Research in Number Theory manuscript No.
(will be inserted by the editor)

Elliptic curves with Galois-stable cyclic subgroups of order 4

Carl Pomerance · Edward F. Schaefer

Received: date / Accepted: date

Abstract Infinitely many elliptic curves over $\mathbf{Q}$ have a Galois-stable cyclic subgroup of order 4. Such subgroups come in pairs, which intersect in their subgroups of order 2. Let $N_j(X)$ denote the number of elliptic curves over $\mathbf{Q}$ with at least j pairs of Galois-stable cyclic subgroups of order 4, and height at most X. In this article we show that $N_1(X) = c_{1,1}X^{1/3}+c_{1,2}X^{1/6}+O(X^{0.105})$. We also show, as $X \to \infty$, that $N_2(X) = c_{2,1}X^{1/6} + o(X^{1/12})$, the precise nature of the error term being related to the prime number theorem and the zeros of the Riemann zeta-function in the critical strip. Here, $c_{1,1} = 0.95740\ldots$, $c_{1,2} = -0.87125\ldots$, and $c_{2,1} = 0.035515\ldots$ are calculable constants. Lastly, we show no elliptic curve over $\mathbf{Q}$ has more than 2 pairs of Galois-stable cyclic subgroups of order 4.

Keywords elliptic curve · Galois-stable subgroup · isogeny · Principle of Lipschitz

Mathematics Subject Classification (2010) 11G05 · 14H52

1 Introduction

Let $E/\mathbf{Q}$ be an elliptic curve and let $\mathrm{Gal}_{\mathbf{Q}}$ be the absolute Galois group of $\mathbf{Q}$. We say that a finite subgroup of E is Galois-stable if it is stable under the

The first author is grateful for the hospitality of Santa Clara University and was funded by their Paul R. and Virginia P. Halmos Endowed Professorship in Mathematics and Computer Science.

C. Pomerance
Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053, USA and Mathematics Department, Dartmouth College, Hanover, NH 03755, USA. E-mail: carl.pomerance@dartmouth.edu

E.F. Schaefer
Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053, USA. E-mail: eschaefer@scu.edu

action of $\mathrm{Gal}_{\mathbf{Q}}$. Note that such a subgroup is the kernel of a $\mathbf{Q}$-rational isogeny on E. One can consider the distribution of $E/\mathbf{Q}$ with a Galois-stable subgroup of a given type. The distribution for order 2 subgroups can be found in [4, Thm. 5.5] and order 3 subgroups were recently handled in [6]. This brings us to order 4 Galois-stable subgroups. As a subgroup of E isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is the kernel of the multiplication-by-2 map, it is automatically Galois-stable. This article studies the distribution of elliptic curves which contain a Galois-stable copy of $\mathbf{Z}/4\mathbf{Z}$.

In Section 3 we prove that Galois-stable cyclic subgroups of order 4 come in pairs—the two intersect in the same subgroup of order 2. To be clear, each subgroup in the pair is, itself, Galois-stable. We will show that a given $E/\mathbf{Q}$ can have zero, one, or two pairs of such subgroups. We also provide necessary and sufficient conditions for $E/\mathbf{Q}$ to have at least one pair of such subgroups and similarly for two pairs. In addition, we work out the rational parametrization of elliptic curves $E/\mathbf{Q}$ with at least one pair, resp. two pairs, of Galois-stable cyclic subgroups of order 4. We can do a change of coordinates and parametrize such elliptic curves for the model $y^2 = x^3 + Ax + B$. The resulting parametrizations satisfy the conditions of [4, Prop. 4.1], from which it follows that the number of them with height at most X is of magnitude $X^{1/3}$ in the case of one pair of groups and of magnitude $X^{1/6}$ in the case of two pairs.

Let $N_j(X)$ count the number of $E/\mathbf{Q}$ of height at most X with at least j pairs of Galois-stable cyclic subgroups of order 4. In [2], among many other interesting results, the authors show that $N_1(X) = c_{1,1}X^{1/3} + O(X^{1/6})$, with $c_{1,1} = 0.95740\ldots$ a calculable constant. This asymptotic plus error estimate was worked out using the Principle of Lipschitz for counting lattice points.

In Section 4 we use Huxley's improvement on the Principle of Lipschitz (see [5]) and thus discover a lower-order main term with a power-saving error bound below that. As far as we know this is the first time this type of strong Lipschitz Principle has been used in the arithmetic statistics of elliptic curves. We are then able prove our main theorem for $E/\mathbf{Q}$ with at least one pair of Galois-stable cyclic subgroups of order 4, namely: $N_1(X) = c_{1,1}X^{1/3} + c_{1,2}X^{1/6} + O(X^{0.105})$, with $c_{1,2} = -0.87125\ldots$ a calculable constant. The $X^{1/6}$ term takes into account lattice points giving singular curves $y^2 = x^3 + Ax + B$ and $N_2(X)$ as well. We report on a computer experiment in Section 4 that illustrates the above asymptotic.

In Section 5, we find a 3-variable integer parametrization for $E/\mathbf{Q}$ of height at most X with two pairs of Galois-stable cyclic subgroups of order 4. We use that parametrization in Section 5 to find a bijection between the set of elliptic curves counted by $N_2(X)$ and certain lattice points in a 3-dimensional region with tails. In Section 5 we compute three constants, which turn out to be related, that will help us solve our counting problem in each tail. We present some useful results from analytic number theory in Section 5 and adapt them to the local restrictions imposed on our counting arguments.

The local restrictions require us to consider subsets of the lattice points in similar 3-dimensional hyperbolic regions of different sizes. We do this in

Section 5. In that section we also cover each region by two sets, each set encompassing a tail, and also consider the intersection of those two sets. We then count the appropriate lattice points in each of the three subsets in the covering. In only one of the two tails can we use the Principle of Lipschitz. We develop new techniques to count the appropriate lattice points in the other tail.

We assemble those results in Section 5 and prove our main theorem for $E/\mathbf{Q}$ with two pairs of Galois-stable cyclic subgroups of order 4, namely : $|N_2(X) - c_{2,1}X^{1/6}| \leq X^{1/12}/\exp((\log X)^{3/5+o(1)})$ as $X \to \infty$, with $c_{2,1} = 0.035515\ldots$ a calculable constant. It is to be remarked that the error estimate here relies on the best known zero-free region of the Riemann zeta function in the critical strip. If the Riemann Hypothesis could be assumed, there would be a corresponding power-saving reduction in the error estimate. We report on a computer experiment in Section 5 that illustrates the above asymptotic.

Our work is similar to [6]. In that article the authors found that the number of $E/\mathbf{Q}$ of height at most X and with a Galois-stable subgroup of order 3 is $\frac{2}{3\sqrt{3}\zeta(6)}X^{1/2} + \eta_1 X^{1/3}\log X + \eta_2 X^{1/3} + O(X^{7/24})$ for calculable constants η_1 and η_2. They too were unable to use the Principle of Lipschitz. This work built on [4] which studies the number of elliptic curves over $\mathbf{Q}$, up to a given height bound, with each possible subgroup of $\mathbf{Q}$-rational torsion points.

There are many related unsolved problems. For a finite group of order greater than 4, we can study the distribution of $E/\mathbf{Q}$ containing a Galois-stable subgroup of this type. One difficulty that will be faced dealing with groups of larger order will be finding a suitable parameterization as in our Propositions 1 and 2. Our work with two pairs of Galois-stable cyclic subgroups of order 4 suggests considering $E/\mathbf{Q}$ with more than one Galois-stable subgroup of a certain type, starting with $\mathbf{Z}/3\mathbf{Z}$ (which would extend the result of [6]). Note by $\mathbf{Z}/3\mathbf{Z}$ we mean the group, not the Galois-module. A short exploration shows that our work in Section 5, covering each tail of the region with a different set, is useful in the count of elliptic curves with two Galois-stable subgroups isomorphic to $\mathbf{Z}/3\mathbf{Z}$. We expect this technique to be useful in many such cases.

One could also consider the distribution of $E/\mathbf{Q}$ with a given Galois-stable finite subgroup and a given Galois action on that subgroup. For example, for $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, the results of [2, Prop. 5.3.5] and [4, Thm. 5.5], give us the distributions for two of the four possible Galois actions. Resolving the other two requires separating the cases where the Galois group of the field gotten by adjoining the coordinates of all 2-torsion points is isomorphic to $\mathbf{Z}/3\mathbf{Z}$ or S_3. This is likely to be tractable.

2 Notation

Let us set down some notation used throughout the article. For a given $E/\mathbf{Q}$, let $E(\mathbf{Q})$ denote the Mordell-Weil group, i.e. the set of points of E fixed by $\mathrm{Gal}_{\mathbf{Q}}$. If G is a group and $g \in G$ we use $\langle g \rangle$ to denote the cyclic subgroup of G generated by g.

There will be several constants defined in this article. In order that they be easy to find, we define them all here.

Let $\mu(d)$ denote the Möbius function. For $n > 1$ we have $\sum_{d=1}^{\infty} \mu(d)/d^n = \zeta(n)^{-1}$. We will need $\zeta(2) = \pi^2/6 \doteq 1.644934066848$ and $\zeta(4) = \pi^4/90 \doteq 1.082323233711$. (When we write $\zeta(2) \doteq 1.644934066848$, for example, we mean that $|\zeta(2) - 1.644934066848| < 5 \cdot 10^{-13}$.)

Let

$$\begin{aligned}
\alpha_1 &:= ((\sqrt{6}+\sqrt{3})/18)^{1/3} - ((\sqrt{6}-\sqrt{3})/18)^{1/3} \doteq 0.273145782170,\\
\alpha_2 &:= \frac{1}{2^{1/3}3^{1/2}} \doteq 0.458243212333,\\
i_1 &:= 2\int_0^{\alpha_1} (3u^2 + \frac{1}{4^{1/3}})^{1/2}\,du \doteq 0.458048107496,\\
i_2 &:= 2\int_{\alpha_1}^{2\alpha_2} (2u^2 + \frac{1}{27^{1/2}u})^{1/2}\,du \doteq 1.359101651471,\\
i_3 &:= 2\int_{\alpha_2}^{2\alpha_2} (3u^2 - \frac{1}{4^{1/3}})^{1/2}\,du \doteq 0.780933086923,\\
i_4 &:= i_1 + i_2 - i_3 \doteq 1.036216672043, \text{ and}\\
c_{1,1} &:= \frac{i_4}{\zeta(4)} \doteq 0.957400377048.
\end{aligned}$$

For $p_8(v,w) = v^8 + 14v^4w^4 + w^8$, define

$$\begin{aligned}
s_0' &:= \sum_{\substack{1\le v<w\\ v\not\equiv w \pmod 2}} \frac{1}{\sqrt{p_8(v,w)}} \doteq 0.064679702530,\\
s_1' &:= \sum_{\substack{1\le v<w\\ 2\nmid vw}} \frac{1}{\sqrt{p_8(v,w)}} \doteq 0.016169925632,
\end{aligned}$$

and let

$$\begin{aligned}
c_{2,1} &:= \frac{16\alpha_2}{15\zeta(2)\zeta(4)}(s_0' + 4s_1') \doteq 0.035515448016,\\
c_{1,2} &:= -\frac{3\alpha_2}{\zeta(2)} - c_{2,1} \doteq -0.871250852070.
\end{aligned}$$

3 Characterizing elliptic curves with Galois-stable cyclic subgroups of order 4

For Lemma 1, Propositions 1 and 3, and Corollary 1, we remove our restriction that our elliptic curve be defined over $\mathbf{Q}$. Let K be a field of characteristic other than 2.

Lemma 1 *Let E be an elliptic curve defined over K. Let E be given by $y^2 = (x-\rho_1)(x-\rho_2)(x-\rho_3)$. The four 4-torsion points doubling to the 2-torsion point $(\rho_1, 0)$ have coordinates*

$$(\rho_1 \pm \sqrt{\rho_1-\rho_2}\sqrt{\rho_1-\rho_3}, \pm\sqrt{\rho_1-\rho_2}\sqrt{\rho_1-\rho_3}(\sqrt{\rho_1-\rho_2} \pm \sqrt{\rho_1-\rho_3}))$$

where the first and third $\pm$ must agree.

Proof The proof is a straightforward computation. This result appeared in [7, p. 112].

Proposition 1 and Corollary 1 were independently proven in Lemma 5.1.3 and the proof of Proposition 5.1.4 in [2].

Proposition 1 *Let R be a point of order 4 on the elliptic curve E/K. The following are equivalent.*

i) The group $\langle R\rangle$ is Galois-stable.
ii) For all $\sigma \in \mathrm{Gal}_K$ (the absolute Galois group of K), we have $\sigma R = \pm R$.
iii) We have $x(R) \in K$ (where $x(R)$ denotes the x-coordinate of R).
iv) E/K has a model $y^2 = x(x^2+\gamma x+\delta^2)$ with $\gamma \in K$, $\delta \in K^\times$, and $\gamma^2 - 4\delta^2 \neq 0$ where $x(R) \in \{\pm\delta\}$ and $2R = (0, 0)$.

Proof It is clear that i) and iii) are each equivalent to ii). Let us prove ii) implies iv). Assume for all $\sigma \in \mathrm{Gal}_K$, that $\sigma R = \pm R$. Then $\sigma(2R) = 2R$ so $2R \in E(K)[2]$ (the 2-torsion subgroup of $E(K)$). So E has a model $y^2 = x(x^2+\gamma x+\epsilon)$ with $\gamma, \epsilon \in K$ and $2R = (0, 0)$. Since the cubic in x cannot have repeated roots we have $\epsilon \in K^\times$ and $\gamma^2 - 4\epsilon \neq 0$. From Lemma 1, $x(R) \in \{\pm\sqrt{\epsilon}\}$. Since ii) implies iii), we have $\epsilon = \delta^2$ for some $\delta \in K^\times$.

Now we prove iv) implies i). It is a straightforward calculation that the two points with x-coordinate δ, the point $(0, 0)$, and the $\mathcal{O}$-point of the elliptic curve form a Galois-stable cyclic group of order 4. The same is true if we replace δ by $-\delta$ in the previous sentence.

Corollary 1 *The Galois-stable cyclic subgroups of order 4 of E/K, with model $y^2 = x(x^2+\gamma x+\delta^2)$, come in pairs where the x-coordinate of the generators of one subgroup is the negative of the x-coordinate of the generators of the other. The intersection of the two groups of order 4 is the subgroup of each of order 2. The point generating this subgroup of order 2 is K-rational.*

Proof This follows from the proof of Proposition 1.

Temporarily, we return to an elliptic curve $E/\mathbf{Q}$. Note the number of points of order 4 on E over the algebraic closure of $\mathbf{Q}$ is 12. So E has six cyclic subgroups of order 4. Thus, there are at most three pairs of Galois-stable subgroups. In Proposition 3, we will show it is impossible to have three pairs of Galois-stable cyclic subgroups of order 4 over $\mathbf{Q}$. Note, when we refer to a pair of Galois-stable subgroups, we mean that each subgroup within the pair is itself Galois-stable.

Proposition 2 *The elliptic curve $E/\mathbf{Q}$ has two pairs of Galois-stable cyclic subgroups of order 4 if and only if $E/\mathbf{Q}$ has exactly one model of the form*

$$y^2 = x(x-r)\Big(x - r\Big(\frac{1-\tau^2}{1+\tau^2}\Big)^2\Big) \tag{1}$$

with r a squarefree positive integer and $\tau \in \mathbf{Q}$, with $0 < \tau < 1$.

Proof Assume E has two pairs of such subgroups, namely $\{G_1, G_2\}$ and $\{G_3, G_4\}$. Assume $G_1 \cap G_2 = \langle T_1 \rangle$ and $G_3 \cap G_4 = \langle T_2 \rangle$ where T_1, T_2 are points of order 2. There are exactly four points of order 4 which double to T_1 and those are the generators of G_1 and G_2. So $T_2 \neq T_1$. We see T_1, T_2 generate $E[2]$, which from Corollary 1 is contained in $E(\mathbf{Q})$. Combining this with the fact that E has at least one pair of such subgroups, we get, from Proposition 1, that E has a model $y_1^2 = x_1(x_1 - r_1)(x_1 - r_1\beta_1^2)$ with r_1 a nonzero integer and $\beta_1 \in \mathbf{Q} \setminus \{-1, 0, 1\}$ (so that the cubic does not have a double root).

Without loss of generality, assume $T_1 = (0, 0)$ and $T_2 = (r_1, 0)$. We make the change of variables $x_2 := x_1 - r_1$ and get the model for E given by $y_1^2 = x_2(x_2 + r_1)(x_2 + r_1(1 - \beta_1^2))$ or $y_1^2 = x_2(x_2^2 + r_1(2 - \beta_1^2)x_2 + r_1^2(1 - \beta_1^2))$. Note T_2 has coordinates $(x_2, y_1) = (0, 0)$. Given that E has a pair of such subgroups, each containing T_2, we see from Proposition 1 that $1 - \beta_1^2 = \eta_1^2$ for some $\eta_1 \in \mathbf{Q}^\times$. We know from a famous parametrization of the unit circle that $\eta_1 = (1 - \tau_1^2)/(1 + \tau_1^2)$ for some $\tau_1 \in \mathbf{Q}$, with $0 < \tau_1 < 1$ (we remove $\tau_1 = 0, 1$ from consideration as the cubic has a double root in those cases). There is a unique choice of τ_1 since $(1 - \tau_1^2)/(1 + \tau_1^2)$ is monotonic on $0 < \tau_1 < 1$.

There is a unique change in variables, by scaling x_2 and y_1 to x_3 and y_2, respectively, so that $E/\mathbf{Q}$ has form $y_2^2 = x_3(x_3 - r_2)(x_3 - r_2((1-\tau_1^2)/(1+\tau_1^2))^2)$ with r_2 a non-zero squarefree integer. Namely, let r_2 be the unique nonzero squarefree integer such that there exists $\gamma_1 \in \mathbf{Q}^*$ such that $r_1 = \gamma_1^2 r_2$. Then we let $x_3 := x_2/\gamma_1^2$ and $y_2 := y_1/\gamma_1^3$.

To look for other possible models of $E/\mathbf{Q}$, as specified in the statement of this proposition, we translate each of the two non-zero roots of $x_3(x_3 - r_2)(x_3 - r_2((1 - \tau_1^2)/(1 + \tau_1^2))^2)$ to zero. First, let $x_4 := x_3 - r_2$. We get

$$y_2^2 = x_4(x_4 + r_2)\Big(x_4 + r_2\Big(\frac{2\tau_1}{1+\tau_1^2}\Big)^2\Big) \text{ or } y_2^2 = x_4(x_4 - r_3)\Big(x_4 - r_3\Big(\frac{1-\tau_2^2}{1+\tau_2^2}\Big)^2\Big)$$

where $r_3 := -r_2$ and $\tau_2 := \frac{1-\tau_1}{1+\tau_1}$. This is of the form of (1).

Second, let $x_5 := x_3 - r_2((1 - \tau_1^2)/(1 + \tau_1^2))^2$. When we make the substitution, the coefficient of x_5 in the model for the elliptic curve is $-(2r_2(\tau_1^3 - \tau_1)/(\tau_1^2 + 1)^2)^2$ and hence cannot be a square. So from Proposition 1, we do not get a third model of the form specified in 1.

Given that r_2 is non-zero, exactly one of r_2 and r_3 is positive — that is the one we choose for our model.

The proof of the reverse implication is a straightforward computation using Proposition 1, its proof, and Corollary 1.

Proposition 3 *Let K be a field of characteristic other than 2. Assume E/K has two pairs of Galois-stable cyclic subgroups of order 4. Then the other pair of cyclic subgroups of order 4 are defined over K if and only if K contains i. In the case that K contains i, the other pair of cyclic subgroups of order 4 will each be Galois-stable.*

Proof Identify $E[4]$ with $(\mathbf{Z}/4\mathbf{Z})^2$. Without loss of generality, we can identify the two pairs of Galois-stable cyclic subgroups of order 4 with the following pairs of generators: $\{(1,0),(1,2)\}$ and $\{(0,1),(2,1)\}$. Then the image $\overline{\rho}_{E,4}(\mathrm{Gal}_K)$ of the mod 4 representation contains only diagonal matrices. This image fixes the groups in the third pair (with generators $\{(1,1),(3,1)\}$) if and only if the determinant of each element of $\overline{\rho}_{E,4}(\mathrm{Gal}_K)$ is 1. Since the 4-Weil pairing is bilinear, non-degenerate, and compatible with the Galois-actions on $E[4]$ and the 4th roots of unity, the latter is true if and only if K contains i.

This result shows that no elliptic curve $E/\mathbf{Q}$ has more than 2 pairs of Galois-stable cyclic subgroups of order 4.

4 Counting elliptic curves with at least one pair of Galois-stable cyclic subgroups of order 4

From now on, our elliptic curves will be defined over $\mathbf{Q}$. A given $E/\mathbf{Q}$ has a unique model of the form $y^2 = x^3 + Ax + B$ where $A, B \in \mathbf{Z}$ and there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$. We define the height of $E/\mathbf{Q}$ to be $\max\{|4A^3|, |27B^2|\}$. This gives a bijection between $E/\mathbf{Q}$ and pairs (A, B), as described above, for which $4A^3 + 27B^2 \neq 0$. We will count such pairs (A, B) for which $y^2 = x^3 + Ax + B$ has height at most $X \geq 1$ and at least one pair of Galois-stable cyclic subgroups of order 4.

The results in the following paragraphs up to Proposition 4 can be found in [2, pp. 30 - 33]. From Corollary 1, $E/\mathbf{Q}$ has a pair of Galois-stable cyclic subgroups of order 4 if and only if there exists a rational number b, a root of $x^3 + Ax + B$, and when we replace x by $x + b$ the coefficient of x is a square. Note that since $x^3 + Ax + B$ is monic and $A, B \in \mathbf{Z}$, we can replace the word rational in the previous sentence by the word integer. If we replace x by $x + b$ in $x^3 + Ax + B$ we get $x^3 + 3bx^2 + (3b^2 + A)x + (b^3 + Ab + B)$. So we are looking for integers b for which there is an integer a such that $3b^2 + A = a^2$. We now have a map sending the integer pair (a, b) to the integer pair $(A, B) = (a^2 - 3b^2, 2b^3 - a^2b)$.

Given a height bound $X \geq 1$, we define a region, which we denote

$$\mathcal{R}_1'(X) := \{(a,b) \in \mathbf{R} \times \mathbf{R} \ : \ 4|a^2 - 3b^2|^3 \leq X \text{ and } 27|2b^3 - a^2b|^2 \leq X\}.$$

Most lattice points $(a, b) \in \mathcal{R}_1'(X)$ give rise to a pair $(E/\mathbf{Q}, \mathcal{T})$ where $\mathcal{T}$ is a pair of Galois-stable cyclic subgroups of E of order 4. The exceptions are those lattice points giving singular curves. That occurs when $0 = 4A^3 + 27B^2 = 4(a^2 - 3b^2)^3 + 27(a^2b - 2b^3) = 4a^6 - 9b^2a^4 = a^4(4a^2 - 9b^2)$. So we must

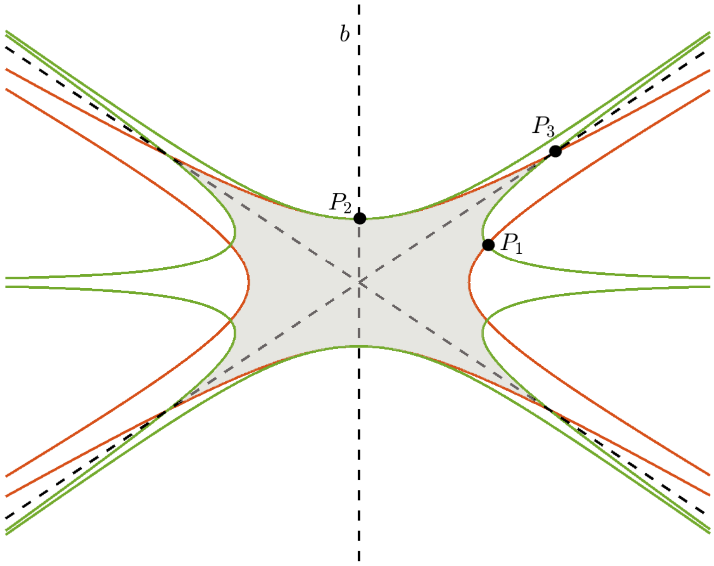

Fig. 1 The region $\mathcal{R}_1'(1)$

remove from consideration the points in $\mathcal{R}_1'(X)$ on the singular locus: $a = 0$ and $a = \pm 3b/2$.

In Figure 1, the shaded region indicates $\mathcal{R}_1'(1)$. To avoid clutter, we include only the b-axis. The red curve is the graph of $4|a^2 - 3b^2|^3 = 1$ and the green curve is the graph of $27|2b^3 - a^2b|^2 = 1$. The green components $2b^3 - a^2b = \sqrt{1/27}$ for $b > 0$ and $2b^3 - a^2b = -\sqrt{1/27}$ for $b < 0$ are superfluous as boundaries of $\mathcal{R}_1'(1)$.

For $i = 1, 2, 3$, each point P_i is an intersection point of $4|a^2 - 3b^2|^3 = 1$ with $27|2b^3 - a^2b|^2 = 1$. The b-coordinates of P_1, P_2, and P_3 are α_1, α_2, and $2\alpha_2$, respectively. See Section 2 for the definitions of the α_i's. Again referring to Section 2, we can see from these b-coordinates and curve equations that i_4 gives the area of the part of $\mathcal{R}_1'(1)$ with $a \geq 0$. We restrict to $a \geq 0$ since the pairs (a, b) and $(-a, b)$ give the same pair (A, B). The singular locus is indicated by dashed lines.

An easy exercise shows that for all primes ℓ we have $\ell^4 \mid A$ and $\ell^6 \mid B$ if and only if $\ell^2 \mid a$ and $\ell^2 \mid b$. Let $\mathcal{R}_1(X)$ be the subset of $\mathcal{R}_1'(X)$ for which $a \geq 0$. If we remove from $\mathcal{R}_1(X)$ the lattice points (a, b) on the singular locus, and those for which there is a prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$, then we get an injection from the remaining lattice points to pairs $(E/\mathbf{Q}, \mathcal{T})$, where $\mathcal{T}$ is a pair of Galois-stable cyclic subgroups of order 4.

Recall that $N_j(X)$ is the number of $E/\mathbf{Q}$ with at least j pairs of Galois-stable cyclic subgroups of order 4. From Proposition 3, it is impossible for $E/\mathbf{Q}$ to have three pairs of Galois-stable cyclic subgroups of order 4. Thus, the number of lattice points in $\mathcal{R}_1(X)$, not on the singular locus, and for which there is no prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$, gives the number of $E/\mathbf{Q}$ for which there is exactly one pair of Galois-stable cyclic subgroups of order 4 plus twice the number of $E/\mathbf{Q}$ for which there is exactly two pairs. We restate this result in the following proposition.

Proposition 4 *The number $N_1(X) + N_2(X)$ is equal to the number of lattice points in $\mathcal{R}_1(X)$, not on $a = 0$ or $a = 3|b|/2$, and for which there is no prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$.*

Proof This follows from [2, pp. 30-33] and Proposition 3.

With the above proposition and an important result of Huxley [5], we can estimate the count. The Huxley result asserts that if $\mathcal{R}$ is a compact, convex region in the plane, of area A, and with the boundary being piecewise smooth, with the curvature on each piece non-zero and 3 times continuously differentiable, then the number of lattice points (i.e., integer points) contained in $\mathcal{R}$ scaled by a large factor r is $Ar^2 + O(r^{0.63})$. (The actual error bound is $r^{131/208}(\log r)^{O(1)}$, see [5, p. 592].) We would like to apply this theorem to $\mathcal{R}_1'(X)$, which is a compact region with piecewise smooth boundary and non-zero curvature scaled by a factor $X^{1/6}$, however, the boundary segments are concave with respect to the interior, not convex. We can nevertheless apply the Huxley theorem by recognizing the region as the union of differences of convex sets with boundaries being piecewise smooth and with nonzero curvature. (A simple example is a lune, which is the difference of two convex sets.) Since the area of $\mathcal{R}_1'(X)$ is $2i_4X^{1/3}$ (see Section 2), it follows that the number of lattice points in $\mathcal{R}_1'(X)$ is equal to $2i_4X^{1/3} + O(X^{0.105})$.

We next want to count the number of lattice points in $\mathcal{R}_1'(X)$ for which there is no prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$. For a given positive integer d, the number of lattice points $(a, b) \in \mathcal{R}_1'(X)$ for which $d^2 \mid a$ and $d^2 \mid b$ is equal to the number of lattice points in $\mathcal{R}_1'(X)$ when it has been scaled down by d^2 in both dimensions. Since the number of lattice points in this scaled down region is $2i_4X^{1/3}/d^4 + O((X^{1/6}/d^2)^{0.63})$, the number of lattice points in $\mathcal{R}_1'(X)$ for which there is no prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$ is

$$\sum_{d \leq \sqrt{\alpha_2}X^{1/12}} \left(\frac{2i_4\mu(d)}{d^4} X^{1/3} + O\Big(\frac{X^{0.105}}{d^{1.26}}\Big) \right) = \frac{2i_4}{\zeta(4)} X^{1/3} + O(X^{0.105}).$$

Here, we used that $\sum_d \mu(d)/d^4 = 1/\zeta(4)$ and that the error in truncating this sum at $\sqrt{\alpha_2}X^{1/12}$ is, by an elementary argument, $O(1/X^{1/4})$.

As lattice points on $a = 0$ give singular curves $y^2 = x^3 + Ax + B$, we are ultimately interested in lattice points with $a > 0$. The lattice points on $a = 0$ in $\mathcal{R}_1'(X)$ are the points $(0, b)$ with $|b| \leq \alpha_2X^{1/6}$. For such points, there is a prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$ if and only if $\ell^2 \mid b$. So the number of lattice points in $\mathcal{R}_1'(X)$ on $a = 0$ for which there is no prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$ is $\frac{2\alpha_2}{\zeta(2)}X^{1/6} + O(X^{1/12})$, arguing as above. Thus, the number of lattice points in $\mathcal{R}_1(X)$ with $a > 0$ and for which there is no prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$ is $\frac{i_4}{\zeta(4)}X^{1/3} - \frac{\alpha_2}{\zeta(2)}X^{1/6} + O(X^{0.105})$. Recall $c_{1,1} = \frac{i_4}{\zeta(4)}$.

The remaining pairs (a, b) giving singular curves $y^2 = x^3 + Ax + B$ are those on $a = 3|b|/2$. We have already removed those for which $\ell^2 \mid a$ and $\ell^2 \mid b$. The part of $a = 3|b|/2$ in $\mathcal{R}_1(X)$ is that for which $|b| \leq 2\alpha_2 X^{1/6}$. The lattice points on $a = 3|b|/2$ are of the form $(3|k|, 2k)$ for $k \in \mathbf{Z}$ with $|k| \leq \alpha_2 X^{1/6}$. So there are $2\alpha_2 X^{1/6} + O(1)$ of them. If ℓ is prime then $\ell^2 \mid 2k$ and $\ell^2 \mid 3|k|$ if and only if $\ell^2 | k$. So the number of lattice points on $a = 3|b|/2$ in $\mathcal{R}_1(X)$ for which there is no prime ℓ such that $\ell^2 \mid a$ and $\ell^2 \mid b$ is $\frac{2\alpha_2}{\zeta(2)} X^{1/6} + O(X^{1/12})$. Thus $N_1(X) + N_2(X) = c_{1,1}X^{1/3} - \frac{3\alpha(2)}{\zeta(2)} X^{1/6} + O(X^{0.105})$. We show in Theorem 2 that the number of $E/\mathbf{Q}$ of height at most X with two pairs of Galois-stable cyclic subgroups of order 4 is $N_2(X) = c_{2,1}X^{1/6} + O(X^{1/12})$.

Recall $c_{1,1} \doteq 0.957400377048$ and $c_{1,2} = -\frac{3\alpha_2}{\zeta(2)} - c_{2,1} \doteq -0.871250852070$ (see Section 2).

Theorem 1 *The number of $E/\mathbf{Q}$ of height at most X with at least one pair of Galois-stable cyclic subgroups is* $N_1(X) = c_{1,1}X^{1/3} + c_{1,2}X^{1/6} + O(X^{0.105})$.

Proof This follows from Proposition 4 and the computations above.

4.1 Numerical illustration — one pair

In this section we numerically illustrate Theorem 1. In the table below we present $N_1(X)$ and $N_1(X) - c_{1,1}X^{1/3} - c_{1,2}X^{1/6}$ (which we round to one digit past the decimal point) for various values of X.

X	$N_1(X)$	$N_1(X) - c_{1,1}X^{1/3} - c_{1,2}X^{1/6}$
10^{18}	956574	44.9
10^{21}	9571217	−31.6
10^{24}	95731445	119.8
10^{27}	957372610	−215.7
10^{30}	9573916722	76.6

5 Counting elliptic curves with two pairs of Galois-stable cyclic subgroups of order 4

5.1 The parametrization

In this section, we want to find an integer parametrization of elliptic curves with two pairs of Galois-stable cyclic subgroups of order 4. From Proposition 2 such an elliptic curve has a model of the form in 1 with r a squarefree positive integer, $\tau \in \mathbf{Q}$ and $0 < \tau < 1$.

We want to find a model for such an elliptic curve of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbf{Z}$, and for which there is no prime ℓ such that $\ell^4 \mid A$

and $\ell^6 \mid B$. In the model given by (1), we replace τ by v/w where v, w are variables representing relatively prime integers with $1 \le v < w$. Then we replace x by $(x + 6r(v^4 + w^4))/(9(v^2 + w^2)^2)$ and y by $y/(27(v^2 + w^2)^3)$. We get $y^2 = x^3 + Ax + B$ where $A = -27r^2(v^8 + 14v^4w^4 + w^8)$ and $B = 54r^3(v^{12} - 33v^8w^4 - 33v^4w^8 + w^{12})$. Set

$$p_8(v, w) := v^8 + 14v^4w^4 + w^8, \quad p_{12}(v, w) := v^{12} - 33v^8w^4 - 33v^4w^8 + w^{12}.$$

We now need to ensure there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

Lemma 2 *Let $1 \le v < w$ with $\gcd(v, w) = 1$. If $2 \mid vw$, then $\gcd(p_8(v, w), p_{12}(v, w)) = 1$. If $2 \nmid vw$, then $16 \mid p_8(v, w)$, $64 \mid p_{12}(v, w)$, and $\gcd(\frac{1}{16}p_8(v, w), \frac{1}{64}p_{12}(v, w)) = 1$.*

Proof The homogeneous resultant of p_8 and p_{12} is $2^{40}3^{12}$. Since $\gcd(v, w) = 1$, any prime divisor of both $p_8(v, w)$ and $p_{12}(v, w)$ is $\ell = 2$ or $\ell = 3$. We check all nine cases for v and w mod 3 and note that $3 \mid p_8(v, w)$ and $3 \mid p_{12}(v, w)$ if and only if $3 \mid v$ and $3 \mid w$.

We check all four cases for v and w mod 2 and note that $2 \mid p_8(v, w)$ and $2 \mid p_{12}(v, w)$ if and only if $v \equiv w \pmod 2$. Since $\gcd(v, w) = 1$ it suffices to consider the case $v \equiv w \equiv 1 \pmod 2$. A straightforward exercise shows then that $p_8(v, w) \equiv 16 \pmod{64}$ and $p_{12}(v, w) \equiv -64 \pmod{256}$. Therefore $\gcd(\frac{1}{16}p_8(v, w), \frac{1}{64}p_{12}(v, w)) = 1$.

Define the functions $A(r, v, w)$ and $B(r, v, w)$ in the following way.

(i) $A(r, v, w) := -27r^2p_8(v, w)$, $B(r, v, w) := 54r^3p_{12}(v, w)$ when $3 \nmid r$ and $2 \mid vw$,
(ii) $A(r, v, w) := -\frac{1}{3}r^2p_8(v, w)$, $B(r, v, w) := \frac{2}{27}r^3p_{12}(v, w)$ when $3 \mid r$ and $2 \mid vw$,
(iii) $A(r, v, w) := -\frac{27}{16}r^2p_8(v, w)$, $B(r, v, w) := \frac{27}{32}r^3p_{12}(v, w)$ when $3 \nmid r$ and $2 \nmid vw$, and
(iv) $A(r, v, w) := -\frac{1}{48}r^2p_8(v, w)$, $B(r, v, w) := \frac{1}{864}r^3p_{12}(v, w)$ when $3 \mid r$ and $2 \nmid vw$.

Lemma 3 *Let E be the elliptic curve with two pairs of Galois-stable cyclic subgroups of order 4 given by the model in (1). Let $\tau = v/w$ with $v, w \in \mathbf{Z}$, $1 \le v < w$, and $\gcd(v, w) = 1$. The unique model for E of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbf{Z}$ and for which there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$ is given by $A = A(r, v, w)$ and $B = B(r, v, w)$.*

Proof At the beginning of this section we found that E has an integer model $y^2 = X^3 + Ax + B$ with $A = -27r^2p_8(v, w)$ and $B = 54r^3p_{12}(v, w)$.

Now we consider the cases where there is a prime ℓ with $\ell^4 \mid A$ and $\ell^6 \mid B$. Given Lemma 2 and that r is squarefree, $A = -27r^2p_8(v, w)$, and $B = 54r^3p_{12}(v, w)$, the only possible primes ℓ are $\ell = 2, 3$. We see that $3^4 \mid A$ and $3^6 \mid B$ if and only if $3 \mid r$. If $3 \mid r$ then replace A by $A/3^4$ and replace B by $B/3^6$. From Lemma 2, we have that $2^4 \mid A$ and $2^6 \mid B$ if and only if $2 \nmid vw$, and in this case $A/2^4$ and $B/2^6$ are odd. In this case replace A by $A/2^4$ and B by $B/2^6$.

Now there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

Recall that the height of the elliptic curve $y^2 = x^3 + Ax + B$, where $A, B \in \mathbf{Z}$, is at most X if and only if $|A| \le A_b$ and $|B| \le B_b$ where $A_b := \frac{1}{4^{1/3}} X^{1/3}$ and $B_b := \frac{1}{27^{1/2}} X^{1/2}$.

Lemma 4 *Assume the elliptic curve $y^2 = x^3 + Ax + B$, where $A, B \in \mathbf{Z}$, has two pairs of Galois-stable cyclic subgroups of order 4. The height of this elliptic curve is at most X if and only if $|A| \le A_b$ where $A_b := \frac{1}{4^{1/3}} X^{1/3}$.*

Proof Since the elliptic curve has two Galois-stable cyclic subgroups of order 4, the polynomial $x^3 + Ax + B$ has three rational roots from Proposition 2. Therefore the discriminant of $x^3 + Ax + B$ is positive. Thus $-4A^3 - 27B^2 > 0$. Thus $-4A^3 > 27B^2 \ge 0$. Thus $\max\{|4A^3|, |27B^2|\} = |4A^3|$. So the height of this elliptic curve is $|4A^3|$.

5.2 Bijections used in counting

We gave a homogeneous integer parametrization in Lemma 3 for $E/\mathbf{Q}$ with two pairs of Galois-stable cyclic subgroups of order 4. A dehomogenization of this parametrization to a rational parametrization satisfies the conditions of [4, Prop. 4.1]. It follows that if $\mathcal{S}_{\text{pairs}}$ is the set of integer pairs (A, B) such that there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$, and $y^2 = x^3 + Ax + B$ is an elliptic curve of height at most X with two pairs of Galois-stable cyclic subgroups of order 4, then $\#\mathcal{S}_{\text{pairs}}$ is of order of magnitude $X^{1/6}$. We will prove an even stronger result.

Let $\mathcal{S}_E$ denote the set of $E/\mathbf{Q}$ (up to isomorphism), with two pairs of Galois-stable cyclic subgroups of order 4 and height at most X. In this section we determine an asymptotic plus error estimate for the size of $\mathcal{S}_E$. There is a bijection from $\mathcal{S}_{\text{pairs}}$ to $\mathcal{S}_E$ sending (A, B) to the elliptic curve $y^2 = x^3+Ax+B$.

Let $\mathcal{S}_{r,v,w}$ denote the set of triples (r, v, w) with r a squarefree positive integer, $v, w \in \mathbf{Z}$ with $1 \le v < w$, $\gcd(v, w) = 1$, and $|A(r, v, w)| \le A_b$.

Proposition 5 *There is a bijection between $S_{r,v,w}$ and $\mathcal{S}_{\text{pairs}}$ sending (r, v, w) to $(A(r, v, w), B(r, v, w))$.*

Proof This follows from Lemmas 3 and 4, where we take $\theta = 1, \frac{1}{3}, \frac{1}{2}, \frac{1}{6}$ in Cases (i) - (iv) (listed before Lemma 3) respectively.

To determine the size of the set $\mathcal{S}_E$ we will instead determine the identical size of the set $\mathcal{S}_{r,v,w}$. We see, from the four cases presented immediately before Lemma 3, that we want to count the number of triples (r, v, w) of positive integers with $r^2 p_8(v, w) \le \eta X^{1/3}$ for η a constant, r squarefree, $v < w$, and $\gcd(v, w) = 1$.

5.3 Useful constants

In (r, v, w)-space, the region with all variables positive and $r^2 p_8(v, w) \leq \eta X^{1/3}$ (for $\eta < 1$ a constant) can be considered to have two tails — one for r large and one for p_8 large. Our counting argument of valid triples (r, v, w) requires us to consider those tails differently. In particular, the Principle of Lipschitz, commonly used in similar counting arguments, is useful in only one of the tails. Certain constants arise within the counting argument for each tail and we compute them here. As the function $A(r, v, w)$ depends on the residue classes of v and w modulo 2, we will need to take that into consideration when dealing with these constants. For $i, j \in \{0, 1\}$, with $(i, j) \neq (0, 0)$, let

$$T_{ij} = \{(v, w) \in \mathbf{Z}^2 \mid v \equiv i \pmod 2,\ w \equiv j \pmod 2\}.$$

The following proposition will be useful when computing the number of lattice points in the tail with p_8 large.

Proposition 6 *Let*

$$\alpha_3 = \int_0^1 \frac{1}{\sqrt{p_8(u, 1)}}\, du \doteq 0.691002044641$$

and let

$$\alpha_4 = \int_1^2 \int_{g(t)}^1 \frac{1}{\sqrt{p_8(u, 1)}}\, du\, dt \doteq 0.122364455649$$

where $g(t) = ((t^4 + 48)^{1/2} - 7)^{1/4}$. *Then for* $y \geq 1$,

$$\sum_{\substack{1 \leq v < w \\ p_8(v,w) > y \\ (v,w) \in T_{i,j}}} \frac{1}{\sqrt{p_8(v, w)}} = \frac{\alpha_3 + \alpha_4}{8 y^{1/4}} + O\Big(\frac{1}{y^{3/8}}\Big).$$

Proof For each fixed value of $w > y^{1/8}$ and all v with $1 \leq v < w$, we have $p_8(v, w) > y$. Further

$$\sum_{\substack{1 \leq v < w \\ v \equiv i \pmod 2}} \frac{1}{\sqrt{p_8(v, w)}} = \frac{1}{w^4} \sum_{\substack{1 \leq v < w \\ v \equiv i \pmod 2}} \frac{1}{\sqrt{p(v/w, 1)}}$$

$$= \frac{1}{2w^3} \sum_{\substack{1 \leq v < w \\ v \equiv i \pmod 2}} \frac{1}{\sqrt{p(v/w, 1)}} \cdot \frac{2}{w}.$$

This last sum is a Riemann sum for the integral α_3, and by monotonicity is equal to $\alpha_3 + O(1/w)$. Thus,

$$\sum_{\substack{1 \leq v < w \\ v \equiv i \pmod 2}} \frac{1}{\sqrt{p_8(v, w)}} = \frac{\alpha_3}{2w^3} + O\left(\frac{1}{w^4}\right).$$

Summing this expression for $w > y^{1/8}$ gives

$$\sum_{\substack{w>y^{1/8}\\ w\equiv j \pmod 2}} \frac{\alpha_3}{2w^3} + O\left(\frac{1}{w^4}\right) = \sum_{k>y^{1/8}/2}\left(\frac{\alpha_3}{2(2k+j)^3} + O\Big(\frac{1}{k^4}\Big)\right),$$

which is equal to $\frac{\alpha_3}{8y^{1/4}} + O(\frac{1}{y^{3/8}})$.

We now consider the case $w \le y^{1/8}$. For $p_8(v,w) > y$ with $1 \le v < w$, it is necessary that $w > y^{1/8}/\sqrt{2}$. For a given value of w we sum on v, noting that $g(y^{1/4}/w^2)w \le v < w$. Thus, we have the contribution

$$\sum_{\substack{g(y^{1/4}/w^2)w\le v<w\\ v\equiv i \pmod 2}} \frac{1}{\sqrt{p_8(v,w)}} = \frac{1}{2w^3}\int_{g(y^{1/4}/w^2)}^{1} \frac{1}{\sqrt{p_8(u,1)}}\,du + O\Big(\frac{1}{w^4}\Big).$$

We now sum this expression on w with $y^{1/8}/\sqrt{2} < w \le y^{1/8}$, $w \equiv j \pmod 2$ getting

$$\begin{aligned}
&\sum_{\substack{y^{1/8}/\sqrt{2}<w\le y^{1/8}\\ w\equiv j \pmod 2}} \left(\frac{1}{2w^3}\int_{g(y^{1/4}/w^2)}^{1}\frac{1}{\sqrt{p_8(u,1)}}\,du + O\Big(\frac{1}{w^4}\Big)\right)\\
&\quad = \frac{1}{2}\int_{y^{1/8}/\sqrt{2}}^{y^{1/8}} \frac{1}{2x^3}\int_{g(y^{1/4}/x^2)}^{1}\frac{1}{\sqrt{p_8(u,1)}}\,du\,dx + O\Big(\frac{1}{y^{3/8}}\Big)\\
&\quad = \frac{1}{8y^{1/4}}\int_1^2\int_{g(t)}^{1}\frac{1}{\sqrt{p_8(u,1)}}\,du\,dt + O\Big(\frac{1}{y^{3/8}}\Big),
\end{aligned}$$

where we use the substitution $t = y^{1/4}/x^2$. This gives the contribution $\frac{\alpha_4}{8y^{1/4}} + O(\frac{1}{y^{3/8}})$, completing the proof.

Corollary 2 *We have*

$$\sum_{\substack{1\le v<w\\ \gcd(v,w)=1\\ p_8(v,w)>y\\ (v,w)\in T_{ij}}} \frac{1}{\sqrt{p_8(v,w)}} = \frac{\alpha_3+\alpha_4}{6\zeta(2)y^{1/4}} + O\Big(\frac{\log y}{y^{3/8}}\Big).$$

Proof First note that

$$\sum_{\substack{1\le v<w\\ d\,|\,v,\, d\,|\,w}} \frac{1}{\sqrt{p_8(v,w)}} = \frac{1}{d^4}\sum_{1\le v<w}\frac{1}{\sqrt{p_8(v,w)}} = O\Big(\frac{1}{d^4}\Big).$$

Thus,

$$\sum_{\substack{1\le v<w\\ \gcd(v,w)=1\\ p_8(v,w)>y\\ (v,w)\in T_{ij}}} \frac{1}{\sqrt{p_8(v,w)}} = \left(\sum_{\substack{d\le y^{1/8}\\ d\,\mathrm{odd}}}\ \sum_{\substack{1\le v<w\\ d\,|\,v,\, d\,|\,w\\ p_8(v,w)>y\\ (v,w)\in T_{ij}}} \frac{\mu(d)}{\sqrt{p_8(v,w)}}\right) + O\Big(\frac{1}{y^{3/8}}\Big),$$

recalling that $\mu(d)$ denotes the Möbius function. By Proposition 6, the double sum here is

$$\sum_{\substack{d\le y^{1/8}\\ d\,\mathrm{odd}}}\frac{\mu(d)}{d^4}\left(\frac{\alpha_3+\alpha_4}{8(y/d^8)^{1/4}}+O\Big(\frac{1}{(y/d^8)^{3/8}}\Big)\right)=\frac{\alpha_3+\alpha_4}{6\zeta(2)y^{1/4}}+O\Big(\frac{\log y}{y^{3/8}}\Big),$$

completing the proof. The last step used the fact that for p prime, $h>1$ an integer, and $x\ge 1$, we have

$$\sum_{n\le x,\,p\nmid n}\frac{\mu(n)}{n^h}=\frac{1}{\zeta(h)(1-p^{-h})}+O\left(\frac{1}{(h-1)x^{h-1}}\right). \tag{2}$$

Indeed, the infinite sum has an Euler product which we recognize as $1/(\zeta(h)$ $(1-p^{-h}))$. Further, the tail for $n>x$ converges absolutely to a sum that is $O(1/((h-1)x^{h-1}))$.

The following proposition will be useful when computing the number of lattice points in the tail with r large.

Proposition 7 *Let $z\ge 1$ and let $\mathcal{R}_2(z)$ be the region in the v,w plane with*

$$0\le v\le w,\quad p_8(v,w)\le z,$$

and let $A(z)$ be the area of $\mathcal{R}_2(z)$. Then $A(z)=\beta z^{1/4}$, where

$$\beta=\frac12\int_{\pi/4}^{\pi/2}\frac{1}{p_8(1,\tan\theta)^{1/4}\cos^2\theta}\,d\theta\doteq 0.406683250145.$$

Further, the projection of $\mathcal{R}_2(z)$ on any line has length $O(z^{1/8})$.

Proof We have

$$A(z)=\int_{\pi/4}^{\pi/2}\int_0^B r\,dr\,d\theta,$$

where B is the distance to the origin of the point on $p_8(v,w)=z$ with $\theta=\arctan(w/v)$. We have at this point that $z=p_8(v,w)=p_8(1,\tan\theta)v^8$ and $w=v\tan\theta$. Thus,

$$\begin{aligned}B=(v^2+w^2)^{1/2}=v(1+\tan^2\theta)^{1/2}&=(z/p_8(1,\tan\theta))^{1/8}(1+\tan^2\theta)^{1/2}\\&=\frac{z^{1/8}}{p_8(1,\tan\theta)^{1/8}\cos\theta}.\end{aligned}$$

Thus,

$$A(z)=\int_{\pi/4}^{\pi/2}\frac12 B^2\,d\theta=\frac12 z^{1/4}\int_{\pi/4}^{\pi/2}\frac{1}{p_8(1,\tan\theta)^{1/4}\cos^2\theta}\,d\theta,$$

completing the proof. The final assertion of the lemma follows from the fact that all points $(v,w)\in\mathcal{R}_2(z)$ satisfy $\max\{|v|,|w|\}\le z^{1/8}$.

Corollary 3 *Let $z \geq 1$ and let $L(z)$ denote the number of lattice points (v,w) in $\mathcal{R}_2(z)$ with $(v,w) \in T_{i,j}$ and let $L'(z)$ be the number of lattice points (v,w) in $\mathcal{R}_2(z)$ with $(v,w) \in T_{i,j}$ and* $\gcd(v,w) = 1$. *Then*

$$L(z) = \frac{\beta}{4} z^{1/4} + O(z^{1/8}) \quad \textit{and} \quad L'(z) = \frac{\beta}{3\zeta(2)} z^{1/4} + O(z^{1/8}\log z).$$

Proof The first assertion is immediate from Proposition 7 and the Principle of Lipschitz. For the second assertion, let $L_d(z)$ be the number of lattice points $(dv, dw) \neq (0,0)$ in $\mathcal{R}_2(z)$, where d is a positive integer. We have

$$L'(z) = \sum_{d \,\mathrm{odd}} \mu(d) L_d(z) = \sum_{\substack{d < z^{1/8} \\ d \,\mathrm{odd}}} \mu(d) L_d(z),$$

since if $d \geq z^{1/8}$, then $L_d(z) = 0$. Note that $L_d(z)$ is the number of lattice points in $\mathcal{R}_2(z/d^8) \setminus \{(0,0)\}$. So, by Equation (2),

$$L'(z) = \frac{\beta}{4} z^{1/4} \sum_{\substack{d < z^{1/8} \\ d \,\mathrm{odd}}} \frac{\mu(d)}{d^2} + O\Big(z^{1/8} \sum_{\substack{d < z^{1/8} \\ d, \mathrm{odd}}} \frac{1}{d} \Big) = \frac{\beta}{3\zeta(2)} z^{1/4} + O\big(z^{1/8} \log x\big).$$

5.4 Facts from analytic number theory

We now present some useful facts from analytic number theory. Let

$$M(x) := \sum_{n \leq x} \mu(n),\ Q(x) := \sum_{n \leq x} \mu(n)^2,\ Z(x) := \sum_{n \leq x} \frac{\mu(n)}{n},\ S(x) := \sum_{n \leq x} \frac{\mu(n)^2}{\sqrt{n}}.$$

Proposition 8 *We have the following inequalities: As $x \to \infty$,*

(1) $|M(x)| \leq x/\exp((\log x)^{3/5+o(1)})$,
(2) $|Q(x) - x/\zeta(2)| \leq x^{1/2}/\exp((\log x)^{3/5+o(1)})$,
(3) $|Z(x)| \leq \exp(-(\log x)^{3/5+o(1)})$, *and*
(4) $|S(x) - (2/\zeta(2))\sqrt{x}| \leq \exp(-(\log x)^{3/5+o(1)})$.

Proof Facts (1) and (2) may be found in Walfisz [9, p. 146].

For fact (3), first note that from the prime number theorem, $\sum_{n \geq 1} \frac{\mu(n)}{n} = 0$, see [8, p. 43]. Thus, by partial (Abel) summation,

$$Z(x) = -\sum_{n > x} \frac{\mu(n)}{n} = -\int_x^\infty \frac{M(t) - M(x)}{t^2}\, dt$$

and the result follows from fact (1).

For fact (4), let $\epsilon > 0$ be arbitrarily small, and fixed. We let

$$y = \exp((\log x)^{3/5-\epsilon})$$

and let $z = (x/y)^{1/2}$. We have

$$S(x) = \sum_{n\le x}\sum_{d^2\,|\,n}\frac{\mu(d)}{\sqrt{n}} = \sum_{ad^2\le x}\frac{\mu(d)}{d\sqrt{a}}$$
$$= \sum_{a\le y}\sum_{d\le\sqrt{x/a}}\frac{\mu(d)}{d\sqrt{a}} + \sum_{d\le z}\sum_{a\le x/d^2}\frac{\mu(d)}{d\sqrt{a}} - \sum_{a\le y}\sum_{d\le z}\frac{\mu(d)}{d\sqrt{a}} = s_1 + s_2 - s_3,$$

say. Using $\sum_{a\le y} 1/\sqrt{a} = O(\sqrt{y})$, we have, as $x\to\infty$,

$$|s_1| \le \exp(-(\log x)^{3/5+o(1)}),$$

from fact (3). Almost the same calculation works for s_3. Note that

$$\sum_{n\le x} 1/\sqrt{n} = 2\sqrt{x} + \zeta(1/2) + O(1/\sqrt{x}), \text{ when } x\ge 1,$$

see Apostol [1, Theorem 3.2 (b)]. Thus,

$$s_2 = \sum_{d\le z}\frac{\mu(d)}{d}\big(2\sqrt{x/d^2} + \zeta(1/2) + O(1/\sqrt{x/d^2})\big)$$
$$= 2\sqrt{x}\sum_{d\le z}\frac{\mu(d)}{d^2} + \left(\zeta(1/2)\sum_{d\le z}\frac{\mu(d)}{d}\right) + O(z/\sqrt{x}).$$

Note that $z/\sqrt{x} = \exp(-\frac{1}{2}(\log x)^{3/5-\epsilon})$. We shall use fact (3) on the second sum here, and for the first sum,

$$\sum_{d\le z}\frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} - \sum_{d>z}\frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} - \int_z^\infty (M(t)-M(z))\cdot\frac{2}{t^3}\,dt.$$

We can estimate the integral using fact (1), so that

$$|s_2 - 2\sqrt{x}/\zeta(2)| = O\Big(\exp\big(-\frac{1}{2}(\log x)^{3/5-\epsilon}\big)\Big).$$

Since $\epsilon > 0$ is arbitrary, this completes the proof of fact (4) and the proposition.

As the definition of $A(r,v,w)$ depends on whether or not $3\mid r$, we must adapt Proposition 8 to each of these two cases. It suffices to consider the case $3\mid r$, since then the case $3\nmid r$ can be found by subtracting from the full sum. Let

$$M_3(x) := \sum_{\substack{n\le x\\ 3\,|\,n}}\mu(n),\quad Q_3(x) := \sum_{\substack{n\le x\\ 3\,|\,n}}\mu(n)^2,\quad Z_3(x) := \sum_{\substack{n\le x\\ 3\,|\,n}}\frac{\mu(n)}{n},$$

$$S_3(x) := \sum_{\substack{n\le x\\ 3\,|\,n}}\frac{\mu(n)^2}{\sqrt{n}}.$$

Corollary 4 *We have the following inequalities: As $x \to \infty$,*

1. $|M_3(x)| \le x/\exp((\log x)^{3/5+o(1)})$,
2. $|Q_3(x) - x/(4\zeta(2))| \le x^{1/2}/\exp((\log x)^{3/5+o(1)})$,
3. $|Z_3(x)| \le \exp(-(\log x)^{3/5+o(1)})$, *and*
4. $|S_3(x) - \sqrt{x}/(2\zeta(2))| \le \exp(-(\log x)^{3/5+o(1)})$.

Proof We show by induction that

$$M_3(x) = -\sum_{j\ge 1} M(x/3^j). \tag{3}$$

Indeed, this holds trivially for $x < 3$. Assume it holds for $x < 3^k$. Then for $x < 3^{k+1}$, we have

$$M_3(x) = \sum_{m\le x/3} \mu(3m) = -\sum_{\substack{m\le x/3\\ 3\nmid m}} \mu(m) = -M(x/3) + M_3(x/3),$$

and so (3) follows by using the induction hypothesis on $M_3(x/3)$. Next, (3) implies that

$$M_3(x) = -\sum_{\substack{j\ge 1\\ 3^j\le\sqrt{x}}} M(x/3^j) - \sum_{3^j>\sqrt{x}} M(x/3^j).$$

For the first sum we use (1) of Propostion 8 on each term, and for the second sum we use the trivial bound $|M(x/3^j)| \le x/3^j$, thus establishing part (1) of the corollary.

Similar induction proofs show that

$$Q_3(x) = \sum_{j\ge 1} (-1)^{j-1} Q(x/3^j), \quad Z_3(x) = -\sum_{j\ge 1} \frac{1}{3^j} Z(x/3^j), \text{ and}$$

$$S_3(x) = \sum_{j\ge 1} \frac{(-1)^{j-1}}{3^{j/2}} S(x/3^j),$$

and so parts (2)–(4) follow from parts (2)–(4) of Proposition 8.

5.5 Breaking the region into four cases

The different formulae for $A(r, v, w)$ depending on whether $3 \mid r$ and the values of v and w modulo 2 suggest that we break the computation into four cases:
(i) $3 \nmid r$, $2 \mid vw$,
(ii) $3 \mid r$, $2 \mid vw$,
(iii) $3 \nmid r$, $2 \nmid vw$, and
(iv) $3 \mid r$, $2 \nmid vw$.

We give the details in the first case, and show how the constants change in the subsequent cases. Let $N^{(\mathrm{i})}(X)$ be the number of (r,v,w) in the first of the four cases with $|A(r,v,w)| = 27r^2p_8(v,w) \le A_b$, that is, $r^2p_8(v,w) \le \frac{1}{4^{1/3}27}X^{1/3}$. Define

$$\mathcal{S}_0 := \{(v,w) \mid v \not\equiv w \,(\mathrm{mod}\ 2),\ 1 \le v < w,\ \gcd(v,w) = 1\},$$

$$s_0 := \sum_{\mathcal{S}_0} \frac{1}{\sqrt{p_8(v,w)}}.$$

Let $N^{(\mathrm{i})}(Y,X)$ be the number of triples r,v,w counted by $N^{(\mathrm{i})}(X)$ with $p_8(v,w) \le Y$, let $N_Z^{(\mathrm{i})}(Y,X)$ be the number of these triples where also $r \le Z$, and let $N_Z^{(\mathrm{i})}(X)$ be the number of triples with $r \le Z$ and $p_8(v,w)$ unrestricted. Then, if $Z^2Y = \eta X^{1/3}$, for $\eta = \frac{1}{4^{1/3}27}$, we have

$$N^{(\mathrm{i})}(X) = N^{(\mathrm{i})}(Y,X) + N_Z^{(\mathrm{i})}(X) - N_Z^{(\mathrm{i})}(Y,X).$$

We will choose $Z = X^\delta$, where $\delta > 0$ is fairly small. We then have $Y = \eta X^{1/3-2\delta}$.

The calculation of $N^{(\mathrm{i})}(Y,X)$

Let $Q_3'(x) = Q(x) - Q_3(x)$, so that from Proposition 8 and Corollary 4 we have

$$Q_3'(x) = \frac{3}{4\zeta(2)}x + R_3'(x), \text{ where } |R_3'(x)| \le x^{1/2}/\exp((\log x)^{3/5+o(1)}) \qquad (4)$$

as $x \to \infty$. Thus,

$$N^{(\mathrm{i})}(Y,X) = \sum_{\substack{(v,w)\in\mathcal{S}_0\\ p_8(v,w)\le Y}} \sum_{\substack{r \le \frac{\eta^{1/2}X^{1/6}}{\sqrt{p_8(v,w)}}\\ r \text{ squarefree}\\ 3\nmid r}} 1 \qquad (5)$$

$$= \frac{3\eta^{1/2}}{4\zeta(2)}X^{1/6} \sum_{\substack{(v,w)\in\mathcal{S}_0\\ p_8(v,w)\le Y}} \frac{1}{\sqrt{p_8(v,w)}} + \sum_{\substack{(v,w)\in\mathcal{S}_0\\ p_8(v,w)\le Y}} R_3'\Big(\frac{\eta^{1/2}X^{1/6}}{\sqrt{p_8(v,w)}}\Big).$$

Since $\eta^{1/2}X^{1/6}/\sqrt{p_8(v,w)} \ge \eta^{1/2}X^{1/6}/Y^{1/2} = \eta^{1/2}Z = \eta^{1/2}X^\delta$, the remainder term has absolute value at most

$$\frac{X^{1/12}}{\exp((\log X)^{3/5+o(1)})} \sum_{\substack{(v,w)\in\mathcal{S}_0\\ p_8(v,w)\le Y}} \frac{1}{p_8(v,w)^{1/4}} = \frac{X^{1/12}}{\exp((\log X)^{3/5+o(1)})}$$

as $X \to \infty$, since the sum here is $O(\log Y)$.

The main term for $N^{(\mathrm{i})}(Y,X)$ is

$$\frac{3\eta^{1/2}}{4\zeta(2)}X^{1/6}\Bigg(\sum_{(v,w)\in\mathcal{S}_0} \frac{1}{\sqrt{p_8(v,w)}} - \sum_{\substack{(v,w)\in\mathcal{S}_0\\ p_8(v,w)> Y}} \frac{1}{\sqrt{p_8(v,w)}}\Bigg).$$

The first sum is the constant s_0. The second sum is estimated in Corollary 2 for the cases i, j being $0, 1$ and $1, 0$. Thus, we have, as $X \to \infty$,

$$N^{(\mathrm{i})}(Y,X) = \frac{3\eta^{1/2}}{4\zeta(2)} s_0 X^{1/6} - \frac{\eta^{1/2}(\alpha_3+\alpha_4)}{4\zeta(2)^2}\frac{X^{1/6}}{Y^{1/4}} + O\Big(\frac{X^{1/6}\log Y}{Y^{3/8}}\Big) + E_1(X),$$

where $|E_1(x)| \le X^{1/12}/\exp((\log X)^{3/5+o(1)})$. We shall take $\delta < 1/18$, and so since $Y = \eta X^{1/3-2\delta}$, the O-term above is absorbed into $E_1(X)$, and we have, as $X \to \infty$,

$$N^{(\mathrm{i})}(Y,X) = \frac{3\eta^{1/2}}{4\zeta(2)} s_0 X^{1/6} - \frac{\eta^{1/2}(\alpha_3+\alpha_4)}{4\zeta(2)^2} X^{1/12+\delta/2} + E_2(X),$$

where $|E_2(X)| \le X^{1/12}/\exp((\log X)^{3/5+o(1)})$.

It is convenient to compute the infinite sum s_0 numerically without the coprimality condition for v and w, so let

$$s_0' = \sum_{\substack{1\le v<w \\ v \not\equiv w \pmod 2}} \frac{1}{\sqrt{p_8(v,w)}} \doteq 0.064679703204$$

(as in Section 2). Note that if $v = dv_0$ and $w = dw_0$, for some d, then $\sqrt{p_8(v,w)}$ $= d^4\sqrt{p_8(v_0,w_0)}$. So

$$s_0 = s_0' \sum_{d\,\mathrm{odd}} \frac{\mu(d)}{d^4}.$$

From (2), we have $s_0 = \frac{16}{15\zeta(4)} s_0'$.

The calculation of $N_Z^{(\mathrm{i})}(Y,X)$

The calculation of $N_Z^{(\mathrm{i})}(Y,X)$ parallels that of $N^{(\mathrm{i})}(Y,X)$. In place of (5) we have

$$N_Z^{(\mathrm{i})}(Y,X) = \Big(\frac{3}{4\zeta(2)} Z + R_3'(Z)\Big) \sum_{\substack{(v,w)\in\mathcal{S}_0 \\ p_8(v,w)\le Y}} 1.$$

By Corollary 3 in the cases i, j being $0, 1$ and $1, 0$, the sum here is $\frac{2\beta Y^{1/4}}{3\zeta(2)}$ $+O(Y^{1/8}\log Y)$. By (4) we thus have, as $X \to \infty$,

$$\Big| N_Z^{(\mathrm{i})}(Y,X) - \frac{\eta^{1/4}\beta}{2\zeta(2)^2} X^{1/12+\delta/2} \Big| \le \frac{X^{1/12}}{\exp((\log X)^{3/5+o(1)})}.$$

The calculation of $N_Z^{(\mathrm{i})}(X)$

We have

$$N_Z^{(\mathrm{i})}(X) = \sum_{\substack{r\le Z\\ r \text{ squarefree}\\ 3\nmid r}} \sum_{\substack{(v,w)\in\mathcal{S}_0\\ p_8(v,w)\le \eta X^{1/3}/r^2}} 1$$
$$= \sum_{\substack{r\le Z\\ r \text{ squarefree}\\ 3\nmid r}} \left(\frac{2\eta^{1/4}\beta X^{1/12}}{3\zeta(2)r^{1/2}} + O\Big(\frac{X^{1/24}\log X}{r^{1/4}}\Big)\right),$$

using Corollary 3 for i, j being $0, 1$ and $1, 0$. The remainder term here is $O(X^{1/24}Z^{3/4}\log X)$, which is negligible. For the main term we need to sum $1/r^{1/2}$ fairly precisely, which follows from Proposition 8 and Corollary 4. So, as $X \to \infty$,

$$\left|N_Z^{(\mathrm{i})}(X) - \frac{\eta^{1/4}\beta}{\zeta(2)^2}X^{1/12+\delta/2}\right| \le \frac{X^{1/12}}{\exp((\log X)^{3/5+o(1)})}.$$

5.6 The main theorem for two pairs

Recall $N^{(\mathrm{i})}(X)$ is the number of (r, v, w) in the first of the four cases described at the beginning of Section 5, such that $|A(r, v, w)| \le A_b$. And recall $N^{(\mathrm{i})}(X) = N^{(\mathrm{i})}(Y, X) + N_Z^{(\mathrm{i})}(X) - N_Z^{(\mathrm{i})}(Y, X)$, which is

$$\frac{3}{4}\cdot\frac{1}{2^{1/3}27^{1/2}\zeta(2)}\cdot\frac{16}{15\zeta(4)}s_0X^{1/6} + \frac{\eta^{1/4}}{4\zeta(2)^2}(2\beta-\alpha_3-\alpha_4)X^{1/12+\delta/2} + E_3(X),$$

where $|E_3(X)| \le X^{1/12}/\exp((\log X)^{3/5+o(1)})$ as $X \to \infty$. This holds for any value of δ with $0 < \delta < \frac{1}{18}$. Yet if $2\beta \ne \alpha_3 + \alpha_4$, then the above statement cannot be true for more than one value of δ. So $2\beta = \alpha_3 + \alpha_4$ and, as $X \to \infty$,

$$\left|N^{(\mathrm{i})}(X) - \frac{3}{4}\cdot\frac{1}{2^{1/3}27^{1/2}\zeta(2)}\cdot\frac{16}{15\zeta(4)}s_0X^{1/6}\right| \le \frac{X^{1/12}}{\exp((\log X)^{3/5+o(1)})}.$$

We can also prove $2\beta = \alpha_3 + \alpha_4$ directly. We have

$$\alpha_3 + \alpha_4 = \int_0^1 \int_0^{p_8(u,1)^{-1/2}} \int_0^{p_8(u,1)^{1/4}} dt\,dz\,du = \int_0^1 \int_0^{p_8(u,1)^{-1/4}} da\,du.$$

Make the change of variables $a = x^2$, $u = y/x$. The Jacobian has value 2. The region described by the limits of integration of the last double integral is transformed to the region in the first quadrant of the xy-plane bounded by $p_8(x, y) = 1$, $y = 0$, and $y = x$. The latter region has the same area as $\mathcal{R}_2(1)$, i.e. β.

The remaining three cases are similar. Let

$$s_1' = \sum_{\substack{1\le v<w\\ 2\nmid vw}} \frac{1}{\sqrt{p_8(v,w)}} \doteq 0.016169925632$$

(as in Section 2). If $N^{(j)}(X)$ is the count of the number of (r, v, w) with $A(r, v, w) \le A_b$ in Case (j) of the four cases, then as $X \to \infty$ we have

$$\left| N^{(\mathrm{ii})}(X) - \frac{1}{4} \cdot \frac{1}{2^{1/3}(1/3)^{1/2}\zeta(2)} \cdot \frac{16}{15\zeta(4)} s_0' X^{1/6} \right| \le \frac{X^{1/12}}{\exp((\log X)^{3/5+o(1)})},$$

$$\left| N^{(\mathrm{iii})}(X) - \frac{3}{4} \cdot \frac{1}{2^{1/3}(27/16)^{1/2}\zeta(2)} \cdot \frac{16}{15\zeta(4)} s_1' X^{1/6} \right| \le \frac{X^{1/12}}{\exp((\log X)^{3/5+o(1)})},$$

$$\left| N^{(\mathrm{iv})}(X) - \frac{1}{4} \cdot \frac{1}{2^{1/3}(1/48)^{1/2}\zeta(2)} \cdot \frac{16}{15\zeta(4)} s_1' X^{1/6} \right| \le \frac{X^{1/12}}{\exp((\log X)^{3/5+o(1)})}.$$

Recall (from Section 2) that

$$c_{2,1} = \frac{16}{2^{1/3}27^{1/2}5\zeta(2)\zeta(4)} \left(s_0' + 4s_1'\right).$$

Theorem 2 *The number of $E/\mathbf{Q}$ of height at most X with two pairs of Galois-stable cyclic subgroups is $N_2(X) = c_{2,1}X^{1/6} + O_{\pm}(X^{1/12}/\exp((\log X)^{3/5+o(1)}))$ as $X \to \infty$, where $c_{2,1} \doteq 0.035515448016$ as in Section 2.*

Proof This follows from Proposition 5 and the computations above.

We remark that if the Riemann Hypothesis is assumed we can obtain power-saving error estimates over those recorded in Proposition 8 and Corollary 4 and so obtain an error estimate for $N_2(X)$ that shaves a constant off of the exponent 1/12.

5.7 Numerical illustration — two pairs

In this section we numerically illustrate Theorem 2. In the table below we present $N_2(X)$ and $N_2(X) - c_{2,1}X^{1/6}$ for various values of X. In the last column, we round to one digit past the decimal point.

X	$N_2(X)$	$N_2(X) - c_{2,1}X^{1/6}$
10^{30}	3544	−7.5
10^{36}	35486	−29.4
10^{42}	355140	−14.5
10^{48}	3551596	51.2
10^{54}	35515580	132.0
10^{60}	355154548	67.8

6 Declarations

6.1 Funding

The first author is grateful for the hospitality of Santa Clara University and was funded by their Paul R. and Virginia P. Halmos Endowed Professorship in Mathematics and Computer Science.

6.2 Conflicts of Interest/Competing Interests

Not applicable.

6.3 Availability of data and material

Not applicable.

6.4 Code availability

Not applicable.

6.5 Authors' contributions

Not applicable.

Acknowledgements The authors are grateful to John Voight for several useful conversations, to Paul Pollack for his suggestion of using (3), and to two very thorough referees for their helpful corrections and suggestions. In particular, one referee suggested a better proof of Proposition 3 and the other a better proof of Lemma 4. The authors are also grateful to Mehdi Ahmadi for creating the figure. The authors made use of GP-PARI and Mathematica.

References

[1] Apostol, T. M.: Introduction to analytic number theory. Springer, New York (1976)
[2] Cullinan, J., Kenney, M., Voight, J.: On a probabilistic local-global principle for torsion on elliptic curves. arXiv, https://arxiv.org/abs/2005.06669
[3] Davenport, H., Heilbronn, H.: On the class-number of binary cubic forms. II. J. London Math. Soc. 26, 192–198 (1951)
[4] Harron, R., Snowden, A.: Counting elliptic curves with prescribed torsion. J. Reine Angew. Math. 729, 151–170 (2017)
[5] Huxley, M.N., Exponential sums and lattice points III. Proc. London Math. Soc. 87 no. 3, 591–609 (2003)
[6] Pizzo, M., Pomerance, C., Voight, J.: Counting elliptic curves with an isogeny of degree three. Proc. Amer. Math. Soc., Ser. B, 7, 28–42 (2020)
[7] Schaefer, E.F.: Class groups and Selmer groups. J. Number Theory, 56 no. 1, 79–114 (1996)

[8] Tenenbaum, G.: Introduction to analytic and probabilistic number theory. Cambridge University Press, Cambridge (1995)
[9] Walfisz, A.: Weylsche Exponentialsummen in der neueren Zahlentheorie. Mathematische Forschungsberichte, XV. VEB Deutscher Verlag der Wissenschaften, Berlin (1963)