined in (4.2.6), we have*

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

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 $m = 5$ we must compute the local sieve factors. We run the Magma script of Lemma 4.3.8 applied to the polynomials of this section and conclude that $D = 2^5 3^5 7$ and $D' = 2^5 3^5 7^{10}$. We therefore need to compute δ_q and δ'_q for $q \in \{2, 3, 7\}$. Similar to the situation $m = 5$, we have two cases: those for the sieve factor is a zeta-factor, and those for which it is not. We combine all of the information in the following lemma.

Lemma 4.4.3. *For $q \in \{2, 3, 7\}$, we have:*

(4.4.4)

q	δ_q	δ'_q
2	1/4	1/4
3	1/5	1/5
7	1/49	1/13

Proof. We verify that

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

if and only if $a \equiv b \equiv 0 \pmod{q}$ for $q = 2, 7$, and that

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

if and only if $a \equiv b \equiv 0 \pmod{q}$ for $q = 2$, giving the indicated values of δ_2, δ'_2, and δ_7.

Now we compute δ_3 and δ'_3 simultaneously because both D and D' are divisible by the same power of 3. We proceed exactly as in Lemma 4.3.11: adopting notation appropriately, we compute

(4.4.5)

$$n_1 = 3^{22}5, n_2 = 3^{22}$$
$$n'_1 = 3^{22}5, n'_2 = 3^{22}$$

and so $\delta_3 = \delta'_3 = 1/5$; similarly,

(4.4.6)

$$\delta'_7 = \frac{n'_2}{n'_1} = \frac{7^{22}}{7^{22}13} = \frac{1}{13}.$$

completing the proof. □

Corollary 4.4.7. *We have*

$$P_7 = \frac{49\sqrt{7}}{49\sqrt{7} + 52} \approx 71.37\%$$

Proof. By (4.2.4), we have

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

and by (4.2.5) we have

$$\frac{c'}{c} = \frac{\text{area}(R'(1))}{\text{area}(R(1))} \prod_{q \in \{2,3,7\}} \frac{1 - \delta_q}{1 - \delta'_q}.$$

Apply Lemmas 4.4.1 and 4.4.3 to get

$$\frac{c'}{c} = \frac{1}{\sqrt{7}} \cdot \frac{1 - 1/49}{1 - 1/13},$$

from which the exact value of P_7 follows. □

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 [8, §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 $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and so can be written in the form

$$\begin{pmatrix} 1 + 2\alpha & \beta \\ 2\gamma & 1 + 2\delta \end{pmatrix}$$

with $2 \mid \beta\gamma$. But then $2 \mid \gamma$ (or else $E(F)[2] = \mathbf{Z}/2 \times \mathbf{Z}/2$) and so the mod 4 representation lies in the group $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ and so E admits a rational cyclic 4-isogeny.

Now suppose we are in Case (ii). In light of Lemma 5.1.3, let $a \in F^{\mathrm{al}}$ 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. It is easy to check that 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 biquadratic 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 (3.2.5) attached to the elliptic curve (5.2.1). Applying the Principle of Lipschitz we see that

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

In particular, observe that

$$\operatorname{area} R_1(1) = 9 \operatorname{area} R_{-3}(1). \tag{5.2.2}$$

Remark 5.2.3. 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 5.2.4. *We have $P_3 = 1/2$.*

Proof. Appealing to and expanding the notation of (3.2.11), 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. 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 (5.2.2) 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 5.2.5. We confirm Proposition 5.2.4 experimentally: in a naive way, we compute

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

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 [9, 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 1.3.4. 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 $\mathbf{Z}/4$-subgroup is given by*

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

for an explicitly computable constant c.

Proof. Elliptic curves over $\mathbf{Q}$ with a rational point of order 4 are parameterized by

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

and the number of integral equations is 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

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

The compactness of $R(H)$ allows for a Lipschitz analysis. A homogeneity argument with the Weierstrass coefficients shows immediately that $\text{area}(R(H)) = \text{area}(R(1))H^{1/4}$ and $O(\text{len}(\text{bd}(R(H)))) = O(H^{1/6})$. The boundary of $R(H)$ is rectifiable (given by polynomials)

and so the area of $R(1)$ is calculable. The constant c is 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 1.3.4. After this, we count curves admitting a cyclic 4-isogeny in Proposition 5.3.9. From there, it is then a simple matter to fit the pieces together to obtain an exact expression for P_4; this is Corollary 5.3.11.

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

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

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

$$\begin{aligned} A(a,b) &= -(a^2 - ab + b^2)/3 \\ B(a,b) &= -(a+b)(2a-b)(a-2b)/27. \end{aligned}$$

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

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

We therefore put

$$R_4(H) = \{(a,b) \in \mathbf{R}\times\mathbf{R} : 4|A(a,b)|^3 \leq H\}. \tag{5.3.7}$$

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 (5.3.7).

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

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

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

$$-\frac{1}{3}(a^2 - ab + b^2) \in \mathbf{Z} \Leftrightarrow \frac{1}{27}(-2a^3 + 3a^2b + 3ab^2 - 2b^3) \in \mathbf{Z}$$

and that this occurs for $1/3$ of all integral pairs $(a,b) \in \mathbf{Z} \times \mathbf{Z}$. Therefore,

$$\frac{\mathrm{area}\, R_4(1)}{18} \tag{5.3.8}$$

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 (5.3.8), this sieve, and the area of the ellipse $R_4(1)$, we see that

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

which completes the proof. □

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

Proposition 5.3.9. *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

$$\begin{aligned} c &= \frac{\text{area } R_4'(1)}{2\zeta(4)} \approx 0.9572 \\ 1/d &= 1/3 \\ 1/e &= 1/6, \end{aligned}$$

with the exact value of c given in Lemma 5.3.10.

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 $\text{area}(R_4'(H)) = \text{area}(R_4'(1))H^{1/3}$ 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 $\text{len bd}(R_4'(H)) = O(H^{1/6})$.

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 5.3.10 immediately following this proof for an exact value of this area and numerical approximation). The map

$$(a,b) \to (A(a,b), B(a,b))$$

is 2-to-1 outside a finite set of points (observe that the points $(\pm a, b)$ give rise to the identical Weierstrass model); thus the associated quantity "r", analogous to the $r(G)$ of Theorem 3.2.1, equals 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

$$c = \frac{1}{2} \cdot \frac{1}{\zeta(4)} \text{area}(R_4'(1)) \approx 0.9572,$$

where the numerical approximation is given by the result of Lemma 5.3.10. □

Lemma 5.3.10. *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

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

Corollary 5.3.11. *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 5.3.9. □

Remark 5.3.12. In [15], Pomerance–Schaefer count elliptic curves with Galois-stable cyclic subgroups of order 4 and obtain a finer estimate than our Proposition 5.3.9, 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 5.3.9.

Example 5.3.13. Returning to Example 2.2.13, 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 [12] label 350.b.

Remark 5.3.14. We give some experimental confirmation of Corollary 5.3.11. Enumerating curves in a naive way, among the curves $E \in \mathscr{E}_{4?} \cap \mathscr{E}_{\le 10^{13}}$ 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

(5.3.15)
$$\frac{\#\{E \in \mathscr{E}_{\leq 10^{13}} : \#E(\mathbf{Q})_{\mathrm{tor}}[2^\infty] \simeq \mathbf{Z}/2 \times \mathbf{Z}/2\}}{\#\{E \in \mathscr{E}_{4?} \cap \mathscr{E}_{\leq 10^{13}} : \#E(\mathbf{Q})_{\mathrm{tor}}[2^\infty] \leq \mathbf{Z}/2 \times \mathbf{Z}/2\}} = \frac{8126}{20612+8126} = \frac{8126}{28738} \approx 0.283$$

which matches Corollary 5.3.11 reasonably well.

Remark 5.3.16. 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

$$4 \times \left(\frac{(\alpha_+\beta_+ - \alpha_-\beta_-)}{2} + \frac{\log\left((\beta_+ + \sqrt{3}\alpha_+)(\beta_- + \sqrt{3}\alpha_-)\right)}{2\sqrt{3}} + I(\alpha_+, \alpha_-) \right) \approx 4.019,$$

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] Garen Chiloyan, Álvaro Lozano-Robledo, *A classification of isogeny-torsion graphs of elliptic curves over* $\mathbf{Q}$, preprint, 2020, `arXiv:2001.05616`.

[2] Eran Assaf, *Computing classical modular forms for arbitrary congruence subgroups*, preprint, 2020, `arXiv:2002.07212`.

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

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

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

[6] Pierre Deligne and Michael 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.

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

[8] Irene García-Selfa and José 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.

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

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

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

[12] The LMFDB Collaboration, The L-functions and Modular Forms Database, `http://www.lmfdb.org`, 2020, [Online; accessed May 5, 2020].

[13] Irwin Kra, *On lifting Kleinian groups to* $\mathrm{SL}(2, \mathbf{C})$, Differential geometry and complex analysis, Springer, Berlin, 1985, 181–193.
[14] Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Etudes Sci. Publ. Math., no. 47, 1977, 33–186.
[15] Carl Pomerance, Edward F. Schaefer, *Elliptic curves with Galois-stable cyclic subgroups of order 4*, 2020 https://arxiv.org/abs/2004.14947
[16] Maggie Pizzo, Carl Pomerance, and John Voight, *Counting elliptic curves with an isogeny of degree three*, accepted to Proc. Amer. Math. Soc.
[17] Abdellah Sebbar, *Classification of torsion-free genus zero congruence groups*, Proc. Amer. Math. Soc. **129** (2001), no. 9, 2517–2527.
[18] Jean-Pierre Serre, *Abelian ℓ-adic representations and elliptic curves*, Res. Notes Math., vol. 7, A K Peters, Ltd., Wellesley, MA, 1998.
[19] Goro 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.
[20] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Math., Friedr. Vieweg & Sohn, Braunschweig, 1997.
[21] William A. Stein, *Modular forms, a computational approach*, with an appendix by Paul E. Gunnells, Graduate Studies in Math., vol. 79, Amer. Math. Soc., Providence, 2007.
[22] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.
[23] John Voight and David Zureick-Brown, *The canonical ring of a stacky curve*, to appear in Mem. Amer. Math. Soc.
[24] David Zywina, *Possible indices for the Galois image of elliptic curves over* $\mathbf{Q}$, preprint, 2015, arXiv:1508.07663.

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

Department of Mathematics, University of Minnesota, Minneapolis, MN 55455
Email address: kenn0699@umn.edu

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