# COUNTING ELLIPTIC CURVES WITH PRESCRIBED LEVEL STRUCTURES OVER NUMBER FIELDS

PETER BRUIN AND FILIP NAJMAN

Abstract. Harron and Snowden [8] 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 We prove our results by defining a *size function* on $\mathbb{P}(w_0, w_1)$ following unpublished work of Deng [5], and working out how to count the number of points on $\mathbb{P}(w_0, w_1)$ up to size $X$.

## 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 $r \geq 0$, 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 [8] 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

$$\rho_{E,n} \colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

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 $N_{G,K} \colon \mathbb{R}_{>0} \to \mathbb{Z}_{\geq 0}$ by

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

---

*Date*: August 12, 2020.

2010 *Mathematics Subject Classification.* 11G05, 11G18, 11G50, 14D23, 14G40.

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.

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 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 $K_G$. By Lemma 4.1, we can then attach a positive integer $e$ to the canonical morphism $X_G \to X(1)$. 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 $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. 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 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 $e$ be as in Lemma 4.1. Furthermore, assume $e = 1$ or $w = (1, 1)$ holds. Then for every finite extension $K$ of $K_G$, we have*

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

*where*

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

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 [8, 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 [10] 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.

Similarly, Pomerance and Schaefer [11] 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 $K$; in the case $K = \mathbb{Q}$, this follows from the sharper results of [11].

Cullinan, Kenney and Voight [3, Theorem 1.3.3] proved a sharper version of Theorem 1.1 in the special case where $X_G$ is a projective line (i.e. 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 [8, 11]) correspond to weighted projective lines and are therefore generalized to number fields by Theorem 1.1.

*Remark* 1.2. The 12-th power is included for easier comparison with the height function in [8]; see Remark 7.2.

*Remark* 1.3. Our result gives a more conceptual interpretation of $d(G, K)$; cf. [8, §1.2]. Namely, we show that $d(G, K)$ 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 $e$, 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 [8, Remark 1.5].

## 2. Weighted projective spaces

**Definition 2.1.** Given an $(n+1)$-tuple $w = (w_0, \ldots, w_n)$ 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

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

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

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

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 $\mu_m$. 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 [5]; we do not restrict to weighted projective spaces that are "well-formed" in the sense of [5].

**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 $(\mathfrak{b}_0, \ldots, \mathfrak{b}_n)$ of fractional ideals of $\mathcal{O}_K$, the *scaling ideal* of $(\mathfrak{b}_0, \ldots, \mathfrak{b}_n)$, denoted by $\mathcal{I}_w(\mathfrak{b}_0, \ldots, \mathfrak{b}_n)$, 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 non-zero and satisfies

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

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

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

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

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

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

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

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 $m$-th power free, then 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 $m \ge 2$ and $x \in \mathbb{Z} \setminus \{0\}$ is $m$-th power free, then

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

but

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

**Theorem 3.7.** *Let $n$ be a non-negative integer, let $w = (w_0, \dots, w_n)$ be an $(n+1)$-tuple of positive integers, and let $K$ be a number field. Let $r_1$, $r_2$, $d_K$, $h_K$, $R_K$, $\mu_K$ and $\zeta_K$ be the number of real places, number of non-real complex places, discriminant, class number, regulator, number of roots of unity and Dedekind $\zeta$-function of $K$, respectively. We write*

$$|w| = w_0 + w_1 + \dots + w_n,$$

$$\mu_K^w = \frac{\mu_K}{\gcd\{w_0, w_1, \dots, w_n, \mu_K\}}$$

*and*

$$C_K^w = \frac{h_K R_K}{\mu_K^w \zeta_K(|w|)} \left( \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d_K|}} \right)^{n+1} |w|^{r_1+r_2-1}.$$

*Then we have*

$$\#\{x \in \mathbb{P}(w)(K) \mid S_{w,K}(x) \le T\} \sim C_K^w T^{|w|}.$$

*Proof.* This was proved by Deng [5, Theorem (A)] in the case where $\mathbb{P}(w)$ is *well-formed*, i.e. each $n$ elements from $w$ are coprime. However, the proof works in general with only minor changes: in the paragraph before [5, 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 non-zero contain $\mu_K^w$ points, and the factor $w$ (denoting the number of roots of unity) in [5, Proposition 4.2, Proposition 4.5, Corollary 4.6 and Theorem (A)] has to be replaced by $\mu_K^w$. □

In the remainder of this article, we will only consider *weighted projective lines*, i.e. 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 begin by proving two facts about morphisms $\mathbb{P}(w) \to \mathbb{P}(u)$ showing that they satisfy similar properties as morphisms $\mathbb{P}^1 \to \mathbb{P}^1$.

**Lemma 4.1.** *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:*

1. *There exists $e \in \mathbb{Z}_{\geq 0}$ for which $f_0$ and $f_1$ are homogeneous of degrees $eu_0$ and $eu_1$, respectively.*
2. *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 $\mathbb{P}(w) \to \mathbb{P}(u)$ sending the class of $(f_0, f_1) \in P_{u,w}(K)$ to the morphism induced by the ring 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.3 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 $h$,
- $a\colon G \times X \to X$ is the weight $w$ action, given on points by $a(g, x) = (g^{w_0} x_0, g^{w_1} x_1)$,
- $b\colon H \times Y \to Y$ 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 $h\colon G \times X \to H$ satisfying the "cocycle condition" (7) from Lemma A.3. A morphism $h\colon G \times X \to H$ 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 (7) if and only if $\lambda = 1$, i.e. $h$ is of the form $h(g, x) = g^e$. We now determine the possible pairs $(f, h)$ for a given such $h$. Every morphism $f\colon X \to Y$ is given by a pair $(f_0, f_1) \in R \times R$, and such a pair 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 (8) from Lemma A.3 translates to the condition that $f_j$ is homogeneous of degree $eu_j$ for $j = 0, 1$. In particular, morphisms $f\colon X \to Y$ such that $(f, h)$ defines a morphism $[G\backslash X] \to [H\backslash Y]$ only exist if $e \geq 0$; 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.3. ☐

*Remark* 4.2. One can show that a morphism $\mathbb{P}(u) \to \mathbb{P}(w)$ is representable if and only if the integer $e$ from Lemma 4.1 satisfies

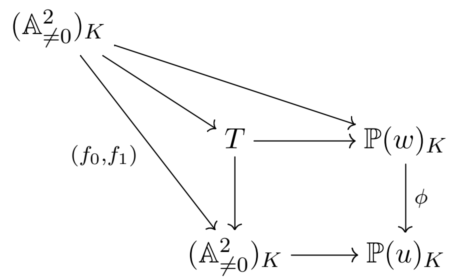
$$\gcd(w_0, e) = \gcd(w_1, e) = 1.$$

**Lemma 4.3.** *Let $K$ be a field, let $u$, $w$ be two pairs of positive integers, and let $\phi\colon \mathbb{P}(w)_K \to \mathbb{P}(u)_K$ be a non-constant representable morphism. Then $\phi$ is finite.*

*Proof.* By Lemma 4.1, the morphism $\phi$ is defined by a pair of homogeneous polynomials $f_0, f_1 \in K[x_0, x_1]$ with $\sqrt{(f_0, f_1)} \supseteq (x_0, x_1)$. Since $\phi$ is non-constant, the polynomials $f_0$ and $f_1$ are non-constant, and hence we actually have $\sqrt{(f_0, f_1)} = (x_0, x_1)$. We consider the graded $K$-algebra $R = K[x_0, x_1]$ and its graded subalgebra $S = K[f_0, f_1]$, and we write $R_+ = Rx_0 + Rx_1$ and $S_+ = Sf_0 + Sf_1$ for their homogeneous maximal ideals. Furthermore, we put $I = Rf_0 + Rf_1 = RS_+$. Then we have $R_+ \supseteq I$ and $R_+^m \subseteq I$ for $m$ sufficiently large. Hence the graded ring $R/I$ is a quotient of $R/R_+^m$ and is therefore finite-dimensional as a $K$-vector space. Choose homogeneous elements $g_1, \ldots, g_r \in R$ 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 $\mathbb{Z}_{\geq 0}$-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 [6, Exercise 4.6]) that $M = 0$ and hence $R = Sg_1 + \cdots + Sg_r$. We conclude that $K[x_0, x_1]$ is finitely generated as a $K[f_0, f_1]$-module. Thus we have a commutative diagram




in which the square (where $T$ is by definition the fibre product, which is a scheme by the representability of $\phi$) is Cartesian and the leftmost morphism is finite. The last two conditions imply that the morphism $T \to (\mathbb{A}^2_{\neq 0})_K$, and therefore $\phi$, is finite. □

**Corollary 4.4.** *With the notation of Lemma 4.3, 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 4.3, the morphism $\phi$ 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 non-negative integers such that $k_0w_0+k_1w_1 = d$, 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 $\mathfrak{b}_1, \ldots, \mathfrak{b}_d$ are fractional ideals of $K$ such that $c_i \in \mathfrak{b}_i$ for all $i$. Then we have*

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

*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

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

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 $\phi\colon \mathbb{P}(w)_K \to \mathbb{P}(u)_K$ be a non-constant 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 $\phi$.

By Lemma 4.1, the morphism $\phi$ is defined by a pair of non-constant homogeneous polynomials $f_0, f_1 \in K[x_0, x_1]$ of degrees $eu_0$ and $eu_1$, respectively, for some positive integer $e$. 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 $\nu_i, \delta_i$ coprime positive integers.

By integrality of $K[x_0, x_1]$ over $K[f_0, f_1]$, 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

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

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

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

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 non-zero, 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 $1 \leq l \leq m_i$. We can therefore rewrite (1) as

$$x_i^{m_i\delta_i} + \sum_{l=1}^{m_i} g_{i,l\delta_i}(f_0, f_1) x_i^{(m_i-l)\delta_i} = 0 \quad \text{in } K[x_0, x_1] \tag{2}$$

and note that

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

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

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

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 $l = 0, \ldots, m_i$, we write

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

Substituting $(x_0, x_1) = (z_0, z_1)$ in (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

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

The ideal on the right-hand side equals $\mathcal{I}_{(1,\ldots,m_i)}(\mathfrak{c}_{i,1}, \ldots, \mathfrak{c}_{i,m_i})\mathfrak{m}^{\nu_i} = \mathfrak{d}_i\mathfrak{m}^{\nu_i}$. □

**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 $\phi\colon \mathbb{P}(w)_K \to \mathbb{P}(u)_K$ be a non-constant morphism. Let $e$ be as in Lemma 4.1, and for $i = 0, 1$ write $w_i/e = \nu_i/\delta_i$ with $\nu_i$, $\delta_i$ 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 $\phi$.*

*Proof.* We apply Lemma 4.1, which gives us homogeneous polynomials $f_0, f_1 \in K[x_0, x_1]$ such that $\phi$ 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

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

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

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

and

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

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

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

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

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

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

**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 $\phi$.*

*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 conditions "$e = 1$ or $w = (1, 1)$" in Corollary 6.5 are similar to the condition "$n = 1$ or $m = 1$" in [8, Proposition 2.1].

*Remark* 6.7. By Remark 4.2, 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 "$\phi$ is representable". For example, take $u = (1, 3)$ and $w = (1, 3)$, and consider the morphism

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

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

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

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

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

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 non-zero differential $\omega$ 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 $\omega$ gives the same point of $\mathbb{P}(4, 6)_{\mathbb{Q}}$, so $\iota$ is well defined.

**Definition 7.1.** Let $K$ be a number field. Using the morphism $\iota$, 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 $E$ as defined in [8] 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

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

**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:*

(1) *There is a commutative diagram*

$$\begin{array}{ccc} Y_G & \xrightarrow{\iota_G} & \mathbb{P}(w)_{K_G} \\ {\scriptstyle\pi_G}\downarrow & & \downarrow{\scriptstyle\phi} \\ Y(1)_{K_G} & \xrightarrow{\iota} & \mathbb{P}(4,6)_{K_G} \end{array}$$

*of algebraic stacks over $K_G$, where $\iota_G$ is an open immersion and $\phi$ is representable.*

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

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

*Proof.* The equivalence of (2) and (3) follows from the fact that the integral closure from (2) is canonically isomorphic to the moduli space of generalized elliptic curves with $G$-level structure [4, IV, Théorème 6.7(ii)].

The implication (2) $\implies$ (1) 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 (1) $\implies$ (2) follows from Corollary 4.4 applied to $V = \iota_G(Y_G)$. □

*Remark* 7.4. For a group $G$ satisfying the equivalent conditions of Lemma 7.3, the coarse moduli space of $X_G$ is isomorphic to $\mathbb{P}^1$. The converse does not hold; for example, 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.

*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 a pair $(w_0, w_1)$ of positive integers, and let $e$ be as in Lemma 4.1. Furthermore, assume $e = 1$ or $w = (1,1)$ holds. Then for every finite extension $K$ of $K_G$, we have*

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

*where*

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

*Proof.* Using the commutative diagram of Lemma 7.3 and noting that for counting purposes we may ignore the cusps (cf. [5, Remark 6.2]), we obtain

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

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

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

Applying Theorem 3.7, we obtain

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

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.

| $G$ | $\Gamma$ | $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ | $(w_0, w_1)$ | $e$ | $d$ |
|---|---|---|---|---|---|
| $G_1(1)$ | $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ | 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 |

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

In Table 1 we use the following notation: 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 we give its inverse image $\Gamma$ under the canonical group homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, the index of $\Gamma$ in $\mathrm{SL}_2(\mathbb{Z})$, the weights of the corresponding weighted projective line, and the values $e$ and $d$. The first 12 groups can also be found in [9, Examples 2.1 and Example 2.5], and the 12 groups with $e = 1$ 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 $e$ and $d$ can be expressed as

$$\begin{aligned} e &= \frac{w_0 w_1}{24}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma], \\ d &= \frac{w_0 w_1}{2(w_0 + w_1)}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]. \end{aligned}$$

## 9. Future work

It would be interesting to obtain a result similar to the one we obtain here for moduli stacks of elliptic curves that are of the form $\mathbb{P}(2) \times \mathbb{P}(1,1)$. An example of such a moduli stack is $X_0(6)$, so such a result would enable one to count the number of elliptic curves with a 6-isogeny over any number field.

Another direction that seems worth investigating is 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 will require extending the work of Deng [5], but is conceptually simpler than the approach we have taken here.

Finally, the size functions on weighted projective stacks that we use in this paper look similar to the height functions on algebraic stacks defined by Ellenberg, Satriano and Zureick-Brown [7]. The latter work 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. It seems likely that our size functions are a special case of the height functions of [7], and it would be interesting to verify this.

## 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 $S$, let $X$ and $Y$ be two $S$-schemes, let $a\colon G \times_S X \to X$ be an action of $G$ on $X$, and let $b\colon H \times_S Y \to Y$ be an action of $H$ on $Y$. We consider the quotient stacks $[G\backslash X]$ and $[H\backslash Y]$, writing quotients on the left because $a$ and $b$ are left actions. We seek an explicit description of the groupoid of morphisms $[G\backslash X] \to [H\backslash Y]$ of stacks over (the *fppf* site of) $S$.

Let $m_G\colon G \times_S G \to G$ and $m_H\colon H \times_S H \to H$ be the group operations. Let $p_2\colon G \times_S X \to X$ 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. For any $X$-scheme $Q$, let $\tilde{p}_2$, $\tilde{a}$ be the canonical morphisms appearing in the pull-back diagrams

$$\begin{array}{ccc} p_2^*Q & \xrightarrow{\tilde{p}_2} & Q \\ \downarrow & & \downarrow \\ G\times_S X & \xrightarrow[p_2]{} & X, \end{array} \qquad \begin{array}{ccc} a^*Q & \xrightarrow{\tilde{a}} & Q \\ \downarrow & & \downarrow \\ G\times_S X & \xrightarrow[a]{} & X. \end{array}$$

**Lemma A.1.** *Let $\mathcal{Y}$ be a stack in groupoids over $S$. Then the groupoid of morphisms $[G\backslash X] \to \mathcal{Y}$ is canonically equivalent to the following groupoid. The objects are the pairs $(T, j)$ where $T$ is an object of $\mathcal{Y}_X$ and $j$ is a descent datum for $T$, i.e. an isomorphism $j\colon a^*T \xrightarrow{\sim} p_2^*T$ over $G \times_S X$ such that the diagram*

$$\begin{array}{ccccc} (m_G\times \mathrm{id}_X)^*a^*T & \xrightarrow[\sim]{(m_G\times\mathrm{id}_X)^*j} & (m_G\times \mathrm{id}_X)^*p_2^*T & \xrightarrow[\sim]{} & p_{2,3}^*p_2^*T \\ \downarrow\wr & & & & \uparrow{\scriptstyle p_{2,3}^*j}\ \wr \\ (\mathrm{id}_G\times a)^*a^*T & \xrightarrow[\sim]{(\mathrm{id}_G\times a)^*j} & (\mathrm{id}_G\times a)^*p_2^*T & \xrightarrow[\sim]{} & p_{2,3}^*a^*T \end{array}$$

*is commutative. The morphisms from $(T, j)$ to $(T', j')$ are the isomorphisms $\xi\colon T \xrightarrow{\sim} T'$ over $X$ such that the diagram*

$$\begin{array}{ccc} a^*T & \xrightarrow[\sim]{\iota} & p_2^*T \\ {\scriptstyle a^*\xi}\downarrow\wr & & \wr\downarrow{\scriptstyle p_2^*\xi} \\ a^*T' & \xrightarrow[\sim]{\iota'} & p_2^*T' \end{array}$$

*is commutative.*

*Proof (sketch).* This follows from the description of morphisms from the quotient stack $[G\backslash X]$ to $\mathcal{Y}$ given in [12, tag 044U] and the canonical equivalence between the groupoid of morphisms from the stack represented by $X$ to $\mathcal{Y}$ and the fibre category $\mathcal{Y}_X$. □

**Lemma A.2.** *The groupoid of morphisms $[G\backslash X] \to [H\backslash Y]$ is canonically equivalent to the following groupoid. The objects are the triples $(Q, \phi, \iota)$ consisting of an $H$-torsor $Q$ over $X$, an $H$-equivariant morphism $\phi\colon Q \to Y$ of $S$-schemes and an isomorphism $\iota\colon a^*Q \xrightarrow{\sim} p_2^*Q$ of $H$-torsors over $G \times_S X$ such that the diagrams*

(3)
$$\begin{array}{ccccc} a^*Q & \xrightarrow{\tilde{a}} & Q & \xrightarrow{\phi} & Y \\ {\scriptstyle\iota}\downarrow\wr & & & \nearrow{\scriptstyle\phi} & \\ p_2^*Q & \xrightarrow{\tilde{p}_2} & Q & & \end{array}$$

*and*

(4)
$$\begin{array}{ccccc} (m_G\times \mathrm{id}_X)^*a^*Q & \xrightarrow[\sim]{(m_G\times\mathrm{id}_X)^*\iota} & (m_G\times \mathrm{id}_X)^*p_2^*Q & \xrightarrow[\sim]{} & p_{2,3}^*p_2^*Q \\ \downarrow\wr & & & & \uparrow{\scriptstyle p_{2,3}^*\iota}\ \wr \\ (\mathrm{id}_G\times a)^*a^*Q & \xrightarrow[\sim]{(\mathrm{id}_G\times a)^*\iota} & (\mathrm{id}_G\times a)^*p_2^*Q & \xrightarrow[\sim]{} & p_{2,3}^*a^*Q \end{array}$$

*are commutative. The morphisms* $(Q, \phi, \iota) \to (Q', \phi', \iota')$ *are the isomorphisms* $\tau\colon Q \xrightarrow{\sim} Q'$ *of* $H$*-torsors over* $X$ *such that the diagrams*

$$\begin{array}{ccc} Q & \xrightarrow{\phi} & Y \\ {\scriptstyle\tau}\downarrow\wr & \nearrow{\scriptstyle\phi'} & \\ Q' & & \end{array} \tag{5}$$

*and*

$$\begin{array}{ccc} a^*Q & \xrightarrow[\sim]{\iota} & p_2^*Q \\ {\scriptstyle a^*\tau}\downarrow\wr & & \wr\downarrow{\scriptstyle p_2^*\tau} \\ a^*Q' & \xrightarrow[\sim]{\iota'} & p_2^*Q' \end{array} \tag{6}$$

*are commutative.*

*Proof.* We apply Lemma A.1 with $\mathcal{Y} = [H\backslash Y]$. Using the explicit description of $[H\backslash Y]$ given in [12, tag 04UV], we view objects of $[H\backslash Y]$ over $X$ as pairs $(Q, \phi)$ consisting of an $H$-torsor $Q$ over $X$ and an $H$-equivariant morphism $\phi\colon Q \to Y$ of $S$-schemes. The morphisms $(Q, \phi) \to (Q', \phi')$ are the isomorphisms $\tau\colon Q \xrightarrow{\sim} Q'$ of $H$-torsors over $X$ such that the diagram (5) is commutative. Similarly, an isomorphism $a^*(Q, \phi) \xrightarrow{\sim} p_2^*(Q, \phi)$ over $G \times_S X$ is an isomorphism $\iota\colon a^*Q \xrightarrow{\sim} p_2^*Q$ of $H$-torsors over $G \times_S X$ such that the diagram (3) is commutative. Such an isomorphism is a descent datum for $(Q, \phi)$ if and only if the diagram (4) is commutative. Finally, the commutativity of the last diagram in Lemma A.1 translates to the commutativity of (6). □

To state the next corollary, we recall the following. Given a left action of a group $\Gamma$ on a set $Z$, the *quotient groupoid* $\Gamma \mathbin{\backslash\backslash} Z$ 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 $\Gamma$. The set of isomorphism classes of $\Gamma \mathbin{\backslash\backslash} Z$ is just the quotient set $\Gamma\backslash Z$.

**Lemma A.3.** *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*

$$h(g'g, x) = h(g', gx)h(g, x) \tag{7}$$

*and*

$$f(a(g, x)) = b(h(g, x), f(x)). \tag{8}$$

*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*

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

*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 natural bijection between the set of isomorphism classes of such morphisms and the quotient set $H(X)\backslash Z$.*

*Proof.* In the groupoid described by Lemma A.2, we take the full subcategory with objects of the form $(H \times_S X, \phi, \iota)$. In this setting, $\phi$ can be written as

$$\phi(h, x) = hf(x)$$

for a unique morphism $f\colon X \to Y$, namely $f(x) = \phi(1, x)$. Furthermore, we can identify both $p_2^*Q$ and $a^*Q$ with $H \times_S G \times_S X$, so $\iota\colon H \times_S G \times_S X \xrightarrow{\sim} H \times_S G \times_S X$ corresponds to multiplication by an element $h \in H(G \times_S X)$. Finally, an isomorphism $\tau$ as in Lemma A.2 corresponds to multiplication by an element $c \in H(X)$.

From this one can deduce that the groupoid of morphisms $[G\backslash X] \to [H\backslash Y]$ is canonically equivalent to the following groupoid. The objects are pairs $(f\colon X \to Y, h\colon G \times_S X \to H)$ of morphisms of $S$-schemes such that the diagrams

$$\begin{array}{ccc} G \times_S X & \xrightarrow{a} & X \\ {\scriptstyle (h, f\circ p_2)}\downarrow & & \downarrow{\scriptstyle f} \\ H \times_S Y & \xrightarrow{b} & Y \end{array}$$

and

$$\begin{array}{ccccc} G \times_S G \times_S X & \xrightarrow{m_G \times \mathrm{id}_X} & G \times_S X & \xrightarrow{h} & H \\ {\scriptstyle (\mathrm{id}_G \times a, p_{2,3})}\downarrow & & & \nearrow{\scriptstyle m_H} & \\ (G \times_S X) \times_S (G \times_S X) & \xrightarrow{(h,h)} & H \times_S H & & \end{array}$$

are commutative. On $T$-valued points, the commutativity of these diagrams comes down to (8) and (7), respectively, so the pairs $(f, h)$ as above are precisely the elements of $Z$. The morphisms $(f, h) \to (f', h')$ are morphisms $c\colon X \to H$ of $S$-schemes such that the diagrams

$$\begin{array}{ccc} X & \xrightarrow{f'} & Y \\ {\scriptstyle (c,f)}\downarrow & \nearrow{\scriptstyle b} & \\ H \times Y & & \end{array}$$

and

$$\begin{array}{ccc} G \times_S X & \xrightarrow{(c\circ a, h')} & H \times H \\ {\scriptstyle (h, c\circ p_2)}\downarrow & & \downarrow{\scriptstyle m_H} \\ H \times H & \xrightarrow[m_H]{} & H \end{array}$$

are commutative. Therefore the morphisms $(f, h) \to (f', h')$ correspond to the elements of $H(Z)$ sending $(f, h)$ to $(f', h')$ under the given action of $H(X)$ on $Z$. $\square$

*Acknowledgments.* 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.

## 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, 245–254, Adv. Stud. Pure Math., 32, Math. Soc. Japan, Tokyo, 2001. 12, 14

[2] B. Boggess and S. Sankar, *Counting elliptic curves with a rational $N$-isogeny for small $N$.* In preparation. 2, 14

[3] J. Cullinan, M. Kenney and J. Voight, *On a probabilistic local-global principle for torsion on elliptic curves.* Preprint, `http://arxiv.org/abs/2005.06669` 2

[4] 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), pp. 143–316. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973. 12

[5] An-Wen Deng, *Rational points on weighted projective spaces.* Preprint, `https://arxiv.org/abs/math/9812082`. 1, 3, 4, 12, 14

[6] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry. Graduate Texts in Mathematics **150**. Springer, New York, 1995. 6

[7] J. S. Ellenberg, M. Satriano and D. Zureick-Brown, *Heights on stacks and a generalized Batyrev–Manin–Malle conjecture.* In preparation. 14

[8] R. Harron and A. Snowden, *Counting elliptic curves with prescribed torsion*, J. Reine Angew. Math. **729** (2017), 151–170. 1, 2, 10, 11

[9] Lennart Meier, *Additive decompositions for rings of modular forms.* Preprint, `https://arxiv.org/abs/1710.03461`. 14

[10] 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. 2

[11] C. Pomerance and E. F. Schaefer, *Elliptic curves with Galois-stable cyclic subgroups of order 4*, preprint, `https://arxiv.org/abs/2004.14947`. 2

[12] The Stacks project authors, The Stacks project, `https://stacks.math.columbia.edu`, 2020. 15, 16



Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, Netherlands
*Email address*: `P.J.Bruin@math.leidenuniv.nl`
*URL*: `http://pub.math.leidenuniv.nl/~bruinpj/`

University of Zagreb, Faculty of Science, Department of Mathematics, Bijenička cesta 30, 10000 Zagreb, Croatia
*Email address*: `fnajman@math.hr`
*URL*: `http://web.math.pmf.unizg.hr/~fnajman/`