COUNTING ELLIPTIC CURVES WITH A CYCLIC m-ISOGENY OVER $\mathbb{Q}$

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Mathematics

by

Grant Molnar

DARTMOUTH COLLEGE

Hanover, New Hampshire

April 24, 2023

Examining Committee:

John Voight, Chair

Asher Auel

Robert Lemke Oliver

Carl Pomerance

F. Jon Kull, Ph.D.
Dean of Graduate and Advanced Studies

Abstract

Using methods from analytic number theory, for $m > 5$ and for $m = 4$, we obtain asymptotics with power-saving error terms for counts of elliptic curves with a cyclic m-isogeny up to quadratic twist over the rational numbers. For $m > 5$, we then apply a Tauberian theorem to achieve asymptotics with power saving error for counts of elliptic curves with a cyclic m-isogeny up to isomorphism over the rational numbers.

Preface

Throughout my academic and personal life, I have been blessed with support and guidance of many wonderful people. I would like to begin by honoring my mother and father, Wanda and Steven Molnar, for giving me a firm foundation to stand on and for fostering my love of exploration and enquiry. My parents have given me roots and wings throughout my life, and I am who I am because of them.

In the same breath, I recognize my wife, Brianna Molnar, for her heartfelt support, encouragement, and understanding. I like to think of myself as eloquent, but even perfectly placed words cannot capture or convey my affection and appreciation for her. Brianna is brave, and creative, and strong, and true. I love Brianna, and I have learned a great deal from her example.

My thanks go out to to my thesis advisor, John Voight, whose expertise, enthusiasm, and example have been instrumental in teaching me to do mathematics gracefully. I came to Dartmouth College to work with John, and I cannot imagine a better advisor than he is. John's patient mentorship and constructive feedback have been essential in guiding my work: were it not for John, this thesis would not exist.

I likewise thank the members of my thesis committee, John Voight, Asher Auel, Robert Lemke Oliver, and Carl Pomerance, for taking the time to read and refine my work.

I am grateful to Eran Assaf, Jesse Elliott, Mits Kobayashi, David Lowry-Duda, Tristan Phillips, and Rakvi for their helpful comments and discussions, which have greatly improved

the quality of my thesis.

I am deeply delighted to have made this academic voyage alongside my cohort: Lizzie Buchanan, Steve Fan, Richard Haburcak, and Alexander Wilson. Their support and encouragement have been invaluable, and I could not have asked for better colleagues.

Nor are they the only fellow-travelers who I now salute. Along with Steve Fan, I thank Jennifer Molnar and Taylor Petty for commiserating with me about the challenges of thesis work. Both their griping and goodwill kept me going. I also want to extol the 2021-2022 Dartmouth Graduate Student Council Executive Board and the Dartmouth Graduate Student Council Ad Hoc Healthcare Committee, for their work and for our friendship. Most especially, I thank Elizabeth Bien, Keighley Rockcliffe, and Kelly Cantwell. Their energy and dedication to improving the graduate student experience has been inspiring, and I am privileged to have worked alongside them.

I laud the tireless and ofttimes thankless work of the Baker-Berry Library staff, who processed and accommodated hundreds of my requests for books and papers during the half-decade I have been at Dartmouth. Finally, I would like to acknowledge the Gridley Fund for Graduate Mathematics and the Simons Collaboration (grant 550029, to John Voight) for their financial support, which enabled me to pursue my research.

Contents

Chapter 1

Introduction

In section 1.1, we briefly motivate the study of the count of ellipic curves with a cyclic m-isogeny over $\mathbb{Q}$, and establish the notation necessary to state our main results. In section 1.2, we report on our asymptotics for elliptic curves equipped with or admitting a cyclic m-isogeny over $\mathbb{Q}$, first up to $\mathbb{Q}$-isomorphism, and then up to twist equivalence. In section 1.3, we sketch our approach for proving these asymptotics. Finally, in section 1.4, we outline the structure for the remainder of this thesis.

Section 1.1

Motivation and setup

In this section, we outline the scope of our results and give impetus for studying the count of elliptic curves with a cyclic m-isogeny over $\mathbb{Q}$ whose naïve height is less than or equal to X (readers unfamiliar with elliptic curves or cyclic isogenies are directed to section 2.1). We then set up the notation necessary to state our results.

Motivation

Elliptic curves have been an object of fascination for number theorists and geometers for over a century. Much effort has gone into developing tools to understand the behavior of particular elliptic curves. But in the last twenty years, there has been an explosion of interest in the statistical behavior of families of elliptic curves [3, 5, 7, 9, 16, 19, 20, 24, 27, 28, 45, 51, 53, 55, 56, 67, 70]. For more on the history of the arithmetic statistics of elliptic curves, see section 2.2.

In this thesis, we recount and strengthen arguments made in [45] to estimate the number of elliptic curves equipped with (or admitting) a cyclic 7-isogeny over $\mathbb{Q}$. We then go further, and adapt the methods of [45] to estimate the number of elliptic curves equipped with (or admitting) a cyclic m-isogeny for $m \in \{6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$, improving on prior results [51] and giving entirely new asymptotics for $m \in \{10, 13, 25\}$. Finally, we give asymptotics for the number of elliptic curves equipped with (or admitting) a cyclic m-isogeny for $m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}$, where the associated compactified modular curve $X_0(m)$ has nonzero genus.

In conjunction with earlier work, for all $m \in \mathbb{Z}_{>0}$ except $m = 5$, we establish asymptotics for the number of elliptic curves equipped with or admitting a cyclic m-isogeny over $\mathbb{Q}$ (see section 1.2 and section 2.3).

These asymptotics are a natural area of study for several reasons. Concretely, individual elliptic curves can be rather delicate objects to work with, and it is interesting to ask what behavior is typical of elliptic curves: for instance, section 1.2 and section 2.3 together show that almost all elliptic curves $E/\mathbb{Q}$ have no cyclic isogenies besides the trivial automorphisms $\pm 1 : E \xrightarrow{\sim} E$. As a consequence, counting elliptic curves by height up to (cyclic) isogeny yields the same asymptotics as counting elliptic curves by height up to $\mathbb{Q}$-isomorphism.

In addition, the modular curve $Y_0(m) \subseteq X_0(m)$ is a moduli space for elliptic curves equipped with a cyclic m-isogeny, so counting elliptic curves equipped with a cyclic m-

isogeny over $\mathbb{Q}$ may serve as an example and prototype for counting elliptic curves with other level structure (see [16, 52]). More abstractly, counting elliptic curves with a cyclic m-isogeny requires overtly or implicitly grappling with the "stackiness" of modular curves like $X_0(7)$ and therefore has implications for the Batyrev–Manin conjecture and even larger questions in arithmetic geometry [21].

Setup

In this subsection, we establish notation which will be necessary to state our main theorems. We then recall notation for asymptotics from analytic number theory.

We begin by setting up a fragment of the theory of elliptic curves. Every elliptic curve E over $\mathbb{Q}$ has a unique minimal Weierstrass model of the form

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

where $A, B \in \mathbb{Z}$, $4A^3 + 27B^2 \neq 0$, and for every prime ℓ we have $\ell^4 \nmid A$ or $\ell^6 \nmid B$. If the minimal model for E is given by (1.1.1), we define the (naïve) height of E to be

$$\operatorname{ht}(E) := \max(4\,|A|^3\,, 27\,|B|^2). \tag{1.1.2}$$

Let $\mathscr{E}$ be the set of elliptic curves over $\mathbb{Q}$ in their minimal model, and let

$$\mathscr{E}_{\leq X} := \{E \in \mathscr{E} : \operatorname{ht}(E) \leq X\}. \tag{1.1.3}$$

For $m \in \mathbb{Z}_{>0}$ and $E, E' \in \mathscr{E}$, a cyclic m-isogeny $\phi : E \to E'$ is a morphism of elliptic curves such that $\ker \phi \subseteq E(\mathbb{Q}^{\mathrm{al}})$ is a cyclic group of order m (the unfamiliar reader may peruse section 2.1 for more information). Here, as usual, $\mathbb{Q}^{\mathrm{al}}$ denotes the algebraic closure of $\mathbb{Q}$. In this thesis, all isogenies are defined over $\mathbb{Q}$ unless otherwise indicated. An unsigned isogeny is an isogeny up to postcomposition by ±1.

We define

$$\begin{aligned}\widetilde{N}_m(X) &:= \#\left\{(E,\phi) : E \in \mathscr{E}_{\le X} \text{ and } \phi : E \to E' \text{ an unsigned cyclic } m\text{-isogeny}\right\},\\ N_m(X) &:= \#\left\{E \in \mathscr{E}_{\le X} : E \text{ admits a cyclic } m\text{-isogeny}\right\},\end{aligned} \tag{1.1.4}$$

where as usual the cyclic m-isogeny ϕ is defined over $\mathbb{Q}$, and $E' \in \mathscr{E}$.

Let E have a Weierstrass model

$$E : y^2 = x^3 + Ax + B, \tag{1.1.5}$$

which is not necessarily minimal, i.e., we might have $d^4 \mid A$ and $d^6 \mid B$ for some $d > 1$. For $c \in \mathbb{Q}^\times$, the quadratic twist $E^{(c)}$ of E via c is defined by the Weierstrass equation

$$E^{(c)} : y^2 = x^3 + c^2Ax + c^3B, \tag{1.1.6}$$

and we have a $\mathbb{Q}^{\mathrm{al}}$-isomorphism $E \xrightarrow{\sim} E^{(c)}$ given by $(x,y) \mapsto (cx, c^{3/2}y)$. We say $E, E' \in \mathscr{E}$ are twist equivalent if $E' = E^{(c)}$ for some $c \in \mathbb{Q}^\times$; if $j(E) \neq 0, 1728$, then $E, E' \in \mathscr{E}$ are twist equivalent if and only if they are $\mathbb{Q}^{\mathrm{al}}$-isomorphic (see Corollary 2.1.12).

We let $\mathscr{E}^{\mathrm{tw}}$ denote the set of elliptic curves over $\mathbb{Q}$ up to twist equivalence. We define the twist height of E to be

$$\operatorname{twht}(E) := \min\left\{\operatorname{ht}(E') : E' \in \mathscr{E} \text{ is twist equivalent to } E\right\}, \tag{1.1.7}$$

and we let

$$\mathscr{E}^{\mathrm{tw}}_{\le X} := \{E \in \mathscr{E}^{\mathrm{tw}} : \operatorname{twht}(E) \le X\}. \tag{1.1.8}$$

Twist equivalence preserves (cyclic) isogenies (Corollary 2.1.37), so it is natural to define

$$\begin{aligned} \widetilde{N}_m^{\mathrm{tw}}(X) &:= \#\left\{(E,\phi) : E \in \mathscr{E}_{\leq X}^{\mathrm{tw}} \text{ and } \phi : E \to E' \text{ unsigned cyclic } m\text{-isogeny}\right\}, \\ N_m^{\mathrm{tw}}(X) &:= \#\left\{E \in \mathscr{E}_{\leq X}^{\mathrm{tw}} : E \text{ admits a cyclic } m\text{-isogeny}\right\} \end{aligned} \tag{1.1.9}$$

(as above, the m-isogeny ϕ is defined over $\mathbb{Q}$, and $E' \in \mathscr{E}$). The functions defined in (1.1.4) and (1.1.9) are the main objects of study in this thesis.

We adopt the following notations from analytic number theory. For eventually positive functions $f, g, h : \mathbb{R}_{>0} \to \mathbb{R}$, we write

$$f(X) = g(X) + O(h(X)) \tag{1.1.10}$$

for $X \geq X_0$ if there is a constant C such that for all $X \geq X_0$ we have

$$|f(X) - g(X)| < Ch(X). \tag{1.1.11}$$

If we write (1.1.10) without specifying an X_0, then (1.1.11) holds for all X sufficiently large. If $f(X) = O(g(X))$, we also may write $f(X) \ll g(X)$.

Similarly, we write

$$f(X) = g(X) + o(h(X)) \tag{1.1.12}$$

if

$$\lim_{X\to\infty} \left| \frac{f(X) - g(X)}{h(X)} \right| = 0. \tag{1.1.13}$$

If $g(X) = h(X)$ in (1.1.12), we write $f(X) \sim g(X)$. As the notation suggests, this is an equivalence relation.

Finally, we write

$$f(X) \asymp g(X) \tag{1.1.14}$$

if there are constants $C_1, C_2 \in \mathbb{R}_{>0}$ such that

$$C_1 f(X) < g(X) < C_2 f(X) \tag{1.1.15}$$

for all X sufficiently large.

Section 1.2

Results

In this section, we give asymptotics for $\widetilde{N}_m(X)$ and $N_m(X)$ for $m > 5$. We then give asymptotics for $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$ for $m > 5$ and for $m = 4$. To our knowledge, for $m \in \{7, 10, 13, 25\}$, even the order of growth for $N_m(X)$ and $\widetilde{N}_m(X)$ was previously unknown (see [7, Remark 4.2]).

Main results

In this subsection, we present asymptotics for $\widetilde{N}_m(X)$ and $N_m(X)$ for all m such that the compactified modular curve $X_0(m)$ has genus 0 and $m > 5$, i.e., for

$$m \in \{6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}. \tag{1.2.1}$$

We then present results for all m such that $X_0(m)$ has nonzero genus and the noncompactified modular curve $Y_0(m)$ has $Y_0(m)(\mathbb{Q}) \neq \emptyset$, i.e., for

$$m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}. \tag{1.2.2}$$

Theorem 1.2.3. *Let $m \in \{6, 7, 8, 9\}$. Then there are effectively computable constants $\widetilde{c}_m$,*

$\widetilde{c}'_m$, c_m, and c'_m such that for any $\epsilon > 0$, we have

$$\widetilde{N}_m(X) = \widetilde{c}_m X^{1/6} \log X + \widetilde{c}'_m X^{1/6} + O(X^{1/8+\epsilon}) \tag{1.2.4}$$

and

$$N_m(X) = c_m X^{1/6} \log X + c'_m X^{1/6} + O(X^{1/8+\epsilon}) \tag{1.2.5}$$

for $X \geq 1$. The implicit constant depends on m and ϵ.

Theorem 1.2.6. *Let $m \in \{10, 12, 13, 16, 18, 25\}$. Then there are effectively computable constants $\widetilde{c}_m$ and c_m such that for any $\epsilon > 0$, we have*

$$\widetilde{N}_m(X) = \widetilde{c}_m X^{1/6} + O(X^{1/8+\epsilon}) \tag{1.2.7}$$

and

$$N_m(X) = c_m X^{1/6} + O(X^{1/8+\epsilon}) \tag{1.2.8}$$

for $X \geq 1$. The implicit constant depends on m and ϵ.

In both Theorem 1.2.3 and Theorem 1.2.6, the constants $\widetilde{c}_m$ and c_m are positive, but the constants $\widetilde{c}'_m$ and c'_m need not be: for instance, when $m = 7$, we have

$$\widetilde{c}'_7 = c'_7 \approx -0.16. \tag{1.2.9}$$

Theorem 1.2.3 summarizes results given in Theorem 4.4.11, Theorem 7.2.16, and Corollary 7.2.28; likewise, Theorem 1.2.6 summarizes results given in Theorem 5.4.11, Theorem 6.4.5, Theorem 7.2.16, and Corollary 7.2.28. Theorem 1.2.3 and Theorem 1.2.6 extend and strengthen results in the literature [51]; see section 2.2 for more details.

The cases $m \in \{7, 10, 13, 25\}$ are of special interest, because their associated modular curves $X_0(m)$ have multiple elliptic points. Consequently, for these m, the elliptic surfaces that parameterize elliptic curves equipped with a cyclic m-isogeny have points of additive reduction.

We now present the asymptotics for $\widetilde{N}_m(X) = N_m(X)$ when $X_0(m)$ has nonzero genus and $Y_0(m) \subseteq X_0(m)$ has $Y_0(m)(\mathbb{Q}) \neq \emptyset$.

Theorem 1.2.10 (Theorem 8.2.8 and Theorem 8.2.10)**.** *Let*

$$m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}. \tag{1.2.11}$$

Then there is a positive, effectively computable constant c_m such that

$$\widetilde{N}_m(X) = N_m(X) = c_m X^{1/6} + o\left(X^{1/12}\right). \tag{1.2.12}$$

If the Riemann hypothesis holds, then for any $\epsilon > 0$, we may replace the error term with $O\left(X^{11/210+\epsilon}\right)$ for $X \geq 1$, with the implicit constant now depending on ϵ.

Theorem 1.2.10 is almost immediate from Walfisz's and Liu's estimates for counts of squarefree integers [42, 66], both of which utilize zero-free regions for the Riemann zeta function. In fact, Walfisz's estimate gives a slight improvement on the $o(X^{1/12})$ error in Theorem 1.2.10. The equality $\widetilde{N}_m(X) = N_m(X)$ in Theorem 1.2.10 is exact: no elliptic curve over $\mathbb{Q}$ admits more than one cyclic m-isogeny when $X_0(m)(\mathbb{Q}) < \infty$. The constants c_m are given explicitly in Table 8.2.12.

The cases $m \in \{1, 2, 3, 4, 5\}$ were handled by previous authors, and we report them in section 2.3; in the case $m = 5$, only the order of growth for $\widetilde{N}_5(X)$ and $N_5(X)$ is given (Theorem 2.3.13). For all $m > 5$ not addressed by Theorem 1.2.3, Theorem 1.2.6, and Theorem 1.2.10, Mazur's theorem on isogenies (Theorem 2.1.48) implies $\widetilde{N}_m(X) = N_m(X) = 0$ identically. Thus for all $m \neq 5$, we have asymptotics with power-saving error for $\widetilde{N}_m(X)$ and $N_m(X)$. Of course, much work remains to be done in counting elliptic curves with a cyclic m-isogeny over global fields.

Twist results

In this subsection, we present asymptotics for $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$ for all m such that $X_0(m)$ has genus 0 and $m \notin \{2,3,5\}$. These asymptotics are stepping stones to the results in the previous subsection, but we view them as natural and interesting in their own right.

Theorem 1.2.13. *Let $m \in \{1,4,6,7,8,9,10,12,13,16,18,25\}$. Then there are positive, effectively computable constants c_m^{tw} and $\widetilde{c}_m^{\mathrm{tw}}$ such that for all $\epsilon > 0$, we have*

$$\widetilde{N}_m^{\mathrm{tw}}(X) = \widetilde{c}_m^{\mathrm{tw}} X^{1/d(m)} + O\left(X^{1/e(m)+\epsilon}\right) \tag{1.2.14}$$

and

$$N_m^{\mathrm{tw}}(X) = c_m^{\mathrm{tw}} X^{1/d(m)} + O\left(X^{1/e(m)+\epsilon}\right) \tag{1.2.15}$$

for $X \geq 1$. The exponents $d(m)$ and $e(m)$ are given in Table 1.2.16 below. The implicit constants depend on m and ϵ.

It turns out that $\widetilde{c}_m^{\mathrm{tw}} = c_m^{\mathrm{tw}}$ when $m \in \{5,6,7,9,13,18,25\}$, and that $\widetilde{c}_m^{\mathrm{tw}} = 2c_m^{\mathrm{tw}}$ when $m \in \{4,8,12,16\}$ (see Corollary 2.1.50 and Lemma 7.2.23).

m	1	4	6	7	8	9	10	12	13	16	18	25
$d(m)$	6/5	3	6	6	6	6	12	12	12	12	18	18
$e(m)$	2	6	12	12	12	12	21	24	15	24	36	33

Table 1.2.16: Exponents for asymptotics of $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$

Theorem 1.2.13 summarizes the asymptotics given by (2.3.3), Theorem 4.3.57, Theorem 5.4.11, Theorem 6.4.5, and Theorem 7.2.16. We have coarsened the error terms of these theorems slightly for uniformity and clarity of exposition.

We do not have asymptotics for $\widetilde{N}_2^{\mathrm{tw}}(X)$, $N_2^{\mathrm{tw}}(X)$, $\widetilde{N}_3^{\mathrm{tw}}(X)$, $N_3^{\mathrm{tw}}(X)$, $\widetilde{N}_5^{\mathrm{tw}}(X)$, or $N_5^{\mathrm{tw}}(X)$ (see Remark 5.3.51). To our knowledge, no prior work has been done on counting elliptic curves with a cyclic m-isogeny over global fields up to quadratic twist.

Section 1.3

Our approach

In this section, we sketch our methodology for proving Theorem 1.2.3, Theorem 1.2.6, Theorem 1.2.10, and Theorem 1.2.13. We revisit and expand on this sketch in section 3.5 below.

Choose m so that $X_0(m)$ is of genus 0. Our approach to proving Theorem 1.2.3, Theorem 1.2.6, and Theorem 1.2.13 proceeds through five main steps.

(1) We employ the modular curve $X_0(m)$ to establish a parameterization for the family of elliptic curves equipped with a cyclic m-isogeny. We obtain two polynomials $f_m(t)$ and $g_m(t)$ such that up to twist equivalence, each elliptic curve with a cyclic m-isogeny may be written in the form

$$E : y^2 = x^3 + f_m(t)x + g_m(t) \tag{1.3.1}$$

for some $t \in \mathbb{Q}$ (Lemma 3.2.1).

(2) Writing $t = a/b$ and homogenizing (1.3.1), the elliptic curves equipped with a cyclic m-isogeny up to twist equivalence are parameterized by coprime pairs $(a, b) \in \mathbb{Z}^2$. We apply the Principle of Lipschitz (Theorem 3.3.2), which asserts that the number of lattice points within a region can be approximated by the area of that region, to derive a coarse estimate for the count of Weierstrass equations of the form $E : y^2 = x^3+Ax+B$ that arise from (1.3.1) in this fashion (Corollary 3.3.11).

(3) The discrepancy between the coefficients of the model (1.3.1) and the twist height of

E may be quite large. However, the set of pairs (a, b) for which this "twist minimality defect" (see (3.1.9)) is divisible by a given integer e can be expressed as a finite union of sublattices of $\mathbb{Z}^2$, and therefore can be estimated using step 2. In addition, a single elliptic curve E may occur more than once in the estimates given above, since $da/db = a/b$. Recall that the Möbius sieve is a method that applies the inclusion-exclusion principle to the prime factorizations of integers. Using two Möbius sieves (see Lemma 3.5.7 and for example Lemma 4.3.16), one for each of these issues, we write $\widetilde{N}_m^{\mathrm{tw}}(X)$ in terms of the estimates obtained in the previous step. This gives us Theorem 1.2.13 for $\widetilde{N}_m^{\mathrm{tw}}(X)$.

(4) We bound the difference between $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$ or $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $2N_m^{\mathrm{tw}}(X)$ (Corollary 2.1.50 and Lemma 7.2.23). For each proper divisor n of m, there is a modular curve parameterizing elliptic curves equipped with a pair of cyclic m-isogenies whose kernels have intersection of order n. If $m \in \{4, 8, 12, 16\}$ and $n = m/2$, this modular curve is $X_0(m)$ itself: this is why $\widetilde{c}_m^{\mathrm{tw}} = 2c_m^{\mathrm{tw}}$ for these m. Otherwise, when the modular curves indexed by m and n are of genus 0, we emulate our first step (see also [16, Theorem 3.3.1]) to bound this contribution to $\widetilde{N}_m^{\mathrm{tw}}(X) - N_m^{\mathrm{tw}}(X)$ or to $\widetilde{N}_m^{\mathrm{tw}}(X) - 2N_m^{\mathrm{tw}}(X)$, depending on whether $4 \mid m$. When the modular curves are of genus greater than 1, Faltings's theorem [22, 23] assures us that we get a contribution of at most $O(1)$ to $\widetilde{N}_m^{\mathrm{tw}}(X) - N_m^{\mathrm{tw}}(X)$ or $\widetilde{N}_m^{\mathrm{tw}}(X) - 2N_m^{\mathrm{tw}}(X)$. When the modular curves are of genus 1, the contribution is still $O(1)$ by inspection. We obtain Theorem 1.2.13 in its entirety.

(5) Finally, we wish to estimate $\widetilde{N}_m(X)$ and $N_m(X)$ using our estimates for $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$. We first use Theorem 1.2.13 to establish a half-plane of convergence for the height zeta functions $\widetilde{L}_m^{\mathrm{tw}}(s)$ and $L_m^{\mathrm{tw}}(X)$ associated to $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$ (see for example Corollary 4.3.66). The height zeta functions $\widetilde{L}_m^{\mathrm{tw}}(s)$ and $L_m^{\mathrm{tw}}(s)$ are closely related to the height zeta functions $\widetilde{L}_m(s)$ and $L_m(s)$ of $\widetilde{N}_m(X)$ and $N_m(X)$ (Theorem 3.5.26).

> Recall that a Tauberian theorem establishes a connection between the asymptotics of a sequence and the analytic behavior of an associated function. We use Landau's Tauberian theorem (Theorem 3.4.37) as presented by Roux [58] to express the asymptotics of $\widetilde{N}_m(X)$ and $N_m(X)$ in terms of residues of $X^s\widetilde{L}_m(s)/s$ and $X^sL_m(s)/s$. This gives us Theorem 1.2.3 and Theorem 1.2.6.

Our key innovations occur in step 3, where we address the discrepancy between the size of a model and the twist of the associated elliptic curve, and in step 5, where our estimates for $\widetilde{N}_m^{\text{tw}}(X)$ and $N_m^{\text{tw}}(X)$ to obtain estimates for $\widetilde{N}_m(X)$ and $N_m(X)$.

Remark 1.3.2. In conjunction with earlier work, we obtain asymptotics for $\widetilde{N}_m(X)$ and $N_m(X)$ for all $m \neq 5$. In the case $m = 5$, steps 1 and 2 of our approach go through without obstruction, and we able to set up the sieves in step 3 as well. However, in this case our sieve tells us only that

$$\widetilde{N}_5^{\text{tw}}(X), N_5^{\text{tw}}(X) = O(X^{1/6}\log X), \tag{1.3.3}$$

rather than giving us a power-saving asymptotic for $m = 5$. On a technical level, this occurs because the polynomials appearing in (1.3.1) are of too low degree. If we were able to obtain an asymptotic for $\widetilde{N}_5^{\text{tw}}(X)$ with power-saving error, we could follow steps 4 and 5 of our approach without further obstruction. See Remark 5.3.51 for more details.

Remark 1.3.4. The techniques of this thesis may be adapted to count the fibers of an elliptic surface

$$E(t) : y^2 = x^3 + f(t)x + g(t) \tag{1.3.5}$$

over $\mathbb{P}^1$ according to their twist heights, provided that the geometry of this elliptic surface is sufficiently similar to the elliptic surfaces we obtain in section 3.2.

If the compactified modular curve $X_0(m)$ has nonzero genus, and the noncompactified modular curve $Y_0(m) \subseteq X_0(m)$ has $Y_0(m)(\mathbb{Q}) \neq \emptyset$, we can use the classical enumeration of the rational points on $X_0(m)$ (see Table 8.1.2 or [43]) in conjunction with Walfisz's count of squarefree integers (Theorem 3.4.16) and Liu's contingent refinement (Theorem 3.4.18) to deduce Theorem 1.2.10.

Section 1.4

Contents

In this section, we summarize the contents in the remainder of the thesis.

In chapter 2, we review the fundamentals of elliptic curves and relay the history and context for our problem. In chapter 3, we gather several results from geometry and analysis for later use. We close the chapter by expanding on section 1.3 to give a more detailed outline of the argument we will use to prove our main theorems. In chapter 4, we apply the material from chapter 3 to prove Theorem 1.2.3 and Theorem 1.2.13 when $m = 7$, establishing the asymptotics for $\widetilde{N}_7^{\text{tw}}(X) = N_7^{\text{tw}}(X)$ and $\widetilde{N}_7(X) = N_7(X)$. In chapter 5, we adapt the methods of chapter 4 to prove Theorem 1.2.6 and Theorem 1.2.13 when $m = 10, 25$, establishing the asymptotics for these $\widetilde{N}_m^{\text{tw}}(X) = N_m^{\text{tw}}(X)$ and $\widetilde{N}_m(X) = N_m(X)$. In chapter 6, we elaborate on the methods of chapter 4 and chapter 5 to prove Theorem 1.2.6 and Theorem 1.2.13 when $m = 13$, establishing the asymptotics for $\widetilde{N}_{13}^{\text{tw}}(X) = N_{13}^{\text{tw}}(X)$ and $\widetilde{N}_{13}(X) = N_{13}(X)$.. In chapter 7, we prove Theorem 1.2.3, Theorem 1.2.6, and Theorem 1.2.13 for all other $m > 5$ for which $X_0(m)$ has genus 0, establishing the asymptotics for these $\widetilde{N}_m^{\text{tw}}(X)$, $N_m^{\text{tw}}(X)$, $\widetilde{N}_m(X)$, and $N_m(X)$, as well as for $\widetilde{N}_4^{\text{tw}}(X)$ and $N_4^{\text{tw}}(X)$. In chapter 8, we prove Theorem 1.2.10, establishing asymptotics for $\widetilde{N}_m(X) = N_m(X)$ when $X_0(m)$ is of nonzero genus.

Chapter 2

Historical background

In section 2.1, we review the basic theory of elliptic curves and their isogenies. In section 2.2, we survey the history of the arithmetic statistics of elliptic curves, with a slant towards our main problem. In section 2.3, we recall several results from the literature which, taken in conjunction with the results of section 1.2, yield an almost complete picture of the asymptotics for counts of elliptic curves over $\mathbb{Q}$ with a cyclic m-isogeny.

This chapter may be skimmed or skipped in its entirety by readers familiar with both elliptic curves and the history of our problem.

Section 2.1

A primer on elliptic curves

In this section, we briefly review and motivate the study of elliptic curves, and highlight several important results from the discipline. We do not aim for generality in this section, and freely assume that our elliptic curves are defined over a field of characteristic 0 or even over $\mathbb{Q}$ whenever convenient. The curious reader can learn more from any of a number of standard references [39, 61, 62, 63] (see also [29, Chapter IV.4]).

An elliptic curve is a pair (E, O), where E is a nonsingular projective curve of genus 1, and $O \in E$. We typically write E for the elliptic curve (E, O), and elide the description of this distinguished point. If K is a field, the elliptic curve E is defined over K, written E/K, if E is defined over K as a curve and $O \in E(K)$. In this thesis, we shall be interested in elliptic curves over the rational numbers $\mathbb{Q}$, so we typically take $K = \mathbb{Q}$ to be the field of rational numbers.

Elliptic curves are natural objects of study for many reasons. We record several of them now.

The genus $g \in \mathbb{Z}_{\geq 0}$ of a curve provides a coarse measure of its geometric and arithmetic complexity, and it is well-known that a curve has genus 0 if and only if it is birationally equivalent to the projective line $\mathbb{P}^1$ [29, Example IV.1.3.5]. We therefore have a thorough geometric understanding of genus 0 curves, and genus 1 curves like elliptic curves are the natural next case to study.

Arithmetic geometry concerns itself in large part with determining the rational points of a variety $V/\mathbb{Q}$. If a curve of genus $g = 0$ has any rational points, then it has infinitely many rational points. On the other hand, Faltings proved the following remarkable theorem for curves of genus greater than 1.

Theorem 2.1.1 (Faltings's Theorem)**.** *Let $C/\mathbb{Q}$ be a nonsingular algebraic curve of genus g. If $g > 1$, then C has at most finitely many rational points.*

Proof. Faltings [22, 23]. □

Algebraic curves of genus 1 lie on the boundary of these two cases: they can have no rational points, finitely many rational points, or infinitely many rational points.

There are ample other reasons to be fascinated with elliptic curves. For instance, the modularity theorem [18, Preface] asserts that every elliptic curve arises from a modular form. An elliptic curve E also induces an adelic Galois representation via its Tate modules [62, Section III.7], and gives rise to an L-function via its $\mathbb{F}_p$-points [62, Appendix C.16]. These four objects–elliptic curves, modular forms, Galois representations, and L-functions–are all interrelated via the Langlands program, which remains a lively area of research [13, 15, 25, 26, 41]. The Birch and Swinnerton-Dyer Conjecture, one of the seven famed millenium problems, relates the L-function of an elliptic curve to its set of rational points [1].

Although elliptic curves are rather abstract objects as we have defined them, every elliptic curve may be concretely realized as the zero set of a Weierstrass equation, as the following theorem shows.

Theorem 2.1.2 ([62, Proposition 3.1])**.** *Let E be an elliptic curve defined over a field K of characteristic 0.*

(a) *There exist functions $x, y \in K(E)$ such that the map*

$$\begin{aligned} \phi &: E \to \mathbb{P}^2 \\ \phi &= (x : y : 1) \end{aligned} \tag{2.1.3}$$

gives a K-isomorphism of E/K onto a curve given by a (simplified) Weierstrass equation

$$E : y^2 = x^3 + Ax + B \tag{2.1.4}$$

with coefficients $A, B \in K$, and such that $\phi(O) = (0 : 1 : 0) \in \mathbb{P}^2$.

(b) *Any two Weierstrass equations as in (a) are related by a linear change of variables of the form*

$$(x, y) \mapsto (u^2 x, u^3 y) \tag{2.1.5}$$

with $u \in K^\times$. This change of variables yields the model

$$E^{(u^2)} : y^2 : x^3 + u^4 Ax + u^6 B \tag{2.1.6}$$

(c) *Conversely, every nonsingular cubic curve C given by a Weierstrass equation of the form* (2.1.4) *is an elliptic curve defined over K with distinguished point $\infty = (0 : 1 : 0)$. Nonsingularity is equivalent to the discriminant*

$$\Delta(E) = \Delta(A, B) = -16(4A^3 + 27B^2) \tag{2.1.7}$$

of the model being nonzero.

Remark 2.1.8. [62, Proposition 3.1] only affirms a K-isomorphism from E to a curve C in $\mathbb{P}^2$ of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \tag{2.1.9}$$

however, because we have assumed K is not of characteristic 2 or 3, a linear change of variables reduces (2.1.9) to (2.1.4).

Theorem 2.1.2(a) is a consequence of the Riemann–Roch theorem; like many results about elliptic curves, it is proven using tools from algebraic geometry. Here and later in the thesis, we will have no direct need of divisors, Jacobians, the Riemann–Roch theorem, or anything of the sort: while we will freely reference results proven using such techniques, we elide the techniques themselves as a technical distraction.

If E has (2.1.4) as its Weierstrass equation, we define the j-invariant $j(E)$ of E as follows:

$$j(E) = j(A, B) := -1728\frac{(4A)^3}{\Delta(A, B)} = \frac{2^8 \cdot 3^3 \cdot A^3}{4A^3 + 27B^2}. \tag{2.1.10}$$

Two elliptic curves have the same j-invariant if and only if they are $\mathbb{Q}^{\mathrm{al}}$-isomorphic [62, Proposition 1.4(b)].

Theorem 2.1.2 gives us an infinite family of models for every elliptic curve, but each such elliptic curve has a canonical minimal model over $\mathbb{Q}$. Indeed, as noted in section 1.2, every elliptic curve $E/\mathbb{Q}$ has a unique Weierstrass model of the form

$$E\colon y^2 = x^3 + Ax + B, \tag{2.1.11}$$

where $A, B \in \mathbb{Z}$, $\Delta(A, B) \neq 0$, and for every prime ℓ we have $\ell^4 \nmid A$ or $\ell^6 \nmid B$. Recall that $\mathscr{E}$ is the set of Weierstrass models of this form. With this notation in mind, Theorem 2.1.2 has the following corollary.

Corollary 2.1.12. *Let $E, E' \in \mathscr{E}$, and suppose E is $\mathbb{Q}^{\mathrm{al}}$-isomorphic to E'. The following statements hold.*

- *If $j(E) \neq 0, 1728$, then E' is a quadratic twist of E.*
- *If $j(E) = 0$, then E' is a sextic twist of E.*
- *If $j(E) = 1728$, then E' is a quartic twist of E.*

Proof. Write

$$E : y^2 = x^3 + Ax + B. \tag{2.1.13}$$

By Theorem 2.1.2(b), the $\mathbb{Q}^{\mathrm{al}}$-isomorphism of E with E' implies

$$E' = E^{(u^2)} : y^2 : x^3 + u^4Ax + u^6B \tag{2.1.14}$$

for some $u \in (\mathbb{Q}^{\mathrm{al}})^{\times}$. On the other hand, as $E' \in \mathscr{E}$, we see $u^4A, u^6B \in \mathbb{Q}$.

If $j(E) \neq 0, 1728$ then $A, B \neq 0$, so comparing these equations we see $u^4, u^6 \in \mathbb{Q}^{\times}$. Thus $u^2 = u^6/u^4 \in \mathbb{Q}^{\times}$, and E' is a quadratic twist of E as desired.

If $j(E) = 0$, then $u^6 \in \mathbb{Q}^{\times}$, so E' is a sextic twist of E. If $j(E) = 1728$, then $u^4 \in \mathbb{Q}^{\times}$, so E' is a quartic twist of E. □

The group law for an elliptic curve

In this subsection, we give a concrete description of the group law for an elliptic curve, and recall Mordell's Theorem (Theorem 2.1.20) and Mazur's theorem on torsion (Theorem 2.1.20 and Theorem 2.1.22). The material outlined here is classical.

Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass model (2.1.4), and let $P, Q \in E(\mathbb{Q})$. Let L denote the line in $\mathbb{P}^2$ passing through both P and Q (if $P = Q$, we take L to be tangent to P), and let R be the third point of intersection of L with E. Let L' be the line passing through R and ∞, and let R' be the third point of intersection of L' with E. We define $P + Q := R'$. For $P = (x_0, y_0) \in E$, we define $-P = (x, -y)$; in particular, the unique line L passing through both P and $-P$ also passes though ∞. By definition, we have $P + Q = -R$.

Example 2.1.15. *Let $E : y^2 = x^3 - 3x + 62$, let $P = (-1, 8)$, and let $Q = (2, -8)$. The line L is given in blue in Figure 2.1.17, and passes through the points P, Q, and $R = (247/9, -3880/27)$. The line L' is given in green in Figure 2.1.17, and passes through the points ∞, R, and $R' = (247/9, 3880/27)$. Thus*

$$(-1, 8) + (2, -8) = (247/9, 3880/27) \tag{2.1.16}$$

in E.

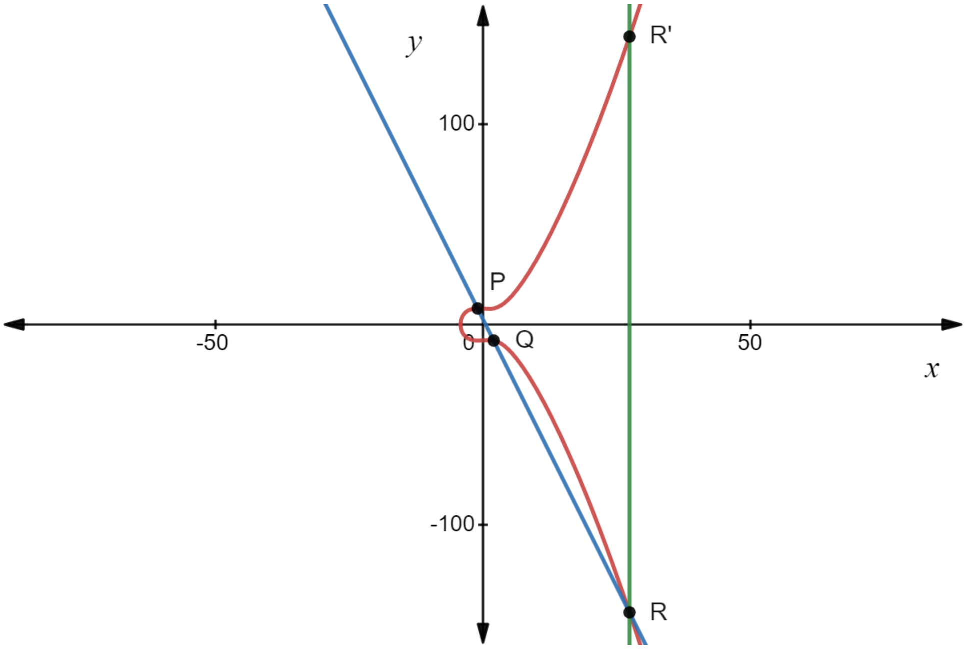

Figure 2.1.17: The elliptic curve $E : y^2 = x^3 - 3x + 62$, with some additions

As our notation suggests, we have the following theorem.

Theorem 2.1.18 ([62, Proposition 2.2])**.** *Let E be an elliptic curve with Weierstrass equation (2.1.4). The elliptic curve E is an abelian group under the binary operation $+$ defined above, with identity element ∞ and with inversion given by $P \mapsto -P$.*

Remark 2.1.19. Every elliptic curve E is isomorphic to its own Jacobian as an algebraic curve. The Jacobian of an elliptic curve is an abelian group by definition. Although we have given the group law of the elliptic curve geometrically, this group law is also induced on E via its the isomorphism with its Jacobian.

We can derive an explicit formula for calculating the sum of points on the elliptic curve E by examining its Weierstrass equation [62, Group Law Algorithm 2.3].

Note that if $K/\mathbb{Q}$ is a field extension of $\mathbb{Q}$ and $P, Q \in E(K)$, then $P + Q \in E(K)$ as well. Thus, E defines not a single group, but a family of groups, one for every field extension of $\mathbb{Q}$. This is the essential reason that E defines a group scheme. However, in this thesis we will never have occasion to consider groups other than $E(\mathbb{Q})$ and $E(\mathbb{Q}^{\mathrm{al}})$, so this rich structure will be largely invisible to us.

Theorem 2.1.18 tells us that $E(\mathbb{Q})$ is an abelian group, so it is natural to inquire about and classify its structure. This classification was done almost completely in the following two theorems, due to Mordell and Mazur.

Theorem 2.1.20 (Mordell's Theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the abelian group $E(\mathbb{Q})$ is finitely generated.*

Proof. Mordell [46]. Weil extended Mordell's theorem to number fields [68]. □

Due to Theorem 2.1.20 and Weil's extension thereof to number fields [68], we now call $E(\mathbb{Q})$ the Mordell–Weil group of E. Theorem 2.1.20 shows that we may write

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{\mathrm{tors}}, \tag{2.1.21}$$

where $r \geq 0$ is an integer and $E(\mathbb{Q})_{\mathrm{tors}}$ is a finite abelian group. The quest to understand the ranks of elliptic curves over $\mathbb{Q}$ is over a hundred years old [54, page 173] and remains an active area of study to this day (see [1, 5, 49]); by contrast, Mazur completely determined the possible torsion of an elliptic curve over $\mathbb{Q}$.

Theorem 2.1.22 (Mazur's Theorem on torsion)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. The group $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to one of the following fifteen groups:*

$$\begin{gathered} \mathbb{Z}/N\mathbb{Z} \text{ with } 1 \leq N \leq 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \text{ with } 1 \leq N \leq 4. \end{gathered} \tag{2.1.23}$$

Moreover, each of these fifteen groups occurs as the torsion group of infinitely many elliptic curves over $\mathbb{Q}$.

Proof. Mazur [43]. □

Isogenies

In this subsection, we define isogenies between elliptic curves and outline several of their remarkable properties. We finish the section by recalling Mazur's theorem on isogenies (Theorem 2.1.48). The material outlined here is classical.

If we agree that elliptic curves are interesting objects, it is natural to ask what constitutes a map between elliptic curves. If $E_1, E_2 \in \mathscr{E}$ are elliptic curves, such a map should at least give a morphism of curves $E_1 \to E_2$, and should also preserve the distinguished point ∞, so $\infty \mapsto \infty$. In the previous subsection, we also showed that the points of an elliptic curve have a natural group structure. Should we demand that our map of elliptic curves preserve this group structure? As it turns out, we get this property for free.

Theorem 2.1.24 ([62, Theorem 4.8])**.** *Let $E_1, E_2 \in \mathscr{E}$, and let $\phi : E_1 \to E_2$ be a morphism of curves (over $\mathbb{Q}$) with $\phi(\infty) = \infty$. Then for all points P, Q of E, we have*

$$\phi(P + Q) = \phi(P) + \phi(Q). \tag{2.1.25}$$

We refer to a morphism of curves $\phi : E_1 \to E_2$ for which $\phi(\infty) = \infty$ as an isogeny. Unless otherwise specified, we restrict our attention to nonconstant isogenies, which are necessarily surjective as maps over $\mathbb{Q}^{\mathrm{al}}$. Theorem 2.1.2 and the definition of $\mathscr{E}$ already gives us the following result.

Proposition 2.1.26. *Let $E_1, E_2 \in \mathscr{E}$ be elliptic curves over $\mathbb{Q}$, and let $\phi : E_1 \to E_2$ be an isomorphism of elliptic curves over $\mathbb{Q}$. Then $E_1 = E_2$, and ϕ is either the identity map $P \mapsto P$ or the negative map $P \mapsto -P$.*

Proof. By definition, $\mathscr{E}$ only contains one elliptic curve from each $\mathbb{Q}$-isomorphism class, so $E_1 = E_2$. Now by Theorem 2.1.2(b), ϕ is of the form

$$\phi : (x, y) \mapsto (u^2 x, u^3 y) \tag{2.1.27}$$

for some $u \in \mathbb{Q}^\times$, and we have $A = u^4 A\ B = u^6 B$. As a consequence, u is a fourth root of unity or a sixth root of unity, but the only roots of unity in $\mathbb{Q}$ are ± 1, so $u = \pm 1$. The claim follows. □

To avoid excessive clutter in our writing, we assume all isogenies given are isogenies over $\mathbb{Q}$ unless otherwise specified.

Somewhat remarkably, isogenies induce an equivalence relation on elliptic curves $E \in \mathscr{E}$. More precisely, we have the following proposition.

Proposition 2.1.28. *Let E_1, E_2 be elliptic curves, and let $\phi : E_1 \to E_2$ be a nonconstant degree m isogeny. There is a unique isogeny $\widehat{\phi} : E_2 \to E_2$ with*

$$\widehat{\phi} \circ \phi : P \mapsto mP \text{ and } \phi \circ \widehat{\phi} : P \mapsto mP. \tag{2.1.29}$$

Proof. Silverman [62, Theorem 6.1]. □

We say $E, E' \in \mathscr{E}$ are isogenous if there is a nonconstant isogeny $\phi : E \to E'$. By Proposition 2.1.28, this is an equivalence relation, which is coarser than $\mathbb{Q}$-isomorphism.

If $\phi, \widehat{\phi}$ are as in Proposition 2.1.28, we refer to $\widehat{\phi}$ as the dual isogeny of ϕ. We define the dual of the constant isogeny $0 : E_1 \to E_2$ to be the constant isogeny $0 : E_2 \to E_1$.

A morphism of curves is of degree m if it is generically m-to-one. If $\phi : E_1 \to E_2$ is a degree m isogeny, we say ϕ is an m-isogeny. Note that if $\phi : E_1 \to E_2$ is an m-isogeny and $\psi : E_2 \to E_3$ is an n-isogeny, then $\psi \circ \phi$ is an mn-isogeny. We now report some charming additional properties of dual isogenies.

Theorem 2.1.30. *Let $E_1, E_2 \in \mathscr{E}$, and let $\phi : E_1 \to E_2$ be a (nonconstant) isogeny. The following statements hold.*

(a) *If ϕ is an m-isogeny, then $\widehat{\phi}$ is an m-isogeny.*

(b) *Let $\psi : E_2 \to E_3$ be another isogeny. We have*

$$\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}. \tag{2.1.31}$$

(c) *Let $\phi' : E_1 \to E_2$ be another isogeny. We have*

$$\widehat{\phi + \phi'} = \widehat{\phi} + \widehat{\phi}'. \tag{2.1.32}$$

(d) *We have $\widehat{\widehat{\phi}} = \phi$.*

(e) *If $[m]$ is defined by*

$$[m] : P \mapsto mP, \tag{2.1.33}$$

then $\deg[m] = m^2$, *and $\widehat{[m]}$ is also defined by*

$$\widehat{[m]} : P \mapsto mP. \tag{2.1.34}$$

Proof. Silverman [62, Theorem 6.2] proves a more general result. □

If $\phi : E_1 \to E_2$ is an isogeny, we write $\ker \phi \subseteq E(\mathbb{Q}^{\mathrm{al}})$ for the kernel of ϕ. It turns out that the $\ker \phi$ determines almost the entire behavior of ϕ.

Theorem 2.1.35. *Let $E_1, E_2 \in \mathscr{E}$, and let $\phi : E_1 \to E_2$ be an isogeny. The following statements hold.*

(a) *If ϕ is an m-isogeny, then $\# \ker \phi = m$.*

(b) *Suppose $E_2' \in \mathscr{E}$ and $\phi' : E_1 \to E_2'$ is another isogeny, and suppose that $\ker \phi \subseteq \ker \phi'$. There is a unique isogeny $\psi : E_2 \to E_2'$ such that $\psi \circ \phi = \phi'$.*

Proof. Silverman [62, Theorem 4.10, Corollary 4.11] proves a more general result. □

We define an unsigned isogeny $\phi : E_1 \to E_2$ to be an isogeny up to postcomposition by ±1. By Proposition 2.1.26, an isogeny over $\mathbb{Q}$ up to postcomposition by the $\mathbb{Q}$-automorphisms of E_2 is the same as an unsigned isogeny over $\mathbb{Q}$.

Theorem 2.1.36. *Let $E \in \mathscr{E}$, and let $\Phi \subseteq E(\mathbb{Q}^{\mathrm{al}})$ be a finite group which is stabilized by the absolute Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$ of $\mathbb{Q}$. Then there is a unique elliptic curve $E' \in \mathscr{E}$, and a unique unsigned isogeny $\phi : E \to E'$ with $\ker \phi = \Phi$.*

Proof. Silverman [62, Proposition 4.12] (see also Vélu [65] for a more direct construction). □

As a consequence of Theorem 2.1.36, for each elliptic curve $E \in \mathscr{E}$, there is a bijection between (nonconstant) unsigned isogenies with domain E and finite subgroups of $E(\mathbb{Q}^{\mathrm{al}})$ which are stabilized by the absolute Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$, which we henceforth abbreviate as $\mathrm{Gal}_{\mathbb{Q}}$.

Corollary 2.1.37. *Let $E \in \mathscr{E}$ be an elliptic curve, and let E' be a quadratic twist of E. If $\Phi \subseteq E(\mathbb{Q}^{\mathrm{al}})$ is a finite abelian group stabilized by $\mathrm{Gal}_{\mathbb{Q}}$, then the image Φ' of Φ in E' under that quadratic twist is also an abelian group stabilized by $\mathrm{Gal}_{\mathbb{Q}}$. Moreover, $\Phi \simeq \Phi'$ as abelian groups.*

Proof. Let $\Phi \subseteq E(\mathbb{Q}^{\mathrm{al}})$ be a finite subgroup, and let

$$f(t) = \prod_{\substack{\pm P \in \Phi \\ P \neq \infty}} (t - x(P)) \in \mathbb{Q}^{\mathrm{al}}[t] \tag{2.1.38}$$

be the product of all linear terms $t - x(P)$ as x varies over the x-coordinates of the affine points in Φ. We see that $f(t) \in \mathbb{Q}[t]$ if and only if Φ is stable under $\mathrm{Gal}_{\mathbb{Q}}$.

Now write $E' = E^{(c)}$ for appropriately chosen $c \in \mathbb{Q}^{\times}$, and let $\iota^{(c)} : E \to E'$ be the $\mathbb{Q}^{\mathrm{al}}$-isomorphism $\iota^{(c)} : (x, y) \mapsto (c^2 x, c^3 y)$. By definition, we have $\Phi' = \iota^{(c)}(\Phi)$, so $\Phi' \simeq \Phi$ as abelian groups. On the other hand, the polynomial

$$f^{(c)}(t) = \prod_{\substack{\pm P \in \Phi' \\ P \neq \infty}} (t - x(P)) = \prod_{\pm P \in \Phi} (t - c^2 x(P)) \in \mathbb{Q}^{\mathrm{al}}[t] \tag{2.1.39}$$

is in $\mathbb{Q}[t]$ if and only Φ' is stable under $\mathrm{Gal}_{\mathbb{Q}}$. But

$$f^{(c)}(t) = c^{2 \deg f} f(t/c^2) \in \mathbb{Q}[t]. \tag{2.1.40}$$

Thus Φ' is stabilized under $\mathrm{Gal}_{\mathbb{Q}}$ as desired. □

By Corollary 2.1.37, an m-isogeny ϕ of an elliptic curve $E \in \mathscr{E}$ induces an m-isogeny ϕ' with isomorphic kernel for every quadratic twist E' of E. By contrast, if $j(E) = 0$ or $j(E) = 1728$, quartic or sextic twists E' or E might or might not preserve a given isogeny ϕ: in other words, the induced isogeny ϕ' on E' might or might not be defined over $\mathbb{Q}$.

Example 2.1.41. *The elliptic curve*

$$E : y^2 = x^3 + 1 \tag{2.1.42}$$

admits both a 2-isogeny and a 3-isogeny. Every sextic twist of E preserves its 3-isogeny (see [53, Lemma 2.7]), but only quadratic twists of E preserve its 2-isogeny (see the proof of Lemma 3.2.1).

We now turn our attention to a special class of isogenies, which will occupy us for the remainder of the manuscript. We say that an isogeny ϕ is cyclic if $\ker \phi$ is a cyclic group.

Proposition 2.1.43. *Let $E, E' \in \mathscr{E}$, and let $\phi : E \to E'$ be a cyclic m-isogeny. Then $\widehat{\phi} : E' \to E$ is also a cyclic m-isogeny.*

Proof. We prove that if ϕ is not cyclic then $\widehat{\phi}$ is also not cyclic. Indeed, if ϕ is not cyclic then for some prime p, the p-torsion subgroup $E[p]$ of $E(\mathbb{Q}^{\mathrm{al}})$ is contained in $\ker\phi$. But $E[p]$ is the kernel of the p-multiplication map $[p] : P \mapsto pP$, so by Theorem 2.1.35 we may write $\phi = \phi' \circ [p]$ for some isogeny $\phi' : E \to E'$. Now by Theorem 2.1.30(b) and Theorem 2.1.30(e), we see $\widehat{\phi} = [p] \circ \widehat{\phi}'$, where we now interpret $[p] : P \mapsto pP$ as an endomorphism of E'. As $[p]$ is not cyclic, $\widehat{\phi}$ cannot be cyclic, and our claim follows. □

Proposition 2.1.44. *Let $E, E' \in \mathscr{E}$, and let $\phi : E \to E'$ be a cyclic m-isogeny with $m > 1$. Write $m = p_1 \dots p_r$, where $p_1, \dots, p_r$ are (not necessarily distinct) primes. Then we may write*

$$\phi = \phi_r \circ \phi_{r-1} \circ \cdots \circ \phi_1, \tag{2.1.45}$$

where each ϕ_i is a cyclic p_i-isogeny.

Proof. We proceed by induction on m. If $m = p$ is prime, we may take $\phi_1 = \phi$. Otherwise, write $m = pm'$, with p prime. As the p-torsion elements of $\ker\phi$ form a group of order p that is stabilized by $\mathrm{Gal}_{\mathbb{Q}}$, we may apply Theorem 2.1.35 and Theorem 2.1.36 to write $\phi = \phi' \circ \phi_1$, where ϕ_1 is a cyclic p-isogeny and ϕ' is a cyclic m'-isogeny. By induction hypothesis, our claim follows. □

Proposition 2.1.46. *Let $E, E', E'' \in \mathscr{E}$, and let $\phi : E \to E'$ and $\psi : E' \to E''$ be cyclic p-isogenies (over $\mathbb{Q}$) for a given prime p. Then exactly one of the following conditions holds:*

- *the composition $\psi \circ \phi$ is a cyclic p^2-isogeny;*
- *$E = E''$, ψ and ϕ are dual isogenies up to sign, and $\psi \circ \phi$ is multiplication by $\pm p$ in E.*

Proof. The kernel of $\psi \circ \phi$ in $E(\mathbb{Q}^{\mathrm{al}})$ is an abelian group of order 25, and thus either isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In the former case, $\psi \circ \phi$ is cyclic by definition. In the latter case, $\psi \circ \phi$ has the same kernel as multiplication by p, and so is the same map up to sign and isomorphism. But $\mathscr{E}$ contains only one elliptic curve from each $\mathbb{Q}$-isomorphism class, so $E = E''$, and ψ and ϕ are dual isogenies up to sign. □

Proposition 2.1.47. *Let $E, E', E'' \in \mathscr{E}$, let $\phi : E \to E'$ be a cyclic m-isogeny (over $\mathbb{Q}$), and let $\psi : E' \to E''$ be cyclic n-isogenies (over $\mathbb{Q}$). If $\gcd(m, n) = 1$, then $\psi \circ \phi$ is a cyclic mn-isogeny.*

Proof. The kernel of $\psi \circ \phi$ in $E(\mathbb{Q}^{\mathrm{al}})$ is an abelian group of order mn which contains both $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. If $\gcd(m, n) = 1$, then this kernel is necessarily $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$, which is cyclic, and our claim follows. □

We have proven some interesting trivia about cyclic isogenies, but a larger question looms: for what $m \in \mathbb{Z}_{>0}$ do cyclic m-isogenies exist? Building on earlier work of Ogg [47, 48], Mazur [44] reduced this problem to the assertion that $Y_0(m)(\mathbb{Q}) = \emptyset$ for $m \in \{39, 65, 91, 125, 169\}$, and Kenku verified this assertion [34, 35, 36, 37].

Theorem 2.1.48 ([38, Theorem 1], Mazur's theorem on isogenies)**.** *Let $m \in \mathbb{Z}_{>0}$. The following are equivalent:*

- *There exist (infinitely many) elliptic curves $E, E'/\mathbb{Q}$ with a cyclic m-isogeny $\phi : E \to E'$;*
- *$m \in \{1, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}$.*

In [14], Chiloyan and Lozano-Robledo give a precise description of all possible interrelationships of cyclic isogenies and underlying Mordell–Weil groups for elliptic curves $E/\mathbb{Q}$. Using Proposition 2.1.44, we extract the following result from [14].

Theorem 2.1.49. *Let $m \in \mathbb{Z}_{>0}$. The following are equivalent:*

(a) There exist elliptic curves $E, E_1, E_2 \in \mathscr{E}$ and cyclic m-isogenies $\phi_1 : E \to E_1$ and $\phi_2 : E \to E_2$ with distinct kernels;

(b) $m \in \{2, 3, 4, 5, 6, 8, 12, 16\}$.

Proof. By Proposition 2.1.44, we can understand cyclic m-isogenies as compositions of cyclic p-isogenies. If m is not of the form $2^u \cdot 3^v \cdot 5^w$, then [14, Theorem 4.3] precludes the existence of cyclic m-isogenies $\phi_1 : E \to E_1$ and $\phi_2 : E \to E_2$ with distinct kernels (see also [38, Theorem 2]). By Theorem 2.1.48, we may restrict our attention to $m \in \{2, 3, 4, 5, 6, 8, 9, 10, 12, 16, 18, 24, 25, 27\}$.

Let $m \in \{2, 4, 8, 16\}$. In these cases, (a) is implied by the isogeny graph $T8$ [14, page 4]. Indeed, by taking compositions of cyclic 2-isogenies, we obtain distinct isogenies of order $2, 4, 8, 16$. These compositions are necessarily cyclic, as otherwise some of the elliptic curves pictured would be isomorphic over $\mathbb{Q}$.

Let $m = 3$. In this case, (a) follows by inspecting the isogeny graph $L3(9)$ [14, page 4].

Let $m = 5$. In this case, (a) follows by inspecting the isogeny graph $L3(25)$ [14, page 4].

Let $m \in \{6, 12\}$. In these cases, (a) follows by inspecting the isogeny graph S [14, page 6].

Let $m = 9, 27$. In these cases, (a) is impossible because we cannot compose two 3-isogenies in two different ways starting from the same node.

Let $m = 10$. In this case, every cyclic 10-isogeny arises from the isogeny graph $R_4(10)$ [14, page 5]. By Proposition 2.1.44, the 10-isogeny we obtain by composing a 2-isogeny with a 5-isogeny can also be factored as a 5-isogeny composed with a 2-isogeny, so going around the rectangle in either direction must yield the same 10-isogeny. Thus (a) is precluded in this case.

Let $m = 18$. In this case, every 18-isogeny arises from the isogeny graph S or the isogeny graph $R6$ [14, page 5-6]. But we obtain two distinct 18-isogenies starting from a single node, we find that at least one of them factors as multiplication by 3 composed with a 2-isogeny.

Let $m = 24$. In this case, (a) is impossible by Theorem 2.1.48.

Let $m = 25$. In this case, (a) is precluded by the absence of any isogeny graphs with more than two 5-isogenies. □

Corollary 2.1.50. *Let*

$$m \in \{1, 7, 9, 10, 11, 13, 14, 15, 17, 18, 19, 21, 25, 27, 37, 43, 67, 163\}\,. \tag{2.1.51}$$

For all $X > 0$, we have

$$\widetilde{N}_m^{\mathrm{tw}}(X) = N_m^{\mathrm{tw}}(X), \textit{ and } \widetilde{N}_m(X) = N_m(X). \tag{2.1.52}$$

Proof. Immediate from Theorem 2.1.49. □

For $m \in \{2, 3, 4, 5, 6, 8, 12, 16, 18\}$, see Theorem 3.2.28 and Lemma 7.2.23.

Section 2.2

Counting elliptic curves: a brief history

In this section, we briefly recount the history of arithmetic statistics of elliptic curves. We place special emphasis on how one can define the size of an elliptic curve, and on discussing the asymptotics of elliptic curves with level structure (specifically, the asymptotics of elliptic curves with a given torsion group or a cyclic m-isogeny for particular m).

What is the size of an elliptic curve?

Mathematicians have long been curious about the statistical behavior of families of elliptic curves. Intuitively natural questions abound. What is the average rank of an elliptic curve over $\mathbb{Q}$ [3]? What proportion of elliptic curves over $\mathbb{Q}$ have trivial torsion [28]? In order to make sense of these and similar questions, mathematicians needed to endow elliptic curves with a notion of size.

One natural notion is the (absolute value of the) discriminant $\Delta(E)$ of an elliptic curve E (2.1.7). The discriminant $\Delta(E)$ is a nonzero integer, and it is divisible precisely by the primes for which $E(\mathbb{F}_p)$ is singular. Guided by the intuition that for reasonably chosen regions $\mathcal{R} \subseteq \mathbb{R}^2$, we should expect $\#\left(\mathcal{R} \cap \mathbb{Z}^2\right) \sim \mathrm{Area}(\mathcal{R})$ (see Theorem 3.3.2), Brumer and McGuinness conjectured [11, section 5] that

$$\#\left\{E \in \mathscr{E} : |\Delta(E)| \leq X\right\} \sim \frac{\alpha_\Delta}{\zeta(10)} X^{5/6}, \tag{2.2.1}$$

where

$$\alpha_\Delta := \frac{3+\sqrt{3}}{10} \int_1^\infty \frac{\mathrm{d}u}{\sqrt{u^3-1}} = \frac{2\sqrt{\pi}\left(3+\sqrt{3}\right)\Gamma\left(7/6\right)}{10\Gamma\left(2/3\right)} = 2.428\,650\,6\ldots. \tag{2.2.2}$$

Elliptic curves have a second invariant, the conductor $\mathrm{cond}(E)$ of E. Like the discriminant $\Delta(E)$, the conductor $\mathrm{cond}(E)$ is a nonzero integer, and it is divisible precisely by the primes for which $E(\mathbb{F}_p)$ is singular. For such p, the conductor conveys more about the singularities of $E(\mathbb{F}_p)$ than the discriminant does. In [12], Brumer and Silverman proved coarse bounds for the number of elliptic curves with given (and hence with bounded) conductor. In [67], Watkins built on [11], re-establishing the heuristic (2.2.1), and making several other heuristic claims. Notably, Watkins conjectured [67, Heuristic 4.1] that for an explicit $\alpha_{\mathrm{cond}} > 0$ we have

$$\#\left\{E \in \mathscr{E} : \mathrm{cond}(E) \leq X\right\} \sim \frac{\alpha_{\mathrm{cond}}}{\zeta(10)} X^{5/6}. \tag{2.2.3}$$

In [22, 23], Faltings introduced a third invariant for an elliptic curve E (or more generally, of an abelian variety A), which we now refer to as the Faltings height $\mathrm{ht}_F(E)$ of E. The Faltings height of an elliptic curve also relates to its arithmetic properties, albeit in a subtler way than the discriminant or the conductor do. In 2016, Hortsch [59, Theorem 1.2] used a reformulation of the Faltings height for elliptic curves due to Silverman [60, Proposition 1.1] to prove that there is an explicit constant $\alpha_{\mathrm{ht}_F} > 0$ such that

$$\#\{E \in \mathscr{E} : \mathrm{ht}_F(E) \leq X\} = \frac{\alpha_{\mathrm{ht}_F}}{\zeta(10)} X^{5/6} + O(X^{1/2} \log^3 X), \tag{2.2.4}$$

where

$$\alpha_{\mathrm{ht}_F} \approx 349\,068 \tag{2.2.5}$$

is given by an explicit integral.

The naïve height is another natural notion of size for an elliptic curve. For $E \in \mathscr{E}$ with Weierstrass equation as in (1.1.1) or (2.1.4), we define

$$\mathrm{ht}(E) := \max(4\,|A|^3\,, 27\,|B|^2). \tag{2.2.6}$$

This notion of size is much easier to study and bound than the discriminant, conductor, or Faltings height. Unlike the discriminant, the naïve height cannot fall victim to drastic cancellation between $4A^3$ and $27B^2$. Unlike the conductor, the naïve height does not require an understanding of the behavior of the elliptic curve at primes of bad reduction. Unlike the Faltings height, the naïve height is an integer. One can easily derive the power-savings asymptotic

$$\#\{E \in \mathscr{E} : \mathrm{ht}(E) \leq X\} = \frac{\alpha_{\mathrm{ht}}}{\zeta(10)} X^{5/6} + O(X^{1/2}) \tag{2.2.7}$$

(see Theorem 2.3.1 below), where

$$\alpha_{\mathrm{ht}} := \frac{2^{4/3}}{3^{3/2}} = 0.484\,943\,838\ldots. \tag{2.2.8}$$

At least conjecturally, then, elliptic curves counted by naïve height grow at the same rate as elliptic curves counted by discriminant, conductor, and Faltings height. The naïve height naturally arises from the embedding the coordinates $(A : B)$ from (1.1.1) in $\mathbb{P}(4,6)(\mathbb{Q})$

(see Remark 3.1.17). It is also natural to view the naïve height as arising from the "two components" of the discriminant. Throughout the remainder of this paper, when we write about the "height" of an elliptic curve, we refer *only* to its naïve height, *not* its Faltings height.

In 1992, Brumer showed that the generalized Birch–Swinnerton-Dyer conjecture and Riemann hypothesis together imply that the average rank of the elliptic curves in $\mathscr{E}$, ordered by height, is at most 2.3 [10]. Under the same hypotheses, Heath-Brown improved this bound from 2.3 to 2 [30], and Young improved it to $25/14 = 1.785\,714\ldots$ [70]. In 2010, Bhargava and Shankar proved unconditionally that the average rank of elliptic curves over $\mathbb{Q}$, ordered by height, is at most $3/2 = 1.5$ [5].

Remark 2.2.9. Some authors (notably, Duke [20] and Harron and Snowden [28]) define the naïve height of an elliptic curve $E \in \mathscr{E}$ to be

$$\max(|A|^3, |B|^2). \tag{2.2.10}$$

We follow [5] in using (2.2.6), but our results would all go through without issue if we used (2.2.10). Only the coefficients, *not the exponents*, in our asymptotics would be changed.

Since then, numerous authors have studied elliptic curves ordered by the naïve height [7, 9, 28, 51, 53, 55]. Throughout the remainder of this paper, we concentrate on elliptic curves counted by height, and neglect the interesting parallel questions about how elliptic curves with a cyclic m-isogeny would look counted by discriminant, or conductor, or Faltings height.

Counting elliptic curves with torsion by height

In 2013, Harron and Snowden [28] studied the arithmetic statistics of elliptic curves with a given torsion group (see also previous work of Duke [20] and Grant [27]). They showed that for each finite abelian group T given by Mazur's theorem on torsion (Theorem 2.1.22), there is an explicit rational number $d(T)$ such that

$$\#\{E \in \mathscr{E} : E(\mathbb{Q})_{\mathrm{tors}} \simeq T,\ \mathrm{ht}(E) \leq X\} \asymp X^{1/d(T)}. \tag{2.2.11}$$

Moreover, for $T \in \{0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}\}$, they gave an asymptotic for the left-hand side of (2.2.11) with a power-saving error term [28, Theorem 5.5]. For $T \in \{0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}\}$, their argument proceeds in three steps: first, they establish parameterizations for those elliptic curves

$$E : y^2 = x^3 + Ax + B \tag{2.2.12}$$

equipped with each of these torsion groups, then they use the Principle of Lipschitz (Theorem 3.3.2) and some elementary sieving to estimate the number of elliptic curves in these families, and finally they show that the discrepancy between elliptic curves with torsion containing T and torsion exactly T is relatively small. For larger $T \neq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, they use the theory of modular curves to establish a universal elliptic curve over an open subset of the affine line $\mathbb{A}^1$ equipped with a subgroup isomorphic to T; essentially equivalently, they found an elliptic surface

$$E_T : y^2 = x^3 + f_T(t)x + g_T(t) \tag{2.2.13}$$

over $\mathbb{P}^1$ for which evaluation at $t \in \mathbb{P}^1(\mathbb{Q})$ (away from a finite set) yields all elliptic curves with torsion containing T. Once they had this universal elliptic curve, they used elementary analytic and algebraic arguments to obtain upper and lower bounds for the number of elliptic curves with bounded height occurring in this family. The case $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ requires its own argument.

In 2022, Cullinan, Kenney, and Voight [16] improved on Harron and Snowden's work by attaining asymptotics for the left-hand side of (2.2.11) with power-saving error for all torsion groups T given by Mazur's theorem on torsion. Moreover, they provided satisfactory interpretations of the exponent of X and the constants appearing in these asymptotics. Their work was in fact more general, and gave an asymptotic with power-saving asymptotic for counts of elliptic curves for which the Galois representation on the N-torsion subgroup $E[N]$ of $E(\mathbb{Q}^{\mathrm{al}})$ is isomorphic to a fixed group G, so long as the associated modular group Γ_G is torsion-free, and the associated modular curve X_G has genus 0 and no irregular cusps [16, Theorem 1.3.3]. Their proof extends the arguments given in Harron and Snowden: after establishing a universal elliptic curve, applying the Principle of Lipschitz, and doing some elementary sieving, they also needed to address the discrepancy between counting elliptic curves equipped with level structure, and counting the elliptic curves themselves. There is a negligible contribution here from curves with Galois representation properly contained within G, and an integer factor arising from the index of G inside its normalizer.

Counting elliptic curves with a cyclic isogenies by height

In this subsection, we highlight several known results regarding counts of elliptic curves with a cyclic isogeny.

Just as it is natural to study asymptotics for elliptic curves with a given torsion group, as in Theorem 2.1.22, it is natural to study asymptotics for elliptic curves admitting a cyclic m-isogeny, as in Theorem 2.1.48. Equivalently, we wish to study elliptic curves E with a cyclic subgroup of $E(\mathbb{Q}^{\mathrm{al}})$ with size m that is stable under $\mathrm{Gal}_{\mathbb{Q}}$ (Theorem 2.1.36).

Recall the definitions of $\widetilde{N}_m(X)$ and $N_m(X)$ (1.1.4). We note in passing that the map $(E, \phi) \mapsto E$ defines a surjection

$$\begin{tikzcd}
\{(E,\phi) : E \in \mathscr{E}_{\leq X} \text{ and } \phi : E \to E' \text{ an unsigned cyclic } m\text{-isogeny}\} \arrow[d, two heads] \\
\{E \in \mathscr{E}_{\leq X} : E \text{ admits a cyclic } m\text{-isogeny}\}
\end{tikzcd}$$

from the set that $\widetilde{N}_m^{\mathrm{tw}}(X)$ counts to the set that $N_m^{\mathrm{tw}}(X)$ counts.

We are interested in the asymptotics of $\widetilde{N}_m(X)$ and $N_m(X)$.

The cases $m = 1$ is well-known (Theorem 2.3.1). The case $m = 2$ is handled by Harron and Snowden's work (Theorem 2.3.4); indeed, if $E(\mathbb{Q}^{\mathrm{al}})$ has a cyclic subgroup of size 2 which is stabilized by $\mathrm{Gal}_{\mathbb{Q}}$, that subgroup is necessarily defined over $\mathbb{Q}$.

Counting elliptic curves with given torsion and counting elliptic curves with a cyclic m-isogeny are both examples of counting elliptic curves with level structure. However, elliptic curves with a cyclic m-isogeny have a feature that elliptic curves with torsion do not share. If two elliptic curves are twist equivalent, then one admits a cyclic m-isogeny if and only if the other does (Corollary 2.1.37). Therefore, we must count both the (noncuspidal) points on the modular curve $X_0(m)$ and their quadratic twists.

In 2019, Pizzo, Pomerance, and Voight [53] gave a power-saving asymptotic for $\widetilde{N}_3(X)$ and $N_3(X)$ (see Theorem 2.3.6 below). Pizzo, Pomerance, and Voight characterized elliptic curves with a cyclic 3-isogeny in terms of the factorization of the 3-division polynomial, rather than directly producing a universal elliptic curve with a cyclic 3-isogeny. They parameterize the elliptic curves (with $j(E) \neq 0$) that have a cyclic 3-isogeny in terms of a triple (u, v, w) of integers satisfying certain arithmetic conditions, then carefully summed over such triples using techniques from analytic number theory. In 2020, Pomerance and Schaefer [55] provided asymptotics for $N_4(X)$ and $\widetilde{N}_4(X)$, among other results. Both [53] and [55] used intricate analytic number-theoretic arguments (including a refinement of the Principle of Lipschitz by Huxley [32]) to improve their errors as far as feasible.

In 2020, building on the arguments outlined above, Boggess and Sankar provided at least an order of growth for $N_m(X)$ for $m \in \{2, 3, 4, 5, 6, 8, 9, 12, 16, 18\}$: these m, together with $m = 7, 10, 13, 25$, are precisely the integers m from Theorem 2.1.48 for which the associated modular curve $X_0(m)$ is of genus 0. Although they still use the Principle of Lipschitz, their approach is qualitatively different from those taken in [16, 28, 55, 53]. Boggess and Sankar leverage a modular curve $X_{1/2}(m)$, which is a degree 2 cover of $X_0(m)$; this modular curve lets them track the twists of the elliptic curves arising from $X_0(m)$, and thereby establish orders of growth for $m \in \{2, 3, 4, 5, 6, 8, 9, 12, 16, 18\}$. The ring of modular forms for $X_0(5)$ is especially difficult to handle, and they do so separately from the other m in their list. In 2022, the author and John Voight obtained asymptotics for $\widetilde{N}_7(X) = N_7(X)$ using the methods which we develop in this thesis [45].

Mathematicians are also interested in counting elliptic curves with a cyclic m-isogeny over number fields [9, 51] and even global fields [2, 50, 52]. In 2020, Bruin and Najman [9] gave an order of growth estimate for the number of elliptic curves over a number field K admitting a G-level structure whenever the associated modular curve X_G over K is isomorphic to a weighted projective line. In 2022, Phillips [51] gave an asymptotic for the number of elliptic curves over a number field K admitting a G-level structure under similar hypotheses. He recovered the asymptotics for $\widetilde{N}_m(X)$ for $m \in \{2, 4\}$, and gave the leading term for the asymptotics of $\widetilde{N}_m(X)$ for $m \in \{6, 8, 9, 12, 16, 18\}$, albeit without an explicit error term (power-saving or otherwise). In [52], he gave similar asymptotics for these m over well-behaved functions fields of characteristic greater than 3.

Section 2.3

Previous results for $m \leq 5$

In this section, we state the asymptotics of $\widetilde{N}_m(X)$ and $N_m(X)$ for $1 \leq m < 5$, and the order of growth for $\widetilde{N}_5(X)$ and $N_5(X)$. Combined with the findings in section 1.2, these furnish estimates for the number of elliptic curves with a cyclic m-isogeny for all $m \in \mathbb{Z}_{>0}$.

Here and throughout the remainder of the thesis, the notation $c \approx \ldots$ indicates that the estimate given for c is numerically supported, but does not have clear and well-bounded error.

The first theorem is folklore (but see [59, Theorem 2.1] for a nice treatment).

Theorem 2.3.1. *We have*

$$\widetilde{N}_1(X) = N_1(X) = \frac{2^{4/3}}{3^{3/2}\zeta(10)} X^{5/6} + O\left(X^{1/2}\right) \tag{2.3.2}$$

for $X \geq 1$.

Essentially the same argument yields the asymptotic

$$\widetilde{N}_1^{\mathrm{tw}}(X) = N_1^{\mathrm{tw}}(X) = \frac{2^{4/3}}{3^{3/2}\zeta(5)} X^{5/6} + O\left(X^{1/2}\right). \tag{2.3.3}$$

The equalities in Theorem 2.3.1 and (2.3.3) are exact, because no elliptic curve has more than one unsigned isomorphism over $\mathbb{Q}$.

Theorem 2.3.4. *There exists an effective computable constant* c_2 *such that*

$$\widetilde{N}_2(X), N_2(X) = c_2 X^{1/2} + O(X^{1/3}) \tag{2.3.5}$$

for $X \geq 1$.

Proof. Harron and Snowden prove the claim for $N_2(X)$ in [28, Theorem 5.5], and [28, Table 1] assures us that counting elliptic curves with distinct 2-isogenies separately can contribute at most $O(X^{1/3})$ more to this sum. □

Theorem 2.3.6 ([53, Theorem 1.3])**.** *There exist effective computable constants*

$$\begin{aligned} c_3 &= 0.107\,437\,255\,02\ldots \quad \textit{and} \\ c_3' &\approx 0.16 \end{aligned} \tag{2.3.7}$$

such that

$$\widetilde{N}_3(X), N_3(X) = \frac{2}{3^{3/2}\zeta(6)}X^{1/2} + c_3 X^{1/3}\log X + c_3' X^{1/3} + O(X^{7/24}) \tag{2.3.8}$$

for $X \geq 1$.

Theorem 2.3.9 ([55, Theorem 4.2, Theorem 5.11])**.** *There exist effectively computable constants*

$$\begin{aligned} c_4 &= 0.957\,400\,377\,047\ldots, \\ \widetilde{c}_4' &= -1.742\,501\,704\,06\ldots, \ \textit{and} \\ c_4' &= -0.835\,735\,404\,05\ldots \end{aligned} \tag{2.3.10}$$

such that

$$\widetilde{N}_4(X) = 2c_4 X^{1/3} + \widetilde{c}_4' X^{1/6} + O(X^{21/200}) \tag{2.3.11}$$

and

$$N_4(X) = c_4 X^{1/3} + c_4' X^{1/6} + O(X^{21/200}) \tag{2.3.12}$$

for $X \geq 1$.

Theorem 2.3.13 ([7, Proposition 5.9])**.** *We have*

$$\widetilde{N}_5(X) \sim N_5(X) \asymp X^{1/6}\log^2 X \tag{2.3.14}$$

as $X \to \infty$.

For completeness, we also record the following folklore theorem in our notation (this result was known to Kenku [38] and Mazur [44]).

Theorem 2.3.15 (Theorem 8.1.7)**.** *For X sufficiently large, we have the following identities:*

$$\begin{aligned}&N_{11}^{\mathrm{tw}}(X)=3,\ N_{14}^{\mathrm{tw}}(X)=2,\ N_{15}^{\mathrm{tw}}(X)=4,\ N_{17}^{\mathrm{tw}}(X)=2,\ N_{19}^{\mathrm{tw}}(X)=1, N_{21}^{\mathrm{tw}}(X)=4,\\ &N_{27}^{\mathrm{tw}}(X)=1,\ N_{37}^{\mathrm{tw}}(X)=2,\ N_{43}^{\mathrm{tw}}(X)=1,\ N_{67}^{\mathrm{tw}}(X)=1,\ N_{163}^{\mathrm{tw}}(X)=1.\end{aligned} \tag{2.3.16}$$

For $m \notin \{1,\dots,19,21,25,27,37,43,67,163\}$, we have

$$\widetilde{N}_m^{\mathrm{tw}}(X)=N_m^{\mathrm{tw}}(X)=0 \tag{2.3.17}$$

identically by Mazur's theorem on isogenies (Theorem 2.1.48).

Chapter 3

Technical preliminaries

In this chapter, we recall and build upon a number of results from the literature [6, 16, 17, 22, 23, 31, 33, 40, 42, 45, 51, 55, 58, 64, 66, 69] which will be important in proving our main theorems (Theorem 1.2.3, Theorem 1.2.6, Theorem 1.2.13, Theorem 2.3.15).

In section 3.1, we examine the naïve height and the twist height of an elliptic curve more carefully, and we establish additional notation for later use in this thesis. In section 3.2, for

$$m \in \{4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}, \tag{3.0.1}$$

we give a universal elliptic curve

$$y^2 = x^3 + f_m(t)x + g_m(t) \tag{3.0.2}$$

over an open subset of the affine line $\mathbb{A}^1$ equipped with a cyclic m-isogeny. For each proper divisor n of m, we also report the modular curve parameterizing elliptic curves equipped with a pair of cyclic m-isogenies whose kernels have intersection of order n, as long as this moduler curve is defined over $\mathbb{Q}$; when this modular curve is of genus 0 but is not $X_0(m)$, we give a universal elliptic curve

$$y^2 = x^3 + f_{m,n}(t)x + g_{m,n}(t) \tag{3.0.3}$$

over an open subset of the affine line $\mathbb{A}^1$ equipped with such pairs of isogenies. In section 3.3 we recall the Principle of Lipschitz, and use it to obtain counts of Weierstrass models arising from the universal elliptic curves given by (3.0.2). In section 3.4 we recall a number of results from analytic number theory which we will require later in the thesis. In section 3.5, we outline the approach we take in resolving this problem. The material in this section mirrors and abstracts material from [45, §2.1, §4.1, §5.1].

Impatient readers may restrict their attention to section 3.1, section 3.2, and section 3.5, and refer back to the intervening sections of this chapter as needed.

Section 3.1

Height, minimality, and defect

In this section, we define the height and twist height of an elliptic curve over $\mathbb{Q}$ without reference to minimal models. We also define the minimality defect and twist minimality defect of a Weierstrass equation, which measure the discrepancy between the size of the coefficients of a given Weierstrass model and the height or twist height of the associated elliptic curve.

Let E be an elliptic curve over $\mathbb{Q}$, and let

$$y^2 = x^3 + Ax + B \tag{3.1.1}$$

be a Weierstrass model for E with $A, B \in \mathbb{Z}$. Unlike in section 1.2 and section 2.1, we do not assume $E \in \mathscr{E}$; that is, we do not assume that this model is minimal. Define

$$H(A,B) := \max(\left|4A^3\right|, \left|27B^2\right|). \tag{3.1.2}$$

Note that $H(A,B)$ depends on our choice of model, and not only on our choice of elliptic curve E.

Example 3.1.3. *The Weierstrass equations*

$$y^2 = x^3 + 4x + 8 \tag{3.1.4}$$

and

$$y^2 = x^3 + 324x + 5832 \tag{3.1.5}$$

are models for the same elliptic curve over $\mathbb{Q}$. *However,* $H(4,8) = 108$ *while* $H(324,1458) = 918\,330\,048$.

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 (3.1.1). Explicitly, we have

$$\mathrm{md}(A,B) := \prod_{\ell} \ell^{v_\ell}, \quad \text{where } v_\ell := \lfloor \min(\mathrm{ord}_\ell(A)/4, \mathrm{ord}_\ell(B)/6) \rfloor, \tag{3.1.6}$$

with the product over all primes ℓ. We now redefine the (naïve) height of E to be

$$\mathrm{ht}(E) = \mathrm{ht}(A,B) := \frac{H(A,B)}{\mathrm{md}(A,B)^{12}}, \tag{3.1.7}$$

which is well-defined up to $\mathbb{Q}$-isomorphism. Indeed, if we write $d = \mathrm{md}(A,B)$, the integral Weierstrass equation

$$y^2 = x^3 + (A/d^4)x + (B/d^6) \tag{3.1.8}$$

has minimality defect 1, and is the unique model for E such that for every prime ℓ we have $\ell^4 \nmid A$ or $\ell^6 \nmid B$. Our new definition (3.1.7) for the naïve height thus agrees with the definition (1.1.2) we gave in the introduction.

We may similarly consider all integral Weierstrass equations which define an elliptic curve that is twist equivalent to E—these are the quadratic twists of E (defined over $\mathbb{Q}$). 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 the model (3.1.1), denoted $\operatorname{tmd}(A, B)$. Explicitly, we have

$$\operatorname{tmd}(A,B) := \prod_{\ell} \ell^{v_\ell}, \quad \text{where } v_\ell := \lfloor \min(\operatorname{ord}_\ell(A)/2, \operatorname{ord}_\ell(B)/3) \rfloor, \tag{3.1.9}$$

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

$$\operatorname{twht}(E) = \operatorname{twht}(A,B) := \frac{H(A,B)}{\operatorname{tmd}(A,B)^6}, \tag{3.1.10}$$

which is well-defined on the $\mathbb{Q}$-isomorphism class of E, and even up to $\mathbb{Q}^{\mathrm{al}}$-isomorphism when $j(E) \neq 0, 1728$. Indeed, if we write $e = \operatorname{tmd}(A, B)$, the integral Weierstrass equations

$$y^2 = x^3 + (A/e^4)x \pm (B/e^3) \tag{3.1.11}$$

have twist minimality defect 1, and are the only models for E such that for every prime ℓ we have $\ell^2 \nmid A$ or $\ell^3 \nmid B$. We refer to Weierstrass models with twist minimality defect 1 as twist minimal: just as the height of $E/\mathbb{Q}$ is the height of its minimal model, the twist height of $E/\mathbb{Q}$ is the twist height of its twist minimal model.

Example 3.1.12. *The Weierstrass equations* (3.1.4) *and* (3.1.5) *given in* (3.1.3) *have naïve height* 1728 *and twist height* 27. *The equation* (3.1.4) *is a minimal model for the elliptic curve described by these equations, and the two twist minimal models for this elliptic curve* *are as follows:*

$$y^2 = x^3 + x \pm 1. \tag{3.1.13}$$

Recall from section 1.1 that $\mathscr{E}^{\mathrm{tw}}$ consists of the elliptic curves in $\mathscr{E}$ up to twist equivalence. By the remarks in the previous paragraph, the twist minimal models

$$E : y^2 = x^3 + Ax + B \tag{3.1.14}$$

for which $B > 0$ or $(A, B) = (1, 0)$ provide a collection of representatives for $\mathscr{E}^{\mathrm{tw}}$, and we identify $\mathscr{E}^{\mathrm{tw}}$ with this set of Weierstrass models for the remainder of the thesis.

With this convention established, we make an elementary observation. We have

$$\mathscr{E} = \left\{ E^{(c)} : E \in \mathscr{E}^{\mathrm{tw}} \text{ and } c \in \mathbb{Z} \text{ squarefree} \right\}. \tag{3.1.15}$$

Here, as in (1.1.6), $E^{(c)}$ is the quadratic twist of E by c. Note that for $E^{(c)}$ as in (3.1.15), we have

$$\mathrm{ht}(E^{(c)}) = c^6\, \mathrm{ht}(E) = c^6\, \mathrm{twht}(E). \tag{3.1.16}$$

Remark 3.1.17. 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 Weierstrass model (3.1.1), 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 [9, §2, §7] and Phillips [51, §2.2]. Similarly, the height of the twist minimal model is given by the height of the point $(A : B) \in \mathbb{P}(2,3)_{\mathbb{Q}}$ 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).

We remark in passing that for $E/\mathbb{Q}$ and $c, c' \in \mathbb{Q}^{\times}$, we have

$$\left(E^{(c)}\right)^{(c')} = E^{(cc')}, \tag{3.1.18}$$

and thus

$$\left(E^{(c)}\right)^{(c)} = E^{(c^2)} = E, \tag{3.1.19}$$

up to $\mathbb{Q}$-isomorphism.

Section 3.2 Parameterizing elliptic curves equipped with a cyclic m-isogeny

In this section, we use the theory of modular curves to parameterize all elliptic curves with a cyclic m-isogeny when $X_0(m)$ is of genus 0 and $m > 3$. We also produce modular curves parameterizing elliptic curves equipped with pairs of distinct cyclic m-isogenies, whenever such pairs exist over $\mathbb{Q}$.

We gather the necessary input from the theory of modular curves. The modular curve $Y_0(m) \subseteq X_0(m)$, defined over $\mathbb{Q}$, parameterizes pairs (E, ϕ) of elliptic curves E equipped with a cyclic m-isogeny ϕ up to isomorphism, or equivalently, a cyclic subgroup of order m stable under the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$ (see Theorem 2.1.36). For $m \in \{4, 5, 6, 8, 9, 10, 12, 13, 16, 18, 25\}$, we observe that $Y_0(m) \subseteq X_0(m)$ is affine open in $\mathbb{P}^1$. In these cases, the objects of interest are parameterized by a coordinate t in this affine open subset.

Lemma 3.2.1. *Let $m \in \{4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$. Then the set of elliptic curves*

E over $\mathbb{Q}$ that admit a cyclic m-isogeny (defined over $\mathbb{Q}$) are precisely those of the form

$$E_m^{(c)}(t)\colon y^2 = x^3 + c^2 f_m(t)x + c^3 g_m(t) \tag{3.2.2}$$

for some $c \in \mathbb{Q}^\times$ and $t \in \mathbb{Q}$ with $t \notin \mathscr{C}_m$, where $\mathscr{C}_m \subseteq \mathbb{P}^1(\mathbb{Q})$ consists of those elements $t \in \mathbb{P}^1(\mathbb{Q})$ for which the Weierstrass equation (3.2.2) is singular. Moreover, the set

$$\{(c,t) \in \mathbb{Z} \times \mathbb{Q} : c \text{ squarefree},\ t \notin \mathscr{C}_m\} \tag{3.2.3}$$

is in bijection with the set of elliptic curves equipped with an unsigned cyclic m-isogeny via the map $(c,t) \mapsto E_m^{(c)}(t)$.

The polynomials $f_m(t)$ are given in Table 3.2.11, the polynomials $g_m(t)$ are given in Table 3.2.12, and $\mathscr{C}_m$ is given in Table 3.2.13.

Proof. The proof follows for elliptic curves E with $j(E) \neq 0, 1728$ by routine calculations with q-expansions for modular forms on the group $\Gamma_0(m) \subseteq \mathrm{SL}_2(\mathbb{Z})$, with the cusps at $t \in \mathscr{C}_m \subseteq \mathbb{P}^1(\mathbb{Q})$. For instance, writing the j-function in terms of the Hauptmodul for $X_0(m)$ yields a parameterization

$$E_m(t) : y^2 = x^3 + f_m(t)x + g_m(t), \tag{3.2.4}$$

for elliptic curves equipped with an unsigned cyclic m-isogeny, up to quadratic twist (see also [16, Proposition 3.3.16]). Taking quadratic twists of (3.2.4), we obtain (3.2.2).

We now turn our attention to the circumstance that $j(E) = 0, 1728$. By inspection, for $E_m(t)$ as in (3.2.4), $j(E_m(t)) = 0$ if and only if $(m,t) \in \{(6,1),(9,0)\}$, and $j(E_m(t)) = 1728$ if and only if $(m,t) = (4,0)$. In these cases, we must investigate the sextic or quartic twists of $E_m(t)$, respectively (Corollary 2.1.12).

First let $m = 6$ and $t = 1$. We compute $g_6(1) = -64$, which after a quadratic twist yields the elliptic curve

$$E : y^2 = x^3 + 1. \tag{3.2.5}$$

Now let

$$E' : y^2 = x^3 \pm c \tag{3.2.6}$$

be a sextic twist of E. If E has a rational 6-isogeny, then *a fortiori* it also has a rational 2-torsion point, so $c^{1/3} \in \mathbb{Q}$. But this implies E' is a quadratic twist of E, as desired.

Now let $m = 9$ and $t = 0$. We compute $g_9(0) = -16$, which after a quadratic twist yields the elliptic curve

$$E : y^2 = x^3 - 2. \tag{3.2.7}$$

Let $\Phi \subseteq E(\mathbb{Q}^{\mathrm{al}})$ be the kernel of the 9-isogeny on E. Inspecting the division polynomial for E, we readily compute the polynomial

$$\prod_{(x,\pm y) \in \Phi} (t - x) = t(t^3 + 6t^2 - 8). \tag{3.2.8}$$

For $u \in (\mathbb{Q}^{\mathrm{al}})^\times$, if $(x, y) \mapsto (u^2x, u^3y)$ is a (not necessarily quadratic) twist of E which sends Φ to another group stabilized by $\mathrm{Gal}_{\mathbb{Q}}$, then

$$t(t^3 + 6u^2t^2 - 8u^6) \tag{3.2.9}$$

is a rational polynomial. In particular, $u^2 \in \mathbb{Q}^\times$, so $(x, y) \mapsto (u^2x, u^3y)$ is a quadratic twist.

Finally, let $m = 4$ and $t = 0$. In this case, we find $f_4(0) = 9$, which after a quadratic twist yields the elliptic curve

$$E : y^2 = x^3 + x. \tag{3.2.10}$$

Note that this elliptic curve has two distinct 4-isogenies over $\mathbb{Q}$, generated by the points $(1, 2^{1/2})$ and $(-1, (-2)^{1/2})$ respectively. If $(x, y) \mapsto (u^2x, u^3y)$ is a twist of E which preserves either of these 4-isogenies, then $\pm u^2 \in \mathbb{Q}^\times$, so again we have a quadratic twist, as desired. $\square$

We highlight that the point $t = 0$ encodes *two distinct* cyclic 4-isogenies over $\mathbb{Q}$. It turns out that elliptic curves equipped with cyclic 4-isogeny always come in pairs (see Corollary 3.2.36 and the paragraphs immediately preceding it), but this is the only case where this pair is indexed by one argument t instead of two arguments t_1 and t_2.

Of course we can ignore the factor c in Lemma 3.2.1 for elliptic curves over $\mathbb{Q}$ up to quadratic twist.

For $m \in \{4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$, we define $d\left(m\right) := \deg g_m(t)$, and note that $\deg f_m(t) = 2d\left(m\right)/3$.

m	$f_m(t)$
4	$-3(t^2+6t-3)$
5	$-3(t^2+1)\cdot(t^2+114t+124)$
6	$-3(t-1)\cdot(t^3+33t^2-117t+99)$
7	$-3(t^2+t+7)\cdot(t^2-231t+735)$
8	$-3(t^4+24t^3-88t^2+96t-32)$
9	$-3t(t^3-24t^2-24t-8)$
10	$-3(t^2+1)\cdot(t^6-118t^5+360t^4-240t^3+240t^2-8t+4)$
12	$-3(t^2-3)\cdot(t^6-108t^5-657t^4-1512t^3-1701t^2-972t-243)$
13	$-3(t^2+t+7)\cdot(t^2+4)\cdot(t^4-235t^3+1211t^2-1660t+6256)$
16	$-3(t^8+48t^7-432t^6+1536t^5-2896t^4+3072t^3-1728t^2+384t+16)$
18	$-3(t^3+6t^2+4)\cdot(t^9+234t^8+756t^7+2172t^6$ $+1872t^5+3024t^4+48t^3+3744t^2+64)$
25	$-3(t^2+4)\cdot(t^{10}+240t^9+2170t^8+8880t^7+34835t^6+83748t^5$ $+206210t^4+313380t^3+503545t^2+424740t+375376)$

Table 3.2.11: $f_m(t)$ for m with $X_0(m)$ of genus 0

m	$g_m(t)$
4	$2t \cdot (t^2 - 18t + 9)$
5	$2(t^2 + 1)^2(t^2 - 261t - 2501)$
6	$2(t^2 - 3)(t^4 - 96t^3 + 426t^2 - 648t + 333)$
7	$2(t^2 + t + 7)(t^4 + 518t^3 - 11025t^2 + 6174t - 64827)$
8	$2(t^2 - 2)(t^4 - 72t^3 + 248t^2 - 288t + 112)$
9	$2(t^6 + 60t^5 - 12t^4 - 124t^3 - 120t^2 - 48t - 8)$
10	$2(t^2 + 1)^2(t^2 - 2t + 2)(t^2 - 11t - 1$ $(t^4 + 268^3 - 66t^2 + 52t - 4)$
12	$2(t^4 - 6t^3 - 36t^2 - 54t - 27)(t^8 + 276t^7 + 1836t^6$ $+4860t^5 + 6750t^4 + 6156t^3 + 4860t^2 + 2916t + 729)$
13	$2(t^2 + t + 7)(t^2 + 4)^2(t^6 + 512t^5 - 13073t^4$ $+34860t^3 - 157099t^2 + 211330t - 655108)$
16	$2(t^4 - 12t^2 + 24t - 14)(t^8 - 144t^7 + 1200t^6 - 4416t^5$ $+9152t^4 - 11520t^3 + 8832t^2 - 3840t + 736)$
18	$2(t^6 + 24t^5 + 24t^4 + 92t^3 - 48t^2 + 96t - 8)(t^{12} - 528t^{11}$ $-3984t^{10} - 14792t^9 - 27936t^8 - 42624t^7 - 37632t^6$ $-52992t^5 - 25344t^4 - 43520t^3 - 6144t^2 - 6144t - 512)$
25	$2(t^2 + 4)^2 \cdot (t^4 + 6t^3 + 21t^2 + 36t + 61)(t^{10} - 510t^9$ $-13580t^8 - 36870t^7 - 190915t^6 - 393252t^5 - 1068040t^4$ $-1508370t^3 - 2581955t^2 - 2087010t - 1885124)$

Table 3.2.12: $g_m(t)$ for m with $X_0(m)$ of genus 0

For $m \in \{4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$, we record $d\,(m)$ and $\mathscr{C}_m$ in the following table. For later use, we also record the resultant $\mathrm{Res}(f_m(t), g_m(t))$ of $f_m(t)$ and $g_m(t)$.

m	$d\,(m)$	$\mathscr{C}_m$	$\operatorname{Res}(f_m(t), g_m(t))$
4	3	$\{1/2, 1, \infty\}$	$2^6 \cdot 3^6$
5	6	$\{11/2, \infty\}$	0
6	6	$\{3/2, 5/3, 3, \infty\}$	$-2^{24} \cdot 3^{15}$
7	6	$\{-7, \infty\}$	0
8	6	$\{1, 3/2, 2, \infty\}$	$2^{24} \cdot 3^{12}$
9	6	$\{-1, \infty\}$	$-2^{16} \cdot 3^{15}$
10	12	$\{-2, 0, 1/2, \infty\}$	0
12	12	$\{-3, -2, -3/2, -1, 0, \infty\}$	$2^{48} \cdot 3^{78}$
13	12	$\{-3, \infty\}$	0
16	12	$\{1, 2, \infty\}$	$2^{48} \cdot 3^{24}$
18	18	$\{-1, 0, 2, \infty\}$	$-2^{144} \cdot 3^{189}$
25	18	$\{1, \infty\}$	0

Table 3.2.13: Miscellaneous data about the model

$$E_m(t) : y^2 = x^3 + f_m(t)x + g_m(t)$$

We emphasize that $f_m(t)$ and $g_m(t)$ are only unique up to fractional linear transformation, and that such fractional linear transformations will also act on $\mathscr{C}_m$. Of course, $\#\mathscr{C}_m$ is independent of our choice of model

$$E_m(t) : y^2 = x^3 + f_m(t)x + g_m(t). \tag{3.2.14}$$

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

$$\begin{aligned} A_m(a, b) &:= b^{2d(m)/3} f_m(a/b), \\ B_m(a, b) &:= b^{d(m)} g_m(a/b). \end{aligned} \tag{3.2.15}$$

For

$$m \in \{4,5,6,7,8,9,10,12,13,16,18,25\}\,, \tag{3.2.16}$$

the set $\mathscr{C}_m \subseteq \mathbb{P}^1(\mathbb{Q})$ described in Lemma 3.2.1 consists of those elements $(a:b) \in \mathbb{P}^1(\mathbb{Q})$ for which

$$E_m(a,b) : y^2 = x^3 + A_m(a,b)x + B_m(a,b) \tag{3.2.17}$$

is singular. Thus

$$\mathscr{C}_m = \left\{(a:b) \in \mathbb{P}^1(\mathbb{Q}) : 4A_m(a,b)^3 + 27B(a,b)^2 = 0\right\}. \tag{3.2.18}$$

Definition 3.2.19. We say that a pair $(a,b) \in \mathbb{Z}^2$ is m-groomed if $\gcd(a,b) = 1$, $b > 0$, and $a/b \notin \mathscr{C}_m$.

Remark 3.2.20. It would be more technically accurate to define a pair $(a,b) \in \mathbb{Z}^2$ to be m-groomed if $\gcd(a,b) = 1$, $b > 0$ or $(a,b) = (1,0)$, and $a/b \notin \mathscr{C}_m$. However, Definition 3.2.19 is harmless because $\infty \in \mathscr{C}_m$ for all $m \in \{4,5,6,7,8,9,10,12,13,16,18,25\}$.

Thus Lemma 3.2.1 asserts that elliptic curves $E \in \mathscr{E}$ that admit a cyclic m-isogeny are precisely those with a model

$$y^2 = x^3 + \frac{c^2 A_m(a,b)}{d^4}x + \frac{c^3 B_m(a,b)}{d^6} \tag{3.2.21}$$

where (a,b) is m-groomed, $c \in \mathbb{Z}$ is squarefree, and $d = \operatorname{md}(c^2 A_7(a,b), c^3 B_7(a,b))$. For $m > 4$, the count $\widetilde{N}_m(X)$ can be computed as

$$\widetilde{N}_m(X) = \# \left\{ (a,b,c) \in \mathbb{Z}^3 : \begin{array}{c} (a,b)\ m\text{-groomed, } c \text{ squarefree, and} \\ \operatorname{ht}(c^2 A_m(a,b), c^3 B_m(a,b)) \leq X \end{array} \right\} \tag{3.2.22}$$

with the height defined as in (3.1.7).

Remark 3.2.23. It is not hard to adapt this asymptotic to estimate $\widetilde{N}_4(X)$. For $X > 0$ a real number, we let

$$S_2(X) := \# \{n \in \mathbb{Z}_{>0} : n \leq X,\ n \text{ a squarefree integer}\}, \tag{3.2.24}$$

so $S_2(X)$ is the number of squarefree positive integers less than or equal to X. When $m = 4$, we need only add $2S_2((X/4)^{1/6})$ to the right-hand side of (3.2.22) to account for the fact that there are two cyclic 4-isogenies associated to each triple of the form $(0, 1, c)$. However, Theorem 2.3.9 addresses the asymptotics of $\widetilde{N}_4(X)$ and $N_4(X)$ to our satisfaction, so we need not pursue this case further.

Similarly, but more simply, for $m \in \{4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$, the subset of $E \in \mathscr{E}^{\text{tw}}$ that admit a cyclic m-isogeny consists of models

$$y^2 = x^3 + \frac{A_m(a,b)}{e^2}x + \frac{|B_m(a,b)|}{e^3} \tag{3.2.25}$$

with (a, b) m-groomed and $e = \operatorname{tmd}(A_m(a, b), B_m(a, b))$ the twist minimality defect (3.1.6). Accordingly, for $m > 4$ we have

$$\widetilde{N}_m^{\text{tw}}(X) = \# \left\{ (a,b) \in \mathbb{Z}^2 : \begin{array}{l} (a,b) \ m\text{-groomed, and} \\ \operatorname{twht}(A_m(a,b), B_m(a,b)) \leq X \end{array} \right\}. \tag{3.2.26}$$

When $m = 4$, the count on the left and the count on the right can differ by at most 1.

Remark 3.2.27. Returning to Remark 3.1.17, we conclude that counting elliptic curves over $\mathbb{Q}$ equipped with a m-isogeny is the same as counting points on $\mathbb{P}(4, 6)_{\mathbb{Q}}$ in the image of the natural map $Y_0(m) \to Y(1) \subseteq \mathbb{P}(4, 6)_{\mathbb{Q}}$. Counting them up to twist replaces this with the further natural quotient by μ_2, giving $\mathbb{P}(2, 3)_{\mathbb{Q}}$.

We now turn our attention to those elliptic curves which admit pairs of cyclic m-isogenies. These elliptic curves are not parameterized by a single modular curve; however, they are paramterized by a family of modular curves, one for each proper divisor n of m. Theorem 3.2.28 and the comments that follow it may be extracted from [14], which proves a great deal more; however, we opt to give a self-contained argument.

Theorem 3.2.28. *Let*

$$m \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\} . \tag{3.2.29}$$

and let n be a proper divisor of m. Then Table 3.2.30 records each modular curve defined over $\mathbb{Q}$ which parameterizes elliptic curves equipped with pairs of unsigned cyclic m-isogenies whose kernels have intersection of order n.

The RSZB labels used in Table 3.2.30 are defined in [57]. Let $\Gamma \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup, and let X_Γ be the associated modular curve. The first three numbers that occur in the RSZB label of X_Γ are its level, the index of Γ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and the genus of X_Γ. For instance, when $m = 6$ and $n = 2$, we obtain the modular curve $X_0(2) \times_{X(1)} X_{\mathrm{sp}}(3)$, which has RSZB label 6.36.0.1. Thus $X_0(2) \times_{X(1)} X_{\mathrm{sp}}(3)$ is level 6, has index 36, and has genus 0.

m	n	RSZB label
2	1	2.6.0.1
3	1	3.12.0.1
4	1	4.24.0.8
4	2	4.6.0.1
5	1	5.30.0.1
6	1	6.72.1.1
6	2	6.36.0.1
6	3	6.24.0.1
7	1	7.56.1.1
8	1	8.96.3.16
8	2	8.24.0.67
8	4	8.12.0.5
9	1	9.108.4.4
9	3	Not defined over $\mathbb{Q}$
10	1	10.180.7.1
10	2	10.90.2.1
10	5	10.36.1.1
12	1	12.288.13.3
12	2	12.72.1.1
12	3	12.96.3.4
12	4	12.72.1.1
12	6	12.24.0.3
13	1	13.182.8.1
16	1	16.384.21.47
16	2	16.96.3.226
16	4	Not defined over $\mathbb{Q}$
16	8	16.24.0.2
18	1	18.648.37.11
18	2	18.324.16.5
18	3	Not defined over $\mathbb{Q}$
18	6	Not defined over $\mathbb{Q}$
18	9	18.72.1.1
25	1	25.750.48.1
25	5	Not defined over $\mathbb{Q}$

Table 3.2.30: Modular curves parameterizing elliptic curves with pairs of unsigned cyclic n-isogenies whose kernels have intersection of order n

Proof of Theorem 3.2.28. Let m be as above, and suppose $E \in \mathscr{E}$ has two distinct unsigned cyclic m-isogenies with kernels $\Phi_1, \Phi_2 \subseteq E(\mathbb{Q}^{\mathrm{al}})$. If we let $n := \#(\Phi_1 \cap \Phi_2)$ in Φ_1, we must have $n \mid m$ by elementary group theory, and $n > 1$ as otherwise $\Phi_1 = \Phi_2$ and our m-isogenies would not be distinct up to sign. We first handle the case where m is a power of a prime, and afterwards we will address the case where m is a product of powers of distinct primes.

Suppose first that m is a power of a prime. There are two subcases: $n = 1$ and $n > 1$.

In the first subcase, $\Phi_1 + \Phi_2 = E[m]$. As the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}}$ stabilizes both Φ_1 and Φ_2, the modular curve $X_{\mathrm{sp}}(m)$ associated to the split Cartan group precisely parameterizes elliptic curves equipped with such a pair of unsigned cyclic isogenies.

On the other hand, if $n > 1$, write $n' = m/n$. Choose P and Q be generators for Φ_1 and Φ_2 as abelian groups, so that $n'P = n'Q$ is a generator for $\Phi_1 \cap \Phi_2$. Choose $P_2 \in E[m](\mathbb{Q}^{\mathrm{al}})$ so that $\{P_1 = P, P_2\}$ is a basis for $E[m](\mathbb{Q}^{\mathrm{al}})$. We therefore have

$$Q = aP_1 + bP_2 \tag{3.2.31}$$

for some $a, b \in \mathbb{Z}$, and

$$n'P = n'Q = an'P_1 + bn'P_2. \tag{3.2.32}$$

As m is a prime power, aQ generates Φ_2, so we may replace Q with aQ and take $a = 1$. As $n'b \equiv 0 \pmod{m}$, b must be a multiple of n in $\mathbb{Z}/m\mathbb{Z}$. But if $b\mathbb{Z}/m\mathbb{Z} \subsetneq n\mathbb{Z}/m\mathbb{Z}$, then the $\#\left(\Phi_1 \cap \Phi_2\right) > n$, a contradiction. So $b = un$ for some $u \in (\mathbb{Z}/m\mathbb{Z})^\times$, and replacing P_2 with uP_2 if necessary, we may assume $b = n$.

Now in the coordinates $\{P_1, P_2\}$, we have

$$P = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } Q = \begin{pmatrix} 1 \\ n \end{pmatrix}. \tag{3.2.33}$$

The image of $\mathrm{Gal}_{\mathbb{Q}}$ in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ maps each of these vectors to a multiple of itself, and a little linear algebra shows that the set of all such matrices in $M_2(\mathbb{Z}/m\mathbb{Z})$ is precisely the set

$$\left\{ \begin{pmatrix} a & b \\ 0 & a + nb + n'c \end{pmatrix} : a \in (\mathbb{Z}/m\mathbb{Z})^\times \text{ and } b, c \in \mathbb{Z}/m\mathbb{Z} \right\}. \tag{3.2.34}$$

Conversely, if the image of $\mathrm{Gal}_{\mathbb{Q}}$ on $\mathrm{GL}(E[m](\mathbb{Q}^{\mathrm{al}})$ is of the form given by (3.2.34) for some choice of basis P_1, P_2, then E has two unsigned cyclic m-isogenies with kernels Φ_1 and Φ_2 having intersection of size n.

Let us consider a product m of distinct prime powers $p_1^{v_1}, \ldots, p_r^{v_r}$. To obtain modular curves that parameterize all elliptic curves with repeated cyclic $p_j^{v_j}$-isogenies, we apply the arguments above to each prime power $p_j^{v_j}$. We then take the fiber products of these modular curves over $X(1)$. However, we must also include the modular curve $X_0(p_j^{v_j})$ for each prime power $p_j^{v_j}$ in the fiber product (corresponding to the case where the p_j-part of the two cyclic isogenies is identical). Of course, the fiber product of all $X_0(p_j^{v_j})$ is $X_0(m)$, and we discard this case. □

A few remarks about Table 3.2.30 are in order.

First, the modular curves for the cases

$$(m, n) \in \{(9, 3), (16, 4), (18, 3), (18, 6), (25, 5)\}. \tag{3.2.35}$$

are not defined over $\mathbb{Q}$, and do not have any $\mathbb{Q}$-points. Indeed, the Weil pairing tells us that the determinant map from image of $\mathrm{Gal}_{\mathbb{Q}}$ in $\mathrm{GL}(E[m])$ to $(\mathbb{Z}/m\mathbb{Z})^{\times}$ must be surjective (see [62, Proposition 8.1 and Corollary 8.1.1]), but in each of these cases the determinant image of (3.2.34) is a proper subgroup of $(\mathbb{Z}/m\mathbb{Z})^{\times}$. Thus, for instance, there are no elliptic curves $E/\mathbb{Q}$ possessing two cyclic 9-isogenies with kernels having an intersection of size 3 (this possibility was also precluded by the isogeny graphs of [14]). '

Second, we note that when $m = 2^v > 2$ and $m/n = n' = 2$, we obtain the modular curve $X_0(m)$. In these cases, cyclic m-isogenies invariably come in pairs (see [55, §3] for a careful treatment of this observation in the case $m = 4$). This property is preserved by fiber products, so cyclic 12-isogenies also come in pairs. This observation gives rise to the following corollary.

Corollary 3.2.36. *Let $m \in \{12, 16, 18\}$. Then we have*

$$\widetilde{N}_m^{\mathrm{tw}}(X) = 2N_m^{\mathrm{tw}}(X) + O(1) \tag{3.2.37}$$

for $X \geq 1$.

Proof. In these cases $Y_0(m)$ parameterizes both elliptic curves equipped with an unsigned cyclic m-isogeny, and elliptic curves equipped with a pair of unsigned cyclic m-isogenies whose kernels have intersection of order $m/2$. Thus the count of elliptic curves we obtain by substituting $t \in \mathbb{Q}$ into the Weierstrass equation

$$y^2 = x^3 + f_m(t)x + g_m(t) \tag{3.2.38}$$

is off by a factor of 2. For all divisors n of m with $1 \leq n < m/2$, the modular curve we obtain has nonzero genus. When the genus is greater than 1, Faltings's theorem (Theorem 2.1.1) gives us a contribution of $O(1)$ to the difference $\widetilde{N}_m^{\mathrm{tw}}(X) - 2N_m^{\mathrm{tw}}(X)$. Otherwise, when $m = 12$ and $n \in \{2, 4\}$, the associated modular curve $X_{\mathrm{sp}}(3) \times_{X(1)} X_0(4)$ has genus 1: by inspection, this modular curve is $\mathbb{Q}$-isomorphic to the elliptic curve

$$y^2 = x^3 + 1, \tag{3.2.39}$$

which has Mordell-Weil group $\mathbb{Z}/6\mathbb{Z}$, and again we get a contribution of $O(1)$ to $\widetilde{N}_{12}^{\mathrm{tw}}(X) - 2N_{12}^{\mathrm{tw}}(X)$. □

If

$$(m, n) \in \{(2,1), (3,1), (4,1), (5,1), (6,2), (6,3), (8,2)\}, \tag{3.2.40}$$

the associated modular curve has genus 0, but is not the moduli space for the space of elliptic curves equipped with a cyclic m-isogeny. In these cases, we can compute universal families

$$E_{m,n}(t) : y^2 = x^3 + f_{m,n}(t)x + g_{m,n}(t) \tag{3.2.41}$$

for elliptic curves (over $\mathbb{Q}$, up to quadratic twist) with this level structure, in the manner of Lemma 3.2.1. For later use, the polynomials $f_{m,n}(t)$ and $g_{m,n}(t)$ are recorded in Tables 3.2.42 and 3.2.43 below.

m	n	$f_{m,n}(t)$
2	1	$-3(3t^2+1)$
3	1	$-3t(2+t)(4-2t+t^2)$
4	1	$-3\left(t^4-2t^3+2t^2+2t+1\right)\left(t^4+2t^3+2t^2-2t+1\right)$
5	1	$-3\left(t^2+4\right)\left(t^2-3t+1\right)\left(t^4-t^3+11t^2+4t+16\right)$ $\left(t^4+4t^3+11t^2+14t+31\right)$
6	2	$-3\left(t^3-2\right)\left(t^3+6t-2\right)\left(t^6-6t^4-4t^3+36t^2+12t+4\right)$
6	3	$-3\left(t^2+3\right)\left(t^6-15t^4+75t^2+3\right)$
8	2	$-3\left(t^4-8t^3+2t^2+8t+1\right)\left(t^4+8t^3+2t^2-8t+1\right)$

Table 3.2.42: $f_{m,n}(t)$ for for
$(m,n) \in \{(2,1),(3,1),(4,1),(5,1),(6,2),(6,3),(8,2)\}$

m	n	$g_{m,n}(t)$
2	1	$2t(t-1)(t+1)$
3	1	$2(t^2-2t-2)(t^4+2t^3+6t^2-4t+4)$
4	1	$2\left(t^2-2t-1\right)\left(t^2+2t-1\right)\left(t^4+1\right)\left(t^4+6t^2+1\right)$
5	1	$2\left(t^2+4\right)^2\left(t^2+2t-4\right)\left(t^4+3t^2+1\right)\left(t^4-6t^3+21t^2-36t+61\right)$ $\left(t^4+4t^3+21t^2+34t+41\right)$
6	2	$2\left(t^2+2t-2\right)\left(t^4-2t^3-8t-2\right)\left(t^4-2t^3+6t^2+4t+4\right)$ $\left(t^8+2t^7+4t^6-16t^5-14t^4+8t^3+64t^2-16t+4\right)$
6	3	$2\left(t^4-6t^2-3\right)\left(t^4-6t^2-24t-3\right)\left(t^4-6t^2+24t-3\right)$
8	2	$2\left(t^2-2t-1\right)\left(t^2+2t-1\right)\left(t^8+132t^6-250t^4+132t^2+1\right)$

Table 3.2.43: $g_{m,n}(t)$ for

$(m,n) \in \{(2,1),(3,1),(4,1),(5,1),(6,2),(6,3),(8,2)\}$

Section 3.3

Lattices and the principle of Lipschitz

In this section, we recall (a special case of) the Principle of Lipschitz, also known as Davenport's Lemma. We apply this result to estimate the number of Weierstrass equations of the form

$$E : y^2 = x^3 + A_m(a,b)x + B_m(a,b) \tag{3.3.1}$$

which satisfy $H(A,B) \leq X$. This count differs substantially from $\widetilde{N}_m^{\mathrm{tw}}(X)$ because the pairs (a,b) and (da,db) give rise to the same elliptic curve, just with different models, and (not unrelatedly) $H(A,B)$ need not be the twist height of E. To obtain $\widetilde{N}_m(X)$ we will also need to sum over quadratic twists of these elliptic curves. Nevertheless, the estimates given in this section are essential building blocks in what follows.

Theorem 3.3.2 (Principle of Lipschitz)**.** *Let $\mathcal{R} \subseteq \mathbb{R}^2$ be a closed and bounded region, with rectifiable boundary $\partial\mathcal{R}$. Then we have*

$$\#(\mathcal{R} \cap \mathbb{Z}^2) = \operatorname{area}(\mathcal{R}) + O(\operatorname{len}(\partial\mathcal{R})). \tag{3.3.3}$$

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 [17]. □

Remark 3.3.4. Davenport's formulation of Theorem 3.3.2 was substantially stronger than what we have recorded. More precisely, he allowed for $\mathcal{R}$ to be a subset of $\mathbb{R}^n$, not just $\mathbb{R}^2$, he imposed weaker conditions $\mathcal{R}$ than we have, and he made his error term explicit.

Applying the Principle of Lipschitz

Specializing to the case of interest, for $m \in \{4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$ and for $X > 0$, let

$$\mathcal{R}_m(X) := \left\{(a, b) \in \mathbb{R}^2 : H(A_m(a, b), B_m(a, b)) \leq X,\ \ b \geq 0\right\}, \tag{3.3.5}$$

and let

$$R_m := \operatorname{area}(\mathcal{R}_m(1)). \tag{3.3.6}$$

Lemma 3.3.7. *Let $m \in \{4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$. For $X > 0$, we have*

$$\operatorname{area}(\mathcal{R}_m(X)) = R_m X^{1/d(m)}. \tag{3.3.8}$$

Proof. Since $f_m(t) = A_m(t, 1)$ and $g_m(t) = B_m(t, 1)$ have no common real root, the region $\mathcal{R}_m(X)$ is compact [16, Proof of Theorem 3.3.1, Step 2]. The homogeneity

$$H(A_m(ua, ub), B_m(ua, ub)) = u^{2d(m)} H(A_m(a, b), B_m(a, b)) \tag{3.3.9}$$

implies

$$\begin{aligned}\operatorname{area}(\mathcal{R}_m(X)) &= \operatorname{area}(\{(X^{1/2d(m)}a, X^{1/2\deg B m}b) : (a,b) \in \mathcal{R}_m(1)\}) \\ &= X^{1/d(m)} \operatorname{area}(\mathcal{R}_m(1)) \qquad (3.3.10) \\ &= R_m X^{1/d(m)}\end{aligned}$$

as desired. □

We obtain the following corollary of Theorem 3.3.2.

Corollary 3.3.11. *Let $m \in \{4,5,6,7,8,9,10,12,13,16,18,25\}$, and let $a_0, b_0, d \in \mathbb{Z}$ with $d \geq 1$. For $X > 0$, we have*

$$\#\{(a,b) \in \mathcal{R}_m(X) \cap \mathbb{Z}^2 : (a,b) \equiv (a_0,b_0) \pmod d\} = \frac{R_m X^{1/d(m)}}{d^2} + O\left(\frac{X^{1/2d(m)}}{d}\right) \qquad (3.3.12)$$

for $X, d \geq 1$. The implied constants are independent of X, d, a_0, and b_0. In particular,

$$\#(\mathcal{R}_m(X) \cap \mathbb{Z}^2) = R_m X^{1/d(m)} + O(X^{1/2d(m)}) \qquad (3.3.13)$$

for $X \geq 1$.

Proof. We combine Lemma 3.3.7 and Theorem 3.3.2 to obtain (3.3.12) for X sufficiently large, say for $X \geq X_0$. But as the left-hand side of (3.3.12) is locally bounded, and $X^{1/2d(m)}/d > 0$ for $X, d \geq 1$ we can choose C large enough that

$$\left|\#\{(a,b) \in \mathcal{R}_m(X) \cap \mathbb{Z}^2 : (a,b) \equiv (a_0,b_0) \pmod d\} - \frac{R_m X^{1/d(m)}}{d^2}\right| \leq C\frac{X^{1/2d(m)}}{d} \qquad (3.3.14)$$

for $1 \leq X \leq X_0$, and (3.3.12) holds for $X, d \geq 1$. □

In the proof of Corollary 3.3.11, we turned an assertion of the form

$$f(X) = g(X) + O(h(X)) \text{ for } X \text{ sufficiently large} \tag{3.3.15}$$

into an assertion of the form

$$f(X) = g(X) + O(h(X)) \text{ for } X \geq 1. \tag{3.3.16}$$

This technique readily generalizes: if $f(X)$ is locally bounded and $h(X) = X^\alpha$, then (3.3.15) implies (3.3.16) essentially by the argument given in the proof of Corollary 3.3.11. Similarly, if $f(X)$ is locally bounded and $h(X) = X^\alpha \log^\beta X$, then (3.3.15) implies

$$f(X) = g(X) + O(h(X)) \text{ for } X \geq 2. \tag{3.3.17}$$

We shall use these observations without further comment throughout the remainder of the thesis.

Remark 3.3.18. Huxley's work [32] implies that if the boundary of $\mathcal{R}$ is defined by nonlinear polynomials, then the error term in (3.3.13) can be improved to $O(X^{1/2d(m)-\delta})$ for some $\delta > 0$ (see [55, page 7]). Of course, this does not hold for $\mathcal{R}_m(X)$ as we have defined it, because the line $b = 0$ gives a lower boundary for $\mathcal{R}_m(X)$. However, if we drop the condition $b \geq 0$ from the definition of $\mathcal{R}_m(X)$, Huxley's result will apply.

Under this convention, the points (a, b) and $(-a, -b)$ correspond to the same elliptic curve, and some additional technical care is needed to attend to those points with $b = 0$. However, such an argument enables us to modestly improve error terms for $M_m(X; e)$ in Lemma 4.3.16, Lemma 5.3.12, and Lemma 6.3.1, and consequently improve the asymptotic error in Theorem 4.3.57, Theorem 5.3.46, and Theorem 6.3.34. For want of time and ease of exposition, we decline to pursue this insight further in this thesis.

We now record graphs of the region $R_m(1)$ for $m \in \{4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$. For each figure, the region graphed in blue is the set

$$\left\{(a,b) \in \mathbb{R}^2 : 4\left|A_m(a,b)\right|^3 \leq 1, b \geq 0\right\}; \tag{3.3.19}$$

similarly, the region graphed in red is the set

$$\left\{(a,b) \in \mathbb{R}^2 : 27\left|B_m(a,b)\right|^2 \leq 1, b \geq 0\right\}. \tag{3.3.20}$$

By definition, $\mathcal{R}_m(1)$ is the intersection of these two regions.

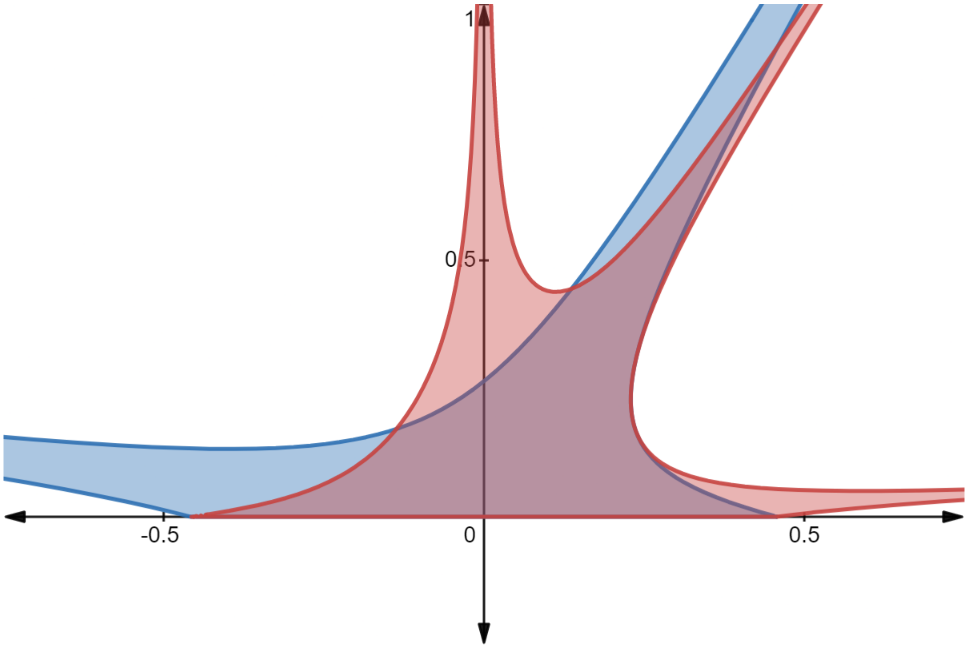

Figure 3.3.21: The region $\mathcal{R}_4(1)$

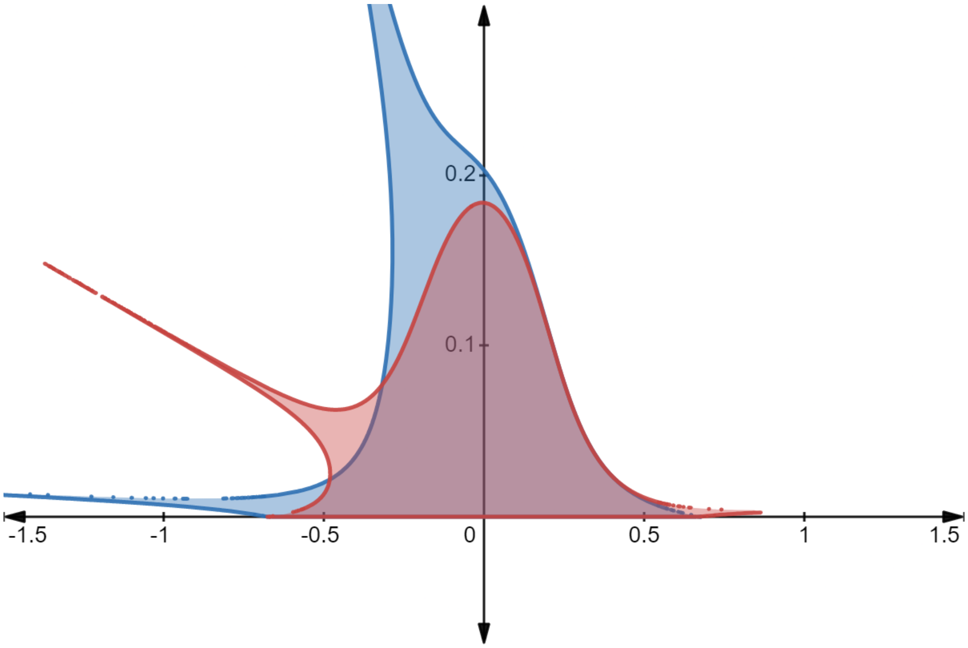

Figure 3.3.22: The region $\mathcal{R}_5(1)$

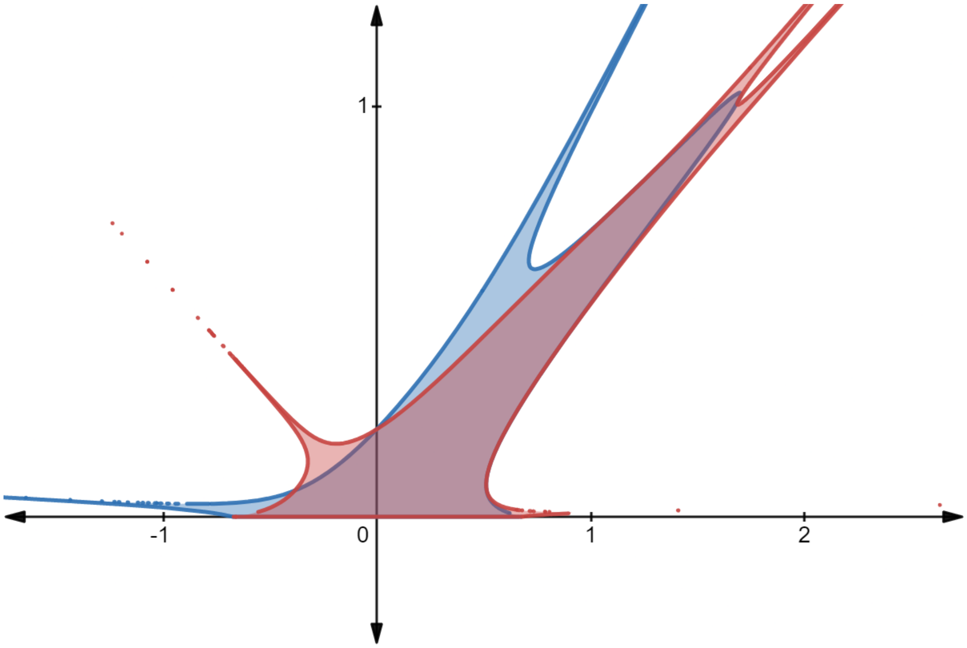

Figure 3.3.23: The region $\mathcal{R}_6(1)$

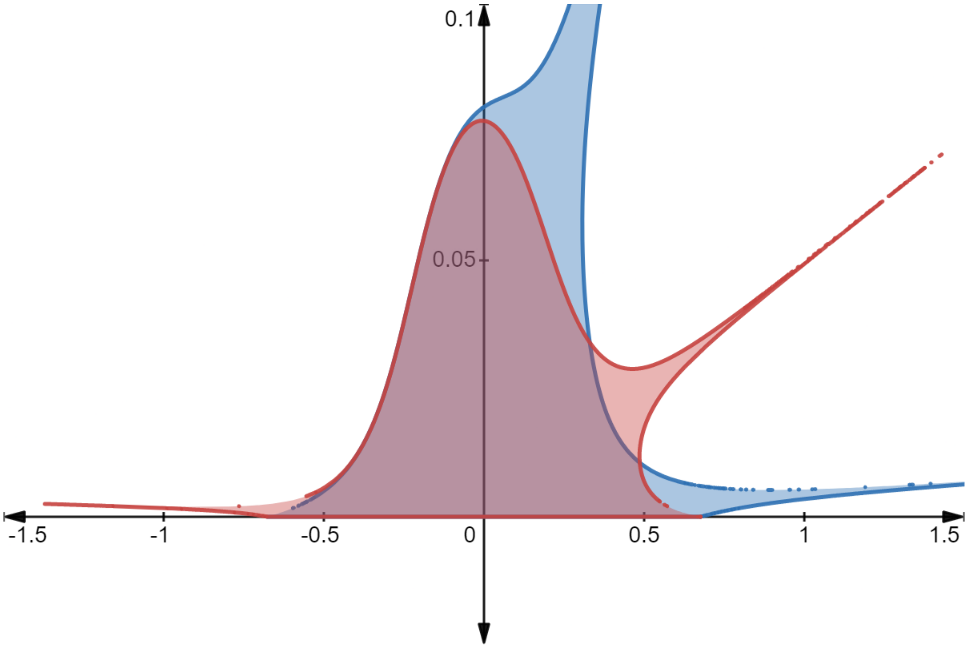

Figure 3.3.24: The region $\mathcal{R}_7(1)$

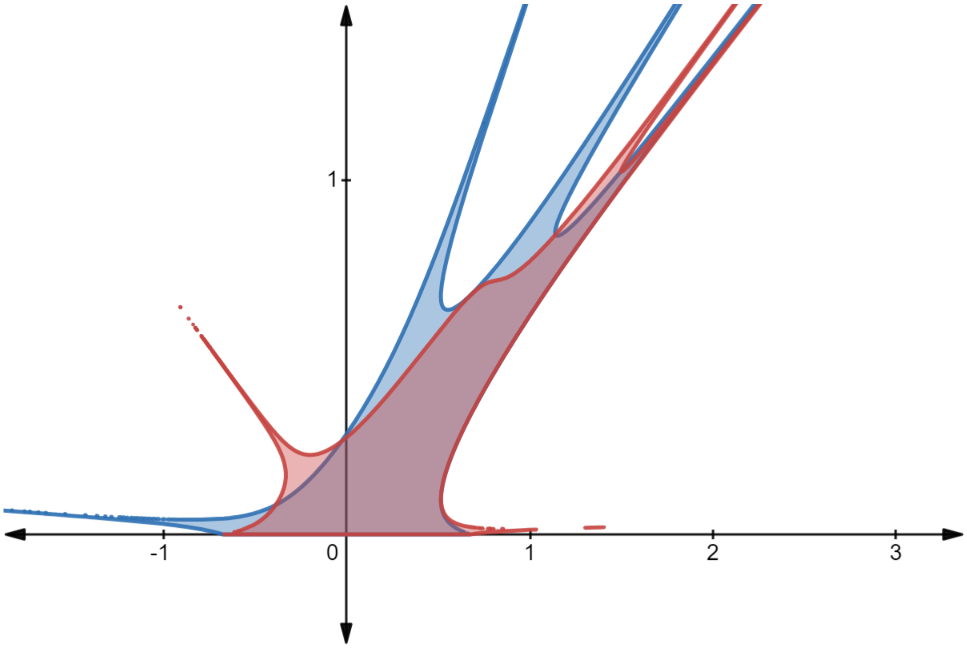

Figure 3.3.25: The region $\mathcal{R}_8(1)$

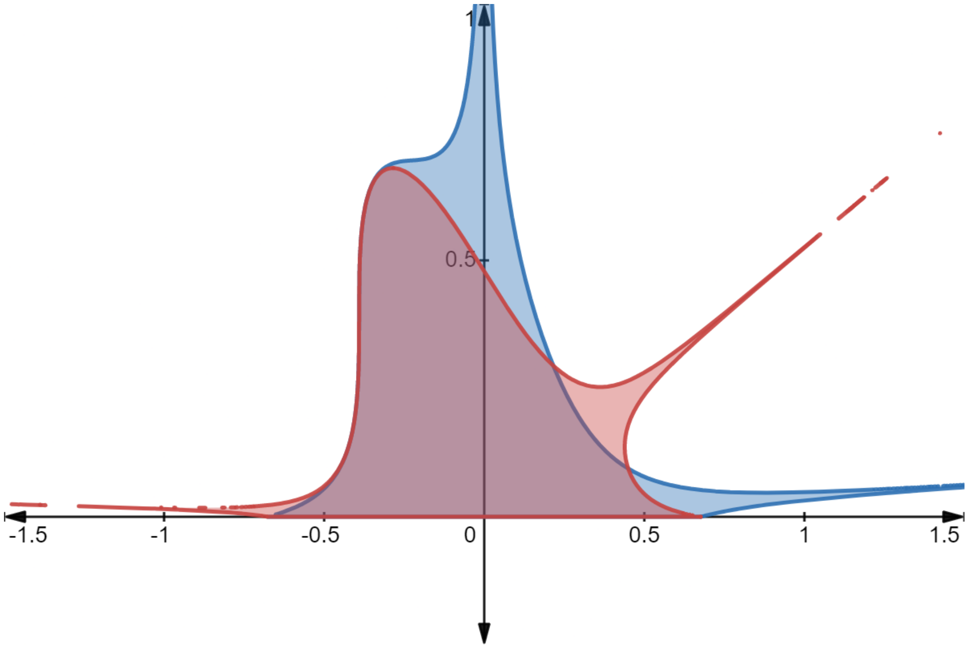

Figure 3.3.26: The region $\mathcal{R}_9(1)$

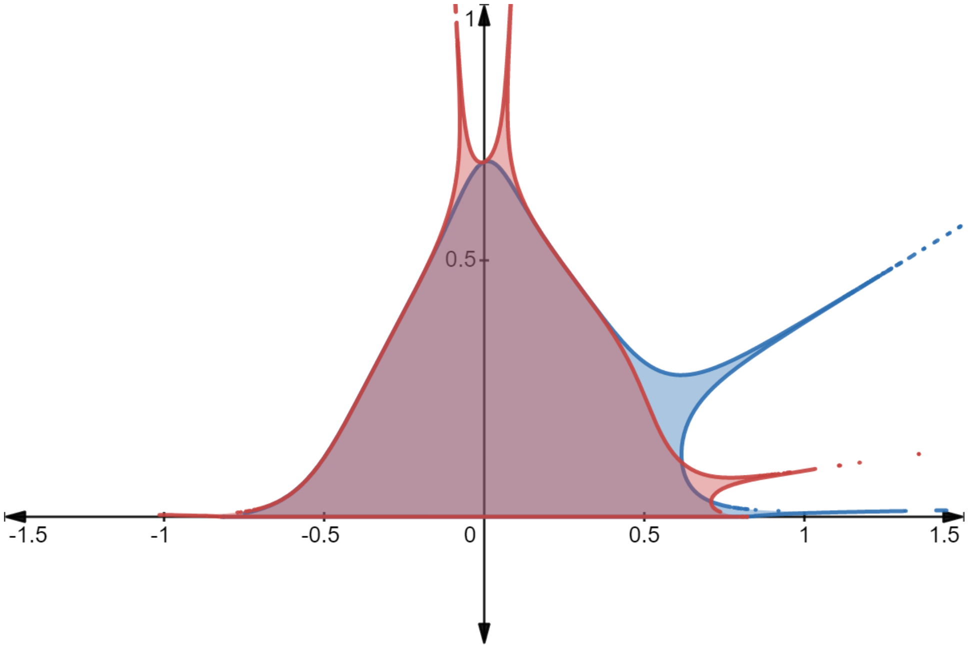

Figure 3.3.27: The region $\mathcal{R}_{10}(1)$

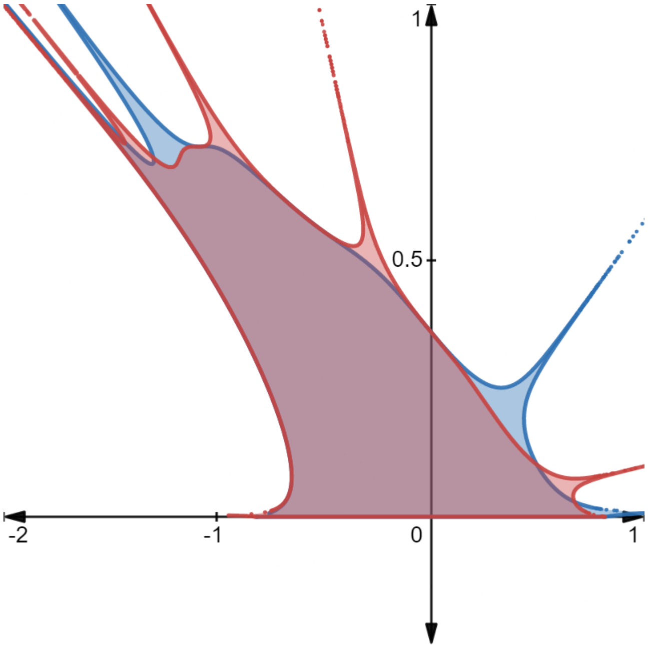

Figure 3.3.28: The region $\mathcal{R}_{12}(1)$

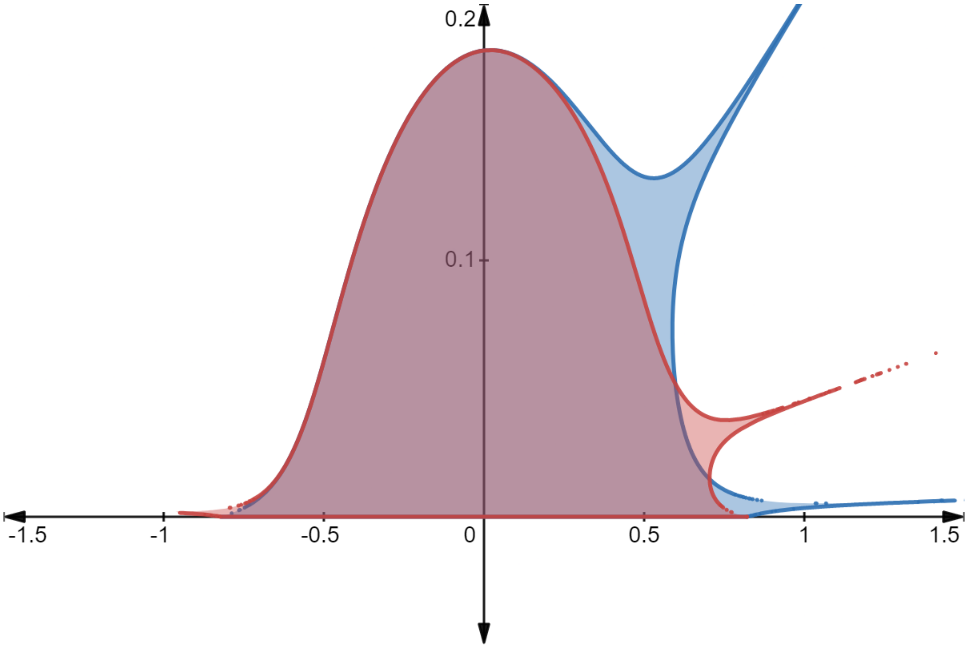

Figure 3.3.29: The region $\mathcal{R}_{13}(1)$

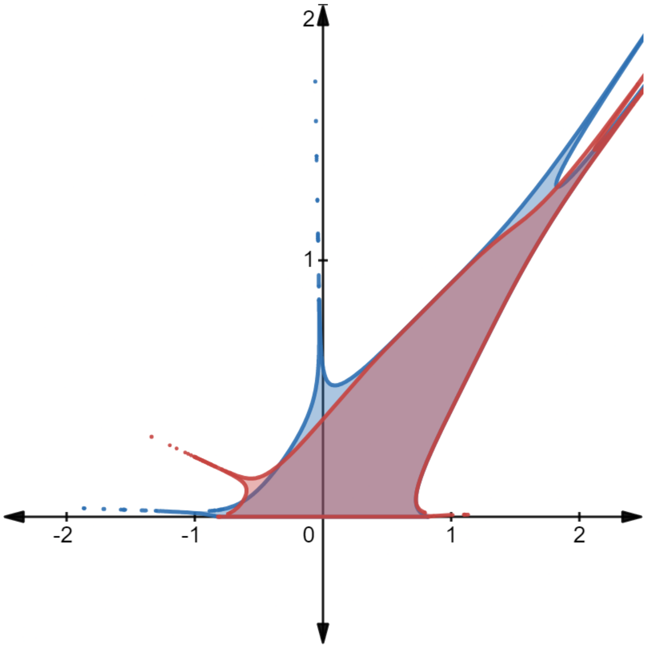

Figure 3.3.30: The region $\mathcal{R}_{16}(1)$

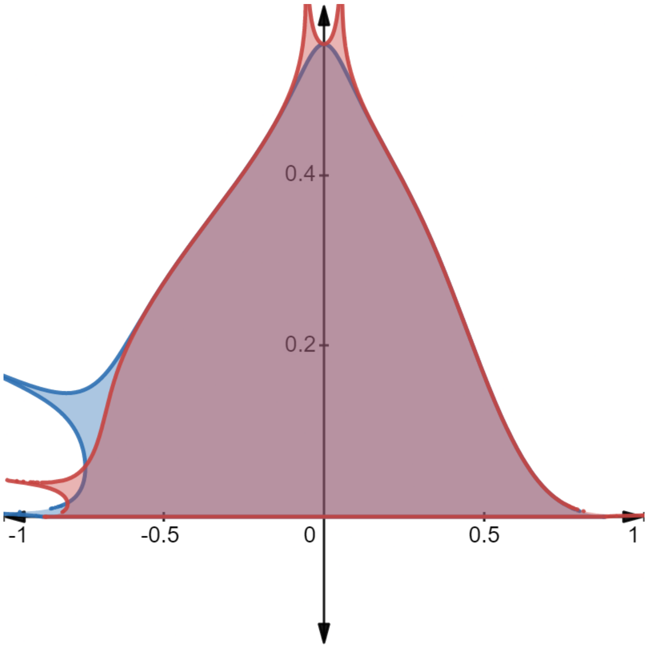

Figure 3.3.31: The region $\mathcal{R}_{18}(1)$

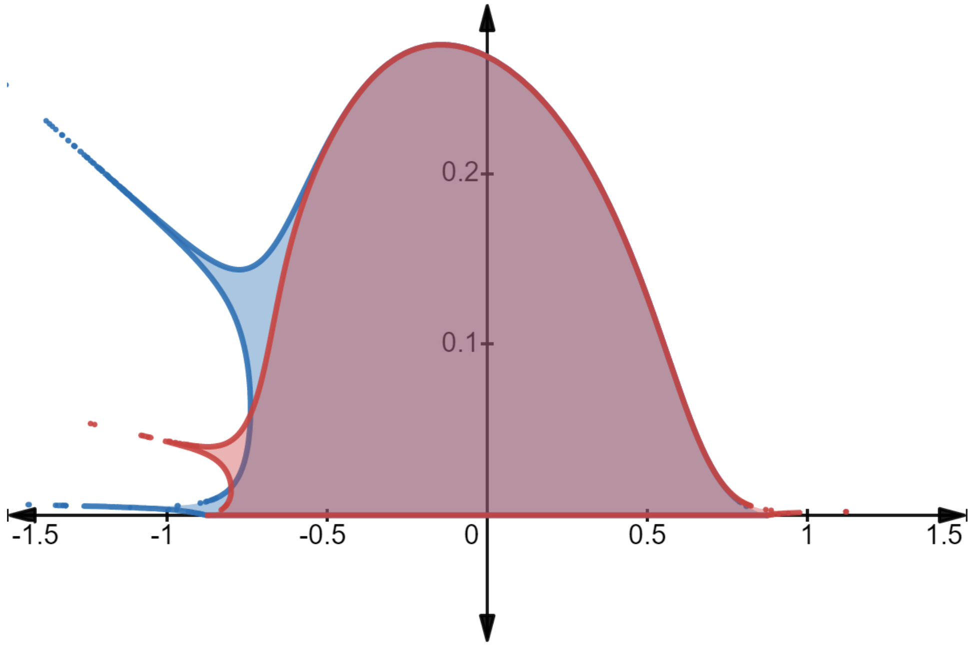

Figure 3.3.32: The region $\mathcal{R}_{25}(1)$

Remark 3.3.33. The region $\mathcal{R}_4(X)$ which we use to parameterize elliptic curves equipped with a cyclic 4-isogeny differs substantially from the region $\mathcal{R}_1'(X)$ from [55, page 6] that Pomerance and Schaefer use to parameterize elliptic curves equipped with a pair of cyclic 4-isogenies.

This discrepancy reflects a difference in derivation. Pomerance and Schaefer parameterize elliptic curves E equipped with a pair of cyclic 4-isogenies essentially by investigating the 2-division polynomial and the 4-division polynomial for E [55, Proposition 3.2], and thus obtain the parameterization

$$(A_4^{\text{P-S}}(a,b), B_4^{\text{P-S}}(a,b)) := (a^2 - 3b^2, (a^2 - 2b^2)b). \tag{3.3.34}$$

We instead parameterize elliptic curves by using the Riemann–Roch theorem to establish an isomorphism from $X_0(4)$ to $\mathbb{P}^1$ (Lemma 3.2.1), and thus obtain the parameterization

$$(A_4(a,b), B_4(a,b)) = (-3(a^2+6ab-3), 2a(a^2-18ab+9b^2)). \tag{3.3.35}$$

This also means that for each elliptic curve E (with $j(E) \neq 0$) equipped with a pair of associated cyclic 4-isogenies, we have two (4-groomed) ordered pairs $(a,b) \in \mathbb{Z}^2$ (one for each isogeny) where Pomerance and Schaefer only have one. For example, the elliptic curve

$$E : y^2 = x^3 - 2x + 1 \tag{3.3.36}$$

arises via our method from the ordered pairs $(3,1)$ and $(3,5)$; on the other hand, for Pomerance and Schaefer, this elliptic curve arises from the ordered pair $(1,-1)$.

Generalizing the Principle of Lipschitz

As stated, Theorem 3.3.2 counts points in the lattice $\mathbb{Z}^2$, but we may easily extend this result to counts of points in more general lattices.

Corollary 3.3.37. *Let $\mathcal{R} \subseteq \mathbb{R}^2$ be a closed and bounded region, with rectifiable boundary $\partial\mathcal{R}$, let $\mathcal{L} \subseteq \mathbb{R}^2$ be a two-dimensional lattice, let $M : \mathbb{R}^2 \to \mathbb{R}^2$ be a linear map which induces a bijection between $\mathbb{Z}^2$ and $\mathcal{L}$, and let $\sigma(M)$ denote the smallest singular value of M. We have*

$$\#(\mathcal{R} \cap \mathcal{L}) = \frac{\operatorname{area}(\mathcal{R})}{|\det M|} + O\left(\frac{\operatorname{len}(\partial\mathcal{R})}{\sigma(M)}\right), \tag{3.3.38}$$

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. Let $M : \mathbb{R}^2 \to \mathbb{R}^2$ be a linear map which induces a bijection from $\mathbb{Z}^2$ to $\mathcal{L}$; if v_1, v_2

are a $\mathbb{Z}$-basis for $\mathcal{L}$, we can take $M = (v_1\ v_2)$. By assumption, we have

$$\#(\mathcal{R} \cap \mathcal{L}) = \#(\mathcal{R} \cap M\mathbb{Z}^2) = \#(M^{-1}\mathcal{R} \cap \mathbb{Z}^2). \tag{3.3.39}$$

By the variational characterization of the singular values of M ([31, Theorem 7.3.8]), M^{-1} stretches $\partial\mathcal{R}$ by at most $1/\sigma(M)$. We now apply Theorem 3.3.2 to obtain our desired result. □

Remark 3.3.40. Note that $|\det M|$ is the covolume of $\mathcal{L}$, and independent of our choice of M. On the other hand, $\sigma(M)$ depends heavily on our choice of linear transform M. This is because shears preserve area but stretch lengths.

For instance, if $\mathcal{L} = \mathbb{Z}^2$, then letting M be the identity map recovers Theorem 3.3.2. On the other hand, if we foolishly let

$$M = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \tag{3.3.41}$$

the error degrades by a factor of more than n. In Figure 3.3.42 below, both the square and the parallelogram are fundamental regions for $\mathbb{Z}^2$, but the square has a perimeter of 4 whereas the parallelogram has a perimeter of $2 + 2\sqrt{2} = 4.828\ldots > 4$.

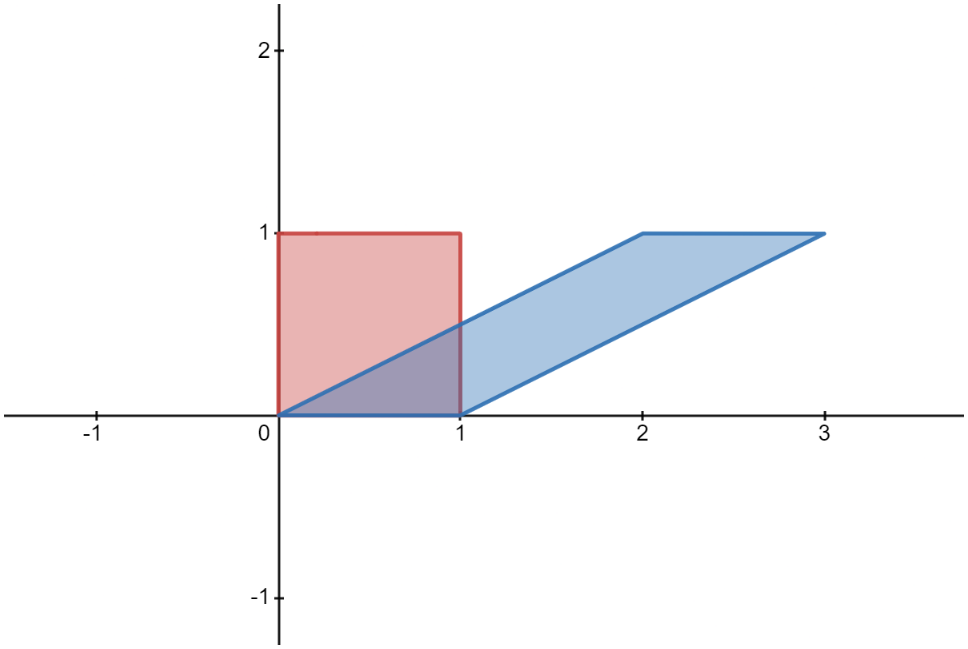

Figure 3.3.42: The unit square under the transformation $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$

Section 3.4

Analytic ingredients

In this section, we record several results from analytic number theory for later use. We begin by recording one half of Karamata's integral theorem for regularly varying functions. We then report estimates for counts of squarefree integers. We proceed to give several results from complex analysis about the convergence and growth rate of Dirichlet series. Finally, we record a Tauberian theorem which we will use to translate our estimates for $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$ to estimates for $\widetilde{N}_m(X)$ and $N_m(X)$.

Regularly varying functions

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

Definition 3.4.1. Let $F\colon \mathbb{R}_{>0} \to \mathbb{R}$ 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

$$\lim_{y\to\infty} \frac{F(\lambda y)}{F(y)} = \lambda^{\rho}. \tag{3.4.2}$$

Theorem 3.4.3 (Karamata's integral theorem)**.** *Let $F\colon \mathbb{R}_{>0} \to \mathbb{R}$ be locally bounded and regularly varying of index ρ. Let $\sigma, \rho \in \mathbb{R}$. Then the following statements hold.*

(a) *If $\sigma > \rho + 1$, then*

$$\int_{y}^{\infty} t^{-\sigma} F(u)\,\mathrm{d}u \sim \frac{y^{1-\sigma}F(y)}{|\sigma - \rho - 1|} \tag{3.4.4}$$

as $y \to \infty$.

(b) *If $\sigma < \rho + 1$, then*

$$\int_{0}^{y} u^{-\sigma} F(u)\,\mathrm{d}u \sim \frac{y^{1-\sigma}F(y)}{|\sigma - \rho - 1|} \tag{3.4.5}$$

as $y \to \infty$.

Proof. See Bingham–Glodie–Teugels [6, Theorem 1.5.11]. (Karamata's integral theorem also includes a converse.) □

Corollary 3.4.6. *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*

$$F(y) := \sum_{n \le y} \alpha(n) \sim \kappa y^{\rho} \log^{\tau} y \tag{3.4.7}$$

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

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

$$\sum_{n>y} n^{-\sigma}\alpha(n) \sim \frac{\rho y^{-\sigma}F(y)}{|\sigma - \rho|} \sim \frac{\kappa \rho y^{\rho-\sigma}\log^{\tau} y}{|\sigma - \rho|}. \tag{3.4.8}$$

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

$$\sum_{n\leq y} n^{-\sigma}\alpha(n) \sim \frac{\rho y^{-\sigma}F(y)}{|\sigma-\rho|} \sim \frac{\kappa\rho y^{\rho-\sigma}\log^{\tau} y}{|\sigma-\rho|}. \tag{3.4.9}$$

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 (3.4.7), $F(y)$ is eventually positive. Now for any $\lambda > 0$, we compute

$$\lim_{y\to\infty}\frac{F(\lambda y)}{F(y)} = \lim_{y\to\infty}\frac{\kappa(\lambda y)^{\rho}\log^{\tau}(\lambda y)}{\kappa y^{\rho}\log^{\tau} y} = \lambda^{\rho}, \tag{3.4.10}$$

so F is regularly varying of index ρ.

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

$$y^{-\sigma}F(y) \sim \kappa y^{\rho-\sigma}\log^{\tau} y \to 0 \tag{3.4.11}$$

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

$$\sum_{n>y} n^{-\sigma}\alpha(n) = -y^{-\sigma}F(y) + \sigma\int_y^{\infty} u^{-\sigma-1}F(u)\,\mathrm{d}u. \tag{3.4.12}$$

Clearly $\sigma + 1 > \rho + 1$, so Theorem 3.4.3(a) tells us

$$\int_y^{\infty} u^{-\sigma-1}F(u)\,\mathrm{d}u \sim \frac{y^{-\sigma}F(y)}{|\sigma-\rho|} \sim \frac{\kappa y^{\rho-\sigma}\log^{\tau} y}{|\sigma-\rho|} \tag{3.4.13}$$

and thus

$$\sum_{n>y} n^{-\sigma}\alpha(n) \sim \frac{\rho y^{-\sigma}F(y)}{|\sigma-\rho|} \tag{3.4.14}$$

as $y \to \infty$.

The case $\rho > \sigma > 0$ is similar. □

Counting squarefree integers

Recall from (3.2.24) that for $X > 0$ a real number, we have

$$S_2(X) := \#\left\{n \in \mathbb{Z}_{>0} : n \leq X,\ n \text{ a squarefree integer}\right\}. \tag{3.4.15}$$

In this subsection, we record estimates for $S_2(X)$ due to Walfisz [66] and Liu [42]. These estimates are obtained by examining the zero-free region of the Riemann zeta function.

Theorem 3.4.16. *Let $X > 0$ be a real number. Then for some constant $\kappa > 0$, we have*

$$S_2(X) = \frac{X}{\zeta(k)} + O\left(X^{1/2} e^{-\kappa \frac{\log^{3/5} X}{\log^{1/5} \log X}}\right) \tag{3.4.17}$$

for $X \geq 1$.

Proof. Walfisz [66, Satz V.6.1] proves a stronger result. □

If the Riemann hypothesis holds, we can say substantially more about $S_2(X)$.

Theorem 3.4.18. *Let $X > 0$ be a real number. If the Riemann hypothesis holds, then for any $\epsilon > 0$, we have*

$$S_2(X) = \frac{X}{\zeta(2)} + O\left(X^{11/35+\epsilon}\right) \tag{3.4.19}$$

for $X \geq 1$. The implicit constant depends on ϵ.

Proof. Liu [42, Theorem 1]. □

Dirichlet series

In this subsection, we record several analytic results about Dirichlet series.

The following theorem is attributed to Stieltjes.

Theorem 3.4.20. *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 for $s = \sigma + it$ with $\sigma > \sigma_0$, and one of these two series converges absolutely, then*

$$L_{\alpha*\beta}(s) := \sum_{n\geq 1} \left(\sum_{d|n} \alpha(d)\beta\left(\frac{n}{d}\right) \right) n^{-s} \tag{3.4.21}$$

converges for $s = \sigma + it$ with $\sigma > \sigma_0$. If both $L_\alpha(s)$ and $L_\beta(s)$ both converge absolutely when $\sigma > \sigma_0$, then so does $L_{\alpha*\beta}(s)$.

Proof. Widder [69, Theorems 11.5 and 11.6b] proves a more general result, or see Tenenbaum [64, proof of Theorem II.1.2, Notes on p. 204]. □

Let

$$\gamma := \lim_{y\to\infty} \Big(\sum_{n\leq y} 1/n - \log y \Big) \tag{3.4.22}$$

be the Euler–Mascheroni constant.

Theorem 3.4.23. *The difference*

$$\zeta(s) - \left(\frac{1}{s-1} + \gamma \right) \tag{3.4.24}$$

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

Proof. Ivić [33, page 4] proves a more general result. □

Recall that a complex function $F(s)$ has finite order on a domain $D \subseteq \mathbb{C}$ if there exists $\xi \in \mathbb{R}_{>0}$ such that

$$F(\sigma \pm it) = O(1 + |t|^\xi) \tag{3.4.25}$$

whenever $\sigma \pm it \in D$. We emphasize that this is a statement about $F(\sigma \pm it)$ for t large, not about F on or close to the real line. If F is of finite order on a right half-plane, we define

$$\mu_F(\sigma) := \inf\{\xi \in \mathbb{R}_{\geq 0} : F(\sigma + it) = O(1 + |t|^{\xi})\} \tag{3.4.26}$$

as $t \to \infty$, where the implicit constant depends on σ and ξ.

Proposition 3.4.27. *Let F and G be complex functions functions of finite order on a right half-plane. We have*

$$\mu_{F+G}(\sigma) \leq \max(\mu_F(\sigma), \mu_G(\sigma)), \tag{3.4.28}$$

and

$$\mu_{FG}(\sigma) = \mu_F(\sigma) + \mu_G(\sigma). \tag{3.4.29}$$

Proof. Immediate from the definition of $\mu_F(\sigma)$. □

Theorem 3.4.30. *Let $L(s)$ be a Dirichlet series with abscissa of absolute convergence σ_a. Then 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 [64, Theorem II.1.21]. □

Theorem 3.4.31. *Let $\zeta(s)$ be the Riemann zeta function, and let $\sigma \in \mathbb{R}$. Then we have*

$$\mu_\zeta(\sigma) \leq \begin{cases} \frac{1}{2} - \sigma, & \text{if } \sigma \leq 0; \\ \frac{1}{2} - \frac{29}{45}\sigma, & \text{if } 0 \leq \sigma \leq \frac{1}{2}; \\ \frac{13}{42}(1 - \sigma), & \text{if } \frac{1}{2} \leq \sigma \leq 1; \\ 0 & \text{if } \sigma \geq 1. \end{cases} \tag{3.4.32}$$

Moreover, equality holds if $\sigma < 0$ or $\sigma > 1$.

Proof. Tenenbaum [64, page 235] proves the claim when $\sigma < 0$ or $\sigma > 1$. Now

$$\mu_\zeta(1/2) \leq 13/84 \tag{3.4.33}$$

by Bourgain [8, Theorem 5], and our result follows from the subconvexity of μ_ζ [64, Theorem II.1.20]. □

Remark 3.4.34. We use Theorem 3.4.31 as an input to Theorem 3.4.37. Although we have stated it in the strongest form we know, for our applications, we could replace (3.4.33) with the much weaker statement

$$\mu_\zeta(1/2) < 1/2. \tag{3.4.35}$$

However, appropriate refinements to Theorem 3.4.37 might enable us to leverage the full strength of Theorem 3.4.31 (see Remark 4.4.14 below).

A Tauberian theorem

We now present a Tauberian theorem, due in essence to Landau [40], and in this formulation to Roux [58]

Definition 3.4.36. 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 $\{s = \sigma + it \in \mathbb{C} : \sigma > \sigma_a - \delta\}$ and only finitely many poles in this region.

(iii) For $\sigma > \sigma_a - \delta$, we have $\mu_{L_\alpha}(\sigma) \leq \xi$.

If $(\alpha(n))_n$ is admissible, let $s_1, \ldots, s_r$ 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 [64, §II.2.1], which is itself an inverse Mellin transform.

Theorem 3.4.37 (Landau's Tauberian Theorem)**.** *Let $(\alpha(n))_{n\geq 1}$ be an admissible sequence (Definition 3.4.36), and write $N_\alpha(X) := \sum_{n \leq X} \alpha(n)$. Then for all $\epsilon > 0$,*

$$N_\alpha(X) = \sum_{j=1}^{r} \operatorname{res}_{s=s_j} \left(\frac{L_\alpha(s) X^s}{s} \right) + O\left(X^{\sigma_a - \frac{\delta}{\lfloor \xi \rfloor + 2} + \epsilon} \right), \tag{3.4.38}$$

as $X \to \infty$, where the main term is a sum of residues. The implicit constant depends on ϵ.

Proof. See Roux [58, Theorem 13.3, Remark 13.4]. □

Remark 3.4.39. Landau's original theorem [40] was fitted to a more general context, and allowed sums of the form

$$\sum_{n \geq 1} \alpha(n) \ell(n)^{-s} \tag{3.4.40}$$

as long as $(\ell(n))_{n\geq 1}$ was increasing and tended to ∞. However, Landau also required that $L_\alpha(s)$ has a meromorphic continuation to all of $\mathbb{C}$, and Roux [58, Theorem 13.3, Remark 13.4] relaxes this assumption. Both Landau and Roux wrote out the expression

$$\operatorname{res}_{s=s_j} \left(\frac{L_\alpha(s) X^s}{s} \right) \tag{3.4.41}$$

in terms of the Laurent series expansion for $L_\alpha(s)$ around $s = s_j$, but we believe expressing the result in terms of residues is more transparent.

We now illustrate the applicability and power of Theorem 3.4.37. Let $\omega(n)$ denote the number of distinct prime divisors of n, and recall the definition of the Euler-Mascheroni constant γ (3.4.22).

Corollary 3.4.42. *for any $\epsilon > 0$, we have*

$$\sum_{n\leq y} 2^{\omega(n)} = \frac{1}{\zeta(2)} y \log y + \frac{(2\gamma - 1)\zeta(2) - 2\zeta'(2)}{\zeta(2)^2} y + O\left(y^{3/4+\epsilon}\right) \\ \approx 0.607927X \log y + 0.786872y + O\left(y^{3/4+\epsilon}\right) \tag{3.4.43}$$

for $y \geq 1$. The implicit constant depends only on ϵ.

Proof. Recall that

$$L_{2^\omega}(s) := \frac{\zeta(s)^2}{\zeta(2s)} = \sum_{n\geq 1} \frac{2^{\omega(n)}}{n^s}. \tag{3.4.44}$$

For $\sigma > 1/2$, this function is holomorphic except at $s = 1$, where it has a simple pole of order 2. Write $\zeta_a(s) := \zeta(as)$. By Theorem 3.4.30, $\mu_{1/\zeta_2}(\sigma) = 0$ for $\sigma > \frac{1}{2}$, and by Theorem 3.4.31, $\mu_\zeta(\sigma) = \frac{13}{42}(1 - \sigma)$ for $\frac{1}{2} \leq \sigma \leq 1$. Thus for any $\epsilon > 0$ and all $\sigma > \frac{1}{2} + \epsilon$, Proposition 3.4.27 tells us

$$\mu_{L_{2^\omega}}(\sigma) \leq \frac{2 \cdot 13}{84} + 0 = \frac{13}{42}. \tag{3.4.45}$$

We conclude that the sequence $\left(2^{\omega(n)}\right)_{n\geq 1}$ is admissible with parameters $(1, 1/2, 13/42)$.

We compute the residue of $L_{2^\omega}(s) \cdot \frac{y^s}{s}$ at $s = 1$, which is

$$\frac{1}{\zeta(2)} y \log y + \frac{(2\gamma - 1)\zeta(2) - 2\zeta'(2)}{\zeta(2)^2} y \tag{3.4.46}$$

Applying Theorem 3.4.37, we conclude

$$\sum_{n\leq y} 2^{\omega(n)} = \frac{1}{\zeta(2)} y \log y + \frac{(2\gamma - 1)\zeta(2) - 2\zeta'(2)}{\zeta(2)^2} y + O\left(y^{3/4+\epsilon}\right) \tag{3.4.47}$$

for any $\epsilon > 0$. □

Remark 3.4.48. Better estimates for $\sum_{n\leq y} 2^{\omega(n)}$ are possible (see [64, Exercise I.3.54]), but we shall not require them.

Although we do not require the strength of the asymptotics of Corollary 3.4.42, it will be useful to have an order of growth for $\kappa^{\omega(n)}$ in greater generality.

Theorem 3.4.49. *Let $\kappa > 0$ be a real number. Then we have*

$$\sum_{n \leq y} \kappa^{\omega(n)} \asymp y \log^{\kappa-1} y. \tag{3.4.50}$$

Proof. Ivić proves a stronger result [33, Theorem 14.10]. □

Section 3.5

Our approach revisited

In this section, we elaborate on the intuitions laid out in section 1.3 and set up a general framework that will enable us to determine the asymptotic number of elliptic curves with a cyclic m-isogeny over $\mathbb{Q}$, up to both quadratic twist and $\mathbb{Q}$-isomorphism, when $m \in \{7, 10, 13, 25\}$. Our method also applies even more easily when $m \in \{4, 6, 8, 9, 12, 16, 18\}$. When $X_0(m)$ is of nonzero genus, i.e., when $m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}$, there are four or fewer elliptic curves in $\mathscr{E}^{\mathrm{tw}}$ with a cyclic m-isogeny, so there is no need to sieve to obtain $\widetilde{N}_m^{\mathrm{tw}}(X) = N_m^{\mathrm{tw}}(X)$ (see chapter 8 for the asymptotics of $N_m^{\mathrm{tw}}(X)$ and $N_m(X)$ for these m).

Choose m so that $X_0(m)$ is of genus 0 and $m > 5$ or $m = 4$. We now elaborate on the steps described in section 1.3. The first step, obtaining a parameterization for the family of elliptic curves with a cyclic m-isogeny up to quadratic twist, was completed in section 3.2. The second step, estimating

$$\#\{(a, b) \in \mathcal{R}_m(X) \cap \mathbb{Z}^2 : (a, b) \equiv (a_0, b_0) \pmod{d}\} \tag{3.5.1}$$

for $a_0, b_0, d \in \mathbb{Z}$, was completed in section 3.3.

We erect a more abstract framework for addressing third step and the fifth step of our approach (the fourth step is addressed by Corollary 2.1.50 and Lemma 7.2.23).

Estimating $N_{\mathcal{E}}^{\mathbf{tw}}(X)$

In this subsection, we abstract the strategy developed in [45, section 4.1] and formulate it in a way that will enable us to estimate $\widetilde{N}_m^{\text{tw}}(X)$ and $N_m^{\text{tw}}(X)$ for

$$m \in \{4, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}. \tag{3.5.2}$$

We establish some notation for brevity and ease of exposition. Suppose $(\alpha(X;n))_{n\geq 1}$ is a sequence of real-valued functions, and $\phi : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is a function. We write

$$\sum_{n\geq 1} \alpha(X;n) = \sum_{n \ll \phi(X)} \alpha(X;n) \tag{3.5.3}$$

if there is a positive constant κ such that for all $X \in \mathbb{R}_{>0}$ and all $n > \kappa\phi(X)$, we have $\alpha(X;n) = 0$.

Let $\mathcal{E}$ denote a multiset of Weierstrass models for elliptic curves over $\mathbb{Q}$ with integral coefficients, as in (3.1.1). Thus $E \in \mathcal{E}$ is given by a Weierstrass equation

$$E : y^2 = x^3 + Ax + B \tag{3.5.4}$$

with $A, B \in \mathbb{Z}$ and $4A^3 + 27B^2 \neq 0$, and we assume nothing further about A and B. For E as in (3.5.4), we abuse notation and write $H(E)$ for $H(A,B)$ and $\text{tmd}(E)$ for $\text{tmd}(A,B)$. For the definition of H and tmd, see (3.1.2) and (3.1.9).

Let

$$N_{\mathcal{E}}^{\text{tw}}(X) := \#\{E \in \mathcal{E} : \text{twht}(E) \leq X\}. \tag{3.5.5}$$

We assume that $N_{\mathcal{E}}^{\text{tw}}(X)$ is finite for all $X > 0$. Note that this framework encompasses both the counts $\widetilde{N}_m^{\mathrm{tw}}(X)$ and the counts $N_m^{\mathrm{tw}}(X)$: the former by letting $\mathcal{E}$ denote the multiset of elliptic curves in $\mathscr{E}^{\mathrm{tw}}$ that admits a cyclic m-isogeny, counted with repetition if the same elliptic curve admits multiple unsigned cyclic m-isogenies, and the latter by letting $\mathcal{E}$ denote simply the set of elliptic curves in $\mathscr{E}^{\mathrm{tw}}$ that possess a cyclic m-isogeny.

Let

$$M_{\mathcal{E}}(X; e) := \#\left\{E \in \mathcal{E} : H(E) \leq X, e \mid \operatorname{tmd}(E)\right\}. \tag{3.5.6}$$

Note that the points counted by $\widetilde{N}_{\mathcal{E}}^{\mathrm{tw}}(X)$ have *twist height* bounded by X, but the points counted by $M_{\mathcal{E}}(X; e)$ have only the function H bounded by X.

For our applications, we estimate $M_{\mathcal{E}}(X; e)$ using Corollary 3.3.11 and sometimes Corollary 3.3.37, together with some sieving. There are important difference between the sieving necessary for $m = 7$, $m = 10$ and $m = 25$, and $m = 13$ (see Lemma 4.3.16, Lemma 5.3.12, and Lemma 6.3.1). These differences stem from certain geometric differences between $X_0(7)$, $X_0(10)$ and $X_0(25)$, and $X_0(13)$: to wit, the elliptic surface parameterizing elliptic curves equipped with a cyclic 7-isogeny has a place of type II additive reduction, the elliptic surfaces parameterizing elliptic curves equipped with a cyclic 10-isogeny and cyclic 25-isogeny have places of type III additive reduction, and the elliptic surface parameterizing elliptic curves equipped with a cyclic 13-isogeny has places of both type II and type III additive reduction.

Once we have estimates for $M_{\mathcal{E}}(X; e)$, however, these geometric disparities play no further role in our technique. Our results in this thesis depend upon the following application of the Möbius sieve.

Lemma 3.5.7. *We have*

$$N_{\mathcal{E}}^{\mathrm{tw}}(X) = \sum_{n \geq 1} \sum_{e \mid n} \mu(n/e) M_{\mathcal{E}}(e^6 X; n). \tag{3.5.8}$$

Proof. As an intermediate step, we define

$$N_{\mathcal{E}}^{\mathrm{tw}}(X;e) = \#\left\{E \in \mathcal{E} : \mathrm{twht}(E) \leq X, \mathrm{tmd}(E) = e\right\}. \tag{3.5.9}$$

By (3.1.10),

$$N_{\mathcal{E}}^{\mathrm{tw}}(X) = \sum_{n \geq 1} N_{\mathcal{E}}^{\mathrm{tw}}(X;e). \tag{3.5.10}$$

Moreover, (3.1.10) yields

$$M_{\mathcal{E}}(X;e) = \sum_{ef \ll X^{1/6}} N_{\mathcal{E}}^{\mathrm{tw}}(X/(ef)^6; ef), \tag{3.5.11}$$

and applying Möbius inversion to (3.5.11) yields

$$N_{\mathcal{E}}^{\mathrm{tw}}(X;e) = \sum_{ef \ll X^{1/6}} \mu(f) M_{\mathcal{E}}(e^6 f^6 X; ef). \tag{3.5.12}$$

Note, however, that any $E \in \mathcal{E}$ with $H(E) > e^6 X$ cannot contribute to $N_{\mathcal{E}}^{\mathrm{tw}}(X;e)$, so in fact we have the equality

$$N_{\mathcal{E}}^{\mathrm{tw}}(X;e) = \sum_{ef \ll X^{1/6}} \mu(f) M_{\mathcal{E}}(e^6 X; ef). \tag{3.5.13}$$

Substituting (3.5.13) into (3.5.10) and letting $n = ef$, we obtain our desired result. □

Before proceeding, we record a modest bound on the summands of (3.5.8), which will be of use in the proofs of Lemma 4.3.60, Lemma 5.3.41, and Lemma 6.3.29.

Proposition 3.5.14. *For all $e, n \in \mathbb{Z}_{>0}$ and $X > 0$, if $e \mid n$ then we have*

$$0 \leq \sum_{e \mid n} \mu(n/e) M_{\mathcal{E}}(e^6 X; n) \leq M_{\mathcal{E}}(n^6 X; n). \tag{3.5.15}$$

Proof. By (3.5.6), $M_{\mathcal{E}}(X;e)$ counts elliptic curves $E \in \mathcal{E}$ with $e \mid \mathrm{tmd}(E)$ and $H(E) \leq X$.

By the inclusion-exclusion principle, we see

$$\sum_{e \mid n} \mu(n/e) M_{\mathcal{E}}(e^6 X; n) \tag{3.5.16}$$

counts elliptic curves $E \in \mathcal{E}$ with $n \mid \operatorname{tmd}(E)$, $H(E) \leq n^6 X$, and $H(E) > e^6 X$ for all e a proper divisor of n. The claim follows. □

Definition 3.5.17. Define

$$N^{\mathrm{tw}}_{\mathcal{E}, \leq y}(X) := \sum_{n \leq y} \sum_{e \mid n} \mu(n/e) M_{\mathcal{E}}(e^6 X; n) \tag{3.5.18}$$

and

$$N^{\mathrm{tw}}_{\mathcal{E}, > y}(X) := \sum_{n > y} \sum_{e \mid n} \mu(n/e) M_{\mathcal{E}}(e^6 X; n). \tag{3.5.19}$$

By Lemma 3.5.7, we have

$$N^{\mathrm{tw}}_{\mathcal{E}}(X) = N^{\mathrm{tw}}_{\mathcal{E}, \leq y}(X) + N^{\mathrm{tw}}_{\mathcal{E}, > y}(X). \tag{3.5.20}$$

Utilizing our estimates for $M_{\mathcal{E}}(X; e)$ (Lemma 4.3.16, Lemma 5.3.12, Lemma 6.3.1, and Lemma 7.2.6), we can obtain asymptotics for $N^{\mathrm{tw}}_{\mathcal{E}, \leq y}(X)$ and $N^{\mathrm{tw}}_{\mathcal{E}, > y}(X)$. Choosing y to minimize the error in (3.5.20), we hope to obtain a good asymptotic for $N^{\mathrm{tw}}_{\mathcal{E}}(X)$ as $X \to \infty$.

This concludes our treatment of the third step of our approach.

Estimating $N_{\mathcal{E}}(X)$

In this subsection, we adapt and abstract the notation and arguments in [45, §5.1], enabling us to derive the asymptotics for $\widetilde{N}_m(X)$ and $N_m(X)$ from those of $\widetilde{N}^{\mathrm{tw}}_m(X)$ and $N^{\mathrm{tw}}_m(X)$. This will clarify the final step described in section 1.3. We continue to use the assumptions and notation set out in section 3.5.

For $X > 0$, we define

$$N_{\mathcal{E}}(X) := \#\left\{E^{(c)} : E \in \mathcal{E},\ c \in \mathbb{Z} \text{ squarefree, and } \operatorname{ht}(E^{(c)}) \leq X\right\}, \tag{3.5.21}$$

where $E^{(c)}$ is as in (1.1.6). Here we consider the right-hand side to be the count of a multiset.

The function $N_{\mathcal{E}}(X)$ counts (with repetition) all elliptic curves in $\mathscr{E}$ with rational height less than or equal to X which are quadratic twists of elliptic curve in $\mathcal{E}$.

We wish to obtain asymptotics for $N_{\mathcal{E}}(X)$ as $X \to \infty$. By Lemma 3.2.1, this framework encompasses both the counts $\widetilde{N}_m(X)$ and the counts $N_m(X)$: the former by letting $\mathcal{E}$ denote the multiset of elliptic curves in $\mathscr{E}^{\text{tw}}$ that possess a cyclic m-isogeny, counted with repetition of the same elliptic curve admits multiple unsigned cyclic m-isogenies, and the latter by letting $\mathcal{E}$ denote simply the set of elliptic curves in $\mathscr{E}^{\text{tw}}$ that admit a cyclic m-isogeny.

We adopt the convention $N_{\mathcal{E}}^{\text{tw}}(0) = N_{\mathcal{E}}(0) = 0$. For $n \geq 1$, write

$$\Delta N_{\mathcal{E}}^{\text{tw}}(n) := N_{\mathcal{E}}^{\text{tw}}(n) - N_{\mathcal{E}}^{\text{tw}}(n-1); \tag{3.5.22}$$

likewise, write

$$\Delta N_{\mathcal{E}}(n) := N_{\mathcal{E}}(n) - N_{\mathcal{E}}(n-1). \tag{3.5.23}$$

Then $\Delta N_{\mathcal{E}}^{\text{tw}}(n)$ counts the number of elliptic curves $E \in \mathscr{E}$ of twist height n, and $\Delta N_{\mathcal{E}}(n)$ counts the number of elliptic curves $E \in \mathscr{E}$ of height n that are quadratic twists of elements of $\mathcal{E}$.

We define

$$L_{\mathcal{E}}^{\text{tw}}(s) := \sum_{n \geq 1} \Delta N_{\mathcal{E}}^{\text{tw}}(n) n^{-s} \tag{3.5.24}$$

and

$$L_{\mathcal{E}}(s) := \sum_{n \geq 1} \Delta N_{\mathcal{E}}(n) n^{-s} \tag{3.5.25}$$

wherever these Dirichlet series converge.

Note $N_{\mathcal{E}}^{\mathrm{tw}}(X) = \sum_{n\le X} \Delta N_{\mathcal{E}}^{\mathrm{tw}}(n)$, and conversely we have $L_{\mathcal{E}}^{\mathrm{tw}}(s) = \int_0^\infty u^{-s}\,\mathrm{d}N_{\mathcal{E}}^{\mathrm{tw}}(u)$. A good asymptotic understanding of $N_{\mathcal{E}}^{\mathrm{tw}}(X)$ therefore enables us to develop a good analytic understanding of $L_{\mathcal{E}}^{\mathrm{tw}}(s)$ (for instance, see Corollary 4.3.66). Similarly, $N_{\mathcal{E}}(X) = \sum_{n\le X} \Delta N_{\mathcal{E}}(n)$, and conversely we have $L_{\mathcal{E}}(s) = \int_0^\infty u^{-s}\,\mathrm{d}N_{\mathcal{E}}(u)$.

Theorem 3.5.26. *The following statements hold.*

(a) We have

$$\Delta N_{\mathcal{E}}(n) = 2\sum_{c^6\mid n} |\mu(c)|\,\Delta N_{\mathcal{E}}^{\mathrm{tw}}\left(n/c^6\right) \tag{3.5.27}$$

(b) We have

$$L_{\mathcal{E}}(s) = \frac{2\zeta(6s)L_{\mathcal{E}}^{\mathrm{tw}}(s)}{\zeta(12s)} \tag{3.5.28}$$

wherever both sides converge.

Proof. For (a), we first collect the terms that contribute to $\Delta N_{\mathcal{E}}(n)$ by the quadratic twist factor c:

$$\Delta N_{\mathcal{E}}^{(c)}(n) := \#\left\{E\in\mathcal{E} : \mathrm{ht}(E^{(c)}) = n\right\} \tag{3.5.29}$$

By (3.1.16) we have $\mathrm{ht}(E^{(c)}) = c^6\,\mathrm{ht}(E)$, so

$$\Delta N_{\mathcal{E}}^{(c)}(n) = \begin{cases} \Delta N_{\mathcal{E}}^{\mathrm{tw}}(n/c^6), & \text{if } c^6 \mid n; \\ 0, & \text{otherwise.}\end{cases} \tag{3.5.30}$$

Therefore

$$\Delta N_{\mathcal{E}}(n) = \sum_{c \text{ squarefree}} \Delta N_{\mathcal{E}}^{(c)}(n) = 2\sum_{c\ge 1} |\mu(c)|\,\Delta N_{\mathcal{E}}^{(c)}(n) = 2\sum_{c^6\mid n} |\mu(c)|\,\Delta N_{\mathcal{E}}^{\mathrm{tw}}\left(n/c^6\right) \tag{3.5.31}$$

proving (a).

Part (b) simply reframes (a) in the language of Dirichlet series rather than Dirichlet convolutions. □

Thus, we can leverage our understanding of $L_{\mathcal{E}}^{\text{tw}}(s)$ to obtain information about $L_{\mathcal{E}}(s)$. Finally, using Landau's Tauberian theorem (Theorem 3.4.37), we can transform analytic information about $L_{\mathcal{E}}(s)$ into asymptotic information about $N_{\mathcal{E}}(s)$.

Remark 3.5.32. In this thesis, we apply Landau's Tauberian theorem (Theorem 3.4.37) to Theorem 3.5.26(b) in order to obtain asymptotics for $L_{\mathcal{E}}(s)$. In doing so, we implicitly invoke the apparatus of complex analysis, which is used in the proof of Perron's formula and of Landau's Tauberian theorem. However, we believe an elementary argument applying Dirichlet's hyperbola method [64, Theorem I.3.1] to Theorem 3.5.26(a) could achieve similar asymptotics, and perhaps even modestly improve on the error term.

We now specialize to the notation we have developed in this section to our problems of interest.

When $\mathcal{E}$ is the multiset of elliptic curves in $\mathscr{E}^{\text{tw}}$ that possess a cyclic m-isogeny, counted with repetition if the same elliptic curve possesses multiple cyclic m-isogenies, we have $N_{\mathcal{E}}^{\text{tw}}(X) = \widetilde{N}_m^{\text{tw}}(X)$. For this choice of $\mathcal{E}$, we write

$$\begin{aligned}
\widetilde{N}_m^{\text{tw}}(X;e) &:= N_{\mathcal{E}}^{\text{tw}}(X;e),\\
\widetilde{N}_{m,\leq y}^{\text{tw}}(X) &:= N_{\mathcal{E},\leq y}^{\text{tw}}(X),\\
\widetilde{N}_{m,>y}^{\text{tw}}(X) &:= N_{\mathcal{E},>y}^{\text{tw}}(X),\\
\Delta\widetilde{N}_m^{\text{tw}}(n) &:= \Delta N_{\mathcal{E}}^{\text{tw}}(n),\\
\widetilde{L}_m^{\text{tw}}(s) &:= L_{\mathcal{E}}^{\text{tw}}(n),\\
\Delta\widetilde{N}_m(n) &:= \Delta N_{\mathcal{E}}, \text{ and}\\
\widetilde{L}_m(s) &:= L_{\mathcal{E}}(s).
\end{aligned} \tag{3.5.33}$$

Thus for instance $\widetilde{L}_m^{\mathrm{tw}}(s)$ is the height zeta function whose nth coefficient $\Delta\widetilde{N}_m(n)$ is the number of pairs (E,ϕ) of elliptic curves E up to quadratic twist with an unsigned cyclic m-isogeny ϕ.

Similarly, when $\mathcal{E}$ is the set of elliptic curves in $\mathscr{E}^{\mathrm{tw}}$ admitting a cyclic m-isogeny, we have $N_{\mathcal{E}}^{\mathrm{tw}}(X) = N_m^{\mathrm{tw}}(X)$. In analogy with (3.5.33), for this $\mathcal{E}$ we write

$$\begin{aligned} N_m^{\mathrm{tw}}(X;e) &:= N_{\mathcal{E}}^{\mathrm{tw}}(X;e), \\ N_{m,\leq y}^{\mathrm{tw}}(X) &:= N_{\mathcal{E},\leq y}^{\mathrm{tw}}(X), \\ N_{m,>y}^{\mathrm{tw}}(X) &:= N_{\mathcal{E},>y}^{\mathrm{tw}}(X), \\ \Delta N_m^{\mathrm{tw}}(n) &:= \Delta N_{\mathcal{E}}^{\mathrm{tw}}(n), \\ L_m^{\mathrm{tw}}(s) &:= L_{\mathcal{E}}^{\mathrm{tw}}(n), \\ \Delta N_m(n) &:= \Delta N_{\mathcal{E}}, \text{ and} \\ L_m(s) &:= L_{\mathcal{E}}(s). \end{aligned} \tag{3.5.34}$$

Thus for instance $L_m^{\mathrm{tw}}(s)$ is the height zeta function whose nth coefficient $\Delta N_m^{\mathrm{tw}}(n)$ is the number of of elliptic curves E up to quadratic twist admitting an unsigned cyclic m-isogeny.

Chapter 4

Counting elliptic curves with a cyclic m-isogeny for $m = 7$

In this chapter, we prove Theorem 1.2.3 (Theorem 4.4.11), and Theorem 1.2.13 (Theorem 4.3.57) when $m = 7$. The arguments in this chapter are taken (in many cases verbatim) from [45]. However, we make several refinements and adjustments to the arguments of [45], which account for our much improved error term. Notably, we have furnished a second proof for Lemma 4.3.16 which improves its error term. We also establish improved estimates for the order of growth for $L_7^{\mathrm{tw}}(s)$. Both improvements propagate through the rest of the chapter.

In section 4.1, we establish notations pertaining to $f_7(t)$ and $g_7(t)$ which will be used throughout the remainder of the chapter. In section 4.2, we develop bounds relating the twist minimality defect to the greatest common divisor of $f_7(t)$ and $g_7(t)$. In section 4.3, we apply the framework developed in section 3.5 to prove Theorem 1.2.3 when $m = 7$, with a slightly improved error term. In section 4.4, we prove Theorem 1.2.3 when $m = 7$. In section 4.5, we enumerate the elliptic curves with a cyclic 7-isogeny and twist height at most 10^{42}, estimate the constants appearing in Theorem 4.3.57 and Theorem 4.4.11, and empirically confirm that the count of elliptic curves with a cyclic 7-isogeny aligns with our theoretical estimate.

Section 4.1

Establishing notation for $m = 7$

By Corollary 2.1.50, we have

$$\widetilde{N}_7^{\mathrm{tw}}(X) = N_7^{\mathrm{tw}}(X) \text{ and } \widetilde{N}_7(X) = N_7(X) \tag{4.1.1}$$

for all $X > 0$, so we may use either notation interchangeably. We opt to work with $N_7^{\mathrm{tw}}(X)$ and related functions.

Pursuant to the notation established in section 3.2, we define $h_7(t) = \gcd(f_7(t), g_7(t))$, and we define $f_7'(t)$ and $g_7'(t)$ so that

$$f_7(t) = f_7'(t)h_7(t) \text{ and } g_7(t) = g_7'(t)h_7(t). \tag{4.1.2}$$

We emphasize that f_7' and g_7' are *not* the derivatives of f_7 and g_7. We have

$$\begin{aligned} h_7(t) &= t^2 + t + 7, \\ f_7'(t) &= -3(t^2 - 231t + 735), \text{ and} \\ g_7'(t) &= 2(t^4 + 518t^3 - 11025t^2 + 6174t - 64827). \end{aligned} \tag{4.1.3}$$

To work with integral models, as discusssed in section 1.3, we take $t = a/b$ (in lowest terms) and homogenize, obtaining

$$\begin{aligned}
C_7(a,b) &:= b^2 h_7(a/b) = a^2 + ab + 7b^2, \\
A'_7(a,b) &:= b^2 f'_7(a/b) = -3(a^2 - 231ab + 735b^2), \text{ and} \\
B'_7(a,b) &:= b^4 g'_7(a/b) = 2(a^4 + 518a^3b - 11025a^2b^2 + 6174ab^3 - 64827b^4)
\end{aligned} \tag{4.1.4}$$

In analogy with (4.1.3), we have

$$\begin{aligned}
C_7(a,b) &= \gcd(A_7(a,b), B_7(a,b)) \in \mathbb{Z}[a,b], \\
A_7(a,b) &= A'_7(a,b)C_7(a,b), \text{ and} \\
B_7(a,b) &= B'_7(a,b)C_7(a,b).
\end{aligned} \tag{4.1.5}$$

Section 4.2

The twist minimality defect for $m = 7$

In this section, we study the twist minimality defect for

$$E_7(a,b) : y^2 = x^3 + A_7(a,b)x + B_7(a,b) \tag{4.2.1}$$

using the polynomials $A'_7(a,b)$, $B'_7(a,b)$, and $C_7(a,b)$.

We begin with the following lemma, which shows that when $\gcd(a,b) = 1$, the largest cube dividing $C_7(a,b)$ almost determines the twist minimality defect.

Lemma 4.2.2. *Let $(a,b) \in \mathbb{Z}^2$ be 7-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 $\ell^v \mid \operatorname{tmd}(A_7(a,b), B_7(a,b))$ if and only if $\ell^{3v} \mid C_7(a,b)$.*

(b) *$\ell^{3v} \mid C_7(a,b)$ if and only if $\ell \nmid b$ and $h_7(a/b) \equiv 0 \pmod{\ell^{3v}}$.*

(c) *If $\ell \neq 3$, then $\ell \mid C_7(a,b)$ implies $\ell \nmid (\partial C_7/\partial a)(a,b) = 2a+b$.*

We give two proofs of Lemma 4.2.2, one using resultants and the other using the polynomial division algorithm.

First proof of Lemma 4.2.2. We argue as in Cullinan–Kenney–Voight [16, Proof of Theorem 3.3.1, Step 3]. For part (a), we compute the resultants

$$\operatorname{Res}(A_7'(t,1), B_7'(t,1)) = \operatorname{Res}(f_7'(t), g_7'(t)) = -2^8 \cdot 3^7 \cdot 7^{14} = \operatorname{Res}(A_7'(1,u), B_7'(1,u)). \quad (4.2.3)$$

If $\ell \neq 2,3,7$, then $\ell \nmid \gcd(A_7'(a,b), B_7'(a,b))$; so by (3.1.6), if $\ell^v \mid \operatorname{tmd}(A_7(a,b), B_7(a,b))$ then $\ell^{2v} \mid C_7(a,b)$. But also

$$\operatorname{Res}(B_7'(t,1), C_7(t,1)) = \operatorname{Res}(g_7'(t), h_7(t)) = 2^8 \cdot 3^3 \cdot 7^7 = \operatorname{Res}(B_7'(1,u), C_7(1,u)), \quad (4.2.4)$$

so $\ell \nmid \gcd(B_7'(a,b), C_7(a,b))$ and thus $\ell^v \mid \operatorname{tmd}(A_7(a,b), B_7(a,b))$ if and only if $\ell^{3v} \mid C_7(a,b)$. If $\ell = 2$, a short computation confirms that $B_7(a,b)$ is odd whenever (a,b) is 7-groomed, so our claim also holds in this case.

For (b), by homogeneity it suffices to show that $\ell \nmid b$: this holds since if $\ell \mid b$ then $A_7(a,0) \equiv -3a^4 \equiv 0 \pmod{\ell}$ and $B_7(b,0) \equiv 2a^6 \equiv 0 \pmod{\ell}$ so $\ell \mid a$, a contradiction.

Part (c) follows from (b) and the fact that $h_7(t)$ has discriminant $\operatorname{disc}(h_7(t)) = -3^3$. $\square$

Second proof of Lemma 4.2.2. Let $F \neq G$ be homogeneous polynomials in a and b whose homogenizations are coprime over $\mathbb{Q}$. Applying the polynomial division algorithm to F and G to cancel all occurences of the variable a, we obtain coprime homogeneous polynomials $P_{F,G}^{(1)}(a,b) \in \mathbb{Z}[a,b]$ and $Q_{F,G}^{(1)}(a,b) \in \mathbb{Z}[a,b]$, and a positive integer $m_{F,G}^{(1)}$, such that

$$P_{F,G}^{(1)}(a,b)F(a,b) + Q_{F,G}^{(1)}(a,b)G(a,b) \quad (4.2.5)$$

equals $m_{F,G}^{(1)}$ times a power of b. Likewise, applying the polynomial division algorithm to F and G to cancel all occurences of the variable b, we obtain coprime homogeneous polynomials $P_{F,G}^{(2)}(a,b) \in \mathbb{Z}[a,b]$ and $Q_{F,G}^{(2)}(a,b) \in \mathbb{Z}[a,b]$, and a positive integer $m_{F,G}^{(2)}$, such that

$$P_{F,G}^{(2)}(a,b)F(a,b) + Q_{F,G}^{(2)}(a,b)G(a,b) \tag{4.2.6}$$

equals $m_{F,G}^{(2)}$ times a power of a.

Explicitly, when $(F,G) =\in \left\{(A_7', B_7'), (B_7', C_7), (C_7, \frac{\partial}{\partial a}C_7)\right\}$, we have

$$\begin{aligned}
P_{A_7',B_7'}^{(1)}(a,b) &= 2\left(13a^3 + 6776a^2b - 121422ab^2 - 303555b^3\right), \\
Q_{A_7',B_7'}^{(1)}(a,b) &= -3\left(13a - 2961b\right), \\
P_{A_7',B_7'}^{(2)}(a,b) &= -2\left(1835a^3 - 44037a^2b + 23373ab^2 - 259308b^3\right), \\
Q_{A_7',B_7'}^{(2)}(a,b) &= -9\left(303a - 980b\right), \\
P_{B_7',C_7}^{(1)}(a,b) &= 1763a - 239b, \\
Q_{B_7',C_7}^{(1)}(a,b) &= 2\left(1763a^3 + 911232a^2b - 20484450ab^2 + 27625563b^3\right), \\
P_{B_7',C_7}^{(2)}(a,b) &= -\left(13a + 20b\right), \text{ and} \\
Q_{B_7',C_7}^{(2)}(a,b) &= 2\left(10571a^3 - 17325a^2b + 76293ab^2 + 185220b^3\right), \\
P_{C_7,\frac{\partial}{\partial a}C_7}^{(1)}(a,b) &= 2^2, \\
Q_{C_7,\frac{\partial}{\partial a}C_7}^{(1)}(a,b) &= -(2a - b), \\
P_{C_7,\frac{\partial}{\partial a}C_7}^{(2)}(a,b) &= 1, \\
Q_{C_7,\frac{\partial}{\partial a}C_7}^{(2)}(a,b) &= 13a - 7b,
\end{aligned} \tag{4.2.7}$$

so

$$\begin{aligned} m^{(1)}_{A'_7,B'_7} &= 2^4 \cdot 3^3 \cdot 7^8 \text{ and } m^{(2)}_{A'_7,B'_7} = 2^4 \cdot 3 \cdot 7^3, \\ m^{(1)}_{B'_7,C_7} &= 2^4 \cdot 3^3 \cdot 7^7 \text{ and } m^{(2)}_{B'_7,C_7} = 2^4 \cdot 3^3 \cdot 7^2, \text{ and} \\ m^{(1)}_{C_7,\frac{\partial}{\partial a}C_7} &= 3^3 \text{ and } m^{(2)}_{C_7,\frac{\partial}{\partial a}C_7} = 3^3. \end{aligned} \tag{4.2.8}$$

Let p be a prime not dividing $m^{(i)}_{F,G}$ for each $F \neq G$ chosen from $\{A'_7, B'_7, C_7\}$ and $i \in \{1,2\}$. In other words, $p \neq 2, 3, 7$. Let a and b be coprime integers, and suppose v is a positive integer such that $p^v \mid \operatorname{tmd}(A(a,b), B(a,b))$.

Suppose by way of contradiction that $p^{2v} \nmid C_7(a,b)$. We must have $p \mid A'_7(a,b), B'_7(a,b)$, and this implies

$$p \mid P^{(1)}_{A'_7,B'_7}(a,b)A'_7(a,b) + Q^{(1)}_{A'_7,B'_7}(a,b)B'_7(a,b) = 2^4 \cdot 3^3 \cdot 7^8 \cdot b^5, \tag{4.2.9}$$

so $p \mid b^5$. Similarly, $p \mid a^5$, but $\gcd(a,b) = 1$, so we have obtained a contradiction, and we conclude $p^{2v} \mid C_7(a,b)$. Now it $p^{3v} \nmid C_7(a,b)$, then $p \mid B'_7(a,b), C_7(a,b)$, and an argument of exactly the same style using $P^{(1)}_{B'_7,C_7}, Q^{(1)}_{B'_7,C_7}, P^{(2)}_{B'_7,C_7}, Q^{(2)}_{B'_7,C_7}$ gives us another contradiction. We conclude that $p^{3v} \mid C_7(a,b)$ as desired. Finally, comparing $C_7(a,b)$ against $\frac{\partial}{\partial a}C_7(a,b) = 2a+b$, we find that if p divides the former integer it cannot divide the latter, and we have proven our lemma in the case $p \neq 2, 3, 7$.

Now let $p = 2$. A short computation confirms that for a and b coprime, $B'_7(a,b) \not\equiv 0 \pmod 2$ and $C_7(a,b) \not\equiv 0 \pmod 2$, so our claim holds vacuously in this case. □

This proof gives bounds on the discrepancy e' between the largest cube dividing $C_7(a,b)$ and cube of the twist minimality defect. Indeed, if $C_7(a,b) = e_0^3 n_0$ with n_0 cubefree, and $\operatorname{tmd}(A_7(a,b), B_7(a,b)) = e_0 e'$, then

$$(e')^3 \mid \operatorname{lcm}(m^{(1)}_{A'_7,B'_7}, m^{(2)}_{A'_7,B'_7}) \cdot \operatorname{lcm}(m^{(1)}_{B'_7,C_7}, m^{(2)}_{B'_7,C_7}) = 2^8 \cdot 3^6 \cdot 7^{15}. \tag{4.2.10}$$

In conjunction with the last paragraph of our second proof, we conclude

$$e' \mid 3^2 \cdot 7^5. \tag{4.2.11}$$

This bound is not sharp, as we shall see.

Definition 4.2.12. For $e \in \mathbb{Z}_{>0}$, let $\widetilde{\mathcal{T}}_7(e)$ denote the image of

$$\big\{(a,b) \in \mathbb{Z}^2 : (a,b) \text{ 7-groomed},\ e \mid \operatorname{tmd}(A_7(a,b), B_7(a,b))\big\} \tag{4.2.13}$$

under the projection

$$\mathbb{Z}^2 \to (\mathbb{Z}/e^3\mathbb{Z})^2, \tag{4.2.14}$$

and let $\widetilde{T}_7(e) := \#\widetilde{\mathcal{T}}_7(e)$. Similarly, let $\mathcal{T}_7(e)$ denote the image of

$$\big\{t \in \mathbb{Z} : e^2 \mid g_7(t) \text{ and } e^3 \mid g_7(t)\big\} \tag{4.2.15}$$

under the projection

$$\mathbb{Z} \to \mathbb{Z}/e^3\mathbb{Z}, \tag{4.2.16}$$

and let $T_7(e) := \#\mathcal{T}_7(e)$.

Lemma 4.2.17. *The following statements hold.*

(a) $\widetilde{\mathcal{T}}_7(e)$ *consists of those pairs* $(a,b) \in (\mathbb{Z}/e^3\mathbb{Z})^2$ *which satisfy the following conditions:*

- $A_7(a,b) \equiv 0 \pmod{e^2}$ *and* $B_7(a,b) \equiv 0 \pmod{e^3}$, *and*
- $\ell \nmid \gcd(a,b)$ *for all primes* $\ell \mid e$.

(b) *Let* $(a,b) \in \mathbb{Z}^2$. *If* $(a,b) \pmod{e^3} \in \widetilde{\mathcal{T}}_7(e)$ *then* $e \mid \operatorname{tmd}(A_7(a,b), B_7(a,b))$.

(c) *The functions* $\widetilde{T}_7(e)$ *and* $T_7(e)$ *are multiplicative, and* $\widetilde{T}_7(e) = \varphi(e^3)T_7(e)$.

(d) *For all prime $\ell \neq 3, 7$ and all $v \geq 1$, we have*

$$T_7(\ell^v) = T_7(\ell) = 1 + \left(\frac{\ell}{3}\right). \tag{4.2.18}$$

(e) *We have*

$$T_7(3) = 2 \cdot 3^2 = 18,\ T_7(3^2) = 3^3 = 27,\ \textit{and}\ \ T_7(3^v) = 0\ \textit{for}\ v \geq 3. \tag{4.2.19}$$

We also have

$$T_7(7) = 1 + 7^2 = 50,\ T_7(7^2) = 1 + 7^4 = 2402,\ \textit{and}\ \ T_7(7^v) = 1 + 7^7 = 823544\ \textit{for}\ v \geq 3. \tag{4.2.20}$$

(f) *We have $T_7(e) = O(2^{\omega(e)})$ for $e \geq 1$, where $\omega(e)$ is the number of distinct prime divisors of e.*

Proof. Parts (a) and (b) are immediate from Definition 4.2.12.

For part (c), 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

$$\begin{aligned} \mathcal{T}_7(\ell^v) \times (\mathbb{Z}/\ell^{3v})^\times &\to \widetilde{\mathcal{T}}_7(\ell^v) \\ (t, u) &\mapsto (tu, u) \end{aligned} \tag{4.2.21}$$

We observe $A(1,0) = -3$ and $B(1,0) = 2$ are coprime, so no pair (a, b) with $b \equiv 0 \pmod{\ell}$ can be a member of $\widetilde{\mathcal{T}}_7(\ell^v)$. Surjectivity of the given map follows, and counting both sides gives the result.

Now part (d). For $\ell \neq 3, 7$, Lemma 4.2.2(a)–(b) yield

$$\mathcal{T}_7(\ell^v) = \left\{t \in \mathbb{Z}/\ell^{3v}\mathbb{Z} : h_7(t) \equiv 0 \pmod{\ell^{3v}}\right\}. \tag{4.2.22}$$

By Lemma 4.2.2(c), $h_7(t) \equiv 0 \pmod{\ell}$ implies $\frac{\mathrm{d}}{\mathrm{d}t} h_7(t) \not\equiv 0 \pmod{\ell}$, so Hensel's lemma applies and we need only count roots of $h_7(t)$ modulo ℓ. By quadratic reciprocity, this count is

$$1 + \left(\frac{-3}{\ell}\right) = 1 + \left(\frac{\ell}{3}\right) = \begin{cases} 2, & \text{if } \ell \equiv 1 \pmod{3}; \\ 0, & \text{else.} \end{cases} \tag{4.2.23}$$

Next, part (e). For $\ell = 3$, we just compute $T_7(3) = 18$, $T_7(3^2) = 27$, and $T_7(3^3) = 0$; the observation $T_7(3^3) = 0$ implies $T_7(3^v) = 0$ for all $v \geq 3$. For $\ell = 7$, we compute

$$T_7(7) = 1 + 7^2,\ T_7(7^2) = 1 + 7^4,\ T_7(7^3) = \cdots = T_7(7^6) = 1 + 7^7. \tag{4.2.24}$$

Hensel's lemma still applies to $h_7(t)$: let t_0, t_1 be the roots of $h_7(t)$ in $\mathbb{Z}_7$ with $t_0 := 248\,044 \pmod{7^7}$ (so that $t_1 = -1 - t_0$). We claim that

$$\mathcal{T}_7(7^{3v}) = \{t_0\} \sqcup \left\{ t_1 + 7^{3v-7} u \in \mathbb{Z}/7^{3v}\mathbb{Z} : u \in \mathbb{Z}/7^7\mathbb{Z} \right\}, \tag{4.2.25}$$

for $3v \geq 7$. Indeed, $g_7'(t_1) \equiv 0 \pmod{7^7}$, so we can afford to approximate t_1 modulo 7^{3v-7}. As $g_7(t_0) \not\equiv 0 \pmod{7}$ and $g_7(t_1) \not\equiv 0 \pmod{7^8}$, no other values of t suffice. Thus $T_7(7^{3v}) = 1 + 7^7 = 823544$.

Finally, part (f). From (c)–(e) we conclude

$$T_7(e) \leq \frac{27 \cdot 823\,544}{4} \cdot \prod_{\substack{\ell \mid e \\ \ell \neq 3,7}} \left(1 + \left(\frac{\ell}{3}\right)\right) \leq 5\,558\,922 \cdot 2^{\omega(e)} \tag{4.2.26}$$

so $T_7(e) = O(2^{\omega(e)})$ as claimed. □

The common factor $C_7(a,b)$

In view of Lemma 4.2.2, the twist minimality defect away from the primes $2, 3, 7$ is determined by the quadratic form $C_7(a,b) = a^2 + ab + 7b^2 = b^2 h_7(a/b)$. We define

$$\mathcal{C}_7(e) := \left\{(a,b) \in \mathbb{Z}^2 : C_7(a,b) = e \text{ and } \gcd(a,b) = 1\right\}, \tag{4.2.27}$$

and note $\#\mathcal{C}_7(e) \leq 2^{\omega(e)+1}$.

Fortunately, $C_7(a,b)$ is the norm form of a quadratic order of class number 1, namely $\mathbb{Z}[3\zeta_6]$, where ζ_6 is a primitive 6th root of unity. We record some elementary algebraic observations about $C_7(a,b)$ and the order $\mathbb{Z}[3\zeta_6]$.

Lemma 4.2.28. *The following statements hold.*

(a) *The right regular representation of $\mathbb{Z}[\zeta_6]$ in the basis $\{1, -1 + 3\zeta_6\}$ induces the map $\gamma_7 : \mathbb{Z}^2 \to \mathrm{M}_2(\mathbb{Z})$ given by*

$$\gamma_7 : (a,b) \mapsto \begin{pmatrix} a & b \\ -7b & a+b \end{pmatrix}. \tag{4.2.29}$$

(b) *For all $a, b, c, d, e \in \mathbb{Z}$, we have the following implication:*

$$C_7(a,b) = e \implies e \mid C_7((c,d) \cdot \gamma_7(a,b)). \tag{4.2.30}$$

(c) *Conversely, if c', d', e, k are integers such that $k \geq 1$, $e^k \mid C_7(c', d')$, and*

$$\gcd(c', d', e) = \gcd(3, e) = 1, \tag{4.2.31}$$

then there are integers $a, b, c, d \in \mathbb{Z}$ with $(a, b) \in \mathcal{C}_7(e)$ and

$$(c', d') = (c, d) \cdot \gamma_7(a, b)^k. \tag{4.2.32}$$

Proof. Part (a) is a short computation.

Part (b) follows from the observation that $C_7(a, b)$ is the norm on $\mathbb{Z}[3\zeta_6]$ in the basis $\{1, -1 + 3\zeta_6\}$.

Let $e, k \in \mathbb{Z}_{>0}$ and $\alpha' \in \mathbb{Z}[\zeta_6]$. Part (c) will follow if we can prove the following statement. If no inert prime divides both e and $\alpha' \in \mathbb{Z}[3\zeta_6]$, $e \mid \mathrm{Nm}(\alpha')$, and $\gcd(3, e) = 1$, then there are algebraic integers $\alpha, \beta \in \mathbb{Z}[3\zeta_6]$ such that $\alpha' = \alpha\beta^k$ and $\mathrm{Nm}(\beta) = e$.

We now prove this assertion. The order $\mathbb{Z}[3\zeta_6]$ is a suborder of the Euclidean domain $\mathbb{Z}[\zeta_6]$ of conductor 3, and it inherits the following almost unique factorization: up to sign, every nonzero $\alpha \in \mathbb{Z}[3\zeta_6]$ can be written uniquely as

$$\alpha = \beta\pi_1^{e_1} \cdots \pi_r^{e_r}, \tag{4.2.33}$$

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.

Write

$$\alpha' = \beta'\pi_1^{e_1} \cdots \pi_r^{e_r}. \tag{4.2.34}$$

As every prime dividing both α' and e splits, $\mathrm{Nm}(\pi_j) = p_j$ is a rational prime whenever $\pi_j \mid e$. Moreover, because $\gcd(c', d', e) = 1$, if p prime divides e then $\mathrm{Nm}(\pi_i) = \mathrm{Nm}(\pi_j) = p$ implies $\pi_i = \pi_j$. Write $e = \prod_{j=1}^r p_j^{f_j}$, and let $\beta = \prod_{j=1}^r \pi_j^{f_j}$. Necessarily, $\beta^k \mid \alpha'$; letting $\alpha = \beta' \prod_{j=1}^r \pi_j^{e_j - kf_j}$, our claim follows. □

The twist minimality defect measures the disparity between $H(A, B)$ and $\mathrm{twht}(A, B)$: this disparity cannot be too large compared to $C_7(a, b)$, as the following theorem shows.

Theorem 4.2.35. *The following statements hold.*

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

$$108C_7(a,b)^6 \leq H(A_7(a,b),B_7(a,b)) \leq \kappa_7 C_7(a,b)^6, \tag{4.2.36}$$

where the constant $\kappa_7 = 311\,406\,871.990\,204\ldots$ is an algebraic number given by evaluating $H(A_7(a,b),B_7(a,b))$ at appropriate roots of (4.2.38).

(b) *If $C_7(a,b) = e_0^3 n_0$, with n_0 cubefree, then $\operatorname{tmd}(A_7(a,b),B_7(a,b)) = e_0 e'$ for some $e' \mid 3 \cdot 7^3$, and*

$$\frac{2^2}{3^3 \cdot 7^{18}} e_0^{12} n_0^6 \leq \operatorname{twht}(A_7(a,b),B_7(a,b)) \leq \kappa_7 e_0^{12} n_0^6. \tag{4.2.37}$$

Proof. We first prove (a). We wish to find the extrema of $H(A_7(a,b),B_7(a,b))/C_7(a,b)^6$. As this expression is homogeneous of degree 0, and $C_7(a,b)$ is positive definite, we may assume without loss of generality that $C_7(a,b) = 1$. Using the theory of Lagrange multipliers, and examining the critical points of $H(A_7(a,b),B_7(a,b))$ subject to $C_7(a,b) = 1$, we verify that (4.2.36) holds. Moreover, the lower bound is attained at $(1,0)$, and the upper bound is attained when a and b are appropriately chosen roots of

$$\begin{aligned}
&1296a^8 - 2016a^6 + 2107a^4 - 1596a^2 + 252\\
=&2^4 \cdot 3^4 \cdot a^8 - 2^5 \cdot 3^2 \cdot 7 \cdot a^6 + 7^2 \cdot 43 \cdot a^4 - 2^2 \cdot 3 \cdot 7 \cdot 19 \cdot a^2 + 2^2 \cdot 3^2 \cdot 7, \text{ and}\\
&1\,067\,311\,728b^8 - 275\,298\,660b^6 + 43\,883\,077b^4 - 3\,623\,648b^2 + 1849\\
=&2^4 \cdot 3^4 \cdot 7^7 \cdot b^8 - 2^2 \cdot 3^2 \cdot 5 \cdot 7^6 \cdot 13 \cdot b^6 + 7^6 \cdot 373 \cdot b^4 - 2^5 \cdot 7^2 \cdot 2311 \cdot b^2 + 43^2
\end{aligned} \tag{4.2.38}$$

respectively. For $(a,b) = (0.450\,760\,996\,604\,693\,04\ldots, -0.371\,118\,011\,382\,744\,86\ldots)$, the arguments that maximize the ratio

$$H(A_7(a,b),B_7(a,b))/C_7(a,b)^6, \tag{4.2.39}$$

we have $27\,|B_7(a,b)|^2 > 4\,|A_7(a,b)|^3$.

We now prove (b). Write $C_7(a,b) = e_0^3 n_0$ with n_0 cubefree, and write

$$\operatorname{tmd}(A_7(a,b), B_7(a,b)) = e_0 e'. \tag{4.2.40}$$

By Lemma 4.2.2, $e' = 3^v \cdot 7^w$ for some $v, w \geq 0$; a short computation shows $v \in \{0,1\}$, and (4.2.25) shows $w \leq \lceil 7/3 \rceil = 3$.

As

$$H(A_7(a,b), B_7(a,b)) = e_0^6\,(e')^6 \operatorname{twht}(A_7(a,b), B_7(a,b)), \tag{4.2.41}$$

we see

$$\frac{108}{(e')^6} e_0^{12} n_0^6 \leq \operatorname{twht}(A_7(a,b), B_7(a,b)) \leq \frac{\kappa_7}{(e')^6} e_0^{12} n_0^6. \tag{4.2.42}$$

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

Unsurprisingly, Theorem 4.2.35 shows that the bound on e' given by (4.2.11) is not sharp.

Corollary 4.2.43. *Let (a,b) be a 7-groomed pair. We have*

$$\operatorname{tmd}(A_7(a,b), B_7(a,b)) \leq \frac{3^{5/4} \cdot 7^{9/2}}{2^{1/6}} \operatorname{twht}(A_7(a,b), B_7(a,b))^{1/12} \tag{4.2.44}$$

where $3^{5/4} \cdot 7^{9/2}/2^{1/6} = 22\,344.227\,186\ldots$

Proof. In the notation of Theorem 4.2.35(c),

$$e_0^{12} m^6 \leq \frac{3^3 \cdot 7^{18}}{2^2} \operatorname{twht}(A_7(a,b), B_7(a,b)). \tag{4.2.45}$$

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. □

Remark 4.2.46. We could instead prove Theorem 4.2.35(a) as follows. We assume without loss of generality that $C_7(a,b) = 1$. Now the level set

$$\left\{(a,b) \in \mathbb{R}^2 : C_7(a,b) = a^2 + ab + 7b^2 = 1\right\} \tag{4.2.47}$$

is parameterized by the function

$$\phi : \theta \mapsto \left(\cos\theta - \frac{1}{3\sqrt{3}}\sin\theta, \frac{2}{3\sqrt{3}}\sin\theta\right). \tag{4.2.48}$$

We can now use a computer to show

$$\begin{aligned} &\min_\theta H(A_7(\phi(\theta)), B_7(\phi(\theta))) = 108, \text{and} \\ &\max_\theta H(A_7(\phi(\theta)), B_7(\phi(\theta))) =: \kappa_7 = 311\,406\,871.990\,204\ldots, \end{aligned} \tag{4.2.49}$$

with the minimum attained when $t = 0$ and $(a,b) = (1,0)$, and the maximum attained when $t = 4.980\,802\,4\ldots$ and $(a,b) = (0.450\ldots, -0.371 ldots)$. It is straightforward to show $H(A_7(1,0), B_7(1,0)) = 108$ but

$$\frac{H(A_7(a,1), B_7(a,1))}{C(a,1)^6} > 108 \tag{4.2.50}$$

for all a, so this minimum value is exact. This argument does not express κ_7 as an algebraic number, however.

Section 4.3
Estimates for twist classes for $m = 7$

In this section, we use section 3.5 to estimate $N_7^{\mathrm{tw}}(X)$, counting the number of twist minimal elliptic curves over $\mathbb{Q}$ admitting a cyclic 7-isogeny.

Recall (3.5.6), as well as (3.5.33) and (3.5.34). By section 3.2, $M_7(X; e)$ counts pairs $(a, b) \in \mathbb{Z}^2$ with

- (a, b) 7-groomed,
- $H(A_7(a, b), B_7(a, b)) \leq X$, and
- $e \mid \operatorname{tmd}(A_7(a, b), B_7(a, b))$.

The following proposition refines Lemma 3.5.7, and specifies both an order of growth and an explicit upper bound past which the summands of (3.5.8) vanish when $m = 7$.

Proposition 4.3.1. *We have*

$$N_7^{\mathrm{tw}}(X) = \sum_{n \ll X^{1/12}} \sum_{e \mid n} \mu(n/e) M_7(e^6 X; n); \tag{4.3.2}$$

more precisely, we can restrict our sum to

$$n \leq \frac{3^{5/4} \cdot 7^{9/2}}{2^{1/6}} \cdot X^{1/12}. \tag{4.3.3}$$

Proof. Let $(a, b) \in \mathbb{Z}^2$, and suppose

$$H(A_7(a, b), B_7(a, b)) \leq e^6 X \text{ and } e \mid \operatorname{tmd}(A_7(a, b), B_7(a, b)). \tag{4.3.4}$$

If we can prove

$$e \leq \frac{3^{5/4} \cdot 7^{9/2}}{2^{1/6}} \cdot X^{1/12}, \tag{4.3.5}$$

then our claim will follow.

Write $C_7(a, b) = e_0^3 n_0$, with n_0 cube-free. By Theorem 4.2.35(a), we have

$$108 e_0^{18} n_0^6 \leq e^6 X. \tag{4.3.6}$$

On the other hand, by Theorem 4.2.35(b), we have $e \mid 3 \cdot 7^3 \cdot e_0$, and *a fortiori*

$$e \leq 3 \cdot 7^3 e_0. \tag{4.3.7}$$

Multiplying (4.3.6) through by $(3 \cdot 7^3)^{18}$ and utilizing (4.3.7), we conclude

$$2^2 \cdot 3^3 e^{18} \cdot n_0^6 \leq 3^{18} \cdot 7^{54} e^6 X. \tag{4.3.8}$$

Rounding n_0 down to 1 and rearranging, we obtain (4.3.5). □

Recall that a pair $(a, b) \in \mathbb{Z}^2$ is 7-groomed if $\gcd(a, b) = 1$, $b > 0$, and $a/b \notin \mathscr{C}_7 = \{-7, \infty\}$ (see Definition 3.2.19 and Table 3.2.13). In order to estimate $M_7(X; e)$, we further unpack the 7-groomed condition on pairs (a, b). We therefore let $M_7(X; d, e)$ denote the number of pairs $(a, b) \in \mathbb{Z}^2$ with

- $\gcd(da, db, e) = 1$, $b > 0$, and $a/b \notin \mathscr{C}_7$,
- $H(A_7(da, db), B_7(da, db)) \leq X$, and
- $e \mid \operatorname{tmd}(A_7(da, db), B_7(da, db))$.

By Theorem 4.2.35, and because $H(A_7(a, b), B_7(a, b))$ is homogeneous of degree 12, a Möbius sieve yields

$$M_7(X; e) = \sum_{\substack{d \ll X^{1/12} \\ \gcd(d,e)=1}} \mu(d) M_7(X; d, e); \tag{4.3.9}$$

more precisely, we can restrict our sum to

$$d \leq \frac{1}{2^{1/6} \cdot 3^{1/4}} \cdot X^{1/12}. \tag{4.3.10}$$

Before proceeding, we give an outline of the argument employed in this section. In Lemma 4.3.16, we use the Principle of Lipschitz to estimate $M_7(X; d, e)$, then piece these estimates together using (4.3.9) to estimate $M_7(X;e)$. Heuristically,

$$M_7(X;d,e) \sim \frac{R_7 T_7(e) X^{1/6}}{d^2 e^3} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell}\right) \tag{4.3.11}$$

(where R_7 is the area of (3.3.5) when $m = 7$ and T_7 is the arithmetic function investigated in Lemma 4.2.17) by summing over the congruence classes modulo e^3 that satisfy $e \mid \operatorname{tmd}(A_7(da,db), B_7(da,db))$. Then (4.3.9) suggests

$$M_7(X;e) \sim \frac{R_7 T_7(e) X^{1/6}}{\zeta(2) e^3 \prod_{\ell \mid e} \left(1 + \frac{1}{\ell}\right)}. \tag{4.3.12}$$

Substituting (4.3.12) into Lemma 3.5.7, we obtain the heuristic estimate

$$N_7^{\mathrm{tw}}(X) \sim \frac{Q_7 R_7 X^{1/6}}{\zeta(2)}, \tag{4.3.13}$$

where

$$Q_7 := \sum_{n \geq 1} \frac{T_7(n) \varphi(n)}{n^3 \prod_{\ell \mid n} \left(1 + \frac{1}{\ell}\right)}. \tag{4.3.14}$$

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 (4.3.2) in accordance with Definition 3.5.17, so

$$N_7^{\mathrm{tw}}(X) = N_{7,\leq y}^{\mathrm{tw}}(X) + N_{7,>y}^{\mathrm{tw}}(X). \tag{4.3.15}$$

We then estimate $N_{7,\leq y}^{\mathrm{tw}}(X)$ in Proposition 4.3.42, and treat $N_{7,>y}^{\mathrm{tw}}(X)$ as an error term which we bound in Lemma 4.3.60. Setting the error from our estimate equal to the error arising from $N_{7,>y}^{\mathrm{tw}}(X)$, we obtain Theorem 4.3.57.

In the remainder of this section, we follow the outline suggested here by successively estimating $M_7(X;d,e)$, $M_7(X;e)$, $N_{7,\leq y}^{\mathrm{tw}}(X)$, $N_{7,>y}^{\mathrm{tw}}(X)$, and finally $N_7^{\mathrm{tw}}(X)$.

We first estimate $M_7(X;d,e)$ and $M_7(X;e)$.

Lemma 4.3.16. *The following statements hold.*

(a) *If* $\gcd(d, e) > 1$*, then* $M_7(X; d, e) = 0$*. If* $\gcd(d, e) = 1$*, we have*

$$M_7(X; d, e) = \frac{R_7 T_7(e) X^{1/6}}{d^2 e^3} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell}\right) + O\left(\frac{2^{\omega(e)} X^{1/12}}{d e^{3/2}}\right) \tag{4.3.17}$$

for $X, d, e \geq 1$*. Here,* R_7 *is the area of* (3.3.5) *when* $m = 7$*.*

(b) *We have*

$$M_7(X; e) = \frac{R_7 T_7(e) X^{1/6}}{\zeta(2) e^3 \prod_{\ell \mid e} \left(1 + \frac{1}{\ell}\right)} + O\left(\frac{2^{\omega(e)} X^{1/12} \log X}{e^{3/2}}\right) \tag{4.3.18}$$

for $X \geq 2$*,* $d, e \geq 1$*.*

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

We give two partial proofs of Lemma 4.3.16. The first proof gives an intuitive interpretation of the coefficient of $X^{1/6}$, and generalizes readily to other elliptic surfaces with type II additive reduction, but yields only a degraded error term. The second proof leverages the observation that $C_7(a, b)$ is the norm of the order $\mathbb{Z}[3\zeta_6]$ to give the full error term, but does not make the leading coefficient as explicit.

First proof of Lemma 4.3.16. We begin with (a) and examine the summands $M_7(X; d, e)$. If d and e are not coprime, then $M_7(X; d, e) = 0$ 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 $M_7(X; 1, e)$ to the pairs counted by $M_7(d^{12}X; d, e)$ given by $(a, b) \mapsto (da, db)$.

Combining Lemma 4.2.17(c) and Corollary 3.3.11, we have

$$\begin{aligned} M_7(X;1,e) &= \sum_{(a_0,b_0)\in\widetilde{\mathcal{T}}_7(e)} \#\{(a,b)\in\mathcal{R}_7(X)\cap\mathbb{Z}^2 : (a,b)\equiv(a_0,b_0) \pmod{e^3}, (a,b)\notin\mathscr{C}_7\} \\ &= \varphi(e^3)T_7(e)\left(\frac{R_7X^{1/6}}{e^6}+O\left(\frac{X^{1/12}}{e^3}\right)\right) \\ &= \frac{R_7T_7(e)X^{1/6}}{e^3}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)+O(T_7(e)X^{1/12}). \end{aligned} \tag{4.3.19}$$

Scaling by d and invoking Lemma 4.2.17(f), we obtain

$$M_7(X;d,e) = \frac{R_7T_7(e)X^{1/6}}{d^2e^3}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)+O\left(\frac{2^{\omega(e)}X^{1/12}}{d}\right). \tag{4.3.20}$$

For part (b), we compute

$$\begin{aligned} M_7(x;e) &= \sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}} \mu(d)M_7(X;d,e) \\ &= \sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}} \mu(d)\left(\frac{T_7(e)R_7X^{1/6}}{d^2e^3}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)+O\left(\frac{2^{\omega(e)}X^{1/12}}{d}\right)\right) \\ &= \frac{R_7T_7(e)X^{1/6}}{e^3}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)\sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}}\frac{\mu(d)}{d^2}+O\left(2^{\omega(e)}X^{1/12}\sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}}\frac{1}{d}\right). \end{aligned} \tag{4.3.21}$$

We plug the straightforward estimates

$$\sum_{\substack{d\ll X^{1/12}\\ \gcd(d,e)=1}}\frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)}\prod_{\ell\mid e}\left(1-\frac{1}{\ell^2}\right)^{-1}+O(X^{-1/12}) \tag{4.3.22}$$

and

$$\sum_{d \leq X^{1/12}} \frac{1}{d} = \frac{1}{12} \log X + O(1) \tag{4.3.23}$$

into (4.3.21), along with Lemma 4.2.17(f). Simplifying now gives

$$M_7(x; e) = \frac{R_7 T_7(e) X^{1/6}}{\zeta(2) e^3 \prod_{\ell \mid e} \left(1 + \frac{1}{\ell}\right)} + O(2^{\omega(e)} X^{1/12} \log X) \tag{4.3.24}$$

proving (b) with a degraded error term. □

We now give our second proof of Lemma 4.3.16.

Second proof of Lemma 4.3.16. As in the previous proof, we may restrict our attention to $M_7(X; 1, e)$. Throughout this proof, d will not refer to the second argument of $M_7(X; d, e)$.

Let $e \in \mathbb{Z}_{>0}$, and let e_0 be the smallest integer for which $e \mid 3{\cdot}7^3 e_0$. By Theorem 4.2.35(b), if $e \mid \operatorname{tmd}(A_7(a, b), B_7(a, b))$, then $e_0^3 \mid C_7(a, b)$. By Lemma 4.2.28(b), if $\gcd(3, e_0) = 1$, we have the following implications for all $a_0, b_0, c, d \in \mathbb{Z}$:

$$C_7(a_0, b_0) = e_0 \implies e_0^3 \mid C_7((c, d) \cdot \gamma_7(a_0, b_0)^3), \tag{4.3.25}$$

where $\gamma_7 : \mathbb{Z}^2 \to \mathrm{M}_2(\mathbb{Z})$ is defined in (4.2.29). By Lemma 4.2.28(c), if $\gcd(c', d', e_0) = 1$, we also have the converse implication

$$e_0^3 \mid C_7(c', d') \implies (c', d') = (c, d) \cdot \gamma_7(a_0, b_0)^3 \tag{4.3.26}$$

for some $(a_0, b_0) \in \mathcal{C}_7(e_0)$ and $(c, d) \in \mathbb{Z}$. Our aim is to use (4.3.25) and (4.3.26), in tandem with Corollary 3.3.37, to improve on the error term given in the last proof.

For $e \geq 1$, let $\widetilde{\mathcal{T}}_7(a_0, b_0, e)$ denote the image of

$$\left\{(c', d') \in \mathbb{Z}^2 \cdot \gamma_7(a_0, b_0)^3 : e \mid \operatorname{tmd}(A_7(c', d'), B_7(c', d') \text{ and } (c', d') \text{ 7-groomed}\right\} \tag{4.3.27}$$

under the projection

$$\mathbb{Z}^2 \to (\mathbb{Z}/e^3\mathbb{Z})^2. \tag{4.3.28}$$

We also let $\widetilde{T}_7(a_0, b_0, e) := \#\widetilde{\mathcal{T}}_7(a_0, b_0, e)$. If $e_0 \mid e$, we have the straightforward equality

$$\#\left(e_0^3\mathbb{Z}/e^3\mathbb{Z}\right) = e^3/e_0^3. \tag{4.3.29}$$

Thus if $C_7(a_0, b_0) = e_0$ and e/e_0 is an integer dividing $3 \cdot 7^3$, we have the bound $\widetilde{T}_7(a_0, b_0, e) \leq 3^6 \cdot 7^{18}$.

If $\gcd(3^2, e) > 3$, then $M_7(X; 1, e) = 0$ by Lemma 4.2.17. Otherwise, we let e_0 be the smallest integer for which $e \mid 3 \cdot 7^3 \cdot e_0$. In this case, $M_7(X; 1, e)$ is the sum over $(a_0, b_0) \in \mathcal{C}_7(e_0)$ and $(c_0, d_0) \in \widetilde{\mathcal{T}}_7(a_0, b_0, e)$ of

$$\#\left\{(c', d') \in \mathcal{R}_7(X) \cap (\mathbb{Z}^2 \cdot \gamma_7(a_0, b_0)^3) : (c', d') \equiv (c_0, d_0) \pmod{e^3},\ c'/d' \notin \mathscr{C}_7\right\}. \tag{4.3.30}$$

By Corollary 3.3.37, we therefore have

$$M_7(X; 1, e) = \sum_{(a_0,b_0)\in\mathcal{C}_7(e_0)} \sum_{(c_0,d_0)\in\widetilde{\mathcal{T}}_7(a_0,b_0,e)} \left(\frac{R_7 X^{1/6}}{(\det \gamma_7(a_0, b_0))^3} + O\left(\frac{X^{1/12}}{\sigma(\gamma_7(a_0, b_0))^3}\right)\right). \tag{4.3.31}$$

But $\det \gamma_7(a_0, b_0) = e_0$ by assumption, and on the other hand the singular values of $\gamma_7(a_0, b_0)$ are

$$\sigma_\pm(a_0, b_0) = \left(\frac{2a_0^2 + 2a_0b_0 + 51b_0^2 \pm b_0\sqrt{148a_0^2 + 148a_0b_0 + 2405b_0^2}}{2}\right)^{1/2}. \tag{4.3.32}$$

We use Lagrange multipliers to find the extrema of $\sigma_-(a_0, b_0)$ subject to the constraint

$C_7(a_0, b_0) = 1$, and thus of $\sigma_-(a_0, b_0)/C_7(a_0, b_0)^{1/2}$. We thereby obtain

$$\left(\frac{101 - 16\sqrt{37}}{27}\right)^{1/2} e_0^{1/2} \leq \sigma_-(\gamma_7(a_0, b_0)) \leq \left(\frac{101 + 16\sqrt{37}}{27}\right)^{1/2} e_0^{1/2}. \tag{4.3.33}$$

These extrema are both attained when $a_0/b_0 = -1/2$.

Now as $\#\mathcal{C}_7(e_0) = O(2^{\omega(e)})$ and $\widetilde{T}_7(a_0, b_0, e) = O(1)$, we have

$$M_7(X; 1, e) = \frac{R_7 X^{1/6}}{e_0^3} \sum_{(a_0, b_0) \in \mathcal{C}_7(e_0)} \widetilde{T}_7(a_0, b_0, e) + O\left(2^{\omega(e)} \frac{X^{1/12}}{e^{3/2}}\right). \tag{4.3.34}$$

By considering the limit

$$\lim_{X \to \infty} \frac{M_7(X; 1, e)}{X^{1/6}}, \tag{4.3.35}$$

we deduce

$$\frac{R_7}{e_0^3} \sum_{(a_0, b_0) \in \mathcal{C}_7(e_0)} \widetilde{T}_7(a_0, b_0, e) = \frac{R_7 T_7(e)}{e^3}. \tag{4.3.36}$$

We turn our attention at last to $M_7(X; d, e)$: scaling by d as in the previous proof, we conclude

$$M_7(X; d, e) = \frac{R_7 T_7(e) X^{1/6}}{d^2 e^3} \prod_{\ell | e} \left(1 - \frac{1}{\ell}\right) + O\left(2^{\omega(e)} \frac{X^{1/12}}{d e^{3/2}}\right), \tag{4.3.37}$$

where the implicit constant is independent of X, d, and e.

Following the proof of part (b) above, we obtain

$$M_7(X; e) = \frac{R_7 T_7(e) X^{1/6}}{\zeta(2) e^3 \prod_{\ell | e} \left(1 + \frac{1}{\ell}\right)} + O\left(\frac{2^{\omega(e)} X^{1/12} \log X}{e^{3/2}}\right). \tag{4.3.38}$$

□

We let

$$Q_7 := \sum_{n \geq 1} \frac{\varphi(n) T_7(n)}{n^3 \prod_{\ell | n} \left(1 + \frac{1}{\ell}\right)}, \tag{4.3.39}$$

and we let

$$c_7^{\mathrm{tw}} := \frac{Q_7 R_7}{\zeta(2)}. \tag{4.3.40}$$

Here, as always, R_7 is the area of the region

$$\mathcal{R}_7(1) = \left\{(a,b) \in \mathbb{R}^2 : H(A_7(a,b), B_7(a,b)) \leq 1, b \geq 0\right\}. \tag{4.3.41}$$

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

Proposition 4.3.42. *Suppose $y \ll X^{\frac{1}{12}}$. Then*

$$N_{7,\leq y}^{\mathrm{tw}}(X) = c_7^{\mathrm{tw}} X^{1/6} + O\left(\max\left(\frac{X^{1/6}\log y}{y}, X^{1/12}\log X \log^4 y\right)\right) \tag{4.3.43}$$

for $X, y \geq 2$. The constant c_7^{tw} is given in (4.3.40).

Proof. Substituting the asymptotic for $M_7(X;e)$ from Lemma 4.3.16(b) into the defining series (3.5.18) for $N_{7,\leq y}^{\mathrm{tw}}(X)$, we have

$$N_{7,\leq y}^{\mathrm{tw}}(X) = \sum_{n\leq y}\sum_{e|n} \mu\left(n/e\right)\left(\frac{R_7 T_7(n) e X^{1/6}}{\zeta(2) n^3 \prod_{\ell | n}\left(1+\frac{1}{\ell}\right)} + O\left(\frac{2^{\omega(e)} e^{1/2} X^{1/12}\log(e^6 X)}{n^{3/2}}\right)\right). \tag{4.3.44}$$

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

$$\begin{aligned}\sum_{n\leq y}\sum_{e|n} \mu\left(n/e\right)\frac{R_7 T_7(n) e X^{1/6}}{\zeta(2) n^3 \prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} &= \frac{R_7 X^{1/6}}{\zeta(2)}\sum_{n\leq y}\frac{T_7(n)}{n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)}\sum_{e|n}\mu\left(n/e\right)e \\ &= \frac{R_7 X^{1/6}}{\zeta(2)}\sum_{n\leq y}\frac{\varphi(n) T_7(n)}{n^3\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)}.\end{aligned} \tag{4.3.45}$$

By Lemma 4.2.17(f), we see

$$\frac{\varphi(n)T_7(n)}{n^3\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}=O\left(\frac{2^{\omega(n)}}{n^2}\right). \tag{4.3.46}$$

By Corollary 3.4.6 and Corollary 3.4.42, we have

$$\sum_{n>y}\frac{2^{\omega(n)}}{n^2}\sim\frac{\log y}{\zeta(2)y}. \tag{4.3.47}$$

A fortiori,

$$\sum_{n>y}\frac{\varphi(n)T_7(n)}{n^3\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}=O\left(\sum_{n>y}\frac{2^{\omega(n)}}{n^2}\right)=O\left(\frac{\log y}{y}\right), \tag{4.3.48}$$

so the series

$$\sum_{n\geq 1}\frac{\varphi(n)T_7(n)}{n^3\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}=Q_7 \tag{4.3.49}$$

is absolutely convergent, and

$$\begin{aligned}\sum_{n\leq y}\sum_{e\mid n}\mu\left(n/e\right)\left(\frac{R_7T_7(n)eX^{1/6}}{\zeta(2)n^3\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}\right)&=\frac{R_7X^{1/6}}{\zeta(2)}\left(Q_7+O\left(\frac{\log y}{y}\right)\right)\\&=c_7^{\mathrm{tw}}X^{1/6}+O\left(\frac{X^{1/6}\log y}{y}\right).\end{aligned} \tag{4.3.50}$$

As the summands of (4.3.49) constitute a nonnegative multiplicative arithmetic function, we can factor Q_7 as an Euler product. For p prime, Lemma 4.2.17 yields

$$Q_7(p):=\sum_{a\geq 0}\frac{\varphi(p^a)T_7(p^a)}{p^{3a}\left(1+\frac{1}{p}\right)}=\begin{cases}1+\dfrac{2}{p^2+1}, & \text{if } p\equiv 1 \pmod 3 \text{ and } p\neq 7;\\ 13/6, & \text{if } p=3;\\ 63/8, & \text{if } p=7;\\ 1 & \text{else.}\end{cases} \tag{4.3.51}$$

Thus

$$Q_7 = \prod_{p \text{ prime}} Q_7(p) = Q_7(3)Q_7(7) \prod_{\substack{p\neq 7 \text{ prime} \\ p\equiv 1 \pmod 3}} \left(1 + \frac{2}{p^2+1}\right). \tag{4.3.52}$$

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

$$\begin{aligned}&\sum_{n\leq y}\sum_{e|n} \mu\left(n/e\right) O\left(\frac{2^{\omega(n)} e^{1/2} X^{1/12} \log\left(e^6 X\right)}{n^{3/2}}\right) \\ =&O\left(X^{1/12}\log X \sum_{n\leq y} \frac{2^{\omega(n)}}{n^{3/2}} \sum_{e|n} \left|\mu\left(n/e\right)\right| e^{1/2}\right).\end{aligned} \tag{4.3.53}$$

The inequality

$$\sum_{e|n} \left|\mu\left(n/e\right)\right| e^{1/2} < 2^{\omega(n)}\sqrt{n} \tag{4.3.54}$$

implies

$$\sum_{n\leq y} \frac{2^{\omega(n)}}{n^{3/2}} \sum_{e|n} \left|\mu\left(n/e\right)\right| e^{1/2} = O\left(\sum_{n\leq y} \frac{4^{\omega(n)}}{n}\right). \tag{4.3.55}$$

But Theorem 3.4.49 together with Abel summation imply that (4.3.55) is $O(\log^4 y)$, yielding our desired result. □

We emphasize that (4.3.51) and (4.3.52) from the proof of Proposition 4.3.42 have given us the following Euler product expansion for Q_7:

$$Q_7 = Q_7(3)Q_7(7) \prod_{\substack{p\neq 7 \text{ prime} \\ p\equiv 1 \pmod 3}} \left(1 + \frac{2}{(p+1)^2}\right), \tag{4.3.56}$$

where $Q_7(3) = 13/6$ and $Q_7(7) = 63/8$.

We are now ready to prove Theorem 1.2.13 when $m = 7$, which we restate here with an improved error term in the notations we have established. We give two proofs of this important statement. The first proof is an easy argument using Proposition 4.3.1 and Proposition 4.3.42. The second proof requires deriving a bound on $N^{\text{tw}}_{7,>y}(X)$ which is in some sense superfluous; however, this proof is more typical of our arguments in the remaining chapters of this thesis.

Theorem 4.3.57. *We have*

$$N_7^{\mathrm{tw}}(X) = c_7^{\mathrm{tw}} X^{1/6} + O(X^{1/12}\log^5 X) \tag{4.3.58}$$

for $X \geq 2$. The constant c_7^{tw} is given in (4.3.40).

First Proof of Theorem 4.3.57. Let $X > 0$, and let y be slightly larger than $\frac{3^{5/4}\cdot 7^{9/2}}{2^{1/6}} \cdot X^{1/12}$. By Proposition 4.3.1,

$$N_{7,\leq y}^{\mathrm{tw}}(X) = N_7^{\mathrm{tw}}(X), \tag{4.3.59}$$

and the result is now immediate from Proposition 4.3.42. □

We now bound $N_{7,>y}^{\mathrm{tw}}(X)$ as a step towards our alternate proof. The proof below is somewhat cleaner than that given in [45].

Lemma 4.3.60. *We have*

$$N_{7,>y}^{\mathrm{tw}}(X) = O\left(\frac{X^{1/6}\log y}{y}\right) \tag{4.3.61}$$

for $X, y \geq 2$.

Proof. By Lemma 4.2.17(f), $T_m(e) = O(2^{\omega(e)})$, so by Lemma 4.3.16, we have

$$M_m(X;e) = O\left(\frac{2^{\omega(e)}X^{1/6}}{e^3}\right). \tag{4.3.62}$$

Now by Proposition 3.5.14, we see

$$\widetilde{N}_{m,>y}^{\mathrm{tw}}(X) = O\left(\sum_{n>y}\frac{2^{\omega(n)}X^{1/6}}{n^2}\right). \tag{4.3.63}$$

Combining Corollary 3.4.42 and Corollary 3.4.6, we conclude

$$\widetilde{N}^{\mathrm{tw}}_{m,>y}(X) = O\left(\frac{X^{1/6}\log y}{y}\right) \tag{4.3.64}$$

as desired. □

Second Proof of Theorem 4.3.57. Let y be a positive quantity with $y \ll X^{1/12}$; in particular, $\log y \ll \log X$. Proposition 4.3.42 and Lemma 4.3.60 together tell us

$$N^{\mathrm{tw}}_7(X) = c^{\mathrm{tw}}_7 X^{1/6} + O\left(\max\left(\frac{X^{1/6}\log y}{y}, X^{1/12}\log X\log^4 y\right)\right). \tag{4.3.65}$$

Now letting $y = X^{1/12}$, our claim follows. □

L-series

To conclude this section, we set up section 4.4 by interpreting Theorem 4.3.57 in terms of Dirichlet series. Recall (3.5.22), (3.5.23), (3.5.24), and (3.5.25).

Corollary 4.3.66. *The following statements hold.*

(a) The Dirichlet series $L^{\mathrm{tw}}_7(s)$ has abscissa of (absolute) convergence $\sigma_a = \sigma_c = 1/6$ and has a meromorphic continuation to the region

$$\{s = \sigma + it \in \mathbb{C} : \sigma > 1/12\}. \tag{4.3.67}$$

(b) The function $L^{\mathrm{tw}}_7(s)$ has a simple pole at $s = 1/6$ with residue

$$\operatorname{res}_{s=\frac{1}{6}} L^{\mathrm{tw}}_7(s) = \frac{c^{\mathrm{tw}}_7}{6}; \tag{4.3.68}$$

it is holomorphic elsewhere on the region (4.3.67).

(c) We have

$$\mu_{L_7^{\mathrm{tw}}}(\sigma) < 13/84 \tag{4.3.69}$$

for $\sigma > 1/12$.

Proof. We first prove part (a). Let $s = \sigma + it \in \mathbb{C}$ be given with $\sigma > 1/6$. Abel summation yields

$$\begin{aligned}\sum_{n \le X} \Delta N_7^{\mathrm{tw}}(n) n^{-s} &= N_7^{\mathrm{tw}}(X) X^{-s} + s \int_1^X N_7^{\mathrm{tw}}(u) u^{-s-1}\,\mathrm{d}u \\ &= O\left(X^{1/6-\sigma} + s \int_1^X u^{-5/6-\sigma}\,\mathrm{d}u\right);\end{aligned} \tag{4.3.70}$$

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

$$\sum_{n \ge 1} \Delta N_7^{\mathrm{tw}}(n) n^{-s} = s \int_1^\infty N_7^{\mathrm{tw}}(u) u^{-1-s}\,\mathrm{d}u \tag{4.3.71}$$

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 $\Delta N_7^{\mathrm{tw}}(n) \ge 0$ for all n, $1/6$ is also the abscissa of *absolute* convergence $\sigma_a = \sigma_c$.

Now define $L_{7,\mathrm{rem}}^{\mathrm{tw}}(s)$ so that

$$L_7^{\mathrm{tw}}(s) = c_7^{\mathrm{tw}} \zeta(6s) + L_{7,\mathrm{rem}}^{\mathrm{tw}}(s). \tag{4.3.72}$$

Abel summation and the substitution $u \mapsto u^{1/6}$ yields the following equality for $\sigma > 1/6$:

$$\zeta(6s) = s \int_1^\infty \left\lfloor u^{1/6} \right\rfloor u^{-1-s}\,\mathrm{d}u = s \int_1^\infty \left(u^{1/6} + O(1)\right) u^{-1-s}\,\mathrm{d}u. \tag{4.3.73}$$

Let

$$\chi_6(n) := \begin{cases} 1, & \text{if } n = k^6 \text{ for some } k \in \mathbb{Z}; \\ 0, & \text{else.} \end{cases} \tag{4.3.74}$$

Then

$$\begin{aligned} L^{\mathrm{tw}}_{7,\mathrm{rem}}(s) &= \sum_{n\geq 1} \left(\Delta N^{\mathrm{tw}}_7(n) - c^{\mathrm{tw}}_7 \chi_6(n)\right) n^{-s} \\ &= s\int_1^\infty \left(N^{\mathrm{tw}}_7(u) - c^{\mathrm{tw}}_7 \left\lfloor u^{1/6} \right\rfloor\right) u^{-1-s}\,\mathrm{d}u \end{aligned} \tag{4.3.75}$$

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

$$N^{\mathrm{tw}}_7(u) - c^{\mathrm{tw}}_7 \left\lfloor u^{1/6} \right\rfloor = O(u^{1/12+\epsilon}) \tag{4.3.76}$$

by Theorem 4.3.57. Substituting (4.3.76) into (4.3.75), we obtain

$$L^{\mathrm{tw}}_{7,\mathrm{rem}}(s) = s\int_1^\infty \left(N^{\mathrm{tw}}_7(u) - c^{\mathrm{tw}}_7 \left\lfloor u^{1/6} \right\rfloor\right) u^{-1-s}\,\mathrm{d}u = O\left(s\int_1^\infty u^{-11/12-\sigma+\epsilon}\,\mathrm{d}u\right) \tag{4.3.77}$$

where the integral converges whenever $\sigma > 1/12 + \epsilon$. Letting $\epsilon \to 0$, we obtain an analytic continuation of $L^{\mathrm{tw}}_{7,\mathrm{rem}}(s)$ to the region (4.3.67).

We proceed to part (b). The Dirichlet series $\zeta(6s)$ has meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1/6$ with residue $1/6$. Thus looking back at (4.3.72), we find that

$$L^{\mathrm{tw}}_7(s) = c^{\mathrm{tw}}_7 \zeta(6s) + s\int_1^\infty \left(N^{\mathrm{tw}}_7(u) - c^{\mathrm{tw}}_7 \left\lfloor u^{1/6} \right\rfloor\right) u^{-1-s}\,\mathrm{d}u \tag{4.3.78}$$

when $\sigma > 1/6$, but in fact the right-hand side of this equality defines a meromorphic function on the region (4.3.67) with a simple pole at $s = 1/6$ and no other poles in this region.

Finally, we prove part (c). By Theorem 3.4.30, $\mu_{L^{\mathrm{tw}}_{7,\mathrm{rem}}}(\sigma) = 0$ for $\sigma > 1/12$, so by Proposition 3.4.27 and Theorem 3.4.31,

$$\mu_{L^{\mathrm{tw}}_7}(\sigma) = \mu_{\zeta_6}(\sigma) < 13/84 \tag{4.3.79}$$

for $\sigma > 1/12$. Our claim follows. □

Section 4.4

Estimates for rational isomorphism classes for $m = 7$

In section 4.3, we counted the number of elliptic curves over $\mathbb{Q}$ with a (cyclic) 7-isogeny up to quadratic twist (Theorem 4.3.57). In this section, we count all isomorphism classes over $\mathbb{Q}$ by enumerating over twists using Landau's Tauberian theorem (Theorem 3.4.37). We first describe the analytic behavior of $L_7(s)$.

Theorem 4.4.1. *The following statements hold.*

(a) *The Dirichlet series $L_7(s)$ has a meromorphic continuation to the region (4.3.67) with a double pole at $s = 1/6$ and no other singularities on this region.*

(b) *The principal part of $L_7(s)$ at $s = 1/6$ is*

$$\frac{1}{3\zeta(2)}\left(\frac{c_7^{\mathrm{tw}}}{6}\left(s-\frac{1}{6}\right)^{-2} + \left(\ell_{7,0} + c_7^{\mathrm{tw}}\left(\gamma - \frac{2\zeta'(2)}{\zeta(2)}\right)\right)\left(s-\frac{1}{6}\right)^{-1}\right), \tag{4.4.2}$$

where c_7^{tw} is given in (4.3.40), and

$$\ell_{7,0} := c_7^{\mathrm{tw}}\gamma + \frac{1}{6}\int_1^\infty \left(N_7^{\mathrm{tw}}(u) - c_7^{\mathrm{tw}}\left\lfloor u^{1/6}\right\rfloor\right) u^{-7/6}\,\mathrm{d}u \tag{4.4.3}$$

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

Proof. For part (a), since $\zeta(s)$ is nonvanishing when $\sigma > 1$, the ratio $\zeta(6s)/\zeta(12s)$ is meromorphic function for $\sigma > 1/12$. But Corollary 4.3.66 gives a meromorphic continuation of $L_7^{\mathrm{tw}}(s)$ to the region (4.3.67). The function $L_7(s)$ is a product of these two meromorphic functions on (4.3.67), 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 deduce part (b) by computing Laurent expansions. We readily verify

$$\frac{\zeta(6s)}{\zeta(12s)} = \frac{1}{\zeta(2)}\left(\frac{1}{6}\left(s-\frac{1}{6}\right)^{-1} + \left(\gamma - \frac{2\zeta'(2)}{\zeta(2)}\right) + \dots\right), \tag{4.4.4}$$

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

$$L_7^{\mathrm{tw}}(s) = \frac{c_7^{\mathrm{tw}}}{6}\left(s-\frac{1}{6}\right)^{-1} + \ell_{7,0} + \dots, \tag{4.4.5}$$

with $\ell_{7,0}$ given by (4.4.3). Multiplying the Laurent series tails gives the desired result. □

Using Theorem 4.4.1, we deduce the following lemma.

Lemma 4.4.6. *The sequence* $(\Delta N_7(n))_{n\geq 1}$ *is admissible* (Definition 3.4.36) *with parameters* $(1/6, 1/12, 13/42)$.

Proof. We check each condition in Definition 3.4.36. Since $\Delta N_7(n)$ counts objects, we indeed have $\Delta N_7(n) \in \mathbb{Z}_{\geq 0}$.

For (i), Corollary 4.3.66 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 3.5.26(b),

$$L_7(s) = \frac{2\zeta(6s)L_7^{\mathrm{tw}}(s)}{\zeta(12s)}, \tag{4.4.7}$$

and by Theorem 3.4.20 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 $\sigma_a = 1/6$.

For (ii), Corollary 4.3.66 tells us that $L_7^{\mathrm{tw}}(s)$ has a meromorphic continuation when $\sigma = \mathrm{Re}(s) > 1/12$; 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

$$\delta = 1/6 - 1/12 = 1/12. \tag{4.4.8}$$

(The only pole of $L_7(s)/s$ with $\sigma > 1/12$ is the double pole at $s = 1/6$ indicated in Theorem 4.4.1(b).)

For (iii), let $\sigma > 1/12$. By Corollary 4.3.66, $\mu_{L_7^{\mathrm{tw}}}(\sigma) < 13/84$. Let $\zeta_a(s) = \zeta(as)$. Applying Theorem 3.4.31, we have

$$\mu_{\zeta_6}(\sigma) = \mu_{\zeta}(6\sigma) < \frac{13}{42}\left(1 - \frac{6}{12}\right) = \frac{13}{84} \tag{4.4.9}$$

if $\sigma \leq 1/6$, and by Theorem 3.4.30, $\mu_{\zeta_6}(\sigma) = 0$ if $\sigma > 1/6$. Finally, as $\zeta(12s)^{-1}$ is absolutely convergent for $s > 1/12$, Theorem 3.4.30 tells us $\mu_{{\zeta_{12}}^{-1}}(\sigma) = 0$. Taken together, we see

$$\mu_{L_7}(\sigma) < \frac{13}{84} + \frac{13}{84} + 0 = \frac{13}{42}, \tag{4.4.10}$$

so the sequence $(\Delta N_7(n))_{n\geq 1}$ is admissible with final parameter $\xi = 13/42$. □

We now prove Theorem 1.2.3 when $m = 7$, which we restate here in this special case in our established notation.

Theorem 4.4.11. *We define*

$$\begin{aligned} c_7 &:= \frac{Q_7 R_7}{3\zeta(2)^2}, \\ c_7' &:= \frac{2}{\zeta(2)}\left(\ell_{7,0} + c_7^{\mathrm{tw}}\left(\gamma - 1 - \frac{2\zeta'(2)}{\zeta(2)}\right)\right), \end{aligned} \tag{4.4.12}$$

where c_7^{tw} is defined in (4.3.40), and $\ell_{7,0}$ is defined in (4.4.3). Then for all $\epsilon > 0$, we have

$$N_7(X) = c_7 X^{1/6}\log X + c_7' X^{1/6} + O\left(X^{1/8+\epsilon}\right) \tag{4.4.13}$$

for $X \geq 1$. The implicit constant depends only on ϵ.

Proof. By Lemma 4.4.6, $(\Delta N_7(n))_{n \geq 1}$ is admissible with parameters $(1/6, 1/12, 13/42)$. We now apply Theorem 3.4.37 to the Dirichlet series $L_7(s)$, and our claim follows. □

Remark 4.4.14. We believe that with sufficient care and appropriate hypotheses, the denominator $\lfloor \xi \rfloor + 2$ in the exponent of the error for Theorem 3.4.37 can be replaced with $\xi + 1$. If so, the exponent $1/8 + \epsilon$ in the error term may be replaced with $17/165 + \epsilon$, and further improvements in the estimate of $\mu_\zeta(\sigma)$ will translate directly to improvements in the error term of $N_7(X)$. If the Lindelöf hypothesis holds, the exponent of our the error term for $N_7(X)$, like $N_7^{\mathrm{tw}}(X)$, would be reduced to $O(X^{1/12+\epsilon})$.

Section 4.5

Computations for $m = 7$

In this section, we furnish computations that make Theorem 4.3.57 and Theorem 4.4.11 completely explicit.

Enumerating elliptic curves with a cyclic 7-isogeny

We begin by outlining an algorithm for computing all elliptic curves (up to quadratic twist) with twist height at most X that admit a cyclic 7-isogeny. In a nutshell, we iterate over possible factorizations $e^3 m$ with m cubefree to find all 7-groomed pairs (a, b) for which $C_7(a, b) = e^3 m$, then check if $\operatorname{twht}(A_7(a, b), B_7(a, b)) \leq X$.

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 4.2.35(a)).

2. For each pair $(a, b) \in \mathbb{Z}^2$ with $b > 0$, $\gcd(a, b) = 1$, $b > 0$, and $C_7(a, b)$ coprime to 3 and less than Y, we compute $C_7(a, b)$. 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 $C_7(a,b)=c$. 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 7-groomed pairs $(a,b)\in\mathbb{Z}^2$ with $C_7(a,b)=e_0^3m$. If $\gcd(e_0,3)=\gcd(m,3)=1$, we can do this as follows. If $e_0^3<Y$, we iterate over 7-groomed pairs (a_e,b_e) and (a_m,b_m) yielding $C_7(a_e,b_e)=e_0^3$ and $C_7(a_m,b_m)=m$ respectively, and taking the product
$$(a_e+b_e\,(-1+3\zeta_6))(a_m+b_m\,(-1+3\zeta_6)) = a+b\,(-1+3\zeta_6)\in\mathbb{Z}[3\zeta_6] \qquad (4.5.1)$$
as in the proof of Lemma 4.2.28. If $e_0^3>Y$, we iterate over 7-groomed pairs (a_e',b_e') with $C_7(a_e',b_e')=e_0$ instead of over 7-groomed pairs (a_e,b_e), and compute
$$(a_e'+b_e\,(-1+3\zeta_6))^3(a_m+b_m\,(-1+3\zeta_6)) = a+b\,(-1+3\zeta_6)\in\mathbb{Z}[3\zeta_6]. \qquad (4.5.2)$$
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 7-groomed pairs $(a_3,b_3)\in\mathbb{Z}^2$ with $C_7(a_3,b_3)$ an appropriate power of 3 (which is no greater than 27, by 4.2.17).

4. For each pair (a,b) with $C_7(a,b)=e_0^3m$, obtained in the previous step, we compute $H(A_7(a,b),B_7(a,b))$. 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 $e=\operatorname{lcm}(e_0,e_3,e_7)$. We compute the twist height using the reduced pairs $(A_7(a,b)/e^2, \left|B_7(a,b)\right|/e^3)$. 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.

We list the first few twist minimal elliptic curves admitting a (cyclic) 7-isogeny in Table 4.5.3.

(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 4.5.3: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 7-isogeny and $\mathrm{twht}\, E \leq 10^9$

Running this algorithm out to $X = 10^{42}$ in Python took us approximately 34 CPU hours on a single core, producing 4 582 079 elliptic curves admitting a (cyclic) 7-isogeny in $\mathscr{E}^{\mathrm{tw}}_{\leq 10^{42}}$. 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

$$\frac{N_7^{\mathrm{tw}}(10^{42})}{c_7^{\mathrm{tw}}(10^{42})^{1/6}} = 0.99996\ldots, \tag{4.5.4}$$

which is close to 1. We compute $c_7^{\mathrm{tw}} = Q_7 R_7/\zeta(2)$ below.

Reorganizing the sum in Theorem 3.5.26(a), we find

$$N_7(X) = 2 \sum_{n \leq X} \sum_{c \leq (X/n)^{1/6}} \Delta N_7^{\mathrm{tw}} \left(n/c^6\right) |\mu(c)| \,. \tag{4.5.5}$$

Letting $X = 10^{42}$ and using our list of 4 582 079 elliptic curves admitting a (cyclic) 7-isogeny, we compute that there are 88 157 174 elliptic curves admitting a (cyclic) 7-isogeny in $\mathscr{E}_{\leq 10^{42}}$.

Computing c_7^{tw}

In this subsection, we estimate the constant c_7^{tw} appearing in Theorem 4.4.11 by estimating Q_7 and R_7.

We begin with Q_7, given by (4.3.52). Truncating the Euler product as a product over $p \leq Y$ gives us a lower bound

$$Q_{7,\leq Y} := \frac{273}{16} \prod_{\substack{7 < p \leq Y \\ p \equiv 1 \pmod{3}}} \left(1 + \frac{2}{p^2+1}\right) \tag{4.5.6}$$

for Q_7. To obtain an upper bound, we compute

$$Q_7 < Q_{7,\leq Y} \exp\left(2 \sum_{\substack{p > Y \\ p \equiv 1 \pmod{3}}} \frac{1}{p^2+1}\right). \tag{4.5.7}$$

Suppose $Y \geq 8 \cdot 10^9$. Using Abel summation and Bennett–Martin–O'Bryant–Rechnitzer [4, Theorem 1.4], we obtain

$$\begin{aligned}\sum_{\substack{p>Y\\ p\equiv 1 \pmod 3}} \frac{1}{p^2+1} &= -\frac{\pi(Y;3,1)}{Y^2+1} + 2\int_Y^\infty \frac{\pi(u;3,1)u}{(u^2+1)^2}\,\mathrm{d}u \\ &< -\frac{Y}{2\,(Y^2+1)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\int_Y^\infty \frac{u^2}{(u^2+1)^2}\,\mathrm{d}u \\ &= \frac{1}{2}\left(\frac{5Y}{2(Y^2+1)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\left(\frac{\pi}{2} - \tan^{-1}(Y)\right)\right)\end{aligned} \tag{4.5.8}$$

so

$$Q_7 < Q_{7,\le Y}\cdot \exp\left(\frac{5Y}{2(Y^2+1)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\left(\frac{\pi}{2} - \tan^{-1}(Y)\right)\right). \tag{4.5.9}$$

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

$$17.460\,405\,231\,126\,620 < Q_7 < 17.460\,405\,231\,134\,835 \tag{4.5.10}$$

This computation took approximately 9 CPU days.

We now turn our attention to R_7, given in (3.3.6). We observe

$$\mathcal{R}_7(1) \subseteq [-0.677, 0.677] \times [0, 0.078], \tag{4.5.11}$$

so we can estimate $\mathcal{R}_7(1)$ by performing rejection sampling on the rectangle $[-0.677, 0.677]\times[0, 0.078]$, which has area 0.105612.

We find $r_7 := 243\,228\,665\,965$ of our first $s_7 := 595\,055\,000\,000$ samples lie in R_7, so

$$R_7 \approx 0.105612 \cdot \frac{r_7}{s_7} = 0.04316889\ldots \tag{4.5.12}$$

with standard error

$$0.105612 \cdot \sqrt{\frac{r_7(s_7 - r_7)}{s_7^3}} < 6.8 \cdot 10^{-8}. \tag{4.5.13}$$

This took 11 CPU weeks to compute. Thus $c_7^{\mathrm{tw}} = 0.45822276\ldots$, with error bounded by $6.6 \cdot 10^{-7}$.

Computing c_7 and c_7'

In this subsection, we estimate the constants c_7 and c_7', which are defined in (4.4.12) and used in Theorem 4.4.11.

We have the identity $c_7 = c_7^{\mathrm{tw}}/3\zeta(2)$, so $c_7 = 0.092\,855\,36\ldots$ with an error of $6.02 \cdot 10^{-8}$

We now turn our attention to c_7'. As an intermediate step, we wish to approximate the constant $\ell_{7,0}$. We can approximate $\ell_{7,0}$ by truncating the integral (4.4.3) and using our approximation for c_7^{tw}. This yields $\ell_{7,0} \approx -0.463\,530$. In Theorem 4.3.57, we have shown that for some $M > 0$ and for all $u > X$, we have

$$\left| N_7^{\mathrm{tw}}(u) - c_7^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor \right| < M u^{1/12} \log^5 u. \tag{4.5.14}$$

Thus

$$\begin{aligned} &\left| \int_X^\infty \left(N_7^{\mathrm{tw}}(u) - c_7^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor \right) u^{-7/6} \,\mathrm{d}u \right| \\ &\quad < M \int_X^\infty u^{-13/12} \log^5 u \,\mathrm{d}u \\ &\quad = 12 M X^{-1/12} (\log^5 X + 60 \log^4 X + 2880 \log^3 X \\ &\quad + 103680 \log^2 X + 2488320 \log X + 29859840); \end{aligned} \tag{4.5.15}$$

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

$$-5.11 \cdot 10^{-6} \leq \frac{N_7^{\mathrm{tw}}(u) - c_7^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor}{u^{1/12} \log^5 u} \leq 6.29 \cdot 10^{-7}. \tag{4.5.16}$$

If we assume these bounds continue to hold for larger u, we find the truncation error for $\ell_{7,0}$ is bounded by 68.95, which catastrophically dwarfs our initial estimate.

We can do better by sidestepping the logarithms. We know that $N_7^{\mathrm{tw}}(X) - c_7^{\mathrm{tw}} X^{1/6} = O(X^{1/12+\epsilon})$ for every $\epsilon > 0$. We let $\epsilon := 10^{-4}$, and find that for $1 \le u \le 10^{42}$,

$$-1.2174 \le \frac{N_7^{\mathrm{tw}}(u) - c_7^{\mathrm{tw}} \lfloor u^{1/6} \rfloor}{u^{1/12+\epsilon}} \le 0.52272. \tag{4.5.17}$$

If we assume these bounds continue to hold for larger u, we get an estimated truncation error of $2.43 \cdot 10^{-5}$, which is much more manageable.

Our estimate of $\ell_{7,0}$ is also skewed by our estimates of c_7^{tw}. An error of ϵ in our estimate for c_7^{tw} induces an error of

$$\frac{\epsilon}{6} \int_1^X \lfloor u^{1/6} \rfloor \, u^{-7/6} \, \mathrm{d}u < \frac{\epsilon}{6} \int_1^X u^{-1} \, \mathrm{d}u = \frac{\epsilon \log X}{6} \tag{4.5.18}$$

in our estimate of $\ell_{7,0}$. When $X = 10^{42}$, this gives an additional error of $1.15 \cdot 10^{-5}$, for an aggregate error of 36.34 or $2.43 \cdot 10^{-5}$, depending on our assumptions.

Given c_7^{tw} and $\ell_{7,0}$, it is straightforward to compute c_7' using the expression given in (4.4.12). We have $c_7' \approx -0.164\,044\,749$ with an error of 83.84 or of $2.98 \cdot 10^{-5}$, depending on the assumptions made above. Note that both of these error terms for c_7' depended on empirical rather than theoretical estimates for the implicit constant in the error term of Theorem 4.4.11. As a sanity check, we verify that

$$\frac{N_7(10^{42})}{10^7} - 42 c_7 \log 10 = -0.164\,186\,667\ldots \approx c_7', \tag{4.5.19}$$

which agrees to three decimal places with the estimate for c_7' we gave above.

Chapter 5

Counting elliptic curves with a cyclic m-isogeny for $m = 10, 25$

In this chapter, we prove Theorem 1.2.6 (Theorem 5.4.11), and Theorem 2.3.15 (Theorem 5.3.46) when $m = 10, 25$. These results are new, but our arguments mirror those in chapter 4 (and thus also [45]), and we encourage anyone reading to skim them on a first perusal of this thesis. There is one major new complication, however: viewed as an elliptic curve over $\mathbb{Q}(t)$, the elliptic surfaces describing elliptic curves with a cyclic 5-isogeny, with a cyclic 10-isogeny, and with a cyclic 25-isogeny exhibit potential type III additive reduction rather than potential type II additive reduction. This forces us change how we define $T_m(e)$ and related functions (see Definition 5.2.5), and changes the details of our sieving somewhat.

Although we are unable to derive asymptotics for $\widetilde{N}_5^{\mathrm{tw}}(X)$ or $\widetilde{N}_5(X)$, this case is structurally similar enough to $m = 10, 25$ that we opt to provide some preliminary information about the structure of $M_5(X)$ and related functions.

In section 5.1, for $m \in \{5, 10, 25\}$, we establish notations pertaining to $f_m(t)$ and $g_m(t)$ which will be used throughout the remainder of the chapter. In section 5.3, we develop bounds relating the twist minimality defect to the greatest common divisor of $f_m(t)$ and

$g_m(t)$. In section 5.1, we apply the framework developed in section 3.5 to prove Theorem 1.2.6 for $m = 10, 25$. In section 5.4, we prove Theorem 1.2.6 for $m = 10, 25$. In section 5.5, we produce supplementary computations to estimate the constants appearing in Theorem 5.3.46 and Theorem 5.4.11 and empirically confirm that the count of elliptic curves with a cyclic m-isogeny aligns with our theoretical estimates when $m = 10, 25$.

Section 5.1
Establishing notation for $m \in \{5, 10, 25\}$

By Corollary 2.1.50, for $m = 10, 25$, we have

$$\widetilde{N}_m^{\mathrm{tw}}(X) = N_m^{\mathrm{tw}}(X) \text{ and } \widetilde{N}_m(X) = N_m(X) \tag{5.1.1}$$

for all $X > 0$, so we may use either notation interchangeably. On the other hand, $\widetilde{N}_5^{\mathrm{tw}}(X) \neq N_5^{\mathrm{tw}}(X)$ in general. We work with $\widetilde{N}_m^{\mathrm{tw}}(X)$ until we can proceed no further on the case $m = 5$, and then transition over to using the notation $N_m^{\mathrm{tw}}(X)$.

Let $m \in \{5, 10, 25\}$. Pursuant to the notation established in section 3.2, we define $h_m(t) = \gcd(f_m(t), g_m(t))$, and we define $f'_m(t)$ and $g'_m(t)$ so that

$$f_m(t) = f'_m(t)h_m(t) \text{ and } g_m(t) = g'_m(t)h_m(t)^2. \tag{5.1.2}$$

Note that $h_m(t)^2$ divides $g_m(t)$, whereas only $h_7(t)$ divides $g_7(t)$. From (5.1.2) we conclude

$$\begin{aligned} h_5(t) = h_{10}(t) = t^2 + 1,& \text{ and} \\ h_{25}(t) = t^2 + 4.& \end{aligned} \tag{5.1.3}$$

To work with integral models, we take $t = a/b$ (in lowest terms) and homogenize, obtaining

$$\begin{aligned} C_m(a,b) &:= b^2 h_m(a/b), \\ A'_m(a,b) &:= b^{2d(m)/3-2} f'_m(a/b, \text{ and} \\ B'_m(a,b) &:= b^{d(m)-4} g'_m(a/b). \end{aligned} \tag{5.1.4}$$

Of course, we have

$$\begin{aligned} C_m(a,b) &= \gcd(A_m(a,b), B_m(a,b)) \in \mathbb{Z}[a,b], \\ A_m(a,b) &= A'_m(a,b) C_m(a,b), \text{ and} \\ B_m(a,b) &= B'_m(a,b) C_m(a,b)^2. \end{aligned} \tag{5.1.5}$$

Recall $d\,(5) = 6$, $d\,(10) = 12$, and $d\,(25) = 18$.

Section 5.2

The twist minimality defect for $m \in \{5, 10, 25\}$

In this section, for $m \in \{5, 10, 25\}$, we study the twist minimality defect for

$$y^2 = x^3 + A_m(a,b)x + B_m(a,b) \tag{5.2.1}$$

using the polynomials $A'_m(a,b)$, $B'_m(a,b)$, and $C_m(a,b)$. This section mirrors section 4.2, but our definition of $T_m(e)$ is changed.

Lemma 5.2.2. *Let $m \in \{5, 10, 25\}$, let $(a,b) \in \mathbb{Z}^2$ be m-groomed, let ℓ be prime, and let $v \in \mathbb{Z}_{\geq 0}$. Then the following statements hold.*

(a) *If $\ell \neq 2, 5$, then $\ell^v \mid \operatorname{tmd}(A_m(a,b), B_m(a,b))$ if and only if $\ell^{2v} \mid C_m(a,b)$.*

(b) *We have $\ell^{2v} \mid C_m(a,b)$ if and only if $\ell \nmid b$ and $h_m(a/b) \equiv 0 \pmod{\ell^{2v}}$.*

(c) *If $\ell \neq 2$, then $\ell \mid C_m(a,b)$ implies $\ell \nmid (\partial C_m/\partial a)(a,b)$.*

Proof. The proof of part (a) is essentially the same as the proof for Lemma 4.2.2, with two modifications. First, as $C_m(a,b)^2 \mid B_m(a,b)$, the condition $\ell^{2v} \mid C_m(a,b)$ implies $\ell \mid \operatorname{tmd}(A_m(a,b), B_m(a,b))$. Second, we have the resultants:

$$\begin{aligned}
\operatorname{Res}(A_5'(t,1), B_5'(t,1)) &= \operatorname{Res}(f_5'(t), g_5'(t)) = -2^2 \cdot 3^4 \cdot 5^{10} = \operatorname{Res}(A_5'(1,u), B_5'(1,u)),\\
\operatorname{Res}(A_5'(t,1), C_5(t,1)) &= \operatorname{Res}(f_5'(t), h_5(t)) = 3^4 \cdot 5^5 = \operatorname{Res}(A_5'(1,u), C_5(1,u)),\\
\operatorname{Res}(A_{10}'(t,1), B_{10}'(t,1)) &= \operatorname{Res}(f_{10}'(t), g_{10}'(t)) = -2^{18} \cdot 3^{16} \cdot 5^{35} = \operatorname{Res}(A_{10}'(1,u), B_{10}'(1,u)),\\
\operatorname{Res}(A_{10}'(t,1), C_{10}(t,1)) &= \operatorname{Res}(f_{10}'(t), h_{10}(t)) = 3^4 \cdot 5^5 = \operatorname{Res}(A_{10}'(1,u), C_{10}(1,u)),\\
\operatorname{Res}(A_{25}'(t,1), B_{25}'(t,1)) &= \operatorname{Res}(f_{25}'(t), g_{25}'(t)) = -2^{38} \cdot 3^{28} \cdot 5^{118} = \operatorname{Res}(A_{25}'(1,u), B_{25}'(1,u)),\\
\operatorname{Res}(A_{25}'(t,1), C_{25}(t,1)) &= \operatorname{Res}(f_{25}'(t), h_{10}(t)) = 2^4 \cdot 3^4 \cdot 5^9 = \operatorname{Res}(A_{25}'(1,u), C_{25}(1,u)).
\end{aligned} \tag{5.2.3}$$

So $2, 3$, and 5 are our badly behaved primes. A short computation shows that 3 divides neither $\operatorname{tmd}(A_m(a,b), B_m(a,b))$ nor $C_m(a,b)$, however, which proves (a).

Part (b) proceeds as in the proof of Lemma 4.2.2.

Part (c) follows from (b) and the fact that $h_5(t) = h_{10}(t)$ has discriminant -2^2, and $h_{25}(t)$ has discriminant $\operatorname{disc}(h_{25}(t)) = -2^4$. □

Remark 5.2.4. We could have adapted the second proof of Lemma 4.2.2 to give an alternate proof of Lemma 5.2.2.

Definition 5.2.5. For $m \in \{5, 10, 25\}$ and for $e \geq 1$, let $\widetilde{\mathcal{T}}_m(e)$ denote the image of

$$\left\{(a,b) \in \mathbb{Z}^2 : (a,b)\ m\text{-groomed},\ e \mid \operatorname{tmd}(A_m(a,b), B_m(a,b))\right\} \tag{5.2.6}$$

under the projection

$$\mathbb{Z}^2 \to (\mathbb{Z}/e^2\mathbb{Z})^2. \tag{5.2.7}$$

For $m \in \{5, 10, 25\}$, let $\widetilde{T}_m(e) := \#\widetilde{\mathcal{T}}_m(e)$. Similarly, for $m \in \{5, 10, 25\}$, let $\mathcal{T}_m(e)$ denote the image of

$$\left\{t \in \mathbb{Z} : e^2 \mid f_m(t \text{ and } e^3 \mid g_m(t)\right\} \tag{5.2.8}$$

under the projection

$$\mathbb{Z} \to \mathbb{Z}/e^2\mathbb{Z}, \tag{5.2.9}$$

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

Note that for $m \in \{5, 10, 25\}$, the set $\widetilde{\mathcal{T}}_m(e)$ is a subset of $(\mathbb{Z}/e^2\mathbb{Z})^2$, whereas $\widetilde{\mathcal{T}}_7(e)$ is a subset of $(\mathbb{Z}/e^2\mathbb{Z})^2$! This reflects the difference between potential type II additive reduction and potential type III additive reduction, which manifests in the discrepancy between Lemma 4.2.2(a) and Lemma 5.2.2(a).

Lemma 5.2.10. *Let $m \in \{5, 10, 25\}$. The following statements hold.*

(a) *If $2^3 \mid e$, then $\widetilde{\mathcal{T}}_m(e) = \emptyset$. Otherwise, $\widetilde{\mathcal{T}}_m(e)$ consists of those pairs $(a, b) \in (\mathbb{Z}/e^2\mathbb{Z})^2$ which satisfy the following conditions:*

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

(b) *Let $(a, b) \in \mathbb{Z}^2$. If $(a, b) \pmod{e^2} \in \widetilde{\mathcal{T}}_m(e)$, then $e \mid \operatorname{tmd}(A(a, b), B(a, b))$.*

(c) *The functions $\widetilde{T}_m(e)$ and $T_m(e)$ are multiplicative, and $\widetilde{T}_m(e) = \varphi(e^2)T_m(e)$.*

(d) *For all $\ell \neq 2, 5$ and $v \geq 1$,*

$$T_m(\ell^v) = T_m(\ell) = 1 + \left(\frac{-1}{\ell}\right). \tag{5.2.11}$$

(e) *For $e \in \{2, 2^2, 5, 5^2, 5^3, 5^4\}$, the nonzero values of $T_m(e)$ are given in Table 5.2.21 and*

Table 5.2.22 below. We have

$$T_5(2^v) = 0 \textit{ for } v \geq 1,\ T_{10}(2^v) = 0 \textit{ for } v \geq 2,\ \textit{and } T_{25}(2^v) = 0 \textit{ for } v \geq 3; \qquad (5.2.12)$$

we also have

$$T_5(5^v) = 1 + 5^5 \textit{ for } v \geq 4,\ T_{10}(5^v) = 1 + 5^5 \textit{ for } v \geq 3,\ \textit{and } T_{10}(2^v) = 1 + 5^9 \textit{ for } v \geq 5. \qquad (5.2.13)$$

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

Proof. For parts (a) and (b), by the CRT (Sun Zi theorem), it suffices to consider $e = \ell^v$ a power of a prime. For $\ell \neq 2, 5$, both claims follow from Lemma 5.2.2(a)–(b). But a finite computation verifies our claim when $\ell = 2, 5$ as well (see the proof of (e) below).

Parts (c) and (d) follow by essentially the same arguments as in the proof of 4.2.17.

Next, part (e). For $\ell = 2$, the claim is a finite computation. For $\ell = 5$, we first certify the assertion computationally for $v < 9$. Hensel's lemma still applies to $h_m(t)$: let t_0, t_1 be the roots of $h_m(t)$ in the 5-adic integers $\mathbb{Z}_5$, with $t_0 \equiv 2 \pmod 5$ and with $t_1 \equiv -2 \pmod 5$ if $m = 5, 10$, and $t_0 \equiv -1 \pmod 5$ and $t_1 \equiv 1 \pmod 5$ if $m = 25$. It is easy to verify

$$f'_m(t_0) \not\equiv 0 \pmod 5,\ g'_m(t_0) \not\equiv 0 \pmod 5, \qquad (5.2.14)$$

and on the other hand that for $m = 5, 10$, we have

$$f'_m(t_1) \equiv g'_{10}(t_1) \equiv 0 \pmod{5^5} \text{ but } f'_{10}(t_1) \not\equiv 0 \pmod{5^6}, \qquad (5.2.15)$$

and that for $m = 25$, we have

$$f'_{25}(t_1) \equiv g'_{25}(t_1) \equiv 0 \pmod{5^9} \text{ but } g'_{25}(t_1) \not\equiv 0 \pmod{5^9}. \qquad (5.2.16)$$

For $m = 5, 10$, we therefore have

$$\mathcal{T}_m(5^v) = \{t_0\} \sqcup \left\{t_1 + 5^{2v-5}u : u \in \mathbb{Z}/5^5\mathbb{Z}\right\} \text{ for } v \geq 5, \tag{5.2.17}$$

and for $m = 25$, we have

$$\mathcal{T}_{25}(5^v) = \{t_0\} \sqcup \left\{t_1 + 5^{2v-9}u : u \in \mathbb{Z}/5^9\mathbb{Z}\right\} \text{ for } v \geq 9. \tag{5.2.18}$$

Part (e) is now clear.

Finally, part (f). From (d)–(e) we conclude that for $m = 5, 10$, we have

$$T_m(e) \leq 3126 \cdot \prod_{\substack{\ell \mid e \\ \ell \neq 5}} \left(1 + \left(\frac{-1}{\ell}\right)\right) \leq 1563 \cdot 2^{\omega(e)}, \tag{5.2.19}$$

and for $m = 25$ we have

$$T_{25}(e) \leq 8 \cdot 1953126 \cdot \prod_{\substack{\ell \mid e \\ \ell \neq 2,5}} \left(1 + \left(\frac{-1}{\ell}\right)\right) \leq 7812504 \cdot 2^{\omega(e)}, \tag{5.2.20}$$

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

m	$T_m(2^1)$	$T_m(2^2)$
5	–	–
10	2	–
25	2	2^3

Table 5.2.21: All nonzero $T_m(2^v)$ for $m \in \{5, 10, 25\}$

m	$T_m(5^1)$	$T_m(5^2)$	$T_m(5^3)$	$T_m(5^4)$
5	$1+5$	$1+5^2$	$1+5^3$	$1+5^5$
10	$1+5$	$1+5^3$	$1+5^5$	$1+5^5$
25	$1+5$	$1+5^3$	$1+5^5$	$1+5^7$

Table 5.2.22: All $T_m(5^v)$ for $m \in \{5, 10, 25\}$ and $v \leq 4$

The common factor $C_m(a, b)$

In view of Lemma 5.2.2, when $m \in \{5, 10, 25\}$, the twist minimality defect away from the primes $2, 5$ is determined by the quadratic form

$$C_5(a, b) = C_{10}(a, b) = a^2 + b^2 = b^2 h_5(a/b) = b^2 h_{10}(a/b) \tag{5.2.23}$$

or the quadratic form

$$C_{25}(a, b) = a^2 + 4b^2 = b^2 h_{25}(a/b) \tag{5.2.24}$$

respectively. For $m \in \{5, 10, 25\}$, we define

$$\mathcal{C}_m(e) := \left\{(a, b) \in \mathbb{Z}^2 : C_m(a, b) = e \text{ and } \gcd(a, b) = 1\right\}, \tag{5.2.25}$$

and note $\#\mathcal{C}_m(e) \leq 2^{\omega(e)+1}$.

Just like C_7, the polynomials $C_5 = C_{10}$ and C_{25} are both norm forms of quadratic orders with class number 1, namely $\mathbb{Z}[\zeta_4]$ or $\mathbb{Z}[2\zeta_4]$, where ζ_4 is a primitive 4th root of unity, i.e., a square root of -1. We record some elementary algebraic observations about $C_5(a, b) = C_{10}(a, b)$ and $C_{25}(a, b)$ and the associated orders $\mathbb{Z}[\zeta_4]$ and $\mathbb{Z}[2\zeta_4]$.

Lemma 5.2.26. *Let $m \in \{5, 10, 25\}$. The following statements hold.*

(a) *The right regular representation of $\mathbb{Z}[\zeta_4]$ in the basis $\{1, \zeta_4\}$ induces the map $\gamma_5 = \gamma_{10}$:*

$\mathbb{Z}^2 \to \mathrm{M}_2(\mathbb{Z})$ given by

$$\gamma_5 = \gamma_{10} : (a, b) \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \tag{5.2.27}$$

and the right regular representation of $\mathbb{Z}[2\zeta_4]$ in the basis $\{1, 2\zeta_4\}$ induces the map $\gamma_{25} : \mathbb{Z}^2 \to \mathrm{M}_2(\mathbb{Z})$ given by

$$\gamma_5 = \gamma_{10} : (a, b) \mapsto \begin{pmatrix} a & 2b \\ -2b & a \end{pmatrix}. \tag{5.2.28}$$

(b) *For all $a, b, c, d, e \in \mathbb{Z}$, we have the following implication:*

$$C_m(a, b) = e \implies e \mid C_m((c, d) \cdot \gamma_m(a, b)). \tag{5.2.29}$$

(c) *Conversely, if c', d', e, k are integers such that $k \geq 1$, $e^k \mid C_m(c', d')$, and*

$$\gcd(c', d', e) = \gcd(2, e) = 1, \tag{5.2.30}$$

then there are integers $a, b, c, d \in \mathbb{Z}$ with $(a, b) \in \mathcal{C}_m(e)$ and

$$(c', d') = (c, d) \cdot \gamma_m(a, b)^k. \tag{5.2.31}$$

Proof. The proof is essentially identical to that of Lemma 4.2.28. □

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

Theorem 5.2.32. *Let $m \in \{5, 10, 25\}$. The following statements hold.*

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

$$108C_m(a,b)^{d(m)} \le H(A_m(a,b),B_m(a,b)) \le \kappa_m C_m(a,b)^{d(m)}, \tag{5.2.33}$$

where the constants

$$\begin{aligned} \kappa_5 &= 679\,212\,199.08278056\ldots, \\ \kappa_{10} &= 211\,362\,386.0164477\ldots, \text{ and} \\ \kappa_{25} &= 26\,367\,187\,500, \end{aligned} \tag{5.2.34}$$

are algebraic numbers given by evaluating $H(A_5(a,b),B_5(a,b))$ *at appropriate roots of* (5.2.38)*, evaluating* $H(A_{10}(a,b),B_{10}(a,b))$ *at appropriate roots of* (5.2.39)*, and evaluating* $H(A_{25}(a,b),B_{25}(a,b))$ *at the appropriate roots of* (5.2.40)*, respectively.*

(b) *If* $C_m(a,b) = e_0^2 n_0$*, with* n_0 *squarefree, then* $\operatorname{tmd}(A_m(a,b),B_m(a,b)) = e_0e'$*, where* $e' \mid 5^3$ *if* $m=5$*,* $e' \mid 2\cdot 5^3$ *if* $m=10$*, and* $e' \mid 2^2\cdot 5^5$ *if* $m=25$*. We have*

$$\frac{2^2\cdot 3^3}{5^{18}}e_0^6n_0^6 \le \operatorname{twht}(A_5(a,b),B_5(a,b)) \le \kappa_5 e_0^6 n_0^6, \tag{5.2.35}$$

$$\frac{3^3}{2^4\cdot 5^{18}}e_0^{18}n_0^{12} \le \operatorname{twht}(A_{10}(a,b),B_{10}(a,b)) \le \kappa_{10} e_0^{18} n_0^{12}, \tag{5.2.36}$$

and

$$\frac{3^3}{2^{10}\cdot 5^{30}}e_0^{30}n_0^{18} \le \operatorname{twht}(A_{25}(a,b),B_{25}(a,b)) \le \kappa_{25} e_0^{30} n_0^{18}. \tag{5.2.37}$$

Proof. The proof follows the contours of Theorem 4.2.35.

Part (a) is proven exactly as in the proof of Theorem 4.2.35. The lower bound 108 of (5.2.33) is attained at $(1,0)$, and the upper bound κ_m is attained when a and b are appropriately chosen roots of

$$\begin{aligned}
&312500a^4 - 312500a^2 + 841\\
=&2^2 \cdot 5^7 \cdot a^4 - 2^2 \cdot 5^7 \cdot a^2 + 29^2, \text{ and}\\
&312500b^4 - 312500b^2 + 841\\
=&2^2 \cdot 5^7 \cdot b^4 - 2^2 \cdot 5^7 \cdot b^2 + 29^2,
\end{aligned} \tag{5.2.38}$$

if $m = 5$, and of

$$\begin{aligned}
&225000000a^{16} - 768750000a^{14} + 1004103125a^{12}\\
&- 601050000a^{10} + 139912500a^8 + 4642000a^6\\
&- 3343200a^4 - 507264a^2 + 64\\
=&2^6 \cdot 3^2 \cdot 5^8 \cdot a^{16} - 2^4 \cdot 3 \cdot 5^8 \cdot 41 \cdot a^{14} + 5^5 \cdot 321313 \cdot a^{12}\\
&- 2^4 \cdot 3 \cdot 5^5 \cdot 4007 \cdot a^{10} + 2^2 \cdot 3 \cdot 5^5 \cdot 7 \cdot 13 \cdot 41 \cdot a^8 + 2^4 \cdot 5^3 \cdot 11 \cdot 211 \cdot a^6\\
&- 2^5 \cdot 3 \cdot 5^2 \cdot 7 \cdot 199 \cdot a^4 - 2^7 \cdot 3 \cdot 1321 \cdot a^2 + 2^6, \text{ and}\\
&225000000b^{16} - 1031250000b^{14} + 1922853125b^{12} - 1879818750b^{10}\\
&+ 1039959375b^8 - 329604500b^6 + 57354675b^4\\
&- 4501086b^2 + 7225\\
=&2^6 \cdot 3^2 \cdot 5^8 \cdot b^{16} - 2^4 \cdot 3 \cdot 5^9 \cdot 11 \cdot b^{14} + 5^5 \cdot 615313 \cdot b^{12} - 2 \cdot 3^2 \cdot 5^5 \cdot 23 \cdot 1453 \cdot b^{10}\\
&+ 3 \cdot 5^5 \cdot 7 \cdot 13 \cdot 23 \cdot 53 \cdot b^8 - 2^2 \cdot 5^3 \cdot 17^2 \cdot 2281 \cdot b^6 + 3 \cdot 5^2 \cdot 7 \cdot 107 \cdot 1021 \cdot b^4\\
&- 2 \cdot 3 \cdot 89 \cdot 8429 \cdot b^2 + 5^2 \cdot 17^2
\end{aligned} \tag{5.2.39}$$

if $m = 10$, and of

$$
\begin{aligned}
&53833007812500a^{28} - 891577148437500a^{26} + 7403853759765625a^{24}\\
&- 38650180664062500a^{22} + 139358151855468750a^{20} - 361638379062500000a^{18}\\
&+ 690434893630859375a^{16} - 979823552140625000a^{14} + 1042891876273125000a^{12}\\
&- 839328158831937500a^{10} + 509588953407434375a^{8} - 227793758883072500a^{6}\\
&+ 70659569038784950a^{4} - 13323520820064520a^{2} + 1058114957485041\\
=&2^2 \cdot 3^2 \cdot 5^{15} \cdot 7^2 \cdot a^{28} - 2^2 \cdot 3 \cdot 5^{14} \cdot 7 \cdot 37 \cdot 47 \cdot a^{26} + 5^{13} \cdot 19 \cdot 319223 \cdot a^{24}\\
&- 2^2 \cdot 3 \cdot 5^{13} \cdot 13 \cdot 17 \cdot 11939 \cdot a^{22} + 2 \cdot 3 \cdot 5^{13} \cdot 739 \cdot 25747 \cdot a^{20}\\
&- 2^5 \cdot 5^{10} \cdot 197 \cdot 677 \cdot 8677 \cdot a^{18} + 5^9 \cdot 149 \cdot 2372501111 \cdot a^{16}\\
&- 2^3 \cdot 5^9 \cdot 31 \cdot 2022861527 \cdot a^{14} + 2^3 \cdot 3 \cdot 5^7 \cdot 47 \cdot 61 \cdot 10321 \cdot 18797 \cdot a^{12}\\
&- 2^2 \cdot 5^6 \cdot 11 \cdot 19 \cdot 11251 \cdot 5711029 \cdot a^{10} + 5^5 \cdot 163068465090379 \cdot a^{8}\\
&- 2^2 \cdot 5^4 \cdot 91117503553229 \cdot a^6 + 2 \cdot 5^2 \cdot 7 \cdot 43 \cdot 4694987975999 \cdot a^4\\
&- 2^3 \cdot 5 \cdot 13 \cdot 8221 \cdot 3116671381 \cdot a^2 + 3^2 \cdot 10842893^2, \text{ and}\\
&861328125000000b^{28} + 551660156250000b^{26} + 712154541015625b^{24}\\
&- 62065429687500b^{22} + 109768066406250b^{20} - 83235166015625b^{18}\\
&+ 33729880859375b^{16} - 11477761718750b^{14} + 4976470781250b^{12}\\
&- 1567605921875b^{10} + 2819493406250b^{8} - 27367628750b^{6}\\
&+ 1121883700b^4 - 210823450b^2 + 7056\\
=&2^6 \cdot 3^2 \cdot 5^{15} \cdot 7^2 \cdot b^{28} + 2^4 \cdot 3 \cdot 5^{14} \cdot 7 \cdot 269 \cdot b^{26} + 5^{13} \cdot 583397 \cdot b^{24}\\
&- 2^2 \cdot 3 \cdot 5^{13} \cdot 19 \cdot 223 \cdot b^{22} + 2 \cdot 3 \cdot 5^{13} \cdot 7 \cdot 2141 \cdot b^{20} - 5^{10} \cdot 13 \cdot 655637 \cdot b^{18}\\
&+ 5^9 \cdot 1231 \cdot 14029 \cdot b^{16} - 2 \cdot 5^9 \cdot 2938307 \cdot b^{14} + 2 \cdot 3 \cdot 5^7 \cdot 2777 \cdot 3823 \cdot b^{12}\\
&- 5^6 \cdot 7 \cdot 2011 \cdot 7127 \cdot b^{10} + 5^5 \cdot 2377 \cdot 37957 \cdot b^8 - 2 \cdot 5^4 \cdot 7 \cdot 11^2 \cdot 25849 \cdot b^6\\
&+ 2^2 \cdot 5^2 \cdot 7 \cdot 1602691 \cdot b^4 - 5 \cdot 4216469 \cdot b^2 + 2^4 \cdot 3^2 \cdot 7^2
\end{aligned}
\tag{5.2.40}
$$

if $m = 25$. For $m \in \{5, 10, 25\}$, the arguments that maximize the ratio

$$H(A_m(a,b), B_m(a,b))/C_{10}(a,b)^6 \tag{5.2.41}$$

have $27\,|B_m(a,b)|^2 > 4\,|A_m(a,b)|^3$. For the reader's information,

$$(a,b) = (0.051946913\ldots, 0.998649847\ldots) \tag{5.2.42}$$

maximizes this ratio when $m = 5$,

$$(a,b) = (-0.766646866\ldots, 0.642068986\ldots) \tag{5.2.43}$$

maximizes this ratio when $m = 10$, and

$$(a,b) = (0.447213595\ldots, 0.447213595\ldots) \tag{5.2.44}$$

maximizes this ratio when $m = 25$.

We now prove (b). Write $C_m(a,b) = e_0^2 n_0$ with n_0 squarefree, and write

$$\operatorname{tmd}(A_m(a,b), B_m(a,b)) = e_0 e'. \tag{5.2.45}$$

By 5.2.2, $e' = 2^v \cdot 5^w$ for some $v, w \geq 0$. A short computation shows that if $m = 5$ then $v = 0$, if $m = 10$ then $v \in \{0, 1\}$, and that if $m = 25$ then $v \in \{0, 1, 2\}$. On the other hand, (5.2.17) shows $w \leq \lceil 5/2 \rceil = 3$ if $m = 5, 10$, and (5.2.18) shows $w \leq \lceil 9/2 \rceil = 5$ if $m = 25$.

As

$$H(A_m(a,b), B_m(a,b)) = e_0^6\,(e')^6 \operatorname{twht}(A_m(a,b), B_m(a,b)), \tag{5.2.46}$$

we see

$$\frac{108}{(e')^6} e_0^{2d(m)-6} n_0^{d(m)} \leq \operatorname{twht}(A_m(a,b), B_m(a,b)) \leq \frac{\kappa_m}{(e')^6} e_0^{2d(m)-6} n_0^{d(m)}. \tag{5.2.47}$$

Rounding e' up to 5^3 (if $m = 5$), $2 \cdot 5^3$ (if $m = 10$), or $2^2 \cdot 5^5$ (if $m = 25$), on the left, and rounding down to 1 on the right gives the desired result. □

Note that (5.2.35), in contrast to (5.2.36) and (5.2.37), has matching exponents for e_0 and n_0. From a certain perspective, this is what makes the case $m = 5$ difficult to handle.

Corollary 5.2.48. *For $m \in \{5, 10, 25\}$, let (a, b) be a m-groomed pair. We have*

$$\operatorname{tmd}(A_5(a,b), B_5(a,b)) \leq \frac{5^6}{2^{1/3} \cdot 3^{1/2}} \operatorname{twht}(A_5(a,b), B_5(a,b))^{1/6}, \tag{5.2.49}$$

where $5^6/2^{1/3} \cdot 3^{1/2} = 7\,160.050\ldots$, and

$$\operatorname{tmd}(A_{10}(a,b), B_{10}(a,b)) \leq \frac{2^{11/9} \cdot 5^4}{3^{1/6}} \operatorname{twht}(A_{10}(a,b), B_{10}(a,b))^{1/18}, \tag{5.2.50}$$

where $2^{11/9} \cdot 5^4/3^{1/6} = 1\,214.186\ldots$, and

$$\operatorname{tmd}(A_{25}(a,b), B_{25}(a,b)) \leq \frac{2^{211/90} \cdot 5^6}{3^{1/12}} \operatorname{twht}(A_{25}(a,b), B_{25}(a,b))^{1/30}, \tag{5.2.51}$$

where $2^{211/90} \cdot 5^6/3^{1/12} = 72\,411.579\ldots$.

Proof. We prove the case $m = 10$; the cases $m = 5$ and $m = 25$ are entirely similar. In the notation of Theorem 5.2.32(c),

$$\frac{3^3}{2^4 \cdot 5^{18}} e_0^{18} n_0^{12} \leq \operatorname{twht}(A_{10}(a,b), B_{10}(a,b)) \leq \kappa_{10} e_0^{18} n_0^{12} \tag{5.2.52}$$

Multiplying through by $(e')^{18}$, rounding n_0 down to 1 on the left, rounding e' up to $2 \cdot 5^3$ on the right, and taking 18th roots of both sides, we obtain the desired result. □

Section 5.3

Estimates for twist classes for $m = 10, 25$

In this section, we use section 3.5 to estimate $N_m^{\mathrm{tw}}(X)$ for $m = 10, 25$, counting the number of twist minimal elliptic curves over $\mathbb{Q}$ admitting a m-isogeny for $m = 10, 25$. We also indicate why our method fails for $m = 5$.

Recall (3.5.6), (3.5.33), and (3.5.34). By section 3.2, $M_m(X; e)$ counts pairs $(a, b) \in \mathbb{Z}^2$ with

- (a, b) m-groomed,
- $H(A_m(a, b), B_m(a, b)) \leq X$, and
- $e \mid \operatorname{tmd}(A_m(a, b), B_m(a, b))$.

The following proposition refines Lemma 3.5.7, and specifies both an order of growth and an explicit upper bound past which the summands of (3.5.8) vanish when $m \in \{5, 10, 25\}$.

Proposition 5.3.1. *For $m \in \{5, 10, 25\}$, we have*

$$\widetilde{N}_m^{\mathrm{tw}}(X) = \sum_{n \ll X^{1/(2d(m)-6)}} \sum_{e \mid n} \mu(n/e) M_m(e^6 X; n); \tag{5.3.2}$$

more precisely, if $m = 5$ we can restrict our sum to

$$n \leq \frac{5^6}{2^{1/3} \cdot 3^{1/2}} \cdot X^{1/6}, \tag{5.3.3}$$

if $m = 10$ we can restrict our sum to

$$n \leq \frac{2^{11/9} \cdot 5^4}{3^{1/6}} \cdot X^{1/18}, \tag{5.3.4}$$

and if $m = 25$*, we can restrict our sum to*

$$n \leq \frac{2^{7/3} \cdot 5^6}{3^{1/10}} X^{1/18}. \tag{5.3.5}$$

Proof. We prove the case $m = 10$ by way of illustration, although the argument precisely mirrors Proposition 4.3.1. Let $(a, b) \in \mathbb{Z}^2$, and suppose $H(A_{10}(a, b), B_{10}(a, b)) \leq e^6 X$ and $e \mid \operatorname{tmd}(A_{10}(a, b), B_{10}(a, b))$. If we can prove

$$e \leq \frac{2^{11/9} \cdot 5^4}{3^{1/6}} \cdot X^{1/18}, \tag{5.3.6}$$

then our claim will follow.

Write $C_{10}(a, b) = e_0^2 n_0$, with n_0 square-free. By Theorem 5.2.32(a), we have

$$108 e_0^{24} n_0^{12} \leq e^6 X. \tag{5.3.7}$$

On the other hand, by Theorem 5.2.32(b), we have $e \mid 2 \cdot 5^3 \cdot e_0$, and *a fortiori*

$$e \leq 2 \cdot 5^3 e_0. \tag{5.3.8}$$

Multiplying (5.3.7) through by $(2 \cdot 5^3)^{24}$ and utilizing (5.3.8), we conclude

$$2^2 \cdot 3^3 e^{24} n_0^{12} \leq 2^{24} \cdot 5^{72} e^6 X. \tag{5.3.9}$$

Rounding n_0 down to 1 and rearranging, we obtain (5.3.6). □

Let $m \in \{5, 10, 25\}$. As in section 4.3, in order to estimate $M_m(X; e)$, we further unpack the m-groomed condition on pairs (a, b). For the reader's convenience, we recall from Table 3.2.13 that $\mathscr{C}_5 = \{11/2, \infty\}$, $\mathscr{C}_{10} = \{-2, 0, 1/2, \infty\}$, and $\mathscr{C}_{25} = \{1, \infty\}$. Exactly as in section 4.3, for $m \in \{5, 10, 25\}$ we let $M_m(X; d, e)$ denote the number of pairs $(a, b) \in \mathbb{Z}^2$ with

- $\gcd(da, db, e) = 1$, $b > 0$, and $a/b \notin \mathscr{C}_m$;
- $H(A_m(da, db), B_m(da, db)) \leq X$;
- $e \mid \operatorname{tmd}(A_m(da, db), B_m(da, db))$;

By Theorem 5.2.32, and because $H(A_m(a, b), B_m(a, b))$ is homogeneous of degree $2d\,(m)$, another Möbius sieve yields

$$M_m(X; e) = \sum_{\substack{d \ll X^{1/2d(m)} \\ \gcd(d,e)=1}} \mu(d) M_m(X; d, e). \tag{5.3.10}$$

The following lemma gives asymptotics for $M_m(X)$, which depend on the observation that the largest square dividing $C_m(a, b)$ is essentially the square of the twist minimality defect. Once we have Lemma 5.3.12, the rest of our argument proceeds along the lines given in the paragraph after (4.3.9), and the type III additive reduction for the elliptic surface

$$y^2 = x^3 + f_m(t)x + g_m(t) \tag{5.3.11}$$

has no additional relevance.

Lemma 5.3.12. *Let $m \in \{5, 10, 25\}$. The following statements hold.*

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

$$M_m(X; d, e) = \frac{R_m T_m(e) X^{1/d(m)}}{d^2 e^2} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell}\right) + O\left(\frac{2^{\omega(e)} X^{1/2d(m)}}{de}\right) \tag{5.3.13}$$

for $X, d, e \geq 1$. where R_m is the area of (3.3.5).

(b) *We have*

$$M_m(X;e) = \frac{R_m T_m(e) X^{1/d(m)}}{\zeta(2) e^2 \prod_{\ell \mid e}\left(1+\frac{1}{\ell}\right)} + O\left(\frac{2^{\omega(e)} X^{1/2d(m)} \log X}{e}\right) \tag{5.3.14}$$

for $X \geq 2$, $d, e \geq 1$.

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

As with Lemma 4.3.16, we prove Lemma 5.3.12 by means of two partial proof. The first proof gives an intuitive interpretation of the coefficient of $X^{1/d(m)}$, and generalizes readily to other elliptic surfaces with type III additive reduction. It differs from the first proof of Lemma 4.3.16 only in that we sum over congruence classes modulo e^2 rather than e^3. The second proof leverages the observation that $C_m(a,b)$ is the norm of the order $\mathbb{Z}[\zeta_4]$ or $\mathbb{Z}[2\zeta_4]$ to give an enhanced error term.

We write out the first proof to give a flavor for the differences between the case $m = 7$ and the cases $m \in \{5, 10, 25\}$, but largely omit the write-up of the second proof to spare the readers' time.

First proof of Lemma 5.3.12. Our proof mirrors that of Lemma 4.3.16. Let $m \in \{5, 10, 25\}$. We begin with (a) and examine the summands $M_m(X; d, e)$. If d and e are not coprime, then $M_m(X; d, e) = 0$ 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 $M_m(X; 1, e)$ to the pairs counted by $M_m(d^{2d(m)}X; d, e)$ given by $(a, b) \mapsto (da, db)$.

Combining Lemma 5.2.10(b) and Corollary 3.3.11, we have

$$\begin{aligned}
M_m(X;1,e) &= \sum_{(a_0,b_0)\in\widetilde{\mathcal{T}}_m(e)} \#\{(a,b)\in\mathcal{R}_m(X)\cap\mathbb{Z}^2 : (a,b)\equiv(a_0,b_0) \pmod{e^2}, (a,b)\notin\mathscr{C}_m\} \\
&= \varphi(e^2)T_m(e)\left(\frac{R_mX^{1/d(m)}}{e^4}+O\left(\frac{X^{1/2d(m)}}{e^2}\right)\right) \\
&= \frac{R_mT_m(e)X^{1/d(m)}}{e^2}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)+O(T_m(e)X^{1/2d(m)}),
\end{aligned} \tag{5.3.15}$$

and thus

$$M_m(X;d,e) = \frac{R_mT_m(e)X^{1/d(m)}}{d^2e^2}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)+O\left(\frac{T_m(e)X^{1/2d(m)}}{d}\right). \tag{5.3.16}$$

For part (b), we compute

$$\begin{aligned}
M_m(x;e) &= \sum_{\substack{d\ll X^{1/2d(m)}\\ \gcd(d,e)=1}} \mu(d)M_m(X;d,e) \\
&= \sum_{\substack{d\ll X^{1/2d(m)}\\ \gcd(d,e)=1}} \mu(d)\left(\frac{T_m(e)R_mX^{1/d(m)}}{d^2e^2}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)+O\left(T_m(e)\frac{X^{1/2d(m)}}{d}\right)\right) \\
&=\frac{R_mT_m(e)X^{1/d(m)}}{e^2}\prod_{\ell\mid e}\left(1-\frac{1}{\ell}\right)\sum_{\substack{d\ll X^{1/2d(m)}\\ \gcd(d,e)=1}}\frac{\mu(d)}{d^2} \\
&\quad +O\left(T_m(e)X^{1/2d(m)}\sum_{\substack{d\ll X^{1/2d(m)}\\ \gcd(d,e)=1}}\frac{1}{d}\right).
\end{aligned} \tag{5.3.17}$$

We plug the straightforward estimates

$$\sum_{\substack{d\ll X^{1/2d(m)}\\ \gcd(d,e)=1}}\frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)}\prod_{\ell\mid e}\left(1-\frac{1}{\ell^2}\right)^{-1}+O(X^{-1/2d(m)}) \tag{5.3.18}$$

and

$$\sum_{d \leq X^{1/2d(m)}} \frac{1}{d} = \frac{1}{2d\,(m)} \log X + O(1) \tag{5.3.19}$$

into (5.3.17), along with Lemma 5.2.10(f). Simplifying, we now obtain

$$M_m(x;e) = \frac{R_m T_m(e) X^{1/d(m)}}{\zeta(2) e^2 \prod_{\ell \mid e} \left(1 + \frac{1}{\ell}\right)} + O(2^{\omega(e)} X^{1/2d(m)} \log X), \tag{5.3.20}$$

which proves (b). □

Second proof of Lemma 5.3.12. This proof is, *mutatis mutandis*, the same as the proof we gave for Lemma 4.3.16. However, when we apply Lemma 5.2.26(c), we do so with $k = 2$ rather than $k = 3$. □

Let $\kappa \in \mathbb{R}$. We write

$$\varphi_\kappa(n) := \sum_{d \mid n} \mu(n/d) d^\kappa = n^\kappa \prod_{\ell \mid n} \left(1 - \frac{1}{\ell^\kappa}\right) \tag{5.3.21}$$

for the generalized Jordan totient function.

For $m = 10, 25$, we let

$$Q_m := \sum_{n \geq 1} \frac{\varphi_{6/d(m)}(n) T_m(n)}{n^2 \prod_{\ell \mid n} \left(1 + \frac{1}{\ell}\right)}. \tag{5.3.22}$$

Note that the sum defining Q_m diverges when $m = 5$! We let

$$c_m^{\text{tw}} := \frac{Q_m R_m}{\zeta(2)}. \tag{5.3.23}$$

Here, as always, R_m is the area of the region

$$\mathcal{R}_m(1) = \left\{(a,b) \in \mathbb{R}^2 : H(A_m(a,b), B_m(a,b)) \leq 1, b \geq 0\right\}. \tag{5.3.24}$$

We are now in a position to estimate $N^{\mathrm{tw}}_{m,\leq y}(X)$. Here, at last, we must leave $m = 5$ behind.

Lemma 5.3.25. *Let $m \in 10, 25$. Suppose $y \ll X^{1/2d(m)}$. Then*

$$N^{\mathrm{tw}}_{m,\leq y}(X) = \frac{Q_m R_m X^{1/d(m)}}{\zeta(2)} + O\left(\max\left(\frac{X^{1/d(m)}\log y}{y^{1-6/d(m)}}, X^{1/2d(m)}y^{3/d(m)}\log X\log^2 y\right)\right) \tag{5.3.26}$$

for $X, y \geq 2$. The constant c^{tw}_m is given in (5.3.23).

Proof. Substituting the asymptotic for $M_m(X;e)$ from Lemma 5.3.12(b) into the defining series (3.5.18) for $N^{\mathrm{tw}}_{m,\leq y}(X)$, we have

$$N^{\mathrm{tw}}_{m,\leq y}(X) = \sum_{n\leq y}\sum_{e|n}\mu\left(n/e\right)\left(\frac{R_m T_m(n)e^{6/d(m)}X^{1/d(m)}}{\zeta(2)n^2\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} + O\left(\frac{2^{\omega(n)}e^{3/d(m)}X^{1/2d(m)}\log X}{n}\right)\right). \tag{5.3.27}$$

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

$$\sum_{n\leq y}\sum_{e|n}\mu\left(n/e\right)\frac{R_m T_m(n)e^{6/d(m)}X^{1/d(m)}}{\zeta(2)n^2\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} = \frac{R_m X^{1/d(m)}}{\zeta(2)}\sum_{n\leq y}\frac{\varphi_{6/d(m)}(n)T_m(n)}{n^2\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)}. \tag{5.3.28}$$

By Lemma 5.2.10(f), we see

$$\frac{\varphi_{6/d(m)}(n)T_m(n)}{n^2\prod_{\ell|n}\left(1+\frac{1}{\ell}\right)} = O\left(\frac{2^{\omega(n)}}{n^{2-6/d(m)}}\right). \tag{5.3.29}$$

By Corollary 3.4.6 and Corollary 3.4.42, we have

$$\sum_{n>y}\frac{2^{\omega(n)}}{n^{2-6/d(m)}} \sim \frac{d\left(m\right)\log y}{(d\left(m\right)-6)\zeta(2)y^{1-6/d(m)}} \tag{5.3.30}$$

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

$$\sum_{n>y} \frac{\varphi_{6/d(m)}(n) T_m(n)}{n^2 \prod_{\ell \mid n} \left(1+\frac{1}{\ell}\right)} = O\left(\frac{2^{\omega(n)}}{n^{2-6/d(m)}}\right) = O\left(\sum_{n>y} \frac{2^{\omega(n)}}{n^{2-6/d(m)}}\right) = O\left(\frac{\log y}{y^{1-6/d(m)}}\right), \quad (5.3.31)$$

so the series

$$\sum_{n\geq 1} \frac{\varphi_{6/d(m)}(n) T_m(n)}{n^2 \prod_{\ell \mid n} \left(1+\frac{1}{\ell}\right)} = Q_m \quad (5.3.32)$$

is absolutely convergent, and

$$\begin{aligned}\sum_{n\leq y} \sum_{e \mid n} \mu\left(n/e\right) \frac{R_m T_m(n) e^{6/d(m)} X^{1/d(m)}}{\zeta(2) n^2 \prod_{\ell \mid n} \left(1+\frac{1}{\ell}\right)} &= \frac{R_7 X^{1/6}}{\zeta(2)} \left(Q_m + O\left(\frac{\log y}{y^{1-6/d(m)}}\right)\right) \\ &= c_m^{\text{tw}} X^{1/6} + O\left(\frac{X^{1/6} \log y}{y^{1-d(m)/6}}\right).\end{aligned} \quad (5.3.33)$$

As the summands of (4.3.49) constitute a nonnegative multiplicative arithmetic function, we can factor Q_m as an Euler product. We have

$$Q_m = Q_m(2) Q_m(5) \prod_{\substack{p\neq 5 \text{ prime} \\ p \equiv 1 \pmod 4}} \left(1 + \frac{2p\left(p^{6/d(m)}-1\right)}{(p+1)\left(p^2 - p^{6/d(m)}\right)}\right).; \quad (5.3.34)$$

by Lemma 5.2.10 the terms $Q_m(p)$ can be computed as follows:

$$\begin{aligned} Q_m(p) &:= \sum_{a\geq 0} \frac{\varphi_{6/d(m)}(p^a)T_m(p^a)}{(1+1/p)\,p^{2a}} \\ &= \begin{cases} 1+\frac{2p\left(p^{6/d(m)}-1\right)}{(p+1)\left(p^2-p^{6/d(m)}\right)}, & \text{if } p\equiv 1 \pmod 4 \text{ and } p\neq 5; \\ \frac{1}{3}\left(2+\sqrt{2}\right), & \text{if } m=10 \text{ and } p=2; \\ \frac{2}{31}\left(15+13\sqrt{5}\right), & \text{if } m=10 \text{ and } p=5; \\ \frac{1}{3}\left(2+2^{2/3}\right), & \text{if } m=25 \text{ and } p=5; \\ \frac{2}{781}\left(375+15\cdot 5^{1/3}+313\cdot 5^{2/3}\right), & \text{if } m=25 \text{ and } p=5; \\ 1 & \text{else.} \end{cases} \end{aligned} \tag{5.3.35}$$

The square and cubic roots appear in (5.3.35) because of the generalized Jordan totient functions $\varphi_{1/2}$ and $\varphi_{1/3}$. For instance, for $m=25$ and $p=2$ we have

$$\begin{aligned} Q_{25}(2) &= 1+\frac{\varphi_{1/3}(2)T_{25}(2)}{(1+1/2)\,2^2}+\frac{\varphi_{1/3}(2^2)T_{10}(2^2)}{(1+1/2)\,2^4} \\ &= 1+\frac{(2^{1/3}-1)2}{(1+1/2)\,2^2}+\frac{\left(2^{2/3}-2^{1/3}\right)2^3}{(1+1/2)\,2^4} \\ &= \frac{1}{3}\left(2+2^{2/3}\right). \end{aligned} \tag{5.3.36}$$

We now turn to the error term. Since $y \ll X^{1/2d(m)}$, for $e\leq y$ we have $\log(e^6X)\ll\log X$. We obtain

$$\begin{aligned} &\sum_{n\leq y}\sum_{e\mid n}\mu\left(n/e\right)O\left(\frac{2^{\omega(n)}e^{3/d(m)}X^{1/2d(m)}\log X}{n}\right) \\ =&O\left(X^{1/2d(m)}\log X\sum_{e\leq y}\frac{2^{\omega(e)}}{e^{1-3/d(m)}}\sum_{f\leq y/e}\frac{2^{\omega(f)}}{f}\right). \end{aligned} \tag{5.3.37}$$

Using Corollary 3.4.42 and Corollary 3.4.6 in tandem, we obtain

$$\begin{aligned} &O\left(X^{1/2d(m)}\log X\sum_{e\leq y}\frac{2^{\omega(e)}}{e^{1-3/d(m)}}\sum_{f\leq y/e}\frac{2^{\omega(f)}}{f}\right) \\ =&O\left(X^{1/2d(m)}\log X\sum_{e\leq y}\frac{2^{\omega(e)}}{e^{1-3/d(m)}}\log(y/e)\right) \\ =&O\left(X^{1/2d(m)}y^{3/d(m)}\log X\log^2 y\right), \end{aligned} \tag{5.3.38}$$

which proves our desired result. □

We emphasize that the proof of Lemma 5.3.25 has given us the following Euler product expansion for Q_m:

$$Q_m = Q_m(2)Q_m(5)\prod_{\substack{p\neq 5 \text{ prime} \\ p\equiv 1 \pmod 4}}\left(1+\frac{2p\left(p^{6/d(m)}-1\right)}{(p+1)\left(p^2-p^{6/d(m)}\right)}\right), \tag{5.3.39}$$

where

$$\begin{aligned} Q_{10}(2) &= \frac{1}{3}\left(2+\sqrt{2}\right), \\ Q_{10}(5) &= \frac{2}{31}\left(15+13\sqrt{5}\right), \\ Q_{25}(2) &= \frac{1}{3}\left(2+2^{2/3}\right), \text{ and} \\ Q_{25}(5) &= \frac{2}{781}\left(375+15\cdot 5^{1/3}+313\cdot 5^{2/3}\right). \end{aligned} \tag{5.3.40}$$

We now bound $N^{\text{tw}}_{m,>y}(X)$ for $m\in\{10,25\}$. Our proof here follows the archetype set by Lemma 4.3.60.

Lemma 5.3.41. *Let $m=10,25$. We have*

$$N^{\text{tw}}_{m,>y}(X) = O\left(\frac{X^{1/d(m)}\log y}{y^{1-6/d(m)}}\right) \tag{5.3.42}$$

for $X, y\geq 2$.

Proof. By Lemma 5.2.10, $T_m(e) = O(2^{\omega(e)})$, so by Lemma 5.3.12, we have

$$M_m(X;e) = O\left(\frac{2^{\omega(e)}X^{1/d(m)}}{e^2}\right). \tag{5.3.43}$$

Now by Proposition 3.5.14, we see

$$N^{\mathrm{tw}}_{m,>y}(X) = O\left(\sum_{n>y}\frac{2^{\omega(n)}X^{1/d(m)}}{n^{2-6/d(m)}}\right). \tag{5.3.44}$$

Combining Corollary 3.4.42 and Corollary 3.4.6, we conclude

$$N^{\mathrm{tw}}_{m,>y}(X) = O\left(\frac{X^{1/d(m)}\log y}{y^{1-6/d(m)}}\right) \tag{5.3.45}$$

as desired. □

We are now ready to prove Theorem 1.2.13 for $m = 10, 25$, which we restate here with a modestly improved error term in the notations we have established.

Theorem 5.3.46. *Let $m = 10, 25$. Then we have*

$$N^{\mathrm{tw}}_m(X) = c^{\mathrm{tw}}_m X^{1/d(m)} + O\left(X^{1/2(d(m)-3)}\log^{(d(m)+3)/(d(m)-3)} X\right) \tag{5.3.47}$$

for $X \geq 2$. The constant c^{tw}_m is given in (5.3.23). The implicit constant depends only on m.

Proof. Let $m = 10, 25$, and let y be a positive quantity with $y \ll X^{1/2d(m)}$; in particular, $\log y \ll \log X$. Lemma 5.3.25 and Lemma 5.3.41 together tell us

$$N^{\mathrm{tw}}_7(X) = c^{\mathrm{tw}}_m X^{1/d(m)} + O\left(\max\left(\frac{X^{1/d(m)}\log y}{y^{1-6/d(m)}}, X^{1/2d(m)}y^{3/d(m)}\log X\log^2 y\right)\right). \tag{5.3.48}$$

We let $y = X^{1/2(d(m)-3)} \log^{2d(m)/(d(m)-3)} X$, so

$$\frac{X^{1/d(m)} \log y}{y^{1-6/d(m)}} \asymp X^{1/2d(m)} y^{3/d(m)} \log X \log^2 y \asymp X^{1/2(d(m)-3)} \log^{(d(m)+3)/(d(m)-3)} X, \tag{5.3.49}$$

and we conclude

$$N_m^{\mathrm{tw}}(X) = c_m^{\mathrm{tw}} X^{1/d(m)} + O\left(X^{1/2(d(m)-3)} \log^{(d(m)+3)/(d(m)-3)} X\right) \tag{5.3.50}$$

as desired. □

Remark 5.3.51. When $m = 5$, we can follow the proof of Lemma 5.3.25 up through (5.3.29), but here we are stymied by a lack of understanding of the series

$$\sum_{n \leq y} \frac{\varphi(n) T_5(n)}{n^2 \prod_{\ell \mid n} \left(1 + \frac{1}{\ell}\right)} \tag{5.3.52}$$

appearing on the right-hand side of (5.3.28), which is $O(\log y)$ when $m = 5$. We suspect that (5.3.52) behaves similarly to the harmonic sum $\sum_{n \leq y} 1/n$, and that for appropriately chosen constants Q_5 and Q_5' we may write

$$\sum_{n \leq y} \frac{\varphi(n) T_5(n)}{n^2 \prod_{\ell \mid n} \left(1 + \frac{1}{\ell}\right)} = Q_5 \log y + Q_5' + O(1/y). \tag{5.3.53}$$

Even assuming (5.3.53), however, we find ourselves obstructed by Lemma 5.3.41: to handle $m = 5$, we would require not only a bound on $N_{5,>y}^{\mathrm{tw}}(X)$, but an asymptotic estimate for $N_{5,>y}^{\mathrm{tw}}(X)$ with a power-saving error term. This is far more than Lemma 5.3.41 aspires to offer. We conjecture that for every $\epsilon > 0$ we have

$$\widetilde{N}_5^{\mathrm{tw}}(X), N_5^{\mathrm{tw}}(X) = c_5^{\mathrm{tw}} X^{1/6} \log X + c_5^{\mathrm{tw}\prime} X^{1/6} + O(X^{1/12+\epsilon}). \tag{5.3.54}$$

If so, the associated Dirichlet series $\widetilde{L}_5^{\mathrm{tw}}(s)$ and $L_5^{\mathrm{tw}}(s)$ will have a double pole at $s = 1/6$, in contrast to the Dirichlet series $L_7^{\mathrm{tw}}(s)$ studied in Corollary 4.3.66, which has a simple pole at $s = 1/6$. Given (5.3.54), it would be straightforward to obtain asymptotics for $\widetilde{N}_5(X)$ and $N_5(X)$ with power-saving error terms.

We do not believe that the case $m = 5$ is intractable, but we have little hope that the sieving methods we employ in this thesis will unlock this case. We suspect other methods, such as Poisson summation, may achieve better results.

L-series

To conclude this section, we set up section 5.4 by interpreting Theorem 5.3.46 in terms of Dirichlet series. Recall (3.5.22), (3.5.23), (3.5.24), and (3.5.25).

Corollary 5.3.55. *Let $m = 10, 25$. The following statements hold.*

(a) The Dirichlet series $L_m^{\mathrm{tw}}(s)$ has abscissa of (absolute) convergence $\sigma_a = \sigma_c = 1/d(m)$ and has a meromorphic continuation to the region

$$\{s = \sigma + it \in \mathbb{C} : \sigma > 1/2(d(m) - 3)\}. \tag{5.3.56}$$

(b) The function $L_m^{\mathrm{tw}}(s)$ has a simple pole at $s = 1/d(m)$ with residue

$$\operatorname{res}_{s=\frac{1}{d(m)}} L_m^{\mathrm{tw}}(s) = \frac{c_m^{\mathrm{tw}}}{d(m)}; \tag{5.3.57}$$

it is holomorphic elsewhere on the region (5.3.56).

(c) We have

$$\mu_{L_m^{\mathrm{tw}}}(\sigma) < 13/84 \tag{5.3.58}$$

for $\sigma > 1/(2d(m) - 3)$.

Proof. The proof is structurally identical to the one given for Corollary 4.3.66. □

Section 5.4

Estimates for rational isomorphism classes for $m = 10, 25$

In 5.3, we counted the number of elliptic curves over $\mathbb{Q}$ with a (cyclic) m-isogeny up to quadratic twist (Theorem 5.3.46) for $m = 10, 25$. In this section, we count all isomorphism classes over $\mathbb{Q}$ by enumerating over twists using Landau's Tauberian theorem (Theorem 3.4.37). We first describe the analytic behavior of $L_m(s)$ for $m = 10, 25$.

Theorem 5.4.1. *Let $m = 10, 25$. The following statements hold.*

(a) *The Dirichlet series $L_m(s)$ has a meromorphic continuation to the region*

$$\{s = \sigma + it \in \mathbb{C} : \sigma > 1/12\} \tag{5.4.2}$$

with a simple pole at $s = 1/6$ and no other singularities on this region.

(b) *The principal part of $L_m(s)$ at $s = 1/6$ is*

$$\frac{L_m^{\mathrm{tw}}(1/6)}{3\zeta(2)} \left(s - \frac{1}{6}\right)^{-1}. \tag{5.4.3}$$

Proof. We proceed as in the proof of Theorem 4.4.1. For (a), since $\zeta(s)$ is nonvanishing when $\sigma > 1$, the ratio $\zeta(6s)/\zeta(12s)$ is meromorphic function for $\sigma > 1/12$. But Corollary 5.3.55 gives a meromorphic continuation of $L_m^{\mathrm{tw}}(s)$ to the region (5.4.2). By Theorem 3.5.26, the function $L_m(s)$ is a product of these two meromorphic functions on (5.4.2), and so it is a meromorphic function on this region. The holomorphy and singularity for $L_m(s)$ then follow from those of $L_m^{\mathrm{tw}}(s)$ and $\zeta(s)$.

We conclude (b) by computing Laurent expansions. We recall (4.4.4), and of course the Laurent expansion for $L_m^{\mathrm{tw}}(s)$ at $s = 1/6$ begins

$$L_m^{\mathrm{tw}}(s) = L_m^{\mathrm{tw}}(1/6) + \dots . \tag{5.4.4}$$

Multiplying the Laurent series tails gives the desired result. □

Using Theorem 5.4.1, we deduce the following lemma.

Lemma 5.4.5. *Let* $m = 10, 25$. *The sequence* $(\Delta N_m(n))_{n \geq 1}$ *is admissible* (Definition 3.4.36) *with parameters* $(1/6, 1/12, 13/84)$.

Proof. The proof is similar to, but simpler than, the one given for Lemma 4.4.6. The critical difference is this: by Corollary 5.3.55, the Dirichlet series defining $L_m^{\mathrm{tw}}(s)$ converges absolutely when $\sigma = \mathrm{Re}(s) > 1/12$.

Let $m \in \{10, 25\}$. We check each condition in Definition 3.4.36. Since $\Delta N_m(n)$ counts objects, we indeed have $\Delta N_7(n) \in \mathbb{Z}_{\geq 0}$.

For (i), note $\dfrac{\zeta(6s)}{\zeta(12s)}$ has 1/6 as its abscissa of absolute convergence. Now by Theorem 3.5.26(b), we have

$$L_m(s) = \frac{2\zeta(6s)L_m^{\mathrm{tw}}(s)}{\zeta(12s)}, \tag{5.4.6}$$

and by Theorem 3.4.20 this series converges absolutely for $\sigma > 1/6$, so the abscissa of absolute convergence for $L_m(s)$ is at most 1/6. But for $\sigma < 1/6$, we have

$$L_m(\sigma) > \frac{2\zeta(6s)}{\zeta(12s)} \tag{5.4.7}$$

by termwise comparison of coefficients, so the Dirichlet series for $L_m(s)$ diverges when $\sigma < 1/6$, and (i) holds with $\sigma_a = 1/6$.

For (ii), 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

$$\delta = 1/6 - 1/12 = 1/12. \tag{5.4.8}$$

(The only pole of $L_m(s)/s$ with $\sigma > 1/12$ is the simple pole at $s = 1/6$ indicated in Theorem 5.4.1(b).)

For (iii), let $\sigma > 1/12$. By Theorem 3.4.30, $\mu_{L_m^{\mathrm{tw}}}(\sigma) = 0$. Recall the notation $\zeta_a(s) = \zeta(as)$. As in (4.4.9), we have

$$\mu_{\zeta_6}(\sigma) < \frac{13}{84} \tag{5.4.9}$$

if $\sigma \leq 1/6$, and by Theorem 3.4.30, $\mu_{\zeta_6}(\sigma) = 0$ if $\sigma > 1/6$. Finally, as $\zeta(12s)^{-1}$ is absolutely convergent for $s > 1/12$, Theorem 3.4.30 tells us $\mu_{\zeta_{12}{}^{-1}}(\sigma) = 0$. Taken together, we see

$$\mu_{L_m}(\sigma) < 0 + \frac{13}{84} + 0 = \frac{13}{84}, \tag{5.4.10}$$

so the sequence $(\Delta N_m(n))_{n\geq 1}$ is admissible with final parameter $\xi = 13/84$. □

We now prove Theorem 1.2.6 for $m = 10, 25$, which we restate here for ease of reference in our established notation.

Theorem 5.4.11. *Let $m = 10, 25$, and define*

$$c_m := \frac{2L_m^{\mathrm{tw}}(1/6)}{\zeta(2)}. \tag{5.4.12}$$

Then for all $\epsilon > 0$, we have

$$N_m(X) = c_m X^{1/6} + O\left(X^{1/8+\epsilon}\right) \tag{5.4.13}$$

for $X \geq 1$. The implicit constant depends only on ϵ.

Proof. By Lemma 5.4.5, $(\Delta N_m(n))_{n\geq 1}$ is admissible with parameters $(1/6, 1/12, 13/42)$. We now apply Theorem 3.4.37 to the Dirichlet series $L_m(s)$, and our claim follows. □

Remark 5.4.14. We suspect that the true error on $N_m(X)$ is at most $O(X^{1/12+\epsilon})$, and the true error on $N_m^{\mathrm{tw}}(X)$ is at most $O(X^{1/2d(m)+\epsilon})$, but we have been unable to bound the error terms this far using our techniques. See Remark 4.4.14 for some related thoughts.

Section 5.5

Computations for $m = 10, 25$

In this section, we furnish computations that make Theorem 5.3.46 and Theorem 5.4.11 completely explicit.

Enumerating elliptic curves with m-isogeny for $m = 10, 25$

The algorithm described in section 4.5 can be adapted to enumerate elliptic curves admitting a cyclic m-isogeny for $m = 10, 25$. Doing so requires paying special attention to the primes 2 and 5, rather than 3 and 7, and of course requires writing $C_m(a, b) = e_0^2 n_0$ rather than $e_0^3 n_0$. In addition, when $m = 10$, the lookup table we generate in step 2 is restricted to pairs (a, b) with $a \geq b$ to avoid generating redundant pairs by multiplying associates; to restore our full complement of possibilities, in step 3 we take products and powers not only of the elements in our lookup table with $C(a_m, b_m) = m$ and $C(a_e, b_e) = e_0$, but also products of their conjugates.

For $m = 10$, running our algorithm out to $X = 10^{96}$ in Python took us approximately 17 CPU hours on a single core, producing 106 785 277 elliptic curves admitting a cyclic 10-isogeny. To check the accuracy of our code, we confirmed that the j-invariants of these curves are distinct. For $X = 10^{96}$, we have

$$\frac{N_{10}^{\mathrm{tw}}(10^{96})}{c_{10}^{\mathrm{tw}}(10^{96})^{1/12}} = 0.999\,671\ldots, \tag{5.5.1}$$

which is close to 1. We compute c_{10}^{tw} below.

For $m = 25$, running our algorithm out to $X = 10^{138}$ took us approximately 10 CPU hours on a single core, producing 34 908 299 elliptic curves admitting a cyclic 25-isogeny. To check the accuracy of our code, we confirmed that the j-invariants of these curves are distinct. For $X = 10^{138}$, we have

$$\frac{N_{25}^{\mathrm{tw}}(10^{138})}{c_{25}^{\mathrm{tw}}(10^{138})^{1/18}} = 0.997\,115\ldots, \tag{5.5.2}$$

which is close to 1. We compute c_{10}^{tw} below. It is interesting to note that the ratios in (4.5.4), (5.5.1), (5.5.2) are all less than 1. We do not know if this bias is systematic or coincidental.

We list the first few twist minimal elliptic curves admitting a cyclic 10-isogeny in Table 5.5.3, and the first few twist minimal elliptic curves admitting a cyclic 25-isogeny in Table 5.5.4.

(A, B)	(a, b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(6, 88)$	$(3, 1)$	209088	125
$(-66, 200)$	$(-1, 3)$	1149984	125
$(-435, 4750)$	$(4, 3)$	609187500	250
$(6981, 92950)$	$(8, 1)$	1360858296564	250
$(-7635, 256750)$	$(-3, 4)$	1780275091500	125
$(-8130, 187000)$	$(1, 7)$	2149471188000	125
$(-4035, 474050)$	$(2, 1)$	6067531867500	2
$(-26571, 1570426)$	$(2, 9)$	75038421469644	250
$(-29370, 1937000)$	$(-7, 1)$	101337883812000	125
$(-30459, 774358)$	$(-1, 8)$	113033431970316	125
$(-65091, 6383806)$	$(-4, 7)$	1103120162194284	250
$(-77979, 8511050)$	$(6, 7)$	1955825246767500	250
$(-46371, 10131550)$	$(7, 4)$	2771504245867500	125
$(-119235, 15795650)$	$(-1, 2)$	6780648933211500	1
$(-280227, 56930654)$	$(-12, 1)$	88021734784228332	250
$(-405507, 980606)$	$(1, 12)$	266719677879435372	125
$(-418251, 104112250)$	$(-9, 2)$	292665112764269004	125
$(-504570, 137620600)$	$(1, 3)$	513835691175972000	1

Table 5.5.3: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 10-isogeny and $\mathrm{twht}\, E \leq 10^{18}$

(A, B)	(a, b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(-12, 38)$	$(-4, 1)$	38988	12500
$(-4035, 98750)$	$(-3, 2)$	263292187500	3125
$(-8634, 308792)$	$(6, 1)$	2574519136416	12500
$(-11586, 480008)$	$(-2, 3)$	6221007361728	12500
$(-281532, 57496282)$	$(0, 1)$	89257205983235148	4
$(622149, 500328938)$	$(-9, 1)$	6758884247405611788	3125
$(-1768386, 917586232)$	$(-2, 1)$	22733041315210861248	4
$(-2010243, 1096965250)$	$(11, 1)$	32494186355919275628	15625
$(-3333819, 2450621162)$	$(-7, 3)$	162149690150340216588	3125
$(-4367235, 3512882050)$	$(-1, 1)$	333189188024729467500	1
$(-5840211, 5432389742)$	$(7, 2)$	796793174499269255724	3125
$(-6208059, 5953630358)$	$(-1, 4)$	957034289871878620428	3125
$(-6915540, 6999826250)$	$(8, 3)$	1322934323315597856000	12500
$(8365830, 6918545000)$	$(-14, 1)$	2342001110975069148000	12500
$(-23656314, 44286231688)$	$(2, 1)$	52954298562326815548576	4
$(-149675916, 704409673682)$	$(16, 1)$	13412686238635561555901184	12500
$(18529341, 811299953342)$	$(-13, 2)$	17771605585903747178162028	3125
$(-273426411, 1988757501158)$	$(-11, 4)$	106789222757129734026206028	3125
$(-275757339, 2198498350282)$	$(-3, 1)$	130501664897202240375947148	1
$(-463781604, 3844524236618)$	$(-8, 7)$	399069898360466822606103948	12500
$(-593007330, 5558251655000)$	$(2, 7)$	834142359428376453675000000	12500

Table 5.5.4: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 25-isogeny and $\operatorname{twht} E \leq 10^{27}$

Computing c_{10}^{tw} and c_{25}^{tw}

In this subsection, for $m = 10, 25$, we estimate the constant c_m^{tw} appearing in Theorem 5.4.11 by estimating Q_m and R_m.

We begin with Q_m. Letting $m = 10, 25$, truncating the Euler product (5.3.34) as a product over $p \leq Y$ gives us a lower bound

$$Q_{m,\leq Y} := Q_m(2)Q_m(5) \prod_{\substack{p \neq 5 \text{ prime} \\ p \equiv 1 \pmod 4}} \left(1 + \frac{2p\left(p^{6/d(m)} - 1\right)}{(p+1)\left(p^2 - p^{6/d(m)}\right)}\right) \tag{5.5.5}$$

for Q_m. The values $Q_m(2)$ and $Q_m(5)$ are recorded in (5.3.40). To obtain an upper bound, we observe

$$\begin{aligned} Q_m &< Q_{m,\leq Y} \cdot \exp\left(2 \sum_{\substack{p > Y \\ p \equiv 1 \pmod 4}} \frac{2p\left(p^{6/d(m)} - 1\right)}{(p+1)\left(p^2 - p^{6/d(m)}\right)}\right) \\ &< Q_{m,\leq Y} \cdot \exp\left(2 \sum_{\substack{p > Y \\ p \equiv 1 \pmod 4}} \frac{1}{p^2+1}\right). \end{aligned} \tag{5.5.6}$$

Suppose $Y \geq 8 \cdot 10^9$. Using Abel summation and Bennett–Martin–O'Bryant–Rechnitzer [4, Theorem 1.4], we obtain

$$\begin{aligned} \sum_{\substack{p > Y \\ p \equiv 1 \pmod 4}} \frac{1}{p^2+1} &= -\frac{\pi(Y;4,1)}{Y^2+1} + 2\int_Y^\infty \frac{\pi(u;4,1)u}{(u^2+1)^2}\,\mathrm{d}u \\ &< -\frac{Y}{2\left(Y^2+1\right)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\int_Y^\infty \frac{u^2}{(u^2+1)^2}\,\mathrm{d}u \\ &= \frac{1}{2}\left(\frac{5Y}{2(Y^2+1)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\left(\frac{\pi}{2} - \tan^{-1}(Y)\right)\right) \end{aligned} \tag{5.5.7}$$

so

$$Q_m < Q_{m,\leq Y} \cdot \exp\left(\frac{5Y}{2(Y^2+1)\log Y} + \left(\frac{1}{\log Y} + \frac{5}{2\log^2 Y}\right)\left(\frac{\pi}{2} - \tan^{-1}(Y)\right)\right). \tag{5.5.8}$$

In particular, letting $Y = 10^{11}$, we compute

$$3.636\,493\,079\,001\,437\,6 < Q_{10} < 3.636\,493\,079\,020\,102, \tag{5.5.9}$$

and

$$4.244\,853\,881\,138\,272\,6 < Q_{25} < 4.244\,853\,881\,160\,06; \tag{5.5.10}$$

these estimates require approximately 15 CPU hours apiece.

We now turn our attention to R_m for $m = 10, 25$, given in (3.3.5). We compute R_{10} and R_{25} by performing rejection sampling on the rectangles $[-0.8228, 0.8228] \times [0, 0.6934]$ and $[-0.8781, 0.8781] \times [0, 0.2754]$ respectively.

We find $r_{10} := 58\,560\,198\,103$ of our first $s_{10} := 138\,290\,000\,000$ samples lie in R_{10}, so

$$R_{10} \approx 1.141\,059\,04 \cdot \frac{r_{10}}{s_{10}} = 0.483\,192\,157\,275\,428\,47, \tag{5.5.11}$$

with standard error

$$1.141\,059\,04 \cdot \sqrt{\frac{r_{10}(s_{10} - r_{10})}{s_{10}^3}} < 1.6 \cdot 10^{-8}. \tag{5.5.12}$$

This took 2 CPU weeks to compute.

We find $r_{25} := 245\,430\,977\,211$ of our first $s_{25} := 406\,130\,000\,000$ samples lie in R_{25}, so

$$R_{25} \approx 0.483\,657\,48 \cdot \frac{r_{25}}{s_{25}} = 0.292\,282\,096\,746\,878\,3, \tag{5.5.13}$$

with standard error

$$0.483\,657\,48 \cdot \sqrt{\frac{r_{25}(s_{25} - r_{25})}{s_{25}^3}} < 3.8 \cdot 10^{-7}. \tag{5.5.14}$$

This took 13 CPU weeks to compute.

We therefore have

$$\begin{aligned} c_{10}^{\mathrm{tw}} &= 1.068\,204 \text{ with error bounded by } 3.4 \cdot 10^{-6}, \\ c_{25}^{\mathrm{tw}} &= 0.754\,252\,0 \text{ with error bounded by } 9.6 \cdot 10^{-7}. \end{aligned} \tag{5.5.15}$$

We have computed the constants which appear in Theorem 5.3.46.

Computing c_{10} and c_{25}

In this subsection, we estimate $c_{10} = 2N_{10}^{\mathrm{tw}}(1/6)/\zeta(2)$ and $c_{25} = 2N_{10}^{\mathrm{tw}}(1/6)/\zeta(2)$, the constants which appear in Theorem 5.4.11, by computing the partial sums of $L_{10}^{\mathrm{tw}}(1/6)$ and $L_{25}^{\mathrm{tw}}(1/6)$:

$$\begin{aligned} \sum_{n \le 10^{96}} \frac{\Delta N_{10}^{\mathrm{tw}}(n)}{n^{1/6}} &= 0.869\,838\,621\,652\,207\,3, \text{ and} \\ \sum_{n \le 10^{138}} \frac{\Delta N_{25}^{\mathrm{tw}}(n)}{n^{1/6}} &= 0.206\,338\,924\,690\,954\,36. \end{aligned} \tag{5.5.16}$$

We empirically confirm that

$$N_{10}^{\mathrm{tw}}(X) < 1.095\,26 X^{1/12} \text{ for } X \le 10^{96}, \text{ and} \tag{5.5.17}$$

$$N_{25}^{\mathrm{tw}}(X) < 0.909\,77 X^{1/18} \text{ for } X \le 10^{138}. \tag{5.5.18}$$

If these bounds continue to hold for larger X, then

$$\begin{aligned} \sum_{n > 10^{96}} \frac{\Delta \widetilde{N}_{10}^{\mathrm{tw}}(n)}{n^{1/6}} &= \int_{10^{96}}^{\infty} x^{-1/6} dN_{10}^{\mathrm{tw}}(x) < 1.09526 \cdot 10^{-8} \text{ and} \\ \sum_{n > 10^{144}} \frac{\Delta \widetilde{N}_{25}^{\mathrm{tw}}(n)}{n^{1/6}} &= \int_{10^{126}}^{\infty} x^{-1/6} dN_{25}^{\mathrm{tw}}(x) < 2 \cdot 0.90977 \cdot 10^{-7}. \end{aligned} \tag{5.5.19}$$

Assuming (5.5.17), $L_{10}^{\mathrm{tw}}(1/6) \approx 0.869838622$ with an error bounded by $5.5 \cdot 10^{-9}$; assuming (5.5.18), $L_{25}^{\mathrm{tw}}(1/6) \approx 0.206339016$ with an error bounded by $9.1 \cdot 10^{-8}$.

We therefore have

$$\begin{aligned} c_{10} &\approx 1.0575969453 \text{ with error bounded by } 6.7 \cdot 10^{-9}, \\ c_{25} &\approx 0.25087816 \text{ with error bounded by } 1.2 \cdot 10^{-7}. \end{aligned} \tag{5.5.20}$$

We emphasize that our estimates for c_{10} and c_{25} depend on empirical rather than theoretical estimates for the implicit constant in the error term in the asymptotics of $N_{10}^{\mathrm{tw}}(X)$ and $N_{25}^{\mathrm{tw}}(X)$.

Chapter 6

Counting elliptic curves with a cyclic m-isogeny for $m = 13$

In this chapter, we prove Theorem 1.2.6 (Theorem 6.4.5) and Theorem 1.2.13 (Theorem 6.3.34) when $m = 13$. These results are new, but our arguments mirror those in chapter 4 and chapter 5, and we encourage anyone reading to skim them on a first perusal of this thesis. However, handling $m = 13$ is subtler than handling $m \in \{7, 10, 25\}$ because $X_0(13)$ has elliptic points of both orders 2 and 3, and the elliptic surfaces describing elliptic curves with a cyclic 13-isogeny thus exhibit *both* potential type II additive reduction and potential type III additive reduction.

The organization of this chapter mirrors that of chapter 4 and chapter 5. In section 6.1, we establish notations pertaining to $f_{13}(t)$ and $g_{13}(t)$ which will be used throughout the remainder of the chapter. In section 6.2, we develop bounds relating the twist minimality defect to the two factors of the greatest common divisor of $f_{13}(t)$ and $g_{13}(t)$. In section 6.3, we apply the framework developed in section 3.5 to prove Theorem 1.2.13 for $m = 13$, with an improved error term. In section 6.4, we prove Theorem 1.2.6 for $m = 13$. In section 6.5, we produce supplementary computations to estimate the constants appearing in Theorem 6.3.34

and Theorem 6.4.5 and empirically confirm that the count of elliptic curves with a cyclic 13-isogeny aligns with our theoretical estimate

Section 6.1

Establishing notation for $m = 13$

By Corollary 2.1.50,

$$\widetilde{N}_{13}^{\mathrm{tw}}(X) = N_{13}^{\mathrm{tw}}(X) \text{ and } \widetilde{N}_{13}(X) = N_{13}(X) \tag{6.1.1}$$

for all $X > 0$, so we may use either notation interchangeably. We opt to work with $N_{13}^{\mathrm{tw}}(X)$ and related functions.

Note that

$$\gcd(f_{13}(t), g_{13}(t)) = (t^2 + t + 7)(t^2 + 4) \tag{6.1.2}$$

factors over $\mathbb{Q}$. We define

$$\begin{aligned} h_{13,\mathrm{II}}(t) &:= t^2 + t + 7, \text{ and} \\ h_{13,\mathrm{III}}(t) &:= t^2 + 4, \end{aligned} \tag{6.1.3}$$

so $\gcd(f_{13}(t), g_{13}(t)) = h_{13,\mathrm{II}}(t)h_{13,\mathrm{III}}(t)$. We define $f_{13}'(t)$ and $g_{13}'(t)$ so that

$$f_{13}(t) = f_{13}'(t)h_{13,\mathrm{II}}(t)h_{13,\mathrm{III}}(t) \text{ and } g_{13}(t) = g_{13}'(t)h_{13,\mathrm{II}}(t)h_{13,\mathrm{III}}(t)^2. \tag{6.1.4}$$

Thus

$$\begin{aligned} f_{13}'(t) &= -3\left(t^4 - 235t^3 + 1211t^2 - 1660t + 6256\right), \text{ and} \\ g_{13}'(t) &= 2(t^6 + 512t^5 - 13073t^4 + 34860t^3 - 157099t^2 + 211330t - 655108). \end{aligned} \tag{6.1.5}$$

As in the previous chapters, to work with integral models, we take $t = a/b$ (in lowest terms) and homogenize, obtaining

$$\begin{aligned} C_{13,\mathrm{II}}(a,b) &:= b^2 h_{13,\mathrm{II}}(a/b) = a^2 + ab + 7b^2, \\ C_{13,\mathrm{III}}(a,b) &:= b^2 h_{13,\mathrm{III}}(a/b) = a^2 + 4b^2, \\ A'_{13}(a,b) &:= b^4 f'_{13}(a/b) \\ &= -3\left(a^4 - 235a^3b + 1211a^2b^2 - 1660ab^3 + 6256b^4\right), \text{ and} \\ B'_{13}(a,b) &:= b^6 g'_{13}(a/b) \\ &= 2(a^6 + 512a^5b - 13073a^4 + 34860a^3 - 157099a^2 + 211330a - 655108). \end{aligned} \tag{6.1.6}$$

Of course, we have

$$\begin{aligned} A_{13}(a,b) =& A'_{13}(a,b)C_{13,\mathrm{II}}(a,b)C_{13,\mathrm{III}}(a,b), \text{ and} \\ B_{13}(a,b) =& B'_{13}(a,b)C_{13}(a,b)C_{13,\mathrm{III}}(a,b)^2. \end{aligned} \tag{6.1.7}$$

Section 6.2

The twist minimality defect for $m = 13$

As with the previous chapters, we begin by studying the twist minimality defect. The situation here is complicated somewhat, however, because the twist minimality defect may receive contributions from both $C_{13,\mathrm{II}}(a,b)$ and $C_{13,\mathrm{III}}(a,b)$.

Lemma 6.2.1. *Let $(a,b) \in \mathbb{Z}^2$ be 13-groomed, let ℓ be prime, and let $v \in \mathbb{Z}_{\geq 0}$. Then the following statements hold.*

(a) *If $\ell \neq 2, 3, 13$, then $\ell^v \mid \operatorname{tmd}(A_{13}(a,b), B_{13}(a,b))$ if and only if*

$$\ell^{3v} \mid C_{13,\mathrm{II}}(a,b) \text{ or } \ell^{2v} \mid C_{13,\mathrm{III}}(a,b). \tag{6.2.2}$$

Moreover, for $\ell \neq 13$, we cannot have both $\ell \mid C_{13,\mathrm{II}}(a,b)$ and $\ell \mid C_{13,\mathrm{III}}(a,b)$.

(b) $\ell^{3v} \mid C_{13,\mathrm{II}}(a,b)$ *if and only if* $\ell \nmid b$ *and* $h_{13,\mathrm{II}}(a/b) \equiv 0 \pmod{\ell^{3v}}$. *Likewise,* $\ell^{2v} \mid C_{13,\mathrm{III}}(a,b)$ *if and only if* $\ell \nmid b$ *and* $h_{13,\mathrm{III}}(a/b) \equiv 0 \pmod{\ell^{2v}}$.

(c) *If* $\ell \neq 3$, *then* $\ell \mid C_{13,\mathrm{II}}(a,b)$ *implies* $\ell \nmid (\partial C_{13,\mathrm{II}}/\partial a)(a,b) = 2a+b$. *Likewise, if* $\ell \neq 2$, *then* $\ell \mid C_{13,\mathrm{III}}(a,b)$ *implies* $\ell \nmid (\partial C_{13,\mathrm{III}}/\partial a)(a,b) = 2a$.

Proof. We argue as in Cullinan–Kenney–Voight [16, Proof of Theorem 3.3.1, Step 3]. Our argument is more involved than the proofs of Lemma 4.2.2 or Lemma 5.2.2 however. For part (a), we first compute the resultants

$$\operatorname{Res}(C_{13,\mathrm{II}}(t,1), C_{13,\mathrm{III}}(t,1)) = \operatorname{Res}(h_{13,\mathrm{II}}(t), h_{13,\mathrm{III}}(t)) = 13 = \operatorname{Res}(C_{13,\mathrm{II}}(1,u), C_{13,\mathrm{III}}(1,u)). \tag{6.2.3}$$

Thus if $\ell \neq 13$ is prime, then ℓ can divide at most one of $C_{13,\mathrm{II}}(a,b)$ and $C_{13,\mathrm{III}}(a,b)$. We now compute the resultant

$$\operatorname{Res}(A'_{13}(t,1), B'_{13}(t,1)) = \operatorname{Res}(f'_{13}(t), g'_{13}(t)) = -2^{14} \cdot 3^{11} \cdot 13^{24} = \operatorname{Res}(A'_{13}(1,u), B'_{13}(1,u)). \tag{6.2.4}$$

If $\ell \neq 2,3,13$, then $\ell \nmid \gcd(A'_{13}(a,b), B'_{13}(a,b))$; so by (3.1.6), if $\ell^v \mid \operatorname{tmd}(A_{13}(a,b), B_{13}(a,b))$ then $\ell \mid C_{13,\mathrm{II}}(a,b)C_{13,\mathrm{III}}(a,b)$. By (6.2.3), we now have two cases: $\ell \mid C_{13,\mathrm{II}}(a,b)$ or $\ell \mid C_{13,\mathrm{III}}(a,b)$.

Suppose first that $\ell \mid C_{13,\mathrm{II}}(a,b)$. We compute

$$\begin{aligned}\operatorname{Res}(B'_{13}(t,1), C_{13,\mathrm{II}}(t,1)) = \operatorname{Res}(g'_{13}(t), h_{13,\mathrm{II}}(t)) &= 2^8 \cdot 3^3 \cdot 13^6 \\ &= \operatorname{Res}(B'_{13}(1,u), C_{13,\mathrm{II}}(1,u)),\end{aligned} \tag{6.2.5}$$

so $\ell \nmid \gcd(B'_{13}(a,b), C_{13,\mathrm{II}}(a,b))$, and thus (under our hypotheses)

$$\ell^v \mid \operatorname{tmd}(A_{13}(a,b), B_{13}(a,b)) \text{ if and only if } \ell^{3v} \mid C_{13,\mathrm{II}}(a,b). \tag{6.2.6}$$

Suppose instead that $\ell \mid C_{13,\mathrm{III}}(a,b)$. We compute

$$\begin{aligned}\operatorname{Res}(A'_{13}(t,1), C_{13,\mathrm{III}}(t,1)) = \operatorname{Res}(A'_{13}(t), h_{13,\mathrm{III}}(t)) =& 2^4 \cdot 3^4 \cdot 13^4 \\ =& \operatorname{Res}(A'_{13}(1,u), C_{13,\mathrm{III}}(1,u)),\end{aligned} \tag{6.2.7}$$

so $\ell \nmid \gcd(A'_{13}(a,b), C_{13,\mathrm{III}}(a,b))$, and thus (under our hypotheses)

$$\ell^v \mid \operatorname{tmd}(A_{13}(a,b), B_{13}(a,b)) \text{ if and only if } \ell^{2v} \mid C_{13,\mathrm{III}}(a,b). \tag{6.2.8}$$

This proves (a)

For (b), by homogeneity it suffices to show that $\ell \nmid b$, and indeed this holds since if $\ell \mid b$ then $A_{13}(a,0) \equiv -3a^8 \equiv 0 \pmod{\ell}$ and $B_{13}(b,0) \equiv 2a^{12} \equiv 0 \pmod{\ell}$ so $\ell \mid a$, a contradiction.

Part (c) follows from (b) and the fact that $h_{13,\mathrm{II}}(t)$ has discriminant -3^3 and $h_{13,\mathrm{III}}(t)$ has discriminant -2^4. □

We now make our main departure from chapter 4 and chapter 5: in contrast with Definition 4.2.12 and Definition 5.2.5, we define $\widetilde{\mathcal{T}}_{13}$ to be a function with two arguments.

Definition 6.2.9. For $e_1, e_2 \geq 1$, let $\widetilde{\mathcal{T}}_{13}(e_1,e_2)$ denote the image of

$$\left\{ (a,b) \in \mathbb{Z}^2 : \begin{array}{l} (a,b) \text{ 13-groomed, } e_1e_2 \mid \operatorname{tmd}(A_{13}(a,b),\ B_{13}(a,b)), \\ \gcd(e_1^3, C_{13,\mathrm{III}}(a,b)) \mid 13,\ \gcd(e_2^2, C_{13,\mathrm{II}}(a,b)) \mid 13, \\ 3 \mid e_2 \implies 3 \mid h_{13,\mathrm{III}}(a,b), \\ 13 \mid e_2 \implies 13 \nmid C_{13,\mathrm{II}}(a,b) \text{ or } 13^2 \mid C_{13,\mathrm{III}}(a,b) \end{array} \right\} \tag{6.2.10}$$

under the projection

$$\mathbb{Z}^2 \to (\mathbb{Z}/e_1^3e_2^2\mathbb{Z})^2, \tag{6.2.11}$$

and let $\widetilde{T}_{13}(e_1,e_2) := \#\widetilde{\mathcal{T}}_{13}(e_1,e_2)$.

Similarly, we let $\mathcal{T}_{13}(e_1, e_2)$ denote the image of

$$\left\{ t \in \mathbb{Z} : \begin{array}{l} (e_1e_2)^2 \mid f_{13}(t),\ (e_1e_2)^3 \mid g_{13}(t), \\ \gcd(e_1^3, h_{13,\mathrm{III}}(t)) \mid 13,\ \gcd(e_2^2, h_{13,\mathrm{II}}(t)) \mid 13, \\ 3 \mid e_2 \implies 3 \mid h_{13,\mathrm{III}}(t), \\ 13 \mid e_2 \implies 13 \nmid h_{13,\mathrm{II}}(t) \text{ or } 13^2 \mid h_{13,\mathrm{III}}(t) \end{array} \right\} \tag{6.2.12}$$

under the projection

$$\mathbb{Z} \to \mathbb{Z}/e_1^3e_2^2\mathbb{Z}, \tag{6.2.13}$$

and let $T_{13}(e_1, e_2) := \#\mathcal{T}_{13}(e_1, e_2)$.

By Lemma 6.2.1, for $\ell \neq 2, 3, 13$, e_1 is the part of the twist minimality defect arising from $C_{13,\mathrm{II}}(a, b)$ and e_2 is the part of the twist minimality defect arising from $C_{13,\mathrm{III}}(a, b)$. The final two conditions of (6.2.10) and (6.2.13) is necessary to avoid double-counting certain pairs (a, b) for which $3 \mid \operatorname{tmd}(A_{13}(a, b), B_{13}(a, b))$ or $13 \mid \operatorname{tmd}(A_{13}(a, b), B_{13}(a, b))$.

Lemma 6.2.14. *The following statements hold.*

(a) *Suppose* $\gcd(e_1, e_2) = 1$*, and write* $e_1 = 3^{v_1}13^{w_1}e_1'$ *and* $e_2 = 2^{u_2}13^{w_2}e_2'$*, where* $\gcd(e_1', 3 \cdot 13) = \gcd(e_2', 2 \cdot 13) = 1$*. The set* $\widetilde{\mathcal{T}}_{13}(e_1, e_2)$ *consists of those pairs* $(a, b) \in (\mathbb{Z}/e_1^3e_2^2\mathbb{Z})^2$ *which satisfy the following conditions:*

- $C_{13,\mathrm{II}}(a, b) \equiv 0 \pmod{(e_1')^3}$*,*
- $C_{13,\mathrm{III}}(a, b) \pmod{(e_2')^2}$*,*
- $\ell \nmid \gcd(a, b)$ *for all primes* $\ell \mid e_1e_2$*,*
- *if* $u_2 > 0$ *then* $A_{13}(a, b) \equiv 0 \pmod{2^{2u_2}}$ *and* $B_{13}(a, b) \equiv 0 \pmod{2^{3u_2}}$*, and if* $u_1 > 0$ *then no pairs are permitted;*
- *if* $v_1 > 0$ *then* $A_{13}(a, b) \equiv 0 \pmod{3^{2v_1}}$ *and* $B_{13}(a, b) \equiv 0 \pmod{3^{3v_1}}$*, and if* $v_2 > 0$ *then no pairs are permitted;*

- *If* $w_1 > 0$ *then* $A_{13}(a,b) \equiv 0 \pmod{13^{2w_1}}$ *and* $B_{13}(a,b) \equiv 0 \pmod{13^{3w_1}}$*, but* $C_{13,\mathrm{III}}(a,b) \not\equiv 0 \pmod{13^2}$*;*
- *If* $w_2 > 0$ *then* $A_{13}(a,b) \equiv 0 \pmod{13^{2w_1}}$ *and* $B_{13}(a,b) \equiv 0 \pmod{13^{3w_1}}$*, but* $C_{13,\mathrm{II}}(a,b) \not\equiv 0 \pmod{13}$ *or* $C_{13,\mathrm{III}}(a,b) \not\equiv 0 \pmod{13}$*.*

(b) *Let* $(a,b) \in \mathbb{Z}^2$*. If* $(a,b) \pmod{e_1^3e_2^2} \in \widetilde{\mathcal{T}}_{13}(e_1,e_2)$ *then* $e_1e_2 \mid \operatorname{tmd}(A_{13}(a,b), B_{13}(a,b))$*.*

(c) *For all* $e_1, e_2, e_1', e_2' \in \mathbb{Z}_{>0}$ *with*

$$\gcd(e_1,e_2) = \gcd(e_1',e_2') = \gcd(e_1,e_1') = \gcd(e_2,e_2') = 1, \tag{6.2.15}$$

we have

$$\begin{aligned} \widetilde{T}_{13}(e_1e_1', e_2e_2') &= \widetilde{T}_{13}(e_1,e_2)\widetilde{T}_{13}(e_1',e_2') \text{ and} \\ T_{13}(e_1e_1', e_2e_2') &= T_{13}(e_1,e_2)T_{13}(e_1',e_2'), \end{aligned} \tag{6.2.16}$$

and

$$\widetilde{T}_{13}(e_1,e_2) = \varphi(e_1^3)\varphi(e_2^2)T_{13}(e_1,e_2). \tag{6.2.17}$$

If $\gcd(e_1,e_2) > 1$*, then*

$$\widetilde{T}_{13}(e_1,e_2) = T_{13}(e_1,e_2) = 0. \tag{6.2.18}$$

(d) *For all prime* $\ell \neq 2, 3, 13$ *and all* $v \geq 1$*, we have*

$$\begin{aligned} T_{13}(\ell^v,1) =& T_{13}(\ell,1) = 1 + \left(\frac{\ell}{3}\right), \\ T_{13}(1,\ell^v) =& T_{13}(1,\ell) = 1 + \left(\frac{-1}{\ell}\right). \end{aligned} \tag{6.2.19}$$

(e) *For* $e \in \{2, 2^2, 3, 3^2\}$*, the nonzero values of* $T_{13}(e,1)$ *and* $T_{13}(1,e)$ *are given in Table 6.2.25 and Table 6.2.26. We have*

$$T_{13}(2^v,1) = 0 \textit{ for } v \geq 1,\ T_{13}(3^v,1) = 0 \textit{ for } v \geq 3, \tag{6.2.20}$$

and

$$T_{13}(1,2^v)=0 \text{ for } v\geq 3,\ T_{13}(1,3^v)=0 \text{ for } v\geq 1. \tag{6.2.21}$$

(f) *We have* $T_{13}(e_1,e_2)=O(2^{\omega(e_1e_2)})$*, where* $\omega(e)$ *is the number of distinct prime divisors of* e*.*

(g) *If* (a,b) *is a* 13*-groomed pair and* $e \mid \operatorname{tmd}(A_{13}(a,b),B_{13}(a,b))$*, then there is a unique factorization* $e=e_1e_2$ *with* $\gcd(e_1,e_2)=1$ *and* $(a,b)\in\widetilde{\mathcal{T}}_{13}(e_1,e_2)$*.*

Proof. For parts (a) and (b), by the CRT (Sun Zi theorem), it suffices to consider $e=\ell^v$ a power of a prime. For $\ell\neq 2,3,13$, both claims follow from Lemma 6.2.1(a)–(b). But a finite computation verifies our claim in these cases as well (see the proof of (e) below).

We now consider part (c). The assertion (6.2.15) implies (6.2.16) is simply multiplicativity in each argument away from the primes dividing the other argument. This follows from the CRT (Sun Zi theorem). For (6.2.17), let ℓ be a prime, and let $e=\ell^v$ for some $v\geq 1$. Consider the injective map

$$\begin{aligned}\mathcal{T}_{13}(\ell^v,1)\times(\mathbb{Z}/\ell^{3v})^\times &\to \widetilde{\mathcal{T}}_{13}(\ell^v,1)\\ (t,u)&\mapsto(tu,u)\end{aligned}\tag{6.2.22}$$

We observe $A(1,0)=-3$ and $B(1,0)=2$ are coprime, so no pair (a,b) with $b\equiv 0 \pmod{\ell}$ can be a member of $\widetilde{\mathcal{T}}_{13}(\ell^v,1)$. Surjectivity of the given map follows, and counting both sides gives the result in this component. On the other hand, we can consider the injective map

$$\begin{aligned}\mathcal{T}_{13}(1,\ell^v)\times(\mathbb{Z}/\ell^{2v})^\times &\to \widetilde{\mathcal{T}}_{13}(1,\ell^v)\\ (t,u)&\mapsto(tu,u)\end{aligned}\tag{6.2.23}$$

Again, as $A(1,0)=-3$ and $B(1,0)=2$ are coprime, no pair (a,b) with $b\equiv 0 \pmod{\ell}$ can be a member of $\widetilde{\mathcal{T}}_{13}(1,\ell^v)$, and the desired implication follows. Finally, (6.2.18) whenever

$\gcd(e_1, e_2) > 1$ holds by Lemma 6.2.1 when $\gcd(e_1, e_2)$ is not a power of 13. The case $\ell = 13$ follows from the last condition of (6.2.10) together with the observation that for coprime (a, b) we have $\gcd(C_{13,\mathrm{II}}(a, b), C_{13,\mathrm{III}}(a, b)) \mid 13$.

Now part (d). For $\ell \neq 2, 3, 13$, Lemma 6.2.1(a)–(b) yield

$$\begin{aligned} \mathcal{T}_{13}(\ell^v, 1) &= \left\{t \in \mathbb{Z}/\ell^{3v}\mathbb{Z} : h_{13,\mathrm{II}}(t) \equiv 0 \pmod{\ell^{3v}}\right\}, \text{ and} \\ \mathcal{T}_{13}(1, \ell^v) &= \left\{t \in \mathbb{Z}/\ell^{2v}\mathbb{Z} : h_{13,\mathrm{III}}(t) \equiv 0 \pmod{\ell^{2v}}\right\}. \end{aligned} \tag{6.2.24}$$

By Lemma 6.2.1(c), $h_{13,\mathrm{II}}(t) \equiv 0 \pmod{\ell}$ implies $\frac{\mathrm{d}}{\mathrm{d}t} h_{13,\mathrm{II}}(t) \not\equiv 0 \pmod{\ell}$, and likewise for $h_{13,\mathrm{III}}(t)$ so Hensel's lemma applies and we need only count roots of $h_{13}(t)$ modulo ℓ, and our result follows by quadratic reciprocity.

Next, part (e). For $\ell = 2$, we readily verify $T_{13}(2, 1) = 0$, and hence $T_{13}(2^\ell, 1) = 0$ for $\ell \geq 1$. On the other hand, $T_{13}(1, 2) = 2$, $T_{13}(1, 2^2) = 2^3$, and $T_{13}(1, 2^3) = 0$, so $T_{13}(1, 2^v) = 0$ for $v \geq 3$.

For $\ell = 3$, we just compute $T_{13}(3, 1) = 18$, $T_{13}(3^2, 1) = 27$, and $T_{13}(3^3, 1) = 0$; the observation $T_{13}(3^3, 1) = 0$ implies $T_{13}(3^v, 1) = 0$ for all $v \geq 3$. Similarly, $T_{13}(1, 3) = 0$ implies $T_{13}(1, 3^v) = 0$ for all $v \geq 1$.

Part (f) follows from parts (d) and (e).

Finally, for part (g), part (c) assures us that we can take $(e_1, e_2) = (\ell^v, 1)$ or $(e_1, e_2) = (1, \ell^v)$ without loss of generality. If $\ell \neq 2, 3, 13$, the claim now follows from part (d), and if $\ell = 2, 3, 13$, the claim follows from part (e) and by construction. □

Notably, Lemma 6.2.14 does not furnish the values of $T_{13}(13^v, 1)$ and $T_{13}(1, 13^v)$ for $v \geq 1$. By Hensel's Lemma, these functions are constant for sufficiently large v, but our somewhat naïve code runs into memory issues before verifying these plateaued values. Unfortunately, this obstructs the computation of Q_{13} below; however, it poses no issue for our theoretical results.

m	$T_{13}(1,2^1)$	$T_{13}(1,2^2)$
13	2	2^3

Table 6.2.25: All nonzero $T_{13}(3^v,1)$

m	$T_{13}(3^1,1)$	$T_{13}(3^2,1)$
13	$2\cdot 3^2$	3^3

Table 6.2.26: All nonzero $T_{13}(3^v,1)$

The following theorem gives us the tools to relate the twist height to the twist minimality defect for $m = 13$, in imperfect analogy with Theorem 4.2.35 and Theorem 5.4.11.

Theorem 6.2.27. *The following statements hold.*

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

$$\begin{aligned} 108C_{13,\mathrm{II}}(a,b)^{12} &\leq H(A_{13}(a,b),B_{13}(a,b)) \leq \kappa_{II,13}C_m(a,b)^{12},\\ 108C_{13,\mathrm{III}}(a,b)^{12} &\leq H(A_{13}(a,b),B_{13}(a,b)) \leq \kappa_{III,13}C_m(a,b)^{12}, \end{aligned} \tag{6.2.28}$$

where the constants

$$\begin{aligned} \kappa_{II,13} =& 635\,811\,018.28475061\ldots \quad \textit{and} \\ \kappa_{III,13} =& 35\,492\,073\,075.17456568\ldots \end{aligned} \tag{6.2.29}$$

are algebraic numbers given by evaluating $H(A_{13}(a,b),B_{13}(a,b))$ at appropriate roots of (6.2.33) *and* (6.2.34) *respectively.*

(b) *If $C_{13,\mathrm{II}}(a,b) = e_{\mathrm{II}}^3 n_{\mathrm{II}}$, with n_0 cube-free, and $C_{13,\mathrm{III}}(a,b) = e_{\mathrm{III}}^2 n_{\mathrm{III}}$ with n_{III} squarefree, then $\operatorname{tmd}(A_{13}(a,b),B_{13}(a,b)) = e_{\mathrm{II}}e_{\mathrm{III}}e'$, where $e' \mid 2\cdot 3\cdot 13$. In addition, for all $(a,b)\in\mathbb{R}^2$, we have*

$$\lambda_{13}C_{13,\mathrm{III}}(a,b) \leq C_{13,\mathrm{II}}(a,b) \leq \mu_{13}C_{13,\mathrm{III}}(a,b), \tag{6.2.30}$$

where the constants

$$\begin{aligned} \lambda_{13} &= 0.92430609\ldots \ \textit{and} \\ \mu_{13} &= 1.82569390\ldots \end{aligned} \tag{6.2.31}$$

are algebraic numbers given by evaluating $C_{13,\mathrm{III}}(a,b)$ *at appropriate roots of* (6.2.37).

Proof. The proof of this theorem is similar to those of Theorem 4.2.35 and Theorem 5.2.32; however, to aid our reader in parsing the contributions of both factors, especially in part (b), we prove it in its entirety.

We first prove (a). Let $m = 13$. We wish to find the extrema of

$$H(A_{13}(a,b), B_{13}(a,b))/C_{13,\mathrm{II}}(a,b)^{12} \text{ and } H(A_{13}(a,b), B_{13}(a,b))/C_{13,\mathrm{III}}(a,b)^{12}. \tag{6.2.32}$$

As these expressions are homogeneous of degree 0, and $C_{13,\mathrm{II}}(a,b)$ and $C_{13,\mathrm{III}}(a,b)$ are positive definite, we may assume without loss of generality that $C_{13,\mathrm{II}}(a,b) = 1$ or $C_{13,\mathrm{III}}(a,b) = 1$ respectively. Using the theory of Lagrange multipliers, and examining the critical points of $H(A_{13}(a,b), B_{13}(a,b))$ subject to these respective constraints, we verify that (6.2.28) holds. Moreover, the lower bound is attained in both cases at $(1,0)$, and the upper bound is attained when a and b are appropriately chosen roots of

$$\begin{aligned}
&105718701441600a^{20} + 628890736780800a^{18} + 6862077189805968a^{16} \\
&- 3737927951730336a^{14} - 7359872595882599a^{12} - 1358785779700076a^{10} \\
&+ 7533990802873860a^{8} - 2897948832460864a^{6} + 1787484431772288a^{4} \\
&- 2069428838131712a^{2} + 643089024640000 \\
=&2^6 \cdot 3^4 \cdot 5^2 \cdot 13^8 \cdot a^{20} + 2^9 \cdot 3^3 \cdot 5^2 \cdot 13^7 \cdot 29 \cdot a^{18} \\
&+ 2^4 \cdot 3^2 \cdot 13^6 \cdot 2971 \cdot 3323 \cdot a^{16} - 2^5 \cdot 3 \cdot 7^2 \cdot 13^5 \cdot 2140163 \cdot a^{14} \\
&- 13^4 \cdot 103 \cdot 2309 \cdot 1083517 \cdot a^{12} - 2^2 \cdot 7 \cdot 13^4 \cdot 199 \cdot 757 \cdot 11279 \cdot a^{10} \\
&+ 2^2 \cdot 3 \cdot 5 \cdot 13^2 \cdot 742997120599 \cdot a^{8} - 2^6 \cdot 7 \cdot 13 \cdot 6991 \cdot 71175421 \cdot a^{6} \\
&+ 2^7 \cdot 3^2 \cdot 29311 \cdot 52936979 \cdot a^{4} - 2^{11} \cdot 61 \cdot 16564972129 \cdot a^{2} + 2^{10} \cdot 5^4 \cdot 31699^2, \text{ and} \\
&105718701441600b^{20} - 129031030477440b^{18} + 226457312671512b^{16} \\
&- 162954491664432b^{14} + 61397224373329b^{12} - 13194397029476b^{10} \\
&+ 1681210465311b^{8} - 121030573768b^{6} + 4530949623b^{4} \\
&- 78302708b^{2} + 28561 \\
=&2^6 \cdot 3^4 \cdot 5^2 \cdot 13^8 \cdot b^{20} - 2^7 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13^7 \cdot 17 \cdot b^{18} + 2^3 \cdot 3^2 \cdot 13^6 \cdot 613 \cdot 1063 \cdot b^{16} \\
&- 2^4 \cdot 3 \cdot 13^5 \cdot 103 \cdot 88771 \cdot b^{14} + 13^4 \cdot 157 \cdot 13692277 \cdot b^{12} - 2^2 \cdot 13^4 \cdot 115493129 \cdot b^{10} \\
&+ 3 \cdot 13^2 \cdot 3315996973 \cdot b^{8} - 2^3 \cdot 13 \cdot 1091 \cdot 1066687 \cdot b^{6} + 3^3 \cdot 577 \cdot 290837 \cdot b^{4} \\
&- 2^2 \cdot 11 \cdot 1779607 \cdot b^{2} + 13^4,
\end{aligned} \tag{6.2.33}$$

if $C_{13,\mathrm{II}}(a,b) = 1$, and of

$$\begin{aligned}
&469860895296a^{16} - 4490785864656a^{14} + 18528290390389a^{12}\\
&\quad - 42537089721750a^{10} + 58527314729975a^{8} - 48232472033876a^{6}\\
&\quad + 22080850389507a^{4} - 4364808534790a^{2} + 18869692689\\
=&2^6 \cdot 3^2 \cdot 13^8 \cdot a^{16} - 2^4 \cdot 3^2 \cdot 7 \cdot 13^7 \cdot 71 \cdot a^{14} + 13^6 \cdot 3838621 \cdot a^{12}\\
&\quad - 2 \cdot 3 \cdot 5^3 \cdot 13^5 \cdot 152753 \cdot a^{10} + 5^2 \cdot 7 \cdot 13^5 \cdot 23 \cdot 39163 \cdot a^8 - 2^2 \cdot 13^4 \cdot 157 \cdot 1249 \cdot 2153 \cdot a^6\\
&\quad + 3 \cdot 7 \cdot 13 \cdot 13907 \cdot 5815937 \cdot a^4 - 2 \cdot 5 \cdot 11 \cdot 39680077589 \cdot a^2 + 3^4 \cdot 15263^2, \text{ and}\\
&300710972989 44b^{16} + 117103792366608b^{14} + 9955776243 40b^{12}\\
&\quad - 638359599384b^{10} - 130255153795b^{8} - 12900146870b^{6}\\
&\quad - 775262241b^{4} - 64120726b^{2} + 29241\\
=&2^{12} \cdot 3^2 \cdot 13^8 \cdot b^{16} + 2^8 \cdot 3^6 \cdot 13^7 \cdot b^{14} + 2^2 \cdot 5 \cdot 13^6 \cdot 10313 \cdot b^{12}\\
&\quad - 2^3 \cdot 3^2 \cdot 13^5 \cdot 23879 \cdot b^{10} - 5 \cdot 13^5 \cdot 70163 \cdot b^8 - 2 \cdot 5 \cdot 13^4 \cdot 31^2 \cdot 47 \cdot b^6\\
&\quad - 3^2 \cdot 13 \cdot 6626173 \cdot b^4 - 2 \cdot 557 \cdot 57559 \cdot b^2 + 3^4 \cdot 19^2,
\end{aligned} \tag{6.2.34}$$

if $C_{13,\mathrm{III}}(a,b) = 1$. In both cases, $27\,|B_m(a,b)|^2 > 4\,|A_m(a,b)|^3$. For the reader's information,

$$(a,b) = (-0.715678818\ldots, 0.320005592\ldots) \tag{6.2.35}$$

maximizes H subject to $C_{13,\mathrm{II}}(a,b) = 1$, and

$$(a,b) = (-0.066491149\ldots, 0.498893507\ldots) \tag{6.2.36}$$

maximizes H subject to $C_{13,\mathrm{III}}(a,b) = 1$.

We now prove (b). Write $C_{13,\mathrm{II}}(a,b) = e_{\mathrm{II}}^3 n_{\mathrm{II}}$, with n_0 cube-free, and $C_{13,\mathrm{III}}(a,b) = e_{\mathrm{III}}^2 n_{\mathrm{III}}$ with n_{III} square-free. By Lemma 6.2.1(a) and , $e' = 2^u \cdot 3^v \cdot 13^w$ for some $u, v, w \geq 0$. A short computation shows $u = v = w = 1$.

The remainder of the proof of (b) is similar to the proof of (a), but even easier: we wish to find the extrema of $C_{13,\mathrm{II}}(a,b)$ subject to the constraint $C_{13,\mathrm{III}}(a,b) = 1$. We find that these extrema are attained when a and b are appropriately chosen roots of

$$\begin{aligned} &13a^4 - 13a^2 + 1 \text{ and} \\ &208b^4 - 52b^2 + 1 = 2^4 \cdot 13 \cdot b^4 - 2^2 \cdot 13 \cdot b + 1 : \end{aligned} \tag{6.2.37}$$

we maximize the ratio when $(a,b) = (0.289784148\ldots, 0.478546013\ldots)$, and minimze the ratio when $(a,b) = (0.957092026\ldots, -0.144892074\ldots)$. □

Remark 6.2.38. Because $A_{13}(a,b)$ and $B_{13}(a,b)$ have both $C_{13,\mathrm{II}}(a,b)$ and $C_{13,\mathrm{III}}(a,b)$ as common factors, Theorem 4.2.35(b) and Theorem 5.2.32(b) have no perfect analogues. However, Theorem 6.2.27 enables us to bound $H(A_{13}(a,b), B_{13}(a,b))$ with respect to $C_{13,\mathrm{II}}(a,b)^k \cdot C_{13,\mathrm{III}}(a,b)^{12-k}$ for any $k \in \mathbb{R}$, and therefore enables us to derive a whole family of analogues to Theorem 6.2.27(b).

For example, if $C_{13,\mathrm{II}}(a,b) = e_{\mathrm{II}}^3 n_{\mathrm{II}}$, with n_0 cube-free, and $C_{13,\mathrm{III}}(a,b) = e_{\mathrm{III}}^2 n_{\mathrm{III}}$ with n_{III} square-free, then

$$\frac{\lambda_{13}^3}{2^4 \cdot 3^3 \cdot 7^6} e_{II}^{21} n_{II}^9 n_{III}^3 \leq \operatorname{twht}(A_{13}(a,b), B_{13}(a,b)) \leq \mu_{13}^3 \kappa_{13} e_{II}^{21} n_{II}^9 n_{III}^3. \tag{6.2.39}$$

The constants λ_{13} and μ_{13} are given in (6.2.31).

Section 6.3

Estimates for twist classes for $m = 13$

In this section, we use section 3.5 to estimate $N_{13}^{\mathrm{tw}}(X)$, counting the number of twist minimal elliptic curves over $\mathbb{Q}$ admitting a cyclic 13-isogeny.

Recall (3.5.6), (3.5.33), and (3.5.34). By section 3.2, $M_{13}(X;e)$ counts pairs $(a,b) \in \mathbb{Z}^2$ with

- (a,b) 13-groomed,
- $H(A_{13}(a,b), B_{13}(a,b)) \leq X$ and
- $e \mid \operatorname{tmd}(A_{13}(a,b), B_{13}(a,b))$.

To avoid technical inconvenience, and in contrast to Proposition 4.3.1 and Proposition 5.3.1, we opt not to refine Lemma 3.5.7. Instead, we proceed directly to an analogue of Lemma 4.3.16 and Lemma 5.3.12.

Lemma 6.3.1. *The following statements hold.*

(a) *If* $\gcd(d,e) > 1$*, then* $M_{13}(X;d,e) = 0$*. If* $\gcd(d,e) = 1$*, we have*

$$M_{13}(X;d,e) = \frac{R_{13}X^{1/18}}{d^2} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell}\right) \sum_{\substack{e_1e_2 = e \\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^3 e_2^2} + O\left(\frac{2^{\omega(e)}X^{1/24}}{de^{3/2}}\right) \tag{6.3.2}$$

for $X, d, e \geq 1$*. Here,* R_{13} *is the area of* (3.3.5) *for* $m = 13$*.*

(b) *We have*

$$M_{13}(X;e) = \frac{R_{13}X^{1/12}}{\zeta(2)\prod_{\ell \mid e}\left(1 + \frac{1}{\ell}\right)} \sum_{\substack{e_1e_2 = e \\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^3 e_2^2} + O\left(2^{2\omega(e)}X^{1/24}\log X\right) \tag{6.3.3}$$

for $X \geq 2$ *and* $d, e \geq 1$*.*

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

Proof. We begin with (a) and examine the summands $M_{13}(X;d,e)$. If d and e are not coprime, then $M_{13}(X;d,e) = 0$ 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 $M_{13}(X; 1, e)$ to the pairs counted by $M_{13}(d^{24}X; d, e)$ given by $(a, b) \mapsto (da, db)$.

Combining 6.2.14(e)-(g) and Corollary 3.3.11, we have

$$\begin{aligned} M_{13}(X;1,e) = & \sum_{\substack{e_1e_2=e \\ \gcd(e_1,e_2)=1}} \sum_{(a_0,b_0)\in\widetilde{\mathcal{T}}_{13}(e_1,e_2)} \# \left\{ (a,b) \in \mathcal{R}_{13}(X) \cap \mathbb{Z}^2 : \begin{array}{l} (a,b) \equiv (a_0,b_0) \pmod{e_1^3e_2^2}, \\ a/b \notin \mathscr{C}_{13} \end{array} \right\} \\ =& \varphi(e_1^3e_2^2) \left(R_7 X^{1/12} \sum_{\substack{e_1e_2=e \\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^6e_2^4} + O\left(X^{1/24} \sum_{\substack{e_1e_2=e \\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^3e_2^2} \right)\right) \\ =& R_{13}X^{1/12} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell}\right) \sum_{\substack{e_1e_2=e \\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^3e_2^2} + O(X^{1/24} \sum_{\substack{e_1e_2=e \\ \gcd(e_1,e_2)=1}} T_{13}(e_1,e_2)). \end{aligned} \tag{6.3.4}$$

Scaling by d and invoking Lemma 6.2.14(f), we obtain

$$M_{13}(X; d, e) = \frac{R_{13}X^{1/12}}{d^2} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell}\right) \sum_{\substack{e_1e_2=e \\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^3e_2^2} + O\left(\frac{2^{2\omega(e)}X^{1/24}}{d}\right). \tag{6.3.5}$$

For part (b), we compute

$$\begin{aligned}M_{13}(x;e) &= \sum_{\substack{d \ll X^{1/24}\\ \gcd(d,e)=1}} \mu(d) M_{13}(X;d,e)\\ &= \sum_{\substack{d \ll X^{1/24}\\ \gcd(d,e)=1}} \mu(d) \frac{R_{13} X^{1/12}}{d^2} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell}\right) \sum_{\substack{e_1 e_2 = e\\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^3 e_2^2}\\ &\quad + \sum_{\substack{d \ll X^{1/24}\\ \gcd(d,e)=1}} \mu(d) \cdot O\left(\frac{2^{2\omega(e)} X^{1/24}}{d}\right)\\ &= \frac{R_{13} X^{1/12}}{\prod_{\ell \mid e}\left(1 - \frac{1}{\ell}\right)} \sum_{\substack{e_1 e_2 = e\\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^3 e_2^2} \sum_{\substack{d \ll X^{1/24}\\ \gcd(d,e)=1}} \frac{\mu(d)}{d^2}\\ &\quad + O\left(2^{2\omega(e)} X^{1/24} \sum_{\substack{d \ll X^{1/24}\\ \gcd(d,e)=1}} \frac{1}{d}\right).\end{aligned} \tag{6.3.6}$$

Plugging the straightforward estimates

$$\sum_{\substack{d \ll X^{1/24}\\ \gcd(d,e)=1}} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell^2}\right)^{-1} + O(X^{-1/24}) \tag{6.3.7}$$

and

$$\sum_{d \leq X^{1/24}} \frac{1}{d} = \frac{1}{24} \log X + O(1) \tag{6.3.8}$$

into (6.3.6) then simplifies to give

$$M_{13}(x;e) = \frac{R_{13} X^{1/12}}{\zeta(2) \prod_{\ell \mid e}\left(1 + \frac{1}{\ell}\right)} \sum_{\substack{e_1 e_2 = e\\ \gcd(e_1,e_2)=1}} \frac{T_{13}(e_1,e_2)}{e_1^3 e_2^2} + O\left(2^{2\omega(e)} X^{1/24} \log X\right) \tag{6.3.9}$$

proving (b). □

Remark 6.3.10. The alternate proofs for Lemma 4.3.16 and Lemma 5.3.12 do not carry over directly to Lemma 6.3.1, even though both $C_{13,\mathrm{II}}(a,b)$ and $C_{13,\mathrm{III}}(a,b)$ are norms on orders of class number 1, precisely because we have two such factors (i.e., because the elliptic surface under consideration has places of both potential type II and potential type III additive reduction). However, we believe these arguments can be salvaged in part by applying the improved sieving to the larger of e_1 and e_2 for each factorization $e = e_1e_2$ occurring in the outer sum of (6.3.4). This will not yield an error term of the same strength as Lemma 4.3.16 and Lemma 5.3.12, because the other term e_i will be $O(\sqrt{e})$, and must be approximated by summing over congruence classes in the manner indicated in the proof above. Nevertheless, such an argument ought to be able to improve on the error term of Lemma 6.3.1, and therefore of Theorem 6.3.34 and Theorem 6.4.5 below.

We let

$$Q_{13} := \sum_{n\geq 1} \frac{\varphi_{1/2}(n)}{\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)} \sum_{\substack{n_1n_2=n\\ \gcd(n_1,n_2)=1}} \frac{T_{13}(n_1,n_2)}{n_1^3n_2^2}, \tag{6.3.11}$$

and we let

$$c_{13}^{\mathrm{tw}} := \frac{Q_{13}R_{13}}{\zeta(2)}. \tag{6.3.12}$$

Here, as always, R_{13} is the area of the region

$$\mathcal{R}_{13}(1) = \left\{(a,b)\in\mathbb{R}^2 : H(A_m(a,b),B_m(a,b)) \leq 1, b\geq 0\right\}. \tag{6.3.13}$$

We are now in a position to estimate $N_{13,\leq y}^{\mathrm{tw}}(X)$. Our argument is similar to those given in Proposition 4.3.42 and Lemma 5.3.25, but complicated by the necessity of summing over factorizations for the twist minimality defect e.

Lemma 6.3.14. *Suppose $y \ll X^{1/24}$. Then*

$$N_{13,\leq y}^{\mathrm{tw}}(X) = c_{13}^{\mathrm{tw}}X^{1/12} + O\left(\max\left(\frac{X^{1/12}\log^3 y}{y}, X^{1/24}y^{5/4}\log X\log^7 y\right)\right) \tag{6.3.15}$$

for $X, y \geq 2$. The constant c_{13}^{tw} is given in (6.3.12).

Proof. Substituting the asymptotic for $M_{13}(X;e)$ from Lemma 6.3.1(b) into the defining series (3.5.18) for $N_{13,\leq y}^{\mathrm{tw}}(X)$, we have

$$\begin{aligned} N_{13,\leq y}^{\mathrm{tw}}(X) =& \sum_{n\leq y}\sum_{e\mid n}\mu\left(n/e\right)\frac{R_{13}e^{1/2}X^{1/12}}{\zeta(2)\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}\sum_{\substack{n_1n_2=n\\ \gcd(n_1,n_2)=1}}\frac{T_{13}(n_1,n_2)}{n_1^3n_2^2} \\ &+\sum_{n\leq y}\sum_{e\mid n}\mu\left(n/e\right)O\left(2^{2\omega(n)}e^{1/6}X^{1/24}\log e^6X\right). \end{aligned} \tag{6.3.16}$$

We handle the main term and the error of this expression separately. For the main term, recalling the definition of the generalized totient function (5.3.21), we have

$$\begin{aligned} &\sum_{n\leq y}\sum_{e\mid n}\mu\left(n/e\right)\frac{R_{13}e^{1/2}X^{1/12}}{\zeta(2)\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}\sum_{\substack{n_1n_2=n\\ \gcd(n_1,n_2)=1}}\frac{T_{13}(n_1,n_2)}{n_1^3n_2^2} \\ =&\frac{R_{13}X^{1/12}}{\zeta(2)}\sum_{n\leq y}\frac{\varphi_{1/2}(n)}{\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}\sum_{\substack{n_1n_2=n\\ \gcd(n_1,n_2)=1}}\frac{T_{13}(n_1,n_2)}{n_1^3n_2^2}. \end{aligned} \tag{6.3.17}$$

By Lemma 6.2.14(f), we see

$$\frac{\varphi_{1/2}(n)}{\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}\sum_{\substack{n_1n_2=n\\ \gcd(n_1,n_2)=1}}\frac{T_{13}(n_1,n_2)}{n_1^3n_2^2} = O\left(\frac{4^{\omega(n)}}{n^{3/2}}\right). \tag{6.3.18}$$

Corollary 3.4.6 and Theorem 3.4.49 together yield

$$\sum_{n>y}\frac{4^{\omega(n)}}{n^{3/2}} = O\left(\frac{\log^3 y}{y^{1/2}}\right). \tag{6.3.19}$$

Thus, the series

$$\sum_{n\geq 1}\frac{\varphi_{1/2}(n)}{\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}\sum_{\substack{n_1n_2=n\\ \gcd(n_1,n_2)=1}}\frac{T_{13}(n_1,n_2)}{n_1^3n_2^2} = Q_{13} \tag{6.3.20}$$

is absolutely convergent, and

$$\begin{aligned}\frac{R_{13}X^{1/12}}{\zeta(2)}\sum_{n\leq y}\frac{\varphi_{1/2}(n)}{\prod_{\ell\mid n}\left(1+\frac{1}{\ell}\right)}\sum_{\substack{n_1n_2=n\\ \gcd(n_1,n_2)=1}}\frac{T_{13}(n_1,n_2)}{n_1^3n_2^2}&=\frac{R_{13}X^{1/12}}{\zeta(2)}\left(Q_{13}+O\left(\frac{\log^3 y}{y^{1/2}}\right)\right)\\ &=c_{13}^{\mathrm{tw}}X^{1/12}+O\left(\frac{X^{1/24}\log^3 y}{y^{1/2}}\right).\end{aligned} \tag{6.3.21}$$

As the summands of (6.3.20) constitute a nonnegative multiplicative arithmetic function, we can factor Q_{13} as an Euler product. We have

$$Q_{13}=\prod_{p\text{ prime}}Q_{13}(p),; \tag{6.3.22}$$

by Lemma 6.2.14, the terms $Q_{13}(p)$ are computed as follows:

$$\begin{aligned}Q_{13}(p)&:=\sum_{a\geq 0}\frac{\varphi_{1/2}(p^a)}{1+1/p}\left(\frac{T_{13}(p^a,1)}{p^{3a}}+\frac{T_{13}(1,p^a)}{p^{2a}}\right)\\ &=\begin{cases}1+\dfrac{2p^{1/2}\left(p^2+p^{3/2}+2p+2p^{1/2}+2\right)}{(p+1)\left(p+p^{1/2}+1\right)\left(p^2+p^{3/2}+p+p^{1/2}+1\right)}, & \text{if } p\equiv 1 \pmod{12}\\ & \quad\text{and } p\neq 13;\\ 1+\dfrac{2p^{1/2}}{(p+1)\left(p+p^{1/2}+1\right)}, & \text{if } p\equiv 5 \pmod{12};\\ 1+\dfrac{2p^{1/2}}{(p+1)\left(p^2+p^{3/2}+p+p^{1/2}+1\right)}, & \text{if } p\equiv -5 \pmod{12};\\ \frac{4}{3}, & \text{if } p=2;\\ \frac{21+17\sqrt{3}}{36}, & \text{if } p=3;\\ 1 & \text{if } p\equiv -1 \pmod{13}.\end{cases}\end{aligned} \tag{6.3.23}$$

We have been unable to compute $Q_{13}(13)$ because we do not know $T_{13}(13^v,1)$ and $T_{13}(1,13^v)$ for all $v\geq 0$. The square roots appear in (6.3.23) because of the generalized Jordan totient function $\varphi_{1/2}$. For instance, for $p = 3$ we have

$$\begin{aligned} Q_{13}(3) =& 1 + \frac{\varphi_{1/2}(3)}{1+1/3}\left(\frac{T_{13}(3,1)}{3^3} + \frac{T_{13}(1,3)}{3^2}\right) + \frac{\varphi_{1/2}(3^2)}{1+1/3}\left(\frac{T_{13}(3^2,1)}{3^6} + \frac{T_{13}(1,3^2)}{3^4}\right) \\ =& 1 + \frac{\sqrt{3}-1}{1+1/3} \cdot \frac{18}{3^3} + \frac{3-\sqrt{3}}{1+1/3} \cdot \frac{27}{3^6} \\ =& \frac{21+7\sqrt{3}}{36}. \end{aligned} \tag{6.3.24}$$

We now turn to the error term. Since $y \ll X^{1/24}$, for $e \leq y$ we have $\log(e^6 X) \ll \log X$. We obtain

$$\sum_{n \leq y} \sum_{e|n} \mu\left(n/e\right) O\left(4^{\omega(n)} e^{1/4} X^{1/24} \log e^6 X\right) = O\left(X^{1/12} \log X \sum_{n \leq y} 4^{\omega(n)} \sum_{e|n} \left|\mu\left(n/e\right)\right| e^{1/4}\right) \tag{6.3.25}$$

As in the proof of Proposition 4.3.42, we note

$$\sum_{e|n} \left|\mu\left(n/e\right)\right| e^{1/4} \leq n^{1/4} \prod_{p|n} \left(1 + p^{-1/4}\right) \leq 2^{\omega(n)} n^{1/4}; \tag{6.3.26}$$

Theorem 3.4.49 tells us $\sum_{n \leq y} 8^{\omega(n)} = O(y \log^7 y)$, so by Corollary 3.4.6, we have

$$\sum_{n \leq y} 4^{\omega(n)} \sum_{e|n} \left|\mu\left(n/e\right)\right| e^{1/4} = O\left(y^{5/4} \log^7 y\right), \tag{6.3.27}$$

and our desired result follows. □

We emphasize that the proof of Lemma 6.3.14 has given Q_{13} an Euler product expansion

$$Q_{13} = \prod_p Q_{13}(p), \tag{6.3.28}$$

where $Q_{13}(p)$ is given by (6.3.23).

Lemma 6.3.29. *We have*

$$N^{\mathrm{tw}}_{13,>y}(X) = O\left(\frac{X^{1/12}\log^3 y}{y^{1/2}}\right) \tag{6.3.30}$$

for $X, y \geq 2$.

Proof. By Lemma 6.2.14, $T_{13}(e_1, e_2) = O(2^{\omega(e_1 e_2)}$, so by Lemma 6.3.1, we have

$$M_m(X; e) = O\left(\frac{4^{\omega(e)}X^{1/24}}{e^2}\right). \tag{6.3.31}$$

Now by Proposition 3.5.14, we see

$$N^{\mathrm{tw}}_{m,>y}(X) = O\left(\sum_{n>y}\frac{4^{\omega(n)}X^{1/12}}{n^{3/2}}\right). \tag{6.3.32}$$

Combining Theorem 3.4.49 and Corollary 3.4.6, we conclude

$$N^{\mathrm{tw}}_{m,>y}(X) = O\left(\frac{X^{1/12}\log^3 y}{y^{1/2}}\right) \tag{6.3.33}$$

as desired. □

We are now ready to prove Theorem 1.2.13 for $m = 13$, which we restate here with an improved error term in the notations we have established.

Theorem 6.3.34. *We have*

$$N^{\mathrm{tw}}_{13}(X) = N^{\mathrm{tw}}_{13}(X) = c^{\mathrm{tw}}_{13}X^{1/12} + O\left(X^{7/108}\log^{43/9} X\right) \tag{6.3.35}$$

for $X \geq 2$. *The constant* c^{tw}_{13} *is given in* (6.3.12).

Proof. Let y be a positive quantity with $y \ll X^{1/24}$. *A fortiori*, we have $\log y \ll \log X$.

Lemma 6.3.14 and Lemma 6.3.29 together tell us

$$N_{13}^{\text{tw}}(X) = c_{13}^{\text{tw}} X^{1/12} + O\left(\max\left(\frac{X^{1/12}\log^3 y}{y}, X^{1/24} y^{5/4} \log X \log^7 y\right)\right). \tag{6.3.36}$$

We let $y = X^{1/54}/\log^{16/9} X$, so

$$\frac{X^{1/12}\log^3 y}{y} \asymp X^{1/24} y^{5/4} \log X \log^7 y \asymp X^{7/108} \log^{43/9} X, \tag{6.3.37}$$

and we conclude

$$N_{13}^{\text{tw}}(X) = c_m^{\text{tw}} X^{1/d(m)} + O\left(X^{7/108}\log^{43/9} X\right) \tag{6.3.38}$$

as desired. □

L-series

As in the previous two chapters, we set up the next section by interpreting Theorem 6.3.34 in terms of Dirichlet series.

Recall (3.5.22), (3.5.23), (3.5.24), and (3.5.25).

Corollary 6.3.39. *The following statements hold.*

(a) The Dirichlet series $L_{13}^{\text{tw}}(s)$ has abscissa of (absolute) convergence $\sigma_a = \sigma_c = 1/12$ and has a meromorphic continuation to the region

$$\{s = \sigma + it \in \mathbb{C} : \sigma > 7/108\}. \tag{6.3.40}$$

(b) The function $L_{13}^{\text{tw}}(s)$ has a simple pole at $s = 1/12$ with residue

$$\operatorname{res}_{s=\frac{1}{12}} L_{13}^{\text{tw}}(s) = \frac{c_{13}^{\text{tw}}}{12}; \tag{6.3.41}$$

it is holomorphic elsewhere on the region (6.3.40).

(c) *We have*

$$\mu_{L_{13}^{\mathrm{tw}}}(\sigma) < 13/84 \tag{6.3.42}$$

for $\sigma > 7/108$.

Proof. The proof is structurally identical to the one given for Corollary 4.3.66. □

Section 6.4

Estimates for rational isomorphism classes for $m = 13$

In section 6.3, we counted the number of elliptic curves over $\mathbb{Q}$ with a cyclic 13-isogeny up to isomorphism over $\mathbb{Q}^{\mathrm{al}}$ (Theorem 6.3.34) for $m = 13$. In this section, as in section 4.4 and section 5.4, we count all isomorphism classes over $\mathbb{Q}$ by enumerating over twists using a Tauberian theorem (Theorem 3.4.37). We first describe the analytic behavior of $L_m(s)$ for $m = 10, 25$.

Theorem 6.4.1. *The following statements hold.*

(a) *The Dirichlet series* $L_{13}(s)$ *has a meromorphic continuation to the region*

$$\{s = \sigma + it \in \mathbb{C} : \sigma > 1/12\} \tag{6.4.2}$$

with a simple pole at $s = 1/6$ *and no other singularities on this region.*

(b) *The principal part of* $L_{13}(s)$ *at* $s = 1/6$ *is*

$$\frac{L_{13}^{\mathrm{tw}}(1/6)}{3\zeta(2)}\left(s - \frac{1}{6}\right)^{-1}. \tag{6.4.3}$$

Proof. The proof follows by letting $m = 13$ in the argument of Theorem 5.4.1. □

Using Theorem 6.4.1, we deduce the following lemma.

Lemma 6.4.4. *The sequence* $(\Delta N_m(n))_{n\geq 1}$ *is admissible* (Definition 3.4.36) *with parameters* $(1/6, 1/12, 13/84)$.

Proof. The proof is structurally identical to the one given for Lemma 5.4.5. □

We now prove Theorem 1.2.6 for $m = 13$, which we restate here for ease of reference in our established notation.

Theorem 6.4.5. *Define*

$$c_{13} := \frac{2L_{13}^{\mathrm{tw}}(1/6)}{\zeta(2)}. \tag{6.4.6}$$

For all $\epsilon > 0$,

$$N_{13}(X) = c_{13}X^{1/6} + O\left(X^{1/8+\epsilon}\right) \tag{6.4.7}$$

for $X \geq 1$. *The implicit constant depends only on* ϵ.

Proof. By Lemma 5.4.5, $(\Delta N_{13}(n))_{n\geq 1}$ is admissible with parameters $(1/6, 1/12, 13/42)$. We now apply Theorem 3.4.37 to the Dirichlet series $L_{13}(s)$, and our claim follows. □

Remark 6.4.8. We suspect that the true error on $N_m(X)$ is at most $O(X^{1/12+\epsilon})$, and the true error on $N_{13}^{\mathrm{tw}}(X)$ is at most $O(X^{1/24+\epsilon})$, but we have been unable to bound the error terms this far using our techniques. See Remark 4.4.14 for some related thoughts.

Section 6.5

Computations for $m = 13$

In this section, we describe an algorithm to enumerate the elliptic curves with a cyclic 13-isogeny and twist height at most X. We then use the list of elliptic curves admitting a cyclic 13-isogeny to estimate c_13. However, our ignorance about $T_{13}(13^v, 1)$ and $T_{13}(1, 13^v)$ prevents us from computing $Q_{13}(13)$, and thus from computing c_{13}^{tw}.

The algorithms described in section 4.5 and section 5.5 cannot be directly adapted to enumerate elliptic curves admitting a cyclic 13-isogeny, because both the quadratic form $C_{13,\mathrm{II}}(a,b)$ and the quadratic form $C_{13,\mathrm{III}}(a,b)$ can contribute to the twist minimality defect of the pair $(A_{13}(a,b), B_{13}(a,b))$.

We therefore adopt a more naïve algorithm. We first obtain bounds (6.5.3) on the magnitudes of $a, b \in \mathbb{Z}$ subject to the condition $\operatorname{twht}(A_{13}(a,b), B_{13}(a,b)) \leq X$. Recalling Theorem 6.2.27(b) and abiding by its notations, we have

$$\operatorname{tmd}(A_{13}(a,b), B_{13}(a,b)) \leq 2 \cdot 3 \cdot 13 \cdot C_{13,\mathrm{II}}(a,b)^{1/3} \cdot C_{13,\mathrm{III}}(a,b)^{1/2}. \tag{6.5.1}$$

By (3.1.10) and (6.5.1), if $\operatorname{twht}(A_{13}(a,b), B_{13}(a,b)) \leq X$ then

$$\frac{H(A_{13}(a,b), B_{13}(a,b))}{(2 \cdot 3 \cdot 13)^6 \cdot C_{13,\mathrm{II}}(a,b)^2 C_{13,\mathrm{III}}(a,b)^3} \leq X. \tag{6.5.2}$$

The left-hand side of (6.5.2) is homogeneous of degree 14 in a and b; a short computation shows that if $(a,b) \in \mathbb{R}^2$ satisfy (6.5.2), then

$$|a| < 5X^{1/14} \text{ and } |b| < 0.7X^{1/14} \tag{6.5.3}$$

(tighter bounds are possible).

For each coprime pair $(a,b) \in \mathbb{Z}^2$ satisfying (6.5.3) with $b > 0$, we determine the largest integer e such that $e^6 \mid \gcd(A_{13}(a,b)^3, B_{13}(a,b)^2)$ by computing the prime factorization of this expression. Necessarily this e is the twist minimality defect of $(A_{13}(a,b), B_{13}(a,b))$, and we now use (3.1.10) to compute $\operatorname{twht}(A_{13}(a,b), B_{13}(a,b)$. If the twist height is bounded by X, we report (a,b), together with their twist height and any auxiliary information we care to record.

Running our algorithm out to $X = 10^{48}$ in Sage took us approximately 15 CPU hours on a single core, producing 9644 elliptic curves admitting a cyclic 13-isogeny. We list the first few twist minimal elliptic curves admitting a cyclic 13-isogeny in Table 6.5.4.

(A, B)	(a, b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(6, 8)$	$(10, 1)$	1728	26364
$(-84, 322)$	$(4, 3)$	2799468	8788
$(-35, 350)$	$(7, 2)$	3307500	6591
$(-338, 2392)$	$(-2, 5)$	154484928	26364
$(-380, 2850)$	$(-16, 1)$	219488000	26364
$(-795, 8650)$	$(1, 4)$	2020207500	6591
$(-2227, 59534)$	$(11, 5)$	95696023212	19773
$(-9540, 358650)$	$(-8, 7)$	3473005207500	26364
$(1581, 403310)$	$(17, 3)$	4391791814700	10985
$(-12818, 745992)$	$(2, 1)$	15025609729728	12
$(21012, 672590)$	$(36, 1)$	37107540294912	43940
$(-24474, 1473688)$	$(-2, 1)$	58637420676288	12
$(-32844, 2292878)$	$(0, 1)$	141946817117868	4
$(40549, 144566)$	$(23, 1)$	266686134356596	6591
$(-49851, 4284054)$	$(-19, 2)$	495543307368204	6591
$(-82739, 9299442)$	$(5, 7)$	2334949780806828	6591
$(-83595, 9642950)$	$(1, 1)$	2510635086967500	3
$(-109235, 13896050)$	$(-1, 1)$	5213705551267500	3

Table 6.5.4: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 13-isogeny and $\mathrm{twht}\, E \leq 10^{16}$

Computing c_{13}

In this subsection, we estimate $c_{13} = 2N_{13}^{\mathrm{tw}}(1/6)/\zeta(2)$ by computing the partial sums of $L_{13}^{\mathrm{tw}}(1/6)$:

$$\sum_{n\leq 10^{48}} \frac{\Delta N_{13}^{\mathrm{tw}}(n)}{n^{1/6}} = 0.680\,532\,123\,1018\,161. \tag{6.5.5}$$

Multiplying by $2/\zeta(2)$, we estimate

$$c_{13} \approx 0.827\,427\,843. \tag{6.5.6}$$

Ironically, although we have an estimate for c_{13}, we are unable to estimate c_{13}^{tw}, due to our inability to estimate $Q_{13}(13)$. Nevertheless, we can estimate R_{13} by performing rejection sampling on the rectangle $[-0.8228, 0.8228] \times [0, 0.1822]$. We find $r_{13} := 33\,570\,382\,383$ of our first $s_{13} := 61\,749\,000\,000$ samples lie in R_{13}, so

$$R_{13} \approx 0.299\,828\,32 \cdot \frac{r_{13}}{s_{13}} = 0.163\,004\,281\,067\,749\,86, \tag{6.5.7}$$

with standard error

$$0.299\,828\,32 \cdot \sqrt{\frac{r_{13}(s_{13}-r_{13})}{s_{13}^3}} < 6.1 \cdot 10^{-7}. \tag{6.5.8}$$

This took 1 CPU week to compute.

Chapter 7

Counting elliptic curves with a cyclic m-isogeny for $m \in \{6, 8, 9, 12, 16, 18\}$

In this chapter, we prove Theorem 1.2.3 and Theorem 1.2.6 when $m \in \{6, 8, 9, 12, 16, 18\}$ (Theorem 7.3.14 and Theorem 7.3.18), and we prove Theorem 1.2.13 for these m as well as for $m = 4$ (Theorem 7.2.16 and Corollary 7.2.28). These results are new, but our arguments mirror those given in chapter 4, chapter 5, and chapter 6, and we encourage our readers to skim them on a first perusal of this thesis. Indeed, the sieving required for Theorem 7.2.16 is much simpler than what we required in previous chapters.

However, in contrast to chapter 4, chapter 5, and chapter 6, we may have

$$\widetilde{N}_m^{\mathrm{tw}}(X) \neq N_m^{\mathrm{tw}}(X) \text{ and } \widetilde{N}_m(X) \neq N_m(X) \tag{7.0.1}$$

for $m \in \{4, 6, 8, 12, 16\}$ (see Theorem 2.1.49 and Theorem 3.2.28). We therefore first estimate $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $\widetilde{N}_m(X)$, and then utilize these asymptotics to find estimates for $N_m^{\mathrm{tw}}(X)$ and $N_m(X)$ (Corollary 7.2.28). We decline to address the cases $m = 2, 3$ for two reasons: firstly, because the asymptotics of $\widetilde{N}_2(X)$, $N_2(X)$, $\widetilde{N}_3(X)$, and $N_3(X)$ are given by Theorem 2.3.4 and Theorem 2.3.6, and secondly, because the modular curves $X_0(2)$ and $X_0(3)$ each have exactly one elliptic point, which complicates the application of our method.

The organization of this chapter approximates that of chapter 4 and chapter 5. In section 7.1, we determine all possible twist minimality defects for $m \in \{4, 6, 8, 9, 12, 16, 18\}$. In section 7.2, we apply the framework developed in section 3.5 to prove Theorem 1.2.13 for $m \in \{4, 6, 8, 9, 12, 16, 18\}$. In section 7.3, we prove Theorem 1.2.3 and Theorem 1.2.6 for $m \in \{6, 8, 9, 12, 16, 18\}$. In section 7.4, we produce supplementary computations to estimate the constants appearing in Theorem 7.2.16 Theorem 7.3.18, and empirically confirm that the count of elliptic curves with a cyclic m-isogeny aligns with our theoretical estimates.

Section 7.1

The twist minimality defect for $m \in \{4, 6, 8, 9, 12, 16, 18\}$

In this section, we bound the twist minimality defect arising from the parameterization

$$y^2 = x^3 + A_m(a,b)x + B_m(a,b) \tag{7.1.1}$$

for $m \in \{4, 6, 8, 9, 12, 16, 18\}$.

The polynomials $f_m(t)$ and $g_m(t)$ given in Table 3.2.11 and Table 3.2.12 are coprime when $m \in \{4, 6, 8, 9, 12, 16, 18\}$, so it is markedly easier to handle the twist minimality defect in these cases.

Lemma 7.1.2. *Let $m \in \{4, 6, 8, 9, 12, 15, 18\}$, let $(a, b) \in \mathbb{Z}^2$ be m-groomed, and let ℓ be a prime. If $\ell \mid \operatorname{tmd}(A_m(a,b), B_m(a,b))$ then $\ell \in \{2, 3\}$.*

Proof. The resultants of $f_m(t)$ and $g_m(t)$ are given in Table 3.2.13. These resultants are all of the form $\pm 2^v \cdot 3^w$, and the claim follows. □

We now define $T_m(e)$; this definition is, *mutatis mutandis*, the same as Definition 4.2.12.

Definition 7.1.3. Let $m \in \{4, 6, 8, 9, 12, 16, 18\}$. For $e \in \mathbb{Z}_{>0}$, let $\widetilde{\mathcal{T}}_m(e)$ denote the image of

$$\left\{(a, b) \in \mathbb{Z}^2 : (a, b) \ m\text{-groomed}, \ e \mid \operatorname{tmd}(A_m(a, b), B_m(a, b))\right\} \tag{7.1.4}$$

under the projection

$$\mathbb{Z}^2 \to (\mathbb{Z}/e^3\mathbb{Z})^2, \tag{7.1.5}$$

and let $\widetilde{T}_m(e) := \#\widetilde{\mathcal{T}}_m(e)$. Similarly, let $\mathcal{T}_m(e)$ denote the image of

$$\left\{t \in \mathbb{Z} : e^2 \mid g_m(t) \text{ and } e^3 \mid g_m(t)\right\} \tag{7.1.6}$$

under the projection

$$\mathbb{Z} \to \mathbb{Z}/e^3\mathbb{Z}, \tag{7.1.7}$$

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

Let $m \in \{4, 6, 8, 9, 12, 16, 18\}$. By Lemma 7.1.2, $T_m(e) = 0$ whenever e has a prime divisor other than 2 and 3. Of course, much more is true.

Lemma 7.1.8. *Let $m \in \{4, 6, 8, 9, 12, 16, 18\}$. The following statements hold.*

(a) *$\widetilde{\mathcal{T}}_m(e)$ consists of those pairs $(a, b) \in (\mathbb{Z}/e^3\mathbb{Z})^2$ which satisfy the following conditions:*

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

(b) *Let $(a, b) \in \mathbb{Z}^2$. If $(a, b) \pmod{e^3} \in \widetilde{\mathcal{T}}_m(e)$ then $e \mid \operatorname{tmd}(A_m(a, b), B_m(a, b))$.*

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

(d) *Let ℓ be prime and let $v \geq 1$. The nonzero values of $T_m(\ell^v)$ are given in Table 7.1.9 and Table 7.1.10.*

Proof. The proofs of (a)–(c) are exactly as in the proof of Lemma 4.2.17. Part (d) is a short computation. □

m	$T_m(2^1)$	$T_m(2^2)$	$T_m(2^3)$	$T_m(2^4)$
4	2^2	—	—	—
6	2^2	2^5	—	—
8	2^2	2^5	—	—
9	2^2	—	—	—
12	2^2	2^5	—	—
16	2^2	2^5	—	—
18	2^2	2^5	2^8	2^{11}

Table 7.1.9: All nonzero $T_m(2^v)$ for $m \in \{4, 6, 8, 9, 12, 16, 18\}$

m	$T_m(3^1)$	$T_m(3^2)$	$T_m(3^3)$	$T_m(3^4)$	$T_m(3^5)$
4	3^2	—	—	—	—
6	3^2	—	—	—	—
8	—	—	—	—	—
9	3^2	—	—	—	—
12	3^2	3^5	3^8	—	—
16	3^2	3^5	3^8	3^{11}	—
18	3^2	3^5	3^8	3^{11}	3^{14}

Table 7.1.10: All nonzero $T_m(3^v)$ for $m \in \{4, 6, 8, 9, 12, 16, 18\}$

Theorem 4.2.35 can have no direct analogue for $m \in \{4, 6, 8, 9, 12, 16, 18\}$, because $A_m(a, b)$ and $B_m(a, b)$ are coprime polynomials for these m. Nevertheless, we have the following proposition.

Proposition 7.1.11. *Let $m \in \{4, 6, 8, 9, 12, 16, 18\}$, and let (a, b) be an m-groomed pair. We have*

$$\frac{1}{2^{24} \cdot 3^{30}} H(A_m(a,b), B_m(a,b)) \leq \operatorname{twht}(A_m(a,b), B_m(a,b)) \leq H(A_m(a,b), B_m(a,b)) \quad (7.1.12)$$

Proof. Examining Table 7.1.9 and Table 7.1.10, we find $T_m(2^v) = 0$ for $v > 4$ and $T_m(3^v) = 0$ for $v > 5$. The claim now follows from (3.1.10). □

Remark 7.1.13. For particular m, much sharper bounds on $\operatorname{twht}(A_m(a, b)$ may derived than those given in Proposition 7.1.11. For instance, if $m =$ and (a, b) is a 4-groomed pair, then

$$\frac{1}{2^{6} \cdot 3^{6}} H(A_4(a,b), B_4(a,b)) \leq \operatorname{twht}(A_4(a,b), B_4(a,b)) \leq H(A_4(a,b), B_4(a,b)). \quad (7.1.14)$$

We have no need to write down these more careful bounds, however.

Section 7.2

Estimates for twist classes for $m \in \{4, 6, 8, 9, 12, 16, 18\}$

In this section, we use section 3.5 to estimate $\widetilde{N}_m^{\text{tw}}(X)$ for $m \in \{4, 6, 8, 9, 12, 16, 18\}$, counting the number of twist minimal elliptic curves E over $\mathbb{Q}$ equipped with a cyclic m-isogeny.

Recall (3.5.6), (3.5.33), and (3.5.34). By section 3.2, for $m \in \{4, 6, 8, 9, 12, 16, 18\}$, $M_m(X; e)$ counts pairs $(a, b) \in \mathbb{Z}^2$ with

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

If $m = 4$, then by Lemma 3.2.1, we double-count multiples of the pair $(0, 1)$ where it appears.

We have the following refinement of Lemma 3.5.7.

Lemma 7.2.1. *Let $m \in \{4, 6, 8, 9, 12, 16, 18\}$. We have*

$$\widetilde{N}_m^{\text{tw}}(X) = \sum_{n \mid 2^4 \cdot 3^5} \sum_{e \mid n} \mu(n/e) M_m(e^6 X; n). \tag{7.2.2}$$

Proof. Recall (3.2.26). As in the proof of Proposition 7.1.11, we examine Table 7.1.9 and Table 7.1.10. We find $T_m(2^v) = 0$ for $v > 4$ and $T_m(3^v) = 0$ for $v > 5$. By (3.5.6), $M_m(e^6 X; n) = 0$ when $n \nmid 2^4 \cdot 3^5$. □

Remark 7.2.3. As with Proposition 7.1.11, sharper bounds are possible. For instance, when $m = 4$, we have

$$N_4^{\text{tw}}(X) = \sum_{n \mid 2 \cdot 3} \sum_{e \mid n} \mu(n/e) M_m(e^6 X; n). \tag{7.2.4}$$

Let $m \in \{4, 6, 8, 9, 12, 16, 18\}$. In order to estimate $M_m(X; e)$, we further unpack the m-groomed condition on pairs (a, b), as we did before with (4.3.9) and (5.3.10). We therefore let $M_m(X; d, e)$ denote the number of pairs $(a, b) \in \mathbb{Z}^2$ with

- $\gcd(da, db, e) = 1$, $b > 0$, and $a/b \notin \mathscr{C}_m$,
- $H(A_m(da, db), B_m(da, db)) \leq X$, and
- $e \mid \operatorname{tmd}(A_m(da, db), B_m(da, db))$.

Because $H(A_m(a, b), B_m(a, b))$ is homogeneous of degree $2d(m)$, another Möbius sieve yields

$$M_m(X; e) = \sum_{\substack{d \ll X^{1/2d(m)} \\ \gcd(d, e) = 1}} \mu(d) M_m(X; d, e). \tag{7.2.5}$$

Lemma 7.2.6. *Let $m \in \{4, 6, 8, 9, 12, 16, 18\}$. The following statements hold.*

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

$$M_m(X;d,e) = \frac{R_m T_m(e) X^{1/d(m)}}{d^2 e^2} \prod_{\ell \mid e} \left(1 - \frac{1}{\ell}\right) + O\left(\frac{2^{\omega(e)} X^{1/2d(m)}}{d}\right) \tag{7.2.7}$$

for $X, d, e \geq 1$*, where* R_m *is the area of* (3.3.5)*.*

(b) *We have*

$$M_m(X;e) = \frac{R_m T_m(e) X^{1/d(m)}}{\zeta(2) e^3 \prod_{\ell \mid e}\left(1 + \frac{1}{\ell}\right)} + O\left(2^{\omega(e)} X^{1/2d(m)} \log X\right) \tag{7.2.8}$$

for $X \geq 2$ *and* $d, e \geq 1$*.*

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

Because $\gcd(A_m(a,b), B_m(a,b)) = 1$ for $m \in \{4,6,8,9,12,16,18\}$, we are unable to produce proofs akin to the second proofs of Lemma 4.3.16 and Lemma 5.3.12. We do not need them, however, because Proposition 7.1.11 there are only finitely many possible values for $\operatorname{tmd}(A_m(a,b), B_m(a,b))$.

Proof. The proof is, *mutatis mutandis*, the same as the first proof of Lemma 4.3.16. □

In analogy with (4.3.14), for $m \in \{4,6,8,9,12,16,18\}$, we let

$$Q_m := \sum_{n \mid 2^4 \cdot 3^4} \frac{\varphi_{6/d(m)}(n) T_m(n)}{n^3 \prod_{\ell \mid n}\left(1 + \frac{1}{\ell}\right)}, \tag{7.2.9}$$

and we let

$$\widetilde{c}_m^{\mathrm{tw}} := \frac{Q_m R_m}{\zeta(2)}. \tag{7.2.10}$$

Here, as always, R_m is the area of the region

$$\mathcal{R}_m(1) = \left\{(a,b) \in \mathbb{R}^2 : H(A_m(a,b), B_m(a,b)) \leq 1, b \geq 0\right\}. \tag{7.2.11}$$

We also let

$$c_m^{\mathrm{tw}} := \widetilde{c}_m^{\mathrm{tw}} / \delta_m, \tag{7.2.12}$$

where

$$\delta_m := \begin{cases} 2 & \text{if } 4 \mid m, \\ 1 & \text{else.} \end{cases} \tag{7.2.13}$$

The factor δ_m appears because cyclic m-isogenies come in pairs when $4 \mid m$ (Theorem 3.2.28).

m	Q_m	$Q_m(2)$	$Q_m(3)$
4	6	2	3
6	3	2	3/2
8	2	2	—
9	2	4/3	3/2
12	$1+\sqrt{3}$	4/3	$3(1+\sqrt{3})/4$
16	4/3	4/3	—
18	$\left(1+2^{1/3}\right)\left(1+3^{2/3}\right)/2$	$2(1+2^{1/3})/3$	$3(1+3^{2/3})/4$

Table 7.2.14: Q_m and its nontrivial Euler factors for $m \in \{4,6,8,9,12,16,18\}$

We need not estimate $\widetilde{N}_{m,\leq y}^{\mathrm{tw}}(X)$ and $\widetilde{N}_{m,>y}^{\mathrm{tw}}(X)$ in order to estimate $\widetilde{N}_m^{\mathrm{tw}}(X)$, because by Lemma 7.2.1 we have

$$\widetilde{N}_m^{\mathrm{tw}}(X) = \widetilde{N}_{m,\leq y}^{\mathrm{tw}}(X) \tag{7.2.15}$$

whenever $y > 2^4 \cdot 3^5$. We are now in a position to estimate $\widetilde{N}_m^{\mathrm{tw}}(X)$.

Theorem 7.2.16. *Let $m \in \{4,6,8,9,12,16,18\}$. Then we have*

$$\widetilde{N}_m^{\mathrm{tw}}(X) = \widetilde{c}_m^{\mathrm{tw}} X^{1/d(m)} + O\left(X^{1/2d(m)} \log X\right), \tag{7.2.17}$$

for $X \geq 2$. The constant $\widetilde{c}_m^{\mathrm{tw}}$ is given in (7.2.10).

Proof. Substituting the asymptotic for $M_m(X;e)$ from Lemma 7.2.6(b) into (7.2.2) from Lemma 7.2.1, we have

$$\begin{aligned}\widetilde{N}_m^{\mathrm{tw}}(X) = &\sum_{n \mid 2^4 \cdot 3^5} \sum_{e \mid n} \mu\left(\frac{n}{e}\right) \frac{R_m T_m(n) e^{6/d(m)} X^{1/d(m)}}{\zeta(2) n^3 \prod_{\ell \mid n}\left(1+\frac{1}{\ell}\right)} \\ &+ \sum_{n \mid 2^4 \cdot 3^5} \sum_{e \mid n} \mu\left(\frac{n}{e}\right) O\left(2^{\omega(n)} e^{3/d(m)} X^{1/2d(m)} \log e^6 X\right).\end{aligned} \tag{7.2.18}$$

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

$$\begin{aligned}\sum_{n \mid 2^4 \cdot 3^5} \sum_{e \mid n} \mu\left(n/e\right) \frac{R_m T_m(n) e^{6/d(m)} X^{1/d(m)}}{\zeta(2) n^3 \prod_{\ell \mid n}\left(1+\frac{1}{\ell}\right)} &= \frac{R_m X^{1/d(m)}}{\zeta(2)} \sum_{n \mid 2^4 \cdot 3^5} \frac{T_m(n) \varphi_{6/d(m)}(n)}{n^3 \prod_{\ell \mid n}\left(1+\frac{1}{\ell}\right)} \\ &= \widetilde{c}_m^{\mathrm{tw}} X^{1/d(m)},\end{aligned} \tag{7.2.19}$$

where the last equality follows from (7.2.9) and (7.2.12).

The summands of (7.2.19) constitute a nonnegative multiplicative arithmetic function, so we can factor Q_m as an Euler product

$$Q_m = \prod_p Q_m(p). \tag{7.2.20}$$

Moreover, for $p \neq 2, 3$ prime, Lemma 7.1.8 implies $Q_m(p) = 1$, so in fact $Q_m = Q_m(2) Q_m(3)$. The values of Q_m, $Q_m(2)$, and $Q_m(3)$ are recorded in Table 7.2.14 above.

We now turn to the error term. As $e \leq 2^4 \cdot 3^5$, we have $\log(e^6 X) \ll \log X$. We obtain

$$\begin{aligned}
&\sum_{n \mid 2^4 \cdot 3^5} \sum_{e \mid n} \mu\left(n/e\right) O\left(2^{\omega(n)} e^{3/d(m)} X^{1/2d(m)} \log e^6 X\right) \\
=&O\left(X^{1/2d(m)} \log X \sum_{n \mid 2^4 \cdot 3^5} 2^{\omega(n)} \sum_{e \mid n} \left|\mu\left(n/e\right)\right| e^{3/d(m)}\right) \\
=&O\left(X^{1/2d(m)} \log X\right),
\end{aligned} \tag{7.2.21}$$

because

$$\sum_{n \mid 2^4 \cdot 3^5} 2^{\omega(n)} \sum_{e \mid n} \left|\mu\left(n/e\right)\right| e^{3/d(m)} \leq \sum_{n \mid 2^4 \cdot 3^5} 2^{\omega(n)} \prod_{p \mid n} (1+p) = 25 \cdot 41 < \infty, \tag{7.2.22}$$

independent of m. This proves our desired result. □

To finish our proof of Theorem 1.2.13, we bound the difference between $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $\delta_m N_m^{\mathrm{tw}}(X)$ for $m \in \{4, 5, 6, 8, 9, 12, 16, 18\}$.

Lemma 7.2.23. *Let $m \in \{4, 5, 6, 8, 9, 12, 16, 18\}$. We have*

$$\begin{aligned}
\widetilde{N}_4^{\mathrm{tw}}(X) &= 2N_4^{\mathrm{tw}}(X) + O(X^{1/12}), & \widetilde{N}_9^{\mathrm{tw}}(X) &= N_9^{\mathrm{tw}}(X), \\
\widetilde{N}_5^{\mathrm{tw}}(X) &= N_5^{\mathrm{tw}}(X) \quad + O(X^{1/18}), & \widetilde{N}_{12}^{\mathrm{tw}}(X) &= 2N_{12}^{\mathrm{tw}}(X) + O(1), \\
\widetilde{N}_6^{\mathrm{tw}}(X) &= N_6^{\mathrm{tw}}(X) \quad + O(X^{1/12}), & \widetilde{N}_{16}^{\mathrm{tw}}(X) &= 2N_{16}^{\mathrm{tw}}(X) + O(1), \ \textit{and} \\
\widetilde{N}_8^{\mathrm{tw}}(X) &= 2N_8^{\mathrm{tw}}(X) + O(X^{1/12}), & \widetilde{N}_{18}^{\mathrm{tw}}(X) &= N_{18}^{\mathrm{tw}}(X).
\end{aligned} \tag{7.2.24}$$

for $X \geq 1$. The implicit constant depends on m.

Proof. When $m \in \{9, 12, 16, 18\}$, Lemma 7.2.23 is a consequence of Corollary 2.1.50 and Corollary 3.2.36.

We recall Theorem 3.2.28, along with Table 3.2.30, Table 3.2.42, and Table 3.2.43 to address the remaining cases. For each proper divisor n of m, we consider the contribution to $\widetilde{N}_m^{\mathrm{tw}}(X) - \delta_m N_m^{\mathrm{tw}}(X)$ arising from elliptic curves equipped with a pair of unsigned cyclic m-isogenies whose kernels have intersection of order n. When $(m,n) = (6,1)$, the associated modular curve has genus 1, and is $\mathbb{Q}$-isomorphic to the elliptic curve $y^2 = x^3 + 1$, which has Mordell-Weil group $\mathbb{Z}/6\mathbb{Z}$, so this contribution is $O(1)$.

If

$$(m,n) \in \{(2,1),(3,1),(4,1),(5,1),(6,2),(6,3),(8,2)\}, \tag{7.2.25}$$

the associated modular curve has genus 0, but is not $X_0(m)$. In these cases, the universal families

$$y^2 = x^3 + f_{m,n}(t)x + g_{m,n}(t) \tag{7.2.26}$$

for elliptic curves (over $\mathbb{Q}$, up to quadratic twist) with this level structure are recorded in Table 3.2.42 and Table 3.2.43.

For such pairs (m,n), we can repeat the proof of Theorem 7.2.16 essentially verbatim to obtain asympotics for the number of elliptic curves equipped with two cyclic m-isogenies with kernels having order n intersection, with one caveat. When $m = 5$, we must follow the proof of Theorem 5.4.11 rather than of Theorem 7.2.16, because in this case $f_{5,1}$ and $g_{5,1}$ have a common factor $t^2 + 4$, just like $f_{25}(t)$ and $g_{25}(t)$.

Except when $m = 5$ and $n = 1$, i.e., when our modular curve has elliptic points, the asymptotics we obtain are the the same as those predicted by [16, Theorem 3.3.1], although we cannot apply this theorem directly because the congruence groups inducing our modular curves are not torsion-free. They also accord with [51, Theorem 1.2.2, Theorem 1.2.3] wherever these theorems apply.

We record the order of growth for these modular curves, though not the full asymptotics, in Table 3.2.30. □

Remark 7.2.27. It is no coincidence that we can count elliptic curfves equipped with a single unsigned cyclic 25-isogeny, or with two unsigned cyclic 5-isogenies, by essentially the same methods. Indeed, the modular curve $X_{\mathrm{sp}}(p)$ parameterizing elliptic curves equipped with two unsigned cyclic p-isogenies whose kernels have trivial intersection is isomorphic to the curve $X_0(p^2)$, because taking the dual of one of these two isogenies and composing yields a cyclic p^2-isogeny (see [16, Theorem 3.2.1]).

Corollary 7.2.28. *Let $m \in \{4, 6, 8, 9, 12, 16, 18\}$. We have*

$$N_m^{\mathrm{tw}}(X), c_m^{\mathrm{tw}} X^{1/d(m)} + O\left(X^{1/2d(m)} \log X\right), \tag{7.2.29}$$

for $X \geq 2$. We have $c_m^{\mathrm{tw}} = \widetilde{c}_m^{\mathrm{tw}}/2$ if $m \in \{4, 8, 12, 16\}$, and $c_m^{\mathrm{tw}} = \widetilde{c}_m^{\mathrm{tw}}$ if $m \in \{9, 18\}$.

Proof. Immediate from Theorem 7.2.16 and Lemma 7.2.23. □

L-series

To conclude this section, following Corollary 4.3.66, Corollary 5.3.55, and Corollary 6.3.39, we set up section 7.3 by interpreting the asymptotics given by Theorem 7.2.16 in terms of Dirichlet series.

Recall (3.5.22), (3.5.23), (3.5.24), and (3.5.25).

Corollary 7.2.30. *Let $m \in \{4, 6, 8, 9, 10, 12, 16, 18\}$. The following statements hold.*

(a) The Dirichlet series $\widetilde{L}_m^{\mathrm{tw}}(s)$ and $L_m^{\mathrm{tw}}(s)$ have abscissa of (absolute) convergence $\sigma_a = \sigma_c = 1/d\,(m)$, and have a meromorphic continuation to the region

$$\{s = \sigma + it \in \mathbb{C} : \sigma > 1/2d\,(m)\}. \tag{7.2.31}$$

(b) The function $\widetilde{L}_m^{\mathrm{tw}}(s)$ has a simple pole at $s = 1/d\,(m)$ with residue

$$\operatorname{res}_{s=\frac{1}{d(m)}} \widetilde{L}_m^{\mathrm{tw}}(s) = \frac{\widetilde{c}_m^{\mathrm{tw}}}{d\,(m)}, \tag{7.2.32}$$

and is holomorphic elsewhere on this region. Likewise, $L_m^{\mathrm{tw}}(s)$ has a simple pole at $s = 1/d\,(m)$ with residue

$$\operatorname{res}_{s=\frac{1}{d(m)}} L_m^{\mathrm{tw}}(s) = \frac{c_m^{\mathrm{tw}}}{d\,(m)}, \tag{7.2.33}$$

and is holomorphic elsewhere on this region.

(c) *We have*

$$\mu_{L_m^{\mathrm{tw}}}(\sigma) < 13/84 \tag{7.2.34}$$

for $\sigma > 1/2d\,(m)$.

Proof. The proof is structurally identical to the one given for Corollary 4.3.66. □

Section 7.3
Estimates for rational isomorphism classes for $m \in \{6, 8, 9, 12, 16, 18\}$

In section 7.2, we counted the number of elliptic curves over $\mathbb{Q}$ with a (cyclic) m-isogeny up to quadratic twist (Theorem 7.2.16) for $m \in \{4, 6, 8, 9, 12, 16, 18\}$. In this section, we count all isomorphism classes over $\mathbb{Q}$ by enumerating over twists using Landau's Tauberian theorem (Theorem 3.4.37). We will not handle the case $m = 4$ as it has already been addressed previously in [55]; there is no theoretical obstruction to working this case out using our methods, however. As in previous chapters, we first describe the analytic behavior of $\widetilde{L}_m(s)$ and $L_m(s)$ for $m \in \{6, 8, 9, 12, 16, 18\}$.

Theorem 7.3.1. *Let $m \in \{6, 8, 9\}$. The following statements hold.*

(a) *The Dirichlet series $\widetilde{L}_m(s)$ and $L_m(s)$ have a meromorphic continuation to the region* (7.2.31) *(i.e.,* (4.3.67)*) with a double pole at $s = 1/6$ and no other singularities on this region.*

(b) *The principal part of $\widetilde{L}_m(s)$ at $s = 1/6$ is*

$$\frac{1}{3\zeta(2)}\left(\frac{\widetilde{c}_m^{\mathrm{tw}}}{6}\left(s-\frac{1}{6}\right)^{-2}+\left(\widetilde{\ell}_{m,0}+\widetilde{c}_m^{\mathrm{tw}}\left(\gamma-\frac{2\zeta'(2)}{\zeta(2)}\right)\right)\left(s-\frac{1}{6}\right)^{-1}\right), \tag{7.3.2}$$

where $\widetilde{c}_m^{\mathrm{tw}}$ is given in (7.2.10), *and*

$$\widetilde{\ell}_{m,0} := \widetilde{c}_m^{\mathrm{tw}}\gamma + \frac{1}{6}\int_1^\infty \left(\widetilde{N}_m^{\mathrm{tw}}(u) - \widetilde{c}_m^{\mathrm{tw}}\left\lfloor u^{1/6}\right\rfloor\right) u^{-7/6}\,\mathrm{d}u \tag{7.3.3}$$

is the constant term of the Laurent expansion for $\widetilde{L}_m^{\mathrm{tw}}(s)$ around $s = 1/6$. Here, γ denotes the Euler-Mascheroni constant. Likewise, the principal part of $L_m(s)$ at $s = 1/6$ is

$$\frac{1}{3\zeta(2)}\left(\frac{c_m^{\mathrm{tw}}}{6}\left(s-\frac{1}{6}\right)^{-2}+\left(\ell_{m,0}+c_m^{\mathrm{tw}}\left(\gamma-\frac{2\zeta'(2)}{\zeta(2)}\right)\right)\left(s-\frac{1}{6}\right)^{-1}\right), \tag{7.3.4}$$

where c_m^{tw} is given in (7.2.12), *and*

$$\ell_{m,0} := c_m^{\mathrm{tw}}\gamma + \frac{1}{6}\int_1^\infty \left(N_m^{\mathrm{tw}}(u) - c_m^{\mathrm{tw}}\left\lfloor u^{1/6}\right\rfloor\right) u^{-7/6}\,\mathrm{d}u \tag{7.3.5}$$

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

Proof. The proof is, *mutatis mutandis*, the same as the proof of Theorem 4.4.1; however, we must run through the argument given there twice, once for $\widetilde{L}_m(s)$ and once for $L_m(s)$. □

Theorem 7.3.6. *Let $m \in \{12, 16, 18\}$. The following statements hold.*

(a) *The Dirichlet series $\widetilde{L}_m(s)$ and $L_m(s)$ have a meromorphic continuation to the region*

$$\{s = \sigma + it \in \mathbb{C} : \sigma > 1/12\} \tag{7.3.7}$$

with a simple pole at $s = 1/6$ and no other singularities on this region.

(b) *The principal part of* $\widetilde{L}_m(s)$ *at* $s = 1/6$ *is*

$$\frac{\widetilde{L}_m^{\mathrm{tw}}(1/6)}{3\zeta(2)}\left(s - \frac{1}{6}\right)^{-1}; \tag{7.3.8}$$

likewise, the principal part of $L_m(s)$ *at* $s = 1/6$ *is*

$$\frac{L_m^{\mathrm{tw}}(1/6)}{3\zeta(2)}\left(s - \frac{1}{6}\right)^{-1}. \tag{7.3.9}$$

Proof. The proof is, *mutatis mutandis*, the same as the proof of Theorem 5.4.1; however, we must run through the argument given there twice, once for $\widetilde{L}_m(s)$ and once for $L_m(s)$. □

We prove two analogues to Lemma 4.4.6: one for $m \in \{6, 8, 9\}$ and the other for $m \in \{12, 16, 18\}$.

Lemma 7.3.10. *Let* $m \in \{6, 8, 9\}$*. The sequences*

$$\left(\Delta\widetilde{N}_m(n)\right)_{n\geq 1} \text{ and } (\Delta N_m(n))_{n\geq 1} \tag{7.3.11}$$

are admissible (Definition 3.4.36) *with parameters* $(1/6, 1/12, 13/42)$.

Proof. The proof is structurally identical to the one given for Lemma 4.4.6; however, we must run through the argument given there twice, once for $\widetilde{L}_m(s)$ and once for $L_m(s)$. □

Lemma 7.3.12. *Let* $m \in \{12, 16, 18\}$*. The sequences*

$$\left(\Delta\widetilde{N}_m(n)\right)_{n\geq 1} \text{ and } (\Delta N_m(n))_{n\geq 1} \tag{7.3.13}$$

are admissible (Definition 3.4.36) *with parameters* $(1/6, 1/12, 13/84)$.

Proof. The proof is structurally identical to the one given for Lemma 5.4.5; however, we must run through the argument given there twice, once for $\widetilde{L}_m(s)$ and once for $L_m(s)$. □

With Lemma 7.3.10 and Lemma 7.3.12 at the ready, the proofs of Theorem 1.2.3 and Theorem 1.2.6 are essentially identical.

Theorem 7.3.14. *Let $m \in \{6, 8, 9\}$. We define*

$$\begin{aligned}
\widetilde{c}_m &:= \frac{\widetilde{c}_m^{\mathrm{tw}}}{3\zeta(2)}, \\
\widetilde{c}'_m &:= \frac{2}{\zeta(2)}\left(\widetilde{\ell}_{m,0} + \widetilde{c}_m^{\mathrm{tw}}\left(\gamma - 1 - \frac{2\zeta'(2)}{\zeta(2)}\right)\right), \\
c_m &:= \frac{c_m^{\mathrm{tw}}}{3\zeta(2)}, \quad \text{and} \\
c'_m &:= \frac{2}{\zeta(2)}\left(\ell_{m,0} + c_m^{\mathrm{tw}}\left(\gamma - 1 - \frac{2\zeta'(2)}{\zeta(2)}\right)\right),
\end{aligned} \tag{7.3.15}$$

where $\widetilde{c}_m^{\mathrm{tw}}$ is defined in (7.2.10), c_m^{tw} is defined in (7.2.12), $\widetilde{\ell}_{m,0}$ is defined in (7.3.3), and $\ell_{m,0}$ is defined in (7.3.5). Then for all $\epsilon > 0$, we have

$$\widetilde{N}_m(X) = \widetilde{c}_m X^{1/6} \log X + \widetilde{c}'_m X^{1/6} + O(X^{1/8+\epsilon}) \tag{7.3.16}$$

and

$$N_m(X) = c_m X^{1/6} \log X + c'_m X^{1/6} + O(X^{1/8+\epsilon}) \tag{7.3.17}$$

for $X \geq 1$. The implicit constants depend on m and ϵ.

Proof. By Lemma 7.3.10, both $\left(\Delta \widetilde{N}_m(n)\right)_{n\geq 1}$ and $(\Delta N_m(n))_{n\geq 1}$ are admissible with parameters $(1/6, 1/12, 13/42)$. We now apply Theorem 3.4.37 to the Dirichlet series $\widetilde{L}_m(s)$ and $L_m(s)$, and our claim follows. □

Theorem 7.3.18. *Let $m \in \{12, 16, 18\}$. Define*

$$\begin{aligned}
\widetilde{c}_m &= \frac{2\widetilde{L}_m^{\mathrm{tw}}(1/6)}{\zeta(2)}, \quad \text{and} \\
c_m &= \frac{2L_m^{\mathrm{tw}}(1/6)}{\zeta(2)}.
\end{aligned} \tag{7.3.19}$$

Then for all $\epsilon > 0$, we have

$$\widetilde{N}_m(X) = \widetilde{c}_m X^{1/6} \log X + O(X^{1/8+\epsilon}) \tag{7.3.20}$$

and

$$N_m(X) = c_m X^{1/6} + O(X^{1/8+\epsilon}) \tag{7.3.21}$$

for $X \geq 1$. The implicit constants depend on m and ϵ.

Proof. By Lemma 7.3.12, $(\Delta N_m(n))_{n\geq 1}$ is admissible with parameters $(1/6, 1/12, 13/84)$. We now apply Theorem 3.4.37 to the Dirichlet series $L_m(s)$, and our claim follows. □

Section 7.4

Computations for $m \in \{4, 6, 8, 9, 12, 16, 18\}$

In this section, we furnish computations which make Theorem 7.2.16, Corollary 7.2.28, Theorem 7.3.14, and Theorem 7.3.18 completely explicit. These computations mirror those given in section 4.5 and section 5.5.

Enumerating elliptic curves with a cyclic m-isogeny for $m \in \{6, 8, 9, 12, 16, 18\}$

We begin by outlining an algorithm for computing all elliptic curves equipped with (or admitting) a cyclic m-isogeny up to twist height X. Write e_m for the maximum twist minimality defect of a pair $(A_m(a,b), B_m(a,b))$ with $\gcd(a,b) = 1$: these values are determined by Table 7.1.9 and Table 7.1.10. For instance, $e_8 = 2^2$.

Recall from the proof of Lemma 3.3.7 that

$$\mathcal{R}_m(X) = \mathcal{R}_m(1) X^{1/2d(m)}; \tag{7.4.1}$$

however, $\mathcal{R}_m(1)$ is a compact region, and thus is contained within a rectangular enveloping region $[a_{\min}, a_{\max}] \times [0, b_{\max}]$ (see Table 7.4.11). We compute $(A_m(a,b), B_m(a,b))$ for all coprime pairs of integers (a,b) within the enveloping region

$$([a_{\min}, a_{\max}] \times [0, b_{\max}]) \cdot e_m^{3/d(m)} X^{1/2d(m)}. \tag{7.4.2}$$

For each such pair, we compute the twist minimality defect and thence the twist height of $(A_m(a,b), B_m(a,b))$, and we report the result if this twist height is at most X.

This algorithm furnishes all elliptic curves equipped with a cyclic m-isogeny. To instead enumerate elliptic curves admitting a cyclic m-isogeny, we simply omit duplicate elliptic curves.

In Table 7.4.3, we record a bound X and the number of elliptic curves equipped with cyclic m-isogeny up to that bound X, as well as how approximately how many CPU minutes it took us to compute that list of elliptic curves.

m	X	$\widetilde{N}_m^{\mathrm{tw}}(X)$	$N_m^{\mathrm{tw}}(X)$	CPU minutes
4	10^{21}	6 299 452	3 149 720	46
6	10^{42}	7 551 963	7 550 700	60
8	10^{42}	5 855 992	2 927 707	27
9	10^{42}	4 671 446	4 671 446	13
12	10^{84}	10 478 972	5 239 486	74
16	10^{84}	7 836 058	3 918 029	33
18	10^{126}	9 730 625	9 730 625	76

Table 7.4.3: Enumerating elliptic curves up to quadratic twist for $m \in \{4, 6, 8, 9, 12, 16, 18\}$

For $m \in \{4, 6, 8, 9, 12, 16, 18\}$, we list the first few twist minimal elliptic curves admitting a cyclic m-isogeny in Table 7.4.4, Table 7.4.5, Table 7.4.6, Table 7.4.7, Table 7.4.8, Table 7.4.9, and Table 7.4.10 below.

(A, B)	(a, b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(1, 0)$	$(0, 1)$	4	3
$(-2, 1)$	$(3, 1)$ or $(3, 5)$	32	6
$(1, 2)$	$(-3, 1)$ or $(3, 7)$	108	6
$(6, 7)$	$(-1, 1)$ or $(1, 3)$	1323	2
$(-11, 14)$	$(3, 2)$ or $(3, 4)$	5324	3
$(-11, 6)$	$(9, 1)$ or $(9, 17)$	5324	6
$(13, 14)$	$(-3, 5)$ or $(3, 11)$	8788	6
$(-2, 21)$	$(-9, 1)$ or $(9, 19)$	11907	6
$(13, 34)$	$(-3, 2)$ or $(3, 8)$	31212	3
$(22, 23)$	$(-3, 7)$ or $(3, 13)$	42592	6
$(-23, 28)$	$(6, 1)$ or $(6, 11)$	48668	3
$(-23, 42)$	$(9, 5)$ or $(9, 13)$	48668	6
$(-26, 51)$	$(9, 7)$ or $(9, 11)$	70304	6
$(-26, 5)$	$(15, 1)$ or $(15, 29)$	70304	6

Table 7.4.4: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 4-isogeny and $\mathrm{twht}\, E \leq 10^5$

(A,B)	(a,b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(0,1)$	$(1,1)$	27	4
$(-12,11)$	$(9,5)$	6912	12
$(-15,22)$	$(2,1)$	13500	1
$(33,74)$	$(0,1)$	147852	3
$(60,61)$	$(-3,1)$	864000	12
$(93,94)$	$(-1,1)$	3217428	4
$(-120,11)$	$(21,13)$	6912000	12
$(-75,506)$	$(9,7)$	6912972	12
$(-132,481)$	$(11,7)$	9199872	4
$(-123,598)$	$(7,5)$	9655308	4
$(-255,502)$	$(12,7)$	66325500	3
$(-348,2497)$	$(5,1)$	168576768	4
$(-372,2761)$	$(7,3)$	205915392	4
$(-387,766)$	$(7,4)$	231842412	1
$(-408,3107)$	$(9,1)$	271669248	12
$(-423,1342)$	$(8,5)$	302747868	1
$(-327,3454)$	$(4,3)$	322113132	1
$(-435,2162)$	$(27,17)$	329251500	12
$(-372,3611)$	$(15,11)$	352061667	12
$(213,3674)$	$(3,5)$	364453452	12
$(-552,4979)$	$(15,7)$	672786432	12

Table 7.4.5: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 6-isogeny and $\operatorname{twht} E \leq 10^9$

(A,B)	(a,b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(6,7)$	$(0,1)$ or $(4,3)$	1323	4
$(-3,322)$	$(2,3)$ or $(6,5)$	2799468	4
$(-138,623)$	$(4,1)$ or $(8,5)$	10512288	4
$(141,142)$	$(-2,1)$ or $(10,7)$	11212884	4
$(-138,2567)$	$(4,5)$ or $(8,7)$	177916203	4
$(141,4718)$	$(1,2)$ or $(5,4)$	601007148	1
$(-579,5362)$	$(3,1)$ or $(5,3)$	776418156	1
$(582,4417)$	$(-4,1)$ or $(16,11)$	788549472	4

Table 7.4.6: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 8-isogeny and $\mathrm{twht}\, E \leq 10^9$

(A,B)	(a,b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(0,2)$	$(0,1)$	108	2
$(24,2)$	$(2,1)$	55296	6
$(-48,142)$	$(-2,5)$	544428	6
$(-51,142)$	$(-1,2)$	544428	1
$(69,362)$	$(1,2)$	3538188	3
$(-96,362)$	$(-2,1)$	3538944	2
$(-120,502)$	$(-4,1)$	6912000	6
$(-120,506)$	$(-2,3)$	6912972	2
$(-75,506)$	$(-1,4)$	6912972	3
$(165,502)$	$(1,1)$	17968500	1
$(-264,1654)$	$(-4,7)$	73864332	6
$(-219,1654)$	$(-1,3)$	73864332	1

Table 7.4.7: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 9-isogeny and $\mathrm{twht}\, E \leq 10^9$

(A, B)	(a, b)	$\operatorname{twht}(E)$	$\operatorname{tmd}(E)$
$(213, 3674)$	$(-9, 5)$ or $(3, 1)$	364453452	108
$(-1947, 108214)$	$(-5, 3)$ or $(1, 1)$	316177284492	4
$(-5907, 61486)$	$(-9, 7)$ or $(-3, 5)$	824443510572	108
$(-9867, 324934)$	$(-6, 5)$ or $(-3, 4)$	3842513269452	27
$(-41547, 3259514)$	$(-9, 4)$ or $(-6, 1)$	286865949497292	27
$(-65307, 874294)$	$(-4, 3)$ or $(-1, 2)$	1114138529957772	1
$(-71643, 7378058)$	$(-15, 7)$ or $(-9, 1)$	1470893677938828	108
$(-11667, 11349074)$	$(-12, 7)$ or $(3, 2)$	3477639977751852	27
$(-168843, 12140858)$	$(-15, 11)$ or $(-3, 7)$	19253477048692428	108
$(-212043, 28562182)$	$(-7, 5)$ or $(-1, 3)$	38135707808174028	4
$(228813, 5274866)$	$(-21, 11)$ or $(9, 1)$	47918374464655188	108
$(276837, 35589962)$	$(-15, 8)$ or $(6, 1)$	84865738374033012	27
$(-386067, 92329774)$	$(-7, 3)$ or $(-5, 1)$	230169637578251052	4
$(-627483, 187952182)$	$(-9, 8)$ or $(-6, 7)$	988247863401150348	27

Table 7.4.8: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 12-isogeny and $\operatorname{twht} E \leq 10^{18}$

(A, B)	(a, b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(-3, 322)$	$(0, 1)$ or $(4, 3)$	2799468	4
$(-11523, 476098)$	$(3, 1)$ or $(5, 3)$	6120074050668	1
$(-11523, 584962)$	$(2, 3)$ or $(6, 5)$	9238874618988	4
$(-15843, 767522)$	$(4, 1)$ or $(8, 5)$	15906413128428	4
$(-15843, 1441118)$	$(1, 2)$ or $(5, 4)$	56074169427948	1
$(30237, 1524962)$	$(-2, 1)$ or $(10, 7)$	110579874088212	4
$(30237, 3904418)$	$(-1, 1)$ or $(7, 5)$	411600957805548	1
$(-311043, 66769598)$	$(5, 2)$ or $(7, 4)$	120370838936786028	1
$(-311043, 69595202)$	$(4, 5)$ or $(8, 7)$	130774287818361708	4

Table 7.4.9: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 16-isogeny and $\mathrm{twht}\, E \leq 10^{18}$

(A, B)	(a, b)	$\mathrm{twht}(E)$	$\mathrm{tmd}(E)$
$(-75, 506)$	$(-4, 1)$	6912972	3888
$(-1515, 22682)$	$(1, 2)$	13909063500	243
$(-24555, 1485286)$	$(-2, 1)$	59564011548492	16
$(-172227, 27405506)$	$(-2, 5)$	20434485218644332	3888
$(-393195, 94898662)$	$(1, 1)$	243155418015559500	1
$(-1123275, 458221178)$	$(8, 1)$	5669154212905687500	3888
$(-1143435, 440919866)$	$(-1, 4)$	5979907087519351500	243
$(1324653, 1127890514)$	$(-10, 1)$	34347699312421973292	3888
$(-2065467, 1142549354)$	$(4, 5)$	35246400621552810252	3888
$(-2046747, 1164275786)$	$(-5, 2)$	36599528858379780492	243
$(-2752707, 1757875394)$	$(5, 1)$	83433402148362948972	243
$(-4906515, 4040728274)$	$(2, 7)$	472475598685352563500	3888
$(2097645, 14640824018)$	$(-7, 1)$	5787550654003232936748	243
$(-11577747, 12814884434)$	$(1, 5)$	6207720523046065646892	243
$(-24565035, 46858172762)$	$(-4, 7)$	59294191693335605671500	3888
$(-26453307, 52372560746)$	$(-8, 5)$	74057898215523422065932	3888
$(-76172547, 255885590014)$	$(4, 1)$	1767890750702694206045292	16
$(-76182627, 255814479646)$	$(-1, 2)$	1768592684578826203703532	1
$(-88080555, 318174471718)$	$(-2, 3)$	2733380669628994787815500	16
$(-122727387, 523299579766)$	$(2, 3)$	7394085267179261308598412	16
$(-117935067, 566044198774)$	$(-3, 1)$	8650962944073889823783052	1

Table 7.4.10: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic 18-isogeny and $\operatorname{twht} E \leq 10^{25}$

Computing $\widetilde{c}_m^{\mathrm{tw}}$ and c_m^{tw}

In this subsection, we estimate the constants appearing in Theorem 7.2.16 and Corollary 7.2.28. The constants Q_m were computed already in Table 7.2.14.

We can estimate the area R_m of the region $\mathcal{R}_m$ by performing rejection sampling on an enveloping rectangle. This computation proceeds, *mutatis mutandis*, in exactly the same way that the analogous computations for $m \in \{7, 10, 25\}$ proceeded. We record these computations in Table 7.4.11 below, along with how many CPU days it took to complete them.

m	Enveloping region	# of trials	# of successes	CPU days
4	$[-0.4583, 0.4583] \times [0, 0.9166]$	319 525 000 000	65 68 1836 724	24
6	$[-0.677, 1.7036] \times [0, 1.0338]$	331 210 000 000	55 726 701 265	34
8	$[-0.677, 2.0309] \times [0, 1.3539]$	326 270 000 000	42 861 204 516	34
9	$[-0.677, 0.677] \times [0, 0.6801]$	316 167 000 000	131 922 088 793	34
12	$[-1.6456, 0.8228] \times [0, 0.8228]$	224 310 000 000	69 681 481 937	34
16	$[-0.8228, 2.4684] \times [0, 1.6456]$	110 452 000 000	19 715 984 750	14
18	$[-0.8781, 0.8781] \times [0, 0.5532]$	130 060 000 000	61 569 780 450	23

Table 7.4.11: Approximating R_m for $m \in \{4, 6, 8, 9, 12, 16, 18\}$

Recall (7.2.12) and (7.2.10). We have assembled everything we need to compute $\widetilde{c}_m^{\mathrm{tw}}$ and c_m^{tw}. We report each constituent factor of $\widetilde{c}_m^{\mathrm{tw}}$ in Table 7.4.13. The quantity R_m, along with its standard error, is estimated based on the sampling recorded in Table 7.4.11.

In Table 7.4.14, we then record $\widetilde{c}_m^{\mathrm{tw}}$, with an error term, as well as the ratio

$$\frac{\widetilde{N}_m^{\mathrm{tw}}(X)}{\widetilde{c}_m^{\mathrm{tw}} X^{1/d(m)}} \tag{7.4.12}$$

for m and X as in Table 7.4.3. In Table 7.4.15, we perform analogous computations for c_m^{tw}.

m	δ_m	Q_m	R_m	Error on R_m
4	2	6	0.172 703 107	$6.1 \cdot 10^{-7}$
6	1	3	0.414 078 663	$1.6 \cdot 10^{-6}$
8	2	2	0.481 622 136	$2.2 \cdot 10^{-6}$
9	1	2	0.384 231 017	$8.1 \cdot 10^{-7}$
12	2	$1 + \sqrt{3}$	0.630 926 202	$2.0 \cdot 10^{-6}$
16	1	$4/3$	0.966 770 617	$6.3 \cdot 10^{-6}$
18	2	$(1 + 2^{1/3})(1 + 3^{2/3})/2$	0.459 917 568	$1.4 \cdot 10^{-6}$

Table 7.4.13: Ingredients to compute $\widetilde{c}_m^{\mathrm{tw}}$ and c_m^{tw} for $m \in \{4, 6, 8, 9, 12, 16, 18\}$

m	$\widetilde{c}_m^{\mathrm{tw}}$	Error on $\widetilde{c}_m^{\mathrm{tw}}$	$\widetilde{N}_m^{\mathrm{tw}}(X)/\widetilde{c}_m^{\mathrm{tw}} X^{1/d(m)}$
4	0.629 945 396	$2.2 \cdot 10^{-6}$	0.999 999 688 . . .
6	0.755 188 924	$3.0 \cdot 10^{-6}$	1.000 009 767 . . .
8	0.585 582 298	$2.7 \cdot 10^{-6}$	1.000 028 863 . . .
9	0.467 168 897	$9.9 \cdot 10^{-7}$	0.999 947 990 . . .
12	1.047 897 587	$3.3 \cdot 10^{-6}$	0.999 999 630 . . .
16	0.783 634 746	$5.1 \cdot 10^{-6}$	0.999 963 062 . . .
18	0.973 099 640	$2.9 \cdot 10^{-6}$	0.999 961 832 . . .

Table 7.4.14: The constant $\widetilde{c}_m^{\mathrm{tw}}$, its error, and a related ratio

m	c_m^{tw}	Error on c_m^{tw}	$N_m^{\mathrm{tw}}(X)/c_m^{\mathrm{tw}}X^{1/d(m)}$
4	$0.314\,972\,698$	$1.1 \cdot 10^{-6}$	$0.999\,997\,783\ldots$
6	$0.755\,188\,924$	$3.0 \cdot 10^{-6}$	$0.999\,842\,524\ldots$
8	$0.292\,791\,149$	$1.4 \cdot 10^{-6}$	$0.999\,930\,158\ldots$
9	$0.467\,168\,897$	$9.9 \cdot 10^{-7}$	$0.999\,947\,990\ldots$
12	$0.523\,948\,794$	$1.7 \cdot 10^{-6}$	$0.999\,999\,630\ldots$
16	$0.391\,817\,373$	$2.6 \cdot 10^{-6}$	$0.999\,963\,062\ldots$
18	$0.973\,099\,640$	$2.9 \cdot 10^{-6}$	$0.999\,961\,832\ldots$

Table 7.4.15: The constant c_m^{tw}, its error, and a related ratio

Computing $\widetilde{c}_m$, $\widetilde{c}'_m$, c_m, c'_m for $m \in \{6, 8, 9\}$

In this subsection, for $m \in \{6, 8, 9\}$, we estimate the constants $\widetilde{c}_m$, c_m, $\widetilde{c}'_m$ and c'_m, which are defined in (7.3.15) and used in Theorem 7.3.14. Of course, $\widetilde{c}_9 = c_9$ and $\widetilde{c}'_9 = c'_9$ by Lemma 7.2.23.

We follow the same strategy as in section 4.5. For $m \in \{6, 8, 9\}$, we have the identities $\widetilde{c}_m = \widetilde{c}_m^{\mathrm{tw}}/3\zeta(2)$ and $c_m = c_m^{\mathrm{tw}}/3\zeta(2)$, whence we obtain the following table.

m	$\widetilde{c}_m$	Error on $\widetilde{c}_m$	c_m	Error on c_m
6	$0.153\,033\,271$	$4.8 \cdot 10^{-7}$	$0.153\,033\,271$	$4.8 \cdot 10^{-7}$
8	$0.118\,663\,783$	$4.4 \cdot 10^{-7}$	$0.059\,331\,892$	$2.2 \cdot 10^{-7}$
9	$0.094\,668\,211$	$1.7 \cdot 10^{-7}$	$0.094\,668\,211$	$1.7 \cdot 10^{-7}$

Table 7.4.16: The constants $\widetilde{c}_m$ and c_m and their error for $m \in \{6, 8, 9\}$

We can approximate $\widetilde{\ell}_{m,0}$ and $\ell_{m,0}$ by truncating the integrals (7.3.3) and (7.3.5) and using our approximations for $\widetilde{c}_m^{\mathrm{tw}}$ and c_m^{tw}. Truncating this integral at the X recorded in

Table 7.4.3 yields estimates for $\widetilde{\ell}_{m,0}$ and $\ell_{m,0}$ which we record in Table 7.4.20.

We now assess the error in these estimates. In Theorem 7.2.16, we have shown that for some $M > 0$ and for all $u > X$, we have

$$\left|N_m^{\mathrm{tw}}(u) - c_m^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor\right| < M u^{1/12} \log u. \tag{7.4.17}$$

Thus

$$\begin{aligned} &\left|\int_X^\infty \left(N_7^{\mathrm{tw}}(u) - c_7^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor\right) u^{-7/6} \,\mathrm{d}u\right| \\ &\qquad < M \int_X^\infty u^{-13/12} \log u \,\mathrm{d}u \\ &\qquad = 12 M X^{-1/12}(\log X + 12); \end{aligned} \tag{7.4.18}$$

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

$$\begin{aligned} -1.75 \cdot 10^{-1} &\le \frac{\widetilde{N}_6^{\mathrm{tw}}(u) - \widetilde{c}_6^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor}{u^{1/12} \log u} \le 6.52 \cdot 10^{-3}, \\ -1.75 \cdot 10^{-1} &\le \frac{N_6^{\mathrm{tw}}(u) - c_6^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor}{u^{1/12} \log u} \le 0, \\ -1.35 \cdot 10^{-1} &\le \frac{\widetilde{N}_8^{\mathrm{tw}}(u) - \widetilde{c}_8^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor}{u^{1/12} \log u} \le 9.80 \cdot 10^{-3}, \\ -6.72 \cdot 10^{-2} &\le \frac{N_8^{\mathrm{tw}}(u) - c_8^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor}{u^{1/12} \log u} \le 4.59 \cdot 10^{-3}, \\ -1.36 \cdot 10^{-1} &\le \frac{\widetilde{N}_9^{\mathrm{tw}}(u) - \widetilde{c}_9^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor}{u^{1/12} \log u} \le 3.30 \cdot 10^{-2}, \\ -1.36 \cdot 10^{-1} &\le \frac{N_9^{\mathrm{tw}}(u) - c_9^{\mathrm{tw}} \left\lfloor u^{1/6} \right\rfloor}{u^{1/12} \log u} \le 3.30 \cdot 10^{-2}, \end{aligned} \tag{7.4.19}$$

If we assume these bounds continue to hold for larger u, and combine this truncation error with the error arising from our approximations for $\widetilde{c}_m^{\mathrm{tw}}$ and c_m^{tw}, we obtain the estimates for $\widetilde{\ell}_{m,0}$ and $\ell_{m,0}$ given in Table 7.4.20, and the estimates for $\widetilde{c}_m$ and c'_m given in Table 7.4.21.

m	$\widetilde{\ell}_{m,0}$	Error on $\widetilde{\ell}_{m,0}$	$\ell_{m,0}$	Error on $\ell_{m,0}$
6	$-0.572\,182\,786$	$1.13 \cdot 10^{-1}$	$-0.636\,153\,135$	$1.15 \cdot 10^{-1}$
8	$-0.742\,599\,375$	$1.12 \cdot 10^{-1}$	$-0.371\,299\,687$	$5.65 \cdot 10^{-3}$
9	$-0.231\,206\,039$	$1.14 \cdot 10^{-1}$	$-0.231\,206\,039$	$1.14 \cdot 10^{-1}$

Table 7.4.20: The constants $\widetilde{\ell}_{m,0}$ and $\ell_{m,0}$ and their error for $m \in \{6, 8, 9\}$

m	$\widetilde{c}'_m$	Error on $\widetilde{c}'_m$	c'_m	Error on c'_m
6	$-0.037\,215\,321$	$1.78 \cdot 10^{-1}$	$-0.114\,993\,938$	$1.78 \cdot 10^{-1}$
8	$-0.392\,302\,971$	$1.14 \cdot 10^{-1}$	$-0.196\,151\,485$	$1.14 \cdot 10^{-1}$
9	$0.126\,227\,997$	$1.14 \cdot 10^{-1}$	$0.126\,227\,997$	$1.14 \cdot 10^{-1}$

Table 7.4.21: The constants $\widetilde{c}'_m$ and c'_m and their error for $m \in \{6, 8, 9\}$

As a sanity check, we now compute $\widetilde{N}_m(X)$ and $N_m(X)$ for $X = 10^{42}$, and verify

$$\frac{\widetilde{N}^{\mathrm{tw}}_m(X)}{X^{1/6}} - \widetilde{c}_m \log X \approx \widetilde{c}'_m, \tag{7.4.22}$$

and

$$\frac{N^{\mathrm{tw}}_m(X)}{X^{1/6}} - c_m \log X \approx c'_m, \tag{7.4.23}$$

as shown in Table 7.4.24 below.

m	X	$\widetilde{N}_m(X)$	$\frac{\widetilde{N}_m^{\mathrm{tw}}(X)}{X^{1/6}} - \widetilde{c}_m \log X$	$N_m(X)$	$\frac{N_m^{\mathrm{tw}}(X)}{X^{1/6}} - c_m \log X$
6	10^{42}	147 624 808	−0.037 148 635	146 844 192	−0.115 210 235
8	10^{42}	110 837 024	−0.392 102 846	55 418 512	−0.196 051 423
9	10^{42}	92 813 182	0.126 090 504	92 813 182	0.126 090 504

Table 7.4.24: Enumerating elliptic curves up to $\mathbb{Q}$-isomorphism for $m \in \{6, 8, 9\}$

We emphasize that for $m \in \{6, 8, 9\}$, the estimates in Table 7.4.24 for $\widetilde{c}'_m$ and c'_m depend on empirical rather than theoretical estimates for the implicit constant in the error term in the asymptotics of $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$.

Computing $\widetilde{c}_m$ and c_m for $m \in \{12, 16, 18\}$

In this subsection, for $m \in \{12, 16, 18\}$, we estimate

$$\widetilde{c}_m = 2\widetilde{N}_m^{\mathrm{tw}}(1/6)/\zeta(2) \text{ and } c_m = 2N_m^{\mathrm{tw}}(1/6)/\zeta(2), \tag{7.4.25}$$

the constants which appear in Theorem 7.3.18. Of course, $\widetilde{c}_{18} = c_{18}$ by Lemma 7.2.23.

We follow the same strategy as in section 5.5. We first compute the partial sums

$$\begin{aligned}
\sum_{n \leq 10^{84}} \frac{\Delta \widetilde{N}_{12}^{\mathrm{tw}}(n)}{n^{1/6}} &= 0.212\,842\,775\,719\,189\,16, \\
\sum_{n \leq 10^{84}} \frac{\Delta N_{12}^{\mathrm{tw}}(n)}{n^{1/6}} &= 0.106\,421\,387\,859\,584\,87, \\
\sum_{n \leq 10^{84}} \frac{\Delta \widetilde{N}_{16}^{\mathrm{tw}}(n)}{n^{1/6}} &= 0.269\,169\,745\,679\,629\,80, \\
\sum_{n \leq 10^{84}} \frac{\Delta N_{16}^{\mathrm{tw}}(n)}{n^{1/6}} &= 0.134\,584\,872\,839\,728\,06, \text{ and} \\
\sum_{n \leq 10^{126}} \frac{\Delta N_{18}^{\mathrm{tw}}(n)}{n^{1/6}} &= 0.107\,025\,809\,031\,522\,12.
\end{aligned} \tag{7.4.26}$$

We empirically confirm that

$$\begin{aligned}
&\widetilde{N}_{12}^{\mathrm{tw}}(X) < 1.090\,472 X^{1/12} \text{ for } X \leq 10^{84}, \\
&N_{12}^{\mathrm{tw}}(X) < 0.545\,236 X^{1/12} \text{ for } X \leq 10^{84}, \\
&\widetilde{N}_{16}^{\mathrm{tw}}(X) < 0.847\,726 X^{1/12} \text{ for } X \leq 10^{84}, \\
&N_{16}^{\mathrm{tw}}(X) < 0.423\,863 X^{1/12} \text{ for } X \leq 10^{84}, \text{ and} \\
&N_{18}^{\mathrm{tw}}(X) < 1.007\,095 X^{1/18} \text{ for } X \leq 10^{126}.
\end{aligned} \tag{7.4.27}$$

If these bounds continue to hold for larger X, then

$$\begin{aligned}
\sum_{n>10^{84}} \frac{\Delta\widetilde{N}_{12}^{\mathrm{tw}}(n)}{n^{1/6}} &= \int_{10^{84}}^{\infty} x^{-1/6} d\widetilde{N}_{12}^{\mathrm{tw}}(x) < 1.090\,472 X^{1/12} \cdot 10^{-7}, \\
\sum_{n>10^{84}} \frac{\Delta N_{12}^{\mathrm{tw}}(n)}{n^{1/6}} &= \int_{10^{84}}^{\infty} x^{-1/6} dN_{12}^{\mathrm{tw}}(x) < 5.452\,36 \cdot 10^{-8}, \\
\sum_{n>10^{84}} \frac{\Delta\widetilde{N}_{16}^{\mathrm{tw}}(n)}{n^{1/6}} &= \int_{10^{84}}^{\infty} x^{-1/6} d\widetilde{N}_{12}^{\mathrm{tw}}(x) < 8.477\,26 \cdot 10^{-8}, \\
\sum_{n>10^{84}} \frac{\Delta N_{16}^{\mathrm{tw}}(n)}{n^{1/6}} &= \int_{10^{84}}^{\infty} x^{-1/6} dN_{12}^{\mathrm{tw}}(x) < 4.238\,63 \cdot 10^{-8}, \text{ and} \\
\sum_{n>10^{126}} \frac{\Delta N_{18}^{\mathrm{tw}}(n)}{n^{1/6}} &= \int_{10^{126}}^{\infty} x^{-1/6} dN_{18}^{\mathrm{tw}}(x) < 5.035\,48 \cdot 10^{-15}.
\end{aligned} \tag{7.4.28}$$

Assuming (7.4.28), for $m \in \{12, 16, 18\}$, we therefore have the following estimtes for $\widetilde{c}_m$ and c_m.

m	$\widetilde{c}_m$	Error on $\widetilde{c}_m$	c_m	Error on c_m
12	0.258 785 783	$1.4 \cdot 10^{-7}$	0.129 392 891	$6.7 \cdot 10^{-8}$
16	0.327 271 167	$1.1 \cdot 10^{-7}$	0.163 635 583	$5.2 \cdot 10^{-7}$
18	0.130 127 779 816 231 5	$6.2 \cdot 10^{-15}$	0.130 127 779 816 231 5	$6.2 \cdot 10^{-15}$

Table 7.4.29: The constant $\widetilde{c}_m$ and c_m and their error for

$m \in 12, 16, 18$

We emphasize that for $m \in \{12, 16, 18\}$, the estimates in Table 7.4.29 for $\widetilde{c}_m$ and c_m depend on empirical rather than theoretical estimates for the implicit constant in the error term in the asymptotics of $\widetilde{N}_m^{\mathrm{tw}}(X)$ and $N_m^{\mathrm{tw}}(X)$.

Chapter 8

Counting elliptic curves with a cyclic m-isogeny when $X_0(m)$ has nonzero genus

For completeness, we prove Theorem 1.2.10 (Theorem 8.2.8 and Theorem 8.2.10) and Theorem 2.3.15 (Theorem 8.1.7), giving asymptotic counts for the number of elliptic curves over $\mathbb{Q}$ admitting (equivalently, equipped with) a cyclic m-isogeny when

$$m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}\,. \tag{8.0.1}$$

In each of these cases, the compactified moduli space $X_0(m)$ is of genus $g > 0$, so by Faltings's theorem (Theorem 2.1.1), each curve has a finite number of rational points. These points were enumerated classically [44], and summing over their quadratic twists gives us our desired asymptotics. Although we are unaware of any reference for Theorem 1.2.10 in the literature, we expect that the claims of this chapter are familiar to experts in the theory of arithmetic statistics.

Throughout the remainder of this chapter, we assume

$$m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}\,. \tag{8.0.2}$$

By Corollary 2.1.50, we have

$$\widetilde{N}_m^{\mathrm{tw}}(X) = N_m^{\mathrm{tw}}(X) \text{ and } \widetilde{N}_m(X) = N_m(X) \tag{8.0.3}$$

for all $X > 0$, so we may use either notation interchangeably. We opt to work with $N_m^{\mathrm{tw}}(X)$ and related functions.

In section 8.1, we record all elliptic curves admitting a cyclic m-isogeny up to twist equivalence, write $N_m^{\mathrm{tw}}(X)$ in terms of the Heaviside step function, and point out its long-run asymptotics. In section 8.2, we leverage Walfisz's and Liu's asymptotics for the count of squarefree integers to give asymptotics for the number of elliptic curves with a cyclic m-isogeny up to $\mathbb{Q}$-isomorphism.

Section 8.1

Counts for twist classes when $X_0(m)$ has nonzero genus

In this section, we write down all elliptic curves admitting cyclic m-isogeny, up to quadratic twist, and use this explicit enumeration to describe $N_m^{\mathrm{tw}}(X)$ for

$$m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 163\}. \tag{8.1.1}$$

The following table is extracted from [44, page 1].

m	(A, B)	$\mathrm{twht}(E)$	$j(E)$
11	$(-264, 1\,694)$	$77\,480\,172$	-32768
11	$(-363, 10\,406)$	$2\,923\,690\,572$	-121
11	$(-4\,323, 109\,406)$	$323\,181\,166\,572$	-24729001
14	$(-35, 98)$	$259\,308$	-3375
14	$(-595, 5\,586)$	$842\,579\,500$	16581375
15	$(-75, 2\,950)$	$234\,967\,500$	$-25/2$
15	$(-435, 4\,210)$	$478\,550\,700$	$-121945/32$
15	$(3\,165, 31\,070)$	$126\,818\,068\,500$	$46969655/32768$
15	$(-1\,8075, 935\,350)$	$23\,621\,749\,807\,500$	$-349938025/8$
17	$(-95\,115, 12\,657\,350)$	$4\,325\,629\,743\,607\,500$	$-882216989/131072$
17	$(-437\,835, 111\,510\,650)$	$335\,734\,876\,712\,407\,500$	$-297756989/2$
19	$(-152, 722)$	$14\,074\,668$	-884736
21	$(45, 18)$	$364\,500$	$3375/2$
21	$(-75, 262)$	$1\,853\,388$	$-140625/8$
21	$(-1\,515, 46\,106)$	$57\,395\,607\,372$	$-1159088625/2097152$
21	$(-17\,235, 870\,894)$	$20\,478\,321\,699\,372$	$-189613868625/128$
27	$(-270, -1\,708)$	$78\,766\,128$	-12288000
37	$(-1\,155, 16\,450)$	$730\,6267\,500$	-9317
37	$(-29\,963\,955, 6\,313\,1603\,150)$	$107\,611\,181\,539\,805\,427\,907\,500$	-162677523113838677
43	$(-3\,440, 42)$	$162\,830\,336\,000$	-884736000
67	$(-29\,480, 1\,948\,226)$	$102\,480\,782\,771\,052$	-147197952000
163	$(-8\,697\,680, 9\,873\,093\,538)$	$2\,631\,905\,352\,272\,628\,650\,988$	-262537412640768000

Table 8.1.2: $E \in \mathscr{E}^{\mathrm{tw}}$ with a cyclic m-isogeny when $X_0(m)$ has nonzero genus

By the Mazur's theorem on isogenies (Theorem 2.1.48), Table 8.1.2 it is an exhaustive list of elliptic curves admitting cyclic m-isogeny over $\mathbb{Q}$, up to quadratic twist, for

$$m \notin \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 16, 18, 25\}\,. \tag{8.1.3}$$

We emphasize that for each m in Table 8.1.2, each elliptic curve associated to this m admits exactly one unsigned cyclic m-isogeny.

Recall that the Heaviside step function $\theta : \mathbb{R} \to \mathbb{R}$ is given by

$$\theta(X) \coloneqq \begin{cases} 1 & \text{if } X \geq 0, \\ 0 & \text{if } X < 0. \end{cases} \tag{8.1.4}$$

The following lemma is immediate from Table 8.1.2.

Lemma 8.1.5. *Let $X > 0$ be arbitrary. We have the following identities:*

$$\begin{aligned}
N_{11}^{\mathrm{tw}}(X) =& \theta(X - 77\,480\,172) + \theta(X - 2\,923\,690\,572) + \theta(X - 323\,181\,166\,572),\\
N_{14}^{\mathrm{tw}}(X) =& \theta(X - 259\,308) + \theta(X - 842\,579\,500),\\
N_{15}^{\mathrm{tw}}(X) =& \theta(X - 234\,967\,500) + \theta(X - 478\,550\,700)\\
& + \theta(X - 126\,818\,068\,500) + \theta(X - 23\,621\,749\,807\,500),\\
N_{17}^{\mathrm{tw}}(X) =& \theta(X - 4\,325\,629\,743\,607\,500) + \theta(X - 335\,734\,876\,712\,407\,500),\\
N_{19}^{\mathrm{tw}}(X) =& \theta(X - 14\,074\,668),\\
N_{21}^{\mathrm{tw}}(X) =& \theta(X - 364\,500) + \theta(X - 1\,853\,388)\\
& + \theta(X - 57\,395\,607\,372) + \theta(X - 20\,478\,321\,699\,372),\\
N_{27}^{\mathrm{tw}}(X) =& \theta(X - 78\,766\,128),\\
N_{37}^{\mathrm{tw}}(X) =& \theta(X - 730\,6267\,500) + \theta(X - 107\,611\,181\,539\,805\,427\,907\,500),\\
N_{43}^{\mathrm{tw}}(X) =& \theta(X - 162\,830\,336\,000),\\
N_{67}^{\mathrm{tw}}(X) =& \theta(X - 102\,480\,782\,771\,052),\\
N_{163}^{\mathrm{tw}}(X) =& \theta(X - 2\,631\,905\,352\,272\,628\,650\,988).
\end{aligned} \tag{8.1.6}$$

Proof. We inspect the twist heights in Table 8.1.2; as this table is exhaustive, the lemma follows. □

We recover Theorem 2.3.15, which reports the asymptotic behavior of $N_m^{\mathrm{tw}}(X)$, from Lemma 8.1.5.

Theorem 8.1.7. *For X sufficiently large, we have the following identities:*

$$\begin{aligned}
N_{11}^{\mathrm{tw}}(X) =& 3,\ N_{14}^{\mathrm{tw}}(X) = 2,\ N_{15}^{\mathrm{tw}}(X) = 4,\ N_{17}^{\mathrm{tw}}(X) = 2,\ N_{19}^{\mathrm{tw}}(X) = 1, N_{21}^{\mathrm{tw}}(X) = 4,\\
N_{27}^{\mathrm{tw}}(X) =& 1,\ N_{37}^{\mathrm{tw}}(X) = 2,\ N_{43}^{\mathrm{tw}}(X) = 1,\ N_{67}^{\mathrm{tw}}(X) = 1,\ N_{163}^{\mathrm{tw}}(X) = 1.
\end{aligned} \tag{8.1.8}$$

Proof. We take the limits of the identities listed in Lemma 8.1.5. Alternately, examine the first table in [44]. □

Section 8.2
Estimates for rational isomorphism classes when $X_0(m)$ has nonzero genus

In this section, we use the values we read off of Table 8.1.2, together with Walfisz's and Liu's asymptotics (Theorem 3.4.16 and Theorem 3.4.18) to prove Theorem 1.2.10.

Lemma 8.1.5 implies that $L_m^{\mathrm{tw}}(s)$, as a finite sum of terms of the form n^{-s}, is holomorphic on $\mathbb{C}$. For each elliptic curve E occurring in Table 8.1.2, we have $j(E) \neq 0, 1728$, so no additionl casework is necessary. It would therefore be straightforward to apply Theorem 3.4.37 to

$$L_m(s) = \frac{2\zeta(6s)L_m^{\mathrm{tw}}(s)}{\zeta(12s)}, \tag{8.2.1}$$

and obtain results akin to Theorem 4.4.11. For $m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 163\}$, write

$$c_m := \frac{2L_m^{\mathrm{tw}}(1/6)}{\zeta(2)}. \tag{8.2.2}$$

These constants are computed numerically in Table 8.2.12 below. For any $\epsilon > 0$, an argument along the lines we have sketched yields the asymptotic

$$N_m(X) = c_m X^{1/6} + O(X^{1/12+\epsilon}) \tag{8.2.3}$$

for $X \geq 1$.

However, we can do better than this.

Recall (3.2.24), which defines

$$S_2(X) = \#\left\{n \in \mathbb{Z}_{>0} : n \leq X,\ n \text{ squarefree}\right\} \tag{8.2.4}$$

to be the number of squarefree integers with size at most X.

Lemma 8.2.5. *Let $X > 0$ be arbitrary. We have the following identities:*

$$\begin{aligned}
\widetilde{N}_{11}(X) =& S_2\left((X/77\,480\,172)^{1/6}\right) + S_2\left((X/2\,923\,690\,572)^{1/6}\right) \\
&+ S_2\left((X/323\,181\,166\,572)^{1/6}\right), \\
\widetilde{N}_{14}(X) =& S_2\left((X/259\,308)^{1/6}\right) + S_2\left((X/842\,579\,500)^{1/6}\right), \\
\widetilde{N}_{15}(X) =& S_2\left((X/234\,967\,500)^{1/6}\right) + S_2\left((X/478\,550\,700)^{1/6}\right) \\
&+ S_2\left((X/126\,818\,068\,500)^{1/6}\right) + S_2\left((X/23\,621\,749\,807\,500)^{1/6}\right), \\
\widetilde{N}_{17}(X) =& S_2\left((X/4\,325\,629\,743\,607\,500)^{1/6}\right) + S_2\left((X/335\,734\,876\,712\,407\,500)^{1/6}\right), \\
\widetilde{N}_{19}(X) =& S_2\left((X/14\,074\,668)^{1/6}\right), \\
\widetilde{N}_{21}(X) =& S_2\left((X/364\,500)^{1/6}\right) + S_2\left((X/1\,853\,388)^{1/6}\right) \\
&+ S_2\left((X/57\,395\,607\,372)^{1/6}\right) + S_2\left((X/20\,478\,321\,699\,372)^{1/6}\right), \\
\widetilde{N}_{27}(X) =& S_2\left((X/78\,766\,128)^{1/6}\right), \\
\widetilde{N}_{37}(X) =& S_2\left((X/730\,6267\,500)^{1/6}\right) + S_2\left((X/107\,611\,181\,539\,805\,427\,907\,500)^{1/6}\right), \\
\widetilde{N}_{43}(X) =& S_2\left((X/162\,830\,336\,000)^{1/6}\right), \\
\widetilde{N}_{67}(X) =& S_2\left((X/102\,480\,782\,771\,052)^{1/6}\right), \\
\widetilde{N}_{163}(X) =& S_2\left((X/2\,631\,905\,352\,272\,628\,650\,988)^{1/6}\right).
\end{aligned} \tag{8.2.6}$$

Proof. Let E be an elliptic curve from Table 8.1.2. Recalling (3.1.16), we have

$$\begin{aligned}\#\left\{E^{(c)} : c \in \mathbb{Z},\ c \text{ squarefree},\ \operatorname{ht}(E^{(c)}) \leq X\right\} =& \#\left\{c \in \mathbb{Z} : c \text{ squarefree},\ c^6 \leq X/\operatorname{ht}(E)\right\} \\ =& S_2((X/\operatorname{ht}(E))^{1/6}).\end{aligned} \tag{8.2.7}$$

Summing over the elliptic curves E associated to each m, our claim follows. □

We are ready to prove Theorem 1.2.10, with a modestly improved error term.

Theorem 8.2.8. *Let $m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}$, and let c_m be given by (8.2.2). Then for κ sufficiently small, we have*

$$\widetilde{N}_m(X) = c_m X^{1/6} + O\left(X^{1/12} e^{-\kappa \frac{\log^{3/5} X}{\log^{1/5} \log X}}\right) \tag{8.2.9}$$

for $X \geq 2$. The implicit constant depends on κ and m.

Proof. We substitute the asymptotic for $S_2(X)$ given by Theorem 3.4.16 into the identities of Lemma 8.2.5. □

In the present of the Riemann hypothesis, we can use Theorem 3.4.18 to say even more.

Theorem 8.2.10. *Let $m \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}$, and let c_m be given by (8.2.2). Then for any $\epsilon > 0$, we have*

$$\widetilde{N}_m(X) = c_m X^{1/6} + O\left(X^{11/210+\epsilon}\right) \tag{8.2.11}$$

for $X \geq 1$. The implicit constant depends on ϵ and m.

Proof. We substitute the asymptotic for $S_2(X)$ given by Theorem 3.4.18 into the identities of Lemma 8.2.5. □

m	c_m
11	$0.05285852537804229\ldots$
14	$0.09590984282353528\ldots$
15	$0.05837531634681239\ldots$
17	$0.002235272618464 5135\ldots$
19	$0.03912417070300683\ldots$
21	$0.14024402788002174\ldots$
27	$0.02936262794471424\ldots$
37	$0.013888883070281625\ldots$
43	$0.00822676234970696\ldots$
67	$0.002810246610438085\ldots$
163	$0.00016360872509265466\ldots$

Table 8.2.12: c_m when $X_0(m)$ has nonzero genus

Bibliography

[1] *Birch and Swinnerton-Dyer conjecture*, https://www.claymath.org/millennium-problems/birch-and-swinnerton-dyer-conjecture, 2013.

[2] Oishee Banerjee, Jun-Yong Park, and Johannes Schmitt, *Étale cohomological stability of the moduli space of stable elliptic surfaces*, 2022.

[3] Baur Bektemirov, Barry Mazur, William Stein, and Mark Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 2, 233–254. MR 2291676

[4] 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. MR 3922423

[5] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242. MR 3272925

[6] N. H. Bingham, C. M. Goldie, and J. L. Teugels, *Regular variation*, Encyclopedia of Mathematics and its Applications, vol. 27, Cambridge University Press, Cambridge, 1987. MR 898871

[7] Brandon Boggess and Soumya Sankar, *Counting elliptic curves with a rational n-isogeny for small n*, 2020.

[8] J. Bourgain, *Decoupling, exponential sums and the Riemann zeta function*, J. Amer. Math. Soc. **30** (2017), no. 1, 205–224. MR 3556291

[9] 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. MR 4440538

[10] Armand Brumer, *The average rank of elliptic curves. I*, Invent. Math. **109** (1992), no. 3, 445–472. MR 1176198

[11] Armand Brumer and Oisín McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382. MR 1044170

[12] Armand Brumer and Joseph H. Silverman, *The number of elliptic curves over $\mathbb{Q}$ with conductor N*, Manuscripta Math. **91** (1996), no. 1, 95–102. MR 1404420

[13] Ana Caraiani, Matthew Emerton, Toby Gee, David Geraghty, Vytautas Paškūnas, and Sug Woo Shin, *Patching and the p-adic Langlands program for* $\mathrm{GL}_2(\mathbb{Q}_p)$, Compos. Math. **154** (2018), no. 3, 503–548. MR 3732208

[14] Garen Chiloyan and Álvaro Lozano-Robledo, *A classification of isogeny-torsion graphs of $\mathbb{Q}$-isogeny classes of elliptic curves*, Trans. London Math. Soc. **8** (2021), no. 1, 1–34. MR 4203041

[15] Laurent Clozel, *Motifs et formes automorphes: applications du principe de fonctorialité*, Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988), Perspect. Math., vol. 10, Academic Press, Boston, MA, 1990, pp. 77–159. MR 1044819

[16] 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. MR 4450609

[17] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183. MR 43821

[18] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196

[19] Andrzej Dąbrowski and Jacek Pomykała, *Signatures of Dirichlet characters and elliptic curves*, J. Number Theory **220** (2021), 94–106. MR 4177537

[20] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818. MR 1485897

[21] Jordan S. Ellenberg, Matthew Satriano, and David Zureick-Brown, *Heights on stacks and a generalized batyrev-manin-malle conjecture*, 2021.

[22] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR 718935

[23] ______, *Erratum: "Finiteness theorems for abelian varieties over number fields"*, Invent. Math. **75** (1984), no. 2, 381. MR 732554

[24] Clemens Fuchs, Rafael von Känel, and Gisbert Wüstholz, *An effective Shafarevich theorem for elliptic curves*, Acta Arith. **148** (2011), no. 2, 189–203. MR 2786163

[25] Stephen S. Gelbart, *Class field theory, the Langlands program, and its application to number theory*, Automorphic forms and the Langlands program, Adv. Lect. Math. (ALM), vol. 9, Int. Press, Somerville, MA, 2010, pp. 21–67. MR 2581947

[26] N. M. Glazunov, *On Langlands program, global fields and shtukas*, Chebyshevski˘i Sb. **21** (2020), no. 3, 68–83. MR 4196293

[27] David Grant, *A formula for the number of elliptic curves with exceptional primes*, Compositio Math. **122** (2000), no. 2, 151–164. MR 1775416

[28] R. Harron and A. Snowden, *Counting elliptic curves with prescribed torsion*, J. Reine Angew. Math. **729** (2017), 151–170. MR 3680373

[29] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR 0463157

[30] D. R. Heath-Brown, *The average analytic rank of elliptic curves*, Duke Math. J. **122** (2004), no. 3, 591–623. MR 2057019

[31] Roger A. Horn and Charles R. Johnson, *Matrix analysis*, second ed., Cambridge University Press, Cambridge, 2013. MR 2978290

[32] M. N. Huxley, *Exponential sums and lattice points. III*, Proc. London Math. Soc. (3) **87** (2003), no. 3, 591–609. MR 2005876

[33] Aleksandar Ivić, *The Riemann zeta-function*, Dover Publications, Inc., Mineola, NY, 2003, Theory and applications, Reprint of the 1985 original [Wiley, New York; MR0792089 (87d:11062)]. MR 1994094

[34] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), no. 1, 21–23. MR 510395

[35] ———, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), no. 2, 239–244. MR 588271

[36] ______, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), no. 1, 15–20. MR 549292

[37] ______, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), no. 3, 415–427. MR 616546

[38] ______, *On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class*, J. Number Theory **15** (1982), no. 2, 199–202. MR 675184

[39] Neal Koblitz, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR 1216136

[40] 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.

[41] R. P. Langlands, *Automorphic representations, Shimura varieties, and motives. Ein Märchen*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 205–246. MR 546619

[42] H.-Q. Liu, *On the distribution of squarefree numbers*, J. Number Theory **159** (2016), 202–222. MR 3412720

[43] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), With an appendix by Mazur and M. Rapoport. MR 488287

[44] ______, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230

[45] Grant Molnar and John Voight, *Counting elliptic curves over the rationals with a 7-isogeny*, 2022.

[46] Louis Joel Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

[47] A. P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 221–231. MR 0337974

[48] ———, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc. **81** (1975), 14–27. MR 354675

[49] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903. MR 3985613

[50] Tristan Phillips, *Most elliptic curves over global function fields are torsion free*, Acta Arith. **202** (2022), no. 1, 21–28. MR 4378553

[51] ———, *Rational points of bounded height on some genus zero modular curves over number fields*, 2022.

[52] ———, *Rational points of bounded height on some genus zero modular curves*, 2023.

[53] 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. MR 4071798

[54] H. Poincaré, *Sur les courbes tracées sur les surfaces algébriques*, Ann. Sci. École Norm. Sup. (3) **27** (1910), 55–108. MR 1509119

[55] 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. MR 4256691

[56] Bjorn Poonen, *Heuristics for the arithmetic of elliptic curves*, Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. II. Invited lectures, World Sci. Publ., Hackensack, NJ, 2018, pp. 399–414. MR 3966772

[57] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ -adic images of galois for elliptic curves over $\mathbb{Q}$ (and an appendix with john voight)*, Forum of Mathematics, Sigma **10** (2022), e62.

[58] Mathieu Roux, *Théorie de l'information, séries de Dirichlet, et analyse d'algorithmes*, 2011.

[59] Ruthi Hortsch, *Counting elliptic curves of bounded faltings height*, 2016.

[60] Joseph H. Silverman, *Heights and elliptic curves*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 253–265. MR 861979

[61] ______, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368

[62] ______, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[63] Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, second ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR 3363545

[64] Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory*, third ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015, Translated from the 2008 French edition by Patrick D. F. Ion. MR 3363366

[65] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. MR 294345

[66] Arnold Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Mathematische Forschungsberichte, XV, VEB Deutscher Verlag der Wissenschaften, Berlin, 1963. MR 0220685

[67] Mark Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), no. 1, 105–125. MR 2410120

[68] André Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315. MR 1555278

[69] David Vernon Widder, *The Laplace Transform*, Princeton Mathematical Series, vol. 6, Princeton University Press, Princeton, N. J., 1941. MR 0005923

[70] Matthew P. Young, *Low-lying zeros of families of elliptic curves*, J. Amer. Math. Soc. **19** (2006), no. 1, 205–250. MR 2169047