COUNTING ELLIPTIC CURVES OVER THE RATIONALS WITH A 7-ISOGENY

GRANT MOLNAR AND JOHN VOIGHT

Abstract. We count by height the number of elliptic curves over the rationals, both up to isomorphism over the rationals and over an algebraic closure thereof, that admit a cyclic isogeny of degree 7.

Contents

1. Introduction

1.1. **Motivation and setup.** Number theorists have an enduring, and recently renewed, interest in the arithmetic statistics of elliptic curves: broadly speaking, we study asymptotically the number of elliptic curves of bounded size with a given property. More precisely, every elliptic curve E over $\mathbb{Q}$ is defined uniquely up to isomorphism by a Weierstrass equation of the form

$$E\colon y^2 = x^3 + Ax + B \tag{1.1.1}$$

with $A, B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \neq 0$ and such that no prime ℓ has $\ell^4 \mid A$ and $\ell^6 \mid B$. Let $\mathscr{E}$ be the set of elliptic curves of this form: we define the height of $E \in \mathscr{E}$ by

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

For $X \geq 1$, let $\mathscr{E}_{\leq X} := \{E \in \mathscr{E} : \operatorname{ht}(E) \leq X\}$. We then study the count of those $E \in \mathscr{E}_{\leq X}$ which admit (or are equipped with) additional level structure as $X \to \infty$, and then do so more generally over global fields.

In recent work, many instances of this problem have been resolved. For example, we count elliptic curves E for which the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ of the Mordell–Weil group is isomorphic to a given a finite abelian group T, i.e., studying $\#\{E \in \mathscr{E}_{\leq X} : E(\mathbb{Q})_{\text{tors}} \simeq T\}$ as $X \to \infty$. We may restrict to the fifteen groups T indicated by Mazur's theorem on torsion [13], where the classical modular curve $Y_1(N)$ parametrizing elliptic curves equipped with an N-torsion point has genus zero and infinitely many points. For such T, Harron–Snowden [9] and Cullinan–Kenney–Voight [5] (see also previous work of Duke [7] and Grant

[8]) established an asymptotic with an effectively computable constant and a power-saving error term. Moreover, satisfactory interpretations of the exponent of X and the constants appearing in these asymptotics are provided. The main ingredients in the proof are the Principle of Lipschitz (also called Davenport's Lemma [6]) and an elementary sieve.

Moving on, we consider asymptotics for

$$\#\{E \in \mathscr{E}_{\leq X} : E \text{ admits a cyclic } N\text{-isogeny}\} \tag{1.1.2}$$

(where we mean that the N-isogeny is defined over $\mathbb{Q}$). Our attention is again first drawn to the cases where the modular curve $Y_0(N)$, parametrizing elliptic curves with a cyclic N-isogeny, has genus zero: namely, $N = 1, \dots, 10, 12, 13, 16, 18, 25$. For $N \leq 4$, we again have an explicit power-saving asymptotic, with the case $N = 3$ due to Pizzo–Pomerance–Voight [15] and the case $N = 4$ due to Pomerance–Schaefer [16]. For all but four of the remaining values, namely $N = 7, 10, 13, 25$, Boggess–Sankar [3] provide at least the correct growth rate. For both torsion and isogenies, work of Bruin–Najman [4] and Phillips [14] extend these counts to a general number field K.

However, the remaining four cases have quite stubbornly resisted these methods. The obstacle can be seen in quite elementary terms: the 'universal' elliptic curve with an N-isogeny is of the form $dy^2 = x^3 + A(t)x + B(t)$ with $A(t), B(t) \in \mathbb{Q}[t]$ (for $t \in \mathbb{Q}$ away from a finite set and $d \in \mathbb{Z}$ a squarefree twisting parameter), and for these four values of N we have $\gcd(A(t), B(t)) \neq 1$. Phrased geometrically, the corresponding 'universal' elliptic surface over $\mathbb{P}^1$ has places of additive reduction. Either way, this breaks the sieve—and new techniques are required.

1.2. **Results.** For $X \geq 1$, we define

$$N_7(X) := \#\{E \in \mathscr{E}_{\leq X} : E \text{ admits a cyclic 7-isogeny}\}.$$

Our main result is as follows (Theorem 5.2.3).

Theorem 1.2.1. *There exist effectively computable $c_1, c_2 \in \mathbb{R}_{>0}$ such that for every $\epsilon > 0$, we have*

$$N_7(X) = c_1 X^{1/6} \log X + c_2 X^{1/6} + O(X^{7/45+\epsilon})$$

as $X \to \infty$, where the implied constant depends on ϵ.

The constants c_1, c_2 in Theorem 1.2.1 are explicitly given, and estimated numerically in section 6 as $c_1 = 0.0928556\dots$ and $c_2 \approx -0.8$. It turns out that no elliptic curve over $\mathbb{Q}$ admits two 7-isogenies with distinct kernels (Proposition 2.2.5), so $N_7(X)$ also counts elliptic curves *equipped with* a 7-isogeny.

The first step in our strategy to prove Theorem 1.2.1 diverges from the methods of Boggess–Sankar [3] and Phillips [14], where the twists are a resolved by use of a certain modular curve (denoted by $X_{1/2}(N)$). Instead, we first count twist classes directly, as follows. Let $\mathbb{Q}^{\mathrm{al}}$ be an algebraic closure of $\mathbb{Q}$. Up to isomorphism *over* $\mathbb{Q}^{\mathrm{al}}$, every elliptic curve E over $\mathbb{Q}$ with $j(E) \neq 0, 1728$ has a unique Weierstrass model (1.1.1) with the additional property that $B > 0$ and no prime ℓ has $\ell^2 \mid A$ and $\ell^3 \mid B$; such a model is called twist minimal. (See section 2.1 for $j(E) = 0, 1728$.) Let $\mathscr{E}^{\mathrm{tw}} \subset \mathscr{E}$ be the set of twist minimal elliptic curves, and let $\mathscr{E}^{\mathrm{tw}}_{\leq X} := \mathscr{E}^{\mathrm{tw}} \cap \mathscr{E}_{\leq X}$ be those with height at most X. Accordingly, we obtain asymptotics for

$$N_7^{\mathrm{tw}}(X) := \#\{E \in \mathscr{E}^{\mathrm{tw}}_{\leq X} : E \text{ admits a cyclic 7-isogeny}\}$$

as follows (Theorem 4.2.16).

Theorem 1.2.2. *We have*

$$N_7^{\mathrm{tw}}(X) = 3\zeta(2)c_1 X^{1/6} + O(X^{2/15}\log^3 X)$$

as $X \to \infty$, with c_1 as in Theorem 1.2.1.

For an outline of the proof, see section 4.1. The use of the Principle of Lipschitz remains fundamental, but the sieving is more involved: we decompose the function into progressively simpler pieces that can be estimated. We then deduce Theorem 1.2.1 from Theorem 1.2.2 by counting twists using a Tauberian theorem (attributed to Landau). In upcoming work, we expect to extend our methods to resolve the remaining three cases $N = 10, 13, 25$.

1.3. **Contents.** In section 2, we set up basic notation and investigate minimal twists. In section 3, we tersely review some needed facts from analytic number theory. In section 4, we pull together material from the earlier sections to prove Theorem 1.2.2. In section 5, we use Landau's Tauberian theorem and Theorem 1.2.2 to obtain Theorem 1.2.1. In section 6, we describe algorithms to compute the various quantities we study in this paper, and report on their outputs.

1.4. **Acknowledgements.** The authors would like to thank Eran Assaf, Mits Kobayashi, Taylor Petty, Carl Pomerance, and Rakvi for their helpful comments. The authors were supported by a Simons Collaboration grant (550029, to JV).

2. Elliptic curves and isogenies

In this section, we set up what we need from the theory of elliptic curves.

2.1. **Height, minimality, and defect.** We begin with some notation and terminology (repeating and elaborating upon the introduction); we refer to Silverman [17, Chapter III] for background.

Let E be an elliptic curve over $\mathbb{Q}$. Recall that a (simplified) integral Weierstrass equation for E is an affine model of the form

$$y^2 = x^3 + Ax + B \tag{2.1.1}$$

with $A, B \in \mathbb{Z}$. Let

$$H(A,B) := \max(\lvert 4A^3 \rvert, \lvert 27B^2 \rvert). \tag{2.1.2}$$

The largest $d \in \mathbb{Z}_{>0}$ such that $d^4 \mid A$ and $d^6 \mid B$ is called the minimality defect $\mathrm{md}(A,B)$ of the model. We then define the height of E to be

$$\mathrm{ht}(E) = \mathrm{ht}(A,B) := \frac{H(A,B)}{\mathrm{md}(A,B)^{12}}, \tag{2.1.3}$$

well-defined up to isomorphism. In fact, E (up to isomorphism over $\mathbb{Q}$) has unique minimal model

$$y^2 = x^3 + (A/d^4)x + (B/d^6)$$

with minimality defect $d = 1$. Let $\mathscr{E}$ be the set of elliptic curves over $\mathbb{Q}$ in their minimal model, and let

$$\mathscr{E}_{\le X} := \{E \in \mathscr{E} : \mathrm{ht}(E) \le X\}. \tag{2.1.4}$$

Let $\mathbb{Q}^{\mathrm{al}}$ be an algebraic closure of $\mathbb{Q}$. We may similarly consider all integral Weierstrass equations for E which define a curve isomorphic to E *over* $\mathbb{Q}^{\mathrm{al}}$—these are the **twists** of E (defined over $\mathbb{Q}$). Let E have $j(E) \neq 0, 1728$. We call the largest $e \in \mathbb{Z}_{>0}$ such that $e^2 \mid A$ and $e^3 \mid B$ the **twist minimality defect** of a model (2.1.1), denoted $\operatorname{tmd}(A, B)$. Explicitly, we have

$$\text{(2.1.5)} \qquad \operatorname{tmd}(E) = \operatorname{tmd}(A, B) := \prod_{\ell} \ell^{v_\ell}, \quad \text{where } v_\ell := \lfloor \min(\operatorname{ord}_\ell(A)/2, \operatorname{ord}_\ell(B)/3) \rfloor,$$

with the product over all primes ℓ. As above, we then define the **twist height** of E to be

$$\text{(2.1.6)} \qquad \operatorname{twht}(E) = \operatorname{twht}(A, B) := \frac{H(A, B)}{\operatorname{tmd}(A, B)^6},$$

well-defined on the $\mathbb{Q}^{\mathrm{al}}$-isomorphism class of E; and E has a unique model over $\mathbb{Q}$ up to isomorphism over $\mathbb{Q}^{\mathrm{al}}$ with twist minimality defect $e = 1$ and $B > 0$, which we call **twist minimal**, namely,

$$\text{(2.1.7)} \qquad y^2 = x^3 + (A/e^2)x + |B|/e^3.$$

For $j = 0, 1728$, we choose twist minimal models as follows:

- If $j(E) = 0$ (equivalently, $A = 0$), then we take $y^2 = x^3 + 1$ of twist height 27.
- If $j(E) = 1728$ (equivalently, $B = 0$), then we take $y^2 = x^3 + x$ of twist height 4.

Let $\mathscr{E}^{\mathrm{tw}} \subset \mathscr{E}$ be the set of twist minimal elliptic curves, and let $\mathscr{E}^{\mathrm{tw}}_{\leq X} := \mathscr{E}^{\mathrm{tw}} \cap \mathscr{E}_{\leq X}$ be those with twist height at most X. If $E \in \mathscr{E}^{\mathrm{tw}}$ with $j(E) \neq 0, 1728$, then the set of twists of E in $\mathscr{E}$ are precisely those of the form $E^{(c)}\colon y^2 = x^3 + c^2Ax + c^3B$ for $c \in \mathbb{Z}$ squarefree, and

$$\text{(2.1.8)} \qquad \operatorname{ht}(E^{(c)}) = c^6 \operatorname{ht}(E) = c^6 \operatorname{twht}(E).$$

(For $j(E) = 0, 1728$, we instead have sextic and quartic twists, but these will not figure here: see Proposition 2.2.5.)

Remark 2.1.9. This setup records in a direct manner the more intrinsic notions of height coming from moduli stacks. The moduli stack $Y(1)_{\mathbb{Q}}$ of elliptic curves admits an open immersion into a weighted projective line $Y(1) \hookrightarrow \mathbb{P}(4, 6)_{\mathbb{Q}}$ by $E \mapsto (A : B)$ for any choice of model (2.1.1), and the height of E is the height of the point $(A : B) \in \mathbb{P}(4, 6)(\mathbb{Q})$ associated to $\mathscr{O}_{\mathbb{P}(4,6)}(12)$ (with coordinates harmlessly scaled by 4, 27): see Bruin–Najman [4, §2, §7] and Phillips [14, §2.2]. Similarly, the height of the twist minimal model is given by the height of the point $(A : B) \in \mathbb{P}(2, 3)$ associated to $\mathscr{O}_{\mathbb{P}(2,3)}(6)$, which is almost but not quite the height of the j-invariant (in the usual sense).

2.2. **Isogenies of degree 7.** Next, we gather the necessary input from modular curves. Recall that the modular curve $Y_0(7)$, defined over $\mathbb{Q}$, parametrizes pairs (E, ϕ) of elliptic curves E equipped with a 7-isogeny up to isomorphism, or equivalently a cyclic subgroup of order 7 stable under the absolute Galois group $\operatorname{Gal}_{\mathbb{Q}} := \operatorname{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$. We compute that the coarse space of $Y_0(7)$ is an affine open in $\mathbb{P}^1$, so the objects of interest are parametrized by its coordinate $t \neq -7, \infty$ (see Lemma 2.2.2).

More precisely, define

$$\begin{aligned}
f_0(t) &:= -3(t^2 - 231t + 735),\\
&= -3(t^2 - (3\cdot 7\cdot 11)t + (3\cdot 5\cdot 7^2))\\
g_0(t) &:= 2(t^4 + 518t^3 - 11025t^2 + 6174t - 64827)\\
&= 2(t^4 + (2\cdot 7\cdot 31)t^3 - (3^2\cdot 5^2\cdot 7^2)t^2 + (2\cdot 3^2\cdot 7^3)t - (3^3\cdot 7^4))\\
h(t) &:= t^2 + t + 7,\\
f(t) &:= f_0(t)h(t),\\
g(t) &:= g_0(t)h(t).
\end{aligned} \tag{2.2.1}$$

Then $h(t) = \gcd(f(t), g(t))$.

Lemma 2.2.2. *The set of elliptic curves E over $\mathbb{Q}$ that admit a 7-isogeny (defined over $\mathbb{Q}$) are precisely those of the form $E\colon y^2 = x^3 + c^2 f(t)x + c^3 g(t)$ for some $c \in \mathbb{Q}^\times$ and $t \in \mathbb{Q}$ with $t \neq -7$.*

Proof. Routine calculations with q-expansions for modular forms on the group $\Gamma_0(7)$, with the cusps at $t = -7, \infty$. □

Of course, for elliptic curves up to isomorphism over $\mathbb{Q}^{\text{al}}$, we can ignore the factor c in Lemma 2.2.2.

Remark 2.2.3. Let

$$\begin{aligned}
f_0'(t) &:= -3(t^2 + 9t + 15),\\
&= -3(t^2 + (3^2)t + (3\cdot 5))\\
g_0'(t) &:= 2(t^4 + 14t^3 + 63t^2 + 126t + 189)\\
&= 2(t^4 + (2\cdot 7)t^3 + (3^2\cdot 7)t^2 + (2\cdot 3^2\cdot 7)t + (3^3\cdot 7))\\
f'(t) &:= f_0'(t)h(t),\\
g'(t) &:= g_0'(t)h(t),
\end{aligned} \tag{2.2.4}$$

with $h(t)$ as above. The elliptic curve E in Lemma 2.2.2 is 7-isogenous to

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

via the marked 7-isogeny.

Proposition 2.2.5. *No elliptic curve E over $\mathbb{Q}$ admits two 7-isogenies with distinct kernels, and no E over $\mathbb{Q}$ with $j(E) = 0, 1728$ admits a 7-isogeny.*

Proof. For the first statement: if E admits two distinct 7-isogenies, then generators for each kernel give a basis for the 7-torsion of E in which $\mathrm{Gal}_\mathbb{Q}$ acts diagonally. The corresponding completed modular curve, $X_{\text{sp}}(7)$ has genus 1 and 2 rational cusps; it is isomorphic to $X_0(49)$ over $\mathbb{Q}$, and has Weierstrass equation $y^2 + xy = x^3 - x^2 - 2x - 1$ and LMFDB label 49.a4. Its Mordell–Weil group is $\mathbb{Z}/2\mathbb{Z}$, so all rational points are cusps.

For the second statement, we simply observe that $f(t)$ and $g(t)$ have no roots $t \in \mathbb{Q}$. □

To work with integral models, we take $t = a/b$ (in lowest terms) and homogenize, giving the following polynomials in $\mathbb{Z}[a,b]$:

$$\begin{aligned} C(a,b) &:= b^2 h(a/b) = a^2 + ab + 7b^2, \\ A_0(a,b) &:= b^2 f_0(a/b) = -3(a^2 - 231ab + 735b^2), \\ B_0(a,b) &:= b^4 g_0(a/b) = 2(a^4 + 518a^3b - 11025a^2b^2 + 6174ab^3 - 64827b^4), \\ A(a,b) &:= b^4 f(a/b) = C(a,b)A_0(a,b) \\ B(a,b) &:= b^6 f(a/b) = C(a,b)B_0(a,b). \end{aligned} \tag{2.2.6}$$

We have $C(a,b) = \gcd(A(a,b), B(a,b)) \in \mathbb{Z}[a,b]$.

We say that a pair $(a,b) \in \mathbb{Z}^2$ is **groomed** if $\gcd(a,b) = 1$, $b > 0$, and $(a,b) \neq (-7,1)$. Thus Lemma 2.2.2 and Proposition 2.2.5 provide that the elliptic curves $E \in \mathscr{E}$ that admit a 7-isogeny are precisely those with a model

$$y^2 = x^3 + \frac{c^2 A(a,b)}{d^4} x + \frac{c^3 B(a,b)}{d^6} \tag{2.2.7}$$

where (a,b) is groomed, $c \in \mathbb{Z}$ is squarefree, and $d = \operatorname{md}(c^2A(a,b), c^3B(a,b))$. Thus the count

$$N_7(X) := \#\{E \in \mathscr{E}_{\leq X} : E \text{ admits a cyclic 7-isogeny}\} \tag{2.2.8}$$

can be computed as

$$N_7(X) = \#\left\{(a,b,c) \in \mathbb{Z}^3 : \begin{array}{l} (a,b) \text{ groomed, } c \text{ squarefree, and} \\ \operatorname{ht}(c^2A(a,b), c^3B(a,b)) \leq X \end{array}\right\}. \tag{2.2.9}$$

with the height defined as in (2.1.3).

Similarly, but more simply, the subset of $E \in \mathscr{E}^{\mathrm{tw}}$ that admit a 7-isogeny are

$$E_{a,b}\colon y^2 = x^3 + \frac{A(a,b)}{e^2} x + \frac{|B(a,b)|}{e^3} \tag{2.2.10}$$

with (a,b) groomed and $e = \operatorname{tmd}(A(a,b), B(a,b))$ the twist minimality defect (2.1.5). Accordingly, if we define

$$N_7^{\mathrm{tw}}(X) := \#\{E \in \mathscr{E}^{\mathrm{tw}}_{\leq X} : E \text{ admits a cyclic 7-isogeny}\} \tag{2.2.11}$$

then

$$N_7^{\mathrm{tw}}(X) = \#\left\{(a,b) \in \mathbb{Z}^2 : (a,b) \text{ groomed and } \operatorname{twht}(A(a,b), B(a,b)) \leq X\right\}. \tag{2.2.12}$$

2.3. **Twist minimality defect.** The twist minimality defect is the main subtlety in our study of $N_7^{\mathrm{tw}}(X)$, so we analyze it right away.

Lemma 2.3.1. *Let $(a,b) \in \mathbb{Z}^2$ be groomed, let ℓ be prime, and let $v \in \mathbb{Z}_{\geq 0}$. Then the following statements hold.*

(a) *If $\ell \neq 3, 7$, then $\ell^v \mid \operatorname{tmd}(A(a,b), B(a,b))$ if and only if $\ell^{3v} \mid C(a,b)$.*
(b) *$\ell^{3v} \mid C(a,b)$ if and only if $\ell \nmid b$ and $h(a/b) \equiv 0 \pmod{\ell^{3v}}$.*
(c) *If $\ell \neq 3$, then $\ell \mid C(a,b)$ implies $\ell \nmid (2a+b) = (\partial C/\partial a)(a,b)$.*

Proof. We use the notation (2.2.6) and argue as in Cullinan–Kenney–Voight [5, Proof of Theorem 3.3.1, Step 3]. For part (a), we compute the resultants

$$\operatorname{Res}(A_0(t,1), B_0(t,1)) = \operatorname{Res}(f_0(t), g_0(t)) = -2^8 \cdot 3^7 \cdot 7^{14} = \operatorname{Res}(A_0(1,u), B_0(1,u)).$$

So if $\ell \neq 2,3,7$, then $\ell \nmid \gcd(A_0(a,b), B_0(a,b))$; so by (2.1.5), if $\ell^v \mid \operatorname{tmd}(A(a,b), B(a,b))$ then $\ell^{2v} \mid C(a,b)$. But also

$$\operatorname{Res}(B_0(t,1), C(t,1)) = \operatorname{Res}(g_0(t), h(t)) = 2^8 \cdot 3^3 \cdot 7^7 = \operatorname{Res}(B_0(1,u), C(1,u)),$$

so $\ell \nmid \gcd(B_0(a,b), C(a,b))$ and thus $\ell^v \mid \operatorname{tmd}(A(a,b), B(a,b))$ if and only if $\ell^{3v} \mid C(a,b)$. If $\ell = 2$, a short computation confirms that $B(a,b)$ is odd whenever (a,b) is groomed, so our claim also holds in this case.

For (b), by homogeneity it suffices to show that $\ell \nmid b$, and indeed this holds since if $\ell \mid b$ then $A(a,0) \equiv -3a^4 \equiv 0 \pmod{\ell}$ and $B(b,0) \equiv 2a^6 \equiv 0 \pmod{\ell}$ so $\ell \mid a$, a contradiction.

Part (c) follows from (b) and the fact that $h(t)$ has discriminant $\operatorname{disc}(h(t)) = 3^3$. □

Although the twist minimality defect can be somewhat subtle, it is a bit simpler to understand when $e \mid \operatorname{tmd}(A(a,b), B(a,b))$.

For $e \geq 1$, let $\widetilde{\mathcal{T}}(e)$ denote the set of pairs $(a,b) \in (\mathbb{Z}/e^3\mathbb{Z})^2$ such that

- $A(a,b) \equiv 0 \pmod{e^2}$ and $B(a,b) \equiv 0 \pmod{e^3}$, and
- $\ell \nmid \gcd(a,b)$ for all primes $\ell \mid e$.

Let $\widetilde{T}(e) := \#\widetilde{\mathcal{T}}(e)$. Similarly, let

$$\mathcal{T}(e) := \{t \in (\mathbb{Z}/e^3\mathbb{Z})^\times : e^2 \mid f(t) \text{ and } e^3 \mid g(t)\} \tag{2.3.2}$$

and let $T(e) := \#\mathcal{T}(e)$.

Lemma 2.3.3. *The following statements hold.*

(a) $\widetilde{\mathcal{T}}(e)$ *is the image of*

$$\left\{(a,b) \in \mathbb{Z}^2 : (a,b) \text{ groomed},\ e \mid \operatorname{tmd}(A(a,b), B(a,b))\right\}$$

under the projection

$$\mathbb{Z}^2 \to (\mathbb{Z}/e^3\mathbb{Z})^2.$$

(b) *The functions $\widetilde{T}(e)$ and $T(e)$ are multiplicative, and $\widetilde{T}(e) = \varphi(e^3)T(e)$.*

(c) *For all $\ell \neq 3,7$ and $v \geq 1$,*

$$T(\ell^v) = T(\ell) = 1 + \left(\frac{\ell}{3}\right).$$

(d) *We have*

$$T(3) = 18,\ T(3^2) = 27,\ \text{and}\ T(3^v) = 0 \text{ for } v \geq 3,$$

and

$$T(7) = 50,\ T(7^2) = 7^4 + 1 = 2402,\ \text{and}\ T(7^v) = 7^7 + 1 = 823544 \text{ for } v \geq 3.$$

(e) *We have $T(e) = O(2^{\omega(e)})$, where $\omega(e)$ is the number of distinct prime divisors of e.*

Proof. Part (a) is immediate from the definition.

For part (b), multiplicativity follows from the CRT (Sun Zi theorem). For the second statement, let ℓ be a prime, and let $e = \ell^v$ for some $v \geq 1$. Consider the injective map

$$\begin{aligned} \mathcal{T}(\ell^v) \times (\mathbb{Z}/\ell^{3v})^\times &\to \widetilde{\mathcal{T}}(\ell^v) \\ (t, u) &\mapsto (tu, u) \end{aligned} \tag{2.3.4}$$

This map is surjective by Lemma 2.3.1(b), so counting both sides gives the result.

Now part (c). For $\ell \neq 3, 7$, Lemma 2.3.1(a)–(b) yield

$$\mathcal{T}(\ell^v) = \left\{ t \in \mathbb{Z}/\ell^{3v}\mathbb{Z} : h(t) \equiv 0 \pmod{\ell^{3v}} \right\}.$$

By Lemma 2.3.1(c), $h(t) \equiv 0 \pmod{\ell}$ implies $h'(t) \not\equiv 0 \pmod{\ell}$, so Hensel's lemma applies and we need only count roots of $h(t)$ modulo ℓ, which by quadratic reciprocity is

$$1 + \left(\frac{-3}{\ell}\right) = 1 + \left(\frac{\ell}{3}\right) = \begin{cases} 2, & \text{if } \ell \equiv 1 \pmod{3}; \\ 0, & \text{else.} \end{cases}$$

Next, part (d). For $\ell = 3$, we just compute $T(3) = 18$, $T(3^2) = 27$, and $T(3^3) = 0$; then $T(3^3) = 0$ implies $T(3^v) = 0$ for all $v \geq 3$. For $\ell = 7$, we compute

$$T(7) = 50,\ T(7^2) = 2402,\ T(7^3) = \cdots = T(7^6) = 823544.$$

Hensel's lemma still applies to $h(t)$: let t_0, t_1 be the roots of $h(t)$ in $\mathbb{Z}_7$ with $t_0 := 248044 \pmod{7^7}$ (so that $t_1 = -1 - t_0$). We claim that

$$\mathcal{T}(7^{3v}) = \{t_0\} \sqcup \left\{ t_1 + 7^{3v-7}u \in \mathbb{Z}/7^{3v}\mathbb{Z} : u \in \mathbb{Z}/7^7\mathbb{Z} \right\}, \tag{2.3.5}$$

for $3v \geq 7$. Indeed, $g_0(t_1) \equiv 0 \pmod{7^7}$, so we can afford to approximate t_1 modulo 7^{3v-7}. As $g(t_0) \not\equiv 0 \pmod{7}$ and $g(t_1) \not\equiv 0 \pmod{7^8}$, no other values of t suffice. Thus $T(7^{3v}) = 1 + 7^7 = 823544$.

Finally, part (e). From (b)–(d) we conclude

$$T(e) \leq 27 \cdot 823544 \cdot \prod_{\substack{\ell \mid e \\ \ell \neq 3,7}} \left(1 + \left(\frac{\ell}{3}\right)\right) \leq 2^{\omega(e)} \leq 5558922 \cdot 2^{\omega(e)}$$

so $T(e) = O(2^{\omega(e)})$ as claimed. $\square$

2.4. **The common factor $C(a, b)$.** In view of Lemma 2.3.1, the twist minimality defect away from the primes $2, 3, 7$ is given by the quadratic form $C(a, b) = a^2 + ab + 7b^2 = b^2 h(a/b)$. Fortunately, this is the norm form of a quadratic order of class number 1, so although this is ultimately more than what we need, we record some consequences of this observation which take us beyond Lemma 2.3.3.

For m a nonnegative integer, let

$$c(m) := \#\{(a, b) \in \mathbb{Z}^2 : b > 0,\ \gcd(a, b) = 1,\ C(a, b) = m\}. \tag{2.4.1}$$

Lemma 2.4.2. *The following statements hold.*

(a) *We have $c(mn) = c(m)c(n)$ for $m, n \in \mathbb{Z}_{>0}$ coprime.*

(b) *We have*

$$c(3) = 0,\ c(3^2) = 2,\ c(3^3) = 3,\ \textit{and}\ c(3^v) = 0\ \textit{for}\ v \geq 4;$$

for $p \neq 3$ prime and $k \geq 1$ an integer, we have

$$c(p) = c(p^k) = 1 + \left(\frac{p}{3}\right). \tag{2.4.3}$$

(c) *For m and n positive integers, we have*

$$c(n^3 m) \leq 3 \cdot 2^{\omega(n)-1} c(m).$$

Proof. Let $\zeta := (1+\sqrt{-3})/2$, so $\overline{\zeta} = 1-\zeta = (1-\sqrt{-3})/2$. The quadratic form

$$C(a,b) = a^2 + ab + 7b^2 = (a + b(-1+3\zeta))(a + b\overline{(-1+3\zeta)}) = \mathrm{Nm}(a + b(-1+3\zeta))$$

is the norm on the order $\mathbb{Z}[3\zeta]$ in basis $\{1, -1+3\zeta\}$. Recall that $\alpha \in \mathbb{Z}[3\zeta]$ is primitive if no $n \in \mathbb{Z}_{>1}$ divides α. Thus, accounting for sign,

$$2c(m) = \#\{\alpha \in \mathbb{Z}[3\zeta] \text{ primitive} : \mathrm{Nm}(\alpha) = m\}. \tag{2.4.4}$$

The order $\mathbb{Z}[3\zeta]$ is a suborder of the Euclidean domain $\mathbb{Z}[\zeta]$ of conductor 3. It inherits from $\mathbb{Z}[\zeta]$ the following variation on unique factorization: up to sign, every nonzero $\alpha \in \mathbb{Z}[3\zeta]$ can be written uniquely as

$$\alpha = \beta \pi_1^{e_1} \cdots \pi_r^{e_r},$$

where $\mathrm{Nm}(\beta)$ is a power of 3, $\pi_1, \ldots, \pi_r$ are distinct irreducibles coprime to 3, and $e_1, \ldots, e_r$ are positive integers. Note that α is primitive if and only if β is primitive and for $1 \leq i, j \leq r$ (not necessarily distinct) we have $\pi_i \neq \overline{\pi_j}$. Thus if m and n are coprime integers, $\alpha \in \mathbb{Z}[3\zeta]$ is primitive, and $\mathrm{Nm}(\alpha) = mn$, then α may be factored uniquely (up to sign) as $\alpha = \alpha_1\alpha_2$, where $\mathrm{Nm}(\alpha_1) = m$ and $\mathrm{Nm}(\alpha_2) = n$. This proves (a).

We now prove (b). If $p \neq 3$ is inert in $\mathbb{Z}[3\zeta]$ (equivalently, in $\mathbb{Z}[\zeta]$), then no primitive α satisfies $\mathrm{Nm}(\alpha) = p^v$, so $c(p^v) = 0$. If $p \neq 3$ splits in $\mathbb{Z}[3\zeta]$ (equivalently, in $\mathbb{Z}[\zeta]$), then no primitive α is divisible by more than one of the two primes above p, so $c(p^v) = 2$. This proves (2.4.3) (compare Lemma 2.3.3). Finally, if $p = 3$, we compute $c(3) = 0$, $c(3^2) = 2$, and $c(3^3) = 3$. Congruence conditions show $c(3^v) = 0$ for $v \geq 4$.

Part (c) follows immediately from (a) and (b). ☐

Remark 2.4.5. We prove Lemma 2.4.2(a) and Lemma 2.4.2(b) only as a means to proving Lemma 2.4.2(c). Although the algebraic structure of the Eisenstein integers $\mathbb{Z}[\zeta]$ may not be available in the study of other families of elliptic curves that exhibit potential additive reduction, we expect analogues of Lemma 2.4.2(c) to hold in a general context.

The twist minimality defect measures the discrepancy between $H(A,B)$ and $\mathrm{twht}(A,B)$: this discrepancy cannot be too large compared to $C(a,b)$, as the following theorem shows.

Theorem 2.4.6. *We have the following.*

(a) *For all $(a,b) \in \mathbb{R}^2$, we have*

$$108C(a,b)^6 \leq H(A(a,b), B(a,b)) \leq \kappa C(a,b)^6,$$

where $\kappa = 3.114068719902043\ldots \cdot 10^8$ is explicitly computable.

(b) *If* $C(a,b) = e_0^3 m$*, with* m *cubefree, then* $\operatorname{tmd}(A(a,b), B(a,b)) = e_0 e'$ *for some* $e' \mid 3\cdot 7^3$*, and*

$$\frac{2^2}{3^3 \cdot 7^{18}} e_0^{12} m^6 \le \operatorname{twht}(A(a,b), B(a,b)) \le \kappa e_0^{12} m^6.$$

Proof. We wish to find the extrema of $H(A(a,b), B(a,b))/C(a,b)^6$. As this expression is homogeneous of degree 0, and $C(a,b)$ is positive definite, we may assume without loss of generality that $C(a,b) = 1$. But the level set

$$\left\{(a,b) \in \mathbb{R}^2 : C(a,b) = a^2 + ab + 7b^2 = 1\right\}$$

is parameterized by the function

$$\phi : \theta \mapsto \left(\cos\theta - \frac{1}{3\sqrt{3}}\sin\theta, \frac{2}{3\sqrt{3}}\sin\theta\right).$$

We can now use a computer to show

$$\min_\theta H(A(\phi(\theta)), B(\phi(\theta))) = 108, \text{and}$$
$$\max_\theta H(A(\phi(\theta)), B(\phi(\theta))) =: \kappa = 3.114068719902043 \cdot 10^8.$$

It is straightforward to show $H(A(1,0), B(1,0)) = 108$ but

$$\frac{H(A(a,1), B(a,1))}{C(a,1)^6} > 108$$

for all a, so this value is exact.

Now write $C(a,b) = e_0^3 m$ with m cubefree, and write $\operatorname{tmd}(A(a,b), B(a,b)) = e_0 e'$. By Lemma 2.3.1, $e' = 3^v 7^w$ for some $v, w \ge 0$; a short computation shows $v \in \{0,1\}$, and (2.3.5) shows $w \le \lceil 7/3 \rceil = 3$. Now as

$$H(A(a,b), B(a,b)) = e_0^6 (e')^6 \operatorname{twht}(A(a,b), B(a,b)),$$

we see

$$\frac{108}{(e')^6} e_0^{12} m^6 \le \operatorname{twht}(A(a,b), B(a,b)) < \frac{\kappa}{(e')^6} e_0^{12} m^6.$$

Rounding e' up to $3 \cdot 7^3$ on the left and down to 1 on the right gives the desired result. □

Corollary 2.4.7. *Let* (a,b) *be a groomed pair. We have*

$$\operatorname{tmd}(A(a,b), B(a,b)) \le \frac{3^{5/4} \cdot 7^{9/2}}{2^{1/6}} \operatorname{twht}(A(a,b), B(a,b))^{1/12}$$

where $3^{5/4} \cdot 7^{9/2}/2^{1/6} = 22344.5\ldots$

Proof. In the notation of Theorem 2.4.6(b),

$$e_0^{12} m^6 \le \frac{(e')^6}{108} \operatorname{twht}(A(a,b), B(a,b)).$$

Multiplying through by $(e')^{12}$, rounding m down to 1 on the left, rounding e' up to $3 \cdot 7^7$ on the right, and taking 12th roots of both sides, we obtain the desired result. □

3. Analytic ingredients

In this section, we record some results from analytic number theory used later.

3.1. **Lattices and the principle of Lipschitz.** We recall (a special case of) the Principle of Lipschitz, also known as Davenport's Lemma.

Theorem 3.1.1 (Principle of Lipschitz)**.** *Let $\mathcal{R} \subseteq \mathbb{R}^2$ be a closed and bounded region, with rectifiable boundary $\partial\mathcal{R}$. We have*

$$\#(\mathcal{R} \cap \mathbb{Z}^2) = \operatorname{area}(\mathcal{R}) + O(\operatorname{len}(\partial R)),$$

where the implicit constant depends on the similarity class of $\mathcal{R}$, but not on its size, orientation, or position in the plane $\mathbb{R}^2$.

Proof. See Davenport [6]. □

Specializing to the case of interest, for $X \geq 0$ let

$$\mathcal{R}(X) := \left\{(a,b) \in \mathbb{R}^2 : H(A(a,b), B(a,b)) \leq X,\ b \geq 0\right\}, \tag{3.1.2}$$

and let $R := \operatorname{area}(\mathcal{R}(1))$. The region $\mathcal{R}(1)$ is the common region in Figure 3.1.3.

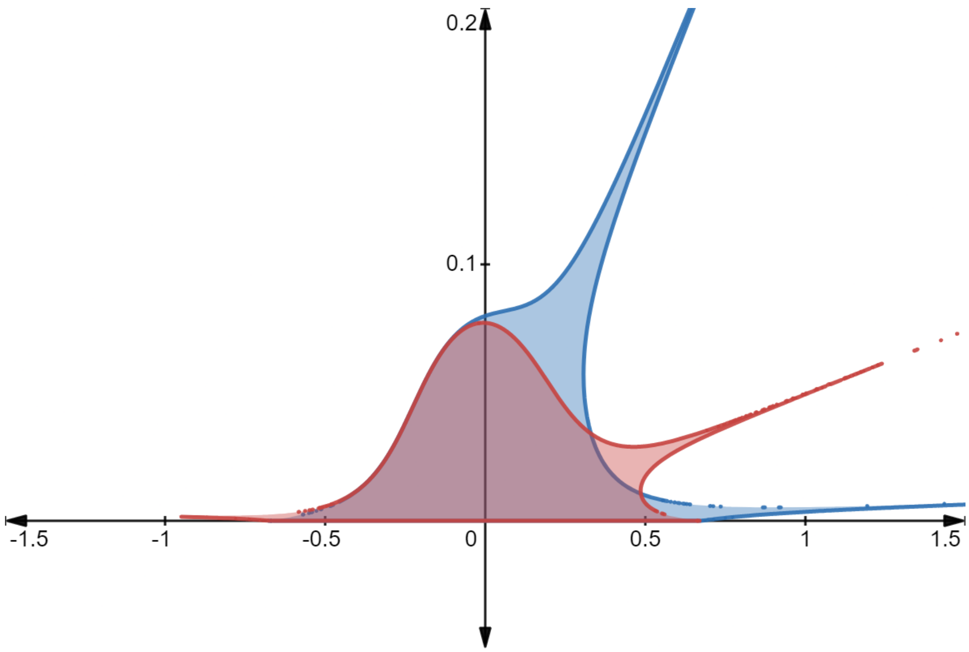

Figure 3.1.3: The region $\mathcal{R}(1)$

Lemma 3.1.4. *For $X > 0$, we have $\operatorname{area}(\mathcal{R}(X)) = RX^{1/6}$.*

Proof. Since $f(t) = A(t,1)$ and $g(t) = B(t,1)$ have no common real root, the region $\mathcal{R}(X)$ is compact [5, Proof of Theorem 3.3.1, Step 2]. The homogeneity

$$H(A(ua,ub), B(ua,ub)) = u^{12} H(A(a,b), B(a,b))$$

implies

$$\operatorname{area}(\mathcal{R}(X)) = \operatorname{area}(\{(X^{1/12}a, X^{1/12}b) : (a,b) \in \mathcal{R}(1)\}) = X^{1/6} \operatorname{area}(\mathcal{R}(1)) = RX^{1/6}$$

as desired. □

The following corollaries are immediate.

Corollary 3.1.5. *For $a_0, b_0, d \in \mathbb{Z}$ with $d \geq 1$, we have*

$$\#\{(a,b) \in \mathcal{R}(X) \cap \mathbb{Z}^2 : (a,b) \equiv (a_0, b_0) \pmod{d}\} = \frac{RX^{1/6}}{d^2} + O\left(\frac{X^{1/12}}{d}\right).$$

The implied constants are independent of X, d, a_0, and b_0. In particular,

$$\#(\mathcal{R}(X) \cap \mathbb{Z}^2) = RX^{1/6} + O(X^{1/12}). \tag{3.1.6}$$

Proof. Combine Lemma 3.1.4 and Theorem 3.1.1. □

Corollary 3.1.7. *Let $(c(m))_{m\geq 1}$ be as in (2.4.1). We have*

$$\sum_{m \leq X} c(m) = O(X).$$

Proof. Immediate from Corollary 3.1.5. □

3.2. **Dirichlet series.** The following theorem is attributed to Stieltjes.

Theorem 3.2.1. *Let $\alpha, \beta : \mathbb{Z}_{>0} \to \mathbb{R}$ be arithmetic functions. If $L_\alpha(s) := \sum_{n\geq 1} \alpha(n) n^{-s}$ and $L_\beta(s) := \sum_{n \geq 1} \beta(n) n^{-s}$ both converge when $\mathrm{Re}(s) > \sigma$, and one of these two series converges absolutely, then*

$$L_{\alpha * \beta}(s) := \sum_{n \geq 1} \left(\sum_{d \mid n} \alpha(d) \beta\left(\frac{n}{d}\right) \right) n^{-s}$$

converges for s with $\mathrm{Re}(s) > \sigma$. If both $L_\alpha(s)$ and $L_\beta(s)$ both converge absolutely when $\mathrm{Re}(s) > \sigma$, then so does $L_{\alpha*\beta}(s)$.

Proof. Widder [19, Theorems 11.5 and 11.6b] proves a more general result, or see Tenenbaum [18, proof of Theorem II.1.2, Notes on p. 204]. □

Let $\gamma := \lim_{y \to \infty} \left(\sum_{n \leq y} \frac{1}{n} \right) - \log y$ be the Euler–Mascheroni constant.

Theorem 3.2.2. *The difference*

$$\zeta(s) - \left(\frac{1}{s-1} + \gamma \right)$$

is entire on $\mathbb{C}$ and vanishes at $s = 1$.

Proof. Ivić [10, page 4] proves a more general result. □

3.3. **Regularly varying functions.** We require a fragment of Karamata's integral theorem for regularly varying functions.

Definition 3.3.1. Let $F \colon \mathbb{R}_{\geq 0} \to \mathbb{R}$ be measurable and eventually positive. We say that F is regularly varying of index $\rho \in \mathbb{R}$ if for each $\lambda > 0$ we have

$$\lim_{y \to \infty} \frac{F(\lambda y)}{F(y)} = \lambda^\rho.$$

Theorem 3.3.2 (Karamata's integral theorem)**.** *Let $F \colon \mathbb{R}_{\geq 0} \to \mathbb{R}$ be locally bounded and regularly varying of index ρ. Let $\sigma, \rho \in \mathbb{R}$. Then the following statements hold.*

(a) *For any* $\sigma > \rho + 1$ *(and for* $\sigma = \rho + 1$ *if* $\int_0^\infty t^{-\rho-1} F(t)dt < \infty$*), we have*

$$\int_y^\infty t^{-\sigma} F(t)dt \sim \frac{y^{1-\sigma} F(y)}{|\sigma - \rho - 1|}$$

as $y \to \infty$.

(b) *For any* $\sigma \le \rho + 1$*, we have*

$$\int_0^y t^{-\sigma} F(t)dt \sim \frac{y^{1-\sigma} F(y)}{|\sigma - \rho - 1|}$$

as $y \to \infty$.

Proof. See Bingham–Glodie–Teugels [2, Theorem 1.5.11]. (Karamata's integral theorem also includes a converse.) □

Corollary 3.3.3. *Let* $\alpha\colon \mathbb{Z}_{>0} \to \mathbb{R}$ *be an arithmetic function, and suppose that for some* $\kappa, \rho, \tau \in \mathbb{R}$ *with* $\kappa \neq 0$*, we have*

$$F(y) := \sum_{n \le y} \alpha(n) \sim \kappa y^\rho \log^\tau y \tag{3.3.4}$$

as $y \to \infty$*. Let* $\sigma, \rho > 0$*. Then the following statements hold, as* $y \to \infty$*.*

(a) *If* $\sigma > \rho > 0$*, then*

$$\sum_{n > y} n^{-\sigma} \alpha(n) \sim \frac{\rho y^{-\sigma} F(y)}{|\sigma - \rho|} \sim \frac{\kappa \rho y^{\rho - \sigma} \log^\tau y}{|\sigma - \rho|}.$$

(b) *If* $\rho \ge \sigma > 0$*, then*

$$\sum_{n \le y} n^{-\sigma} \alpha(n) \sim \frac{\rho y^{-\sigma} F(y)}{|\sigma - \rho|} \sim \frac{\kappa \rho y^{\rho - \sigma} \log^\tau y}{|\sigma - \rho|}.$$

Proof. Replacing α and F with $-\alpha$ and $-F$ if necessary, we may assume $\kappa > 0$. As a partial sum of an arithmetic function, $F(y)$ is measurable and locally bounded; by (3.3.4), $F(y)$ is eventually positive. Now for any $\lambda > 0$, we compute

$$\lim_{y \to \infty} \frac{F(\lambda y)}{F(y)} = \lim_{y \to \infty} \frac{\kappa (\lambda y)^\rho \log^\tau (\lambda y)}{\kappa y^\rho \log^\tau y} = \lambda^\rho,$$

so F is regularly varying of index ρ.

Suppose first $\sigma > \rho > 0$. Since

$$y^{-\sigma} F(y) \sim \kappa y^{\rho - \sigma} \log^\tau y \to 0$$

as $y \to \infty$, Abel summation yields

$$\sum_{n > y} n^{-\sigma} \alpha(n) = -y^{-\sigma} F(y) + \sigma \int_y^\infty t^{-\sigma - 1} F(t) dt.$$

Clearly $\sigma + 1 > \rho + 1$, so Theorem 3.3.2(a) tells us

$$\int_y^\infty t^{-\sigma-1} F(t)dt \sim \frac{y^{-\sigma} F(y)}{|\sigma - \rho|} \sim \frac{\kappa y^{\rho - \sigma} \log^\tau y}{|\sigma - \rho|}$$

and thus

$$\sum_{n>y} n^{-\sigma}\alpha(n) \sim \frac{\rho y^{-\sigma}F(y)}{|\sigma-\rho|}$$

as $y\to\infty$.

The case $\rho \geq \sigma > 0$ is similar. ☐

3.4. **Bounding Dirichlet series on vertical lines.** Recall that a complex function $F(s)$ has finite order on a domain D if there exists $\xi \in \mathbb{R}_{>0}$ such that

$$F(s) = O(1+|t|^{\xi})$$

whenever $s=\sigma+it\in D$. If F is of finite order on a right half-plane, we define

$$\mu_F(\sigma) := \inf\{\xi\in\mathbb{R}_{\geq 0} : F(\sigma+it) = O(1+|t|^{\xi})\}$$

where the implicit constant depends on σ and ξ.

Let $L(s)$ be a Dirichlet series with abscissa of absolute convergence σ_a and abscissa of convergence σ_c.

Theorem 3.4.1. *We have $\mu_L(\sigma)=0$ for all $\sigma>\sigma_a$, and $\mu_L(\sigma)$ is nonincreasing (as a function of σ) on any region where L has finite order.*

Proof. Tenenbaum [18, Theorem II.1.21]. ☐

Theorem 3.4.2. *Let $\sigma_0 \leq \sigma_c+1$ and $\epsilon>0$. Then uniformly on*

$$\{s=\sigma+it\in\mathbb{C} : \sigma_0\leq\sigma\leq\sigma_c+1,\ |t|\geq 1\},$$

we have

$$L(\sigma+it) = O(t^{1+\sigma_c-\sigma+\epsilon}).$$

Proof. Tenenbaum [18, Theorem II.1.19]. ☐

Corollary 3.4.3. *For all $\sigma>\sigma_c$, we have*

$$\mu_L(\sigma)\leq \max(0, 1+\sigma_c-\sigma).$$

Proof. It is well-known that $\sigma_a\leq\sigma_c+1$, so the claim holds for $\sigma>\sigma_c+1$ by Theorem 3.4.1. Now for $\sigma_c<\sigma<\sigma_c+1$, our claim follows by letting $\epsilon\to 0$ in Theorem 3.4.2. ☐

Theorem 3.4.4. *For $0\leq\sigma\leq 1$ and $\zeta(s)$ the Riemann zeta function, we have*

$$\mu_\zeta(\sigma)\leq\begin{cases}(3-4\sigma)/6, & \text{if } 0\leq\sigma\leq\frac{1}{2};\\ (1-\sigma)/3, & \text{if } \frac{1}{2}\leq\sigma\leq 1.\end{cases}$$

Proof. Tennenbaum [18, Theorem II.3.8]. ☐

3.5. **A Tauberian theorem.** We now present a Tauberian theorem, due in essence to Landau [11].

Definition 3.5.1. Let $(\alpha(n))_{n\geq 1}$ be a sequence with $\alpha(n)\in\mathbb{R}_{\geq 0}$ for all n, and let $L_\alpha(s) := \sum_{n\geq 1}\alpha(n)n^{-s}$. We say the sequence $(\alpha(n))_{n\geq 1}$ is admissible with (real) parameters (σ_a,δ,ξ) if the following hypotheses hold:

(i) $L_\alpha(s)$ has abscissa of absolute convergence σ_a.

(ii) The function $L_\alpha(s)/s$ has meromorphic continuation to $\{s : \mathrm{Re}(s) > \sigma_a - \delta\}$ and only finitely many poles in this region.
(iii) For $\sigma > \sigma_a - \delta$, we have $\mu_{L_\alpha}(\sigma) \le \xi$.

If $(\alpha(n))_n$ is admissible, let $s_1, \dots, s_r$ denote the poles of $L_\alpha(s)/s$ with real part greater than $\sigma_a - \delta/(\xi+2)$.

The following theorem is essentially an application of Perron's formula, which is itself an inverse Mellin transform.

Theorem 3.5.2 (Landau's Tauberian Theorem). *Let $(\alpha(n))_{n\ge1}$ be an admissible sequence (Definition 3.5.1), and write $N_\alpha(X) := \sum_{n\le X}\alpha(n)$. Then for all $\epsilon > 0$,*

$$N_\alpha(X) = \sum_{j=1}^{r} \mathrm{res}_{s=s_j}\left(\frac{L_\alpha(s)X^s}{s}\right) + O\Big(X^{\sigma_a - \frac{\delta}{\lfloor\xi\rfloor+2}+\epsilon}\Big),$$

where the main term is a sum of residues and the implicit constant depends on ϵ.

Proof. See Roux [12, Theorem 13.3, Remark 13.4]. □

Remark 3.5.3. Landau's original theorem [11] was fitted to a more general context, and allowed sums of the form

$$\sum_{n\ge1}\alpha(n)\ell(n)^{-s}$$

as long as $(\ell(n))_{n\ge1}$ was increasing and tended to ∞. Landau also gave an explicit expansion of

$$\mathrm{res}_{s=s_j}\left(\frac{L_\alpha(s)X^s}{s}\right)$$

in terms of the Laurent series expansion for $L_\alpha(s)$ around $s = s_j$. However, Landau also required that $L_\alpha(s)$ has a meromorphic continuation to all of $\mathbb{C}$, and Roux [12, Theorem 13.3, Remark 13.4] relaxes this assumption.

Let $d(n)$ denote the number of divisors of n, and let $\omega(n)$ denote the number of distinct prime divisors of n. Theorem 3.5.2 has the following easy corollary.

Corollary 3.5.4. *We have*

$$\sum_{n\le y} 2^{\omega(n)} = \frac{y\log y}{\zeta(2)} + O(y) \quad \textit{and} \quad \sum_{n\le y} d(n)^2 = \frac{y\log^3 y}{6\zeta(2)} + O(y\log^2 y).$$

as $y\to\infty$.

Proof. Recall that

$$\frac{\zeta(s)^2}{\zeta(2s)} = \sum_{n\ge1}\frac{2^{\omega(n)}}{n^s} \text{ and } \frac{\zeta(s)^4}{\zeta(2s)} = \sum_{n\ge1}\frac{d(n)^2}{n^s}.$$

It is straightforward to verify that $\{2^{\omega(n)}\}_{n\ge1}$ and $\{d(n)^2\}_{n\ge1}$ are both admissible with parameters $(1, 1/2, 1/3)$. We apply Theorem 3.5.2 and discard lower-order terms to obtain the result. □

Remark 3.5.5. Theorem 3.5.2 furnishes lower order terms for the sums $\sum_{n\le y}2^{\omega(n)}$ and $\sum_{n\le y}d(n)^2$, and even better estimates are known (e.g. Tenenbaum [18, Exercise I.3.54] and Zhai [20, Corollary 4]), but Corollary 3.5.4 suffices for our purposes and illustrates the use of Theorem 3.5.2.

4. Estimates for twist classes

In this section, we decompose $N_7^{\text{tw}}(X)$, counting the number of twist minimal elliptic curves over $\mathbb{Q}$ admitting a 7-isogeny (2.2.11) in terms of progressively simpler functions. We then estimate those simple functions, and piece these estimates together until we arrive at an estimate for $N_7^{\text{tw}}(X)$; the main result is Theorem 4.2.16, which proves Theorem 1.2.2.

4.1. **Decomposition and outline.** The function $N_7^{\text{tw}}(X)$ is difficult to understand chiefly because of the twist minimality defect. Fortunately, the twist minimality defect cannot get too large relative to X (see Corollary 2.4.7). So we partition our sum based on the value of $\operatorname{tmd}(A(a,b),B(a,b))$ in terms of the parametrization provided in section 2.2.

For $e \geq 1$, let $N_7^{\text{tw}}(X;e)$ denote the number of pairs $(a,b) \in \mathbb{Z}^2$ with

- (a,b) groomed,
- $\operatorname{twht}(A(a,b),B(a,b)) \leq X$, and
- $\operatorname{tmd}(A(a,b),B(a,b)) = e$.

By (2.2.12) and Corollary 2.4.7, we have

$$N_7^{\text{tw}}(X) = \sum_{e \ll X^{1/12}} N_7^{\text{tw}}(X;e). \tag{4.1.1}$$

Determining when e *divides* $\operatorname{tmd}(A,B)$ is easier than determining when e *equals* $\operatorname{tmd}(A,B)$, so we also let $M(X;e)$ denote the number of pairs $(a,b) \in \mathbb{Z}^2$ with

- (a,b) groomed;
- $H(A(a,b),B(a,b)) \leq X$;
- $e \mid \operatorname{tmd}(A(a,b),B(a,b))$.

Note that the points counted by $N_7^{\text{tw}}(X;e)$ have *twist* height bounded by X, but the points counted by $M(X;e)$ have only the function H bounded by X.

Corollary 2.4.7 and the Möbius sieve together yield

$$N_7^{\text{tw}}(X;e) = \sum_{f \ll \frac{X^{1/18}}{e^{2/3}}} \mu(f) M(e^6 X; ef) \tag{4.1.2}$$

for $e \neq H(A(-7,1),B(-7,1)) = 2^2 \cdot 3^3 \cdot 7^{18} = 175868668574328492$. This exception arises because the point $(-7,1)$ is ungroomed, and thus the count on the left of (4.1.2) may differ by at most 1 from the count on the right for $e = 2^2 \cdot 3^3 \cdot 7^{18}$.

In order to estimate $M(X;e)$, we further unpack the groomed condition on pairs (a,b). We therefore let $M(X;d,e)$ denote the number of pairs $(a,b) \in \mathbb{Z}^2$ with

- $\gcd(da,db,e) = 1$ and $b > 0$;
- $H(A(da,db),B(da,db)) \leq X$;
- $e \mid \operatorname{tmd}(A(da,db),B(da,db))$.

As $H(A(a,b),B(a,b))$ is homogeneous of degree 12, yet another Möbius sieve yields

$$M(X;e) = \sum_{\substack{d \ll X^{1/12} \\ \gcd(d,e)=1}} \mu(d) M(X;d,e). \tag{4.1.3}$$

Before proceeding, we now give an outline of the argument used in this section. In Lemma 4.2.1, we use the Principle of Lipschitz to estimate $M(X;d,e)$, then piece these estimates together using (4.1.3) to estimate $M(X;e)$. Heuristically,

$$M(X;d,e) \sim \frac{RT(e)X^{1/6}}{d^2e^3}\prod_{\ell \mid e}\left(1-\frac{1}{\ell}\right)$$

(where R is the area of (3.1.2) and T is the arithmetic function investigated in Lemma 2.3.3) by summing over the congruence classes modulo e^3 that satisfy $e \mid \operatorname{tmd}(A(da,db),B(da,db))$. Then (4.1.3) suggests

$$M(X;e) \sim \frac{RT(e)X^{1/6}}{\zeta(2)e^3\prod_{\ell \mid e}\left(1+\frac{1}{\ell}\right)}. \tag{4.1.4}$$

To go further, we substitute (4.1.2) into (4.1.1), and let $n = ef$ to obtain

$$N_7^{\mathrm{tw}}(X) = \sum_{n \ll X^{1/12}}\sum_{e \mid n}\mu\left(\frac{n}{e}\right)M(e^6X;n) + O(1). \tag{4.1.5}$$

Substituting (4.1.4) into (4.1.5), and recalling $\varphi(n) = \sum_{e \mid n}\mu(n/e)e$, we obtain the heuristic estimate

$$N_7^{\mathrm{tw}}(X) \sim \frac{QRX^{1/6}}{\zeta(2)},$$

where

$$Q := \sum_{n \geq 1}\frac{T(n)\varphi(n)}{n^3\prod_{\ell \mid n}\left(1+\frac{1}{\ell}\right)}.$$

To make this estimate for $N_7^{\mathrm{tw}}(X)$ rigorous, and to get a better handle on the size of order of growth for its error term, we now decompose (4.1.5) based on the size of n into two pieces:

$$\begin{aligned} N_{7,\leq y}^{\mathrm{tw}}(X) &:= \sum_{n \leq y}\sum_{e \mid n}\mu\left(\frac{n}{e}\right)M(e^6X;n), \\ N_{7,>y}^{\mathrm{tw}}(X) &:= \sum_{n > y}\sum_{e \mid n}\mu\left(\frac{n}{e}\right)M(e^6X;n). \end{aligned} \tag{4.1.6}$$

So

$$N_7^{\mathrm{tw}}(X) = N_{7,\leq y}^{\mathrm{tw}}(X) + N_{7,>y}^{\mathrm{tw}}(X) + O(1).$$

We then estimate $N_{7,\leq y}^{\mathrm{tw}}(X)$ in Proposition 4.2.6, and treat $N_{7,>y}^{\mathrm{tw}}(X)$ as an error term which we bound in Lemma 4.2.12. Setting the error from our estimate equal to the error arising from $N_{7,>y}^{\mathrm{tw}}(X)$, we obtain Theorem 4.2.16.

In the remainder of this section, we follow the outline suggested here by successively estimating $M(X;d,e)$, $M(X;e)$, $N_{7,\leq y}^{\mathrm{tw}}(X)$, $N_{7,>y}^{\mathrm{tw}}(X)$, and finally $N_7^{\mathrm{tw}}(X)$.

4.2. **Asymptotic estimates.** We first estimate $M(X;d,e)$ and $M(X;e)$.

Lemma 4.2.1. *The following statements hold.*

(a) *If* $\gcd(d,e) > 1$, *then* $M(X;d,e) = 0$. *Otherwise, we have*

$$M(X;d,e) = \frac{RT(e)X^{1/6}}{d^2e^3}\prod_{\ell \mid e}\left(1-\frac{1}{\ell}\right) + O\left(\frac{T(e)X^{1/12}}{d}\right).$$

where R *is the area of* (3.1.2).

(b) *We have*

$$M(X;e) = \frac{RT(e)X^{1/6}}{\zeta(2)e^3\prod_{\ell \mid e}\left(1+\frac{1}{\ell}\right)} + O(T(e)X^{1/12}\log X).$$

In both cases, the implied constants are independent of d, e, and X.

Proof. We begin with (a) and examine the summands $M(X;d,e)$. If d and e are not coprime, then $M(X;d,e) = 0$ because $\gcd(da,db,e) \geq \gcd(d,e) > 1$. On the other hand, if $\gcd(d,e) = 1$, we have a bijection from the pairs counted by $M(X;1,e)$ to the pairs counted by $M(d^{12}X;d,e)$ given by $(a,b) \mapsto (da,db)$.

Combining Lemma 2.3.3(a)–(b) and Corollary 3.1.5, we have

$$\begin{aligned} M(X;1,e) &= \sum_{(a_0,b_0)\in\widetilde{\mathcal{T}}(e)} \#\{(a,b) \in \mathcal{R}(X)\cap\mathbb{Z}^2 : (a,b) \equiv (a_0,b_0) \pmod{e^3}\} \\ &= \varphi(e^3)T(e)\left(\frac{RX^{1/6}}{e^6} + O\left(\frac{X^{1/12}}{e^3}\right)\right) \qquad (4.2.2)\\ &= \frac{RT(e)X^{1/6}}{e^3}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right) + O(T(e)X^{1/12}), \end{aligned}$$

and thus

$$M(X;d,e) = \frac{RT(e)X^{1/6}}{d^2e^3}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right) + O\left(\frac{T(e)X^{1/12}}{d}\right).$$

For part (b), we compute

$$\begin{aligned} M(x;e) &= \sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}} \mu(d)M(X;d,e) \\ &= \sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}} \mu(d)\left(\frac{T(e)RX^{1/6}}{d^2e^3}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right) + O\left(T(e)\frac{X^{1/12}}{d}\right)\right) \qquad (4.2.3)\\ &= \frac{RT(e)X^{1/6}}{e^3}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)\sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}}\frac{\mu(d)}{d^2} + O\left(T(e)X^{1/12}\sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}}\frac{1}{d}\right). \end{aligned}$$

Plugging the straightforward estimates

$$\sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}}\frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)}\prod_{\ell\mid e}\left(1-\frac{1}{\ell^2}\right)^{-1} + O(X^{-1/12}) \qquad (4.2.4)$$

and

$$\sum_{d\leq X^{1/12}}\frac{1}{d} = \frac{1}{12}\log X + O(X^{-1/12})$$

into (4.2.3) then simplifies to give

$$M(x;e) = \frac{RT(e)X^{1/6}}{\zeta(2)e^3\prod_{\ell|e}\left(1+\frac{1}{\ell}\right)} + O(T(e)X^{1/12}\log X) \tag{4.2.5}$$

proving (b). $\square$

We are now in a position to estimate $N^{\mathrm{tw}}_{7,\leq y}(X)$.

Proposition 4.2.6. *Suppose $y \ll X^{\frac{1}{12}}$. Then*

$$N^{\mathrm{tw}}_{7,\leq y}(X) = \frac{QRX^{1/6}}{\zeta(2)} + O\left(\max\left(\frac{X^{1/6}\log y}{y}, X^{1/12}y^{\frac{3}{2}}\log X\log^3 y\right)\right)$$

where

$$Q := \sum_{n\geq 1}\frac{\varphi(n)T(n)}{n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} = Q_3Q_7\prod_{\substack{p\neq 7\text{ prime}\\ p\equiv 1\pmod 3}}\left(1+\frac{2}{(p+1)^2}\right),$$

$Q_3 = \frac{13}{6}$, *and* $Q_7 = \frac{63}{8}$.

Proof. Substituting the asymptotic for $M(X;e)$ from Lemma 4.2.1 into the defining series for $N^{\mathrm{tw}}_{7,\leq y}(X)$, we have

$$N^{\mathrm{tw}}_{7,\leq y}(X) = \sum_{n\leq y}\sum_{e|n}\mu\left(\frac{n}{e}\right)\left(\frac{RT(n)eX^{1/6}}{\zeta(2)n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} + O\left(T(n)e^{1/2}X^{1/12}\log(e^6X)\right)\right).$$

We handle the main term and the error of this expression separately. For the main term, we have

$$\begin{aligned}\sum_{n\leq y}\sum_{e|n}\mu\left(\frac{n}{e}\right)\left(\frac{RT(n)eX^{1/6}}{\zeta(2)n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)}\right) &= \frac{RX^{1/6}}{\zeta(2)}\sum_{n\geq 1}\frac{T(n)}{n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)}\sum_{e|n}\mu\left(\frac{n}{e}\right)e \\ &= \frac{RX^{1/6}}{\zeta(2)}\sum_{n\leq y}\frac{\varphi(n)T(n)}{n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)}.\end{aligned} \tag{4.2.7}$$

By Lemma 2.3.3(e), we see

$$\frac{\varphi(n)T(n)}{n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} = O\left(\frac{2^{\omega(n)}}{n^2}\right).$$

By Corollary 3.3.3 and Corollary 3.5.4, we have

$$\sum_{n>y}\frac{2^{\omega(n)}}{n^2} \sim \frac{\log y}{\zeta(2)y}$$

as $y\to\infty$. *A fortiori,*

$$\sum_{n>y}\frac{\varphi(n)T(n)}{n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} = O\left(\sum_{n>y}\frac{2^{\omega(n)}}{n^2}\right) = O\left(\frac{\log y}{y}\right),$$

so the series

$$\sum_{n\geq 1}\frac{\varphi(n)T(n)}{n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} = Q \tag{4.2.8}$$

is absolutely convergent, and

$$\sum_{n\le y}\sum_{e|n}\mu\left(\frac{n}{e}\right)\left(\frac{RT(n)eX^{1/6}}{\zeta(2)n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)}\right)=\frac{RX^{1/6}}{\zeta(2)}\left(Q-O\left(\frac{\log y}{y}\right)\right)$$
$$=\frac{QRX^{1/6}}{\zeta(2)}+O\left(\frac{X^{1/6}\log y}{y}\right).$$

As the summands of (4.2.8) constitute a nonnegative multiplicative arithmetic function, we can factor Q as an Euler product. For p prime, Lemma 2.3.3 yields

$$Q_p:=\sum_{a\ge 0}\frac{\varphi(p^a)T(p^a)}{p^{3a}\prod_{\ell|p}\left(1+\frac{1}{\ell}\right)}=\begin{cases}1+\dfrac{2}{p^2+1}, & \text{if } p\equiv 1 \pmod 3 \text{ and } p\neq 7;\\ 13/6, & \text{if } p=3;\\ 63/8, & \text{if } p=7;\\ 1 & \text{else.}\end{cases}$$

Thus

$$Q=\prod_{p\text{ prime}}Q_p=Q_3Q_7\prod_{\substack{p\neq 7\text{ prime}\\ p\equiv 1 \pmod 3}}\left(1+\frac{2}{p^2+1}\right). \tag{4.2.9}$$

We now turn to the error term. Since $y\ll X^{1/12}$, for $e\le y$ we have $\log(e^6X)\ll\log X$. Applying Lemma 2.3.3(e), we obtain

$$\sum_{n\le y}\sum_{e|n}\mu\left(\frac{n}{e}\right)O\left(T(n)e^{1/2}X^{1/12}\log\left(e^6X\right)\right)=O\left(X^{1/12}\log X\sum_{n\le y}T(n)\sum_{e|n}\left|\mu\left(\frac{n}{e}\right)\right|e^{1/2}\right)$$
$$=O\left(X^{1/12}\log X\sum_{n\le y}2^{2\omega(n)}n^{1/2}\right) \tag{4.2.10}$$

Corollary 3.3.3 and Corollary 3.5.4, together with the trivial inequality $2^{2\omega(n)}\le d(n)^2$, yield

$$\sum_{n\le y}2^{2\omega(n)}n^{1/2}=O(y^{3/2}\log^3 y). \tag{4.2.11}$$

Substituting (4.2.11) into (4.2.10) gives our desired result. □

We now bound $N^{\mathrm{tw}}_{7,>y}(X)$.

Lemma 4.2.12. *We have*

$$N^{\mathrm{tw}}_{7,>y}(X)=O\left(\frac{X^{1/6}\log^3 y}{y}\right)$$

Proof. We have

$$N^{\mathrm{tw}}_{7,>y}(X)=\sum_{n>y}\sum_{e|n}\mu\left(\frac{n}{e}\right)M(e^6X;n)\le\sum_{n>y}2^{\omega(n)}M(n^6X;n). \tag{4.2.13}$$

Write $n=3^v7^wn'$ where $\gcd(n',3)=\gcd(n',7)=1$. We define

$$n_0:=3^{\max(v-1,0)}7^{\max(w-3,0)}n',$$

so

$$\frac{n}{3\cdot 7^3} \le n_0 \le n.$$

Let $(a,b)\in\mathbb{Z}^2$ be a groomed pair. By Theorem 2.4.6(a), $H(A(a,b),B(a,b))\le n^6X$ implies $C(a,b)\le n^6X$, and by Theorem 2.4.6(b), $n\mid \operatorname{tmd}(A(a,b),B(a,b))$ implies $n_0^3\mid C(a,b)^3$. Thus

$$M(n^6X;n)\le \#\left\{(a,b)\in\mathbb{Z}^2 \text{ groomed} : 108C(a,b)^6\le n^6X,\ n_0^3\mid C(a,b)\right\}.$$

Recalling (2.4.1) and Lemma 2.4.2(c), we deduce

$$M(n^6X;n)\le \sum_{m\ll X^{1/6}/n^2} c(n_0^3m)\le 3\cdot 2^{\omega(n_0)-1}\sum_{m\ll X^{1/6}/n^2} c(m).$$

But $2^{\omega(n)}\le 4\cdot 2^{\omega(n_0)}$, so by Corollary 3.1.7, we have

$$M(n^6X;n)=O\left(\frac{2^{\omega(n)}X^{1/6}}{n^2}\right),$$

and substituting this expression into (4.2.13) yields

$$N_{7,>y}^{\mathrm{tw}}(X)=O\left(\sum_{n>y}\frac{\left(2^{\omega(n)}\right)^2X^{1/6}}{n^2}\right)=O\left(X^{1/6}\sum_{n>y}\frac{2^{2\omega(n)}}{n^2}\right). \tag{4.2.14}$$

As in the proof of Proposition 4.2.6, combining Corollary 3.3.3 and Corollary 3.5.4 together with the trivial inequality $2^{2\omega(n)}\le d(n)^2$ yields

$$\sum_{n>y}\frac{2^{2\omega(n)}}{n^2}=O\left(\frac{\log^3 y}{y}\right). \tag{4.2.15}$$

Substituting (4.2.15) into (**??**) gives our desired result. □

We are now in a position to prove Theorem 1.2.2, which we restate here with the notations we have established.

Theorem 4.2.16. *We have*

$$N_7^{\mathrm{tw}}(X)=\frac{QRX^{1/6}}{\zeta(2)}+O(X^{2/15}\log^3 X),$$

where

$$Q=\sum_{n\ge 1}\frac{\varphi(n)T(n)}{n^3\prod_{\ell\mid n}(1+1/\ell)}$$

and R is the area of the region

$$\mathcal{R}(1)=\left\{(a,b)\in\mathbb{R}^2 : H(A(a,b),B(a,b))\le 1, b\ge 0\right\}.$$

Proof. Let y be a positive quantity with $y\ll X^{1/12}$; in particular, $\log y\ll \log X$. Proposition 4.2.6 and Lemma 4.2.12 together tell us

$$N_7^{\mathrm{tw}}(X)=\frac{QRX^{1/6}}{\zeta(2)}+O\left(\max\left(\frac{X^{1/6}\log^3 X}{y}, X^{1/12}y^{\frac{3}{2}}\log^3 y\right)\right).$$

We let $y = X^{1/30}$ so that

$$\frac{X^{1/6}\log^3 X}{y} = X^{1/12}y^{3/2}\log^3 y = X^{2/15}\log^3 X,$$

and we conclude

$$N_7^{\mathrm{tw}}(X) = \frac{QRX^{1/6}}{\zeta(2)} + O\left(X^{2/15}\log^3 X\right)$$

as desired. □

4.3. ***L*-series.** To conclude, we set up the next section by interpreting Theorem 4.2.16 in terms of Dirichlet series. Let

$$h_7^{\mathrm{tw}}(n) := \#\left\{(a,b)\in\mathbb{Z}^2 \text{ groomed} : \operatorname{twht}(A(a,b),B(a,b)) = n\right\} \tag{4.3.1}$$

and define

$$L_7^{\mathrm{tw}}(s) := \sum_{n\geq 1}\frac{h_7^{\mathrm{tw}}(n)}{n^s} \tag{4.3.2}$$

wherever this series converges. Then $N_7^{\mathrm{tw}}(X) = \sum_{n\leq x} h_7^{\mathrm{tw}}(n)$, and conversely we have $L_7^{\mathrm{tw}}(s) = \int_0^\infty x^{-s}\,\mathrm{d}N_7^{\mathrm{tw}}(x)$.

Corollary 4.3.3. *The Dirichlet series $L_7^{\mathrm{tw}}(s)$ has abscissa of (absolute) convergence $\sigma_a = \sigma_c = 1/6$ and has a meromorphic continuation to the region*

$$\{s\in\mathbb{C} : \operatorname{Re}(s) > 2/15\}. \tag{4.3.4}$$

Moreover, $L_7^{\mathrm{tw}}(s)$ has a simple pole at $s = 1/6$ with residue

$$\operatorname{res}_{s=\frac{1}{6}} L_7^{\mathrm{tw}}(s) = \frac{QR}{6\zeta(2)}$$

and is holomorphic elsewhere on the region (4.3.4).

Proof. Let $s = \sigma + it \in \mathbb{C}$ be given with $\sigma > 1/6$. Abel summation yields

$$\begin{aligned}\sum_{n\leq X} h_7^{\mathrm{tw}}(n)n^{-s} &= N_7^{\mathrm{tw}}(X)X^{-s} + s\int_1^X N_7^{\mathrm{tw}}(t)t^{-s-1}\log t\,\mathrm{d}t\\ &= O\left(X^{1/6-\sigma} + s\int_1^X t^{-5/6-\sigma}\,\mathrm{d}t\right);\end{aligned}$$

as $X\to\infty$ the first term vanishes and the integral converges. Thus, when $\sigma > 1/6$,

$$\sum_{n\geq 1} h_7^{\mathrm{tw}}(n)n^{-s} = s\int_1^\infty N_7^{\mathrm{tw}}(t)t^{-1-s}\,\mathrm{d}t$$

and this integral converges. A similar argument shows that the sum defining $L_7^{\mathrm{tw}}(s)$ diverges when $\sigma < 1/6$. We have shown $\sigma_c = 1/6$ is the abscissa of convergence for $L_7^{\mathrm{tw}}(s)$, but as $h_7^{\mathrm{tw}}(n)\geq 0$ for all n, it is also the abscissa of *absolute* convergence $\sigma_a = \sigma_c$.

Now write

$$L_7^{\mathrm{tw}}(s) = \frac{QR}{\zeta(2)}\zeta(6s) + L_{7,\mathrm{rem}}^{\mathrm{tw}}(s). \tag{4.3.5}$$

Abel summation and the substitution $t \mapsto t^{1/6}$ yields for $\sigma > 1$

$$\zeta(6s) = s \int_1^\infty \lfloor t^{1/6} \rfloor t^{-1-s}\, du = s \int_1^\infty \left(t^{1/6} + O(1)\right) t^{-1-s}\, du.$$

Letting

$$\delta(n) := \begin{cases} 1 & \text{if } n = k^6 \text{ for some } k \in \mathbb{Z}, \\ 0 & \text{else,} \end{cases}$$

we have

$$\begin{aligned} L_{7,\mathrm{rem}}^{\mathrm{tw}}(s) &= \sum_{n \geq 1} \left(h_7^{\mathrm{tw}}(n) - \frac{QR}{\zeta(2)} \delta(n) \right) n^{-s} \\ &= s \int_1^\infty \left(N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)} \lfloor t^{1/6} \rfloor \right) t^{-1-s}\, \mathrm{d}t \end{aligned} \tag{4.3.6}$$

when $\sigma > 1/6$. But then for any $\epsilon > 0$,

$$N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)} \lfloor t^{1/6} \rfloor = O\left(t^{2/15+\epsilon}\right) \tag{4.3.7}$$

by Theorem 4.2.16. Substituting (4.3.7) into (4.3.6), we obtain

$$s \int_1^\infty \left(N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)} \lfloor t^{1/6} \rfloor \right) t^{-1-s}\, \mathrm{d}t = O\left(s \int_1^\infty t^{-13/15-s+\epsilon}\, \mathrm{d}t \right) \tag{4.3.8}$$

where the integral converges whenever $\sigma > 2/15 + \epsilon$. Letting $\epsilon \to 0$, we obtain an analytic continuation of $L_{7,\mathrm{rem}}^{\mathrm{tw}}(s)$ to the region (4.3.4).

At the same time, $\zeta(6s)$ has meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1/6$ with residue $1/6$. Thus looking back at (4.3.5), we find that

$$L_7^{\mathrm{tw}}(s) = \frac{QR}{\zeta(2)} \zeta(6s) + s \int_1^\infty \left(N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)} \lfloor t^{1/6} \rfloor \right) t^{-1-s} dt$$

when $\sigma > 1/6$, but in fact the right-hand side of this equality defines a meromorphic function on the region (4.3.4) with a simple pole at $s = 1/6$ and no other poles. Our claim follows. ☐

5. Estimates for rational isomorphism classes

In section 4, we counted the number of elliptic curves over $\mathbb{Q}$ with a (cyclic) 7-isogeny up to isomorphism over $\mathbb{Q}^{\mathrm{al}}$ (Theorem 4.2.16). In this section, we count all isomorphism classes over $\mathbb{Q}$ by enumerating over twists using a Tauberian theorem (Theorem 3.5.2).

5.1. **Setup.** Breaking up the sum (2.2.9), let

$$h_7(n) := \#\{(a,b,c) \in \mathbb{Z}^3 : (a,b) \text{ groomed, } c \text{ squarefree, } \mathrm{ht}(c^2 A(a,b), c^3 A(a,b)) = n\}. \tag{5.1.1}$$

Then $h_7(n)$ counts the number of elliptic curves $E \in \mathscr{E}$ of height n that admit a 7-isogeny (2.2.8) and $N_7(X) := \sum_{n \leq X} h_7(n)$. We also let

$$L_7(s) := \sum_{n \geq 1} \frac{h_7(n)}{n^s} \tag{5.1.2}$$

wherever this sum converges.

Theorem 5.1.3. *The following statements hold.*

(a) *We have*

$$h_7(n) = 2 \sum_{c^6 \mid n} |\mu(c)|\, h_7^{\mathrm{tw}}\left(\frac{n}{c^6}\right)$$

(b) *For* $s \in \mathbb{C}$ *with* $\mathrm{Re}(s) > 1/6$ *we have*

$$L_7(s) = \frac{2\zeta(6s)L_7^{\mathrm{tw}}(s)}{\zeta(12s)} \tag{5.1.4}$$

with absolute convergence on this region.

(c) *The Dirichlet series* $L_7(s)$ *has a meromorphic continuation to the region* (4.3.4) *with a double pole at* $s = 1/6$ *and no other singularities on this region.*

(d) *The Laurent expansion for* $L_7(s)$ *at* $s = 1/6$ *begins*

$$L_7(s) = \frac{1}{3\zeta(2)^2}\left(\frac{QR}{6}\left(s - \frac{1}{6}\right)^{-2} + \left(\ell_0 + QR\left(\gamma - \frac{2\zeta'(2)}{\zeta(2)}\right)\right)\left(s - \frac{1}{6}\right)^{-1} + O(1)\right),$$

where

$$\ell_0 := QR\gamma + \frac{\zeta(2)}{6}\int_1^\infty \left(N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)}\left\lfloor t^{1/6}\right\rfloor\right) t^{-7/6}\,\mathrm{d}t \tag{5.1.5}$$

is the constant term of the Laurent expansion for $L_7^{\mathrm{tw}}(s)$ *around* $s = 1/6$.

Proof. For (a), we first collect the terms that contribute to $h_7(n)$ by the quadratic twist factor c:

$$h_7^{(c)}(n) := \#\left\{(a,b) \in \mathbb{Z}^2 \text{ groomed} : \mathrm{ht}(c^2A(a,b), c^3B(a,b)) = n\right\} \tag{5.1.6}$$

By (2.1.8) we have $\mathrm{ht}(c^2A(a,b), c^3B(a,b)) = c^6\,\mathrm{ht}(A(a,b), B(a,b))$, so

$$h^{(c)}(n) = \begin{cases} h_7^{\mathrm{tw}}(n/c^6), & \text{if } c^6 \mid n; \\ 0, & \text{otherwise.} \end{cases} \tag{5.1.7}$$

Therefore

$$h_7(n) = \sum_{c \text{ squarefree}} h^{(c)}(n) = 2\sum_{c \geq 1} |\mu(c)|\, h^{(c)}(n) = 2\sum_{c^6 \mid n} |\mu(c)|\, h_7^{\mathrm{tw}}\left(\frac{n}{c^6}\right)$$

proving (a).

For (b), we see that $h_7(n)$ is the the nth coefficient of the Dirichlet convolution of $L_7^{\mathrm{tw}}(n)$ and

$$2\sum_{c \geq 1} |\mu(c)|\, n^{-6s} = \frac{2\zeta(6s)}{\zeta(12s)}.$$

As both $L_7^{\mathrm{tw}}(s)$ and $\zeta(6s)/\zeta(12s)$ are absolutely convergent when $\mathrm{Re}(s) > 1/6$, we see

$$L_7(s) = \frac{2\zeta(6s)L_7^{\mathrm{tw}}(s)}{\zeta(12s)}$$

when $\sigma > 1/6$, and $L_7(s)$ converges absolutely in this half-plane.

For (c), since $\zeta(s)$ is nonvanishing when $\mathrm{Re}\, s > 1$, the ratio $\zeta(6s)/\zeta(12s)$ is meromorphic function for $\mathrm{Re}(s) > 1/12$. But Corollary 4.3.3 gives a meromorphic continuation of $L_7^{\mathrm{tw}}(s)$ to the region (4.3.4). The function $L_7(s)$ is a product of these two meromorphic functions on

(4.3.4), and so it is a meromorphic function on this region. The holomorphy and singularity for $L_7(s)$ then follow from those of $L_7^{\mathrm{tw}}(s)$ and $\zeta(s)$.

We conclude (d) by computing Laurent expansions. We begin with

$$\frac{\zeta(6s)}{\zeta(12s)} = \frac{1}{\zeta(2)}\left(\frac{1}{6}\left(s-\frac{1}{6}\right)^{-1} + \left(\gamma - \frac{2\zeta'(2)}{\zeta(2)}\right) + O(1)\right), \tag{5.1.8}$$

whereas the Laurent expansion for $L_7^{\mathrm{tw}}(s)$ at $s = 1/6$ begins

$$L_7^{\mathrm{tw}}(s) = \frac{1}{\zeta(2)}\left(\frac{QR}{6}\left(s-\frac{1}{6}\right)^{-1} + \ell_0 + \dots\right), \tag{5.1.9}$$

with ℓ_0 given by (5.1.5). Multiplying the Laurent series tails gives the desired result. □

5.2. **Proof of main result.** We are now poised to finish off the proof of our main result.

Lemma 5.2.1. *The sequence $\{h_7(n)\}_{n\geq 1}$ is admissible (Definition 3.5.1) with parameters $(1/6, 1/30, 16/15)$.*

Proof. We check each condition in Definition 3.5.1. Since $h_7(n)$ counts objects, we indeed have $h_7(n) \in \mathbb{Z}_{\geq 0}$.

For (i), Corollary 4.3.3 tells us that $L_7^{\mathrm{tw}}(s)$ has $1/6$ as its abscissa of absolute convergence. Likewise, $\dfrac{\zeta(6s)}{\zeta(12s)}$ has $1/6$ as its abscissa of absolute convergence. By Theorem 5.1.3(b),

$$L_7(s) = \frac{2\zeta(6s)L_7^{\mathrm{tw}}(s)}{\zeta(12s)},$$

and by Theorem 3.2.1 this series converges absolutely for $\sigma > \sigma_a$, so the abscissa of absolute convergence for $L_7(s)$ is at most $1/6$. But for $\sigma < 1/6$, $L_7(\sigma) > L_7^{\mathrm{tw}}(\sigma)$ by termwise comparison of coefficients, so the Dirichlet series for $L_7(s)$ diverges when $\sigma < 1/6$, and (i) holds with $\sigma_a = \frac{1}{6}$.

For (ii), Corollary 4.3.3 tells us that $L_7^{\mathrm{tw}}(s)$ has a meromorphic continuation when $\sigma = \mathrm{Re}(s) > 2/15$; on the other hand, as $\zeta(12s)$ is nonvanishing for $\sigma > 1/12$, we see that $\zeta(6s)/\zeta(12s)$ has a meromorphic contintuation to $\sigma > 1/12$, and so (ii) holds with $\delta = 1/6 - 2/15 = 1/30$. (The only pole of $L_7(s)/s$ with $\sigma > 2/15$ is the double pole at $s = 1/6$ indicated in Theorem 5.1.3(e).)

For (c), let $\sigma > 2/15$. By Corollary 3.4.3, we have $\mu_{L_7^{\mathrm{tw}}}(\sigma) \leq 1$. Let $\zeta_a(s) = \zeta(as)$. Applying Theorem 3.4.4, we have

$$\mu_{\zeta_6}(\sigma) = \mu_{\zeta}(6\sigma) \leq \frac{1}{3}\left(1 - \frac{6\cdot 2}{15}\right) = \frac{1}{15} \tag{5.2.2}$$

if $\sigma \leq 1/6$, and by Theorem 3.4.1, $\mu_{\zeta_6}(\sigma) = 0$ if $\sigma > 1/6$. Finally, as $\zeta(12s)^{-1}$ is absolutely convergent for $s > 1/12$, Theorem 3.4.1 tells us $\mu_{\zeta_{12}{}^{-1}}(\sigma) = 0$. Taken together, we see

$$\mu_{L_7}(\sigma) \leq 1 + \frac{1}{15} + 0 = \frac{16}{15},$$

so the sequence $\{h_7(n)\}_{n\geq 1}$ is admissible with final parameter $\xi = 16/15$. □

We now prove Theorem 1.2.1, which we restate here for ease of reference in our established notation.

Theorem 5.2.3. *For all $\epsilon > 0$,*

$$N_7(X) = \frac{QR}{3\zeta(2)^2} X^{1/6} \log X + \frac{2}{\zeta(2)^2} \left(\ell_0 + QR \left(\gamma - 1 - \frac{2\zeta'(2)}{\zeta(2)} \right) \right) X^{1/6} + O\left(X^{7/45+\epsilon} \right)$$

as $X \to \infty$, where the implicit constant depends on ϵ. The constants Q, R are defined in Theorem 4.2.16, and ℓ_0 is defined in (5.1.5).

Proof. By Lemma 5.2.1, $\{h_7(n)\}_{n\geq 1}$ is admissible with parameters $\left(\frac{1}{6}, \frac{1}{30}, \frac{16}{15}\right)$. We now apply Theorem 3.5.2 to the Dirichlet series $L_7(s)$, and our claim follows. ☐

Remark 5.2.4. We suspect that the true error on both $N_7(X)$ and $N_7^{\mathrm{tw}}(X)$ is $O(X^{1/12+\epsilon})$, but we have been unable to bound the error term this far using our techniques.

6. Computations

In this section, we conclude by describing some computations which make our main theorems completely explicit.

6.1. **Computing elliptic curves with 7-isogeny.**

We begin by outlining an algorithm for computing all elliptic curves that admit with 7-isogeny up to twist height X. In a nutshell, we iterate over possible factorizations e^3m with m cubefree to find all groomed pairs (a, b) for which $C(a, b) = e^3m$, then check if $\mathrm{twht}(A(a, b), B(a, b)) \leq X$.

In detail, our algorithm proceeds as follows.

1. We list all primes $p \equiv 1 \pmod 3$ up to $(X/108)^{1/6}$ (this bound arises from Theorem 2.4.6(a)).
2. For each pair $(a, b) \in \mathbb{Z}^2$ with $b > 0$, $\gcd(a, b) = 1$, $b > 0$, and $C(a, b)$ coprime to 3 and less than Y, we compute $C(a, b)$. We organize the results into a lookup table, so that for each c we can find all pairs (a, b) with $b > 0$, $\gcd(a, b) = 1$, $b > 0$, and $C(a, b) = c$. We append 1 to our table with lookup value $(1, 0)$. For each c in our lookup table, we record whether c is cubefree by sieving against the primes we previously computed.
3. For positive integer pairs (e_0, m), $e_0^{12}m^6 \leq X/108$, and m cubefree, we find all groomed pairs $(a, b) \in \mathbb{Z}^2$ with $C(a, b) = e_0^3m$. If $\gcd(e_0, 3) = \gcd(m, 3) = 1$, we can do this as follows. If $e_0^3 < Y$, we iterate over groomed pairs (a_e, b_e) and (a_m, b_m) yielding $C(a_e, b_e) = e_0^3$ and $C(a_m, b_m) = m$ respectively, and taking the product
$$(a_e + b_e\rho)(a_m + b_m\rho) = a + b\rho \in \mathbb{Z}[3\zeta]$$
as in the proof of Lemma 2.4.2. If $e_0^3 > Y$, we iterate over groomed pairs (a_e', b_e') with $C(a_e', b_e') = e_0$ instead of over groomed pairs (a_e, b_e), and compute
$$(a_e' + b_e\rho)^3(a_m + b_m\rho) = a + b\rho \in \mathbb{Z}[3\zeta].$$
If $\gcd(e_0, 3) > 1$ or $\gcd(m, 3) > 1$, we perform the steps above for the components of e_0 and m coprime to 3, and then postmultiply by those groomed pairs $(a_3, b_3) \in \mathbb{Z}^2$ with $C(a_3, b_3)$ an appropriate power of 3 (which is necessarily 9 or 27 by Lemma 2.4.2(b).
4. For each pair (a, b) with $C(a, b) = e_0^3m$, obtained in the previous step, we compute $H(A(a, b), B(a, b))$. We compute the 3-component of the twist minimality defect e_3, the 7-component of the twice minimality defect e_7, and thereby compute the twist minimality defect $e = \mathrm{lcm}(e_0, e_3, e_7)$. We compute the twist height using the

reduced pairs $(A(a,b)/e^2, |B(a,b)|/e^3)$. If this result is less than or equal to X, we report (a,b), together with their twist height and any auxiliary information we care to record.

Running this algorithm out to $X = 10^{42}$ took us approximately 34 CPU hours on a single core, producing 4 582 079 elliptic curves admitting 7-isogeny. To check the accuracy of our code, we confirmed that the j-invariants of these curves are distinct.We also confirmed that the 7-division polynomial of each curve has a linear or cubic factor over $\mathbb{Q}$; this took 3.5 CPU hours. For $X = 10^{42}$, we have

$$\frac{\zeta(2)}{QR}\frac{N_7^{\mathrm{tw}}(10^{42})}{(10^{42})^{1/6}} = 0.99996\ldots,$$

which is close to 1.

We list the first few twist minimal elliptic curves admitting a (cyclic) 7-isogeny in Table 6.1.1.

(A,B)	(a,b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(-3,62)$	$(14,5)$	103788	1029
$(13,78)$	$(21,4)$	164268	1029
$(37,74)$	$(42,1)$	202612	1029
$(-35,98)$	$(0,1)$	259308	21
$(45,18)$	$(35,2)$	364500	1029
$(-43,166)$	$(7,13)$	744012	3087
$(-75,262)$	$(-7,8)$	1853388	1029
$(-147,658)$	$(-56,1)$	12706092	1029
$(-147,1582)$	$(7,6)$	67573548	343
$(285,2014)$	$(28,3)$	109517292	343
$(-323,2242)$	$(-21,10)$	135717228	1029
$(-395,3002)$	$(-63,2)$	246519500	1029
$(-155,3658)$	$(21,11)$	361286028	1029
$(357,5194)$	$(7,1)$	728396172	21
$(-595,5586)$	$(-14,1)$	842579500	63
$(285,5662)$	$(91,1)$	865572588	1029
$(-603,5706)$	$(-28,11)$	879077772	1029

Table 6.1.1: $E \in \mathscr{E}^{\mathrm{tw}}$ with 7-isogeny and twht $E \leq 10^9$

6.2. **Computing constants.** We also estimate the constants in our main theorems. First and easiest among these is Q, given by (4.2.9). Truncating the Euler product as a product over $p \leq Y$ gives us a lower bound

$$Q_{\leq Y} := \frac{273}{16}\prod_{\substack{7<p\leq Y\\ p\equiv 1 \pmod 3}}\left(1+\frac{2}{p^2+1}\right)$$

for Q. To obtain an upper bound, we compute

$$Q < Q_{\leq Y} \exp\left(2 \sum_{\substack{p>Y \\ p\equiv 1 \pmod 3}} \frac{1}{p^2+1}\right).$$

Suppose $Y \geq 8 \cdot 10^9$. Using Abel summation and Bennett–Martin–O'Bryant–Rechnitzer [1, Theorem 1.4], we obtain

$$\begin{aligned}\sum_{\substack{p>Y \\ p\equiv 1 \pmod 3}} \frac{1}{p^2+1} &= -\frac{\pi(Y;3,1)}{Y^2+1} + 2\int_Y^\infty \frac{\pi(u;3,1)u}{(u^2+1)^2}\,\mathrm{d}u \\ &< -\frac{Y}{2\,(Y^2+1)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\int_Y^\infty \frac{u^2}{(u^2+1)^2}\,\mathrm{d}u \\ &= \frac{1}{2}\left(\frac{5Y}{2(Y^2+1)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\left(\frac{\pi}{2} - \tan^{-1}(Y)\right)\right)\end{aligned}$$

so

$$Q < Q_{\leq Y} \cdot \exp\left(\frac{5Y}{2(Y^2+1)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\left(\frac{\pi}{2} - \tan^{-1}(Y)\right)\right).$$

In particular, letting $Y = 10^{12}$, we compute

$$17.46040523112662 < Q < 17.460405231134835$$

This computation took approximately 9 CPU days.

We now turn our attention to R, given in (3.1.2). We observe

$$\mathcal{R}(1) \subseteq [-0.677, 0.677] \times [0, 0.078],$$

so we can estimate $\mathcal{R}(1)$ by performing rejection sampling on the rectangle $[-0.677, 0.677] \times [0, 0.078]$, which has area 0.105612. Of our first $s := 2 \cdot 10^{11}$ samples, $r := 81750180560$ lie in R, so

$$R \approx 0.105612 \cdot \frac{r}{s} = 0.0431690\ldots$$

with standard error

$$0.105612 \cdot \sqrt{\frac{r(s-r)}{s^3}} < 1.2 \cdot 10^{-7}.$$

This took 4 CPU weeks to compute.

We can approximate ℓ_0 by truncating the integral (5.1.5) and using our approximations for Q and R. We have shown that for some $M > 0$ and for all $t > X$, we have

$$\left|N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)}\left\lfloor t^{1/6}\right\rfloor\right| < Mt^{2/15}\log^3 t.$$

Thus

$$\begin{aligned}\left|\int_X^\infty \left(N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)}\left\lfloor t^{1/6}\right\rfloor\right) t^{-7/6}\,\mathrm{d}t\right| \\ < M\int_X^\infty t^{-31/30}\log^3 t\,\mathrm{d}t \\ = 30MX^{-1/30}\left(\log^3 X + 90\log^2 X + 5400\log X + 162000\right);\end{aligned} \tag{6.2.1}$$

this gives us a bound on our truncation error. We do not know the exact value for M, but empirically, we find that for $1 \leq t \leq 10^{42}$,

$$-3.8253 \cdot 10^{-4} \leq \frac{N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)} \lfloor t^{1/6} \rfloor}{t^{2/15} \log^3 t} \leq 5.8428379 \cdot 10^{-5}.$$

If we assume $M \approx 3.8252 \cdot 10^{-4}$, we find the truncation error is bounded by 3.943, which dwarfs our initial estimate.

We can do better with stronger assumptions. If indeed $N_7^{\mathrm{tw}}(X) - \frac{QR}{\zeta(2)} X^{1/6} = O(X^{1/12+\epsilon})$, as we guessed in Remark 5.2.4, we can bound the tail of the integral more thoroughly. We let $\epsilon := 10^{-4}$, and find that for $1 \leq t \leq 10^{42}$,

$$-1.2174 \leq \frac{N_7^{\mathrm{tw}}(t) - \frac{QR}{\zeta(2)} \lfloor t^{1/6} \rfloor}{t^{1/12+\epsilon}} \leq 0.5227.$$

If

$$\left| N_7^{\mathrm{tw}}(X) - \frac{QR}{\zeta(2)} X^{1/6} \right| \leq M X^{1/12+\epsilon}$$

for $M \approx 1.2174$, we get an estimated truncation error of $8.8 \cdot 10^{-5}$, which is much more manageable.

Our estimate of ℓ_0 is also skewed by our estimates of QR. An error of ϵ in our estimate for QR induces an error of

$$\frac{\epsilon}{6} \int_1^X \lfloor t^{1/6} \rfloor t^{-7/6} \, \mathrm{d}t < \frac{\epsilon}{6} \int_1^X t^{-1} \, \mathrm{d}t = \frac{\epsilon \log X}{6}$$

in our estimate of ℓ_0. When $X = 10^{42}$, this gives a comparatively negligible error of $1.56 \cdot 10^{-6}$.

Given Q, R, and ℓ_0, it is straightfoward to compute c_1 and c_2 using the expressions given for them in Theorem 5.2.3. We find $c_1 = 0.0928556$ with an error of $1.04 \cdot 10^{-7}$, and $c_2 \approx -0.80037$ with an error of 2.914 or of $8.1 \cdot 10^{-5}$, depending on the assumptions made above. Note that both of these estimates for c_2 depended on empirical rather than theoretical estimates for the implicit constant in the error term of Theorem 5.2.3.

References

[1] Michael A. Bennett, Greg Martin, Kevin O'Bryant, and Andrew Rechnitzer, *Explicit bounds for primes in arithmetic progressions*, Illinois J. Math. **62** (2018), no. 1-4, 427–532.

[2] N. H. Bingham, C. M. Goldie, and J. L. Teugels, *Regular variation*, Encyclopedia Math. Appl., vol. 27, Cambridge University Press, Cambridge, 1987.

[3] Brandon Boggess and Soumya Sankar, *Counting elliptic curves with a rational n-isogeny for small n*, 2020, `arXiv:2009.05223`.

[4] Peter Bruin and Filip Najman, *Counting elliptic curves with prescribed level structures over number fields*, J. Lond. Math. Soc. (2) **105** (2022), no. 4, 2415–2435.

[5] John Cullinan, Meagan Kenney, and John Voight, *On a probabilistic local-global principle for torsion on elliptic curves*, J. Théor. Nombres Bordeaux **34** (2022), no. 1, 41–90.

[6] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.

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

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

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

[10] Aleksandar Ivić, *The Riemann zeta-function*, Dover Publications, Inc., Mineola, 2003.

[11] E. Landau, *Über die anzahl der gitterpunkte in gewissen bereichen. (zweite abhandlung)*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1915** (1915), 209–243.

[12] Mathieu Roux, *Théorie de l'information, séries de Dirichlet, et analyse d'algorithmes*, Ph.D. thesis, Université de Caen, 2011.

[13] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[14] Tristan Phillips, *Rational points of bounded height on some genus zero modular curves over number fields*, 2022, arXiv:2201.10624.

[15] Maggie Pizzo, Carl Pomerance, and John Voight, *Counting elliptic curves with an isogeny of degree three*, Proc. Amer. Math. Soc. Ser. B **7** (2020), 28–42.

[16] Carl Pomerance and Edward F. Schaefer, *Elliptic curves with Galois-stable cyclic subgroups of order 4*, Res. Number Theory **7** (2021), no. 2, Paper No. 35, 19 pages.

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

[18] Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory*, third ed., Grad. Studies in Math., vol. 163, American Mathematical Society, Providence, RI, 2015.

[19] David Vernon Widder, *The Laplace transform*, Princeton Math. Ser., vol. 6, Princeton University Press, Princeton, 1941.

[20] Wenguang Zhai, *Asymptotics for a class of arithmetic functions*, Acta Arith. **2** (2015), 135–160.

Department of Mathematics, Dartmouth College, Hanover, NH 03755-3551
Email address: Grant.S.Molnar.GR@dartmouth.edu
URL: http://www.math.grantmolnar.com

Department of Mathematics, Dartmouth College, Hanover, NH 03755-3551
Email address: jvoight@gmail.com
URL: http://www.math.dartmouth.edu/~jvoight