Counting elliptic curves with prescribed level structures over number fields

Bruin, P.J.; Najman, F.

Received: 23 March 2021 | Revised: 5 October 2021 | Accepted: 8 October 2021

DOI: 10.1112/jlms.12564

RESEARCH ARTICLE

Journal of the London Mathematical Society

Counting elliptic curves with prescribed level structures over number fields

Peter Bruin[1] | **Filip Najman**[2]

[1]Mathematisch Instituut, Universiteit Leiden, The Netherlands

[2]Faculty of Science, Department of Mathematics, University of Zagreb, Croatia

Correspondence
Peter Bruin, Universiteit Leiden, Mathematisch Instituut, Postbus 9512, 2300 RA Leiden, The Netherlands.
Email: p.j.bruin@math.leidenuniv.nl

Funding information
European Regional Development Fund, Grant/Award Number: KK.01.1.1.01.0004; Croatian Science Foundation, Grant/Award Number: IP-2018-01-1313; Dutch Research Council, Grant/Award Number: 024.003.037

Abstract

Harron and Snowden (J. reine angew. Math. **729** (2017), 151–170) counted the number of elliptic curves over $\mathbb{Q}$ up to height X with torsion group G for each possible torsion group G over $\mathbb{Q}$. In this paper, we generalize their result to all number fields and all level structures G such that the corresponding modular curve X_G is a weighted projective line $\mathbb{P}(w_0, w_1)$ and the morphism $X_G \to X(1)$ satisfies a certain condition. In particular, this includes all modular curves $X_1(m, n)$ with coarse moduli space of genus 0. We prove our results by defining a *size function* on $\mathbb{P}(w_0, w_1)$ following unpublished work of Deng (Preprint, https://arxiv.org/abs/math/9812082), and working out how to count the number of points on $\mathbb{P}(w_0, w_1)$ up to size X.

MSC (2020)
11G05 (primary), 11G18, 11G50, 14D23, 14G40 (secondary)

1 | INTRODUCTION

Let E be an elliptic curve over a number field K. The Mordell–Weil theorem says that $E(K)$ is isomorphic to $\mathbb{Z}^r \times E(K)_{\mathrm{tor}}$ for some $r \geqslant 0$, where $E(K)_{\mathrm{tor}}$ is the (finite) torsion subgroup of $E(K)$. It is a natural question which groups appear as $E(K)_{\mathrm{tor}}$, and moreover how often each one of these groups appears. Harron and Snowden [11] studied this question and answered it in the case $K = \mathbb{Q}$. The aim of this paper is to study the same problem, but to both allow K to be any number field and to answer the more general question how often a prescribed G-level structure appears.

To make this question more precise, let n be a positive integer, let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, and let K be a number field. We say that an elliptic curve E over K *admits a G-level structure* if there exists a $(\mathbb{Z}/n\mathbb{Z})$-basis of $E[n](\bar{K})$ such that the Galois representation $\rho_{E,n} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ defined by this basis has image contained in G. We write

$$\mathcal{E}_{G,K} = \{\text{elliptic curves over } K \text{ admitting a } G\text{-level structure}\}/\cong.$$

We will define a *size function* S_K from the set of isomorphism classes of elliptic curves over K to $\mathbb{R}_{>0}$; see Definition 7.1. We define a function $N_{G,K} : \mathbb{R}_{>0} \to \mathbb{Z}_{\geqslant 0}$ by

$$N_{G,K}(X) = \#\{E \in \mathcal{E}_{G,K} \mid S_K(E)^{12} \leqslant X\}.$$

Let X_G be the moduli stack of generalized elliptic curves with G-level structure. This is a one-dimensional proper smooth geometrically connected algebraic stack over the fixed field K_G of the action of G on $\mathbb{Q}(\zeta_n)$ given by $(g, \zeta_n) \mapsto \zeta_n^{\det g}$. We consider cases where X_G is a weighted projective line $\mathbb{P}(w_0, w_1)$ over K_G. We can now state our main result (which is also stated in a slightly different form in Theorem 7.6).

Theorem 1.1. *Let n be a positive integer, and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Assume that the stack X_G over K_G is isomorphic to $\mathbb{P}(w)_{K_G}$, where $w = (w_0, w_1)$ is a pair of positive integers, and let $e(G)$ be the reduced degree of the canonical morphism $X_G \to X(1)$ (see Definition 4.2). Furthermore, assume $e(G) = 1$ or $w = (1, 1)$ holds. Then for every finite extension K of K_G, we have*

$$N_{G,K}(X) \asymp X^{1/d(G)} \quad \text{as } X \to \infty,$$

where

$$d(G) = \frac{12e(G)}{w_0 + w_1}.$$

As all modular curves $X_G = X_1(m, n)$ with coarse moduli space of genus 0 satisfy the assumptions of Theorem 1.1, our result generalizes [11, Theorem 1.2], where this statement was proved in the case where $K = \mathbb{Q}$ and where G is one of the 15 groups corresponding to the torsion groups from Mazur's theorem.

A recent result of Pizzo, Pomerance and Voight [16] is $N_{G,\mathbb{Q}}(X) \sim X^{1/2}$ for G such that $X_G = X_0(3)$. Moreover, they determined the constant in front of the leading term of the function $N_{G,\mathbb{Q}}(X)$ as well as the first two lower order terms. This result falls outside of the reach of our results, as $X_0(3)$ is not a weighted projective line (cf. Remark 7.4).

Similarly, Pomerance and Schaefer [17] proved that $N_{G,\mathbb{Q}}(X) \sim X^{1/3}$ for G such that $X_G = X_0(4)$, and determined the constants in front of the leading term and the first lower order term. Our result implies $N_{G,K} \asymp X^{1/3}$ for all number fields K; for $K = \mathbb{Q}$, this follows from the sharper results of [17].

Cullinan, Kenney and Voight [4, Theorem 1.3.3] proved a sharper version of Theorem 1.1 in the special case where X_G is a projective line (that is, isomorphic to $\mathbb{P}^1 = \mathbb{P}(1, 1)$) and $K = \mathbb{Q}$. More precisely, they give an asymptotic expression for $N_{G,\mathbb{Q}}(X)$ containing an effectively computable leading coefficient and an error term.

Boggess and Sankar [2] determined the growth rate of the number of elliptic curves over $\mathbb{Q}$ with a cyclic n-isogeny for $n \in \{2, 3, 4, 5, 6, 8, 9, 12, 16, 18\}$. Out of these, only the cases $n = 2$ and $n = 4$ (for which a more precise result was already proved in [11, 17]) correspond to weighted projective lines and are therefore generalized to number fields by Theorem 1.1.

Remark 1.2. The 12th power in the definition of $N_{G,K}(X)$ is included for easier comparison with the height function in [11]; see Remark 7.2.

Remark 1.3. Our result gives a more conceptual interpretation of $d(G)$; cf. [11, § 1.2]. Namely, we show that $d(G)$ can be expressed in terms of the pair of positive integers (w_0, w_1) for which X_G is isomorphic to the weighted projective line with weights (w_0, w_1), and $e(G)$, an invariant (similar to the degree) of the morphism $X_G \to X(1)$.

We also remark that our result shows how in certain cases one can count points in the image of a morphism of stacks, partially answering a question in [11, Remark 1.5].

2 | WEIGHTED PROJECTIVE SPACES

Definition 2.1. Given an $(n + 1)$-tuple $w = (w_0, \dots, w_n)$ of positive integers, the *weighted projective space with weights* w is the algebraic stack

$$\mathbb{P}(w) = [\mathbb{G}_{\mathrm{m}} \backslash \mathbb{A}^{n+1}_{\neq 0}]$$

over $\mathbb{Z}$, where $\mathbb{A}^{n+1}_{\neq 0}$ is the complement of the zero section in $\mathbb{A}^{n+1}$ and $\mathbb{G}_{\mathrm{m}}$ acts on $\mathbb{A}^{n+1}_{\neq 0}$ by

$$(\lambda, (x_0, \dots, x_n)) \longmapsto (\lambda^{w_0} x_0, \dots, \lambda^{w_n} x_n).$$

It is known that $\mathbb{P}(w)$ is a proper smooth algebraic stack over $\mathbb{Z}$, and in fact a complete smooth toric Deligne–Mumford stack in the sense of Fantechi, Mann and Nironi [10, Example 7.27]. For every ring R, there is a *groupoid of R-points* of $\mathbb{P}(w)$. We will mostly be interested in the set of isomorphism classes of this groupoid, which we call the *set of R-points* of $\mathbb{P}(w)$ and denote by $\mathbb{P}(w)(R)$. Given a field L, the set $\mathbb{P}(w)(L)$ can be described as

$$\mathbb{P}(w)(L) = L^{\times} \backslash (L^{n+1} \setminus \{0\}),$$

where $L^{\times}$ acts on $L^{n+1} \setminus \{0\}$ by

$$(\lambda, (x_0, \dots, x_n)) \longmapsto (\lambda^{w_0} x_0, \dots, \lambda^{w_n} x_n).$$

The image in $\mathbb{P}(w)(L)$ of an element $x \in L^{n+1} \setminus \{0\}$ will be denoted by $[x]$.

Example 2.2. If $w = (m)$ with m a positive integer, then $\mathbb{P}(m)$ is canonically isomorphic to the classifying stack of the group scheme μ_m. If L is a field, then we have

$$\mathbb{P}(m)(L) = (L^{\times})^m \backslash L^{\times}.$$

3 | SIZE FUNCTIONS

Let w be an $(n+1)$-tuple as above, let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. On the set $\mathbb{P}(w)(K)$, we define a *size function* similarly to Deng [7]; see Definition 3.4. We do not restrict to weighted projective spaces that are 'well-formed' in the sense of [7].

Definition 3.1. For $x \in K^{n+1}$, the *scaling ideal* of x, denoted by $\mathcal{I}_w(x)$, is the intersection of all fractional ideals $\mathfrak{a}$ of $\mathcal{O}_K$ satisfying $x \in \mathfrak{a}^{w_0} \times \cdots \times \mathfrak{a}^{w_n}$. Similarly, for an $(n+1)$-tuple $(\mathfrak{b}_0, \dots, \mathfrak{b}_n)$ of fractional ideals of $\mathcal{O}_K$, the *scaling ideal* of $(\mathfrak{b}_0, \dots, \mathfrak{b}_n)$, denoted by $\mathcal{I}_w(\mathfrak{b}_0, \dots, \mathfrak{b}_n)$, is the intersection of all fractional ideals $\mathfrak{a}$ of $\mathcal{O}_K$ satisfying $\mathfrak{b}_i \subseteq \mathfrak{a}^{w_i}$ for all i.

Remark 3.2. For all $x \in K^{n+1} \setminus \{0\}$, the fractional ideal $\mathcal{I}_w(x)$ is nonzero and satisfies

$$\mathcal{I}_w(x)^{-1} = \{a \in K \mid a^{w_i} x_i \in \mathcal{O}_K \text{ for } i = 0, \dots, n\}.$$

Similarly, for every $(n+1)$-tuple $(\mathfrak{b}_0, \dots, \mathfrak{b}_n)$ of fractional ideals of $\mathcal{O}_K$, not all zero, the fractional ideal $\mathcal{I}_w(\mathfrak{b}_0, \dots, \mathfrak{b}_n)$ is nonzero and satisfies

$$\mathcal{I}_w(\mathfrak{b}_0, \dots, \mathfrak{b}_n)^{-1} = \{a \in K \mid a^{w_i} \mathfrak{b}_i \subseteq \mathcal{O}_K \text{ for } i = 0, \dots, n\}.$$

Definition 3.3. Let $\Omega_{K,\infty}$ denote the set of Archimedean places of K, and for each $v \in \Omega_{K,\infty}$, let $|\,|_v : K \to \mathbb{R}_{\geqslant 0}$ be the corresponding normalized absolute value. The *Archimedean size* on $K^{n+1} \setminus \{0\}$ is the function

$$\begin{aligned} H_{w,\infty} : K^{n+1} \setminus \{0\} &\longrightarrow \mathbb{R}_{>0} \\ x &\longmapsto \prod_{v \in \Omega_{K,\infty}} \max_{0 \leqslant i \leqslant n} |x_i|_v^{1/w_i}. \end{aligned}$$

Definition 3.4. The *size function* on $\mathbb{P}(w)(K)$ is the function

$$\begin{aligned} S_{w,K} : \mathbb{P}(w)(K) &\longrightarrow \mathbb{R}_{>0} \\ [x] &\longmapsto \mathrm{N}(\mathcal{I}_w(x))^{-1} H_{w,\infty}(x). \end{aligned}$$

It is straightforward to check that $S_{w,K}([x])$ does not depend on the choice of the representative x.

Example 3.5. If $w = (m)$ with m a positive integer and $x \in \mathbb{Z} \setminus \{0\}$ is mth power free, we have

$$S_{(m),\mathbb{Q}}([x]) = |x|^{1/m}.$$

Remark 3.6. If L/K is an extension of number fields, we have

$$S_{(1,\dots,1),L}(x) = S_{(1,\dots,1),K}(x)^{[L:K]},$$

but for general weights w such a relation does not hold. For example, if $w = (m)$ with $m \geqslant 2$ and $x \in \mathbb{Z} \setminus \{0\}$ is mth power free, then

$$S_{(m),\mathbb{Q}}([x]) = |x|^{1/m},$$

but

$$S_{(m),\mathbb{Q}(x^{1/m})}([x]) = S_{(m),\mathbb{Q}(x^{1/m})}([1]) = 1.$$

Remark 3.7. Definition 3.4 is a special case of the notion of height for rational points on algebraic stacks defined by Ellenberg, Satriano and Zureick-Brown [9]. Namely, as explained in [9, Section 3.3], we have

$$\log S_{w,\mathbb{Q}}(x) = \mathrm{ht}_{\mathcal{L}}(x),$$

where $\mathrm{ht}_{\mathcal{L}}$ is the height function corresponding to the tautological line bundle $\mathcal{L}$ on $\mathbb{P}(w)$. The work of Ellenberg, Satriano and Zureick-Brown was recently used by Boggess and Sankar [2] to count elliptic curves over $\mathbb{Q}$ with a rational n-isogeny for $n \in \{2, 3, 4, 5, 6, 8, 9\}$, as mentioned in the introduction.

Theorem 3.8. *Let n be a non-negative integer, let $w = (w_0, \ldots, w_n)$ be an $(n+1)$-tuple of positive integers, and let K be a number field. Let r_1, r_2, d_K, h_K, R_K, μ_K and ζ_K be the number of real places, number of nonreal complex places, discriminant, class number, regulator, number of roots of unity and Dedekind ζ-function of K, respectively. We write*

$$\begin{aligned} |w| &= w_0 + w_1 + \cdots + w_n, \\ \mu_K^w &= \frac{\mu_K}{\gcd\{w_0, w_1, \ldots, w_n, \mu_K\}} \\ C_K^w &= \frac{h_K R_K}{\mu_K^w \zeta_K(|w|)} \left(\frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d_K|}} \right)^{n+1} |w|^{r_1+r_2-1}. \end{aligned}$$

Then we have

$$\#\{x \in \mathbb{P}(w)(K) \mid S_{w,K}(x) \leqslant T\} \sim C_K^w T^{|w|} \quad \text{as } T \to \infty.$$

Proof. This was proved by Deng [7, Theorem (A)] in the case where $\mathbb{P}(w)$ is *well-formed*, that is, each n elements from w are coprime. However, the proof works in general with only minor changes: in the paragraph before [7, Proposition 4.2], the statement that the group of roots of unity acts effectively has to be replaced by the statement that all orbits of points with all coordinates nonzero contain μ_K^w points, and the factor w (denoting the number of roots of unity) in [7, Proposition 4.2, Proposition 4.5, Corollary 4.6 and Theorem (A)] has to be replaced by μ_K^w. □

Remark 3.9. Theorem 3.8 also follows from recent results of Darda [5] on counting rational points on weighted projective spaces with respect to more general height functions; see in particular [5, Remark 7.3.2.5].

In the remainder of this article, we will only consider *weighted projective lines*, that is, one-dimensional weighted projective spaces where the weight is given by a pair (w_0, w_1).

4 MORPHISMS BETWEEN WEIGHTED PROJECTIVE LINES

Let $u = (u_0, u_1)$, $w = (w_0, w_1)$ be two pairs of positive integers. In this section, we classify the morphisms of stacks from $\mathbb{P}(w)$ to $\mathbb{P}(u)$ over a field. These morphisms form a groupoid, but for simplicity we will only be interested in the set of isomorphism classes of this groupoid, or in other words the *set of morphisms* from $\mathbb{P}(w)$ to $\mathbb{P}(u)$. We also prove some facts about such morphisms generalizing the corresponding facts about morphisms $\mathbb{P}^1 \to \mathbb{P}^1$.

Lemma 4.1. *Let K be a field, and let $u = (u_0, u_1)$, $w = (w_0, w_1)$ be two pairs of positive integers. We consider $R = K[x_0, x_1]$ as a graded K-algebra where x_0 and x_1 are homogeneous of degrees w_0 and w_1, respectively. Let $P_{u,w}(K)$ be the set of pairs $(f_0, f_1) \in R \times R$ with the following properties.*

(i) *There exists $e = e(f_0, f_1) \in \mathbb{Z}_{\geqslant 0}$ for which f_0 and f_1 are homogeneous of degrees eu_0 and eu_1, respectively.*
(ii) *The homogeneous ideal $\sqrt{(f_0, f_1)} \subseteq R$ contains (x_0, x_1).*

Let $K^\times$ act on $P_{u,w}(K)$ by $c(f_0, f_1) = (c^{u_0} f_0, c^{u_1} f_1)$. Then there is a natural bijection from $K^\times \backslash P_{u,w}(K)$ to the set of morphisms $\mathbb{P}(w)_K \to \mathbb{P}(u)_K$ sending the class of $(f_0, f_1) \in P_{u,w}(K)$ to the morphism induced by the K-algebra homomorphism

$$\begin{aligned} K[y_0, y_1] &\longrightarrow K[x_0, x_1] \\ y_0 &\longmapsto f_0 \\ y_1 &\longmapsto f_1. \end{aligned}$$

Proof. We apply Lemma A.2 to the following data over K:

- $X = \mathbb{A}^2_{\neq 0}$ with coordinates $x = (x_0, x_1)$,
- $Y = \mathbb{A}^2_{\neq 0}$ with coordinates $y = (y_0, y_1)$,
- $G = \mathbb{G}_{\mathrm{m}}$ with coordinate g,
- $H = \mathbb{G}_{\mathrm{m}}$ with coordinate h,
- $a : G \times X \to X$ is the weight w action, given on points by $a(g, x) = (g^{w_0} x_0, g^{w_1} x_1)$,
- $b : H \times Y \to Y$ is the weight u action, given on points by $b(h, y) = (h^{u_0} y_0, h^{u_1} y_1)$.

(Note that the lemma applies because the Picard group of X is trivial.)

We first determine the morphisms $h : G \times X \to H$ satisfying the 'cocycle condition' (A.1) of Lemma A.2. A morphism $h : G \times X \to H$ is given by a monomial of the form $h(g, x) = \lambda g^e$ with $\lambda \in K^\times$ and $e \in \mathbb{Z}$, and h satisfies (A.1) if and only if $\lambda = 1$, i.e. h is of the form $h(g, x) = g^e$.

Given h as above, we now determine the morphisms $f : X \to Y$ such that the pair (f, h) satisfies condition (A.2) of Lemma A.2. Every such f is given by a pair $(f_0, f_1) \in R \times R$, and (f_0, f_1) determines a morphism $X \to Y$ if and only if $\sqrt{(f_0, f_1)}$ contains (x_0, x_1). It is straightforward to check that condition (A.2) translates to the condition that f_j is homogeneous of degree eu_j for $j = 0, 1$. In particular, morphisms $f : X \to Y$ such that (f, h) defines a morphism $[G \backslash X] \to [H \backslash Y]$ only exist if $e \geqslant 0$; moreover, e and therefore h are uniquely determined by f.

Finally, the group $H(X)$ is canonically isomorphic to $K^\times$, and if (f,h) is a pair as above where f is defined by (f_0,f_1), and $c \in H(X)$, then we have $c(f,h)=(f',h)$ where f' is defined by $(c^{u_0}f_0, c^{u_1}f_1)$. The lemma therefore follows from Lemma A.2. □

Definition 4.2. Let K be a field, let u, w be two pairs of positive integers, and let $\phi : \mathbb{P}(w)_K \to \mathbb{P}(u)_K$ be a morphism. The *reduced degree* of ϕ, denoted by $\deg_{\mathrm{red}} \phi$, is the unique integer $e \geqslant 0$ satisfying Lemma 4.1(i) for some (hence every) pair (f_0,f_1) giving rise to ϕ via the bijection of Lemma 4.1.

Remark 4.3. A morphism $\phi : \mathbb{P}(u)_K \to \mathbb{P}(w)_K$ is representable (by which we mean representable in algebraic spaces) if and only if ϕ is faithful as a functor [18, tag 04Y5]. Moreover, it suffices to check this condition on geometric fibres [3, Corollary 2.2.7]. From this one can deduce that ϕ is representable if and only if its reduced degree $e = \deg_{\mathrm{red}} \phi$ satisfies

$$\gcd(w_0, e) = \gcd(w_1, e) = 1.$$

Lemma 4.4. *In the setting of Lemma 4.1, let $(f_0,f_1) \in P_{u,w}(K)$ and assume $e(f_0,f_1) > 0$. Then R is finite over its graded subalgebra $S = K[f_0,f_1]$.*

Proof. We write $R_+ = Rx_0 + Rx_1$, $S_+ = Sf_0 + Sf_1$ and $I = Rf_0 + Rf_1 = RS_+$. By condition (ii) of Lemma 4.1 and the fact that f_0 and f_1 are nonconstant, we have $\sqrt{I} = R_+$. Hence for m sufficiently large, we have $R_+^m \subseteq I$, so the graded K-algebra R/I is a quotient of R/R_+^m and is therefore finite-dimensional over K. Choose homogeneous elements $g_1, \dots, g_r \in R$ such that their images in R/I are a K-basis of R/I. In particular, the g_i generate $R/I = R/RS_+$ over S, so we have

$$R = RS_+ + Sg_1 + \cdots + Sg_r.$$

Hence the $\mathbb{Z}_{\geqslant 0}$-graded S-module $M = R/(Sg_1 + \cdots + Sg_r)$ satisfies $S_+M = M$. It follows from a variant of Nakayama's lemma (see, for example, Eisenbud [8, Exercise 4.6]) that $M = 0$ and hence $R = Sg_1 + \cdots + Sg_r$. □

Lemma 4.5. *Let K be a field, let u, w be two pairs of positive integers, and let $\phi : \mathbb{P}(w)_K \to \mathbb{P}(u)_K$ be a nonconstant representable morphism. Then ϕ is finite.*

Proof. Since $\mathbb{P}(w)_K$ and $\mathbb{P}(u)_K$ are Deligne–Mumford stacks and ϕ is representable, we may choose a Cartesian diagram

$$\begin{tikzcd} T \arrow[r, "\phi'"] \arrow[d] & S \arrow[d] \\ \mathbb{P}(w)_K \arrow[r, "\phi"] & \mathbb{P}(u)_K \end{tikzcd}$$

where S and T are algebraic spaces and the vertical maps are étale coverings. Then ϕ' is proper because ϕ is proper, and is locally quasi-finite because ϕ' has relative dimension 0 [18, tag 04NV].

In particular, ϕ' is representable in schemes [18, tag 0418] and is finite [18, tag 0A4X]. It follows that ϕ is finite. □

Remark 4.6. Alternatively, Lemma 4.5 may be proved using Lemma 4.4.

Corollary 4.7. *With the notation of Lemma 4.5, let $V \subseteq \mathbb{P}(w)_K$ be a dense open substack. Then $\mathbb{P}(w)_K$ is the integral closure of $\mathbb{P}(u)_K$ in V.*

Proof. By Lemma 4.5, the morphism ϕ is finite and in particular integral. Furthermore, $\mathbb{P}(w)_K$ is normal because $K[x_0, x_1]$ is integrally closed. This proves the claim. □

5 | SOME RESULTS ON SCALING IDEALS

Let K be a number field. We prove two elementary results about scaling ideals.

Lemma 5.1. *Let $w = (w_0, w_1)$ be a pair of positive integers. We consider $K[x_0, x_1]$ as a graded K-algebra by assigning weight w_i to x_i. Let $f \in K[x_0, x_1]$ be homogeneous of degree d. Let $\mathfrak{a}(f)$ be the fractional ideal generated by the coefficients of f. Then for all $z \in K^2$, we have*

$$f(z) \in \mathfrak{a}(f)\mathcal{I}_w(z)^d.$$

Proof. We abbreviate

$$\mathfrak{m} = \mathcal{I}_w(z),$$

so we have $z_0 \in \mathfrak{m}^{w_0}$ and $z_1 \in \mathfrak{m}^{w_1}$. We write

$$f = \sum_{k_0,k_1} a_{k_0,k_1} x_0^{k_0} x_1^{k_1}$$

where the sum ranges over all pairs (k_0, k_1) of nonnegative integers such that $k_0 w_0 + k_1 w_1 = d$, and $a_{k_0,k_1} \in K$. We now compute

$$\begin{aligned} f(z_0, z_1) &= \sum_{k_0,k_1} a_{k_0,k_1} z_0^{k_0} z_1^{k_1} \\ &\in \sum_{k_0,k_1} a_{k_0,k_1} (\mathfrak{m}^{w_0})^{k_0} (\mathfrak{m}^{w_1})^{k_1} \\ &= \sum_{k_0,k_1} a_{k_0,k_1} \mathfrak{m}^d \\ &= \mathfrak{a}(f)\mathfrak{m}^d, \end{aligned}$$

which proves the claim. □

Lemma 5.2. *Let $z \in K$, and let*

$$h = x^d + c_1 x^{d-1} + \cdots + c_d \in K[x]$$

be a monic polynomial such that $h(z) = 0$. Suppose $\mathfrak{b}_1, \dots, \mathfrak{b}_d$ are fractional ideals of K such that $c_i \in \mathfrak{b}_i$ for all i. Then we have

$$z \in \mathcal{I}_{(1,\dots,d)}(\mathfrak{b}_1, \dots, \mathfrak{b}_d).$$

Proof. If all the $\mathfrak{b}_i$ are zero, then z vanishes and the claim is trivial. Now assume not all of the $\mathfrak{b}_i$ are zero. We write

$$\mathfrak{a} = \mathcal{I}_{(1,\dots,d)}(\mathfrak{b}_1, \dots, \mathfrak{b}_d)^{-1} = \{a \in K \mid a\mathfrak{b}_1, a^2\mathfrak{b}_2, \dots, a^d\mathfrak{b}_d \subseteq \mathcal{O}_K\}.$$

Then for all $a \in \mathfrak{a}$ we have

$$0 = a^d h(z) = (az)^d + (ac_1)(az)^{d-1} + \cdots + (a^d c_d).$$

By assumption, each $a^i c_i$ lies in $a^i \mathfrak{b}_i$ and hence in $\mathcal{O}_K$. This shows that az is integral over $\mathcal{O}_K$. Thus we have $\mathfrak{a}z \subseteq \mathcal{O}_K$ and hence $z \in \mathfrak{a}^{-1}$. ☐

6 | BEHAVIOUR OF SIZE FUNCTIONS UNDER MORPHISMS

Let K be a number field. Let $w = (w_0, w_1)$ and $u = (u_0, u_1)$ be two pairs of positive integers, and let $\phi : \mathbb{P}(w)_K \to \mathbb{P}(u)_K$ be a nonconstant morphism. Our goal in this section will be to study how the size of a point in $\mathbb{P}(w)(K)$ relates to the size of its image under ϕ.

By Lemma 4.1, the morphism ϕ is defined by a pair of nonconstant homogeneous polynomials $f_0, f_1 \in K[x_0, x_1]$ of degrees eu_0 and eu_1, respectively, where e is the reduced degree of ϕ. For $i \in \{0, 1\}$, let $\mathfrak{a}_i$ be the fractional ideal generated by the coefficients of f_i.

Lemma 6.1. *For all $z \in K^2$, we have*

$$\mathcal{I}_u(f(z)) \subseteq \mathcal{I}_u(\mathfrak{a}_0, \mathfrak{a}_1)\mathcal{I}_w(z)^e.$$

Proof. We abbreviate

$$\mathfrak{m} = \mathcal{I}_w(z).$$

Since f_i is homogeneous of degree eu_i, Lemma 5.1 gives

$$f_i(z) \in \mathfrak{a}_i \mathfrak{m}^{eu_i}.$$

It follows that

$$\mathcal{I}_u(f(z)) \subseteq \mathcal{I}_u(\mathfrak{a}_0 \mathfrak{m}^{eu_0}, \mathfrak{a}_1 \mathfrak{m}^{eu_1}) = \mathcal{I}_u(\mathfrak{a}_0, \mathfrak{a}_1)\mathfrak{m}^e,$$

which proves the claim. ☐

For $i \in \{0, 1\}$, we write the rational number w_i/e in reduced form as

$$\frac{w_i}{e} = \frac{\nu_i}{\delta_i}$$

with ν_i, δ_i coprime positive integers.

By Lemma 4.4, there are integers $d_i > 0$ and polynomials $g_{i,j} \in K[y_0, y_1]$ (for $i = 0, 1$ and $j = 1, \ldots, d_i$) satisfying

$$x_i^{d_i} + g_{i,1}(f_0, f_1)x_i^{d_i-1} + \cdots + g_{i,d_i}(f_0, f_1) = 0 \quad \text{in } K[x_0, x_1]. \tag{6.1}$$

After taking homogeneous components of degree $d_i w_i$, we may and do assume that each $g_{i,j}(f_0, f_1)$ is homogeneous of degree jw_1. After dividing by a power of x_i if necessary, we may and do also assume $g_{i,d_i} \neq 0$. We write

$$g_{i,j} = \sum_{\substack{k_0,k_1 \geqslant 0 \\ e(k_0u_0+k_1u_1)=jw_i}} \gamma_{i,j,(k_0,k_1)} y_0^{k_0} y_1^{k_1} \quad \text{with } \gamma_{i,j,(k_0,k_1)} \in K.$$

In particular, if $g_{i,j} \neq 0$, then e divides jw_i, so j is a multiple of the denominator of w_i/e; in other words, there is a positive integer l with $j = l\delta_i$. Since we have ensured that g_{i,d_i} is nonzero, we obtain in particular a positive integer m_i with

$$d_i = m_i\delta_i,$$

and all j for which $g_{i,j}$ does not vanish are of the form $j = l\delta_i$ with $1 \leqslant l \leqslant m_i$. We can therefore rewrite (6.1) as

$$x_i^{m_i\delta_i} + \sum_{l=1}^{m_i} g_{i,l\delta_i}(f_0, f_1)x_i^{(m_i-l)\delta_i} = 0 \quad \text{in } K[x_0, x_1] \tag{6.2}$$

and note that

$$g_{i,l\delta_i} = \sum_{\substack{k_0,k_1 \geqslant 0 \\ k_0u_0+k_1u_1=l\nu_i}} \gamma_{i,l\delta_j,(k_0,k_1)} y_0^{k_0} y_1^{k_1}.$$

For $i \in \{0, 1\}$ and $1 \leqslant l \leqslant m_i$, we write $\mathfrak{c}_{i,l}$ for the fractional ideal generated by the coefficients of $g_{i,l\delta_i}$, that is,

$$\mathfrak{c}_{i,l} = (\gamma_{i,l\delta_i,(k_0,k_1)} \mid k_0, k_1 \geqslant 0, k_0u_0 + k_1u_1 = l\nu_i).$$

For $i \in \{0, 1\}$, we write

$$\mathfrak{d}_i = \mathcal{I}_{(1,\ldots,m_i)}(\mathfrak{c}_{i,}, \ldots, \mathfrak{c}_{i,m_i}).$$

Lemma 6.2. *For all $z \in K^2$ and $i \in \{0, 1\}$, we have*

$$z_i^{\delta_i} \in \mathfrak{d}_i \mathcal{I}_u(f(z))^{\nu_i}.$$

Proof. For $i = 0, 1$ and $l = 0, \dots, m_i$, we write

$$c_{i,l} = g_{i,l\delta_i}(f(z)) \in K.$$

Substituting $(x_0, x_1) = (z_0, z_1)$ in (6.2), we obtain

$$(z_i^{\delta_i})^{m_i} + \sum_{l=1}^{m_i} c_{i,l}(z_i^{\delta_i})^{m_i - l} = 0 \quad \text{for } i = 0, 1.$$

We abbreviate

$$\mathfrak{m} = \mathcal{I}_u(f(z)).$$

Since $g_{i,l\delta_j}$ is homogeneous of degree $l\nu_i$, Lemma 5.1 gives

$$c_{i,l} \in \mathfrak{c}_{i,l}\mathfrak{m}^{l\nu_i}.$$

Applying Lemma 5.2, we obtain

$$z_i^{\delta_i} \in \mathcal{I}_{(1,\dots,m_i)}(\mathfrak{c}_{i,1}\mathfrak{m}^{\nu_i}, \dots, \mathfrak{c}_{i,m_i}\mathfrak{m}^{m_i\nu_i}) \quad \text{for } i = 0, 1.$$

This last ideal equals $\mathcal{I}_{(1,\dots,m_i)}(\mathfrak{c}_{i,1}, \dots, \mathfrak{c}_{i,m_i})\mathfrak{m}^{\nu_i} = \mathfrak{d}_i\mathfrak{m}^{\nu_i}$. □

Corollary 6.3. *For all $(z_0, z_1) \in K^2$ and $i \in \{0, 1\}$, we have*

$$\mathcal{I}_{(\nu_0,\nu_1)}(z_0^{\delta_0}, z_1^{\delta_1}) \subseteq \mathcal{I}_{(\nu_0,\nu_1)}(\mathfrak{d}_0, \mathfrak{d}_1)\mathcal{I}_u(f(z)).$$

Theorem 6.4. *Let K be a number field, let u, w be two pairs of positive integers, and let $\phi : \mathbb{P}(w)_K \to \mathbb{P}(u)_K$ be a nonconstant morphism. Let e be the reduced degree of ϕ (see Definition 4.2), and for $i = 0, 1$ write $w_i/e = \nu_i/\delta_i$ with ν_i, δ_i coprime positive integers. Then for all $z \in \mathbb{P}(w)(K)$, we have*

$$S_u(\phi(z)) \ll S_w(z)^e$$

and

$$S_u(\phi(z)) \gg S_{(\nu_0,\nu_1)}(z_0^{\delta_0}, z_1^{\delta_1}),$$

where the implied constants depend only on K, u, w and ϕ.

Proof. Lemma 4.1 gives us homogeneous polynomials $f_0, f_1 \in K[x_0, x_1]$ such that ϕ is defined by (f_0, f_1). For every Archimedean place v of K, the set $\mathbb{P}(w)(K_v)$ of points of $\mathbb{P}(w)$ over the completion K_v of K at v is in a natural way a compact topological space. We consider the function

$$q_v : \mathbb{P}(w)(K_v) \longrightarrow \mathbb{R}_{>0}$$
$$z \longmapsto \frac{\max_{0\leqslant i\leqslant 1} |f_i(z)|_v^{1/u_i}}{\max_{0\leqslant i\leqslant 1} |z_i|_v^{e/w_i}}.$$

Using the definitions of the size functions and the q_v, we compute

$$\begin{aligned}\frac{S_u(\phi(z))}{S_w(z)^e} &= \frac{\mathrm{N}(\mathcal{I}_u(f(z)))^{-1}H_{u,\infty}(f(z))}{\mathrm{N}(\mathcal{I}_w(z))^{-e}H_{w,\infty}(z)^e}\\ &= \mathrm{N}\big(\mathcal{I}_w(z)^e\mathcal{I}_u(f(z))^{-1}\big)\prod_{v\in\Omega_{K,\infty}} q_v(z)\end{aligned}$$

and

$$\begin{aligned}\frac{S_u(\phi(z))}{S_{(\nu_0,\nu_1)}(z_0^{\delta_0},z_1^{\delta_1})} &= \frac{\mathrm{N}(\mathcal{I}_u(f(z)))^{-1}H_{u,\infty}(f(z))}{\mathrm{N}(\mathcal{I}_{(\nu_0,\nu_1)}(z_0^{\delta_0},z_1^{\delta_1}))^{-1}H_{(\nu_0,\nu_1),\infty}(z_0^{\delta_0},z_1^{\delta_1})}\\ &= \mathrm{N}\big(\mathcal{I}_{(\nu_0,\nu_1)}(z_0^{\delta_0},z_1^{\delta_1})\mathcal{I}_u(f(z))^{-1}\big)\prod_{v\in\Omega_{K,\infty}} q_v(z).\end{aligned}$$

Let $\mathfrak{a}_i$, $\mathfrak{d}_i$ $(i=0,1)$ be the fractional ideals defined earlier. By Lemma 6.1, we have

$$\mathcal{I}_w(z)^e\mathcal{I}_u(f(z))^{-1} \supseteq \mathcal{I}_u(\mathfrak{a}_0,\mathfrak{a}_1)^{-1},$$

and hence

$$\mathrm{N}\big(\mathcal{I}_w(z)^e\mathcal{I}_u(f(z))^{-1}\big) \leqslant \mathrm{N}(\mathcal{I}_u(\mathfrak{a}_0,\mathfrak{a}_1))^{-1}.$$

By Corollary 6.3, we have

$$\mathcal{I}_{(\nu_0,\nu_1)}(z_0^{\delta_0},z_1^{\delta_1})\mathcal{I}_u(f(z))^{-1} \subseteq \mathcal{I}_{(\nu_0,\nu_1)}(\mathfrak{d}_0,\mathfrak{d}_1),$$

and hence

$$\mathrm{N}\big(\mathcal{I}_{(\nu_0,\nu_1)}(z_0^{\delta_0},z_1^{\delta_1})\mathcal{I}_u(f(z))^{-1}\big) \geqslant \mathrm{N}(\mathcal{I}_{(\nu_0,\nu_1)}(\mathfrak{d}_0,\mathfrak{d}_1)).$$

Finally, for each $v\in\Omega_{K,\infty}$, the function $q_v : \mathbb{P}(w)(K_v)\to\mathbb{R}_{>0}$ is bounded by compactness. From this the theorem follows. $\square$

Corollary 6.5. *In the setting of Theorem 6.4, suppose $e=1$ or $w=(1,1)$ holds. Then for all $z\in\mathbb{P}(w)(K)$, we have*

$$S_u(\phi(z)) \asymp S_w(z)^e,$$

where the implied constants depend only on K, u, w and ϕ.

Proof. First suppose $e = 1$. Then we have $\delta_i = 1$ and $\nu_i = w_i$ for $i \in \{0, 1\}$, and hence

$$S_{\nu_0,\nu_1}(z_0^{\delta_0}, z_1^{\delta_1}) = S_w(z) = S_w(z)^e.$$

Next suppose $w = (1, 1)$. Then we have $\delta_i = e$ and $\nu_i = 1$ for $i \in \{0, 1\}$, and hence

$$S_{(\nu_0,\nu_1)}(z_0^{\delta_0}, z_1^{\delta_1}) = S_{(1,1)}(z_0^e, z_1^e) = S_{(1,1)}(z_0, z_1)^e = S_w(z)^e.$$

In both cases, Theorem 6.4 gives the result. □

Remark 6.6. The condition '$e = 1$ or $w = (1, 1)$' in Corollary 6.5 is reminiscent of the condition '$n = 1$ or $m = 1$' in [11, Proposition 2.1].

Remark 6.7. By Remark 4.3, the assumption $e = 1$ or $w = (1, 1)$ implies that every morphism satisfying the conditions of Corollary 6.5 is representable. However, the conclusion of Corollary 6.5 no longer holds when '$e = 1$ or $w = (1, 1)$' is weakened to 'ϕ is representable'. For example, take $u = (1, 3)$ and $w = (1, 3)$, and consider the morphism

$$\begin{aligned} \phi\colon \mathbb{P}(1,3) &\longrightarrow \mathbb{P}(1,3) \\ (x_0, x_1) &\longmapsto (x_0^2, x_1^2), \end{aligned}$$

which has $e = 2$ and is therefore representable. For all primes p, taking $x = (p, p^2) \in \mathbb{P}(1,3)(\mathbb{Q})$, we get

$$\begin{aligned} S_w(x) &= S_{(1,3)}(p, p^2) = p, \\ S_u(\phi(x)) &= S_{(1,3)}(p^2, p^4) = S_{(1,3)}(p, p) = p. \end{aligned}$$

On the other hand, for all primes p, taking $x = (1, p) \in \mathbb{P}(1,3)(\mathbb{Q})$, we get

$$\begin{aligned} S_w(x) &= S_{(1,3)}(1, p) = p^{1/3}, \\ S_u(\phi(x)) &= S_{(1,3)}(1, p^2) = p^{2/3}. \end{aligned}$$

This shows that the ratio between $S_u(\phi(x))$ and any fixed power of $S_w(x)$ is unbounded as x varies.

7 | POINTS OF BOUNDED SIZE ON MODULAR CURVES

Let $Y(1)$ be the moduli stack over $\mathbb{Q}$ of elliptic curves. There is an open immersion

$$\iota\colon Y(1) \hookrightarrow \mathbb{P}(4,6)_{\mathbb{Q}}$$

defined as follows: given an elliptic curve E over a $\mathbb{Q}$-scheme S, then Zariski locally on S we can choose a nonzero differential ω and define

$$\iota(E) = (c_4(E, \omega), c_6(E, \omega)),$$

where c_4 and c_6 are defined in the usual way. A different choice of ω gives the same point of $\mathbb{P}(4,6)_{\mathbb{Q}}$, so ι is well defined.

Definition 7.1. Let K be a number field. Using the morphism ι, we define the *size function*

$$S_K\colon Y(1)(K) \longrightarrow \mathbb{R}_{>0}$$

as the composition

$$Y(1)(K) \xrightarrow{\iota(K)} \mathbb{P}(4,6)(K) \xrightarrow{S_{(4,6),K}} \mathbb{R}_{>0}.$$

Remark 7.2. If E is given in short Weierstrass form as

$$E\colon y^2 = x^3 + ax + b,$$

then we have

$$\iota(E) = (-48a, -864b)$$

and hence

$$S_K(E) = S_{(4,6),K}(-48a, -864b) \asymp \max\{|a|^{1/4}, |b|^{1/6}\}.$$

This shows that if E is an elliptic curve over $\mathbb{Q}$, then the ratio between $S_{\mathbb{Q}}(E)^{12}$ and the height of E

$$h(E) = \max\{|a|^3, |b|^2\},$$

as defined in [11], is bounded from above and below by a constant.

Now let n be a positive integer, and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let K_G be the subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$ fixed by G, where G acts on $\mathbb{Q}(\zeta_n)$ by $(g, \zeta_n) \mapsto \zeta_n^{\det g}$. Let Y_G be the moduli stack of elliptic curves with G-level structure, viewed as an algebraic stack over K_G. There is a canonical morphism of stacks

$$\pi_G\colon Y_G \to Y(1)_{K_G}.$$

Let K be a finite extension of K_G. We define

$$\mathcal{E}_{G,K} = \{\text{elliptic curves admitting a } G\text{-level structure over } K\}/\cong$$

and

$$N_{G,K}(X) = \#\{E \in \mathcal{E}_{G,K} \mid S_K(E)^{12} \leqslant X\}.$$

Lemma 7.3. *Let n be a positive integer, let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, and let w be a pair of positive integers. The following are equivalent.*

(i) *There is a commutative diagram*

$$\begin{tikzcd} Y_G \arrow[r, "\iota_G"] \arrow[d, "\pi_G"'] & \mathbb{P}(w)_{K_G} \arrow[d, "\phi"] \\ Y(1)_{K_G} \arrow[r, "\iota"] & \mathbb{P}(4,6)_{K_G} \end{tikzcd}$$

of algebraic stacks over K_G, where ι_G is an open immersion and ϕ is representable.

(ii) *The integral closure of $X(1) = \mathbb{P}(4,6)$ in the function field of Y_G is isomorphic to $\mathbb{P}(w)$.*

(iii) *The moduli space of generalized elliptic curves with G-level structure is isomorphic to $\mathbb{P}(w)$.*

Proof. The equivalence of (ii) and (iii) follows from the fact that the integral closure from (ii) is canonically isomorphic to the moduli space of generalized elliptic curves with G-level structure [6, IV, Théorème 6.7(ii)].

The implication (ii) $\Longrightarrow$ (i) follows from the fact that the integral closure of $X(1)$ in the function field of Y_G fits in a commutative diagram as above.

The implication (i) $\Longrightarrow$ (ii) follows from Corollary 4.7 applied to $V = \iota_G(Y_G)$. □

Remark 7.4. If G is a group satisfying the equivalent conditions of Lemma 7.3, then the coarse moduli space of X_G is isomorphic to $\mathbb{P}^1$. The converse does not hold. For example, taking G to be the group of upper-triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ gives the modular curve $X_G = X_0(3)$. The coarse moduli space of $X_0(3)$ is isomorphic to $\mathbb{P}^1$, but $X_0(3)$ itself is not a weighted projective line. One way to see this is to note that the Picard group of a weighted projective line is infinite cyclic, generated by the class of the tautological line bundle [10, Example 7.27], but considering dimensions of spaces of global sections shows that the line bundle of modular forms on $X_0(3)$ cannot be identified with any power of the tautological bundle on a weighted projective line.

Remark 7.5. The equivalent conditions of Lemma 7.3 hold if the graded K_G-algebra of modular forms for G is generated by two homogeneous elements. Over $\mathbb{C}$, the groups for which this happens were classified by Bannai, Koike, Munemasa and Sekiguchi [1].

Theorem 7.6. *Let n be a positive integer, and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let K_G be the fixed field of the action of G on $\mathbb{Q}(\zeta_n)$ given by $(g, \zeta_n) \mapsto \zeta_n^{\det g}$. Assume that G satisfies the equivalent conditions of Lemma 7.3 for some (w_0, w_1), and let $e(G)$ be the reduced degree of the canonical morphism $X_G \to X(1)$ (see Definition 4.2). Furthermore, assume $e(G) = 1$ or $w = (1,1)$ holds. Then for every finite extension K of K_G, we have*

$$N_{G,K}(X) \asymp X^{1/d(G)} \quad \text{as } X \to \infty,$$

where

$$d(G) = \frac{12e(G)}{w_0 + w_1}.$$

Proof. Using the commutative diagram of Lemma 7.3 and noting that for counting purposes we may ignore the cusps (cf. [7, Remark 6.2]), we obtain

$$N_{G,K}(X) \asymp \#\{z \in \mathbb{P}(w)(K) \mid S_{(4,6)}(\phi(z))^{12} \leqslant X\}.$$

By Corollary 6.5 with $u = (4,6)$, the quotient $S_{(4,6)}(\phi(z))/S_w(z)^e$ is bounded. This implies

$$N_{G,K}(X) \asymp \#\{z \in \mathbb{P}(w)(K) \mid S_w(z) \leqslant X^{1/(12e(G))}\}.$$

Applying Theorem 3.8, we obtain

$$N_{G,K}(X) \asymp X^{(w_0+w_1)/(12e(G))}.$$

This proves the claim. □

8 | EXAMPLES

The groups corresponding to the 15 torsion groups from Mazur's theorem satisfy the conditions of Lemma 7.3. In Table 1, we list these groups and a few more satisfying these conditions.

For positive integers $m \mid n$, we write

$$G(m,n) = \left\{ g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \;\middle|\; g = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \text{ and } g \equiv \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix} \pmod{m} \right\}.$$

We also put

$$G_1(n) = G(1,n)$$

and

$$G_0(n) = \left\{ g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \;\middle|\; g = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}.$$

For each group G, we give its inverse image Γ under the canonical group homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, the index of Γ in $\mathrm{SL}_2(\mathbb{Z})$, the weights of the corresponding weighted projective line, and the values $e(G)$ and $d(G)$. The first 12 groups can also be found in [13, Examples 2.1 and Example 2.5], and the 12 groups with $e(G) = 1$ can also be found in [1, Table 1]. By construction, for all groups G in the table, the determinant $G \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective, hence the index $[\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : G]$ equals $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, and K_G equals $\mathbb{Q}$. Furthermore, we note that the numbers $e(G)$ and $d(G)$ can be expressed as

$$e(G) = \frac{w_0 w_1}{24}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma],$$

$$d(G) = \frac{w_0 w_1}{2(w_0 + w_1)}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma].$$

TABLE 1 A selection of groups satisfying the conditions of Lemma 7.3. The first 15 groups are those appearing in Mazur's theorem

G	Γ	$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$	(w_0, w_1)	$e(G)$	$d(G)$
$G_1(1)$	$\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$	1	(4,6)	1	6/5
$G_1(2)$	$\Gamma_1(2) = \Gamma_0(2)$	3	(2,4)	1	2
$G_1(3)$	$\Gamma_1(3)$	8	(1,3)	1	3
$G_1(4)$	$\Gamma_1(4)$	12	(1,2)	1	4
$G_1(5)$	$\Gamma_1(5)$	24	(1,1)	1	6
$G_1(6)$	$\Gamma_1(6)$	24	(1,1)	1	6
$G_1(7)$	$\Gamma_1(7)$	48	(1,1)	2	12
$G_1(8)$	$\Gamma_1(8)$	48	(1,1)	2	12
$G_1(9)$	$\Gamma_1(9)$	72	(1,1)	3	18
$G_1(10)$	$\Gamma_1(10)$	72	(1,1)	3	18
$G_1(12)$	$\Gamma_1(12)$	96	(1,1)	4	24
$G(2,2)$	$\Gamma(2)$	6	(2,2)	1	3
$G(2,4)$	$\Gamma(2,4)$	24	(1,1)	1	6
$G(2,6)$	$\Gamma(2,6)$	48	(1,1)	2	12
$G(2,8)$	$\Gamma(2,8)$	96	(1,1)	4	24
$G_0(4)$	$\Gamma_0(4)$	6	(2,2)	1	3
$G(4,4)$	$\Gamma(4)$	48	(1,1)	2	12
$G_0(8) \cap G_1(4)$	$\Gamma_0(8) \cap \Gamma_1(4)$	24	(1,1)	1	6
$G(3,3)$	$\Gamma(3)$	24	(1,1)	1	6
$G(3,6)$	$\Gamma(3,6)$	72	(1,1)	3	18
$G_0(9) \cap G_1(3)$	$\Gamma_0(9) \cap \Gamma_1(3)$	24	(1,1)	1	6
$G(5,5)$	$\Gamma(5)$	120	(1,1)	5	30

9 | FUTURE WORK

In work of Manterola Ayala and the first author (see [12]), results are proved that make it possible to count points of a moduli stack of the form $\mathbb{P}(w)$ directly with respect to the pull-back of the size function from $X(1)$, rather than first relating this pull-back to the standard size function on $\mathbb{P}(w)$. This approach requires extending the work of Deng [7], but is conceptually simpler than the approach we have taken here. A similar result has been proved independently by Phillips [15, Theorem 1.2.2].

Phillips has also obtained a result similar to Theorem 7.6 for moduli stacks of elliptic curves that are of the form [15, Theorem 5.1.4]. An example of such a moduli stack is $X_0(6)$, so this result enables one to count elliptic curves with a 6-isogeny over any number field.

APPENDIX A: MORPHISMS BETWEEN QUOTIENT STACKS

In this appendix, we assume some knowledge of stacks. We place ourselves in the following situation. Let S be a scheme, let G and H be two group schemes over S, and let $m_G : G \times_S G \to G$ and $m_H : H \times_S H \to H$ be the group operations. Let X and Y be two S-schemes, let $a : G \times_S X \to X$ be a left action of G on X, and let $b : H \times_S Y \to Y$ be a left action of H on Y. Let $p_2 : G \times_S X \to X$

be the second projection, and let $p_{2,3}\colon G\times_S G\times_S X\to G\times_S X$ be the projection onto the second and third factors.

We consider the quotient stacks $[G\backslash X]$ and $[H\backslash Y]$ over (the *fppf* site of) S, writing quotients on the left because a and b are left actions. Below we give an explicit description of the groupoid of morphisms $[G\backslash X]\to[H\backslash Y]$ of stacks over S. For this, we will use the following description of morphisms from the quotient stack $[G\backslash X]$ to another stack $\mathcal{Y}$ given by Noohi [14, Proposition 3.19]; see also [18, tag 044U] for part of this statement.

Lemma A.1. *Let $\mathcal{Y}$ be a stack in groupoids over S, and let $C([G\backslash X],\mathcal{Y})$ be the following groupoid. The objects are the pairs (f,h) where $f\colon X\to\mathcal{Y}$ is a morphism of stacks and h is a descent datum for f, that is, an isomorphism $h\colon f\circ p_2\xrightarrow{\sim}f\circ a$ of functors $G\times_S X\to\mathcal{Y}$ satisfying*

$$(m_G\times\mathrm{id}_X)^*h=(\mathrm{id}_G\times a)^*h\circ p_{2,3}^*h.$$

The morphisms from (f,h) to (f',h') are the isomorphisms $c\colon f\xrightarrow{\sim}f'$ of functors $X\to\mathcal{Y}$ satisfying

$$a^*c\circ h=h'\circ p_2^*c.$$

Then the groupoid of morphisms $[G\backslash X]\to\mathcal{Y}$ is canonically equivalent to $C([G\backslash X],\mathcal{Y})$.

To state the next lemma, we recall the following. Given a left action of a group Γ on a set Z, the *quotient groupoid* $\Gamma\setminus\!\!\setminus Z$ is the following groupoid: the set of objects is Z, the morphisms $z\to z'$ are the elements $\gamma\in\Gamma$ with $\gamma z=z'$, and composition of morphisms is the group operation in Γ. The set of isomorphism classes of $\Gamma\setminus\!\!\setminus Z$ is just the quotient set $\Gamma\backslash Z$.

Lemma A.2. *In the above situation, assume in addition that all H-torsors on X are trivial. Let Z be the set of pairs $(f\colon X\to Y,h\colon G\times_S X\to H)$ of morphisms of S-schemes such that for all S-schemes T, all $x\in X(T)$ and all $g,g'\in G(T)$ we have*

$$h(g'g,x)=h(g',gx)h(g,x)\tag{A.1}$$

and

$$f(a(g,x))=b(h(g,x),f(x)).\tag{A.2}$$

Let the group $H(X)$ act on Z by

$$(c,(f,h))\mapsto(f',h'),$$

where f' and h' are defined on points as follows: for all S-schemes T, all $x\in X(T)$ and all $g\in G(T)$, we have

$$f'(x)=b(c(x),f(x))$$

and

$$h'(g,x) = c(a(g,x))h(g,x)c(x)^{-1}.$$

Then the groupoid of morphisms $[G\backslash X] \to [H\backslash Y]$ is canonically equivalent to the quotient groupoid $H(X) \backslash\backslash Z$. In particular, there is a canonical bijection between the set of isomorphism classes of such morphisms and the quotient set $H(X)\backslash Z$.

Proof. We apply Lemma A.1 with $\mathcal{Y} = [H\backslash Y]$. Because all H-torsors on X are trivial, the groupoid of morphisms $X \to [H\backslash Y]$ is canonically equivalent to the groupoid $D(X, [H\backslash Y])$ defined as follows: the objects of $D(X, [H\backslash Y])$ are the morphisms $f : X \to Y$ of schemes, and the isomorphisms $f \xrightarrow{\sim} f'$ in $D(X, [H\backslash Y])$ are the elements $c \in H(X)$ such that the diagram

$$\begin{tikzcd} X \arrow[r, "f'"] \arrow[d, "{(c,f)}"'] & Y \\ H \times_S Y \arrow[ur, "b"'] & \end{tikzcd}$$

is commutative. Similarly, the isomorphisms $f \circ p_2 \xrightarrow{\sim} f \circ a$ in the groupoid of morphisms $G \times_S X \to [H\backslash Y]$ correspond to the elements $h \in H(G \times_S X)$ such that the diagram

$$\begin{tikzcd} G \times_S X \arrow[r, "f \circ a"] \arrow[d, "{(h, f\circ p_2)}"'] & X \\ H \times_S Y \arrow[ur, "b"'] & \end{tikzcd}$$

is commutative. Furthermore, such an h is a descent datum for f if and only if the diagram

$$\begin{tikzcd} G \times_S G \times_S X \arrow[r, "m_G \times \mathrm{id}_X"] \arrow[d, "{(\mathrm{id}_G \times a, p_{2,3})}"'] & G \times_S X \arrow[r, "h"] & H \\ (G \times_S X) \times_S (G \times_S X) \arrow[r, "h \times h"] & H \times_S H \arrow[ur, "m_H"'] & \end{tikzcd}$$

is commutative. On T-valued points, the commutativity of the last two diagrams comes down to (A.2) and (A.1), respectively, so the objects of $C([G\backslash X], [H\backslash Y])$ correspond to the elements of Z. The isomorphisms $(f, h) \xrightarrow{\sim} (f', h')$ in $C([G\backslash X], [H\backslash Y])$ correspond to the elements $c \in H(X)$ as above such that in addition the diagram

$$\begin{tikzcd} G \times_S X \arrow[r, "{(c\circ a, h)}"] \arrow[d, "{(h', c\circ p_2)}"'] & H \times_S H \arrow[d, "m_H"] \\ H \times_S H \arrow[r, "m_H"] & H \end{tikzcd}$$

is commutative. Equivalently, these isomorphisms correspond to the elements $c \in H(X)$ sending (f, h) to (f', h') under the given action of $H(X)$ on Z. $\square$

ACKNOWLEDGEMENTS

We are grateful to Pieter Moree for his effort in organizing our collaboration at MPIM Bonn, at which a large part of the work leading to this paper was conducted. We would also like to thank Soumya Sankar and Brandon Boggess for sending us an early version of their manuscript [2], and Tristan Phillips for sending us an early version of his manuscript [15]. Finally, we thank the referee for several useful comments, which in particular led to simpler proofs of Lemma 4.5 and Lemma A.2.

This work was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313. The first-named author was partially supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium programme (project number 024.003.037). This project began during a joint stay of the authors at the Max-Planck-Institut für Mathematik, Bonn, in October 2018. We are grateful to MPIM for its funding and hospitality.

REFERENCES

1. E. Bannai, M. Koike, A. Munemasa, and J. Sekiguchi, *Some results on modular forms—subgroups of the modular group whose ring of modular forms is a polynomial ring*, Groups and combinatorics—in memory of Michio Suzuki, Adv. Stud. Pure Math., 32, Math. Soc. Japan, Tokyo, 2001, pp. 245–254.
2. B. Boggess and S. Sankar, *Counting elliptic curves with a rational N-isogeny for small N*, Preprint, https://arxiv.org/abs/2009.05223.
3. B. Conrad, *Arithmetic moduli of generalized elliptic curves*, J. Inst. Math. Jussieu **6** (2007), no. 2, 209–278.
4. J. Cullinan, M. Kenney, and J. Voight, *On a probabilistic local-global principle for torsion on elliptic curves*, J. Théor. Nombres Bordeaux, to appear.
5. R. Darda, *Rational points of bounded height on weighted projective stacks*, Ph.D. thesis, Sorbonne Université. https://arxiv.org/abs/2106.10120.
6. 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, Springer, Berlin, 1973, pp. 143–316.
7. A.-W. Deng, *Rational points on weighted projective spaces*, Preprint, https://arxiv.org/abs/math/9812082.
8. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, vol. 150, Springer, New York, NY, 1995.
9. J. S. Ellenberg, M. Satriano, and D. Zureick-Brown, *Heights on stacks and a generalized Batyrev–Manin–Malle conjecture*, Preprint, https://arxiv.org/abs/2106.11340.
10. B. Fantechi, E. Mann, and F. Nironi, *Smooth toric Deligne-Mumford stacks*, J. reine angew. Math. **648** (2010), 201–244.
11. R. Harron and A. Snowden, *Counting elliptic curves with prescribed torsion*, J. reine angew. Math. **729** (2017), 151–170.
12. I. Manterola Ayala, *Counting rational points on weighted projective spaces over number fields*, MSc thesis, Universität Zürich, 2021.
13. L. Meier, *Additive decompositions for rings of modular forms*, Preprint, https://arxiv.org/abs/1710.03461.

14. B. Noohi, *Foundations of topological stacks I*, Preprint, https://arxiv.org/abs/math/0503247.
15. T. Phillips, *Rational points of bounded height on genus zero modular curves and average analytic ranks of elliptic curves over number fields*. Preprint, https://arxiv.org/abs/2201.10624.
16. M. Pizzo, C. Pomerance, and J. Voight, *Counting elliptic curves with an isogeny of degree three*, Proc. Amer. Math. Soc. Ser. B **7** (2020), 28–42.
17. C. Pomerance and E. F. Schaefer, *Elliptic curves with Galois-stable cyclic subgroups of order 4*, Res. Number Theory **7** (2021), 35.
18. The Stacks project authors, The Stacks project, https://stacks.math.columbia.edu, 2020.