COUNTING 5-ISOGENIES OF ELLIPTIC CURVES OVER $\mathbb{Q}$

SANTIAGO ARANGO-PIÑEROS, CHANGHO HAN, OANA PADURARIU, AND SUN WOO PARK

ABSTRACT. We show that the number of 5-isogenies of elliptic curves defined over $\mathbb{Q}$ with naive height bounded by $H > 0$ is asymptotic to $C_5 \cdot H^{1/6}(\log H)^2$ for some explicitly computable constant $C_5 > 0$. This settles the asymptotic count of rational points on the genus zero modular curves $X_0(m)$. We leverage an explicit $\mathbb{Q}$-isomorphism between the stack $\mathcal{X}_0(5)$ and the generalized Fermat equation $x^2 + y^2 = z^4$ with $\mathbb{G}_m$ action of weights $(4, 4, 2)$.

CONTENTS

TODO LIST

1. INTRODUCTION

1.1. **Setup: arithmetic statistics of elliptic curves.** Let E be an elliptic curve defined over $\mathbb{Q}$. Then E is isomorphic to a unique elliptic curve $E_{A,B}$ with Weierstrass equation of the form

$$y^2 = x^3 + Ax + B,$$

where A, B are integers, the discriminant $\Delta(A, B) := -16(4A^3 + 27B^2)$ is nonzero, and no prime ℓ satisfies $\ell^4 \mid A$ and $\ell^6 \mid B$.

This work originated with discussions at a meeting of the AMS Mathematics Research Community *Explicit Computations with Stacks* supported by the NSF under Grant Number DMS 1916439.

Let $\mathcal{E}$ denote the set of such elliptic curves. The naive height of $E \cong E_{A,B} \in \mathcal{E}$ is defined by

$$\mathrm{Ht}(E) := \mathrm{Ht}(E_{A,B}) := \max(4|A|^3, 27|B|^2). \tag{1.1}$$

For $H \geq 1$, define

$$\mathcal{E}_{\leq H} := \{E \in \mathcal{E} : \mathrm{Ht}(E) \leq H\}. \tag{1.2}$$

Recent work has resolved many instances of counting problems for elliptic curves equipped with additional level structure as $H \to \infty$. For instance, Harron–Snowden [HS17] and Cullinan–Kenney–Voight [CKV22], building on work by Duke [Duk97] and Grant [Gra00], provided asymptotics for the count of $E \in \mathcal{E}_{\leq H}$ where the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ of the Mordell–Weil group is isomorphic to a given finite abelian group T, for each of the 15 groups T described in Mazur's theorem on torsion [Maz78, Theorem 2]. These cases correspond to genus zero modular curves with infinitely many rational points.

Parallel to these cases, a family of modular curves that has received much attention is the classical modular curves $Y_0(m)$. Rational points on these curves correspond to isomorphism classes of rational cyclic m-isogenies. Explicitly, such an object can be thought of as a pair (E, C) where E is an elliptic curve defined over $\mathbb{Q}$, and $C \subset E(\bar{\mathbb{Q}})$ is a cyclic subgroup of order m that is stable under the action of the absolute Galois group. Two such pairs (E, C) and (E', C') are said to be $\mathbb{Q}$-isomorphic, if there exists an isomorphism $\varphi\colon E \to E'$ of elliptic curves over $\mathbb{Q}$ such that $\varphi(C) = C'$. Let $\mathcal{E}_m := Y_0(m)(\mathbb{Q})$ denote the set of isomorphism classes $[E, C]$ of rational cyclic m-isogenies, and consider the finite subsets

$$\mathcal{E}_{m,\leq H} := \{[E, C] \in \mathcal{E}_m : \mathrm{Ht}(E) \leq H\}.$$

As a corollary of Mazur's *Isogeny Theorem* [Maz78, Theorem 1], it is known that $Y_0(m)$ has infinitely many rational points if and only if

$$m \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}. \tag{1.3}$$

These are precisely the levels m for which the completed curve $X_0(m)$ has genus zero.

1.2. **Results.** By recent work of several authors (see Table 1), the asymptotic order of growth of the counting function $N_m(H) := \#\mathcal{E}_{m,\leq H}$ was known for every m in this list, except for the stubborn level $m = 5$, which had eluded all previous attempts. Our main theorem provides the asymptotic count of 5-isogenies of elliptic curves.

Theorem 1.1. *There exist explicitly computable constants $C_5, C_5', C_5'' \in \mathbb{R}$ and $c_5 \in (0, 1)$ such that*

$$N_5(H) = C_5 H^{1/6} (\log H)^2 + C_5' H^{1/6} (\log H) + C_5'' H^{1/6} + O(H^{1/6} \cdot (\log H)^{-c_5}),$$

as $H \to \infty$. Furthermore, the constant C_5 is given by

$$C_5 = \frac{245}{108\pi\sqrt{3}} \cdot V_5 \cdot g_1, \tag{1.4}$$

where V_5 is the volume of the region $\sqrt[4]{\mathcal{R}_5} \subset \mathbb{R}^2$, described in Section 5.4, and g_1 is given by Equation (1.6).

Languasco and Moree [LM25] have numerically estimated the constant C_5 to twenty digists of precision, obtaining

$$C_5 \approx 0.01686810337983459695\ldots \tag{1.5}$$

The previous best known estimate was $N_5(H) \asymp H^{1/6}(\log H)^2$ by work of Bogges–Sankar [BS24, Proposition 5.14]. Our strategy was inspired by their idea of exploiting explicit presentations for the ring of modular forms of $\Gamma_0(5)$. In fact, we refine their estimate and show that Theorem 1.1 is essentially equivalent to to the following.

Theorem 1.2 (Theorem 3.2)**.** *Let $N_{\mathcal{G}}(H)$ denote the counting function of the integer triples (a, b, c) satisfying the following properties:*

- $a^2 + b^2 = c^4$,
- $\gcd(a, b)$ *is* 4^{th} *power free, and*
- $|c| \leq H$.

Then, there exist explicitly computable constants $g_1, g_2, g_3 \in \mathbb{R}$ such that for every $\varepsilon > 0$, we have

$$N_{\mathcal{G}}(H) = g_1 H(\log H)^2 + g_2 H(\log H) + g_3 H + O_\varepsilon(H^{1/2+\varepsilon}),$$

as $H \to \infty$. Furthermore, the constant g_1 is given by the Euler product

$$g_1 = \frac{48}{\pi^4} \prod_{p \equiv 1 \bmod 4} \Big(1 - \frac{4}{(p+1)^2}\Big). \tag{1.6}$$

Languasco an Moree [LM25] have numerically estimated the constant g_1 to extremely high precision, obtaining

$$g_1 \approx 0.41662592496198471660\ldots \tag{1.7}$$

Adding our main result to the list, we now know the classification of asymptotic counts of rational points for the genus zero modular curves $X_0(m)$.

Theorem 1.3. *Suppose that m is in the list (1.3). Then, there exist explicitly computable constants $C_m \in \mathbb{R}_{>0}$, $a_m \in \mathbb{Q}_{\geq 0}$, and $b_m \in \mathbb{Z}_{\geq 0}$ such that*

$$N_m(H) \sim C_m H^{a_m} (\log H)^{b_m}.$$

Moreover, the values of a_m and b_m are presented in Table 1.

Remark 1.4. Since some elliptic curves admit multiple non isomorphic cyclic m-isogenies, the problem of counting elliptic curves that *admit* an isogeny is related but distinct. In particular, [Mol24] denotes our counting function by $\widetilde{N}_m(H)$. For $m = 5$, a single elliptic curve E can admit at most two distinct $\mathbb{Q}$-rational 5-isogenies. See [CLR21].

For $m \neq 5$, the strategy was roughly the following. Use a rational parametrization $\mathbb{P}^1 \cong X_0(m)$ to find polynomial equations $A_m(t)$ and $B_m(t)$ for the Weierstrass coefficients of elliptic curves admitting a rational cyclic m-isogeny. Homogenize these polynomials to turn the estimation of $N_m(H)$ into a lattice point counting problem in the compact region

$$R_{m,\leq H} := \big\{(x, y) \in \mathbb{R}^2 : \max(4|A_m(x, y)|^3, 27B_m(x, y)^2) \leq H\big\},$$

and use the principle of Lipschitz and a careful sieve to conclude the results. This approach is sufficient when the expected power of $\log H$ in the main term of $N_m(H)$ is $b_m = 0$. This

TABLE 1. Powers of H and $\log H$ in the main terms in the asymptotic of the counting functions $N_m(H)$.

m	a_m	b_m	Reference
1	5/6	0	[Bru92, Lemma 4.3]
2	1/2	0	[Gra00, Proposition 1]
3	1/2	0	[PPV20, Theorem 1.3]
4	1/3	0	[PS21, Theorem 4.2]
5	1/6	2	Theorem 1.1
6	1/6	1	[Mol24, Theorem 7.3.14]
7	1/6	1	[MV23, Theorem 1.2.2]
8	1/6	1	[Mol24, Theorem 7.3.14]
9	1/6	1	[Mol24, Theorem 7.3.14]
10	1/6	0	[Mol24, Theorem 5.4.11]
12	1/6	1	[Mol24, Theorem 7.3.18]
13	1/6	0	[Mol24, Theorem 6.4.5]
16	1/6	1	[Mol24, Theorem 7.3.18]
18	1/6	1	[Mol24, Theorem 7.3.18]
25	1/6	0	[Mol24, Theorem 5.4.11]

is not surprising, since the main term predicted by the principle of Lipschitz is the area of the region $R_{m,\leq H}$, which is $\asymp H^a$.

Remarkably, Molnar–Voight [MV23] where able to salvage this approach to show that

$$N_7(H) \sim C_7 H^{1/6}(\log H).$$

They observed that counting 7-isogenies up to $\bar{\mathbb{Q}}$-isomorphism has the effect of removing the $\log H$ factor, which allowed them to use Lipschitz for this *rigidified* count, and then recover the full count by precisely estimating the number of twists with a given height (see [MV23, Theorem 5.1.4]).

Unfortunately, this rigidification method is not enough to count 5-isogenies essentially because we can only remove one factor of $\log H$. Nevertheless, we use their rigidification method to simplify the calculations. For a detailed discussion of why this method fails for $m = 5$, see Remark 1.3.2 and Remark 5.3.53 in Molnar's Ph.D. thesis [Mol24].

1.3. **Sketch of the proof.** Our approach does not use a rational parametrization of $X_0(5)$. Instead, we leverage an explicit embedding of the moduli stack $\mathcal{X}_0(5)$ in weighted projective space. This allows us to parametrize 5-isogenies in terms of (4,4,2)-minimal[1] integral solutions to the generalized Fermat equation $x^2 + y^2 = z^4$.

Remark 1.5 (Ignoring stacks). Keeping stacks in the back of one's mind is enlightening but not crucial for reading this article. If the reader wishes to understand our proof while ignoring stacks completely, they can safely skip Section 2.

[1]An integer triple (a, b, c) is (4,4,2)-minimal, if there is no prime ℓ satisfying $\ell^4 \mid a$, $\ell^4 \mid b$, and $\ell^2 \mid c$.

Remark 1.6 (Embracing stacks). The stacky perspective offers a conceptual framework ideally suited to studying counting problems of this nature. The ideas presented in Section 2 are applicable in other contexts and might provide some insight into the Batyrev–Manin–Malle conjectures for rational points on stacks as in [ESZB23],[DY22], [LS24].

We break the proof into four steps and dedicate one section to each one.

(1) In Section 2, we study the geometry of the moduli stack $\mathcal{X}_0(5)$ (defined over $\mathbb{Q}$) with coarse space $X_0(5)$. We show that $\mathcal{X}_0(5)$ is $\mathbb{Q}$-isomorphic to the closed substack of the weighted projective stack $\mathcal{P}(4,4,2)$ with equation $x^2+y^2=z^4$. The key result of this section towards the proof of our main theorem is the parametrization of 5-isogenies (Lemma 5.1).
(2) In Section 3, we count $(4,4,2)$-minimal Gaussian integers with bounded norm.
(3) In Section 4, we prove the *Main analytic lemma* (Lemma 4.2). This enables us to count integral ideals in the Gaussian integers with numerical norm inside a homogeneously expanding region Ω, as long as Ω is similar enough to a square. This section is independent from the rest of the paper.
(4) In Section 5 we feed our parametrization of 5-isogenies and the count of $(4,4,2)$-minimal Gaussian integers of bounded norm into the *Main analytic lemma*, completing the proof of Theorem 1.1.

Acknowledgements. We thank John Voight, David Zureick-Brown, and Jordan Ellenberg for helpful conversations about this project. We thank Robert Lemke Oliver for suggesting the approach presented in Section 4. We thank Alessandro Languasco and Pieter Moree for their insightful comments on an earlier draft, and for sharing their computations with us. O.P. and S.W.P are very grateful to the Max-Planck-Institut für Mathematik Bonn for their hospitality and financial support.

2. Embedding $\mathcal{X}_0(5)$ into $\mathcal{P}(4,4,2)$

We work in the level of generality required for our applications. In particular, the geometric objects in this section are defined over $\mathbb{Q}$.

2.1. **The stacky proj construction.** We recall the stacky proj construction [Ols16, Example 10.2.8], specializing to the case where the base scheme is $\operatorname{Spec}\mathbb{Q}$. Given a graded $\mathbb{Q}$-algebra $R=\bigoplus_{d\geq 0}R_d$, the multiplicative group $\mathbb{G}_m$ acts on $\operatorname{Spec}R$. The action is determined by the grading, and it fixes the point $0:=V(R_+)$ corresponding to the irrelevant ideal $R_+:=\bigoplus_{d>0}R_d$. Define the stacky proj of R to be the quotient stack

$$\mathbf{Proj}\,R:=[(\operatorname{Spec}R-0)/\mathbb{G}_m].$$

The stack $\mathbf{Proj}\,R$ admits a coarse space, namely the scheme $\operatorname{Proj}R$. Moreover, if R is generated in degree one, then $\mathbf{Proj}\,R=\operatorname{Proj}R$.

Example 2.1 (The moduli space of elliptic curves)**.** Consider the graded algebra $\mathbb{Q}[u^4\mathsf{x},u^6\mathsf{y}]$, where the grading is determined by the dummy variable u. By definition, the weighted projective line $\mathcal{P}(4,6)$ is $\mathbf{Proj}\,\mathbb{Q}[u^4\mathsf{x},u^6\mathsf{y}]$. Using Weierstrass equations, one can show that $\mathcal{P}(4,6)$ is isomorphic to the moduli stack $\mathcal{X}(1)$ of stable elliptic curves over $\mathbb{Q}$. In particular, the groupoid of rational points $\mathcal{X}(1)(\mathbb{Q})$ is equivalent to the groupoid $\mathcal{P}(4,6)(\mathbb{Q})$ with

- **Objects:** pairs $(A,B)\in\mathbb{Q}\times\mathbb{Q}-(0,0)$.

- **Isomorphisms:** elements $\lambda \in \mathbb{Q}^\times$, sending $(A, B) \mapsto (\lambda^6 A, \lambda^4 B)$.

Example 2.2. Consider the graded algebra $R := \mathbb{Q}[u^4\mathsf{x}, u^4\mathsf{y}, u^2\mathsf{z}]/(u^8(\mathsf{x}^2 + \mathsf{y}^2 - \mathsf{z}^4))$, and let $\mathcal{G} := \mathbf{Proj}\, R$. The quotient map $\mathbb{Q}[u^4\mathsf{x}, u^4\mathsf{y}, u^2\mathsf{z}] \to R$ induces a closed embedding $\mathcal{G} \hookrightarrow \mathcal{P}(4, 4, 2)$. We will show that $\mathcal{G}$ is isomorphic to the moduli space $\mathcal{X}_0(5)$ of generalized elliptic curves together with 5-isogenies. In particular, the groupoid of rational points $\mathcal{X}_0(5)(\mathbb{Q})$ is equivalent to the groupoid $\mathcal{G}(\mathbb{Q})$ with

- **Objects:** triples $(a, b, c) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} - (0, 0, 0)$ satisfying $a^2 + b^2 = c^4$.
- **Isomorphisms:** elements $\lambda \in \mathbb{Q}^\times$, sending $(a, b, c) \mapsto (\lambda^4 a, \lambda^4 b, \lambda^2 c)$.

We now explain special properties of $\operatorname{Proj} R$ that are mentioned in [AH11, Section 2]. When the graded $\mathbb{Q}$-algebra R satisfies $R_0 = \mathbb{Q}$, the stack $\mathbf{Proj}\, R$ is special, as the stabilizers of any point of $\mathbf{Proj}\, R$ is a finite subgroup of $\mathbb{G}_m$. If in addition R is a finitely generated graded $\mathbb{Q}$-algebra, then $\mathbf{Proj}\, R$ is a special example of a cyclotomic stack (see [AH11, Definition 2.3.1]). Just like $\mathbf{Proj}\, R$, any cyclotomic stack $\mathcal{X}$ has a coarse moduli space X. Note that both $\mathcal{X}(1)$ and $\mathcal{G}$ from Example 2.1 and Example 2.2 are cyclotomic stacks.

Recall that if the graded $\mathbb{Q}$-algebra R is finitely generated by elements of R_1 and $R_0 = \mathbb{Q}$, then there is a closed immersion $\operatorname{Proj} R \hookrightarrow \mathbb{P}R_1 := \operatorname{Proj} \operatorname{Sym} R_1$. In this case, the line bundle $\mathcal{O}_{\operatorname{Proj} R}(1) = \mathcal{O}_{\mathbb{P}R_1}(1)|_{\operatorname{Proj} R}$ can be recovered from the graded R-module $R(1)$. Similarly, if $R_0 = \mathbb{Q}$ but R is not necessarily generated by R_1, then $\mathbf{Proj}\, R$ is equipped with a line bundle $\mathcal{O}_{\mathbf{Proj}\, R}(1)$; the pullback of $\mathcal{O}_{\mathbf{Proj}\, R}(1)$ via $\operatorname{Spec} R - 0 \to \mathbf{Proj}\, R$ is the $\widetilde{R(1)}|_{\operatorname{Spec} R - 0}$, where $\widetilde{R(1)}$ is the sheaf associated to the graded R-module $R(1)$. Note that $\mathbb{G}_m$ acts faithfully on the line bundle $\widetilde{R(1)}|_{\operatorname{Spec} R - 0}$ over the $\mathbb{G}_m$-variety $\operatorname{Spec} R - 0$. So the stabilizer groups of any point of $\mathbf{Proj}\, R$ act faithfully on the corresponding fiber of $\mathcal{O}_{\mathbf{Proj}\, R}(1)$; such a line bundle is called a uniformizing line bundle (see [AH11, Definition 2.3.11]).

Just as $\mathcal{O}_{\operatorname{Proj} R}(1)$ is an ample line bundle on $\operatorname{Proj} R$, $\mathcal{O}_{\mathbf{Proj}\, R}(1)$ is more than just a uniformizing line bundle.

Definition 2.3 ([AH11, Definition 2.4.1])**.** Suppose that $\mathcal{X}$ is a proper cyclotomic $\mathbb{Q}$-stack with coarse moduli space X. Denote $c\colon \mathcal{X} \to X$ the coarse map. Then a uniformizing line bundle $\mathcal{L}$ on $\mathcal{X}$ is called a polarizing line bundle if there exists an ample line bundle M on X and a positive integer e such that $\mathcal{L}^e \cong c^* M$.

We claim that if R is a finitely generated graded $\mathbb{Q}$-algebra such that $R_0 = \mathbb{Q}$ and $R_{1,m} := \oplus_{1 \le d \le m} R_d$ generates R, then the uniformizing line bundle $\mathcal{O}_{\mathbf{Proj}\, R}(1)$ is a polarizing line bundle; this claim immediately implies that $\mathcal{O}_{\mathcal{X}(1)}(1)$ and $\mathcal{O}_{\mathcal{G}}(1)$ are polarizing line bundles on $\mathcal{X}(1)$ and $\mathcal{G}$ respectively. To see this, recall that $\operatorname{Proj} R$ is a closed subscheme of a weighted projective space $\mathbb{P}R_{1,m} := \operatorname{Proj} R'$, where R' is a free graded $\mathbb{Q}$-algebra generated by the graded $\mathbb{Q}$-vector space $R_{1,m}$; note that R is a graded quotient of R'. Then, there exists a positive integer e such that $\mathcal{O}_{\mathbf{Proj}\, R}(e) \cong c^*(\mathcal{O}_{\mathbb{P}R_{1,m}}(e)|_{\operatorname{Proj} R})$; here, e is not necessarily equal to 1 as $\mathcal{O}_{\mathbb{P}R_{1,m}}(k)$ may not be locally free for some values of k.

2.2. **Rigidification.** Recall the notion of rigidification, as presented for instance in [AGV08, Appendix C]. When $\mathcal{X} = \mathbf{Proj}\, R$, the rigidification construction is very explicit. Indeed, let d be the greatest common divisor of the degrees of the generators of R, so that $R = \bigoplus_{n \ge 0} R_{nd}$. Note that $\mu_d := \operatorname{Spec} \mathbb{Q}[t]/(t^d - 1) \subset \mathbb{G}_m$ acts trivially on $\operatorname{Spec} R$. Consider the graded ring $S := \bigoplus_{n \ge 0} S_n$ defined by $S_n := R_{nd}$. We have a homomorphism $S \to R$ which is the identity

at the level of rings, but multiplies the degree of every homogeneous element of S by d. Then, the corresponding morphism of stacks $\mathbf{Proj}\, R \to \mathbf{Proj}\, S$ is a μ_d-gerbe, and $\mathcal{X}/\!\!/\mu_d = \mathbf{Proj}\, S$ is the *rigidification* of $\mathcal{X}$ by μ_d-inertia. In this case, the pullback of $\mathcal{O}_{\mathbf{Proj}\, S}(1)$ under the rigidification $\mathbf{Proj}\, R \to \mathbf{Proj}\, S$ is $\mathcal{O}_{\mathbf{Proj}\, R}(d)$.

Example 2.4 (The rigidified moduli space of elliptic curves)**.** The rigidification $\mathcal{Z}(1) := \mathcal{X}(1)/\!\!/\mu_2$ is isomorphic to $\mathcal{P}(2,3)$. In particular, the groupoid of rational points $\mathcal{Z}(1)(\mathbb{Q})$ is equivalent to the groupoid $\mathcal{P}(2,3)(\mathbb{Q})$ with

- **Objects:** pairs $(A, B) \in \mathbb{Q} \times \mathbb{Q} - (0,0)$.
- **Isomorphisms:** elements $\lambda \in \mathbb{Q}^\times$, sending $(A, B) \mapsto (\lambda^2 A, \lambda^3 B)$.

Example 2.5. The rigidification of the graded $\mathbb{Q}$-algebra R from Example 2.2 is $S := \mathbb{Q}[u^2\mathsf{x}, u^2\mathsf{y}, u\mathsf{z}]/(u^4(\mathsf{x}^2 + \mathsf{y}^2 - \mathsf{z}^4))$. Let $\mathcal{F} := \mathbf{Proj}\, S$. Then $\mathcal{G} \to \mathcal{F}$ is a μ_2-gerbe, and $\mathcal{F}$ is the rigidification of $\mathcal{G}$. We will show that $\mathcal{F}$ is isomorphic to $\mathcal{Z}_0(5) := \mathcal{X}_0(5)/\!\!/\mu_2$. In particular, the groupoid of rational points $\mathcal{Z}_0(5)(\mathbb{Q})$ is equivalent to the groupoid $\mathcal{F}(\mathbb{Q})$ with

- **Objects:** triples $(a, b, c) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} - (0,0,0)$ satisfying $a^2 + b^2 = c^4$.
- **Isomorphisms:** elements $\lambda \in \mathbb{Q}^\times$, sending $(a, b, c) \mapsto (\lambda^2 a, \lambda^2 b, \lambda c)$.

2.3. **Section rings of stacky curves.** A stacky curve is a smooth proper geometrically connected Deligne–Mumford stack, defined over a field, that contains a dense open subscheme (see [VZB22, Chapter 5]). Let $\mathcal{X}$ be a stacky curve over $\mathbb{Q}$, and let $\mathcal{L}$ be a line bundle on $\mathcal{X}$. The homogeneous coordinate ring relative to $\mathcal{L}$ is the graded ring

$$R_{\mathcal{L}} := \bigoplus_{d \geq 0} H^0(\mathcal{X}, \mathcal{L}^{\otimes d}). \tag{2.1}$$

The degree d piece of $R_{\mathcal{L}}$ is $R_{\mathcal{L},d} := H^0(\mathcal{X}, \mathcal{L}^{\otimes d})$. When $\mathcal{L} \cong \mathcal{O}_{\mathcal{X}}(-D)$ where D is a Cartier divisor, then we call $R_D := R_{\mathcal{L}}$.

Example 2.6. Recall from Example 2.1 that $\mathcal{X}(1) \cong \mathbf{Proj}\, \mathbb{Q}[u^4\mathsf{x}, u^6\mathsf{y}]$. In fact, this isomorphism identifies the polarizing line bundle $\mathcal{O}_{\mathcal{X}}(1)$ with the Hodge bundle λ on $\mathcal{X}(1)$, so that $\mathcal{X}(1) \cong R_\lambda$. Note that $R_\lambda = \mathbb{Q}[E_4, E_6]$ is the ring of modular forms on the modular curve $\mathcal{X}(1)$ (with $\mathbb{Q}$-coefficients), where E_4 and E_6 are the Eisenstein series with constant term 1 in their q-series expansion. Thus, $u^4\mathsf{x}$ is identified with E_4 and $u^6\mathsf{y}$ is identified with E_6 via the isomorphism $R_{\mathcal{O}_{\mathcal{X}(1)}(1)} \cong R_\lambda$.

If $\mathcal{L}$ is a polarizing line bundle on a cyclotomic stacky curve $\mathcal{X}$, then $\mathcal{X}$ can be recovered from $R_{\mathcal{L}}$ by the following slight extension of [AH11, Corollary 2.4.4].

Lemma 2.7. *Suppose that $\mathcal{X}$ is a proper geometrically connected cyclotomic $\mathbb{Q}$-stack with a polarizing line bundle $\mathcal{L}$. Then*

$$\mathcal{X} \cong \mathbf{Proj}\, R_{\mathcal{L}}.$$

Proof. By the proof of [AH11, Proposition 2.3.10], $\mathcal{X} \cong [P_{\mathcal{L}}/\mathbb{G}_m]$, where the $\mathbb{G}_m$-torsor $P_{\mathcal{L}} := \mathcal{X} \times_{B\mathbb{G}_m} \operatorname{Spec} \mathbb{Q}$ on $\mathcal{X}$ is defined by the classifying morphism $\mathcal{X} \to B\mathbb{G}_m$ associated with $\mathcal{L}$. The proof of [AH11, Corollary 2.4.4] implies that $P_{\mathcal{L}}$ is an open subscheme of $\operatorname{Spec} R_{\mathcal{L}}$, so it suffices to show that $P_{\mathcal{L}} \cong \operatorname{Spec} R_{\mathcal{L}} - V(R_{\mathcal{L},+})$ by the definition of $\mathbf{Proj}\, R_{\mathcal{L}}$.

Denote $c\colon \mathcal{X} \to X$ the coarse map. Since $\mathcal{L}$ is a polarizing line bundle, there exists $e \in \mathbb{Z}_+$ and an ample line bundle M on X such that $\mathcal{L}^e \cong c^*M$. Connectedness of $\mathcal{X}$ implies that $R_{\mathcal{L},0} = \mathbb{Q} = R_{M,0}$. Then $X \cong [P_M/\mathbb{G}_m]$ is a projective scheme with an ample line bundle M,

so that $P_M \cong \operatorname{Spec} R_M - V(R_{M,+})$. By the proof of [AH11, Corollary 2.4.4] again, $\operatorname{Spec} R_{\mathcal{L}}$ is isomorphic to the relative normalization of $\operatorname{Spec} R_M$ in $P_{\mathcal{L}}$ via a morphism $P_{\mathcal{L}} \to \operatorname{Spec} R_M$ factoring through P_M. As the induced morphism $P_{\mathcal{L}} \to P_M$ is a finite surjection by loc. cit., the induced inclusion $P_{\mathcal{L}} \hookrightarrow \operatorname{Spec} R_{\mathcal{L}}$ identifies $P_{\mathcal{L}}$ with $\operatorname{Spec} R_{\mathcal{L}} - V(R_{\mathcal{L},+})$, proving the desired assertion. □

For the remainder of this subsection, we apply Lemma 2.7 to describe a modular curve $\mathcal{X}_0(5)$ as a stacky Proj. Let the $\mathbb{Q}$-stack $\mathcal{X}_0(5)$ be the modular curve parameterizing generalized elliptic curves over $\mathbb{Q}$ with $\Gamma_0(5)$-structure, as in [Č17]. By [DR73, IV.6.7], the proper DM stack $\mathcal{X}_0(5)$ is smooth stacky curve, and it admits a projection $J\colon \mathcal{X}_0(5) \to \mathcal{X}(1)$ which forgets the $\Gamma_0(5)$-structure on generalized elliptic curves. Using J, we identify $\mathcal{X}_0(5)$ with the stack $\mathcal{G}$ from Example 2.2.

Lemma 2.8. *The stacks $\mathcal{X}_0(5)$ and $\mathcal{G}$ are isomorphic. Consequently, so are their rigidifications $\mathcal{Z}_0(5)$ and $\mathcal{F}$.*

Proof. Recall from Example 2.6 that $\mathcal{X}(1) \cong R_\lambda$, where λ is the Hodge bundle on $\mathcal{X}(1)$ and R_λ is the ring of modular forms on $\mathcal{X}(1)$. As λ is a polarizing line bundle on $\mathcal{X}(1)$ and $J\colon \mathcal{X}_0(5) \to \mathcal{X}(1)$ is a finite surjection, $\mathcal{X}_0(5)$ is a geometrically connected proper cyclotomic stack equipped with a polarizing line bundle $J^*\lambda$. Thus, $\mathcal{X}_0(5) \cong \mathbf{Proj}\, R_{J^*\lambda}$ by Lemma 2.7, and $R_{J^*\lambda}$ is the ring of modular forms on the modular curve $\mathcal{X}_0(5)$. The computations in the file `X0(5)-abc-parametrization.m` verify that the ring of modular forms $R_{J^*\lambda}$ is isomorphic, as graded $\mathbb{Q}$-algebras, to the ring R from Example 2.2. As $\mathcal{G} \cong \mathbf{Proj}\, R$, we see that $\mathcal{X}_0(5)$ and $\mathcal{G}$ are isomorphic. □

2.4. **Geometric interpretation of the counting problem.** For the original counting problem (Theorem 1.1), the height function comes from pulling back the 12^{th}-power of the Hodge bundle on $\mathcal{X}(1)$ to $\mathcal{X}_0(5)$ via the J-forgetful morphism. For the second counting problem (Theorem 1.2), the height commes from pulling back the line bundle $\mathcal{O}_{\mathcal{P}(4,4,2)}(1)$ via the embedding ι.

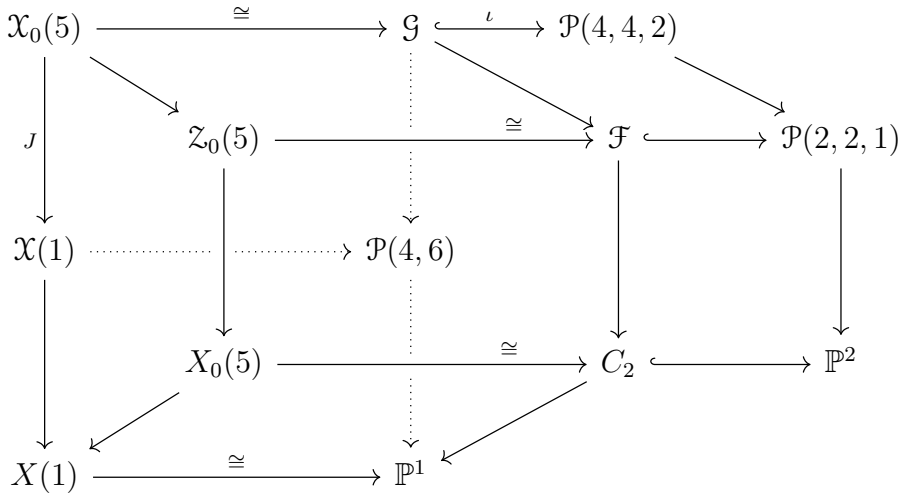


FIGURE 1. This diagram summarizes the stacks considered in this paper and their respective coarse spaces. C_2 is the plane curve $\mathsf{x}^2 + \mathsf{y}^2 = \mathsf{z}^2$.

We use the isomorphism $\mathcal{X}_0(5) \cong \mathcal{G}$ to compare both height functions on the same ambient space. It is necessary to scale these heights appropriately to compare them; concretely this is a matter of making sure that the polynomials describing the sections of these line bundles have the same degree. This allows us to translate our counting problem into a concrete lattice point count problem inside two regions. The region coming from the naive height on elliptic curves is complicated, but the region coming from $\mathcal{P}(4,4,2)$ is just the unit disc.

3. Counting minimal integer solutions to $x^2 + y^2 = z^4$

Recall that we say an integer triple (a,b,c) is (4,4,2)-minimal if no prime ℓ satisfies $\ell^4 \mid a$, $\ell^4 \mid b$, and $\ell^2 \mid c$; equivalently, if the $(4,4,2)$-weighted greatest common divisor of (a,b,c) is one (see [BGS20]). Since we are concerned only with the generalized Fermat equation of signature $(2,2,4)$, we will say that a triple of integers (a,b,c) is a Fermat triple if it satisfies the equation $x^2 + y^2 = z^4$.

Definition 3.1. We will say that a triple of integers (a,b,c) is a minimal Fermat triple if the following conditions are satisfied:

- $a^2 + b^2 = c^4$,
- (a,b,c) is $(4,4,2)$-minimal, and
- $c \neq 0$.

The third condition is clearly redundant. We leave it to emphasize that c can be positive or negative. We let $\mathcal{G}\langle\mathbb{Q}\rangle$ denote the set of minimal Fermat triples, and we consider the counting function

$$N_{\mathcal{G}}(H) := \#\{(a,b,c) \in \mathcal{G}\langle\mathbb{Q}\rangle : |c| \leq H\}. \tag{3.1}$$

From Lemma 5.1, we see that this eccentric counting problem is intimately related to counting 5-isogenies. In this section, we will prove the following theorem.

Theorem 3.2. *There exist explicitly computable constants $g_1, g_2, g_3 \in \mathbb{R}$ such that for every $\varepsilon > 0$, we have*

$$N_{\mathcal{G}}(H) = g_1 H (\log H)^2 + g_2 H (\log H) + g_3 H + O_\varepsilon(H^{1/2+\varepsilon}),$$

as $H \to \infty$. Furthermore, the constant g_1 is given by

$$g_1 = \frac{48}{\pi^4} \prod_{p \equiv 1 \bmod 4} \Big(1 - \frac{4}{(p+1)^2}\Big).$$

3.1. The rigidified count.

Observe that given a minimal Fermat triple (a,b,c) and a square free integer e, the twist (e^2a, e^2b, ec) is another minimal Fermat triple. By factoring out the $(2,2,1)$-greatest common divisor of (a,b,c), and twisting by -1 when $c < 0$, we arrive at a unique smallest twist.

Definition 3.3. An integer triple (a,b,c) is a twist minimal Fermat triple if the following conditions are satisfied:

- $a^2 + b^2 = c^4$,
- (a,b,c) is $(2,2,1)$-minimal, and
- $c > 0$.

Let $\mathcal{F}\langle\mathbb{Q}\rangle$ be the set of twist minimal Fermat triples, and consider the following counting function

$$N_{\mathcal{F}}(H) := \#\{(a,b,c) \in \mathcal{F}\langle\mathbb{Q}\rangle : c \leq H\}. \tag{3.2}$$

To prove Theorem 3.2, we first obtain the asymptotics of $N_{\mathcal{F}}(H)$ and then estimate the number of twists of a given height to recover the asymptotics of $N_{\mathcal{G}}(H)$.

Theorem 3.4. *There exist explicitly computable constants $f_1, f_2 \in \mathbb{R}$ such that for every $\varepsilon > 0$, we have*

$$N_{\mathcal{F}}(H) = f_1 H(\log H) + f_2 H + O_\varepsilon(H^{1/2+\epsilon}),$$

as $H \to \infty$. Furthermore, the constant f_1 is given by

$$f_1 = \frac{\pi^2}{12} g_1 = \frac{4}{\pi^2} \prod_{p \equiv 1 \bmod 4} \left(1 - \frac{4}{(p+1)^2}\right).$$

We start by recording some elementary observations about twist minimal Fermat triples that will be needed in the proof of this theorem. These follow immediately from the definitions, and Fermat's theorem on numbers representable as the sum of two squares.

Lemma 3.5 (Characterization of twist minimal triples)**.** *Suppose that (a,b,c) is a twist minimal Fermat triple. Then, the following are true.*

(a) $\gcd(a,b)$ *is square free.*
(b) If $p \mid \gcd(a,b)$*, then* $p \mid c$*.*
(c) If $p \mid c$*, then* $p \equiv 1 \bmod 4$*.*
(d) $c \equiv 1 \bmod 4$*.*
(e) a *and* b *have distinct parities.*
(f) If $a = 0$*, then* $b^2 = c^2 = 1$*.*
(g) If $b = 0$*, then* $a^2 = c^2 = 1$*.*

Define the height zeta function corresponding to $N_{\mathcal{F}}(H)$ to be the Dirichlet series

$$F(s) := \sum_{c=1}^{\infty} \frac{f(c)}{c^s}, \tag{3.3}$$

where $f(c)$ is the arithmetic height function that counts the number of twist minimal triples (a',b',c') with $c' = c$. The following lemma describes the function $f(c)$ in terms of the prime factorization of c.

Lemma 3.6. *The arithmetic height function $f(c)$ satisfies the following properties.*

(1) For a prime $\ell \not\equiv 1 \bmod 4$, we have $f(\ell^r) = 0$ for every positive integer r.
(2) For a prime $p \equiv 1 \bmod 4$, we have $f(p^r) = 16$ for every positive integer r.
(3) The arithmetic function $f(c)/4$ is multiplicative.

Proof. Let $\mathcal{F}_c$ denote the set of integral ideals $\mathfrak{a} = (\alpha)$ in $\mathbb{Z}[i]$ such that α gives rise to a twist minimal Fermat triple $(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha), c)$.

(1) From Lemma 3.5, we know that $\mathcal{F}_\ell = \emptyset$ when $\ell \not\equiv 1 \bmod 4$.
(2) For such a prime p, write $p\mathbb{Z}[i] = \mathfrak{p}\bar{\mathfrak{p}}$ for the prime ideal factorization. From Lemma 3.5, we deduce that

$$\mathcal{F}_{p^r} = \left\{\mathfrak{p}^{4r}, \bar{\mathfrak{p}}^{4r}, p \cdot \mathfrak{p}^{4r-2}, p \cdot \bar{\mathfrak{p}}^{4r-2}\right\}.$$

It follows that $f(p^r) = 4(\#\mathcal{F}_{p^r}) = 16$ for every $r \geq 1$.

(3) Indeed, $f(c)/4$ counts the number of twist minimal integral ideals. It is straightforward to see that twist minimality is a multiplicative condition for relatively prime ideals. The result follows from the multiplicativity of the ideal norm.

□

Proof of Theorem 3.4. Recall the Dirichlet L-function of the Gaussian field $\mathbb{Q}(i)$, given by

$$L(s) = \prod_{p \equiv 1 \bmod 4} (1 - p^{-s})^{-1} \prod_{q \equiv 3 \bmod 4} (1 + q^{-s})^{-1} = \prod_{p} (1 - \chi_{-4}(p) p^{-s})^{-1},$$

where χ_{-4} denotes the quadratic Dirichlet character modulo 4. Comparison of local Euler factors on either side shows that

$$F(s) = 4 \prod_{p \equiv 1 \bmod 4} \left(\frac{1 + 3p^{-s}}{1 - p^{-s}} \right) = \Big(\frac{2\zeta(s)L(s)}{(1 + 2^{-s})\zeta(2s)} \Big)^2 \prod_{p \equiv 1 \bmod 4} \frac{(1 + 3p^{-s})(1 - p^{-s})}{(1 + p^{-s})^2},$$

where the Euler product converges for $\mathrm{Re}(s) > 1/2$. We deduce the identity

$$F(s) = \zeta(s)^2 P(s), \tag{3.4}$$

where

$$P(s) = \Big(\frac{2L(s)}{(1 + 2^{-s})\zeta(2s)} \Big)^2 \prod_{p \equiv 1 \bmod 4} \frac{(1 + 3p^{-s})(1 - p^{-s})}{(1 + p^{-s})^2} \tag{3.5}$$

converges for $\mathrm{Re}(s) > 1/2$. From 3.4, we see that $F(s)$ has a unique pole at $s = 1$ of order 2, and admits a meromorphic continuation to the half-plane $\mathrm{Re}(s) > 1/2$. The convexity bound for $\zeta(s)^2$ allows us to apply a standard Tauberian theorem (see [CLT01, Théoréme A.1]) to conclude the result. Recalling $L(1) = \pi/4$ and $\zeta(2) = \pi^2/6$, we have $2L(1)/\zeta(2) = 3/\pi$ and hence

$$f_1 = \lim_{s \to 1} (s - 1)^2 F(s) = P(1) = \frac{4}{\pi^2} \prod_{p \equiv 1 \bmod 4} \Big(1 - \frac{4}{(p + 1)^2} \Big).$$

□

Languasco and Moree [LM25] have obtained a precise numerical approximation of f_1 proceding as in Cohen [Coh07, §10.3.6]. They calculated

$$f_1 = 0.342661088551060769496383029936083719053524074825571911660307102 9\ldots \tag{3.6}$$

3.2. **Proof of Theorem 3.2.** As before, we aim to understand the analytic properties of the height zeta function corresponding to $N_{\mathcal{G}}(H)$, that is

$$G(s) := \sum_{n=1}^{\infty} \frac{g(n)}{n^s},$$

where $g(n)$ is the arithmetic height function that counts the number of minimal Fermat triples (a, b, c) with $|c| = n$.

Instead of directly analyzing the zeta function $G(s)$, we follow the strategy employed in [MV23, Theorem 5.1.4] to leverage our understanding of the rigidified zeta function $F(s)$.

Theorem 3.7. *The following statements hold.*

(i) $g(n) = 4(\mu^2 \star f)(n)$, *where* $\mu(n)$ *is the Möbius function and* $\star$ *denotes convolution.*

(ii) $G(s) = 4\frac{\zeta(s)}{\zeta(2s)}F(s)$ *in the half-plane* $\mathrm{Re}(s) > 1$.

(iii) The function $G(s)$ *admits meromorphic continuation to the half-plane* $\mathrm{Re}(s) > 1/2$ *with a triple pole at* $s = 1$ *and no other singularities.*

Proof. For every square free $e \in \mathbb{Z}$, let

$$g^{(e)}(n) := \#\big\{(a,b,c) \in \mathbb{Z}^3 : (e^2a, e^2b, ec) \in \mathcal{G}\langle\mathbb{Q}\rangle \text{ and } |ec| = n\big\}.$$

It follows from the definitions that

$$g^{(e)}(n) = \begin{cases} 2f(n/|e|), & \text{if } e \mid n, \\ 0, & \text{if } e \nmid n. \end{cases} \tag{3.7}$$

Therefore,

$$g(n) = \sum_{\substack{e\in\mathbb{Z} \\ \square \text{ free}}} g^{(e)}(n) = 4\sum_{\substack{e>0 \\ e|n}} \mu^2(e) f(n/e) = 4(\mu^2 \star f)(n),$$

completing the proof of Item (i). Item (ii) follows directly form Item (i), and Item (iii) follows from the identity $F(s) = \zeta(s)^2 P(s)$ and the proof of Theorem 3.4. □

Proof of Theorem 3.2. From the identity $G(s) = 4\zeta(s)F(s)/\zeta(2s) = 4\zeta^3(s)P(s)/\zeta(2s)$, we can apply Tauberian theorem once more to conclude the result. We have that the constant term is

$$\begin{aligned} g_1 &= \tfrac{1}{2}\lim_{s\to 1}(s-1)^3 G(s) \\ &= 2\lim_{s\to 1}(s-1)^3\zeta(s)^3 P(s)/\zeta(2s) = 2P(1)/\zeta(2) = 12P(1)/\pi^2. \end{aligned}$$

□

3.3. **The ideal theoretic point of view.** We end this section by shifting our perspective from integral triples to ideals in $\mathbb{Z}[i]$. This is natural since Fermat triples are invariant under multiplication by i. That is, if (a,b,c) is a (twist minimal) Fermat triple, then so are $(\pm a, \pm b, c)$ and $(\pm b, \pm a, c)$. The exposition becomes clearer if we normalize by this symmetry.

Let $\mathcal{O} := \mathbb{Z}[i]$ denote the ring of Gaussian integers, with fraction field $K := \mathbb{Q}(i)$. Let $\mathcal{I}$ denote the multiplicative monoid of (nonzero) integral ideals in $\mathcal{O}$. For every $\mathfrak{a} = (\alpha) \in \mathcal{I}$, we denote by $N\mathfrak{a} := \#\mathcal{O}/\mathfrak{a} = \alpha\bar{\alpha}$ its norm. If $p \equiv 1 \bmod 4$ is a prime, we let $p\mathcal{O} = \mathfrak{p}\bar{\mathfrak{p}}$ denote the primes above. Similarly, if $q \equiv 3 \bmod 4$ is prime, we let $q\mathcal{O} = \mathfrak{q}$ denote the prime above it in $\mathcal{O}$.

Say that an ideal $\mathfrak{a} \in \mathcal{I}$ is (twist) minimal if any generator α gives rise to a (twist) minimal Fermat triple $(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha), c)$, for some value of $c = (N\mathfrak{a})^{1/4}$. Denote by $\phi, \psi \colon \mathcal{I} \to \{0,1\}$ the characteristic functions of the property of being minimal, and twist minimal, respectively. Consider the corresponding Dirichlet series:

$$L(\phi, s) := \sum_{\mathfrak{a}\in\mathcal{I}} \phi(\mathfrak{a})(N\mathfrak{a})^{-s}, \quad L(\psi, s) := \sum_{\mathfrak{a}\in\mathcal{I}} \psi(\mathfrak{a})(N\mathfrak{a})^{-s}. \tag{3.8}$$

Rearranging the sums and normalizing gives

$$L(\phi, 4s) = \sum_{n=1}^{\infty} \left(\sum_{N\mathfrak{a}=n^4} \phi(\mathfrak{a}) \right) n^{-4s} = \sum_{n=1}^{\infty} \tfrac{1}{8} g(n) n^{-s} = \tfrac{1}{8} G(s),$$
$$L(\psi, 4s) = \sum_{c=1}^{\infty} \left(\sum_{N\mathfrak{a}=c^4} \psi(\mathfrak{a}) \right) c^{-4s} = \sum_{n=1}^{\infty} \tfrac{1}{4} f(n) n^{-s} = \tfrac{1}{4} F(s).$$

In particular, we will consider the counting functions

$$N_{\mathbb{D}}(\phi, H) := \sum_{N\mathfrak{a} \le H^2} \phi(\mathfrak{a}) = \tfrac{1}{8} N_{\mathcal{G}}(H^{1/2}), \tag{3.9}$$

$$N_{\mathbb{D}}(\psi, H) := \sum_{N\mathfrak{a} \le H^2} \psi(\mathfrak{a}) = \tfrac{1}{4} N_{\mathcal{F}}(H^{1/2}). \tag{3.10}$$

This notation will be justified in the following section.

4. Counting equidistributed Gaussian ideals in squareish regions

We consider the problem of counting ideals $\mathfrak{a} \subset \mathbb{Z}[i]$ with bounded norm that satisfy a certain property. However, our interest lies in counting these ideals with respect to a different height function. Geometrically, this corresponds to transforming a lattice point counting problem within a ball into that within a different region Ω. Our goal is to formalize the intuition that if:

- the region Ω is not too different from the ball, and
- the ideals with this property have "uniformly distributed angles",

then asymptotics should have the same shape.

4.1. **Setup.** Let $\mathcal{O} := \mathbb{Z}[i]$ denote the ring of Gaussian integers, with fraction field $K := \mathbb{Q}(i)$. Let $\mathcal{I}$ denote the multiplicative monoid of (nonzero) integral ideals in $\mathcal{O}$. For every $\mathfrak{a} = (\alpha) \in \mathcal{I}$, we denote by $N\mathfrak{a} := \#\mathcal{O}/\mathfrak{a} = \alpha\bar{\alpha}$ its norm. Let $\mathbb{D}$ denote the unit closed ball.

Definition 4.1. We say that a region Ω in $\mathbb{C}$ is squareish if it satisfies the following properties.

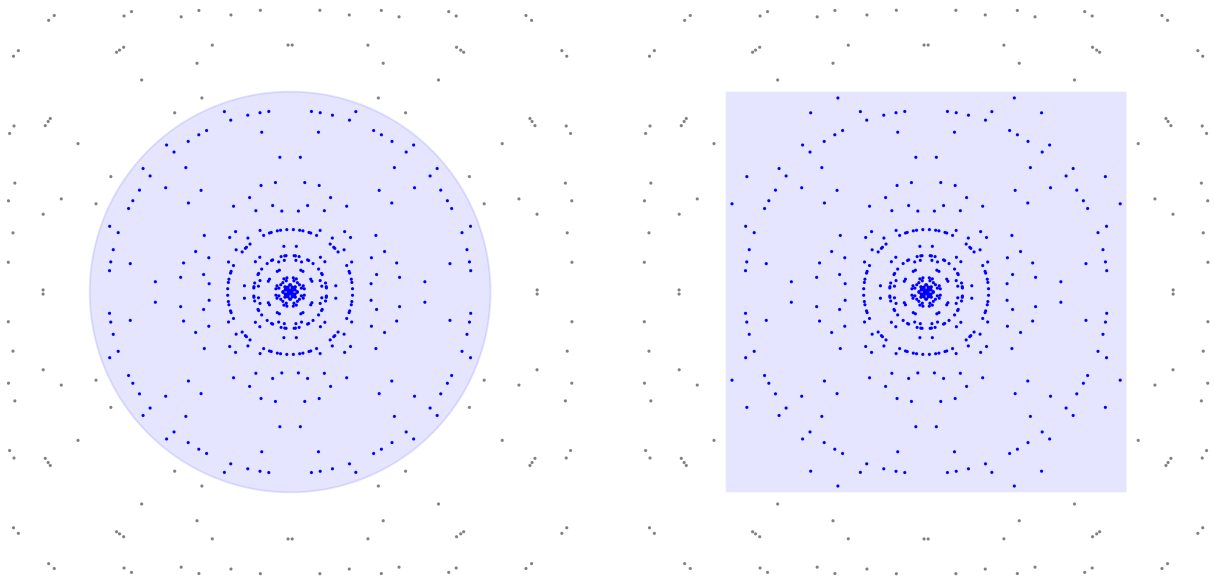
(R1) $0 \in \Omega$.
(R2) Ω is compact.
(R3) The boundary $\partial\Omega$ is parametrized by a continuous piecewise-smooth function

$$\omega \colon [0, 2\pi] \to \mathbb{C}.$$

(R4) The region Ω is invariant under the action of $\mathcal{O}^\times = \{\pm 1, \pm i\}$. In other words, the radius function $\omega(\theta)$ is periodic with period $\pi/2$.

Fix $s \in \mathbb{C}$, and consider the function $\omega(\theta)^{2s}$. This function admits a Fourier expansion of the form

$$\omega(\theta)^{2s} := \sum_{k \in 4\mathbb{Z}} I_{\Omega,k}(s) e^{ik\theta}, \tag{4.1}$$



(A) $\Omega = \mathbb{D} := \{z \in \mathbb{C} : |z| \leq 1\}$. (B) $\Omega = \{x + iy \in \mathbb{C} : \max(|x|, |y|) \leq 1\}$.

FIGURE 2. The lattice points plotted above correspond to Gaussian integers α such that the ideal $\mathfrak{a} = (\alpha)$ is twist minimal. The point is colored in blue if $\alpha \in H\Omega$ for some unspecified value of $H > 0$.

where

$$I_{\Omega,k}(s) = \frac{1}{2\pi} \int_0^{2\pi} \omega(\theta)^{2s} e^{-ik\theta} \, \mathrm{d}\theta = \frac{2}{\pi} \int_0^{\pi/2} \omega(\theta)^{2s} e^{-ik\theta} \, \mathrm{d}\theta. \tag{4.2}$$

Given $\mathfrak{a} \in \mathcal{I}$, let $\theta_{\mathfrak{a}} \in [0, \pi/2)$ be the argument of a generator $(\alpha) = \mathfrak{a}$ lying in the first quadrant. For every $k \in 4\mathbb{Z}$ we have the Hecke characters $\xi_k \colon \mathcal{I} \to \mathbb{C}^\times$ given by

$$\xi_k(\mathfrak{a}) := \left(\frac{\alpha}{|\alpha|}\right)^{ik} = e^{ik\theta_{\mathfrak{a}}}, \tag{4.3}$$

where α is any generator of the ideal $\mathfrak{a}$. The final piece of data is a function $\phi \colon \mathcal{I} \to \mathbb{C}$ defined on ideals, and the corresponding *twisted* Dirichlet series

$$L(s, \phi \otimes \xi_k) := \sum_{\mathfrak{a} \in \mathcal{I}} \phi(\mathfrak{a}) \xi_k(\mathfrak{a}) (N\mathfrak{a})^{-s}, \qquad \text{for } k \in 4\mathbb{Z}. \tag{4.4}$$

For our applications, ϕ is the characteristic function of some property, and an appropriate normalization of these Dirichlet series are L-functions (in the sense of [IK04, Section 5.1]). In particular, (4.4) converges absolutely in the half-plane $\mathrm{Re}(s) > \sigma_0 > 0$. When $k = 0$, we abbreviate $L(s, \phi) := L(s, \phi \otimes \xi_0)$. Note that when $\phi = \mathbf{1}$ is the constant function equal to one, $L(s, \mathbf{1}) = \zeta_K(s)$ is the Dedekind zeta function of $K = \mathbb{Q}(i)$, and $L(s, \mathbf{1} \otimes \xi_k) = L(s, \xi_k)$ are the Hecke L-functions.

4.2. **The main analytic lemma.** Our goal is to understand the asymptotic main term in the counting function

$$N_\Omega(H;\phi) := \sum_{\mathfrak{a}\in H\Omega} \phi(\mathfrak{a}), \tag{4.5}$$

where $H\Omega := \{Hz : z \in \Omega\}$. The abuse of notation $\mathfrak{a} \in H\Omega$ means that any generator α of $\mathfrak{a}$ is in the intersection $\mathcal{O} \cap H\Omega$. Since the norm is a quadratic function, we have that $\mathfrak{a} \in H\Omega$ if and only if $N\mathfrak{a} \le \omega(\theta_\mathfrak{a})^2 H^2$.

Lemma 4.2 (Main analytic lemma)**.** *Suppose that $\Omega \subset \mathbb{Z}$ is a squareish region, and that $\phi\colon \mathcal{I} \to \mathbb{C}$ is a function satisfying the following:*

(i) $L(s,\phi)$ has reasonable analytic properties:
- *a. $\phi(\mathfrak{a}) \in \mathbb{R}_{>0}$ for all $\mathfrak{a} \in \mathcal{I}$.*
- *b. $L(s,\phi)$ converges absolutely in a half-plane $\mathrm{Re}(s) > \sigma_0 > 0$.*
- *c. $L(s,\phi)$ admits a meromorphic continuation to a half-plane $\mathrm{Re}(s) > \sigma_0 - \delta_0 > 0$.*
- *d. In this domain, $L(s,\phi)$ has a unique pole of order $r = r(\phi) > 0$, at $s = \sigma_0$. We denote*
$$\Theta(\phi) := \lim_{s\to\sigma_0} (s-\sigma_0)^r L(s,\phi) > 0.$$
- *e. In the half-plane $\mathrm{Re}(s) > \sigma_0 - \delta_0$, we have the convexity bound*
$$|L(s,\phi)(s-\sigma_0)^r/s^r| = O(|1+\mathrm{Im}(s)|^\kappa),$$
for some $\kappa = \kappa(\phi) > 0$.

(ii) For every $0 \ne k \in 4\mathbb{Z}$, there exist functions $B_\phi(H,k)$ such that $\frac{B_\phi(H,k)}{H^{2\sigma_0}} \to 0$ as $H \to \infty$, $\frac{B_\phi(H,k)}{k^m} \to 0$ as $k \to \infty$ for some positive $m > 0$, and

$$\left| \sum_{N\mathfrak{a}\le H^2} \phi(\mathfrak{a})\xi_k(\mathfrak{a}) \right| \le B_\phi(H,k).$$

Then, there exists a monic polynomial $P(T) = P_{\phi,\Omega}(T) \in \mathbb{R}[T]$ of degree $r-1$ such that for every $0 < \delta < \delta_0$, we have

$$N_\Omega(H;\phi) = \frac{I_{\Omega,0}(\sigma_0)\Theta(\phi)2^{r-1}}{(r-1)!} H^{2\sigma_0} P(\log H) + O\left(\sum_{0\ne k\in 4\mathbb{Z}} \frac{B_\phi(H,k)}{k^{m+2}}, H^{2(\sigma_0-\delta)} \right), \text{ as } H\to\infty.$$

Here, the implicit constant depends on δ, Ω, and ϕ.

A direct consequence is the following.

Corollary 4.3. *In the situation of Lemma 4.2, if $\sigma_0 = 1$, then we have*

$$N_\Omega(H;\phi) \sim \frac{\mathrm{vol}(\Omega)}{\pi} N_{\mathbb{D}}(H;\phi).$$

Proof of Lemma 4.2. Let $c := \sigma_0 + 1$. From Perron's integral, we have for any fixed $\mathfrak{a} \in \mathcal{I}$ that

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \left(\frac{\omega(\theta_\mathfrak{a})^2 H^2}{N\mathfrak{a}}\right)^s \frac{\mathrm{d}s}{s} = \begin{cases} 1, & \text{if } N\mathfrak{a} < \omega(\theta_\mathfrak{a})^2 H^2, \\ \frac{1}{2}, & \text{if } N\mathfrak{a} = \omega(\theta_\mathfrak{a})^2 H^2, \\ 0, & \text{if } N\mathfrak{a} > \omega(\theta_\mathfrak{a})^2 H^2. \end{cases} \tag{4.6}$$

Replacing $\omega(\theta)^{2s}$ by its Fourier expansion (4.1), exchanging the order of integration and summation, and summing over all $\mathfrak{a} \in \mathcal{I}$ we obtain

$$N_\Omega(H;\phi) = \frac{1}{2\pi i}\sum_{k\in 4\mathbb{Z}}\int_{c-i\infty}^{c+i\infty} L(s,\phi\otimes\xi_k)I_{\Omega,k}(s)H^{2s}\frac{\mathrm{d}s}{s}, \tag{4.7}$$

which holds for almost all $H > 0$ [2]. The proof proceeds in two steps. First, we show that the dominant term in the sum is $k = 0$ with negligible error

$$N_\Omega(\phi;H) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} L(s,\phi)I_{\Omega,0}(s)H^{2s}\frac{\mathrm{d}s}{s} + O\left(\sum_{0\neq k\in 4\mathbb{Z}}\frac{B_\phi(H,k)}{k^{m+2}}\right). \tag{4.8}$$

for some positive integer m. Then, we show that

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} L(s,\phi)I_{\Omega,0}(s)H^{2s}\frac{\mathrm{d}s}{s} = \frac{I_{\Omega,0}(\sigma_0)\Theta(\phi)2^{r-1}}{(r-1)!}H^{2\sigma_0}P(\log H) + O(H^{2(\sigma_0-\delta)}). \tag{4.9}$$

We will show these assertions in Lemma 4.4 and Lemma 4.5. When $\sigma_0 = 1$, the corollary follows from the formula for area in polar coordinates:

$$\frac{\mathrm{vol}(\Omega)}{\mathrm{vol}(\mathbb{D})} = \frac{1}{\pi}\int_0^{2\pi}\frac{1}{2}\omega(\theta)^2\,\mathrm{d}\theta = I_{\Omega,0}(1).$$

□

Lemma 4.4. *Assertion (4.8) holds.*

Proof. Let $c := \sigma_0 + 1$. Starting from Equation (4.7), we need to show that for some positive integer m,

$$\frac{1}{2\pi i}\sum_{0\neq k\in 4\mathbb{Z}}\int_{c-i\infty}^{c+i\infty} L(s,\phi\otimes\xi_k)I_{\Omega,k}(s)H^{2s}\frac{\mathrm{d}s}{s} = O\left(\sum_{0\neq k\in 4\mathbb{Z}}\frac{B_\phi(H,k)}{k^{m+2}}\right).$$

For every individual $0 \neq k \in 4\mathbb{Z}$, Item (ii) ensures that there exists a function $B_\phi(H)$, depending only on ϕ, uniformly bounding the sums $\sum\phi(\mathfrak{a})\xi_k(\mathfrak{a})$. On the other hand, the smoothness of the boundary of Ω implies the superpolynomial decay of $I_{\Omega,k}(s)$. This gives us a constant $C_m(\Omega) > 0$, independent of k, such that $|I_{\Omega,k}(s)| \leq C_m(\Omega)|/|k|^m$ for every $m \in \mathbb{Z}_{>0}$. From the triangle inequality, we have that

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} L(s,\phi\otimes\xi_k)I_{\Omega,k}(s)H^{2s}\frac{\mathrm{d}s}{s}\right| &\leq \frac{C_m(\Omega)}{|k|^m}\left|\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} L(s,\phi\otimes\xi_k)H^{2s}\frac{\mathrm{d}s}{s}\right| \\ &\leq \frac{C_m(\Omega)}{|k|^m}\left|\sum_{N\mathfrak{a}\leq H^2}\phi(\mathfrak{a})\xi_k(\mathfrak{a})\right| \leq \frac{C_m(\Omega)}{|k|^m}B_\phi(H,k).\end{aligned}$$

Taking m sufficiently large, and summing over all $0 \neq k \in 4\mathbb{Z}$, we obtain the result. □

Lemma 4.5. *Assertion (4.9) holds.*

[2] In particular, H can be chosen so that the Perron integral does not equal $\frac{1}{2}$ for all $\mathfrak{a} \in \mathcal{I}$

Proof. Let $c := \sigma_0 + 1$. The idea is the standard trick of shifting the vertical segment from $-c - iT$ to $c + iT$ to the vertical segment from $\sigma_0 - \delta - iT$ to $\sigma_0 - \delta + iT$, for some $0 < \delta < \delta_0$, so that we pick up the pole at $s = \sigma_0$. Then we can write the integral on the left hand side of Equation (4.9) as

$$\text{Res}_{s=\sigma_0}\big[L(s,\phi)I_{\Omega,0}(s)H^{2s}/s\big] + \frac{1}{2\pi i}\int_{\Gamma_{\delta,T}} L(s,\phi)I_{\Omega,0}(s)H^{2s}\frac{\mathrm{d}s}{s}. \tag{4.10}$$

Instead of repeating the proof of the Weiner–Ikehara Tauberian theorem (see for instance [CLT01, Appendice A]), we explain how the extraneous factor $I(s) = I_{\Omega,0}(s)$ transforms the asymptotic.

Using the fact that $I(s)$ is uniformly bounded in the strip $\sigma_0 - \delta \leq \text{Re}(s) \leq c$, we see that

$$\frac{1}{2\pi i}\int_{\Gamma_{\delta,T}} L(s,\phi)I(s)H^{2s}\frac{\mathrm{d}s}{s} = O\left(\frac{1}{2\pi i}\int_{\Gamma_{\delta,T}} L(s,\phi)H^{2s}\frac{\mathrm{d}s}{s}\right).$$

Choosing an appropriate value of T in terms of H, the proof of the classical theorem gives that this term is $O(H^{2(\sigma_0-\delta)})$.

To calculate the residue, we compute the Laurent expansions of the terms around $s = \sigma_0$ and calculate the coefficient of $(s-\sigma_0)^{-1}$ in their product. We have:

$$\begin{aligned}
L(s,\phi) &= \sum_{n=-r}^{\infty} \Theta_n (s-\sigma_0)^n, \\
I(s) &= \sum_{a=0}^{\infty} \tfrac{I^{(a)}(\sigma_0)}{a!}(s-\sigma_0)^a, \\
H^{2s} &= \sum_{b=0}^{\infty} \tfrac{H^{2\sigma_0}(2\log H)^b}{b!}(s-\sigma_0)^b, \\
1/s &= \sum_{c=0}^{\infty} \tfrac{(-1)^c}{\sigma_0^{n+1}}(s-\sigma_0)^c,
\end{aligned}$$

It follows that the residue is given by the formula

$$\text{Res}_{s=\sigma_0}\big[L(s,\phi)I(s)H^{2s}/s\big] = \sum_{n+a+b+c=-1} \Theta_n \tfrac{I^{(a)}(1)}{a!}\tfrac{H^2 2^b(\log H)^b}{b!}\tfrac{(-1)^c}{\sigma_0^{c+1}}. \tag{4.11}$$

In particular, the main term occurs when $n = -r$, $b = r-1$, and $a = c = 0$, so that the leading constant in the asymptotic is

$$I_{\Omega,0}(\sigma_0) \cdot \frac{\Theta_{-r} 2^{r-1}}{\sigma_0 (r-1)!} > 0. \tag{4.12}$$

□

5. Proof of Theorem 1.1

We already know how to count minimal Fermat triples with $|c| \leq H$. We give a bijective correspondence between such triples (a,b,c) and 5-isogenies $(E_{a,b,c}, C_{a,b,c})$, up to isomorphism. Thus, we can write our counting function as

$$N_5(H) = \#\{(a,b,c) \in \mathcal{G}\langle\mathbb{Q}\rangle : H(a,b,c) \leq H\},$$

where $H(a,b,c)$ is the naive height of a minimal Weierstrass equation for $E_{a,b,c}$. We have the compact region

$$\mathcal{R}_5 := \Big\{(x,y) \in \mathbb{R}^2 : H\Big(x, y, \sqrt[4]{x^2+y^2}\Big) \leq 1\Big\}. \tag{5.1}$$

The strategy is to write $N_5(H)$ as a rescaling of $N_{\mathcal{R}_5}(H;\phi)$ for some arithmetic function ϕ, and then use the main analytic lemma (Lemma 4.2) to complete the proof. To do this, we need to overcome two obstacles:

(1) The first one, is that the region $\mathcal{R}_5$ is not squareish. To overcome this, we partition $\mathcal{R}_5 = \mathcal{R}_5^{(i)} \sqcup \mathcal{R}_5^{(ii)} \sqcup \mathcal{R}_5^{(iii)} \sqcup \mathcal{R}_5^{(iv)}$ into its quadrants, and rotate each component to obtain four squareish regions $\Omega^{(i)}, \Omega^{(ii)}, \Omega^{(iii)}, \Omega^{(iv)}$. Further details can be found in Section 5.2.

(2) The second one, is that our chosen Weierstrass model for $E_{a,b,c}$ is not always a minimal one. We overcome this issue by carefully quantifying how far is $E_{a,b,c}$ from being minimal, and applying an inclusion-exclusion sieve. Further details can be found in Section 5.1 and Section 5.3.

5.1. **The parametrization.** Given a minimal Fermat triple (a,b,c), consider the curve whose Weierstrass equation is given by

$$\mathsf{y}^2 = \mathsf{x}^3 + A(a,b,c)\mathsf{x} + B(a,b,c), \tag{5.2}$$

where

$$\begin{aligned} A(a,b,c) &:= -6(123a + 114b + 125c^2) \\ &= -(2\cdot 3^2\cdot 41)a - (2^2\cdot 3^2\cdot 19)b - (2\cdot 3\cdot 5^3)c^2, \end{aligned} \tag{5.3}$$

$$\begin{aligned} B(a,b,c) &:= 8c(2502a + 261b + 2500c^2) \\ &= (2^4\cdot 3^2\cdot 139)ac + (2^3\cdot 3^2\cdot 29)bc + (2^5\cdot 5^4)c^3. \end{aligned} \tag{5.4}$$

When the discriminant $\Delta(a,b,c) := -16(4A(a,b,c)^3 + 27B(a,b,c)^2)$ is not zero, the smooth projective model of Equation (5.2) is an elliptic curve $E_{a,b,c}$ defined over $\mathbb{Q}$. Furthermore, this elliptic curve admits a rational 5-isogeny $C_{a,b,c} \subseteq E_{a,b,c}(\bar{\mathbb{Q}})[5]$. Indeed, the 5-division polynomial $\psi_5(T; E_{a,b,c}) \in \mathbb{Z}[a,b,c][T]$ has a quadratic factor

$$h(a,b,c;T) := 5T^2 - 100cT - 2106a - 1750c^2 + 792b. \tag{5.5}$$

The cyclic group $C_{a,b,c}$ is defined as the group generated by the points $P \in E_{a,b,c}(\bar{\mathbb{Q}})[5]$ whose x-coordinates are the roots of $h(a,b,c;T)$.

We will denote by $\mathcal{X}\langle\mathbb{Q}\rangle$ the set of isomorphism classes of the groupoid $\mathcal{X}(\mathbb{Q})$. We have $\mathcal{X}_0(5)\langle\mathbb{Q}\rangle = X_0(5)(\mathbb{Q})$. As a corollary of Lemma 2.8 we have the following parametrization of isomorphism classes of 5-isogenies in terms of minimal Fermat triples. Given a 5-isogeny (E,C), we denote its $\mathbb{Q}$-isomorphism class by $[E,C]$.

Lemma 5.1. *The equivalence of Lemma 2.8 induces a bijection $\Phi\colon \mathcal{G}\langle\mathbb{Q}\rangle \to X_0(5)(\mathbb{Q})$. Under this map, the cusps $\Phi(Q_1), \Phi(Q_2) \in X_0(5)(\mathbb{Q})$ correspond to the minimal triples*

$$Q_1 := (-1,0,1), \quad Q_2 := (-528, 220, 25).$$

In particular, Φ restricts to an isomorphism

$$\Phi\colon \mathcal{G}\langle\mathbb{Q}\rangle - \{Q_1,Q_2\} \longrightarrow Y_0(5)(\mathbb{Q}), \quad (a,b,c) \mapsto [E_{a,b,c}, C_{a,b,c}]. \tag{5.6}$$

The identical parametrization of twist minimal isomorphism classes of 5-isogenies in terms of twist minimal Fermat triples also holds. Given a 5-isogeny (E, C) defined over $\mathbb{Q}$, we denote its $\bar{\mathbb{Q}}$-isomorphism class by $\langle E, C\rangle$.

Lemma 5.2. *The equivalence of Lemma 2.8 induces a bijection* $\Psi\colon \mathcal{F}\langle\mathbb{Q}\rangle \to \mathcal{Z}_0(5)\langle\mathbb{Q}\rangle$. *Likewise, the cusps* $\Psi(Q_1), \Psi(Q_2) \in \mathcal{Z}_0(5)(\mathbb{Q})$ *correspond to the twist minimal Fermat triples*

$$Q_1 := (-1, 0, 1), \quad Q_2 := (-528, 220, 25).$$

In particular, Ψ *restricts to an isomorphism*

$$\Psi\colon \mathcal{F}\langle\mathbb{Q}\rangle - \{Q_1, Q_2\} \longrightarrow (\mathcal{Z}_0(5)\langle\mathbb{Q}\rangle - \{\Psi(Q_1), \Psi(Q_2)\}), \quad (a, b, c) \mapsto \langle E_{a,b,c}, C_{a,b,c}\rangle. \tag{5.7}$$

Observe that the representatives $(E_{a,b,c}, C_{a,b,c})$ of the isomorphism classes in Lemma 5.1 and Lemma 5.2 do not need to correspond to a minimal Weierstrass equation.

Definition 5.3. A Weierstrass equation of the elliptic curve $E : \mathsf{y}^2 = \mathsf{x}^3 + A\mathsf{x} + B$ is twist minimal if no prime p satisfies $p^2 \mid A$ and $p^3 \mid B$.

In light of our definition of height (Equation (1.1)), it is necessary to understand the twist minimal triples (a, b, c) giving rise to Weierstrass equations $E_{a,b,c}$ that are not twist minimal.

Definition 5.4. The twist error of a Fermat triple (a, b, c), denoted by $\mathrm{md}(a, b, c)$, is

$$\mathrm{md}(a, b, c) := \max\{e \in \mathbb{Z}_{>0} \ : \ e^2 \mid A(a, b, c) \text{ and } e^3 \mid B(a, b, c)\}.$$

In the notation of [MV23], this is the *twist minimality defect* of the Weierstrass equation $E_{a,b,c}$. We say that a twist minimal Fermat triple (a, b, c) is exceptional if $\mathrm{md}(a, b, c) > 1$.

We classify the exceptional twist minimal Fermat triples.

Proposition 5.5. *Let* (a, b, c) *be a twist minimal Fermat triple.*

(1) The set of all possible values of $\mathrm{md}(a, b, c)$ *is*

$$\mathrm{md} := \{1, 2, 5, 10, 25, 50, 125, 250\}.$$

(2) $2 \mid \mathrm{md}(a, b, c)$ *if and only if* $2 \mid b$. *Moreover, the 2-adic valuations of* $A, B,$ *and* md *are in Table 2*

(3) $5 \mid \mathrm{md}(a, b, c)$ *if and only if* $\alpha = a + ib$ *for any one of* $\alpha \in \mathbb{Z}[i]$ *provided in Table 3.*

$\mathrm{ord}_2(A)$	$\mathrm{ord}_2(B)$	$\mathrm{ord}_2(\mathrm{md})$
1	3	0
≥ 2	4	1

TABLE 2. 2-adic valuations of $A(a, b, c)$, $B(a, b, c)$, and $\mathrm{md}(a, b, c)$.

Proof. We break up the proof of the proposition into a number of lemmas in modular arithmetic. All the Fermat triples below are assumed to be twist minimal.

The first two statements follow by combining the statements of Lemmas 5.8, 5.9, 5.10, and 5.11. The last statement follows from Lemma 5.12. □

Lemma 5.6. *If a prime* p *satisfies* $p \mid c$ *and* $p^2 \mid A(a, b, c)$, *then* $p = 5$.

$\alpha = a + ib \in \mathbb{Z}[i]$	$\mathrm{ord}_5(A)$	$\mathrm{ord}_5(B)$	$\mathrm{ord}_5(\mathrm{md})$
$(1-2i)^4\beta$	4	5	1
$5(1-2i)^2\beta$	3	4	1
$(1-2i)^{4k}\beta$, $k \geq 2$	5	$k+7$	2
$5(1-2i)^6\beta$	6	9	3
$5(1-2i)^{4k-2}\beta$, $k \geq 3$	6	$k+8$	3

TABLE 3. 5-adic valuations of $A(a,b,c)$, $B(a,b,c)$, and $\mathrm{md}(a,b,c)$. Here, $\beta \in \mathbb{Z}[i]$ is any element of norm coprime to 5.

Proof. From Lemma 3.5, every prime p dividing c satisfies $p \equiv 1 \bmod 4$. Thus, $p \neq 2, 3$. Assume that $p \neq 5$. Reducing Equation (5.3) modulo p^2 that $123a \equiv -114b \bmod p^2$. This implies that

$$\begin{aligned}(123c^2)^2 &= (123a)^2 + (123b)^2 \\ &\equiv (-114b)^2 + (123b)^2 \bmod p^2 \\ &\equiv (114^2 + 123^2)b^2 \bmod p^2 \equiv 3^2 \cdot 5^5 \cdot b^2 \equiv 0 \bmod p^2.\end{aligned}$$

It follows that $p \mid b$, and therefore $p \mid a$ as well. Let $a' := a/p$, $b' := b/p$ and $c' := c/p$. We have that $(a')^2 + (b')^2 = p^2(c')^4$ and $123a' + 114b' + 125p(c')^2 \equiv 0 \bmod p$. Once more, it follows that $123a' \equiv -114b' \bmod p$, and

$$\begin{aligned}(123a')^2 + (123b')^2 &\equiv (114^2 + 123^2)(b')^2 \bmod p \\ &\equiv 3^2 \cdot 5^5 \cdot (b')^2 \equiv 0 \bmod p.\end{aligned}$$

This allows us to conclude that $p \mid b'$, and therefore $p \mid a'$ as well. This contradicts the twist minimality of the triple (a,b,c).

To see that the case $p = 5$ indeed occurs, one can take $(a,b,c) = (-527, -336, 25)$. This triple is twist minimal, since $\gcd(a,b) = 1$, and $A(a,b,c) = 2^4 \cdot 3 \cdot 5^5$. □

Lemma 5.7. *If p is a prime divisor of $\mathrm{md}(a,b,c)$, then $p \in \{2,5\}$.*

Proof. By definition, $p \mid \mathrm{md}(a,b,c)$ if and only if $p^2 \mid A := A(a,b,c)$ and $p^3 \mid B := B(a,b,c)$. If p also divided c, then Lemma 5.6 implies that $p = 5$. For this reason, we assume that p does not divide c.

We use the equations $A \equiv 0 \bmod p^2$ and $B \equiv 0 \bmod p^2$ to find congruence relations between a and b modulo p^2. We find integer linear combinations of cA and B that allow us to cancel the terms with a or b in them, obtaining:

$$1112cA + 41B = -(14000c^3 + 675000bc) = -2^3 5^3 c(14c^2 + 675b) \equiv 0 \bmod p^2,$$

$$58ca + 19B = 337500ac + 336500c^3 = 2^2 5^3 c(673c^2 + 675a) \equiv 0 \bmod p^2.$$

If $p \neq \{2,5\}$, then $(14c^2 + 675b) \equiv 0 \bmod p^2$ and $(673c^2 + 675a) \equiv 0 \bmod p^2$. But in this case, we can reduce the equation $(675a)^2 + (675b)^2 = 675^2 c^4$ modulo p^2 to obtain

$$5^6 \cdot 29 = 14^2 + 673^2 \equiv 675^2 = 3^6 \cdot 5^4 \bmod p^2,$$

producing a contradiction. We conclude that in this case $p \in \{2,5\}$, and the result follows. □

Lemma 5.8. *The following assertions hold.*

(a) $2 \mid \mathrm{md}(a,b,c)$ *if and only if* $2 \mid b$.
(b) $5 \mid \mathrm{md}(a,b,c)$ *if and only if* $a \equiv 7b \bmod 25$ *and* $5 \mid c$.

We say that (a,b,c) *is 2-exceptional when (a) holds, and 5-exceptional when (b) holds.*

Proof.

(a) If $2 \mid \mathrm{md}(a,b,c)$, then $4 \mid A$. This implies that a and c have the same parity. Since $c \equiv 1 \bmod 4$, a must be odd. But since a and b have opposite parity, we conclude that $2 \mid b$. Conversely, suppose that $2 \mid b$. This implies that a is odd. Since $8 \mid B$, we only need to show that $4 \mid A$. But this is visibly true once we know that a is odd.
(b) If $5 \mid \mathrm{md}(a,b,c)$, then $A \equiv 0 \bmod 25$. This implies that $a \equiv 7b \bmod 25$. From this congruence, we see that $c^4 = a^2 + b^2 = 50b^2 \equiv 0 \bmod 25$, so that $5 \mid c$. Conversely, the congruence $a \equiv 7b \bmod 25$ implies that $A \equiv 0 \bmod 25$ and $B/(8c) \equiv 0 \bmod 25$, which is enough to conclude that $5 \mid \mathrm{md}(a,b,c)$.

□

Lemma 5.9. $\mathrm{md}(a,b,c)$ *is not divisible by* 4.

Proof. Suppose that $4 \mid \mathrm{md}(a,b,c)$. By definition, this means that $4^2 \mid A$ and $4^3 \mid B$. From Equations (5.3) and (5.4), we deduce that

$$123a + 114b + 125c^2 \equiv 0 \bmod 8,$$
$$2502a + 261b + 2500c^2 \equiv 0 \bmod 8.$$

Since $c \equiv 1 \bmod 4$ (Lemma 3.5), we have that $c^2 \equiv 1 \bmod 8$, and the above congruences simplify to:

$$3a + 2b + 5 \equiv 0 \bmod 8,$$
$$6a + 5b + 4 \equiv 0 \bmod 8.$$

These imply that $b \equiv 6 \bmod 8$, and $a^2 + b^2 = c^4$ implies that $a^2 \equiv 5 \bmod 8$. But this contradicts the fact that 5 is not a square modulo 8. □

Lemma 5.10. *If* $\mathrm{md}(a,b,c)$ *is divisible by* 2*, then* $\mathrm{ord}_2(A(a,b,c)) \geq 2$ *and* $\mathrm{ord}_2(B(a,b,c)) = 4$*. Otherwise,* $\mathrm{ord}_2(A(a,b,c)) = 1$ *and* $\mathrm{ord}_2(B(a,b,c)) = 3$.

Proof. Suppose $2 \mid \mathrm{md}(a,b,c)$. Using $a^2 + b^2 = c^4 \bmod 16$, one obtains that $4 \mid b$, $a \equiv 1, 7, 9, 15 \bmod 16$, and $c^2 \equiv 1, 9 \bmod 16$. It follows that $\mathrm{ord}_2(A(a,b,c)) \geq 2$ and $\mathrm{ord}_2(B(a,b,c)) = 4$. The case for $2 \nmid \mathrm{md}(a,b,c)$ follows from the fact that b, c are odd. □

Lemma 5.11. $\mathrm{md}(a,b,c)$ *is not divisible by* 5^4.

Proof. Suppose that $5^4 \mid \mathrm{md}(a,b,c)$. By definition, this implies that $5^8 \mid A$ and $5^{12} \mid B$. Using Equations (5.3) and (5.4), we deduce that

$$123a + 114b + 125c^2 \equiv 0 \bmod 5^8$$
$$c(2502a + 261b + 2500c^2) \equiv 0 \bmod 5^{12}.$$

We consider four cases depending on the 5-valuation of c.

Case 1: Suppose $\mathrm{ord}_5(c) \geq 3$. Then, $41a + 38b \equiv 0 \bmod 5^8$. This congruence simplifies to $a \equiv 323932b \bmod 5^8$. Using the equation $a^2 + b^2 = c^4$, we obtain

$$a^2 + b^2 \equiv 300000a^2 = 2^5 \cdot 3 \cdot 5^5 a^2 \equiv 0 \bmod 5^8.$$

This implies that $a \equiv b \equiv 0 \bmod 5^2$, contradicting the twist minimality of (a, b, c).

Case 2: Suppose that $\mathrm{ord}_5(c) = 2$. We obtain the linear system

$$41a + 38b \equiv 0 \bmod 5^7,$$
$$278a + 29b \equiv 0 \bmod 5^7.$$

Solving for b in the first equation and substituting into the second one, we arrive at

$$18750a = 2 \cdot 3 \cdot 5^5 a \equiv 0 \bmod 5^7.$$

This implies that $a \equiv b \equiv 0 \bmod 5^2$, contradicting the twist minimality of (a, b, c).

Case 3: Suppose that $\mathrm{ord}_5(c) = 1$. Then $41a + 38b \equiv 0 \bmod 5^5$. Solving for b we obtain $b \equiv 1068a \bmod 5^5$, which implies

$$a^2 + b^2 \equiv 3125a^2 \equiv 5^5 a^2 \equiv 0 \equiv c^4 \bmod 5^5.$$

This implies that $5^2 \mid c$, a contradiction.

Case 4: Suppose that $\mathrm{ord}_5(c) = 0$. Then Equation (5.4) implies $278a + 29b \equiv 0 \bmod 5^4$. Solving for b, we obtain $b \equiv 497 \bmod 5^4$, which implies

$$c^4 = a^2 + b^2 \equiv 625a^2 \equiv 5^4 a^2 \equiv 0 \bmod 5^4.$$

This implies that $5 \mid c$, a contradiction. □

Lemma 5.12. *Let (a, b, c) be a 5-exceptional triple corresponding to $\alpha = a + bi \in \mathbb{Z}[i]$. Then, we can write $\alpha = \delta \cdot \beta$ where β and δ are coprime twist minimal Gaussian integers, and δ is given in the following table:*

$\mathrm{ord}_5(\mathrm{md}(a, b, c))$	δ
1	$(1 - 2i)^4$
1	$5(1 - 2i)^2$
2	$(1 - 2i)^{4k}$
3	$5(1 - 2i)^{4k-2}$

Proof. Since (a, b, c) is 5-exceptional, we know that $\mathrm{ord}_5(c) = k \geq 1$. Moreover, we can write $\alpha = \delta \cdot \beta$ so that β is coprime to both $1 \pm 2i$. This implies that $\delta \in \left\{(1 \pm 2i)^{4k}, 5(1 \pm 2i)^{4k-2}\right\}$. On the other hand, observe that

$$(1 + 2i)^5 \alpha = (41 - 38i)(a + bi) = (41a + 38b) + i(41b - 38a), \tag{5.8}$$

$$(1 + 2i)^7 \alpha = (29 + 278i)(a + bi) = (29a - 278b) + i(278a + 29b). \tag{5.9}$$

Taking the norm and comparing the parity of $\mathrm{ord}_5(\cdot)$ on each side of the equation, we deduce that

$$\mathrm{ord}_5(41a + 38b) = \mathrm{ord}_5(41b - 38a) = \mathrm{ord}_5((1 + 2i)^5 \alpha),$$
$$\mathrm{ord}_5(278a + 29b) = \mathrm{ord}_5(29a - 278b) = \mathrm{ord}_5((1 + 2i)^7 \alpha).$$

Furthermore, since 5 divides A and B, we must have that $\delta \in \{(1-2i)^{4k}, 5(1-2i)^{4k-2}\}$. Taking $\mathrm{ord}_5(\cdot)$ on Equations (5.3) and (5.4) we obtain

$$\mathrm{ord}_5(A(a,b,c)) \geq \min\{\mathrm{ord}_5((1+2i)^5\delta), 3+2k\}, \tag{5.10}$$

$$\mathrm{ord}_5(B(a,b,c)) \geq k + \min\{\mathrm{ord}_5((1+2i)^7\delta), 4+2k\}, \tag{5.11}$$

with equality when the entries of the minimum functions are distinct. □

5.2. **The rigidified count.** We adopt the strategy of the proof of Theorem 3.2 and apply the main analytic lemma (Lemma 4.2) to obtain an explicit formula for our counting function

$$N_5^{tw}(H,t) := \#\{(a,b,c) \in \mathcal{F}\langle\mathbb{Q}\rangle : \ \mathrm{md}(a,b,c) = t, H(a,b,c) \leq H\}$$

where in the equation above $H(a,b,c)$ is the naive height of $E_{a,b,c}$. That is,

$$H(a,b,c) = \frac{\max\{27|A(a,b,c)|^3, 4B(a,b,c)^2\}}{\mathrm{md}(a,b,c)^6}.$$

We address the minimality of the Weierstrass equation $E_{a,b,c}$ in Section 5.3, where we obtain the asymptotics for the number of elliptic curves over $\mathbb{Q}$ admitting 5-isogenies.

Theorem 5.13. *For each $t \in \mathsf{MD} = \{1,2,5,10,25,50,125,250\}$, there exist explicitly computable constants $\hat{C}_{5,t}, \hat{C'}_{5,t} \in \mathbb{R}$ and a number $c \in (0,1)$ such that*

$$N_5^{tw}(H,t) = \hat{C}_{5,t} H^{\frac{1}{6}} (\log H) + \hat{C'}_{5,t} H^{\frac{1}{6}} + O(H^{\frac{1}{6}} \cdot (\log H)^{-1+c})$$

as $H \to \infty$. The constants $\hat{C}_{5,t}$ are given by:

$$\hat{C}_{5,t} := \begin{cases} \frac{f_1}{8\pi\sqrt{3}} \cdot \mathrm{vol}(\sqrt[4]{\mathcal{R}_5}) & \text{if } t \in \{1,2\}, \\ \frac{f_1}{15\pi\sqrt{3}} \cdot \mathrm{vol}(\sqrt[4]{\mathcal{R}_5}) & \text{if } t \in \{5,10\}, \\ \frac{f_1}{120\pi\sqrt{3}} \cdot \mathrm{vol}(\sqrt[4]{\mathcal{R}_5}) & \text{if } t \in \{25,50,125,250\}, \end{cases}$$

where f_1 is the constant defined in Theorem 3.4.

Given $t \in \mathsf{MD}$, define the twist minimality defect height zeta function corresponding to $N_5^{tw}(H,t)$ to be the Dirichlet series

$$F_t(s) := \sum_{c=1}^{\infty} \frac{f_t(c)}{c^s}, \tag{5.12}$$

where we denote by $f_t(c)$ the twist minimality defect arithmetic height function that counts the number of twist minimal triples (a',b',c') with $c' = c$ and $\mathrm{md}(a',b',c') = t$. The following lemma is an analogue of Lemma 3.6.

Check the newly updated Lemma 5.14.

Lemma 5.14. *The arithmetic height function $f_t(c)$ satisfies the following properties.*

(1) If $p \not\equiv 1 \bmod 4$, then $f_t(p^k) = 0$ for every positive integer k.

(2) Suppose $t \in \{1,2\}$.

- *If $p \equiv 1 \bmod 4$ and $p \neq 5$, then $f_t(p^k) = 8$ for every positive integer k.*
- *If $p = 5$, then $f_t(5^k) = 4$ for every positive integer k.*
- *The arithmetic function $f_t(c)/2$ is multiplicative, but not completely multiplicative.*

(3) Suppose $t \in \{5,10\}$.

- *Given any integer c, if $\mathrm{ord}_5(c) \neq 1$ then $f_t(c) = 0$.*
- *We have $f_t(5) = 4$ and $f_t(5^k) = 0$ for every positive integer $k \geq 2$.*
- *For any c corpime to 5, we have $f_t(5c) = 4f_{\frac{t}{5}}(c)$.*

(4) Suppose $t \in \{25, 50, 125, 250\}$.

- *Given any integer c, if $\mathrm{ord}_5(c) \leq 1$, then $f_t(c) = 0$.*
- *We have $f_t(5) = 0$, and $f_t(5^k) = 2$ for every positive integer $k \geq 2$.*
- *For any c coprime to 5 and $k \geq 2$, we have $f_t(5^k c) = 2f_{\frac{t}{25}}(c)$ if $t \in \{25, 50\}$, and $f_t(5^k c) = 2f_{\frac{t}{125}}(c)$ if $t \in \{125, 250\}$.*

Proof. We recall from Lemma 5.8 that $2 \mid \mathrm{md}(a, b, c)$ if and only if b is even. Because (a, b, c) is twist minimal, c is odd. This implies that one of a and b must be even. Without loss of generality, assume b is even. Multiplication by $\pm i$ flips the role of a and b. Statements (1) and (2) (except for the case where $p = 5$) follow from adapting the technique of the proof shown in Lemma 3.6, in particular by using multiplicativity of ideal norms. To check the statement for $p = 5$, we use Lemma 5.12. Suppose that $I \subset \mathbb{Z}[i]$ is an ideal such that $5 \nmid \mathrm{md}(a, b, c)$ and $N(I) = 5^k$. There are two such ideals, each of which is generated by $(1 + 2i)^k$ and $5 \cdot (1 + 2i)^{k-1}$.

To check statements (3) and (4), we also use Lemma 5.12. If $\mathrm{md}(a, b, c) = 5$ or 10, then there are only two such ideals $I \subset \mathbb{Z}[i]$, generated by $(1 - 2i)^4$ and $5 \cdot (1 - 2i)^2$: both ideals have norm $N(I) = 5^4$. If $\mathrm{md}(a, b, c) = 25$ or 50, then for each $k \geq 2$ such that $N(I) = 5^k$, there is only one ideal $I \subset \mathbb{Z}[i]$ satisfying the aforementioned conditions: it is the ideal generated by $(1 - 2i)^{4k}$. Lastly, if $\mathrm{md}(a, b, c) = 125$ or 250, then for each $k \geq 2$ such that $N(I) = 5^k$, there is only one ideal $I \subset \mathbb{Z}[i]$ satisfying the aforementioned conditions: it is the ideal generated by $5 \cdot (1 - 2i)^{4k-2}$. To relate the arithmetic functions f_t with $f_{\frac{t}{25}}$ or $f_{\frac{t}{125}}$, we use the fact that any ideal I such that $5 \mid \mathrm{md}(a, b, c)$ must be of form $\delta \cdot \beta$ where δ has norm divisible by 5, and β is coprime to 5. □

To prove Theorem 5.13, we check whether the two conditions of the main analytic lemma are satisfied. Given a squareish region $\Omega \subset \mathbb{Z}$ and $t \in \mathrm{md}$, denote by $\phi_t : \mathcal{I} \to \mathbb{C}$ be a function induced from the arithmetic height function f_e.

Lemma 5.15. *The Dirichlet series $F_t(s)$ satisfies all reasonable analytic properties in part (i) of Lemma 4.2, with $\sigma_0 = \frac{1}{4}$, $\delta_0 = \frac{1}{8}$, and $r = 2$.*

Proof. Suppose $t \in \{1, 2\}$. The two arithmetic height functions $f(c)$ and $f_t(c)$ appearing in Lemmas 3.6 and 5.14 are similar to each other in that

$$\frac{f(c)}{4} = \frac{f_t(c)}{2}$$

as long as c is coprime to 5. This implies that for any $t \in \{1, 2\}$, the function $F_t(s)$ can be related to the height zeta function $F(s)$ associated to f as follows:

$$F_t(s) = \frac{1}{2} F(s) \cdot \frac{1 + 5^{-s}}{1 + 3 \cdot 5^{-s}} \text{ if } t \in \{1, 2\}. \tag{5.13}$$

Now suppose that $t \in \{5, 10\}$. Then we have

$$F_t(s) = \sum_{c=1}^{\infty} \frac{f_t(c)}{c^s} = \sum_{\substack{c=1 \\ \mathrm{ord}_5(c)=1}}^{\infty} \frac{4f_{\frac{t}{5}}(\frac{c}{5})}{c^s} = \frac{4}{5^s} \sum_{\substack{c_*=1 \\ 5 \nmid c_*}} \frac{f_{\frac{t}{5}}(c_*)}{c_*^s} = F(s) \cdot \frac{2}{5^s} \cdot \frac{1 - 5^{-s}}{1 + 3 \cdot 5^{-s}}. \tag{5.14}$$

Lastly, suppose that $t \in \{25, 50, 125, 250\}$. Then we have

$$\begin{aligned} F_t(s) &= \sum_{c=1}^{\infty} \frac{f_t(c)}{c^s} = \sum_{k=2}^{\infty} \sum_{\substack{c=1 \\ \mathrm{ord}_5(c)=k}}^{\infty} \frac{2 f_{\frac{t}{5^{\mathrm{ord}_5(e)}}}(\frac{c}{5^k})}{c^s} = \sum_{k=2}^{\infty} \frac{2}{5^{ks}} \sum_{\substack{c_*=1 \\ 5 \nmid c_*}} \frac{f_{\frac{t}{5^{\mathrm{ord}_5(t)}}}(c_*)}{c_*^s} \\ &= \sum_{k=2}^{\infty} \frac{2}{5^{ks}} \cdot \frac{1}{2} F(s) \cdot \frac{1 - 5^{-s}}{1 + 3 \cdot 5^{-s}} = F(s) \cdot \frac{1}{5^{2s}(1 + 3 \cdot 5^{-s})}. \end{aligned} \tag{5.15}$$

Hence, the analytic properties of $F_t(s)$ are identical to those of $F(s)$, which are obtained in the proof of Theorem 3.4. We note that the quantities σ_0 and δ_0 are scaled by $\frac{1}{4}$ because one needs to check the analytic properties of the L-function $L(f_t, s) = \frac{1}{2} F_t(s/4)$. □

Lemma 5.16. *For all $t \in \mathrm{md}$ and $0 \neq k \in 4\mathbb{Z}$, we have*

$$\left| \sum_{N\mathfrak{a} \leq H^2} \phi_t(\mathfrak{a}) \xi_k(\mathfrak{a}) \right| \ll \frac{H^{\frac{1}{2}}}{(\log H)^{1-c}} \cdot \log k,$$

as $H \to \infty$, where $c = \frac{3\sqrt{3}}{4\pi}$.

Proof. The lemma follows from adapting the proof of angular equidistribution of Gaussian integers, as demonstrated in [EH99]. Without loss of generality, we assume that $t = 1$, and abbreviate $\phi_1 = \phi$. The cases for other values of t follow analogously, where the implied constant satisfies $c \in (0, \frac{3\sqrt{3}}{4\pi}]$.

Given an ideal $\mathfrak{a} \in \mathcal{I}$, denote by $\overline{\mathfrak{a}}$ the ideal generated by the complex conjugate of its generator. Given a prime $p \equiv 1 \bmod 4$, we denote by θ_p the argument of a generator of the prime ideal of norm p lying in the first octant. Then because $\theta_{\mathfrak{a}} = \frac{\pi}{2} - \theta_{\overline{\mathfrak{a}}}$ and $\phi(\mathfrak{a}) = \phi(\overline{\mathfrak{a}})$, one can check that if $N\mathfrak{a} = p^\ell$ for some prime $p \equiv 1 \bmod 4$ and a positive integer ℓ, then

$$\phi(\mathfrak{a})\xi_k(\mathfrak{a}) + \phi(\overline{\mathfrak{a}})\xi_k(\overline{\mathfrak{a}}) = \begin{cases} 2\phi(\mathfrak{a}) \cos(k\ell\theta_p) & \text{if } p \nmid \mathfrak{a}, \\ 2\phi(\mathfrak{a}) \cos(k(\ell-2)\theta_p) & \text{if } p \mid\mid \mathfrak{a}, \\ 0 & \text{otherwise .} \end{cases}$$

Hence, we have for each p and k,

$$\sum_{\substack{\mathfrak{a} \in \mathcal{I} \\ N\mathfrak{a} = p^\ell}} \phi(\mathfrak{a})\xi_k(\mathfrak{a}) = 2\phi(\mathfrak{a})(\cos(k\ell\theta_p) + \cos(k(\ell-2)\theta_p)).$$

Using the fact that $\phi(\mathfrak{a})\xi_k(\mathfrak{a})$ is a multiplicative function, $\phi(\mathfrak{a}) = 0$ if the norm of $\mathfrak{a}$ is not a 4-th power, and $\phi(\mathfrak{a}) \leq 4$ for any ideal $\mathfrak{a}$ of norm a 4-multiple power of 5, we obtain:

$$\left| \sum_{N\mathfrak{a} \leq H^2} \frac{\phi(\mathfrak{a})\xi_k(\mathfrak{a})}{N\mathfrak{a}} \right| \leq 8 \cdot \left| \prod_{\substack{p \equiv 1 \bmod 4 \\ 13 \leq p \leq H^{\frac{1}{2}}}} \left(1 + \sum_{\ell=1}^{\infty} \frac{|\cos(k\ell\theta_p) + \cos(k(\ell-2)\theta_p)|}{p^\ell} \right) \right|.$$

We now focus on understanding the following expression:

$$\sum_{\substack{p \equiv 1 \bmod 4 \\ p \leq H^{\frac{1}{2}}}} |\cos(4k\theta_p) + \cos(2k\theta_p)|. \tag{5.16}$$

The period of a trigonometric function $y = \cos(4k\theta)+\cos(2k\theta)$ is equal to $\frac{\pi}{k}$, and in particular over the interval $E = [-\frac{\pi}{2k}, \frac{\pi}{2k}]$, the function is non-negative over the intervals $E_2 = [-\frac{\pi}{6k}, \frac{\pi}{6k}]$, and non-positive over the intervals $E_1 = [-\frac{\pi}{2k}, -\frac{\pi}{6k}]$ and $E_3 = [\frac{\pi}{6k}, \frac{\pi}{2k}]$. Note that at the boundaries of the intervals E_1, E_2, and E_3, we have $\cos(4k\theta) + \cos(2k\theta) = 0$. Equation (5.16) can hence be rewritten as

$$(5.16) = \frac{k}{4} \sum_{\substack{p\equiv 1 \bmod 4 \\ p\leq H^2}} \sum_{i=1}^{3} (-1)^i \cdot \left(\sum_{\theta_p \in E_i} \int_{\theta_p}^{e_i^{sup}} 4k\sin(4k\phi) + 2k\sin(2k\phi) d\phi \right)$$

where $e_i^{sup} := \sup\{x \mid x \in E_i\}$. Note that the extra term $\frac{k}{4}$ originates from the fact that the period of the function $y = \cos(4k\theta) + \cos(2k\theta)$ is equal to $\frac{\pi}{k}$, and that θ_p lies in the first octant of the xy-plane. By Fubini's theorem, we obtain

$$(5.16) = \frac{k}{4} \sum_{i=1}^{3} (-1)^i \cdot \left(\int_{E_i} \left[\sum_{\substack{p\equiv 1 \bmod 4 \\ p\leq H^{\frac{1}{2}} \\ e_i^{inf} < \theta_p \leq \phi}} 1 \right] \times (4k\sin(4k\phi) + 2k\sin(2k\phi)) d\phi \right)$$

where $e_i^{inf} := \inf\{x \mid x \in E_i\}$.

To evaluate the integrals, we recall Kubilius's theorem [Kub50].

Theorem 5.17 ([Kub50]). *The number of Gaussian prime ideals $\mathfrak{w}$ in the sector $0 \leq \alpha \leq arg(\mathfrak{w}) \leq \beta \leq 2\pi$, and $\operatorname{Nm}\mathfrak{w} \leq u$ is equal to:*

$$\frac{2}{\pi}(\beta - \alpha) \int_2^u \frac{dv}{\log v} + O(uExp[-b \cdot \sqrt{\log u}]) \tag{5.17}$$

where b is a positive absolute constant.

Kubilius's theorem allows us to rewrite the desired sum as

$$\begin{aligned}(5.16) &= \frac{k}{4} \left[\frac{2}{\pi} \int_2^{H^{\frac{1}{2}}} \frac{dv}{\log v} \right] \cdot \left(\sum_{i=1}^{3} (-1)^i \cdot \int_{E_i} (\phi - e_i^{inf})(4k\sin(4k\phi) + 2k\sin(2k\phi)) d\phi \right) \\ &\quad + O(kH^{\frac{1}{2}} e^{-b\sqrt{\log H}}) \\ &= c \int_2^{H^{\frac{1}{2}}} \frac{dv}{\log v} + O(kH^{\frac{1}{2}} e^{-b\sqrt{\log H}}).\end{aligned}$$

where

$$c = \frac{k}{2\pi} \cdot \left(\frac{3\sqrt{3}}{8k} + \frac{3\sqrt{3}}{4k} + \frac{3\sqrt{3}}{8k} \right) = \frac{3\sqrt{3}}{4\pi}.$$

Using Abel's partial summation formula, for any $2 \leq \omega \leq H^{\frac{1}{2}}$, we obtain

$$\sum_{\substack{p\equiv 1 \bmod 4 \\ p\leq H^{\frac{1}{2}}}} \frac{1}{p} |\cos(4k\theta_p) + \cos(2k\theta_p)| \leq \frac{1}{2} \log\log w + c \log\left(\frac{\log H^{\frac{1}{2}}}{\log \omega} \right) + O(1) + O(k \cdot e^{-b\sqrt{\log w}}).$$

We may choose $\omega = (\frac{1}{b} \cdot \log k)^2$ to get a uniform bound for $0 \neq k \in 4\mathbb{N}$:

$$\sum_{\substack{p \equiv 1 \bmod 4 \\ p \leq H^{\frac{1}{2}}}} \frac{1}{p} |\cos(4k\theta_p) + \cos(2k\theta_p)| \leq c \log\log H + (1-2c)\log\log k + O(1).$$

Hence, we obtain

$$\left| \sum_{N\mathfrak{a} \leq H^2} \frac{\phi(\mathfrak{a})\xi_k(\mathfrak{a})}{N\mathfrak{a}} \right| \ll (\log H)^c \cdot (\log k)^{1-2c},$$

which in turn implies (as $H \to \infty$),

$$\left| \sum_{N\mathfrak{a} \leq H^2} \phi(\mathfrak{a})\xi_k(\mathfrak{a}) \right| \ll \frac{H^{\frac{1}{2}}}{(\log H)^{1-c}} (\log k)^{1-2c} \ll \frac{H^{\frac{1}{2}}}{(\log H)^{1-c}} (\log k).$$

□

With the two conditions for the main analytic lemma satisfied, we are able to prove the desired point count estimates for $N_5^{tw}(H, e)$.

Proof of Theorem 5.13. Recall the compact region

$$\mathcal{R}_5 := \left\{ (x, y) \in \mathbb{R}^2 \colon H\left(x, y, \sqrt[4]{x^2 + y^2}\right) \leq 1 \right\}.$$

Equivalently, the region is a compact region bounded by the following function in polar coordinates

$$r := r_5(\theta) := \frac{1}{12} \frac{1}{\left(\max\{\frac{1}{2} \cdot |123\cos\theta + 114\sin\theta + 125|^3, |2502\cos\theta + 261\sin\theta + 2500|^2\}\right)^{\frac{1}{3}}}.$$

We note that the above function is well defined because the denominator is positive.

Define $\sqrt[4]{\mathcal{R}_5}$ to be the region whose radius function is given by $r_5(\theta)^{1/4}$. Note that

$$\mathrm{vol}(\sqrt[4]{\mathcal{R}_5}) = \frac{1}{2} \int_0^{2\pi} \sqrt{r_5(\theta)} d\theta. \tag{5.18}$$

We subdivide the compact region into four sub-regions $\sqrt[4]{\mathcal{R}_5}^{(i)}, \sqrt[4]{\mathcal{R}_5}^{(ii)}, \sqrt[4]{\mathcal{R}_5}^{(iii)}, \sqrt[4]{\mathcal{R}_5}^{(iv)}$ based on over which quadrant $\sqrt[4]{\mathcal{R}_5}$ lies in. More explicitly,

$$\begin{aligned}
\sqrt[4]{\mathcal{R}_5}^{(i)} &:= \left\{ (x, y) \in \sqrt[4]{\mathcal{R}_5} \colon x > 0, y > 0 \right\}, \\
\sqrt[4]{\mathcal{R}_5}^{(ii)} &:= \left\{ (x, y) \in \sqrt[4]{\mathcal{R}_5} \colon x < 0, y > 0 \right\}, \\
\sqrt[4]{\mathcal{R}_5}^{(iii)} &:= \left\{ (x, y) \in \sqrt[4]{\mathcal{R}_5} \colon x < 0, y < 0 \right\}, \\
\sqrt[4]{\mathcal{R}_5}^{(iv)} &:= \left\{ (x, y) \in \sqrt[4]{\mathcal{R}_5} \colon x > 0, y < 0 \right\}.
\end{aligned}$$

Denote by $\Omega^{(i)}, \Omega^{(ii)}, \Omega^{(iii)}, \Omega^{(iv)}$ the squareish regions obtained from rotating the four sub-regions above by multiples of $\pi/2$. We note that

$$\mathrm{vol}(\sqrt[4]{\mathcal{R}_5}) = \frac{1}{4}\left(\mathrm{vol}(\Omega^{(i)}) + \mathrm{vol}(\Omega^{(ii)}) + \mathrm{vol}(\Omega^{(iii)}) + \mathrm{vol}(\Omega^{(iv)})\right).$$

For each $t \in \mathrm{md}$, the proof of Lemma 5.15 implies that the residues of the Dirichlet series $F_t(s)$ at $s = 1$ are given by

$$\mathrm{Res}_{s=1}(F_t(s)) = \begin{cases} \frac{3}{8} f_1 & \text{if } t \in \{1, 2\}, \\ \frac{1}{5} f_1 & \text{if } t \in \{5, 10\}, \\ \frac{1}{40} f_1 & \text{if } t \in \{25, 50, 125, 250\}, \end{cases} \tag{5.19}$$

where we recall that $f_1 = \mathrm{Res}_{s=1}(F(s))$.

By the main analytic lemma (Lemma 4.2), there exists a monic polynomial $P(T)$ of degree one such that as $H \to \infty$, we have

$$N_{\sqrt[4]{\mathcal{R}_5}}(H; f_t) = \begin{cases} \frac{3}{4} \cdot \frac{\mathrm{vol}(\sqrt[4]{\mathcal{R}_5})}{\mathrm{vol}(\mathbb{D})} \cdot f_1 \cdot H^{\frac{1}{2}} P(\log H) + O(H^{\frac{1}{2}} \cdot (\log H)^{-1+c}) & \text{if } t \in \{1, 2\}, \\ \frac{2}{5} \cdot \frac{\mathrm{vol}(\sqrt[4]{\mathcal{R}_5})}{\mathrm{vol}(\mathbb{D})} \cdot f_1 \cdot H^{\frac{1}{2}} P(\log H) + O(H^{\frac{1}{2}} \cdot (\log H)^{-1+c}) & \text{if } t \in \{5, 10\}, \\ \frac{1}{20} \cdot \frac{\mathrm{vol}(\sqrt[4]{\mathcal{R}_5})}{\mathrm{vol}(\mathbb{D})} \cdot f_1 \cdot H^{\frac{1}{2}} P(\log H) + O(H^{\frac{1}{2}} \cdot (\log H)^{-1+c}) & \text{if } t \in \{25, 50, 125, 250\}. \end{cases}$$

It remains to determine which bound H one needs to use in order to recover the counting function $N_5^{tw}(H, t)$. We note that the naive height function $H(a, b, c)$ such that $a + bi$ generates $\mathfrak{a} \in \mathcal{I}$ satisfies

$$H(a, b, c) = 2^6 \cdot 3^3 \cdot c^6 \cdot \frac{1}{(12 r_5(\theta_{\mathfrak{a}}))^3}.$$

This implies that

$$N_5^{tw}(H, t) = N_{\sqrt[4]{\mathcal{R}_5}}\left(\frac{H^{\frac{1}{3}}}{12}; f_t\right),$$

from which the statement of the theorem follows. □

5.3. **Proof of Theorem 1.1.** The proof of Theorem 1.1 will be analogous to the idea of the proof presented in Section 3.2. However, there is a technical subtlety where the Weierstrass model of the elliptic curve $E_{a,b,c}$ obtained from a minimal triple (a, b, c) may not be of minimal form. Using the twist minimal defect of (a, b, c) introduced in the previous section, we completely classify the extents to which the models of $E_{a,b,c}$ are far from being minimal.

Check Section 5.3.

Given $t \in \mathrm{md}$ and every square free $e \in \mathbb{Z}$, let

$$g_t^{(e)}(n) := \#\{(a, b, c) \in \mathbb{Z}^3 \colon (e^2 a, e^2 b, ec) \in \mathcal{G}\langle\mathbb{Q}\rangle, \mathrm{md}(a, b, c) = t, \text{ and } |ec| = n\} \tag{5.20}$$

Given a Weierstrass model of an elliptic curve $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, we denote by $\mathrm{md}(E)$ the minimality defect of E defined as

$$\mathrm{md}(E) := \max\{e \in \mathbb{Z} \colon e^4 \mid A \text{ and } e^6 \mid B\}. \tag{5.21}$$

The new model $\tilde{E} : y^2 = x^3 + \frac{A}{\mathrm{md}(E)^4} x + \frac{B}{\mathrm{md}(E)^6}$ is the minimal Weierstrass model for E.

Lemma 5.18. *Let $(a, b, c) \in \mathbb{Z}^3$ be a twist minimal Fermat triple.*

- *The following table classifies the 2-valuation of the minimality defect of $E_{e^2 a, e^2 b, ec}$ given a square free integer e and twist minimal error $\mathrm{md}(a, b, c) = t$.*
- *The following table classifies the 5-valuation of the minimality defect of $E_{e^2 a, e^2 b, ec}$ given a square free integer e and twist minimal error $\mathrm{md}(a, b, c) = t$.*

$\mathrm{ord}_2(\mathrm{md}(a,b,c))$	$\mathrm{ord}_2(e)$	$\mathrm{ord}_2(A(e^2a,e^2b,ec))$	$\mathrm{ord}_2(B(e^2a,e^2b,ec))$	$\mathrm{ord}_2(\mathrm{md}(E_{e^2a,e^2b,ec}))$
0	0	1	3	0
0	1	3	6	0
1	0	≥ 2	4	0
1	1	≥ 4	7	1

$\mathrm{ord}_5(\mathrm{md}(a,b,c))$	$\mathrm{ord}_5(e)$	$\mathrm{ord}_5(A(e^2a,e^2b,ec))$	$\mathrm{ord}_5(B(e^2a,e^2b,ec))$	$\mathrm{ord}_5(\mathrm{md}(E_{e^2a,e^2b,ec}))$
0	0	0	0	0
0	1	2	3	0
1	0	3 *or* 4	4 *or* 5	0
1	1	5 *or* 6	7 *or* 8	1
2	0	5	$k+7, k\geq 2$	1
2	1	7	$k+10, k\geq 2$	1
3	0	6	9 *or* $k+8, k\geq 3$	1
3	1	8	12 *or* $k+11, k\geq 3$	2

Proof. The entries of the table are obtained from using Proposition 5.5 and the fact that $A(e^2a,e^2b,ec) = e^2A(a,b,c)$ and $B(e^2a,e^2b,ec) = e^3B(a,b,c)$. □

We note that the valuation of the minimality defect $\mathrm{md}(E)$ determines how much the upper bound on the naive height must be scaled in order to obtain the explicit leading coefficient term for the asymptotic point count estimate $N_5(H)$. To systematically understand these differences in upper bounds, we introduce some new definitions.

Pick $t \in \mathrm{md}$ and $u := (u_2, u_5) \in \{0,1\}^{\oplus 2}$. Given a minimal triple $(a,b,c) \in \mathcal{G}\langle\mathbb{Q}\rangle$, we define

$$(a,b,c)_u := \left(\frac{a}{2^{2u_2}5^{2u_5}}, \frac{b}{2^{2u_2}5^{2u_5}}, \frac{c}{2^{u_2}5^{u_5}}\right) \in \mathcal{F}\langle\mathbb{Q}\rangle.$$

We denote by $g_{t,u}(n)$ the minimality defect arithmetic height function defined as

$$g_{t,u}(n) := \#\{(a,b,c) \in \mathcal{G}\langle\mathbb{Q}\rangle : \ \mathrm{md}((a,b,c)_u) = t \text{ and } |c| = n\}. \tag{5.22}$$

Associated to the arithmetic height function is the minimality defect height zeta function

$$G_{t,u}(s) := \sum_{n=1}^{\infty} \frac{g_{t,u}(n)}{n^s}. \tag{5.23}$$

We summarize the analytic properties of $G_{t,u}(s)$ as follows.

Theorem 5.19. *The following statements hold for every $t \in \mathrm{md}$ and $u \in \{0,1\}$.*

(1) In the half-plane $\mathrm{Re}(s) > 1$ we have a

$$G_{t,u}(s) = \begin{cases} 4\frac{\zeta(s)}{\zeta(2s)} \cdot \frac{1}{1+2^{-s}} \cdot \frac{1}{1+5^{-s}} \cdot F_t(s) & \text{if } u = (0,0), \\ 4\frac{\zeta(s)}{\zeta(2s)} \cdot \frac{2^{-s}}{1+2^{-s}} \cdot \frac{1}{1+5^{-s}} \cdot F_t(s) & \text{if } u = (1,0), \\ 4\frac{\zeta(s)}{\zeta(2s)} \cdot \frac{1}{1+2^{-s}} \cdot \frac{5^{-s}}{1+5^{-s}} \cdot F_t(s) & \text{if } u = (0,1), \\ 4\frac{\zeta(s)}{\zeta(2s)} \cdot \frac{2^{-s}}{1+2^{-s}} \cdot \frac{5^{-s}}{1+5^{-s}} \cdot F_t(s) & \text{if } u = (1,1). \end{cases}$$

(2) The function $G_{t,u}(s)$ admits meromorphic continuation to the half plane $Re(s) > 1/2$ with a triple pole at $s = 1$ and no other singularities.

Proof. We proceed as in Section 3.2. For every square free $e \in \mathbb{Z}$, let

$$g_{t,u}^{(e)}(n) := \#\{(a,b,c) \in \mathbb{Z}^3 \colon (e^2a, e^2b, ec) \in \mathcal{G}\langle\mathbb{Q}\rangle, \mathrm{md}(a,b,c) = t, \mathrm{ord}_2(e) = u_2, \mathrm{ord}_5(e) = u_5\}.$$

Then by definition, we have

$$g_{t,u}^{(e)}(n) = \begin{cases} 2f_t(n/|e|) & \text{if } e \mid n, \mathrm{ord}_2(e) = u_2, \text{ and } \mathrm{ord}_5(e) = u_5, \\ 0 & \text{otherwise.} \end{cases}$$

We then use the relation

$$g_{t,u}(n) = \sum_{\substack{e \in \mathbb{Z}, \square free \\ \mathrm{ord}_2(e) = u_2 \\ \mathrm{ord}_5(e) = u_5}} g_{t,u}^{(e)}(n) = 4 \sum_{\substack{e \in \mathbb{Z} \\ \mathrm{ord}_2(e) = u_2 \\ \mathrm{ord}_5(e) = u_5}} \mu^2(e) f_t(n/e)$$

to complete the proof of (1). Statement (2) follows from the identity $F(s) = \zeta(s)^2 P(s)$. □

We now have all the ingredients to prove Theorem 1.1.

Proof of Theorem 1.1. Assuming that the upper bound on the naive height $t = 1$ and $u = (0,0)$ is given by H, the corresponding upper bounds on naive heights, which we will denote as $H_{t,u}$, can be computed as in Table 4 using Lemma 5.18. The coefficients for H are determined by the minimality defects $\mathrm{md}(E_{a,b,c})$ obtained for each choice of t and u.

(u_2, u_5)	1	2	5	10	25	50	125	250
(0,0)	H	H	H	H	5^6H	5^6H	5^6H	5^6H
(1,0)	H	2^6H	H	2^6H	5^6H	10^6H	5^6H	10^6H
(0,1)	H	H	5^6H	5^6H	5^6H	5^6H	25^6H	25^6H
(1,1)	H	2^6H	5^6H	10^6H	5^6H	10^6H	25^6H	50^6H

TABLE 4. Upper bound on naive heights $H_{t,u}$ depending on the choice of t and u

By Theorem 5.19, and Equation (5.19), the residues of the minimality defect height zeta functions $G_{t,u}(s)$ for each t and u, denoted as $g_{1,t,u}$, are computed as in Table 5.

(u_2, u_5)	$t = 1, 2$	$t = 5, 10$	$t = 25, 50, 125, 250$
(0,0)	$\frac{5}{2\pi^2} \cdot f_1$	$\frac{4}{3\pi^2} \cdot f_1$	$\frac{1}{6\pi^2} \cdot f_1$
(1,0)	$\frac{5}{4\pi^2} \cdot f_1$	$\frac{2}{3\pi^2} \cdot f_1$	$\frac{1}{12\pi^2} \cdot f_1$
(0,1)	$\frac{1}{2\pi^2} \cdot f_1$	$\frac{4}{15\pi^2} \cdot f_1$	$\frac{1}{30\pi^2} \cdot f_1$
(1,1)	$\frac{1}{4\pi^2} \cdot f_1$	$\frac{2}{15\pi^2} \cdot f_1$	$\frac{1}{60\pi^2} \cdot f_1$

TABLE 5. Residues $g_{1,t,u}$ of minimality defect height zeta functions $G_{t,u}(s)$

By the main analytic lemma (Lemma 4.2) and Theorem 5.13, we obtain that for each $t \in \mathrm{md}$ and $u \in \{0,1\}^{\oplus 2}$ there exists a monic polynomial $P_{t,u}(T)$ of degree two such that

$$N_{\sqrt[4]{\mathcal{R}_5}}(H; g_{t,u}) = 4g_{1,t,u}\frac{\mathrm{vol}(\sqrt[4]{\mathcal{R}_5})}{\pi}H^{\frac{1}{2}}P_{t,u}(\log H) + O(H^{\frac{1}{2}}(\log H)^{-(1-c)}), \text{ as } H \to \infty,$$

where $c = \frac{3\sqrt{3}}{4\pi}$ obtained from Lemma 5.16.

We now use the summation

$$N_5(H) = \sum_{t \in \mathrm{md}} \sum_{u \in \{0,1\}^{\oplus 2}} N_{\sqrt[4]{\mathcal{R}_5}}\left(\frac{H_{t,u}^{\frac{1}{3}}}{12}; g_{t,u}\right) \tag{5.24}$$

to conclude that there exists a monic polynomial $P_5(T)$ of degree 2 such that

$$N_5(H) = \frac{245}{9\pi^3\sqrt{3}} \cdot \mathrm{vol}(\sqrt[4]{\mathcal{R}_5}) \cdot f_1 \cdot H^{\frac{1}{6}}P_5(\log H) + O(H^{\frac{1}{6}}(\log H)^{-(1-c)}), \text{ as } H \to \infty. \tag{5.25}$$

□

5.4. **The constant term.** Let $r_5(\theta) > 0$ be the function giving the radius of the region $\mathcal{R}_5$ defined in Equation (5.1):

$$r_5(\theta) := \frac{1}{12}\frac{1}{\left(\max\{\frac{1}{2}\cdot|123\cos\theta + 114\sin\theta + 125|^3, |2502\cos\theta + 261\sin\theta + 2500|^2\}\right)^{\frac{1}{3}}}.$$

Define $\sqrt[4]{\mathcal{R}_5}$ to be the region whose radius function is given by $r_5(\theta)^{1/4}$. A numerical approximation of the integral, implemented on Magma and Pari/GP, is given by

$$\mathrm{vol}(\sqrt[4]{\mathcal{R}_5}) = \frac{1}{2}\int_0^{2\pi}\sqrt{r_5(\theta)}\,\mathrm{d}\theta \approx 0.097115406944\ldots \tag{5.26}$$

References

[AGV08] Dan Abramovich, Tom Graber, and Angelo Vistoli, *Gromov-Witten theory of Deligne-Mumford stacks*, Amer. J. Math. **130** (2008), no. 5, 1337–1398. MR 2450211

[AH11] Dan Abramovich and Brendan Hassett, *Stable varieties with a twist*, Classification of algebraic varieties, EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich, 2011, pp. 1–38. MR 2779465

[BGS20] L. Beshaj, J. Gutierrez, and T. Shaska, *Weighted greatest common divisors and weighted heights*, J. Number Theory **213** (2020), 319–346. MR 4091944

[Bru92] Armand Brumer, *The average rank of elliptic curves. I*, Invent. Math. **109** (1992), no. 3, 445–472. MR 1176198

[BS24] Brandon Boggess and Soumya Sankar, *Counting elliptic curves with a rational n-isogeny for small n*, Journal of Number Theory **262** (2024), 471–505.

[CKV22] 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

[CLR21] 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

[CLT01] Antoine Chambert-Loir and Yuri Tschinkel, *Fonctions zêta des hauteurs des espaces fibrés*, Rational points on algebraic varieties, Progr. Math., vol. 199, Birkhäuser, Basel, 2001, pp. 71–115. MR 1875171

[Coh07] Henri Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007. MR 2312338

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques.*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972),, Lecture Notes in Math., Vol. 349,, ,, 1973, pp. 143–316. MR 337993

[Duk97] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818. MR 1485897

[DY22] Ratko Darda and Takehiko Yasuda, *The batyrev-manin conjecture for dm stacks*, 2022.

[EH99] P. Erdos and R. Hall, *On the angular distribution of gaussian integers wiht fixed norm*, Discrete Mathematics **200** (1999), no. 1-3, 87–94.

[ESZB23] Jordan S. Ellenberg, Matthew Satriano, and David Zureick-Brown, *Heights on stacks and a generalized Batyrev-Manin-Malle conjecture*, Forum Math. Sigma **11** (2023), Paper No. e14, 54. MR 4557890

[Gra00] David Grant, *A formula for the number of elliptic curves with exceptional primes*, Compositio Math. **122** (2000), no. 2, 151–164. MR 1775416

[HS17] Robert Harron and Andrew Snowden, *Counting elliptic curves with prescribed torsion*, J. Reine Angew. Math. **729** (2017), 151–170. MR 3680373

[IK04] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR 2061214

[Kub50] J. Kubilius, *The distribution of gaussian primes in sectors and contours*, Leningrad Gos. Univ. Uc. Zap. 137 Ser. Mat. Nauk 19 (1950), 40–52.

[LM25] Alessandro Languasco and Pieter Moree, *Easy counting of irreducible self-reciprocal polynomials over a finite field and partial Euler products*, 2025.
[LS24] Daniel Loughran and Tim Santens, *Malle's conjecture and brauer groups of stacks*, 2024.
[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230
[Mol24] Grant Molnar, *Counting elliptic curves with a cyclic m-isogeny over $\mathbb{Q}$*, 2024.
[MV23] Grant Molnar and John Voight, *Counting elliptic curves over the rationals with a 7-isogeny*, Res. Number Theory **9** (2023), no. 4, Paper No. 75, 31. MR 4661854
[Ols16] Martin Olsson, *Algebraic spaces and stacks*, American Mathematical Society Colloquium Publications, vol. 62, American Mathematical Society, Providence, RI, 2016. MR 3495343
[PPV20] 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
[PS21] 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
[Č17] Kęstutis Česnavičius, *A modular description of $\mathcal{X}_0(n)$*, Algebra Number Theory **11** (2017), no. 9, 2001–2089. MR 3735461
[VZB22] John Voight and David Zureick-Brown, *The canonical ring of a stacky curve*, Mem. Amer. Math. Soc. **277** (2022), no. 1362, v+144. MR 4403928

Department of Mathematics, Emory University, Atlanta, GA 30322, USA
Email address: santiago.arango@emory.edu
URL: https://sarangop1728.github.io/

Department of Mathematics, Korea University, Seoul, South Korea
Email address: changho_han@korea.ac.kr
URL: https://sites.google.com/view/changho-han

Max-Planck-Institut für Mathematik, Bonn, Germany
Email address: opadurariu@mpim-bonn.mpg.de
URL: https://sites.google.com/view/oanapadurariu/home

Max-Planck-Institut für Mathematik, Bonn, Germany
Email address: s.park@mpim-bonn.mpg.de
URL: https://sites.google.com/wisc.edu/spark483