PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

COUNTING ELLIPTIC CURVES WITH AN ISOGENY OF DEGREE THREE

MAGGIE PIZZO, CARL POMERANCE, AND JOHN VOIGHT

Abstract. We count by height the number of elliptic curves over $\mathbb{Q}$ that possess an isogeny of degree 3.

1. Introduction

Torsion subgroups of elliptic curves have long been an object of fascination for mathematicians. By work of Duke [1], elliptic curves over $\mathbb{Q}$ with nontrivial torsion are comparatively rare. Recently, Harron–Snowden [3] have refined this result by counting elliptic curves over $\mathbb{Q}$ with prescribed torsion, as follows. Every elliptic curve E over $\mathbb{Q}$ is defined uniquely up to isomorphism by an equation of the form

$$E\colon y^2 = f(x) = x^3 + Ax + B \tag{1.1}$$

with $A, B \in \mathbb{Z}$ such that $4A^3 + 27B^2 \neq 0$ and there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$. We define the height of such E by

$$\mathrm{ht}(E) := \max(|4A^3|, |27B^2|). \tag{1.2}$$

For G a possible torsion subgroup (allowed by Mazur's theorem [5]), Harron–Snowden [3, Theorem 1.5] prove that

$$\#\{E : \mathrm{ht}(E) \leq X \text{ and } E(\mathbb{Q})_{\mathrm{tors}} \simeq G\} \asymp X^{1/d(G)}$$

for $d(G) \in \mathbb{Q}$ explicitly given, and $f(X) \asymp g(X)$ means that there exist $a_1, a_2 \in \mathbb{R}_{>0}$ such that $a_1 g(X) \leq f(X) \leq a_2 g(X)$ for X large. In the case $G \simeq \mathbb{Z}/2\mathbb{Z}$, i.e., the case of 2-torsion, they show the count is $cX^{1/2} + O(X^{1/3})$ for an explicit constant $c \approx 3.1969$ [3, Theorem 5.5]. (For weaker but related results, see also Duke [1, Proof of Theorem 1] and Grant [2, Section 2].)

In this article, we count elliptic curves with a nontrivial cyclic isogeny defined over $\mathbb{Q}$. An elliptic curve has a 2-isogeny if and only if it has a 2-torsion point, so the above result of Duke, Grant, and Harron–Snowden handles this case. The next interesting case concerns isogenies of degree 3.

For $X \in \mathbb{R}_{\geq 1}$, let $N_3(X)$ count the number of elliptic curves E over $\mathbb{Q}$ in the form (1.1) with $\mathrm{ht}(E) \leq X$ that possess a 3-isogeny defined over $\mathbb{Q}$. Our main result is as follows.

Received by the editors 3 July 2019.
2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 14H52.
Key words and phrases. Elliptic curves.

Theorem 1.3. *There exist $c_1, c_2 \in \mathbb{R}$ such that for $X \geq 1$,*

$$N_3(X) = \frac{2}{3\sqrt{3}\zeta(6)} X^{1/2} + c_1 X^{1/3} \log X + c_2 X^{1/3} + O(X^{7/24}).$$

Moreover,

$$c_1 = \frac{c_0}{8\pi^2 \zeta(4)} = 0.107437\ldots$$

where c_0 is an explicitly given integral (4.9), and the constant c_2 is effectively computable.

We obtain the same asymptotic in Theorem 1.3 if we instead count elliptic curves *equipped* with a 3-isogeny (that is, counting with multiplicity): see Proposition 2.9. Surprisingly, the main term of order $X^{1/2}$ counts *just* those elliptic curves with $A = 0$ (having j-invariant 0 and complex multiplication by the quadratic order of discriminant -3). Theorem 1.3 matches computations performed out to $X = 10^{25}$—see section 6.

The difficulty in computing the constant c_2 in the above theorem arises in applying a knotty batch of local conditions; our computations suggest that $c_2 \approx 0.16$. If we count without these conditions, for the coefficient of the $X^{1/3}$ term we find the explicit constant $c_6 = 1.1204\ldots$, given in (5.4)—it is already quite complicated.

Theorem 1.3 may be interpreted in alternative geometric language as follows. Let $X_0(3)$ be the modular curve parametrizing (generalized) elliptic curves equipped with an isogeny of degree 3. Then $N_3(X)$ counts rational points of bounded height on $X_0(3)$ with respect to the height arising from the pullback of the natural height on the j-line $X(1)$. From this vantage point, the main term corresponds to a single elliptic point of order 3 on $X_0(3)$! The modular curves $X_0(N)$ are not fine moduli spaces (owing to quadratic twists), so our proof of Theorem 1.3 is quite different than the method used by Harron–Snowden: in particular, a logarithmic term presents itself for the first time. We hope that our method and the lower-order terms in our result will be useful in understanding counts of rational points on stacky curves more generally.

Contents. The paper is organized as follows. We begin in section 2 with a setup and exhibiting the main term, then in section 3 as a warmup we prove the right order of magnitude for the secondary term. In section 4, we refine this approach to prove an asymptotic for the secondary term, and then we exhibit a tertiary term in section 5. We conclude in section 6 with our computations.

Acknowledgments. The authors thank John Cullinan for useful conversations and Ed Schaefer for helpful corrections. Pizzo was supported by the Jack Byrne Scholars program at Dartmouth College. Voight was supported by a Simons Collaboration grant (550029).

2. Setup

In this section, we set up the problem in a manner suitable for direct investigation. We continue the notation from the introduction.

Let $\mathcal{E}$ denote the set of elliptic curves E over $\mathbb{Q}$ in the form (1.1) (minimal, with nonzero discriminant). For $X \in \mathbb{R}_{\geq 1}$, let

$$\mathcal{E}_{\leq X} := \{E \in \mathcal{E} : \mathrm{ht}(E) \leq X\} \tag{2.1}$$

be the set of elliptic curves E over $\mathbb{Q}$ with height at most X. We are interested in asymptotics for the functions

$$\begin{aligned} N_3(X) &:= \#\{E \in \mathcal{E}_{\leq X} : E \text{ has a 3-isogeny defined over } \mathbb{Q}\}, \\ N_3'(X) &:= \#\{(E, \pm\phi) : E \in \mathcal{E}_{\leq X},\ \phi\colon E \to E' \text{ is a 3-isogeny defined over } \mathbb{Q}\}. \end{aligned} \tag{2.2}$$

In defining $N_3'(X)$, we note that we may always post-compose (or pre-compose) a 3-isogeny by the automorphism -1, giving a different isogeny (negating the y-coordinate) but with same kernel; to avoid this overcounting, we count *unsigned* isogenies (counting an isogeny and its negative just once).

To that end, let $E = E_{A,B} \in \mathcal{E}$, with $A, B \in \mathbb{Z}$. The 3-division polynomial of E [7, Exercise 3.7] is equal to

$$\psi(x) = \psi_{A,B}(x) := 3x^4 + 6Ax^2 + 12Bx - A^2; \tag{2.3}$$

the roots of $\psi(x)$ are the x-coordinates of nontrivial 3-torsion points on E.

Lemma 2.4. *The elliptic curve E has a 3-isogeny defined over $\mathbb{Q}$ if and only if $\psi(x)$ has a root $a \in \mathbb{Q}$.*

Proof. For ($\Rightarrow$), let $\varphi\colon E \to E'$ be a 3-isogeny defined over $\mathbb{Q}$. Then $\ker\varphi = \{\infty, \pm P\}$ is stable under the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}}$, so $\sigma(P) = \pm P$. Thus, $\sigma(x(P)) = x(P)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$ and hence $a = x(P) \in \mathbb{Q}$ is a root of $\psi(x)$ by definition. For ($\Leftarrow$), if $\psi(a) = 0$ with $a \in \mathbb{Q}$, then letting $\pm P := (a, \pm\sqrt{f(a)})$ we obtain $C := \{\infty, \pm P\}$ a Galois stable subgroup of order 3 and accordingly the map $\varphi\colon E \to E/C = E'$ is a 3-isogeny defined over $\mathbb{Q}$. □

Lemma 2.5. *If $a \in \mathbb{Q}$ is a root of $\psi(x)$, then $a \in \mathbb{Z}$.*

Proof. By the rational root test, $a_0 = 3a \in \mathbb{Z}$, and so

$$0 = 27\psi(a) = a_0^4 + 18Aa_0^2 + 108Ba_0 - 27A^2 \tag{2.6}$$

whence $3 \mid a_0$ and $a \in \mathbb{Z}$. □

Although the polynomial $\psi(x)$ is irreducible in $\mathbb{Z}[A, B][x]$, the special case where $A = 0$ gives $\psi_{0,B}(x) = 3x(x^3 + 4B)$ and so $a = 0$ is automatically a root. We count these easily.

Lemma 2.7. *Let $N_3(X)_{A=0}$ and $N_3'(X)_{A=0}$ be defined as in (2.2) but restricted to $E \in \mathcal{E}_{\leq X}$ with $A = 0$. Then*

$$N_3(X)_{A=0} = \frac{2}{3\sqrt{3}\zeta(6)} X^{1/2} + O(X^{1/12}) \quad \text{and} \quad N_3'(X)_{A=0} = N_3(X)_{A=0} + O(X^{1/6}).$$

Proof. In light of the above, we have

$$N_3(X)_{A=0} = \#\{B \in \mathbb{Z} : |27B^2| \leq X \text{ and } \ell^6 \nmid B \text{ for any prime } \ell\};$$

a standard sieve gives this count as $\dfrac{2}{3\sqrt{3}\zeta(6)} X^{1/2} + O(X^{1/12})$, see Pappalardi [6]. If such an elliptic curve had another unsigned 3-isogeny over $\mathbb{Q}$ (i.e., a 3-isogeny other than $\pm\phi$), it would correspond to a root of $\psi(x)/x = x^3 + 4B$, in which case $-4B$ is a cube; the count of such is $O(X^{1/6})$. □

With these lemmas in hand, we define our explicit counting function. For $X > 0$, let $N(X)$ denote the number of ordered triples $(A, B, a) \in \mathbb{Z}^3$ satisfying:

(N1) $A \neq 0$ and $\psi_{A,B}(a) = 0$;

(N2) $|4A^3| \le X$ and $|27B^2| \le X$;
(N3) $4A^3 + 27B^2 \neq 0$; and
(N4) there is no prime ℓ with $\ell^4 \mid A$ and $\ell^6 \mid B$.

That is to say, we define

$$N(X) := \#\{(A, B, a) \in \mathbb{Z}^3 : \text{all conditions (N1)–(N4) hold}\}. \tag{2.8}$$

We have excluded from $N(X)$ the count for $A = 0$ from the function $N(X)$; we have handled this in Lemma 2.7. To conclude this section, we summarize and compare $N_3(X)$ and $N_3'(X)$.

Proposition 2.9. *We have*

$$N_3(X) = N_3'(X) + O(X^{1/6} \log X) = \frac{2}{3\sqrt{3}\zeta(6)} X^{1/2} + N(X) + O(X^{1/6} \log X).$$

Proof. For the first equality, the difference $N_3'(X) - N_3(X)$ counts elliptic curves with more than one unsigned 3-isogeny. Let E be an elliptic curve with 3-isogenies $\varphi_i \colon E \to E_i'$ such that $\varphi_1 \neq \pm\varphi_2$ and let $\ker \varphi_i = \langle P_i \rangle$ for $i = 1, 2$. Then $\langle P_1, P_2 \rangle = E[3]$, and so the image of $\mathrm{Gal}_{\mathbb{Q}}$ acting on $E[3]$ is a subgroup of the group of diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_3)$. This property is preserved by any twist of E, so such elliptic curves are characterized by the form of their j-invariant, explicitly [8, Table 1, 3D^0-3a]

$$j(t) = \left(\frac{t(t+6)(t^2 - 6t + 36)}{(t-3)(t^2 + 3t + 9)} \right)^3 \tag{2.10}$$

for $t \in \mathbb{Q} \setminus \{3\}$. Computing an elliptic surface for this j-invariant, we conclude that every such E is of the form $y^2 = x^3 + u^2 A(t) x + u^3 B(t)$ for some $t, u \in \mathbb{Q}$, where

$$A(t) = -3t(t+6)(t^2 - 6t + 36) = -3t^4 - 648t,$$
$$B(t) = 2(t^2 - 6t - 18)(t^4 + 6t^3 + 54t^2 - 108t + 324) = 2t^6 - 1080t^3 - 11664\,.$$

Then by Harron–Snowden [3, Proposition 4.1] (with $(r, s) = (4, 6)$ so $m = 1$ and $n = 2$), the number of such elliptic curves is bounded above (and below) by a constant times $X^{1/6} \log X$, as claimed.

The second equality is immediate from Lemmas 2.4, 2.5, and 2.7. □

In light of the above, our main result will follow from an asymptotic for the easier function $N(X)$ defined in (2.8), and so we proceed to study this function.

3. Order of magnitude

In this section, we introduce new variables u, v, w that will be useful in the sequel, and provide an argument that shows the right order of magnitude. This argument explains the provenance of the logarithmic term in a natural way and motivates our approach. We recall (2.8), the definition of $N(X)$.

Theorem 3.1. *We have* $N(X) \asymp X^{1/3} \log X$.

Before proving Theorem 3.1, we begin with a few observations and lemmas. If $A, B, a \in \mathbb{Z}$ with $A \neq 0$, and $\psi_{A,B}(a) = 0$, then $a \neq 0$ and

$$12B = \frac{A^2}{a} - 6Aa - 3a^3. \tag{3.2}$$

Lemma 3.3. *Let $A, a \in \mathbb{Z}$ with $a \neq 0$. Then $(A^2/a) - 6Aa - 3a^3 \in 12\mathbb{Z}$ if and only if all of the following conditions hold:*

(B1) *$a \mid A^2$ and $3 \mid (A^2/a)$;*
(B2) *A, a have the same parity; and*
(B3) *If A, a are both even, then $4 \mid (A^2/a)$.*

Proof. The verification is straightforward. □

Lemma 3.4. *Let $A, B, a \in \mathbb{Z}$ satisfy conditions* (N1)–(N2). *Then*

$$|a| \ll X^{1/6} \quad \text{and} \quad A^2/|a| \ll X^{1/2}. \tag{3.5}$$

Proof. Let $\alpha := a/X^{1/6}$. Since $|A| < 4^{-1/3}X^{1/3}$, we have

$$A^2/|a| < 4^{-2/3}|\alpha|^{-1}X^{1/2}, \ |Aa| < 4^{-1/3}|\alpha|X^{1/2}.$$

The inequality for B and (3.2) imply that

$$3|a|^3 \leq \frac{4}{3^{1/2}}X^{1/2} + 6|Aa| + \frac{A^2}{|a|},$$

so that

$$3|\alpha|^3 \leq \frac{4}{3^{1/2}} + \frac{6|\alpha|}{4^{1/3}} + \frac{1}{4^{2/3}|\alpha|}. \tag{3.6}$$

The inequality (3.6) fails for $|\alpha|$ large—in fact, we have $|\alpha| < 11/8$—which proves the first part of (3.5). To get the second part, note that the first part and condition (N2) imply that $|Aa| \ll X^{1/2}$. And since (3.2) implies that

$$A^2/|a| \leq 12|B| + 6|Aa| + 3|a|^3,$$

we have $A^2/|a| \ll X^{1/2}$. □

Proof of Theorem 3.1. We first prove the upper bound. Every nonzero $a \in \mathbb{Z}$ can be written uniquely as $a = uv^2$, where $u \in \mathbb{Z}$ is squarefree and $v \in \mathbb{Z}_{>0}$. Replacing $a = uv^2$, we see that $a \mid A^2$ if and only if $uv \mid A$. Therefore $A = uvw$ with $w \in \mathbb{Z}$ arbitrary. The inequalities in (3.5) imply that there exist $c_3, c_4 > 0$ such that

$$0 < |u|v^2 \leq c_3X^{1/6} \ \text{ and } \ 0 < |u|w^2 \leq c_4X^{1/2}. \tag{3.7}$$

Thus,

$$N(X) \leq \#\{(u,v,w) \in \mathbb{Z}^3 : u \text{ squarefree}, v > 0, \text{ and the inequalities (3.7) hold}\}.$$

For $X \geq 2$, we have

$$\begin{aligned} N(X) &\leq \sum_{|u|v^2 \leq c_3X^{1/6}} \sum_{|u|w^2 \leq c_4X^{1/2}} 1 \ll \sum_{|u|v^2 \leq c_3X^{1/6}} \frac{X^{1/4}}{|u|^{1/2}} \\ &\leq X^{1/4} \sum_{0<v\leq c_3^{1/2}X^{1/12}} \sum_{|u|\leq c_3X^{1/6}/v^2} \frac{1}{|u|^{1/2}} \\ &\ll X^{1/3} \sum_{0<v\leq c_3^{1/2}X^{1/12}} \frac{1}{v} \ll X^{1/3}\log X. \end{aligned} \tag{3.8}$$

For the lower bound, we let u, v, w range over positive, odd, squarefree numbers with $3 \mid w$ and let $a = uv^2$ and $A = uvw$ as in the previous paragraph; these ensure that conditions (B1)–(B3) hold, so by Lemma 3.3 we have $B \in \mathbb{Z}$. Conditions (N1)

and (N4) are also satisfied, and condition (N3) is negligible. To ensure (N2), we choose

$$v \le X^{1/24},\ uv^2 < \frac{1}{2}X^{1/6},\ w < uv^3. \tag{3.9}$$

Then $A = uvw < u^2v^4 < \frac{1}{4}X^{1/3}$ so $|4A^3| \le X$. Moreover,

$$\begin{aligned} -12B = 3u^3v^6 + 6u^2v^3w - uw^2 &= 3u^3v^6\left(1 + 2\frac{w}{uv^3} - \frac{1}{3}\left(\frac{w}{uv^3}\right)^2\right) \\ &< 3\left(\frac{1}{2}X^{1/6}\right)^3\frac{8}{3} = X^{1/2} \end{aligned} \tag{3.10}$$

since $0 < w/uv^3 \le 1$ and the polynomial $1 + 2t - \frac{1}{3}t^2$ on $[0,1]$ is positive and takes the maximum value $\frac{8}{3}$. Thus, all conditions are satisfied.

We now count the choices for u, v, w with the above conditions: we have

$$N(X) \ge \sum_{v \le X^{1/24}} \sum_{uv^2 < \frac{1}{4}X^{1/6}} \sum_{w < uv^3} 1 \gg \sum_{v \le X^{1/24}} \sum_{u < \frac{1}{4}X^{1/6}/v^2} uv^3. \tag{3.11}$$

The inner sum on u is $\gg X^{1/3}/v$, so that $N(X) \gg X^{1/3}\log X$, which completes the proof of the lower bound. □

4. An asymptotic

In this section, we prove an asymptotic for $N(X)$. We recall some notation introduced in the proof of Theorem 3.1. Let $(A, B, a) \in \mathbb{Z}^3$ satisfy (N1), so $a \ne 0$ and B is determined by A, a as in Lemma 3.3. Write

$$\begin{aligned} a &= uv^2 \\ A &= uvw \end{aligned} \tag{4.1}$$

with $u \in \mathbb{Z}$ squarefree, $v \in \mathbb{Z}_{>0}$, and $w \in \mathbb{Z}_{\ne 0}$. Then

$$12B = uw^2 - 6u^2v^3w - 3u^3v^6. \tag{4.2}$$

We rewrite condition (N4) and the conditions in Lemma 3.3 in terms of the quantities u, v, w as follows.

Lemma 4.3. *Conditions (B1)–(B3) and (N4) hold if and only if all of the following conditions hold:*

(W1) $uv \equiv w \pmod 2$;
(W2) *Not both* $2^2 \mid v$ *and* $2^4 \mid w$ *occur;*
(W3) *Not all of* $2 \nmid u$, $2 \parallel v$, *and* $2^3 \parallel w$ *occur;*
(W4) *Not all of* $2 \mid u$, $2 \parallel v$, *and* $2^4 \mid w$ *occur;*
(W5) $3 \mid uw$;
(W6) *Not both* $3 \mid v$ *and* $3^4 \mid uw$ *occur; and*
(W7) *For each prime* $\ell > 3$, *not both* $\ell \mid v$ *and* $\ell^3 \mid w$ *occur.*

Proof. This lemma can be proven by a tedious case-by-case analysis. Alternatively, the conditions (B1)–(B3) are determined by congruence conditions modulo 16 and 81, so we may also just loop over the possibilities by computer. □

Lemma 4.4. *The proportion among* (u, v, w) *(with* u *squarefree) satisfying the conditions (W1)–(W7) is* $(4\zeta(4))^{-1}$.

Proof. For the conditions (W1)–(W6), we just count residue classes (as in Lemma 4.3): we find proportions 15/32 for conditions (W1)–(W4) and 40/81 for (W5)–(W6). For condition (W7), the proportion of cases where $\ell \mid v$ and $\ell^3 \mid w$ is $1/\ell^4$, so the correction factor is

$$\prod_{\ell>3}\left(1-\frac{1}{\ell^4}\right) = \frac{16}{15}\cdot\frac{81}{80}\cdot\frac{1}{\zeta(4)} = \frac{27}{25\zeta(4)}.$$

Thus, the total proportion is

$$\frac{15}{32}\cdot\frac{40}{81}\cdot\frac{27}{25\zeta(4)} = \frac{1}{4\zeta(4)}.$$

□

Let $X > 0$, and suppose (A, B, a) is counted by $N(X)$. Define $\alpha, \beta \in \mathbb{R}_{>0}$ by

$$\begin{aligned} a &= uv^2 = \alpha X^{1/6}, \\ w &= \beta uv^3. \end{aligned} \tag{4.5}$$

(The quantity α arose in the proof of Lemma 3.4.) Moreover, define the functions

$$\begin{aligned} f(\beta) &:= \frac{1}{2^{1/3}|\beta|^{1/2}}, \\ g(\beta) &:= \frac{4^{1/3}}{3^{1/2}|1+2\beta-\frac{1}{3}\beta^2|^{1/3}}, \\ h(\beta) &:= \min\{f(\beta), g(\beta)\}. \end{aligned} \tag{4.6}$$

The function $h(\beta)$ is plotted in Figure 4.7.

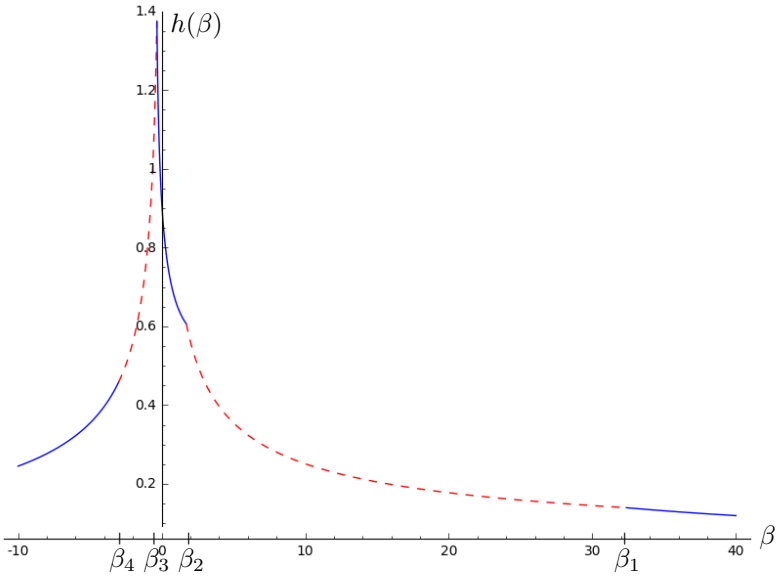

Figure 4.7: Graph of the function $h(\beta)$, defined in (4.6)

The transition points for the piecewise function $h(\beta)$ occur at

$$\beta_1 := 32.37198796\ldots,\ \beta_2 := 1.71119188\ldots,\ \beta_3 := -\frac{1}{3},\ \beta_4 := -3; \tag{4.8}$$

the transition points β_1, β_2 are algebraic numbers. Then $h(\beta) = g(\beta)$ on the intervals $(-\infty, \beta_4)$, (β_3, β_2), and (β_1, ∞) and $h(\beta) = f(\beta)$ on the complementary intervals (β_4, β_3) and (β_2, β_1).

We compute numerically that

$$c_0 := \int_{-\infty}^{\infty} h(\beta)^2 \, d\beta = 9.1812458638\ldots. \tag{4.9}$$

The relevance of these quantities (as well as their weighting) is made plain by the following lemma.

Lemma 4.10. *The triple (u, v, w) satisfies (N2) if and only if*

$$|\alpha| \le h(\beta).$$

Proof. Since $A = uvw = \beta u^2 v^4 = \alpha^2 \beta X^{1/3}$, the first inequality in (N2) is equivalent to

$$|\alpha^2 \beta| \le 4^{-1/3}. \tag{4.11}$$

In addition, we have

$$-12B = 3u^3 v^6 \left(1 + 2w/uv^3 - \frac{1}{3}\left(\frac{w}{uv^3}\right)^2\right) = 3\alpha^3 X^{1/2}\left(1 + 2\beta - \frac{1}{3}\beta^2\right),$$

so that the second inequality in (N2) is equivalent to

$$\left|\alpha^3\left(1 + 2\beta - \frac{1}{3}\beta^2\right)\right| \le \frac{4}{3^{3/2}}. \tag{4.12}$$

The result then follows from (4.11) and (4.12). □

We then have the following first version of our main result.

Theorem 4.13. *We have*

$$N(X) \sim c_1 X^{1/3} \log X$$

where

$$c_1 := \frac{c_0}{8\pi^2 \zeta(4)} = 0.10743725502\ldots$$

and c_0 is defined in (4.9).

Proof. Via (4.1)–(4.2), $N(X)$ counts $(u, v, w) \in \mathbb{Z}^3$ with u squarefree, v positive, $w \ne 0$, such that conditions (N2)–(N3) hold as well as the local conditions (W1)–(W7) (which implies (N4)). We may ignore condition (N3) as negligible: for each choice of u, v there are $O(1)$ choices of w where (N3) fails, subtracting at most $O(X^{1/6})$ from the count.

We first show how to count triples u, v, w satisfying (N2), not necessarily the local conditions, and define

$$N_0(X) := \#\{(u, v, w) \in \mathbb{Z}^3 : u \text{ squarefree}, v > 0, \text{ and (N2) holds}\}. \tag{4.14}$$

We suppress the reminder that u is taken to be squarefree. The number of triples with $w = 0$ is negligible, so we ignore this condition.

Let $X > 0$. For (u, v, w) counted by $N_0(X)$, we organize by the value of $\beta = w/uv^3 \in \mathbb{Q}$. Taking β in an interval I that does not contain a transition point in its interior, the integers u, v are constrained by

$$|a| = |u|v^2 < |\alpha| X^{1/6} < h(\beta) X^{1/6}$$

(with $h(\beta)$ minimal on I, taking left or right endpoint) by Lemma 4.10. Given u, v, we have $w = \beta uv^3 \in uv^3 I$ giving approximately $uv^3\,|I|$ possible values of w. Repeating this argument with Riemann sum estimates, we obtain

$$N_0(X) \sim \int_{-\infty}^{\infty} \sum_{\substack{|u|v^2 < h(\beta)X^{1/6} \\ v>0}} |u| v^3 \,\mathrm{d}\beta \tag{4.15}$$

as $X \to \infty$. (For a more refined approach with an error term, see (5.7) below.)

We now evaluate this integral. Recall that

$$\sum_{|u|\le t} |u| \sim \frac{6}{\pi^2} t^2;$$

inputting this into (4.15) and letting $X \to \infty$, we obtain

$$\begin{aligned}
&\int_{-\infty}^{\infty} \sum_{\substack{v^2 < h(\beta)X^{1/6} \\ v>0}} v^3 \sum_{|u| < h(\beta)X^{1/6}/v^2} |u| \,\mathrm{d}\beta \\
&\qquad \sim \frac{6}{\pi^2} \int_{-\infty}^{\infty} \sum_{v < h(\beta)^{1/2} X^{1/12}} v^3 \frac{h(\beta)^2 X^{1/3}}{v^4} \,\mathrm{d}\beta \\
&\qquad \sim \frac{6X^{1/3}}{\pi^2} \int_{-\infty}^{\infty} h(\beta)^2 \int_1^{h(\beta)^{1/2}X^{1/12}} \frac{1}{v} \,\mathrm{d}v \,\mathrm{d}\beta \\
&\qquad = \frac{6X^{1/3}}{\pi^2} \int_{-\infty}^{\infty} h(\beta)^2 \log(h(\beta)^{1/2} X^{1/12}) \,\mathrm{d}\beta \\
&\qquad \sim \frac{1}{2\pi^2} X^{1/3} \log X \int_{-\infty}^{\infty} h(\beta)^2 \,\mathrm{d}\beta = \frac{c_0}{2\pi^2} X^{1/3} \log X.
\end{aligned} \tag{4.16}$$

Finally, we impose the local constraints (W1)–(W7). The first 6 of these are clear. To impose (W7) note that

$$\frac{27}{25\zeta(4)} = \prod_{\ell>3} \left(1 - \frac{1}{\ell^4}\right) = \sum_{\gcd(d,6)=1} \frac{\mu(d)}{d^4}.$$

The sum converges rapidly, in fact, for $Z > 1$,

$$\left| \frac{27}{25\zeta(4)} - \sum_{\substack{\gcd(d,6)=1 \\ d \le Z}} \frac{\mu(d)}{d^4} \right| \ll \frac{1}{Z^3}.$$

Further, the proportion of triples u, v, w with $d \mid v$ and $d^3 \mid w$ for some $d > Z$ tends to 0 as $Z \to \infty$. So, imposing (W7) introduces the factor $27/(25\zeta(4))$ as in Lemma 4.4. We conclude that

$$N(X) \sim \frac{1}{4\zeta(4)} N_0(X) \sim c_1 X^{1/3} \log X$$

as $X \to \infty$, as claimed. □

5. Secondary term

In this section, we work on a secondary term for $N(X)$ (giving a tertiary term for $N_3(X)$).

We start by explaining how this works for the function $N_0(X)$ defined in (4.14), namely, the triples $(u, v, w) \in \mathbb{Z}^3$ such that u is squarefree, $v > 0$, and $|\alpha| \le h(\beta)$ where α, β are defined by (4.5). We discuss the modifications to this approach for $N(X)$ below.

We begin by working out an analog of Euler's constant for the squarefree harmonic series.

Lemma 5.1. *For real numbers $x \ge 1$ we have*

$$\sum_{\substack{0<u\le x\\ u \text{ squarefree}}} \frac{1}{u} = \frac{1}{\zeta(2)} \log x + \gamma_0 + O(x^{-1/2} \log x),$$

where

$$\gamma_0 := \frac{\gamma\zeta(2) - 2\zeta'(2)}{\zeta(2)^2} = 1.0438945157\ldots \tag{5.2}$$

and γ is Euler's constant.

Proof. The integer variables u, v, d in this proof are positive. We have

$$\begin{aligned}\sum_{\substack{u\le x\\ u \text{ squarefree}}} \frac{1}{u} &= \sum_{u\le x} \sum_{d^2 \mid u} \frac{\mu(d)}{u} = \sum_{d\le x^{1/2}} \frac{\mu(d)}{d^2} \sum_{v\le x/d^2} \frac{1}{v} \\ &= \sum_{d\le x^{1/2}} \frac{\mu(d)}{d^2} \left(\log\Big(\frac{x}{d^2}\Big) + \gamma + O\Big(\frac{d^2}{x}\Big)\right).\end{aligned}$$

The O-terms add up to $O(x^{-1/2})$. Since

$$\sum_{d\le x^{1/2}} \frac{\mu(d)}{d^2} = \sum_{d} \frac{\mu(d)}{d^2} - \sum_{d>x^{1/2}} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} + O(x^{-1/2})$$

and

$$\sum_{d\le x^{1/2}} \frac{2\mu(d)\log d}{d^2} = \sum_{d} \frac{2\mu(d)\log d}{d^2} - \sum_{d>x^{1/2}} \frac{2\mu(d)\log d}{d^2} = \frac{2\zeta'(2)}{\zeta(2)^2} + O\left(x^{-1/2}\log x\right),$$

the result follows. □

Theorem 5.3. *There exists $c_6 \in \mathbb{R}_{>0}$ such that*

$$N_0(X) = \frac{c_0}{2\pi^2} X^{1/3} \log X + c_6 X^{1/3} + O(X^{7/24})$$

where c_0 is defined in (4.9). More precisely, we have

$$c_6 := \left(\frac{\gamma_0}{2} + \frac{6\gamma}{\pi^2} - \frac{3}{2\pi^2}\right) c_0 + \frac{3}{\pi^2} \int_{-\infty}^{\infty} h(\beta)^2 \log h(\beta)\, \mathrm{d}\beta = 1.1204281987\ldots, \tag{5.4}$$

where γ_0 is defined in (5.2) and γ is Euler's constant.

Proof. We return to the derivation of the integral expression (4.15) and consider the contribution of a single term $a = uv^2$. With $\alpha = a/X^{1/6}$, the contribution of a to the integral is

$$\int_{h(\beta)\geq|\alpha|} |u|v^3 \,\mathrm{d}\beta = |u|v^3 \int_{h(\beta)\geq|\alpha|} \mathrm{d}\beta. \tag{5.5}$$

Note that h is continuous. Let $h_1 := h|_{(-\infty,-1/3]}$ and $h_2 := h|_{[-1/3,\infty)}$. Then h_1 is strictly increasing and h_2 is strictly decreasing. Letting j_1, j_2 be the inverses of h_1, h_2, respectively, we have for any $t \in (0, h(-1/3)]$ that

$$\{\beta \in \mathbb{R} : h(\beta) \geq t\} = [j_2(t), j_1(t)]. \tag{5.6}$$

Plugging (5.6) into the integral (5.5), we obtain $j_1(|\alpha|) - j_2(|\alpha|)$.

For a choice of $a = uv^2$, we count the number of nonzero integers w with $w/(|u|v^3) \in [j_2(|\alpha|), j_1(|\alpha|)]$: this is equal to

$$|u|v^3(j_1(|\alpha|) - j_2(|\alpha|)) + O(1).$$

So, the error when considering the integral in (4.15) is $O(X^{1/6})$, i.e.,

$$N_0(X) = \int_{-\infty}^{\infty} \sum_{\substack{|u|v^2\leq h(\beta)X^{1/6}\\ v>0}} |u|v^3 \,\mathrm{d}\beta + O(X^{1/6}). \tag{5.7}$$

We next consider the evaluation of the integrand

$$S := \sum_{\substack{|u|v^2<h(\beta)X^{1/6}\\ v>0}} |u|v^3 \tag{5.8}$$

(with the continued understanding that u is squarefree). Let $H(\beta) := h(\beta)^{1/4}X^{1/24}$, so that if $|u|v^2 \leq h(\beta)X^{1/6}$, then either $|u| \leq H^2$ or $v \leq H$. Let S_1 be the contribution to the integrand when $|u| \leq H^2$, let S_2 be the contribution when $v \leq H$, and let S_3 be the contribution when both $|u| \leq H^2$ and $v \leq H$. Then

$$S = S_1 + S_2 - S_3.$$

Using that $\sum_{0<v\leq t} v^3 = \frac{1}{4}t^4 + O(t^3)$, for a given value of u with $|u| \leq H^2$,

$$\sum_{v\leq h(\beta)^{1/2}X^{1/12}/|u|^{1/2}} |u|v^3 = \frac{1}{4}|u| \left(\frac{h(\beta)^2X^{1/3}}{|u|^2} + O\Big(\frac{h(\beta)^{3/2}X^{1/4}}{|u|^{3/2}}\Big)\right).$$

Summing this over squarefree numbers u with $|u| \leq H^2$ and using Lemma 5.1, we get

$$\begin{aligned} S_1 =& \frac{1}{4}h(\beta)^2X^{1/3} \cdot 2\left(\frac{6}{\pi^2}\log H^2 + \gamma_0\right) \\ &+ O\big(h(\beta)^2X^{1/3}H^{-2}\log H + h(\beta)^{3/2}X^{1/4}H\big) \\ =& \frac{1}{4\pi^2}h(\beta)^2X^{1/3}\log X + h(\beta)^2\left(\frac{1}{2}\gamma_0 + \frac{3}{2\pi^2}\log h(\beta)\right)X^{1/3} \\ &+ O\big(h(\beta)^{3/2}X^{1/4}\log X\big) + O\big(h(\beta)^{7/4}X^{7/24}\big). \end{aligned} \tag{5.9}$$

Next we consider S_2. For a given value of $v \leq H$, we have

$$\sum_{|u|\leq h(\beta)X^{1/6}/v^2} |u|v^3 = 2 \cdot \frac{1}{2} \cdot \frac{6}{\pi^2}h(\beta)^2X^{1/3}v^{-1} + O\Big(h(\beta)^{3/2}X^{1/4}\Big), \tag{5.10}$$

using that the number of squarefree numbers up to a bound x is $(6/\pi^2)x+O(x^{1/2})$ and partial summation. Summing for $v \le H$ we get

$$\begin{aligned} S_2 &= \frac{6}{\pi^2}h(\beta)^2X^{1/3}\Big(\frac{1}{24}\log X+\gamma+\frac{1}{4}\log h(\beta)+O(1/H)\Big) \\ &\quad + O(h(\beta)^{3/2}X^{1/4}H) \\ &= \frac{1}{4\pi^2}h(\beta)^2X^{1/3}\log X+\frac{6}{\pi^2}h(\beta)^2\Big(\gamma+\frac{1}{4}\log h(\beta)\Big)X^{1/3} \\ &\quad + O(h(\beta)^{7/4}X^{7/24}). \end{aligned} \tag{5.11}$$

Finally, for S_3 we have

$$\begin{aligned} S_3 &= \left(\frac{6}{\pi^2}H^4+O(H^3)\right)\left(\frac{1}{4}H^4+O(H^3)\right) = \frac{3}{2\pi^2}H^8+O(H^7) \\ &= \frac{3}{2\pi^2}h(\beta)^2X^{1/3}+O(h(\beta)^{7/4}X^{7/24}). \end{aligned} \tag{5.12}$$

Since $S = S_1 + S_2 - S_3$, combining (5.9), (5.11), and (5.12) we obtain

$$\begin{aligned} S =& \frac{h(\beta)^2}{2\pi^2}X^{1/3}\log X+h(\beta)^2\Big(\frac{\gamma_0}{2}+\frac{6\gamma}{\pi^2}+\frac{3}{\pi^2}\log h(\beta)-\frac{3}{2\pi^2}\Big)X^{1/3} \\ &+O\big(h(\beta)^{3/2}X^{1/4}\log X\big)+O\big(h(\beta)^{7/4}X^{7/24}\big). \end{aligned} \tag{5.13}$$

The expression (5.13) is then to be integrated over all β to obtain $N_0(X)$ as in (5.7). In this integral we may suppose that $|\beta| \ll X^{1/4}$, since $h(\beta) \asymp |\beta|^{-2/3}$ and we may suppose that $h(\beta)X^{1/6} \ge 1$. Thus, integrating the first error term gives $O(X^{1/4}(\log X)^2)$ and integrating the second gives $O(X^{7/24})$. We conclude that

$$\begin{aligned} \int_{-\infty}^{\infty}\sum_{\substack{|u|v^2\le h(\beta)X^{1/6}\\ v>0}}|u|v^3\,\mathrm{d}\beta &= \frac{c_0}{2\pi^2}X^{1/3}\log X+\Big(\frac{\gamma_0}{2}+\frac{6\gamma}{\pi^2}-\frac{3}{2\pi^2}\Big)c_0X^{1/3} \\ &\quad+\frac{3}{\pi^2}X^{1/3}\int_{-\infty}^{\infty}h(\beta)^2\log h(\beta)\,\mathrm{d}\beta+O\big(X^{7/24}\big). \end{aligned} \tag{5.14}$$

We compute numerically that

$$\int_{-\infty}^{\infty}h(\beta)^2\log h(\beta)\,d\beta = -18.0878968694\ldots \tag{5.15}$$

and so the coefficient of the secondary term of $N_0(X)$ is $c_6 = 1.12042819875\ldots$. □

Before proving our main theorem, we prove one lemma, generalizing Lemma 5.1. For $i \mid 6$ with $i > 0$, let

$$H_i(x) := \sum_{\substack{0<u\le x\\ u\ \text{squarefree}\\ \gcd(u,6)=i}}\frac{1}{u}. \tag{5.16}$$

Lemma 5.17. *We have*

$$H_1(x) = \frac{1}{2\zeta(2)}\log x+\gamma_1+O\Big(\frac{\log x}{x^{1/2}}\Big)$$

where

$$\gamma_1 = \frac{\log 432}{24\zeta(2)}+\frac{\gamma}{2\zeta(2)}-\frac{\zeta'(2)}{\zeta(2)^2},$$

and γ is Euler's constant. Moreover, $H_i(x) = \frac{1}{i}H_1(\frac{x}{i})$ for $i \mid 6$.

Proof. The proof follows the same lines as Lemma 5.1. □

We now prove our main result.

Proof of Theorem 1.3. The asymptotic for $N(X)$ was proven in Theorem 4.13 and a secondary term with power-saving error term for $N_0(X)$ was proven in Theorem 5.3. To finish, we claim that the local conditions (W1)–(W7) that move us from $N_0(X)$ to $N(X)$ can be applied in the course of the argument for Theorem 5.3 to obtain an (effectively computable) constant.

Let $i, j, k, d \in \mathbb{Z}_{>0}$ satisfy: $i \mid 6$, d squarefree and coprime to 6, $j \mid 12$, and $k \mid 6^4$. Let $N_{i,j,k,d}(X)$ denote the number of triples u, v, w counted by $N_0(X)$ with $\gcd(u, 6) = i$, $jd \mid v$, and $kd^3 \mid w$. Then with i, j, k running over triples consistent with conditions (W1)–(W6), a signed sum of the counts $N_{i,j,k,d}(X)$ gives $N(X)$. For example, take the case of uvw coprime to 6, which satisfies (W1)–(W6). The contribution of these triples to $N(X)$ is

$$\sum_{j\mid 6}\sum_{k\mid 6}\sum_{\gcd(d,6)=1}\mu(j)\mu(k)\mu(d)N_{1,j,k,d}(X).$$

We have similar expressions for other portions of the u, v, w-domain of triples.

We now estimate $N_{i,j,k,d}$ and control the contribution to $N(X)$ from large d. For the latter, since $|vw| \le A \ll X^{1/3}$, we have $d \ll X^{1/12}$; so we may suppose that d is so bounded. Getting a good estimate for $N_{i,j,k,d}$ follows in exactly the same way as with N_0. In particular, we have the analogue of (5.7):

$$N_{i,j,k,d}(X) = \int_{-\infty}^{\infty}\sum_{\substack{|u|v^2\le h(\beta)X^{1/6}\\ \gcd(u,6)=i\\ jd\,|\,v}}\frac{|u|v^3}{kd^3}\,\mathrm{d}\beta + O(X^{1/6}), \tag{5.18}$$

where it is understood that u is squarefree and $v > 0$. The sum here is estimated in the same way, by first considering the contribution when $|u| \le H^2$, where $H = h(\beta)^{1/4}X^{1/24}$, then the contribution when $v \le H$, and finally the contribution when both $|u| \le H^2$ and $v \le H$. To accomplish this, we use the following estimates:

$$\begin{aligned}\sum_{\substack{0<v\le x\\ jd\,|\,v}} v^3 &= \frac{1}{4}\frac{x^4}{jd} + O(x^3),\\ \sum_{\substack{0<v\le x\\ jd\,|\,v}} \frac{1}{v} &= \frac{1}{jd}\log x + \frac{\gamma - \log(jd)}{jd} + O\Big(\frac{1}{x^{1/2}d^{1/2}}\Big),\\ \sum_{\substack{|u|\ \text{squarefree}\\ |u|\le x\\ \gcd(u,6)=i}} |u| &= \frac{1}{i\zeta(2)}x^2 + O(x^{3/2}).\end{aligned} \tag{5.19}$$

We also need the sum of $1/|u|$, accomplished in Lemma 5.17.

Putting these ingredients together, we get that

$$N_{i,j,k,d}(X) = \frac{c_{i,j,k}}{d^4}X^{1/3}\log X + \frac{c'_{i,j,k}}{d^4}X^{1/3} + O\Big(\frac{X^{7/24}}{d^3}\Big), \tag{5.20}$$

where $c_{i,j,k}, c'_{i,j,k} = O(1)$ uniformly, and summing these contribution gives the result. □

6. Computations

We conclude with some computations that give numerical verification of our asymptotic expression.

We computed the functions $N_0(X)$ and $N(X)$ as follows. First, we restrict to $u > 0$ (still squarefree), since this gives exactly half the count. Second, we loop over u up to $\lfloor \frac{11}{8} X^{1/6} \rfloor$ (valid as in the proof of Lemma 3.4) and keep only squarefree u. Then we loop over v from 0 up to $\lfloor \sqrt{\frac{11}{8} X^{1/6}/u} \rfloor$. This gives us the value of $a = uv^2$. Then plugging into h gives

$$\beta_{\max} \le \max\left(\left\{ \frac{X^{1/3}}{4^{1/3} a^2}, 3 + \sqrt{12 + \frac{4}{\sqrt{3}} \frac{X^{1/2}}{a^3}} \right\} \right). \tag{6.1}$$

Then we loop over w from $-\beta_{\max} uv^3$ to $\beta_{\max} uv^3$, ignoring $w = 0$, and we take $A = uvw$. We then check that $|4A^3| \le X$; and letting

$$B = \frac{1}{12}\left(\frac{A^2}{a} - 6Aa - 3a^3 \right)$$

we check that $|27B^2| \le X$, and if so add to the count for $N_0(X)$. For $N(X)$, we further check the local conditions (B1)–(B3) and (N4) (or, equivalently, (W1)–(W7)).

In this manner, we thereby compute the data in Table 6.2 for $X = 10^m$ with $m \le 25$. We compute an approximate value for the constant $c_2 \approx 0.16$ as indicated in the fourth column.

m	$N_0(X)$	$\frac{c_0}{2\pi^2} X^{1/3} \log X + c_6 X^{1/3}$	$N(X)$	$\frac{N(X) - c_1 X^{1/3} \log X}{X^{1/3}}$
3	40	43	2	-0.54215
4	106	116	16	-0.24688
5	292	301	54	-0.07352
6	728	755	144	-0.04430
⋮	⋮	⋮	⋮	⋮
18	20396372	20398344	4615666	0.16276
19	46250606	46254289	10476028	0.16226
20	104614810	104622964	23720904	0.16285
21	236105316	236113295	53583854	0.16333
22	531764374	531764568	120772894	0.16335
23	1195334414	1195363230	271694240	0.16366
24	2682372754	2682431541	610085848	0.16366
25	6009687100	6009862508	1367646478	0.16347

Table 6.2: Data before and after applying local conditions

References

[1] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818.

[2] David Grant, *A formula for the number of elliptic curves with exceptional primes*, Compositio Math. **122** (2000), no. 2, 151–164.

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

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

[5] Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. No. **47** (1977), 33–186.

[6] Francesco Pappalardi, *A survey on k-freeness*, Number Theory, 71–78, Ramanujan Math. Soc. Lecture Notes Ser., vol. 1, Ramanujan Math. Soc., Mysore, 2005.

[7] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009.

[8] Andrew V. Sutherland and David Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra Number Theory **11** (2017), no. 5, 1199–1229.

Mathematics Department, Dartmouth College, Hanover, NH 03755
Email address: Magdalene.R.Pizzo.19@dartmouth.edu

Mathematics Department, Dartmouth College, Hanover, NH 03755
Email address: carl.pomerance@dartmouth.edu

Mathematics Department, Dartmouth College, Hanover, NH 03755
Email address: jvoight@gmail.com