COUNTING ODD GENUS 2 CURVES WITH A MARKED RATIONAL 3-TORSION POINT

ELVIRA LUPOIAN AND LAZAR RADIČEVIĆ

Abstract. In this paper we count, ordered by naive height, the genus 2 curves over the rationals which admit a monic Weierstrass model of odd degree and whose Jacobian has a marked rational 3-torsion point.

1. Introduction

Let A be an abelian variety defined over $\mathbb{Q}$. The Mordell-Weil theorem states that the group of rational points $A(\mathbb{Q})$ is finitely generated. Beyond elliptic curves, our understanding of the possible rank or torsion of A is limited. An interesting, and more approachable problem, is that of counting abelian varieties whose Mordell-Weil group exhibits certain properties.

Recently, the problem of counting elliptic curves with prescribed level structure has been rather popular. Harron and Snowden [11] determined the frequency with which each torsion subgroup in Mazur's classification [12] occurs. A number of works count elliptic curves with a marked N-isogeny. Boggess-Sankar [1] count elliptic curves with a rational N-isogeny for $N \in \{2, 3, 4, 5, 6\}$, Pizzo-Pomerance-Voight [15] count elliptic curves with a rational isogeny of degree 3, Molnar-Voight [13] count those with a 7-isogeny and Arrango-Han-Padurariu those with a 5-isogeny. Variations of this problem have been considered for other level structures and other fields, for instance in [16], [3], [9], [6], [5].

Very often the problem of counting level-structures reduces to the problem of counting points of bounded height on weighted projective stacks. A number of recent results focus on studying this problem. Phillips [14] gives asymptotics for the number of rational points in the domain of a morphism of weighted projective stacks, and uses this to count elliptic curves with certain level structures. Asymptotics for points on the modular stack of elliptic curves with specified cyclic isogeny are studied by Darda and Han [7].

Beyond the elliptic curve case, Genao, Phillips, Saia, Santens, and Yin [10] count principally polarized abelian surfaces with quaternionic multiplication, or potential quaternionic multiplication, by reducing to counting points on certain genus-zero Shimura curves and their Atkin–Lehner quotients. Chan, Loughran, and Rome [4] show that almost all odd hyperelliptic curves have Jacobians admitting no prescribed level-G structure, under mild hypotheses on the level structure. To the best of our knowledge, the present paper is the first to determine an exact asymptotic formula for the number of curves with prescribed level structure in a setting where the moduli variety is not a curve.

1.1. Main Result.

In this paper we study genus 2 curves with a marked rational 3-torsion point on the Jacobian. The setup of our problems is as follows.

For a square-free polynomial

$$f(x) = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$$

2020 *Mathematics Subject Classification.* 11N45, 11G10, 11D45, 11G50.

we write $C_f/\mathbb{Q}$ for the genus 2 curve with a Weierstrass model $y^2 = f(x)$ and J_f for the Jacobian of C_f. We define the *height of* f to be

$$H(f) = \max\{|a_3|^{1/4}, |a_2|^{1/6}, |a_1|^{1/8}, |a_0|^{1/10}\}.$$

We say that f is *minimal* if there is no prime p such that $p^{10-2i}|a_i$ for all $0 \le i \le 3$.

For $X \in \mathbb{R}_{\ge 0}$, we write $\mathcal{W}^{\mathrm{mark}}(X)$ for the set of pairs (f, T), where

(1) $f = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ is square-free and minimal;
(2) $H(f) \le X$;
(3) $0 \ne T \in J_f(\mathbb{Q})[3]$.

Our main result is the following.

Theorem 1.1. *There exists a positive, effectively computable constant c such that*

$$\#\mathcal{W}^{\mathrm{mark}}(X) = cX^{10} + o(X^{10}).$$

More precisely,

$$c = \mathrm{Vol}(\mathcal{R}(1))\,\beta_{2,3}\prod_{p\ge 5}(1 - p^{-10}), \tag{1.1}$$

where $\mathcal{R}(1)$ is a compact subset of $\mathbb{R}^4$ defined in Section 3, and $\beta_{2,3} > 0$ is the effectively computable local density at the primes 2 and 3, defined in Section 5.

A degree 5 monic integral equation as above determines a genus 2 curve $C/\mathbb{Q}$ with a marked rational Weierstrass point at infinity. Every pair (C, P) consisting of a genus two curve $C/\mathbb{Q}$ and a rational Weierstrass point P can be defined by such an equation, and two such equations $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$ and $y^2 = x^5 + a_3'x^3 + a_2'x^2 + a_1'x + a_0'$ define isomorphic curves if and only if there exists $u \in \mathbb{Q}^\times$ such that $a_i' = u^{10-2i}a_i$ for $0 \le i \le 3$. It follows that any pair (C, P) can be represented by a unique minimal integral f, and so we can view Theorem 1.1 as counting triples (C, P, T) where $T \in \mathrm{Jac}\,C[3]$ is a non-trivial 3-torsion point. The extra data of a Weierstrass point rigidifies the moduli problem and allows us to introduce a simple height function.

1.2. **Methodology.** The main ingredient in our proof is a parametrisation of $(f, T) \in \mathcal{W}^{\mathrm{mark}}(X)$ which is well suited to classical counting methods using the geometry of numbers. We prove the following.

Proposition 1.2. *There exist weighted homogeneous polynomials*

$$\Theta_0(A, B, J, E), \Theta_1(A, B, J, E), \Theta_2(A, B, J, E), \Theta_3(A, B, J, E) \in \mathbb{Z}[A, B, J, E]$$

with no common zeros except $(0, 0, 0, 0)$, which parametrise the set of pairs (f, T), where f is a monic, square-free degree 5 polynomial and T is a marked 3-torsion point on the Jacobian of the genus 2 curve defined by $y^2 = f(x)$.

For the explicit definition of $\Theta_0, \dots, \Theta_3$ see (2.6)–(2.9), and for the precise statement see Proposition 2.2, where we show that for any (f, T) as above,

$$f(x) = F_P(x) = x^5 + \frac{\Theta_3(P)}{729}x^3 + \frac{\Theta_2(P)}{729}x^2 + \frac{\Theta_1(P)}{729}x + \frac{\Theta_0(P)}{729}$$

for some $P = (A, B, J, E)$ defined in terms of the coefficients of f. The marked 3-torsion point T is represented by a divisor cut out by a function whose coefficients are determined by P.

To prove our result, we derive necessary and sufficient conditions on $P = (A, B, J, E)$ to ensure that $(f, T) = (F_P, T_P) \in \mathcal{W}^{\mathrm{mark}}(X)$. The requirements that $f(x) \in \mathbb{Z}[x]$ and that $f(x)$ is minimal correspond to $F_P(x)$ being p-integral and p-minimal for all primes p (see §4 for

definitions). We derive congruence conditions on (A, B, J, E) characterising these properties. This essentially reduces the problem to counting rational points of bounded height on the weighted projective space $\mathbb{P}(1, 2, 3, 4)$, which we do using the geometry of numbers.

Finding the parametrisation $\Theta_0, \dots, \Theta_3$ was the main challenge of this paper. To explain the issue, it is helpful to first consider the analogous problem of counting elliptic curves with a marked rational 3-torsion point treated in [11]. We consider Weierstrass equations

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

ordered by the height function $H(A, B) = \max(|A|^{1/4}, |B|^{1/6})$, and the problem of counting minimal equations with a marked rational 3-torsion point. Every elliptic curve over $\mathbb{Q}$ with a marked rational 3-torsion point T can be put into Tate normal form

$$y^2 + uxy + vy = x^3,$$

with $T = (0, 0)$. Conversely, any such pair $(u, v) \in \mathbb{Q}^2$ with $\Delta(u, v) = (u^3 - 27v)v^3 \neq 0$ defines an elliptic curve with a marked 3-torsion point $(0, 0)$. This is the universal elliptic curve over the affine modular curve $Y_1(3)$. To count short Weierstrass equations with a marked 3-torsion point, we transform the Tate normal form into short Weierstrass form $y^2 = x^3 + c_4(u, v)x + c_6(u, v)$, where c_4 and c_6 are polynomials in u and v, that don't have any common zeros besides $(0, 0)$. It follows that they define a morphism from the compactified modular curve $\mathbb{P}(1, 3) \to \mathbb{P}(4, 6)$. Together with a sieve argument, this reduces the problem to counting integer solutions to the inequality $H(c_4(u, v), c_6(u, v)) \leq X$.

Our genus 2 argument follows the same general strategy. The first step is to write down a rational parametrisation of the family of genus 2 curves with a marked rational 3-torsion point. This shows the modular threefold, which plays the role of the affine modular curve Y in the elliptic curve setting, is birational to the affine 3-space. The tricky part is the analogue of passing from Y to X. To reduce the problem to counting lattice points in a bounded region, we need to compactify the threefold Y into a weighted projective space X in such a way that the rational map from Y to $\mathbb{P}(4, 6, 8, 10)$ extends to a morphism $X \to \mathbb{P}(4, 6, 8, 10)$. We have managed to find such a compactification, and we show that we can take $X = \mathbb{P}(1, 2, 3, 4)$. In the modular curve case, any rational map from a smooth projective curve extends to a morphism, and so this problem is easy to solve, but this is no longer true for higher dimensional varieties. In our case, naively homogenising the formulas will only define a rational map on the compactification, not a morphism.

Our construction is somewhat ad-hoc, and it would be interesting to understand it better, as we expect similar problems to arise when counting curves with more general level structures. For example, one can consider the family of curves (C, P), where C is a hyperelliptic curve of genus g and P is a rational Weierstrass point. In this setting, the analogue of Proposition 2.1 holds, and the affine parameter space is easy to describe; the more delicate issue is to find, if it exists, a weighted projective compactification on which the map to the underlying Weierstrass model is base-point-free, and which therefore reduces the problem to counting lattice points in a compact weighted box.

1.3. **Outline.** This paper is organised as follows. In Section 2 we construct the weighted homogeneous parametrisation of monic degree 5 Weierstrass equations with a marked 3-torsion point. In Section 3 we use this parametrisation to define a compact subset in $\mathbb{R}^4$ in which we count lattice points. In Section 4 we determine the congruence conditions which characterise lattice points that define minimal Weierstrass equations. In Section 5 we combine these ingredients in a sieve and prove Theorem 1.1. The appendix contains `MAGMA` code used to carry out the Groebner basis computations needed in Section 3 and Section 4.

Acknowledgments. We thank Netan Dogra for organising the seminar at which our collaboration began. We thank Ratko Darda and John Voight for helpful conversations. The first author is supported by the EPSRC Doctoral Prize fellowship EP/W524335/1 and the extension UKRI3030. The second author was supported by the Mathematical Institute of Serbian Academy of Sciences and by the UKRI grant MR/T041609/2 during his stay at King's College London.

2. The parametrisation

We begin by recalling the elementary affine description of odd, monic, genus 2 curves with a marked 3-torsion point. A similar description appears in [2, Lemma 3].

Proposition 2.1. *Let K be a field of characteristic different from 2, and let*

$$f(x) = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x]$$

be square-free. Put $C_f : y^2 = f(x)$. Non-zero points $T \in \mathrm{Jac}(C_f)(K)[3]$ are in bijection with triples (A, G, H) where $A \in K^\times$, $G \in K[x]$ is monic of degree 3, $H \in K[x]$ is monic of degree 2, and

$$G(x)^2 - A^2 f(x) = H(x)^3. \tag{2.1}$$

The 3-torsion point corresponding to (A, G, H) is $[D - 2\infty]$, where D is the divisor cut out by

$$H(x) = 0, \qquad Ay = G(x).$$

Proof. Let $0 \neq T \in \mathrm{Jac}(C_f)(K)[3]$. Write $T = [D - 2\infty]$, where D is the reduced effective divisor of degree 2 representing the class, allowing ∞ to occur in D. The divisor D is affine: otherwise $T = [P - \infty]$ for some point P, and the relation $3T = 0$ would give a function in $L(3\infty) = \langle 1, x\rangle$ with a triple zero at P, forcing P to be a Weierstrass point and hence $T = 0$.

Since $3T = 0$, there is a function φ with

$$\mathrm{div}(\varphi) = 3D - 6\infty.$$

Thus $\varphi \in L(6\infty) = \langle 1, x, x^2, x^3, y\rangle$. After scaling, we may write

$$\varphi = Ay - G(x),$$

where G is monic of degree 3. We must have $A \neq 0$; otherwise the zero divisor of φ is invariant under the hyperelliptic involution, which would imply $D \sim 2\infty$ and hence $T = 0$. Let H be the monic quadratic polynomial whose roots are the x-coordinates of the points in support of D (if $D = 2P$ with $P = (x_P, y_P)$, we take $H = (x - x_P)^2$) then

$$(Ay - G)(Ay + G) = A^2 f - G^2 = -H^3,$$

and therefore (2.1) holds.

Conversely, suppose that (A, G, H) satisfies (2.1). Let D be the divisor cut out by $H(x) = 0$ and $Ay = G(x)$. Since f is square-free, G and H are coprime. The identity

$$(Ay - G)(Ay + G) = -H^3$$

then shows that $Ay - G$ vanishes along D with multiplicity 3, and since G has a pole of order 6 at infinity while Ay has a pole of order 5, we obtain

$$\mathrm{div}(Ay - G) = 3D - 6\infty.$$

Thus $[D - 2\infty]$ is a 3-torsion point. It is non-zero. Indeed, if $D \sim 2\infty$, then D is a fibre of the hyperelliptic map. Since D is also cut out by $H(x) = 0$ and $Ay = G(x)$, this would force G and H to have a common zero, and hence would force f to have a double zero. □

Starting from polynomials G and H and a scalar A, if we define $f = (G^2 - H^3)/A^2$, we obtain a genus two curve with a marked rational 3-torsion point. We now give a parametrisation of pairs (G, H) for which the polynomial f is monic and of degree 5 and which is suitable for lattice point counting. We consider the weighted projective space $\mathbb{P}(1, 2, 3, 4)$, with weighted coordinates (A, B, J, E):

$$\mathrm{wt}(A) = 1, \qquad \mathrm{wt}(B) = 2, \qquad \mathrm{wt}(J) = 3, \qquad \mathrm{wt}(E) = 4.$$

Set $P = (A, B, J, E)$ and $u = x + B/3$. We define

$$G_P(x) = u^3 + AJu + \frac{A^2E}{3}, \tag{2.2}$$

$$H_P(x) = u^2 - \frac{A^2}{3}u + \frac{-A^4 + 5A^2B + 6AJ}{9}. \tag{2.3}$$

For $A \neq 0$ set

$$F_P(x) = \frac{G_P(x)^2 - H_P(x)^3}{A^2}. \tag{2.4}$$

We write

$$729F_P(x) = 729x^5 + \Theta_3(P)x^3 + \Theta_2(P)x^2 + \Theta_1(P)x + \Theta_0(P), \tag{2.5}$$

where

$$\Theta_3 = -27(5A^4 - 30A^2B - 36AJ + 30B^2 - 18E), \tag{2.6}$$

$$\Theta_2 = 27(6A^3J + 5A^2B^2 - 24ABJ - 20B^3 + 18BE - 9J^2), \tag{2.7}$$

$$\begin{aligned}\Theta_1 = 9(&A^8 - 10A^6B - 12A^5J + 30A^4B^2 + 72A^3BJ - 20A^2B^3 \\ &+ 36A^2J^2 - 84AB^2J + 54AEJ - 15B^4 + 18B^2E - 18BJ^2),\end{aligned} \tag{2.8}$$

$$\begin{aligned}\Theta_0 = {}&A^{10} - 12A^8B - 18A^7J + 45A^6B^2 + 144A^5BJ - 40A^4B^3 \\ &+ 108A^4J^2 - 252A^3B^2J - 45A^2B^4 - 432A^2BJ^2 + 81A^2E^2 \\ &- 144AB^3J + 162ABEJ - 216AJ^3 - 12B^5 + 18B^3E - 27B^2J^2.\end{aligned} \tag{2.9}$$

The polynomials $\Theta_3, \Theta_2, \Theta_1, \Theta_0$ are weighted homogeneous of weights $4, 6, 8, 10$, respectively. Although (2.4) is written as a quotient for $A \neq 0$, the coefficient formula (2.5) defines F_P for every $P \in K^4$ when 729 is invertible in K.

If $A \neq 0$ and F_P is square-free, then $C_P : y^2 = F_P(x)$ is a smooth genus 2 curve. Let D_P be the effective divisor of degree 2 cut out by

$$H_P(x) = 0, \qquad Ay = G_P(x),$$

and put

$$T_P = [D_P - 2\infty] \in \mathrm{Jac}(C_P).$$

Proposition 2.2. *Let K be a field of characteristic different from 2 and 3. Let*

$$C_f : y^2 = f(x) = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$$

be smooth over K, and let $0 \neq T \in \mathrm{Jac}(C_f)(K)[3]$. Then there is a unique tuple $P = (A, B, J, E) \in K^4$, with $A \neq 0$, such that

$$f = F_P, \qquad T = T_P.$$

Conversely, if $A \neq 0$ and F_P is square-free, then T_P is a non-zero point of order 3 on $\mathrm{Jac}(C_P)$.

Proof. By Proposition 2.1, the pair (f, T) determines a unique triple (A, G, H) with

$$G(x)^2 - A^2 f(x) = H(x)^3,$$

where $A \neq 0$, G is monic cubic, and H is monic quadratic. Write

$$G(x) = x^3 + Bx^2 + g_1 x + g_0.$$

With $u = x + B/3$, we have

$$G(x) = u^3 + \alpha u + \beta,$$

where

$$\alpha = g_1 - \frac{B^2}{3}, \qquad \beta = g_0 - \frac{Bg_1}{3} + \frac{2B^3}{27}.$$

Define

$$J = \frac{\alpha}{A}, \qquad E = \frac{3\beta}{A^2}.$$

Then $G = G_P$. Comparing the coefficients of x^5 and x^4 in $G^2 - A^2 f = H^3$ gives

$$H(x) = u^2 - \frac{A^2}{3}u + \frac{-A^4 + 5A^2B + 6AJ}{9} = H_P(x).$$

Hence $f = F_P$, and the marked torsion point is exactly T_P. This proves existence. The same formulae recover A, B, J, E from the unique triple (A, G, H), so the tuple P is unique.

Conversely, if $A \neq 0$ and F_P is square-free, then

$$G_P(x)^2 - A^2 F_P(x) = H_P(x)^3.$$

Proposition 2.1 therefore gives a non-zero point $T_P \in \mathrm{Jac}(C_P)(K)[3]$. □

3. A compact subset of $\mathbb{R}^4$

For $X \in \mathbb{R}_{\geq 0}$ we define

$$\mathcal{R}(X) = \{P \in \mathbb{R}^4 : H_\Theta(P) \leq X\}$$

where for any $P \in \mathbb{R}^4$,

$$H_\Theta(P) = H(F_P) = \max_{0 \leq i \leq 3} |\Theta_i(P)/729|^{1/(10-2i)}.$$

Lemma 3.1. *The set $\mathcal{R}(1)$ is compact.*

Proof. We first prove that $(0, 0, 0, 0)$ is the only common zero of $\Theta_3, \Theta_2, \Theta_1, \Theta_0$ over $\mathbb{C}$. Let (A, B, J, E) be a solution of $\Theta_0 = \Theta_1 = \Theta_2 = \Theta_3 = 0$. As these polynomials are weighted homogeneous, if $A \neq 0$, we may assume $A = 1$. A Groebner basis computation (see Appendix A) gives

$$1 \in (\Theta_3(1, B, J, E), \Theta_2(1, B, J, E), \Theta_1(1, B, J, E), \Theta_0(1, B, J, E)) \subset \mathbb{Q}[B, J, E], \tag{3.1}$$

and so there are no solutions with $A \neq 0$. Suppose next $A = 0$. The equations $\Theta_3 = \Theta_2 = 0$ imply

$$E = \frac{5}{3}B^2, \qquad 10B^3 - 9J^2 = 0.$$

Substituting these relations into $\Theta_1 = 0$ gives $-5B^4 = 0$. Hence $B = J = E = 0$. Thus the only common zero of the four forms is the origin.

Now put

$$\|P\|_w = \max\{|A|, |B|^{1/2}, |J|^{1/3}, |E|^{1/4}\}$$

and $S_w = \{P \in \mathbb{R}^4 : \|P\|_w = 1\}$. This is a compact set on which the function H_Θ is strictly positive, and hence $m := \min_{P \in S_w} H_\Theta(P) > 0$. For any non-zero $P \in \mathbb{R}^4$, write $\lambda = \|P\|_w$ and $Q = (\lambda^{-1}A, \lambda^{-2}B, \lambda^{-3}J, \lambda^{-4}E)$. Then $Q \in S_w$, and weighted homogeneity gives

$$H_\Theta(P) = \lambda H_\Theta(Q) \geq m\lambda.$$

Thus $\mathcal{R}(1) \subset \{P : \|P\|_w \leq m^{-1}\}$. Since $\mathcal{R}(1)$ is closed, it is compact. □

Lemma 3.2. *Let $v + \Lambda \subset \mathbb{Q}^4$ be an affine lattice of full rank. Then*

$$\#(\mathcal{R}(X) \cap (v + \Lambda)) = \frac{\mathrm{Vol}(\mathcal{R}(1))}{\mathrm{covol}(\Lambda)} X^{10} + O_\Lambda(X^9).$$

If $Z \subset \mathbb{A}^4$ is a proper algebraic subvariety, then

$$\#(\mathcal{R}(X) \cap (v + \Lambda) \cap Z(\mathbb{Q})) = O_{Z,\Lambda}(X^9).$$

Proof. Weighted homogeneity gives

$$\mathcal{R}(X) = \{(XA, X^2B, X^3J, X^4E) : (A, B, J, E) \in \mathcal{R}(1)\}.$$

The determinant of this dilation is $X^{1+2+3+4} = X^{10}$. Since $\mathcal{R}(1)$ is compact and semi-algebraic, Davenport's Lipschitz principle [8] gives the lattice point estimate. The subvariety estimate is an easy consequence of this. □

4. Local conditions

Define

$$c_i(P) = \Theta_i(P)/729 \qquad (i = 0, 1, 2, 3),$$

so that

$$F_P(x) = x^5 + c_3(P)x^3 + c_2(P)x^2 + c_1(P)x + c_0(P).$$

For a prime p we say that F_P is *p-integral* if all four coefficients $c_i(P)$ lie in $\mathbb{Z}_p$. When F_P is p-integral, we say that it is *not p-minimal* if

$$p^4 \mid c_3(P), \qquad p^6 \mid c_2(P), \qquad p^8 \mid c_1(P), \qquad p^{10} \mid c_0(P),$$

and *p-minimal* otherwise.

Proposition 4.1. *Let p be a prime. The set N_p of tuples $P \in \mathbb{Q}_p^4$ for which F_P is p-integral and p-minimal is a compact subset of $\mathbb{Q}_p^4$. Moreover, N_p is described by a finite set of congruence conditions, and there exists a constant M_p such that $p^{M_p} N_p \subset \mathbb{Z}_p^4$.*

Proof. We first show that there is an effectively computable integer M_p such that for any $P \in \mathbb{Q}_p^4$, $F_P \in \mathbb{Z}_p[x]$ only if $P \in p^{-M_p}\mathbb{Z}_p^4$. A `MAGMA` computation (see Appendix A) shows that the common zero locus of the four Θ_i over $\overline{\mathbb{Q}}$ is the origin $(0, 0, 0, 0)$. Hence, for each coordinate $X \in \{A, B, J, E\}$, some power of X belongs to the ideal generated by Θ_i over $\mathbb{Q}$. We have

$$C_X X^{N_X} = R_{X,3}\Theta_3 + R_{X,2}\Theta_2 + R_{X,1}\Theta_1 + R_{X,0}\Theta_0, \tag{4.1}$$

with $C_X \in \mathbb{Z}_{\neq 0}$, $N_X > 0$, and $R_{X,i} \in \mathbb{Z}[A, B, J, E]$. These identities are effectively computable from a Groebner basis.

Now take $P = (A, B, J, E) \in \mathbb{Q}_p^4$, and let n be the smallest integer such that

$$Q = (p^n A,\ p^{2n}B,\ p^{3n}J,\ p^{4n}E) \in \mathbb{Z}_p^4.$$

Since $Q \in \mathbb{Z}_p^4$, the values $R_{X,i}(Q)$ are p-adic integers. The identity (4.1) implies that if all the values $\Theta_i(Q)$ had sufficiently large p-adic valuation, then each coordinate of Q would be

divisible by the corresponding weighted power of p, but this contradicts the the definition of n . It follows that there exists a constant K_p, independent of P, such that, for every such Q,

$$\min_i v_p(\Theta_i(Q)) \le K_p. \tag{4.2}$$

Suppose now that $F_P \in \mathbb{Z}_p[x]$ is integral. As each Θ_i is weighted homogeneous of degree $d_i = 10 - 2i$, we have

$$\Theta_i(Q) = p^{nd_i}\Theta_i(P).$$

Also $c_i = \Theta_i/729$, so $c_i(P) \in \mathbb{Z}_p$ gives

$$v_p(\Theta_i(P)) \ge v_p(729).$$

Thus

$$v_p(\Theta_i(Q)) \ge nd_i + v_p(729) \qquad \text{for all } i.$$

Combining this with (4.2), and using $d_i \ge 4$, gives

$$4n + v_p(729) \le K_p.$$

Hence n is bounded above, and we can take

$$M_p = \max\left\{0, \left\lceil \frac{K_p - v_p(729)}{4} \right\rceil \right\}.$$

Write

$$P = (p^{-M_p}a,\ p^{-2M_p}b,\ p^{-3M_p}j,\ p^{-4M_p}e), \qquad (a,b,j,e) \in \mathbb{Z}_p^4.$$

For each i, choose $e_{p,i} \ge 0$ minimal such that

$$\Psi_{p,i}(a,b,j,e) := p^{e_{p,i}} c_i(p^{-M_p}a, p^{-2M_p}b, p^{-3M_p}j, p^{-4M_p}e)$$

belongs to $\mathbb{Z}_p[a,b,j,e]$. Then

$$c_i(P) \in \mathbb{Z}_p \quad \Longleftrightarrow \quad \Psi_{p,i}(a,b,j,e) \equiv 0 \pmod{p^{e_{p,i}}}.$$

Moreover F_P is not p-minimal exactly when

$$\Psi_{p,3}(a,b,j,e) \equiv 0 \pmod{p^{e_{p,3}+4}}, \quad \Psi_{p,2}(a,b,j,e) \equiv 0 \pmod{p^{e_{p,2}+6}},$$
$$\Psi_{p,1}(a,b,j,e) \equiv 0 \pmod{p^{e_{p,1}+8}}, \quad \Psi_{p,0}(a,b,j,e) \equiv 0 \pmod{p^{e_{p,0}+10}}.$$

Therefore p-integrality and p-minimality are determined by the residue class of (a,b,j,e) modulo p^{L_p}, where $L_p = \max\{e_{p,3}+4, e_{p,2}+6, e_{p,1}+8, e_{p,0}+10\}$. □

For $p \ge 5$ these congruence conditions take a simple form.

Proposition 4.2. *Let $p \ge 5$. For $P \in \mathbb{Z}_p^4$, the polynomial F_P is p-integral. The polynomial F_P is not p-minimal if and only if*

$$p \mid A, \qquad p^2 \mid B, \qquad p^3 \mid J, \qquad p^4 \mid E. \tag{4.3}$$

The density of the subset of $\mathbb{Z}_p^4$ of points P for which F_P is p-minimal is $1 - p^{-10}$.

Proof. The "if" direction is clear. Assume that P is integral and that F_P is not p-minimal. Reducing the four Θ_i modulo p shows first that

$$A \equiv B \equiv J \equiv E \equiv 0 \pmod{p}.$$

If $A \ne 0$, we can assume $A = 1$ by weighted homogeneity. The Groebner basis in Appendix A shows that the corresponding ideal contains 9 over $\mathbb{Z}$, so it has no zero modulo $p \ge 5$. If $A = 0$, then the calculation in the proof of Lemma 3.1 works modulo $p \ge 7$; for $p = 5$ the first three equations give $E = 0$, $J = 0$, and then $\Theta_0 = -12B^5$ gives $B = 0$.

Write $A = pa$, $B = pb$, $J = pj$, and $E = pe$. From $p^4 \mid \Theta_3$ we get

$$\frac{\Theta_3(pa, pb, pj, pe)}{p} \equiv 486e \pmod{p},$$

so $E = p^2 e_1$. From $p^6 \mid \Theta_2$ we get

$$\frac{\Theta_2(pa, pb, pj, p^2 e_1)}{p^2} \equiv -243j^2 \pmod{p},$$

so $J = p^2 j_1$.

Now substitute $A = pa$, $B = pb$, $J = p^2 j_1$, and $E = p^2 e_1$. The conditions $p^4 \mid \Theta_3$ and $p^6 \mid \Theta_2$ give

$$5b^2 - 3e_1 \equiv 0, \qquad -20b^3 + 18be_1 \equiv 0 \pmod{p}.$$

For $p \geq 7$ these imply $10b^3 \equiv 0 \pmod{p}$, so $B = p^2 b_1$ and $E = p^3 e_2$. Substituting $A = pa$, $B = p^2 b_1$, $J = p^2 j_1$, $E = p^3 e_2$ into Θ_2 gives

$$\frac{\Theta_2(pa, p^2 b_1, p^2 j_1, p^3 e_2)}{p^4} \equiv -243 j_1^2 \pmod{p},$$

so $J = p^3 j_2$. Finally

$$\frac{\Theta_3(pa, p^2 b_1, p^3 j_2, p^3 e_2)}{p^3} \equiv 486 e_2 \pmod{p},$$

so $E = p^4 e_3$.

For $p = 5$, the same argument gives $A = 5a$, $B = 5b$, $J = 25j$, and $E = 25e_1$. Using Θ_3 once more gives $e_1 \equiv 0 \pmod{5}$, so $E = 125e$. With $A = 5a$, $B = 5b$, $J = 25j$, $E = 125e$, and since F_P is not 5-minimal we get the four congruences

$$\begin{aligned} 2aj - 2b^2 + e &\equiv 0 \bmod 5, \\ 2abj + 2b^3 + be + 2j^2 &\equiv 0 \bmod 5, \\ -ab^2 j - 2b^4 + 2b^2 e - 2bj^2 &\equiv 0 \bmod 5, \\ -2b^5 &\equiv 0 \bmod 5. \end{aligned}$$

The last congruence gives $b \equiv 0$, the second gives $j \equiv 0$, and the first gives $e \equiv 0$. Thus (4.3) holds also for $p = 5$.

The sub-lattice defined by (4.3) has index $p^{1+2+3+4} = p^{10}$. This gives the density $1 - p^{-10}$ for minimality at p. □

5. The sieve

Proposition 4.1, applied at $p = 2$ and $p = 3$, gives a finite set of congruence conditions on $P = (A, B, J, E) \in \mathbb{Q}^4$ which characterize integrality and minimality at these two primes. We impose these conditions on $\mathbb{Z}[1/6]^4$. The subset $\mathcal{L}_{2,3}^{\min}$ of $\mathbb{Z}[1/6]^4$ consisting of tuples which are integral and minimal at both 2 and 3 is covered by a set I of affine lattices

$$\mathcal{L}_{2,3}^{\min} = \bigsqcup_{\nu \in I} (v_\nu + \Lambda_{2,3}),$$

contained in $\mathbb{Z}[1/6]^4$, with $\Lambda_{2,3} \subset \mathbb{Q}^4$ a lattice of full rank. We define

$$\beta_{2,3} = \frac{\#I}{\operatorname{covol}(\Lambda_{2,3})}.$$

Equivalently, by Lemma 3.2,

$$\#\big(\mathcal{R}(X)\cap\mathcal{L}_{2,3}^{\min}\big)=\mathrm{Vol}(\mathcal{R}(1))\,\beta_{2,3}X^{10}+O(X^9). \tag{5.1}$$

The number $\beta_{2,3}$ is effectively computable from the congruence conditions of Proposition 4.1. This computation could be carried out in practice with enough persistence, but appears to be rather tedious.

For a prime $p\geq 5$ put

$$p\cdot P=(pA,p^2B,p^3J,p^4E).$$

Define

$$\mathcal{M}(X)=\{P\in\mathcal{R}(X)\cap\mathcal{L}_{2,3}^{\min}: A\neq 0,\ \mathrm{disc}(F_P)\neq 0,\\ P\notin p\mathbb{Z}_p\times p^2\mathbb{Z}_p\times p^3\mathbb{Z}_p\times p^4\mathbb{Z}_p \text{ for every prime } p\geq 5\}.$$

The last condition says that, for every prime $p\geq 5$, the four coordinates are not simultaneously divisible by p with weights $1,2,3,4$.

Proposition 5.1. *The map*

$$P\longmapsto(F_P,T_P)$$

is a bijection from $\mathcal{M}(X)$ to $\mathcal{W}^{\mathrm{mark}}(X)$.

Proof. This follows from Proposition 2.2, Proposition 4.1 and Proposition 4.2. □

Remark 5.2. The tuple P need not be integral at the primes 2 and 3. For instance,

$$P=\left(6,0,0,\frac{9}{2}\right)$$

gives

$$F_P(x)=x^5-237x^3+20736x+83025,$$

which is integral and minimal.

Set

$$\mathcal{G}(X)=\{P\in\mathcal{R}(X)\cap\mathcal{L}_{2,3}^{\min}: P\notin p\cdot\mathbb{Z}[1/6]^4 \text{ for every prime } p\geq 5\}.$$

Then

$$\mathcal{M}(X)=\mathcal{G}(X)\setminus\big(\{A=0\}\cup\{\mathrm{disc}(F_P)=0\}\big), \tag{5.2}$$

and Proposition 5.1 identifies $\mathcal{M}(X)$ with $\mathcal{W}^{\mathrm{mark}}(X)$.

Proposition 5.3. *As $X\to\infty$,*

$$\#\mathcal{G}(X)=\mathrm{Vol}(\mathcal{R}(1))\,\beta_{2,3}\prod_{p\geq 5}(1-p^{-10})X^{10}+o(X^{10}).$$

Proof. Let S be a finite set of primes $p\geq 5$. Since $\mathcal{L}_{2,3}^{\min}$ is a finite union of affine lattices whose denominators are supported only at 2 and 3, reduction modulo powers of primes in S behaves as for the standard lattice. Proposition 4.2 and Lemma 3.2 give

$$\#\{P\in\mathcal{R}(X)\cap\mathcal{L}_{2,3}^{\min}: P\notin p\cdot\mathbb{Z}[1/6]^4 \text{ for every } p\in S\}\\ =\mathrm{Vol}(\mathcal{R}(1))\,\beta_{2,3}\prod_{p\in S}(1-p^{-10})X^{10}+O_S(X^9).$$

It remains to pass from the finite sieve to the full sieve. For $M \geq 5$, let $N_M^{\mathrm{tail}}(X)$ be the number of points $P \in \mathcal{R}(X) \cap \mathcal{L}_{2,3}^{\min}$, with $A \neq 0$, such that F_P is non-minimal at some prime $p > M$. We will show that

$$N_M^{\mathrm{tail}}(X) \ll X^{10} \sum_{p>M} p^{-10} + o(X^{10}), \tag{5.3}$$

where the implied constant is independent of M and X.

Points in $\mathcal{R}(X)$ satisfy

$$|A| \ll X, \quad |B| \ll X^2, \quad |J| \ll X^3, \quad |E| \ll X^4.$$

Fix a prime $p \geq 5$. By Proposition 4.2, non-minimality at p is equivalent to

$$p \mid A, \qquad p^2 \mid B, \qquad p^3 \mid J, \qquad p^4 \mid E.$$

Therefore, in any one of the affine lattices $v_\nu + \Lambda_{2,3}$, the number of (A, B, J, E) that give integral equations that are non-minimal at p is bounded by

$$\ll \left(\frac{X}{p} + 1\right)\left(\frac{X^2}{p^2} + 1\right)\left(\frac{X^3}{p^3} + 1\right)\left(\frac{X^4}{p^4} + 1\right),$$

with the implied constant depending only on the finite collection of lattices. Since $A \neq 0$, any such prime p divides the non-zero integer obtained from A after clearing its denominator, which is uniformly bounded by Proposition 4.1, and as $|A| \ll X$ on $\mathcal{R}(X)$, only primes $p \ll X$ can occur. Summing the preceding estimate over $M < p \ll X$ and over the finitely many affine lattices proves (5.3).

The contribution from $A = 0$ is $O(X^9)$ by Lemma 3.2. Taking $X \to \infty$ in the finite sieve estimate and using (5.3) gives

$$\limsup_{X\to\infty} \left| \frac{\#\mathcal{G}(X)}{X^{10}} - \mathrm{Vol}(\mathcal{R}(1))\, \beta_{2,3} \prod_{5\leq p\leq M} (1 - p^{-10}) \right| \ll \sum_{p>M} p^{-10}.$$

The result follows by taking $M \to \infty$. □

Proof of Theorem 1.1. By Proposition 5.3, it remains only to remove the degenerate tuples (A, B, J, E) with $A = 0$ and $\mathrm{disc}(F_P) = 0$. By Lemma 3.2, these loci contribute $O(X^9)$ points. We can identify the remaining tuples with $\mathcal{W}^{\mathrm{mark}}(X)$ by (5.2) and Proposition 5.1, and the conclusion follows. □

Remark 5.4. A natural question one can ask is how our result compares to counting genus 2 curves C whose Jacobian has a non-trivial rational 3-torsion point. This amounts to forgetting the marking of the torsion point T. Let $\mathcal{W}^{\mathrm{unmarked}}(X)$ denote the set of such curves of height at most X. Since $\#\operatorname{Jac}(C)(\bar{\mathbb{Q}})[3] = 81$, we have $\#\mathcal{W}^{\mathrm{unmarked}}(X) = O(X^{10})$. In fact, we can pin down the leading constant exactly, and we have

$$\#\mathcal{W}^{\mathrm{unmarked}}(X) = \frac{c}{2} X^{10} + o(X^{10}).$$

We give a brief sketch of the argument. As the Weil pairing is Galois equivariant, the group $\operatorname{Jac}(C)(\mathbb{Q})[3]$ is isotropic for the Weil pairing, and hence is of order at most 9. Curves with a $\mathbb{Q}$-rational 3-torsion subgroup of order 9 correspond to a thin subset M of $\mathbb{P}(1, 2, 3, 4)(\mathbb{Q})$. To see this, we consider the moduli space of tuples (C, P, T, K) where C is a genus 2 curve, P is a Weierstrass point, T is a 3-torsion point on $\operatorname{Jac} C$, and K is a maximal isotropic subgroup of $\operatorname{Jac} C[3]$ such that $\langle T\rangle \leq K$, and the map $(C, P, T, K) \to (C, P, T)$ which forgets the subgroup K. Then M is contained in the image of this map, and it follows that M is a

thin set in the sense of Serre. Hence, by [4, Theorem 1.1] applied to $\mathbb{P}(1,2,3,4)$, there are $o(X^{10})$ of them. Outside this negligible subset, the rational fibers of the map that forgets the marking $(C,P,T)\mapsto(C,P)$ are of size two, corresponding to the points T and $-T$, and so the asymptotic count is half that of the count of curves with a marked 3-torsion point.

It would be interesting to determine exactly the asymptotic count of genus 2 curves C with $\#\operatorname{Jac}(C)(\mathbb{Q})[3]=9$. We expect that this can be achieved using the results of [2] and the methods of this paper.

References

[1] Brandon Boggess and Soumya Sankar. Counting elliptic curves with a rational N-isogeny for small N. *J. Number Theory*, 262:471–505, 2024.

[2] Nils Bruin, E. Victor Flynn, and Damiano Testa. Descent via $(3,3)$-isogeny on Jacobians of genus 2 curves. *Acta Arith.*, 165(3):201–223, 2014.

[3] Peter Bruin and Filip Najman. Counting elliptic curves with prescribed level structures over number fields. *J. Lond. Math. Soc.*, 105(4):2415–2435, 2022.

[4] Stephanie Chan, Daniel Loughran, and Nick Rome. Thin sets in weighted projective stacks. *arXiv preprint arXiv:2602.05705*, 2026.

[5] Zachary Couvillion and Anwesh Ray. Counting elliptic curves with prescribed entanglements. *Res. Number Theory*, 11(4):Paper No. 106, 2025.

[6] John Cullinan, Meagan Kenney, and John Voight. On a probabilistic local-global principle for torsion on elliptic curves. *J. Théor. Nombres Bordeaux*, 34(1):41–90, 2022.

[7] Ratko Darda and Changho Han. The stacky Batyrev–Manin conjecture and modular curves. *arXiv preprint arXiv:2602.19771*, 2026.

[8] Harold Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, 26(3):179–183, 1951.

[9] Stevan Gajović, Lazar Radičević, and Matteo Verzobio. The density of elliptic curves over $\mathbb{Q}_p$ with a rational 3-torsion point or a rational 3-isogeny. *arXiv preprint arXiv:2502.08583*, 2025.

[10] Tyler Genao, Tristan Phillips, Fredderick Saia, Tim Santens, and John Yin. Counting points on some genus zero Shimura curves. *arXiv preprint arXiv:2504.09400*, 2025.

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

[12] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186, 1977.

[13] Grant Molnar and John Voight. Counting elliptic curves over the rationals with a 7-isogeny. *Res. Number Theory*, 9(4):Paper No. 75, 31, 2023.

[14] Tristan Phillips. Points of bounded height in images of morphisms of weighted projective stacks: with applications to counting elliptic curves. *J. Lond. Math. Soc.*, 113(3):e70486, 2026.

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

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

Appendix A. A Groebner basis computation

The only computer calculation used in the proof is the following integer Groebner basis computation, needed in the proof of Lemma 3.1 and in the proof of Proposition 4.2. Here is the Magma code.

```
Z := Integers();
R<B,J,E> := PolynomialRing(Z, 3, "lex");
A := R!1;

T3 := -27*(5*A^4 - 30*A^2*B - 36*A*J + 30*B^2 - 18*E);
T2 :=  27*(6*A^3*J + 5*A^2*B^2 - 24*A*B*J - 20*B^3
           + 18*B*E - 9*J^2);
```

```
T1 :=   9*(A^8 - 10*A^6*B - 12*A^5*J + 30*A^4*B^2
           + 72*A^3*B*J - 20*A^2*B^3 + 36*A^2*J^2
           - 84*A*B^2*J + 54*A*E*J - 15*B^4
           + 18*B^2*E - 18*B*J^2);
T0 :=      A^10 - 12*A^8*B - 18*A^7*J + 45*A^6*B^2
           + 144*A^5*B*J - 40*A^4*B^3 + 108*A^4*J^2
           - 252*A^3*B^2*J - 45*A^2*B^4 - 432*A^2*B*J^2
           + 81*A^2*E^2 - 144*A*B^3*J + 162*A*B*E*J
           - 216*A*J^3 - 12*B^5 + 18*B^3*E - 27*B^2*J^2;

I := ideal< R | T3, T2, T1, T0 >;
GB := GroebnerBasis(I);
GB;

assert &or[ g eq R!9 or g eq R!-9 : g in GB ];
```

Department of Mathematics, University College London, London, WC1H 0AY, United Kingdom
Email address: e.lupoian@ucl.ac.uk

Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade, Serbia
Email address: lazaradicevic@gmail.com