REPORTS @SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

Bhargava cubes and elliptic curves

*Martí Oller Riera
University of Cambridge
mo512@cam.ac.uk

∗Corresponding author

Resum *(CAT)*

En les seves cèlebres Disquisitiones Arithmeticae, Gauss va descobrir una llei de composició que confereix una estructura de grup al conjunt de classes de formes quadràtiques binàries amb discriminant fixat. Dos segles més tard, Bhargava va donar una reinterpretació d'aquesta llei a través de cubs $2 \times 2 \times 2$ d'enters, ara coneguts com a cubs de Bhargava. El plantejament d'aquest article rau en utilitzar la mateixa idea dels cubs de Bhargava però en cubs $3 \times 3 \times 3$, que donen lloc a corbes planes projectives de grau 3. L'objectiu és determinar lleis de composició anàlogues que involucrin aquestes corbes. A tal fi, es desenvoluparan els coneixements matemàtics pertinents, incloent cohomologia de Galois i geometria algebraica, fent èmfasi en corbes ellptiques i, més en general, en les propietats de corbes de gènere 1.

Abstract *(ENG)*

In his celebrated Disquisitiones Arithmeticae, Gauss discovered a composition law that gives a group structure to the set of classes of binary quadratic forms of a given discriminant. Two centuries later, Bhargava gave a reinterpretation of this law through $2 \times 2 \times 2$ cubes of integers, now known as Bhargava cubes. In this article, we aim to use the same idea of Bhargava cubes but in $3 \times 3 \times 3$ cubes, that yield projective plane curves of degree 3. Our aim is to determine analogous composition laws involving these curves. To this end, we will review the needed mathematical knowledge, including Galois cohomology and algebraic geometry, with an emphasis on elliptic curves and, more generally, in the properties of genus one curves.

Keywords: *Bhargava cubes, genus one curves, elliptic curves, Galois cohomology, arithmetic geometry, number theory.*
MSC (2010): *Primary 11D09, 11G05. Secondary 11R34.*
Received: *July 21, 2022.*
Accepted: *September 28, 2022.*

Acknowledgement

The author wants to thank Jordi Guàrdia and Santi Molina for their guidance during the development of this project, and the anonymous referee for their helpful comments.

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

1. Introduction

In 1801, Gauss published his Disquisitiones Arithmeticae [10], which among many other topics study the composition of binary quadratic forms. More specifically, he found a group law between the classes of binary quadratic forms of a given discriminant. 200 years later, in his PhD thesis, Bhargava studied whether there were higher analogues of this law that could help interpret other number rings and their class groups. He did that by considering different-sized cubes of integers and the forms arising from them. Most notable is his approach in [2] using $2 \times 2 \times 2$ cubes of integers, which yield an elegant reinterpretation of Gauss composition and allows to obtain higher composition laws. His work led to a bigger understanding of parametrizations of quartic and quintic rings and the density of their discriminants.

The next obvious step would be to consider $3 \times 3 \times 3$ cubes. In [3], it is explained that $3 \times 3 \times 3$ cubes give rise to a composition law on general ternary cubic forms, but this composition doesn't directly give information on the corresponding cubic rings. In fact, cubic rings are most naturally related to binary cubic forms, obtained by $2 \times 3 \times 3$ cubes. This is the explanation given by Bhargava to focus on $2 \times 3 \times 3$ cubes rather than on the $3 \times 3 \times 3$ case.

The aim of this article is to explore the behaviour of $3 \times 3 \times 3$ cubes in a more geometrical setting. We will consider cubes with entries in some field K, which will give rise to genus one curves in the projective plane, and we will see how there is an analogous group law satisfied by these curves.

This article will begin with a brief exposition Gauss' composition and Bhargava's work in $2 \times 2 \times 2$ cubes. We will later introduce concepts in arithmetic geometry that will be necessary for us later. This includes a brief introduction to elliptic curves and more generally to genus one curves, and also Galois cohomology and its relation to elliptic curves. We will conclude by explaining results in the aforementioned $3 \times 3 \times 3$ cubes, in parallel with the results in [4].

2. Gauss' composition law and Bhargava cubes

Definition 2.1. A binary quadratic form is a polynomial of the form $f(x, y) = ax^2 + bxy + cy^2$, with $a, b, c \in \mathbb{Z}$. We say that f is primitive if $\gcd(a, b, c) = 1$. The discriminant of a binary quadratic form is defined to be $D := b^2 - 4ac$.

Definition 2.2. We say that two binary quadratic forms f, g are equivalent if there exists a matrix $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $g(x, y) = f(rx + sy, tx + uy)$. We will denote this as $f \sim g$.

It is not difficult to see that equivalence of binary quadratic forms is an equivalence relation, and that any two equivalent binary quadratic forms have the same discriminant.

Definition 2.3. Let f, g be two primitive binary quadratic forms with the same discriminant. A binary quadratic form h is a composition of f and g if the following conditions hold:

$$\begin{cases} f(x, y) \cdot g(z, w) = h(B_1(x, y, z, w), B_2(x, y, z, w)); \\ p_1 q_2 - p_2 q_1 = f(1, 0); \\ p_1 r_2 - p_2 r_1 = g(1, 0); \end{cases}$$

where $B_i(x, y, z, w) = p_i xz + q_i xw + r_i yz + s_i yw$ $(i = 1, 2)$ are two bilinear forms with integer coefficients.

Gauss famously proved that, in fact, composition gives a group law to the set of equivalence classes primitive binary quadratic forms of fixed discriminant D. More precisely:

Theorem 2.4 (Gauss). (i) *Given two primitive binary quadratic forms f, g of given discriminant D, there always exists a composition h of f and g. Moreover, this composition is unique and well-defined up to equivalence, meaning:*

(1) *If h_1, h_2 are two compositions of f and g, then $h_1 \sim h_2$.*

(2) *If h_i is the composition of f_i and g_i for $i = 1, 2$, satisfying $f_1 \sim f_2$ and $g_1 \sim g_2$, then $h_1 \sim h_2$.*

(ii) *The equivalence classes of primitive binary quadratic forms of fixed discriminant D constitute an abelian group under composition.*

(iii) *The identity is given by*

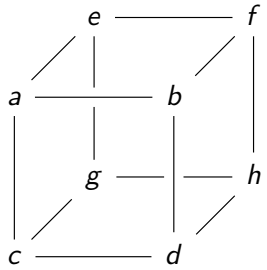
$$Q_{\mathrm{id},D}(x,y) = \begin{cases} \left[x^2 - \dfrac{D}{4}\right], & \text{if } D \equiv 0 \pmod 4, \\ \left[x^2 + xy - \dfrac{D-1}{4}\right], & \text{if } D \equiv 1 \pmod 4, \end{cases}$$

where $[f]$ denotes the equivalence class of f.

There is a reinterpretation of Gauss composition due to Dirichlet, which relates the composition of binary quadratic forms with the multiplication of fractional ideals in orders of number fields; see [6] for more details.

We now present Bhargava's reinterpretation of the Gauss composition law through $2 \times 2 \times 2$ cubes.

Definition 2.5. A Bhargava cube is an element $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. If A is represented by (a, b, c, d, e, f, g, h) under a basis of $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, then it can visualized as:



This cube can be partitioned into two 2×2 matrices in three different ways, according to the three orientations of the cube. Namely, the corresponding matrices are:

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix};$$

$$M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix}, \quad N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix};$$

$$M_3 = \begin{bmatrix} a & e \\ b & f \end{bmatrix}, \quad N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}.$$

Given any such partition, we may obtain a binary quadratic form through:

$$Q_i^A(x,y) = -\det(M_i x - N_i y).$$

Under this setting, a natural question to ask is: how are these three binary quadratic forms related?

Theorem 2.6 (Bhargava). *Let A be a Bhargava cube giving rise to three primitive binary quadratic forms Q_1, Q_2, Q_3. Then,*

(i) *The forms Q_1, Q_2, Q_3 have the same discriminant D.*

(ii) *The three forms satisfy*
$$[Q_1] + [Q_2] + [Q_3] = [Q_{\mathrm{id},D}],$$
where $+$ corresponds to Gauss composition and $Q_{\mathrm{id},D}$ is the identity form defined in Theorem 2.4.

(iii) *Conversely, given any three forms satisfying $[Q_1]+[Q_2]+[Q_3] = [Q_{\mathrm{id},D}]$, there exists a cube A giving rise to $[Q_1]$, $[Q_2]$, $[Q_3]$ (which is unique modulo a suitable action of $\mathrm{SL}_2(\mathbb{Z})$).*

Here, there is an action of $\Gamma = (\mathrm{SL}_2(\mathbb{Z}))^3$ on a cube $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. In terms of the partition, the action of the i-th matrix $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ replaces (M_i, N_i) for $(rM_i + sN_i, tM_i + uN_i)$.

3. Genus one curves

The main goal of this article will be to find an analogue to Theorem 2.6 but for $3 \times 3 \times 3$ cubes. To do that, we first need to introduce some concepts related to genus one curves.

3.1 Preliminaries in algebraic geometry

We will assume some familiarity with the basics of algebraic geometry. For further context, the reader may wish to consult [9] or the first two chapters of [12].

Fix throughout a perfect field K with algebraic closure $\overline{K}$. Let $C \subseteq \mathbb{P}^2$ be a curve, that is, the vanishing locus of an irreducible homogeneous polynomial $f(x, y, z)$ of degree d. We will denote by $C(K)$ the set of K-points of C, and we will typically denote the $\overline{K}$-points just by C.

Definition 3.1. The divisor group of C is the free abelian group generated by the $\overline{K}$-points of C. In other words, a divisor D of C is a formal sum
$$D = \sum_{P \in C(\overline{K})} n_P P,$$
where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P. The degree of a divisor is defined by
$$\deg D = \sum_{P \in C(\overline{K})} n_P.$$
Finally, a principal divisor is of the form
$$\operatorname{div} f = \sum_{P \in C(\overline{K})} \operatorname{ord}_P(f) P,$$
for some $f \in \overline{K}(C)$.

The principal divisors of C form a subgroup of the divisor class group, since for any $f, g \in \overline{K}(C)$:
$$\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g), \quad \operatorname{div}(1/f) = -\operatorname{div}(f).$$

Definition 3.2. The Picard group of C is the quotient of its divisor group by the subgroup of principal divisors.

Another fundamental concept in our study is the genus $g(C)$ of the curve C. In our particular case where $C \subseteq \mathbb{P}^2$ is given by the vanishing locus of a homogeneous polynomial of degree d, the genus of C can be computed to be

$$g(C) = \frac{(d-1)(d-2)}{2},$$

if the curve C is non-singular (see e.g. [9, Chap. 8, Prop. 5]). Note in particular that if $d = 3$, then $g(C) = 1$.

3.2 Elliptic curves

Definition 3.3. An elliptic curve is a genus one curve E/K with a distinguished K-rational point $O_E \in E(K)$.

Proposition 3.4. *Let* $\operatorname{char} K \neq 2, 3$. *Then,* E/K *is isomorphic to a projective plane curve of the form*

$$y^2z = x^3 + axz^2 + bz^3,$$

where the point O_E *corresponds to the point at infinity* $(0 : 1 : 0)$. *The coefficients satisfy* $4a^3 + 27b^2 \neq 0$.

The points of an elliptic curve are known to have a natural group structure. Given two points $P, Q \in E(K)$, we define $P + Q$ with the following procedure, which is represented in Figure 1:

- If $P \neq Q$, the line passing through P and Q intersects E in another point R. Then, the line passing through O_E and R intersects E at a third point, which we define to be $P + Q$.
- If $P = Q$, we choose the first line to be the tangent line of E at P.
- If $R = O_E$, set $P + Q := O_E$.

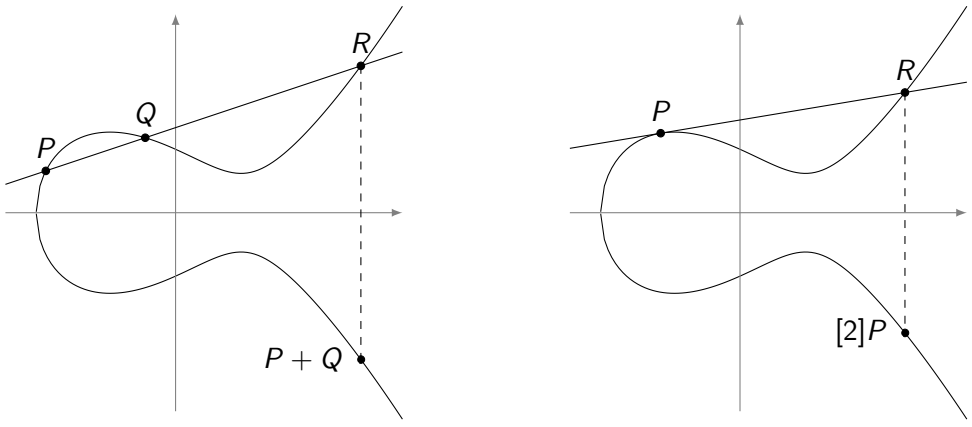


Figure 1: The group law of an elliptic curve. Figure obtained from [8].

Theorem 3.5. *The operation* $+$ *defines an abelian group structure on* E.

We denote by $E[n]$ the group of n-torsion points, that is, the group of points $P \in E$ such that $nP = 0_E$.

3.3 The Jacobian of a genus one curve

Given any genus one curve, there is a natural way to associate to it an elliptic curve, called the Jacobian. This can be made more precise (see [5, Chap. 20, Theor. 1]):

Proposition 3.6. *Let C/K be a genus one curve. Then, there exists an elliptic curve E/K together with an isomorphism $\phi\colon C \to E$ with the property that for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$ the isomorphism $\varphi_\sigma\colon E \to E$ defined by $\varphi_\sigma = ({}^\sigma\phi) \circ \phi^{-1}$ is a translation by a point P_σ, for some $P_\sigma \in E(\overline{K})$. Moreover, E is unique up to K-isomorphism.*

We define the Jacobian of the curve C/K to be the elliptic curve E/K appearing in Proposition 3.6.

Proposition 3.7. *The group structure of the points of the Jacobian E is isomorphic to the degree-0 Picard group of C (which is the group defined in Definition 3.2 restricted to the divisors of degree 0).*

3.4 Models of genus one curves

If a genus one curve has a rational point, then it can be brought to a Weierstrass form, which is the form given by Proposition 3.4. However, if the curve does not have a rational point, we have to seek other models for the curve. We will follow the exposition in [1].

Assume that a genus one curve C/K has a K-rational divisor D, meaning that $\sigma D = D$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Assume $\deg D = n > 0$, and define

$$\mathcal{L}(D) := \{f \in K(C) \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

It is a K-vector space, and the Riemann–Roch theorem in this case tells us that $\dim_K \mathcal{L}(D) = n$ (see [9]).

Let us focus on the case $n = 3$ (the cases $n = 2, 4$ are covered in [1]). Since $\dim_K \mathcal{L}(D) = 3$, we choose a K-basis of $\mathcal{L}(D)$, say $\{x, y, z\}$. Then, the ten elements x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^3, y^2z, yz^2, z^3 all belong to the 9-dimensional space $\mathcal{L}(3D)$, so there exists a linear relation between these elements. In other words, there exists a ternary cubic form U such that

$$U(x, y, z) = 0.$$

In [1], there is an expression for two invariants of U, which we will call c_4 and c_6. We can further define $\Delta = \frac{c_4^3 - c_6^2}{1728}$.

Theorem 3.8. *The equation $U(x, y, z) = 0$ defines a genus one curve if and only if $\Delta \neq 0$. In that case, and if $\mathrm{char}\, K \neq 2, 3$, the Jacobian of the curve is*

$$y^2 = x^3 - 27c_4x - 57c_6.$$

3.5 Galois cohomology and elliptic curves

Let G be a topological group (i.e. G has a topology where the group operation and the inverse are continuous).

Definition 3.9. An abelian group M is a G-module if there is an action $G \times M \to M$ satisfying, for all $g, g' \in G$, $m, m' \in M$:

(i) $g(m + m') = gm + gm'$.

(ii) $(gg')m = g(g'm)$.

(iii) $1m = m$.

(iv) The G-action is continuous with respect to the topology on G and the discrete topology on M.

Definition 3.10. A morphism of G modules is a group morphism $\alpha\colon M \to N$ respecting the G-action on M and N.

Now, let K be a perfect field and set $G_K = \mathrm{Gal}(\overline{K}/K)$. We note that G_K is naturally a topological group under the Krull topology.

Definition 3.11. Let M be a G_K-module. Then, its 0-th cohomology group is

$$H^0(K, M) := M^{G_K} = \{m \in M \mid gm = m \text{ for all } g \in G_K\}.$$

Definition 3.12. Let M be a G_K-module. The group of 1-cocycles is given by

$$Z^1(K, M) = \{\xi\colon G_K \to M \mid \xi(gh) = g(\xi(h)) + \xi(g),\ \xi \text{ continuous}\},$$

Its subgroup of 1-coboundaries $B^1(K, M)$ consists of the cocycles $\xi \in Z^1(K, M)$ such that ξ is of the form $\xi(g) = gm - m$ for some $m \in M$. Then, the 1st cohomology group is

$$H^1(K, M) = \frac{Z^1(K, M)}{B^1(K, M)}.$$

Proposition 3.13. *Consider the exact sequence of G_K-modules given by*

$$0 \longrightarrow P \longrightarrow M \longrightarrow N \longrightarrow 0.$$

Then, there is a long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(K, P) \longrightarrow H^0(K, M) \longrightarrow H^0(K, N) \\ \xrightarrow{\ \delta\ } \\ H^1(K, P) \longrightarrow H^1(K, M) \longrightarrow H^1(K, N). \end{aligned}$$

Remark 3.14. We could define higher cohomology groups ($H^2, H^3 \dots$) that would continue the long exact sequence in an analogous manner.

Let us return to the setting of elliptic curves. For an elliptic curve E/K, there is a natural Galois action defined component-wise. Let us consider the exact sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{\times n} E \longrightarrow 0.$$

Then, Proposition 3.13 gives us a long exact sequence:

$$0 \longrightarrow E(K)[n] \longrightarrow E(K) \xrightarrow{\times n} E(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E) \xrightarrow{\times n} H^1(K, E).$$

From this long exact sequence we can extract a short exact sequence:

$$0 \longrightarrow \frac{E(K)}{nE(K)} \xrightarrow{\delta} H^1(K, E[n]) \xrightarrow{\iota} H^1(K, E)[n] \longrightarrow 0. \tag{1}$$

This sequence is known as the Kummer exact sequence for E/K.

3.6 The twisting principle

We will conclude this section by interpreting what $H^1(K, E[n])$ and $H^1(K, E)$ are. We will assume that $\operatorname{char} K \nmid n$, a harmless assumption given that later we will deal with $n = 3$ and $\operatorname{char}(K) \neq 2, 3$. We will follow the exposition in [7].

We will make use of the twisting principle, which says that if X/K is an object defined over K, then K-isomorphism classes of twists of X (other objects Y/K isomorphic to X over $\overline{K}$) are parametrized by $H^1(K, \operatorname{Aut}(X))$, where $\operatorname{Aut}(X)$ is the automorphism group of X.

Here, the twisting principle is stated rather loosely, but it will be true for all our applications. See [11] and [7] for further details.

In view of the principle, if we are able to find a suitable object such that $\operatorname{Aut}(X)$ is E or $E[n]$, then we will be able to interpret the objects arising in the Kummer sequence.

Definition 3.15. A torsor under E is a pair (C, μ), where C is a smooth projective curve of genus one defined over K, and $\mu\colon E \times C \to C$ is a morphism defined over K that induces a simple transitive action on $\overline{K}$-points.

An isomorphism of torsors $(C_1, \mu_1) \cong (C_2, \mu_2)$ is an isomorphism of the underlying curves that respects the E-action.

Lemma 3.16. *Every torsor under E is a twist of $(E, +)$, where $(E, +)$ is the trivial torsor given by the group law. Moreover,* $\operatorname{Aut}(E, +) = E$.

Hence, by the twisting principle:

Theorem 3.17. *The group $H^1(K, E)$ parametrizes the torsors of E.*

Definition 3.18. A torsor divisor class pair $(C, [D])$ is a pair consisting of a torsor C of E and a K-rational divisor class $[D]$ of degree n. Here, rationality means that $\sigma(D) \sim D$ for all $\sigma \in \operatorname{Gal}(\overline{K}/K)$.

Two such pairs $(C_1, [D_1])$ and $(C_2, [D_2])$ are isomorphic if there is an isomorphism of torsors $\phi\colon C_1 \to C_2$ such that $\phi^* D_2 \sim D_1$.

Lemma 3.19. *Every torsor divisor class pair is a twist of $(E, [nO_E])$, O_E is the point at infinity of E. Moreover,* $\operatorname{Aut}(E, [nO_E]) = E[n]$.

The twisting principle in this case gives

Theorem 3.20. *The group $H^1(K, E[n])$ parametrizes the K-isomorphism classes of torsor divisor class pairs.*

In particular, it can be shown that in the Kummer sequence

$$0 \longrightarrow \frac{E(K)}{nE(K)} \xrightarrow{\delta} H^1(K, E[n]) \xrightarrow{\imath} H^1(K, E)[n] \longrightarrow 0,$$

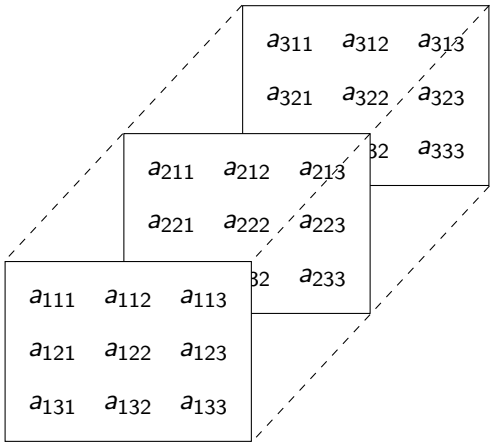
the maps are defined as

$$\delta(P) = (E, [(n-1)O_E + P]) \quad \text{and} \quad \imath(C, [D]) = C.$$

4. $3 \times 3 \times 3$ Bhargava cubes

Most of the results that we present here appear in [4]. However, this article takes a slightly different point of view more focused in the group law of Theorem 4.4.

Assume that K is a perfect field and $\mathrm{char}(K) \neq 2, 3$. Let us consider a $3 \times 3 \times 3$ cube (a_{ijk}) with entries in K. It can be drawn as follows:



Analogously to the $2 \times 2 \times 2$ case, we can partition this cube in three different ways to obtain the "front" section, the "top" section and the "side" section:

$$A_{f,i} = \begin{pmatrix} a_{i11} & a_{i12} & a_{i13} \\ a_{i21} & a_{i22} & a_{i23} \\ a_{i31} & a_{i32} & a_{i33} \end{pmatrix}, \quad A_{t,i} = \begin{pmatrix} a_{1i1} & a_{1i2} & a_{1i3} \\ a_{2i1} & a_{2i2} & a_{2i3} \\ a_{3i1} & a_{3i2} & a_{3i3} \end{pmatrix}, \quad A_{s,i} = \begin{pmatrix} a_{11i} & a_{21i} & a_{31i} \\ a_{12i} & a_{22i} & a_{32i} \\ a_{13i} & a_{23i} & a_{33i} \end{pmatrix},$$

for $i = 1, 2, 3$. These three partitions yield three polynomials using:

$$P_\bullet(X, Y, Z) = \det(A_{\bullet,1}X + A_{\bullet,2}Y + A_{\bullet,3}Z),$$

with $\bullet = f, s, t$.

We note that P_f, P_t, P_s are homogeneous polynomials in X_1, X_2, X_3 of degree 3, and hence define algebraic sets in $\mathbb{P}^2$:

$$C_\bullet = \{(X_1, X_2, X_3) \in \mathbb{P}^2 \mid P_\bullet(X_1, X_2, X_3) = 0\}.$$

By the discussion in Theorem 3.8, any of these algebraic sets define a smooth genus one curve if and only if their discriminant Δ defined in Subsection 3.4 is different from 0.

Lemma 4.1. *All curves C_f, C_s, C_t share the same invariants c_4, c_6, and hence the same discriminant Δ. In particular, if one of the curves is smooth, then they all are smooth.*

The proof can be done with an explicit computation, which we omit. Assume from now on that all three curves are smooth.

Theorem 4.2. *Let C_f, C_s, C_t be the curves arising from a $3\times3\times3$ cube, and assume they are all smooth. Then, all three curves are isomorphic over K.*

Sketch of proof. Let $(x_1, x_2, x_3) \in C_f$, and consider the matrix $M_f(x_1, x_2, x_3) = A_{f,1}x_1 + A_{f,2}x_2 + A_{f,3}x_3$. Then, the columns $c_{f,i}(x_1, x_2, x_3)$ of this matrix are linearly dependent, say by some coefficients $(X_1, X_2, X_3) \in \mathbb{P}^2$. Then, a quick computation shows that

$$\begin{aligned} 0 &= X_1 c_{f,1}(x_1, x_2, x_3) + X_2 c_{f,2}(x_1, x_2, x_3) + X_3 c_{f,3}(x_1, x_2, x_3) \\ &= x_1 c_{s,1}(X_1, X_2, X_3) + x_2 c_{s,2}(X_1, X_2, X_3) + x_3 c_{s,3}(X_1, X_2, X_3). \end{aligned} \tag{2}$$

The assignment $\varphi_{fs}\colon C_f \to C_s$ given by sending $(x_1, x_2, x_3) \mapsto (X_1, X_2, X_3)$ can be seen to be an isomorphism of algebraic curves. □

We can analogously choose φ_{ft}, φ_{sf}, φ_{st}, φ_{tf} and φ_{ts}. It holds that $\varphi_{ij} = \varphi_{ji}^{-1}$ for any choice of i, j; but in general it is not true that $\varphi_{ki} \circ \varphi_{jk} \circ \varphi_{ij}$ is the identity.

We can interpret Theorem 4.2 as the analogue of Theorem 2.6, item (i). Both results restrict how "different" the arising objects can be: the binary quadratic forms have the same discriminant and the genus one curves are isomorphic.

In particular, given that the three curves are isomorphic, they have the same Jacobian curve, which we will call E.

We still need to find out whether these three curves obey some suitable group law. To this end, consider the divisor at infinity D_f of C_f, given by the intersection of C_f with any hyperplane (if we change the hyperplane, we get a linearly equivalent divisor). Similarly, consider the divisors at infinity D_s and D_t of C_s and C_t, let $\Delta_f = D_f$, and let Δ_s and Δ_t be the pullbacks of D_s, D_t with respect to φ_{fs} and φ_{ft}, respectively. Then, define

$$\alpha_f = (C_f, [\Delta_f]), \quad \alpha_s = (C_s, [\Delta_s]), \quad \alpha_t = (C_t, [\Delta_t]).$$

By Theorem 3.20, the elements α_f, α_s, α_t can be interpreted in $H^1(K, E[3])$. Additionally, it can be shown that there exist points P_f, P_s, P_t in C_f such that $3P_\bullet \sim \Delta_\bullet$ for $\bullet = f, s, t$.

Lemma 4.3. *Assume Δ_f, Δ_s, Δ_t arise from a cube. Then,*

$$2\Delta_f \sim \Delta_s + \Delta_t,$$

and Δ_f is not linearly equivalent to either of Δ_s or Δ_t.

Theorem 4.4. *The three cocycles* $\alpha_f, \alpha_s, \alpha_t \in H^1(K, E[3])$ *satisfy*

$$\alpha_f + \alpha_s + \alpha_t = 0.$$

Proof. Recall that a degree 0 divisor can be identified as a point in the Jacobian (see Subsection 3.3). We claim that:

$$Q = P_t + P_s - 2P_f \in E[3].$$

Indeed, remembering that $3P_\bullet \sim \Delta_\bullet$, for $\bullet = f, s, t$, and using the previous lemma:

$$3Q = 3P_t + 3P_s - 6P_f \sim \Delta_t + \Delta_s - 2\Delta_f \sim 0.$$

We conclude that the cocycle $\alpha_f + \alpha_s + \alpha_t$ is given by

$$\begin{aligned}\alpha_f(\sigma) + \alpha_s(\sigma) + \alpha_t(\sigma) &= \sigma(P_f + P_s + P_t) - (P_f + P_s + P_t)\\ &= (\sigma Q - Q) + \sigma(3P_f) - 3P_f\\ &\sim (\sigma Q - Q) + \sigma\Delta_f - \Delta_f = \sigma Q - Q,\end{aligned}$$

since Δ_f is a K-rational divisor. Thus, $\alpha_f + \alpha_s + \alpha_t$ is a coboundary and the result follows. □

4.1 Converse results

Now, we are interested in the converse to Theorem 4.4, namely: given any three cocycles $\alpha_1, \alpha_2, \alpha_3 \in H^1(K, E[3])$, does there exist a cube giving rise to them? To start answering the question, we first state the converse result for divisors.

Theorem 4.5. *There is a bijection between:*

(i) $3 \times 3 \times 3$ *cubes (modulo a suitable action of* $\mathrm{GL}_3(K)$*).*

(ii) *Isomorphism classes of* $(C, \Delta_f, \Delta_s, \Delta_t)$*, where* C *is a genus one curve and* Δ_f*,* Δ_s*,* Δ_t *are* K*-rational divisors of degree* 3 *satsifying* $2\Delta_f \sim \Delta_s + \Delta_t$ *and* $\Delta_f \nsim \Delta_s, \Delta_t$*.*

See [4] for the proof.

Now, we recall again the Kummer exact sequence

$$0 \longrightarrow \frac{E(K)}{nE(K)} \xrightarrow{\delta} H^1(K, E[n]) \xrightarrow{\imath} H^1(K, E)[n] \longrightarrow 0.$$

By the definition of the map $\imath$, if we have any three cocycles $\alpha_1, \alpha_2, \alpha_3 \in H^1(K, E[n])$ we need to have $\imath(\alpha_1) = \imath(\alpha_2) = \imath(\alpha_3)$.

However, there is still one more consideration to make, which is that an element of $H^1(K, E[3])$ is not necessarily represented by a projective cubic plane curve. Given a torsor divisor class pair $(C, [D])$, the divisor D does not necessarily satisfy $\sigma D = D$ for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$, but rather that $\sigma D \sim D$. By the discussion in Subsection 3.4, the curve C needs to have a K-rational divisor D in order to be represented by a projective plane cubic curve.

In [7], an obstruction map Ob is defined, so that $\mathrm{Ob}(\alpha) = 0$ for $\alpha \in H^1(K, E[n])$ if and only if the cocycle α can be represented by $(C, [D])$, with $\sigma D = D$ for all σ in the Galois group.

Finally, observe that the action of a translation by a point $P \in E(K)$ does not change the cocycle. In other words, $(C, [D]) = (C, [D'])$, where D' is obtained by the action of $3P$ on D. If $3E(K) = \{O_E\}$, then in the case where $\alpha_1 = \alpha_2 = \alpha_3$ we would not be able to change the divisor corresponding to the cocycles and hence we would not be able to guarantee the conditions in Lemma 4.3.

Theorem 4.6. *Assume that* $\alpha_1, \alpha_2, \alpha_3 \in H^1(K, E[3])$ *satisfy*

(i) $\alpha_1 + \alpha_2 + \alpha_3 = 0$.

(ii) $\imath(\alpha_1) = \imath(\alpha_2) = \imath(\alpha_3)$.

(iii) $Ob(\alpha_1) = Ob(\alpha_2) = Ob(\alpha_3) = 0$.

(iv) $3E(K) \neq \{O_E\}$ *if* $\alpha_1 = \alpha_2 = \alpha_3$.

Then, there exists a cube giving rise to α_1, α_2, α_3.

As a final remark, observe that we are dealing with elements $\alpha_1, \alpha_2, \alpha_3 \in H^1(K, E[3])$ with $\imath(\alpha_1) = \imath(\alpha_2) = \imath(\alpha_3)$. By looking at the Kummer sequence, we see that the group law is actually taking place more naturally in $E(K)/3E(K)$. Therefore, Theorem 4.6 can be restated more naturally:

Corollary 4.7. *Assume we have a genus one curve* C/K *with Jacobian* E/K, *and suppose given three points* $P_1, P_2, P_3 \in E(K)/3E(K)$ *such that* $P_1 + P_2 + P_3 = 0$ *in* $E(K)/3E(K)$. *Then, there exists a cube giving rise to this information as long as we avoid the case where* $P_1 = P_2 = P_3$ *and* $3E(K) = \{O_E\}$.

References

[1] An Sang Yook et al., "Jacobians of genus one curves", *J. Number Theory* **90(2)** (2001), 304–315.

[2] M. Bhargava, "Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations", *Ann. of Math. (2)* **159(1)** (2004), 217–250.

[3] M. Bhargava, "Higher composition laws. II. On cubic analogues of Gauss composition", *Ann. of Math. (2)* **159(2)** (2004), 865–886.

[4] M. Bhargava, W. Ho, "Coregular spaces and genus one curves", *Camb. J. Math.* **4(1)** (2016), 1–119.

[5] J.W.S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society Student Texts **24**, Cambridge University Press, Cambridge, 1991.

[6] D.A. Cox, *Primes of the Form* x^2+ny^2, Fermat, class field theory and complex multiplication, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.

[7] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, M. Stoll, "Explicit n-descent on elliptic curves. I. Algebra", *J. Reine Angew. Math.* **615** (2008), 121–155.

[8] L. De Feo, "Mathematics of isogeny based cryptography", Preprint (2017), `http://arxiv.org/abs/1711.04062`.

[9] W. Fulton, *Algebraic Curves. An Introduction to Algebraic Geometry*, Notes written with the

collaboration of Richard Weiss, Reprint of 1969 original, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[10] C.F. Gauss, *Disquisitiones Arithmeticae*, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse, Springer-Verlag, New York, 1986.

[11] J.-P. Serre, *Galois Cohomology*, Springer-Verlag, 1964.

[12] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Second edition, Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009.