BOLZA QUATERNION ORDER AND ASYMPTOTICS OF SYSTOLES ALONG CONGRUENCE SUBGROUPS

KARIN KATZ, MIKHAIL KATZ, MICHAEL M. SCHEIN, AND UZI VISHNE

Abstract. We give a detailed description of the arithmetic Fuchsian group of the Bolza surface and the associated quaternion order. This description enables us to show that the corresponding principal congruence covers satisfy the bound $\mathrm{sys}(X) > \frac{4}{3}\log g(X)$ on the systole, where g is the genus. We also exhibit the Bolza group as a congruence subgroup, and calculate out a few examples of "Bolza twins" (using `magma`). Like the Hurwitz triplets, these correspond to the factoring of certain rational primes in the ring of integers of the invariant trace field of the surface. We exploit random sampling combined with the Reidemeister-Schreier algorithm as implemented in `magma` to generate these surfaces.

Contents

Key words and phrases. arithmetic Fuchsian group, hyperbolic surface, invariant trace field, order, principal congruence subgroup, quaternion algebra, systole, totally real field, triangle group, Bolza curve.

1. Introduction

This article pursues several related goals. First, we seek to clarify the algebraic underpinnings of the celebrated Bolza curve which turn out to be more involved than those of the celebrated Klein quartic. Furthermore, we seek to provide explicit algebraic foundations, in terms of a quaternion algebra, for calculating out examples of Riemann surfaces with particularly high systole corresponding to principal congruence subgroups in the Bolza order. In an effort to make the text intelligible to both algebraists and differential geometers, we sometimes give detailed proofs that could have been shortened if addressed to a specific expert audience.

In 2007, Katz, Schaps and Vishne [13] proved a lower bound for the systole of certain arithmetic Riemann surfaces, improving earlier results by Buser and Sarnak (1994 [8, p. 44]). Particularly sharp results were obtained in [13] and [14] for Hurwitz surfaces, namely Riemann surfaces with an automorphism group of the highest possible order in terms of the genus g, yielding a lower bound

$$\operatorname{sys}(X_g) > \frac{4}{3}\log g \tag{1.1}$$

for principal congruence subgroups corresponding to a suitable Hurwitz quaternion order defined over $\mathbb{Q}(\cos\frac{2\pi}{7})$.

Makisumi (2013 [20]) proved that the multiplicative constant $\frac{4}{3}$ in the bound (1.1) is the best possible asymptotic value for congruence subgroups of arithmetic Fuchsian groups. Schmutz Schaller (1998 [24, Conjecture 1(i), p. 198]) conjectured that a 4/3 bound is the best possible among all hyperbolic surfaces. Additional examples of surfaces whose systoles are close to the bound were recently constructed by Akrout & Muetzel (2013 [1], [2]). The foundations of the subject were established by Vinberg (1967 [27]).

We seek to extend the bound (1.1) to the case of the family of Riemann surfaces defined by principal congruence subgroups of the $(3,3,4)$ triangle group corresponding to a quaternion order defined over $\mathbb{Q}(\sqrt{2})$, which is closely related to the Bolza surface.

The Fuchsian group of the Bolza surface, which we henceforth denote B, is arithmetic, being a subgroup of the group of units, modulo $\{\pm 1\}$, in an order of the quaternion algebra

$$D_B = (-3, \sqrt{2}) = K[i, j \mid i^2 = -3,\ j^2 = \sqrt{2},\ ji = -ij] \tag{1.2}$$

over the base field $K = \mathbb{Q}(\sqrt{2})$. The splitting pattern of this algebra is determined in Section 5. Let $O_K = \mathbb{Z}[\sqrt{2}]$ be the ring of integers of K. This is a principal ideal domain, so irreducible elements of O_K are prime.

Lemma 1.1. *The standard order*

$$\operatorname{span}_{O_K} \{1, i, j, ij\}$$

in the algebra D_B is contained in precisely two maximal orders $\mathcal{Q}$ and $\mathcal{Q}'$, which are conjugate to each other.

We will prove Lemma 1.1 in Section 6. This lemma is a workhorse result used in the analysis of maximal orders below. We let $\mathcal{Q}_B = \mathcal{Q}$.

Theorem 1.2. *Almost all principal congruence subgroups of the maximal order $\mathcal{Q}_B$ satisfy the systolic bound* (1.1).

This is proved in Section 9, where a more detailed version of the result is given. In fact, Theorem 1.2 is a consequence of the following more general result. For an order Q in a quaternion algebra D, let Q^1 be the group of units of Q and let d be the dimension over $\mathbb{Q}$ of the center of Q. We define a constant $\Lambda_{D,Q} \geq 1$ depending on the local ramification pattern (see Section 9). Let X_1 be the quotient of the hyperbolic plane $\mathcal{H}^2$ modulo the action of Q^1.

Proposition 1.3. *Suppose $2^{3(d-1)}\Lambda_{D,Q} < \frac{4\pi}{area(X_1)}$. Then almost all the principal congruence covers of X_1 satisfy the bound* $\operatorname{sys} > \frac{4}{3}\log g$.

Note that this is stronger than the Buser–Sarnak bound $\operatorname{sys} X(\Gamma) > \frac{4}{3}\log g(X(\Gamma)) - c(\Gamma_0)$ where the constant $c(\Gamma_0)$ could be arbitrarily large. Returning to the Bolza order, we have the following result.

Theorem 1.4. *There are elements α and β of norm 1 in the algebra D_B of (1.2) such that $\mathcal{Q}_B = O_K[\alpha, \beta]$ as an order. Let $\mathcal{Q}_B^1 = \langle \alpha, \beta \rangle$ be the group generated by α and β. Then $\mathcal{Q}_B^1/\{\pm 1\}$ is isomorphic to the triangle group $\Delta_{(3,3,4)}$.*

In Corollary 10.4 we find that the Bolza group B has index 24 in $\mathcal{Q}_B^1/\{\pm 1\}$ and is generated, as a normal subgroup of $\mathcal{Q}_B^1/\{\pm 1\}$, by the element $(\alpha\beta)^2(\alpha^2\beta^2)^2$. The choice of α and β implies that B is contained in the principal congruence subgroup $\mathcal{Q}_B^1(\sqrt{2})/\{\pm 1\}$. However, this congruence subgroup has torsion: it contains an involution closely related to the hyperelliptic involution of the Bolza surface (see Section 11). Working out the ring structure of $\mathcal{Q}_B/2\mathcal{Q}_B$, we are then able to compute the quotient $B\mathcal{Q}_B^1(2)/\mathcal{Q}_B^1(2)$ and obtain the following.

Theorem 1.5. *The fundamental group B of the Bolza surface is contained strictly between two principal congruence subgroups as follows:*

$$\mathcal{Q}_B^1(2)/\{\pm 1\} \subset B \subset \mathcal{Q}_B^1(\sqrt{2})/\{\pm 1\}.$$

This explicit identification of the Bolza group as a (non-principal) congruence subgroup in the maximal order requires a detailed analysis of quotients, and occupies Sections 10–13. In contrast, the Fuchsian group of the Klein quartic (which is the Hurwitz surface of least genus) does happen to be a principal congruence subgroup in the group of units of the corresponding maximal order; see [14, Section 4].

It follows from Theorem 1.5 that B is a congruence subgroup. Moreover, we show that $\mathcal{Q}_B^1/\langle -1, B\rangle \cong \mathrm{SL}_2(\mathbb{F}_3)$, explaining some of the symmetries of the Bolza surface. The full symmetry group, $\mathrm{GL}_2(\mathbb{F}_3)$, comes from the embedding of the triangle group $\Delta_{(3,3,4)}$ in $\Delta_{(2,3,8)}$; see Corollary 13.4.

In the concluding Sections 14 through 16 we present "twin Bolza" surfaces corresponding to factorisations of rational primes 7, 17, 23, 31, and 41 as a product of a pair of algebraic primes in $\mathbb{Q}(\sqrt{2})$.

Recent publications on systoles include Babenko & Balacheff [3]; Balacheff, Makover & Parlier [4]; Bulteau [7]: Katz & Sabourau [12]; Kowalick, Lafont & Minemyer [15]; Linowitz & Meyer [16].

2. Fuchsian groups and quaternion algebras

A cocompact Fuchsian group $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ defines a hyperbolic Riemann surface $\mathcal{H}^2/\Gamma$, denoted X_Γ, where $\mathcal{H}^2$ is the hyperbolic plane. If Γ is torsion free, the systole $\mathrm{sys}(X_\Gamma)$ satisfies

$$2\cosh\left(\tfrac{1}{2}\,\mathrm{sys}(X_\Gamma)\right) = \min_M |\mathrm{trace}(M)|,$$

or

$$\mathrm{sys}(X_\Gamma) = \min_M 2 \operatorname{arccosh}\left(\tfrac{1}{2}|\mathrm{trace}(M)|\right), \tag{2.1}$$

where M runs over all the nonidentity elements of Γ. We will construct families of Fuchsian groups in terms of suitable orders in quaternion algebras. Since the traces in the matrix algebra coincide with reduced traces (see below) in the quaternion algebra, the information about lengths of closed geodesics, and therefore about systoles, can be read off directly from the quaternion algebra, bypassing the traditional presentation in matrices.

Let k be a finite dimensional field extension of $\mathbb{Q}$, let $a, b \in k^*$, and consider the following associative algebra over k:

$$A = k[i, j \mid i^2 = a, j^2 = b, ji = -ij]. \tag{2.2}$$

The algebra A admits the following decomposition as a k-vector space:

$$A = k1 \oplus ki \oplus kj \oplus kij\ .$$

Such an algebra A, which is always simple, is called a quaternion algebra. The center of A is precisely k.

Definition 2.1. Let $x = x_0 + x_1 i + x_2 j + x_3 ij \in A$. The *conjugate* of x (under the unique symplectic involution) is $x^* = x_0 - x_1 i - x_2 j - x_3 ij$. The *reduced trace* of x is

$$\mathrm{Tr}_A(x) := x + x^* = 2x_0,$$

and the *reduced norm* of x is

$$\mathrm{Nr}_A(x) := xx^* = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2.$$

Definition 2.2 (cf. Reiner 1975 [22])**.** An *order* of a quaternion algebra A (over k) is a subring with unit, which is a finitely generated module over the ring of integers $O_k \subset k$, and such that its ring of fractions is equal to A.

If a and b in (2.2) are algebraic integers in k^*, then the subring $\mathcal{O} \subset A$ defined by

$$\mathcal{O} = O_k 1 + O_k i + O_k j + O_k ij \tag{2.3}$$

is an order of A (see Katok 1992 [10, p. 119]), although not every order has this form; a famous example of an order not having the form (2.3) is the Hurwitz order in Hamilton's quaternion algebra over the rational numbers. Note that in the order the scalars are taken from the ring of integers O_k; the scalars are taken from the field k when passing to the ring of fractions.

3. The (2,3,8) and (3, 3, 4) triangle groups

The Bolza surface can be defined by a subgroup of either the (2,3,8) or the $(3,3,4)$ triangle group. We will study specific Fuchsian groups arising as congruence subgroups of the arithmetic triangle group of type $(3,3,4)$. First we clarify the relation between the $(3,3,4)$ and the (2,3,8) groups. Let $\Delta_{(2,3,8)}$ denote the (2,3,8) triangle group, i.e.

$$\Delta_{(2,3,8)} = \langle x, y \mid x^2 = y^3 = (xy)^8 = 1 \rangle. \tag{3.1}$$

Let $h\colon \Delta_{(2,3,8)} \to \mathbb{Z}/2\mathbb{Z}$ be the homomorphism sending x to the non-trivial element of $\mathbb{Z}/2\mathbb{Z}$ and y to the identity element.

Lemma 3.1. *As a subgroup of $\Delta_{(2,3,8)}$, the kernel of h is given by*

$$\ker(h) = \langle \alpha, \beta \mid \alpha^3 = \beta^3 = (\alpha\beta)^4 = 1 \rangle$$

where $\alpha = y$ and $\beta = xyx$.

Proof. The presentation can be obtained by means of the Reidemeister-Schreier method, but here is a direct proof. Note that $xy^nx = (xyx)^n = \beta^n$. Each element $t \in \ker(h)$ is of one of 4 types:

(1) $t = xy^{n_1}xy^{n_2}\cdots xy^{n_k}x$;
(2) $t = y^{n_1}xy^{n_2}\cdots xy^{n_k}x$;
(3) $t = xy^{n_1}xy^{n_2}\cdots xy^{n_k}$;
(4) $t = y^{n_1}xy^{n_2}\cdots xy^{n_k}$,

with an even number of x's, where all the exponents n_i are either 1 or 2. To show that each element can be expressed in terms of α and β, we argue by induction on the length of the presentation in terms of x's and y's. Type (1) is reduced to (a shorter) type (2) by noting that $xy^{n_1}xy^{n_2}\cdots xy^{n_k}x = \beta^{n_1}y^{n_2}\cdots xy^{n_k}x$. Type (2) is reduced to (a shorter) type (1) by noting that $y^{n_1}xy^{n_2}\cdots xy^{n_k}x = \alpha^{n_1}xy^{n_2}\cdots xy^{n_k}x$. Type (3) is reduced to type (4) by noting that $xy^{n_1}xy^{n_2}\cdots xy^{n_k} = \beta^{n_1}y^{n_2}\cdots xy^{n_k}$. Type (4) is reduced to (a shorter) type (3) by noting that $y^{n_1}xy^{n_2}\cdots xy^{n_k} = \alpha^{n_1}xy^{n_2}\cdots xy^{n_k}$.

To check the relations on $\ker(h)$, note that

- $\alpha^3 = y^3 = 1$;
- $\beta^3 = (xyx)^3 = xy^3x = xx = 1$;
- $(\alpha\beta)^4 = (yxyx)^4 = y(xy)^8y^{-1} = 1$,

completing the proof. □

For a finitely generated non-elementary subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$, we define $\Gamma^{(2)} = \langle t^2 : t \in \Gamma \rangle$.

Lemma 3.2. *For $\Gamma = \Delta_{(2,3,8)}$ we have $\Gamma^{(2)} = \ker(h)$, and therefore the group $\Delta^{(2)}_{(2,3,8)}$ is isomorphic to the triangle group $\Delta_{(3,3,4)}$.*

Proof. We have $\alpha = \alpha^4 = (\alpha^2)^2$ and similarly for β. Thus $\ker(h) \subset \Delta^{(2)}_{(2,3,8)}$. Choosing T to be the right-angle hyperbolic triangle with acute angles $\frac{\pi}{3}$ and $\frac{\pi}{8}$, we note that the "double" of T, namely the union of T and its reflection in its (longer) side opposite the angle $\frac{\pi}{3}$, is an isosceles triangle with angles $\frac{\pi}{3}$, $\frac{\pi}{3}$, and $\frac{\pi}{4}$, proving the lemma. ☐

Definition 3.3 ([19])**.** Let Γ be a finitely generated non-elementary subgroup of $\mathrm{PSL}_2(\mathbb{R})$. The *invariant trace field of* of Γ, denoted by $k\Gamma$, is the field $\mathbb{Q}(\mathrm{tr}\Gamma^{(2)})$.

Definition 3.4. For an (ℓ, m, n) triangle group, let

$$\lambda(\ell,m,n) := 4\cos^2\frac{\pi}{\ell} + 4\cos^2\frac{\pi}{m} + 4\cos^2\frac{\pi}{n} + 8\cos\frac{\pi}{\ell}\cos\frac{\pi}{m}\cos\frac{\pi}{n} - 4.$$

In particular, $\lambda(3,3,4) = \sqrt{2}$. Therefore by [19, p. 265], the invariant trace field of $\Delta_{(3,3,4)}$ (see Definition 3.3) is

$$k\Delta_{(3,3,4)} = \mathbb{Q}(\sqrt{2}). \tag{3.2}$$

By Takeuchi's theorem ([25]; see [19, Theorem 8.3.11]), the (ℓ, m, n) triangle group is arithmetic if and only if for every non-trivial embedding σ of its invariant trace field in $\mathbb{R}$, we have $\sigma(\lambda(\ell, m, n)) < 0$. The field $\mathbb{Q}(\sqrt{2})$ has two imbeddings in $\mathbb{R}$. The non-trivial imbedding sends $\sqrt{2}$ to $-\sqrt{2} < 0$. Therefore by Takeuchi's theorem, the group $\Delta_{(3,3,4)}$ is arithmetic.

4. Partition of Bolza surface

The Bolza surface M is a Riemann surface of genus 2 with a holomorphic automorphism group of order 48, the highest for this genus. The surface M can be viewed as the smooth completion of its affine form

$$y^2 = x^5 - x \tag{4.1}$$

where $(x, y) \in \mathbb{C}^2$. Here M is as a double cover of the Riemann sphere ramified over the vertices of the regular inscribed octahedron; this is immediate from the presentation (4.1) where the branch points are $0, \pm1, \pm i, \infty$. These six vertices lift to the Weierstrass points of M. The hyperelliptic involution of M fixes the six Weierstass points. It also switches the two sheets of the cover and is a lift of the identity map on the Riemann sphere. The hyperelliptic involution can be thought of in affine coordinates (4.1) as the map $(x, y) \mapsto (x, -y)$. The projection of M to the Riemann sphere is induced by the projection to the x-coordinate.

The surface M admits a partition into (2,3,8) triangles, which is obtained as follows. We start with the (octahedral) partition of the sphere into 8 equilateral hyperbolic triangles with angle $\pi/4$. We then consider the barycentric subdivision, so that each equilateral triangle is subdivided into 6 triangles of type (2,3,8).

Here the Weierstrass points correspond to the vertices of the (2,3,8) triangle with angle $\pi/8$. The partition of the Riemann sphere into copies of the (2,3,8) triangle induces a partition of M into such triangles. On the sphere, we have 8 triangles meeting at each branch point (corresponding to a Weierstrass point on the surface), for a total angle of π around the branch point. This conical singularity is "smoothed out" when we pass to the double cover to obtain the hyperbolic metric on M.

To form the $(3,3,4)$ partition, we pair up the $\pi/8$ angles, by combining the (2,3,8) triangles into pairs whose common side lies on an edge of the octahedron. This creates a partition of the sphere into copies of the $(3,3,4)$ triangle and induces a partition of M into copies of the $(3,3,4)$ triangle. Therefore the vertex of the $(3,3,4)$ triangle where the angle is $\pi/4$ lifts to a Weierstrass point on M.

5. The quaternion algebra

For the benefit of geometers who may not be familiar with quaternian algebras, we will give a presentation following Maclachlan and Reid 2003 [19, p. 265] but in more detail. To study the $(3,3,4)$ case, we will exploit the quaternion algebra

$$D_B = K\left[i, j \mid i^2 = -3,\ j^2 = \sqrt{2},\ ij = -ji\right] \tag{5.1}$$

where $K = \mathbb{Q}(\sqrt{2})$. Denote by σ_0 the natural embedding of K in $\mathbb{R}$ and by σ the other embedding, sending $\sqrt{2}$ to $-\sqrt{2}$.

Definition 5.1. A quaternion algebra D is said to *split* under a completion (archimedean or nonarchimedean) if it becomes a matrix algebra. It is said to be *ramified* if it remains a division algebra.

Remark 5.2. In general there is a finite even number of places where a quaternion algebra ramifies, including the archimedean ramified places.[1] Our algebra D_B ramifies at two places: the archimedean place σ and the nonarchimedean place $(\sqrt{2})$ (see below).

Proposition 5.3. *The algebra D_B splits under the natural embedding of the center in $\mathbb{R}$ and remains a division algebra under the other embedding.*

[1] Recall that in the Hurwitz case there are two archimedean ramified places and no nonarchimedean ones (see [13]).

Proof. Since $\sqrt{2} > 0$, we have

$$D_B \otimes_{\sigma_0} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$$

by [10, Theorem 5.2.1]. Meanwhile, under σ the algebra D_B remains a division algebra since $-\sqrt{2} < 0$, and following [10, Theorem 5.2.3], we have $D_B \otimes_\sigma \mathbb{R} \cong \mathbb{H}$ where $\mathbb{H}$ is the Hamilton quaternion algebra. □

Corollary 5.4. *The algebra D_B is a division algebra.*

Proof. Indeed D_B is a domain as a subring of $D_B \otimes_\sigma \mathbb{R}$, and being algebraic over its center, it is a division algebra. □

Proposition 5.5. *The algebra D_B ramifies at the prime $(\sqrt{2})$ and is split at all other non-archimedean places.*

Proof. The ring of integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$, in which the ideals $(\sqrt{2})$ and (3) are prime. The discriminant of D_B is $-6\sqrt{2}$, thus the algebra splits over any prime other than $(\sqrt{2})$ and (3).

Recall that $\mathbb{Q}_p$ denotes the field of p-adic numbers, where p is a rational prime. Notice that 2 is not a square in $\mathbb{Z}/3\mathbb{Z}$, and therefore it cannot be a square in $\mathbb{Q}_3$, so the completion $\mathbb{Q}_3(\sqrt{2})$ of $\mathbb{Q}(\sqrt{2})$ at the prime 3 is a quadratic extension of $\mathbb{Q}_3$. To show that D_B splits at (3), it suffices to present $\sqrt{2}$ as a norm in the quadratic extension $\mathbb{Q}_3(\sqrt{2}, \sqrt{-3})/\mathbb{Q}_3(\sqrt{2})$, namely in the form $x^2 + 3y^2$ for $x, y \in \mathbb{Q}_3(\sqrt{2})$. By Hasse's principle, it suffices to solve the equation in the residue field $\mathbb{Z}_3[\sqrt{2}]/3\mathbb{Z}_3[\sqrt{2}] = \mathbb{F}_9$, where one can take $x = 1 - \sqrt{2}$ and $y = 0$ (indeed $(1-\sqrt{2})^2 = 3 - 2\sqrt{2} \equiv \sqrt{2} \pmod 3$).

Finally we show that D_B remains a division algebra under the completion of $\mathbb{Q}(\sqrt{2})$ at the prime $(\sqrt{2})$, which is $\mathbb{Q}_2(\sqrt{2})$. It suffices to show that $\sqrt{2}$ is not of the form $x^2 + 3y^2$ for $x, y \in \mathbb{Q}_2(\sqrt{2})$. Clearing out common denominators, we will show that there is no non-zero solution to

$$x^2 + 3y^2 = \sqrt{2}z^2$$

with $x, y, z \in \mathbb{Z}_2[\sqrt{2}]$. We may assume not all of x, y, z are divisible by $\sqrt{2}$. This equation does have a solution modulo 4 (indeed, take $x = y = 1$ and $z = 0$). We will show that there is no solution modulo $4\sqrt{2}$. So assume

$$x^2 + 3y^2 \equiv \sqrt{2}z^2 \pmod{4\sqrt{2}}.$$

Observe that if one of x, y is divisible by $\sqrt{2}$, then they both are. But in that case z is also divisible by $\sqrt{2}$, contrary to assumption. So we can write $x = 1 + \sqrt{2}x'$ and $y = 1 + \sqrt{2}y'$ for $x', y' \in \mathbb{Z}_2[\sqrt{2}]$. Substituting, we have

$$2\sqrt{2} + 2x' + \sqrt{2}x'^2 + 2y' + 3\sqrt{2}y'^2 \equiv z^2 \pmod 4,$$

so z is divisible by $\sqrt{2}$ and we can write $z = \sqrt{2}z'$ for $z' \in \mathbb{Z}_2[\sqrt{2}]$. Now

$$2 + \sqrt{2}x' + x'^2 + \sqrt{2}y' + 3y'^2 \equiv \sqrt{2}z'^2 \pmod{2\sqrt{2}},$$

so $y' \equiv x' \pmod{\sqrt{2}}$, and we write $y' = x' + \sqrt{2}y''$ for $y'' \in \mathbb{Z}_2[\sqrt{2}]$. Substituting we get

$$2 + 2y'' + 2y''^2 \equiv \sqrt{2}z'^2 \pmod{2\sqrt{2}},$$

so clearly z is divisible by $\sqrt{2}$, and then

$$2 + 2y'' + 2y''^2 \equiv 0 \pmod{2\sqrt{2}},$$

which implies

$$1 + y'' + y''^2 \equiv 0 \pmod{\sqrt{2}},$$

a contradiction since $y'' + y''^2$ is always divisible by $\sqrt{2}$. □

6. The standard order in D_B and maximal orders containing it

In this section we prove Lemma 1.1. Recall that an order M in a quaternion algebra D over a number field is maximal if and only if its discriminant is equal to the discriminant of D [26, Corollaire III.5.3], where the discriminant of D is the product of the ramified non-archimedean primes. If M happens to be free as an O_K-module, spanned by $x_1, \ldots, x_4$, then its discriminant is easily computed as the square root of the determinant of the matrix of reduced traces $(\mathrm{Tr}_D(x_i x_j))$.

Since $a = -3$ and $b = \sqrt{2}$ are in $O_K = \mathbb{Z}[\sqrt{2}]$, we obtain an order $\mathcal{O} \subset D_B$ by setting

$$\mathcal{O} = O_K\,[i, j] = O_K 1 + O_K i + O_K j + O_K ij.$$

This is the "standard order" resulting from the presentation of D_B, for which we have $\mathrm{disc}(\mathcal{O})^2 = 16a^2b^2$, so that $\mathrm{disc}(\mathcal{O}) = 12\sqrt{2}$. On the other hand $\mathrm{disc}(D_B) = \sqrt{2}$ by Proposition 5.3, so $\mathcal{O}$ is not maximal. We seek a maximal order $\mathcal{Q}$ containing $\mathcal{O}$. Comparing the discriminants, we know in advance that $[\mathcal{Q}:\mathcal{O}] = 144$.

Notice that

$$\alpha = \frac{1}{2}(1 + i) \tag{6.1}$$

is an algebraic integer. We make the following observation.

Proposition 6.1. *The order $\mathcal{O}_1$ generated over $\mathcal{O}$ by α is $O_K[\alpha, j]$, which is spanned as a (free) O_K-module by the elements*

$$1,\ \alpha,\ j,\ \alpha j.$$

In particular $\mathrm{disc}(\mathcal{O}_1) = 3\sqrt{2}$.

Proof. Since $i = 2\alpha - 1$, clearly $\mathcal{O}[\alpha] = O_K[i,j,\alpha] = O_K[\alpha, j]$. To show that this module is equal to $O_K + O_K\alpha + O_K j + O_K\alpha j$, it suffices to note that $j^2 = \sqrt{2}$,

$$\alpha^2 = \alpha - 1$$

and

$$j\alpha = j - \alpha j.$$

The claim on the discriminant of $\mathcal{O}_1$ then follows from computing the determinant of the 4×4 traces matrix, using $\mathrm{tr}(\alpha) = 1$ and $\mathrm{tr}(j\alpha j) = \sqrt{2}$. □

Now let

$$\gamma = \frac{1}{6}(3+i)\left[1 - (1+\sqrt{2})j\right] \tag{6.2}$$

and consider the O_K-module

$$\mathcal{Q} = O_K + O_K\alpha + O_K\gamma + O_K\alpha\gamma.$$

Proposition 6.2. *The module $\mathcal{Q}$ is a maximal order of D_B. Moreover, $\mathcal{Q}$ contains $\mathcal{O}_1$.*

Proof. First note that

$$j = (1-\sqrt{2})(-1 + 2\gamma - \alpha\gamma),$$

so that $\mathcal{O} \subseteq \mathcal{O}_1 \subseteq \mathcal{Q}$.

To prove that $\mathcal{Q}$ is an order it suffices to show it is closed under multiplication, which follows by verifying the relations:

$$\begin{aligned} \alpha^2 &= -1 + \alpha \\ \gamma^2 &= (1+\sqrt{2}) + \gamma \\ \gamma\alpha &= -1 + \alpha + \gamma - \alpha\gamma. \end{aligned}$$

Maximality of $\mathcal{Q}$ follows by computation of the discriminant, which turns out to be $\sqrt{2}$. □

Also let $\gamma' = i\gamma i^{-1} = \frac{1}{6}(3+i)\left[1 + (1+\sqrt{2})j\right]$, and

$$\mathcal{Q}' = O_K + O_K\alpha + O_K\gamma' + O_K\alpha\gamma'.$$

Notice that $\mathcal{Q}' = i\mathcal{Q}i^{-1}$ is conjugate to $\mathcal{Q}$.

Corollary 6.3. *The module $\mathcal{Q}'$ is a maximal order containing $\mathcal{O}_1$.*

Proof. This is immediate because $i\mathcal{O}_1 i^{-1} = \mathcal{O}_1$. □

Proposition 6.4. *The only two maximal orders containing $\mathcal{O}$ are $\mathcal{Q}$ and $\mathcal{Q}'$.*

Proof. Let $y \in D_B$ be an element such that $\mathcal{O}[y]$ is an order. Write

$$y = \frac{1}{2}(x_0 + \frac{x_1}{3}i + \frac{x_2}{\sqrt{2}}j + \frac{x_3}{3\sqrt{2}}ij),$$

where $x_0, x_1, x_2, x_3 \in \mathbb{Q}(\sqrt{2})$. Since $\mathrm{tr}(y\mathcal{O}) \subseteq O_K$, we immediately conclude that in fact $x_0, x_1, x_2, x_3 \in \mathbb{Z}[\sqrt{2}]$. Furthermore, the norm of y is an algebraic integer, proving that $12\sqrt{2}$ divides

$$-3\sqrt{2}x_0^2 - \sqrt{2}x_1^2 + 3x_2^2 + x_3^2$$

in $\mathbb{Z}[\sqrt{2}]$. Working modulo powers of $\sqrt{2}$, we conclude as in Proposition 5.3 that $x_3 = x_2 + 2\sqrt{2}x_3'$, $x_1 = x_0 + 2x_1'$, $x_2 = \sqrt{2}x_2'$ for suitable $x_1', x_2', x_3' \in \mathbb{Z}[\sqrt{2}]$. The remaining condition is that $(x_0 - x_1')^2 \equiv \sqrt{2}(x_2' - x_3')^2 \pmod 3$, so in fact

$$x_0 = x_1' + \theta(1-\sqrt{2})(x_2' - x_3') + 3x_0'$$

for some $x_0' \in \mathbb{Z}[\sqrt{2}]$ where $\theta = \pm 1$. But then

$$\begin{aligned} y - x_0' &= \frac{1}{2}(1+i)(x_0' + x_1') + \frac{1}{2}(j+ij)x_3' \\ &\quad + \frac{1}{6}\left[\theta(1-\sqrt{2})(3+i) + 3j + ij\right](x_2' - x_3') \\ &= (x_0' + x_1')\alpha + x_3'\alpha j + (x_2' - x_3')(1-\sqrt{2})\theta\gamma_\theta, \end{aligned}$$

where $\gamma_{+1} = \gamma$ and $\gamma_{-1} = \gamma'$. Thus y is an element of $\mathcal{Q}$ (if $\theta = 1$) or of $\mathcal{Q}'$ (if $\theta = -1$). □

Note that $\mathcal{Q} + \mathcal{Q}'$ is not an order, since $\gamma + \gamma' = 1 + \frac{i}{3}$ is not an algebraic integer.

7. The Bolza order

In order to present the triangle group $\Delta_{(3,3,4)}$ as a quotient of the group of units in a maximal order, we make the following change of variables. Let

$$\beta = \frac{1}{6}\left(3 + (1+2\sqrt{2})i - 2ij\right). \tag{7.1}$$

Since

$$\beta = \alpha(1 - (1-\sqrt{2})\gamma)$$

(where γ is defined in (6.2)) and

$$\gamma = -(1+\sqrt{2})(1 - \beta + \alpha\beta),$$

we have that

$$\mathcal{Q}_B := O_K[\alpha, \beta] = \mathcal{Q}.$$

In particular, $\mathcal{Q}_B$ is a maximal order by Proposition 6.2.

One has

$$\alpha\beta = -\frac{1}{6}\left(3\sqrt{2} - (2+\sqrt{2})i + 3j - ij\right). \tag{7.2}$$

Theorem 7.1. *The order $\mathcal{Q}_B$ is spanned as a module over O_K by the basis $\{1, \alpha, \beta, \alpha\beta\}$, so that*

$$\mathcal{Q}_B = O_K 1 \oplus O_K \alpha \oplus O_K \beta \oplus O_K \alpha\beta. \tag{7.3}$$

Proof. Let $M = O_K 1 + O_K\alpha + O_K\beta + O_K\alpha\beta$. The following relations are verified by computation:

(1) $\alpha^2 = -1 + \alpha$,
(2) $\beta^2 = -1 + \beta$,
(3) $\beta\alpha = (-1-\sqrt{2}) + \alpha + \beta - \alpha\beta$;

and thus $\alpha(\alpha\beta) = -\beta + \alpha\beta \in M$ and

$$\beta(\alpha\beta) = (-1-\sqrt{2})\beta + \alpha\beta + \beta^2 - \alpha\beta^2 = -1 + \alpha - \sqrt{2}\beta \in M.$$

It follows that $\alpha M, \beta M \subseteq M$, so M is closed under multiplication and is therefore equal to $\mathcal{Q}_B$.

□

8. The triangle group in the Bolza order

Let $\mathcal{Q}_B^1$ denote the group of elements of norm 1 in the order $\mathcal{Q}_B$. Through the embedding $D_B \hookrightarrow \mathrm{M}_2(\mathbb{R})$, we may view $\mathcal{Q}_B^1$ as an arithmetic lattice of $\mathrm{SL}_2(\mathbb{R})$. Furthermore, by Proposition 5.3 the algebra D_B ramifies at all the archimedean places except for the natural one, so it satisfies Eichler's condition; see [26, p. 82]. Therefore $\mathcal{Q}_B^1$ is a co-compact lattice.

Since $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = 1$, the subgroup generated by α, β in $D_B^\times$ is contained in $\mathcal{Q}_B^1$.

Proposition 8.1. *The elements α, β defined in* (6.1) *and* (7.1) *satisfy the relations*

$$\alpha^3 = \beta^3 = (\alpha\beta)^4 = -1.$$

Proof. First we note that $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = 1$. The minimal polynomial of every non-scalar element of D_B is quadratic, determined by the trace and norm of the element. Since $\mathrm{tr}(\alpha) = \mathrm{tr}(\beta) = 1$, both α and β are roots of the polynomial $\lambda^2 - \lambda + 1$, which divides $\lambda^3 + 1$. Similarly $\mathrm{tr}(\alpha\beta) = -\sqrt{2}$, so $\alpha\beta$ is a root of $\lambda^2 + \sqrt{2}\lambda + 1$, which divides $\lambda^4 + 1$. □

A comparison of the areas of the fundamental domains shows that in fact $\mathcal{Q}_B^1 = \langle \alpha, \beta \rangle$ and that $\mathcal{Q}_B^1/\{\pm 1\}$ is isomorphic to the triangle group $\Delta_{(3,3,4)}$.

9. A lower bound for the systole

We give lower bounds on the systole of congruence covers of any arithmetic surface and then specialize to the Bolza surface. Let K be any number field, O_K its ring of integers, D any central division algebra over K, and Q an order in D. Let $X_1 = \mathcal{H}^2/Q^1$, where Q^1 is the group of elements of norm 1 in Q. We let $d = [K:\mathbb{Q}]$.

We quote the definition of the constant $\Lambda_{D,Q}$ from [13, Equation (4.9)]. Let T_1 denote the set of finite places $\mathfrak{p}$ of K for which $D_\mathfrak{p}$ is a division algebra, and let T_2 denote the set of finite places for which $Q_\mathfrak{p}$ is non-maximal. It is well known that T_1 and T_2 are finite. We denote

$$\Lambda_{D,Q} = \prod_{\mathfrak{p}\in T_1\setminus T_2} \left(1+\frac{1}{\mathrm{N}(\mathfrak{p})}\right) \cdot \prod_{\mathfrak{p}\in T_2} 2 \cdot \prod_{\mathfrak{p}\in T_2, \mathfrak{p}\,|\,2} \mathrm{N}(\mathfrak{p})^{e(\mathfrak{p})}, \tag{9.1}$$

where for a diadic prime, $e(\mathfrak{p})$ denotes the ramification index of 2 in the completion $O_\mathfrak{p}$, namely $\mathfrak{p}^{e(\mathfrak{p})}O_\mathfrak{p} = 2O_\mathfrak{p}$, and $\mathrm{N}(I)$ denotes the norm of the ideal I. This constant is chosen in [13] to ensure that $[Q^1 : Q^1(I)] \le \Lambda_{D,Q}\mathrm{N}(I)^3$, for any ideal I.

Recall that if $I \lhd O_K$ is any ideal, then $Q^1(I)$ is the kernel of the natural map $Q^1 \to (Q/IQ)^1$ induced by the ring epimorphism $Q \to Q/IQ$. This congruence subgroup gives rise to the surface $X_I = \mathcal{H}^2/Q^1(I)$, which covers X_1. A bound for the reduced trace was given in [13, Equation (2.5)] as follows. Let $x \ne \pm 1$ in $Q^1(I)$. Then we have

$$|\mathrm{Tr}_D(x)| > \frac{1}{2^{2(d-1)}}\mathrm{N}(I)^2 - 2. \tag{9.2}$$

By [13, Corollary 4.6], we have

$$[Q^1 : Q^1(I)] \le \Lambda_{D,Q} N(I)^3.$$

Therefore

$$\begin{aligned} 4\pi\,(g(X_I)-1) &\le \mathrm{area}(X_I) \\ &= [Q^1 : Q^1(I)] \cdot \mathrm{area}(X_1) \\ &\le \Lambda_{D,Q} N(I)^3 \cdot \mathrm{area}(X_1), \end{aligned}$$

i.e.

$$N(I) \ge \left(\frac{4\pi}{\Lambda_{D,Q}\cdot \mathrm{area}(X_1)}(g-1)\right)^{\frac{1}{3}}.$$

Proposition 9.1. *Suppose $2^{3(d-1)}\Lambda_{D,Q} < \frac{4\pi}{area(X_1)}$. Then all but finitely many principal congruence covers of X_1 satisfy the relation*

$$\mathrm{sys} > \frac{4}{3}\log g.$$

Proof. A hyperbolic element x in a Fuchsian group $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{R})$ is conjugate to a matrix
$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}.$$

Here $\lambda = e^{\ell_x/2} > 1$, where $\ell_x > 0$ is the length of the closed geodesic corresponding to x on the Riemann surface $\mathcal{H}^2/\Gamma$. Since
$$\left|\mathrm{Tr}_{M_2(\mathbb{R})}(x)\right| = \left|\lambda + \lambda^{-1}\right| \leq |\lambda| + \left|\lambda^{-1}\right| \leq |\lambda| + 1,$$
we get
$$\ell_x = 2\log|\lambda| > 2\log\left(\left|\mathrm{Tr}_{M_2(\mathbb{R})}(x)\right| - 1\right).$$

By (9.2),
$$\begin{aligned} \mathrm{sys}(X_I) &> 2\log\left(|\mathrm{Tr}_D(x)| - 1\right) \\ &> 2\log\left(\frac{1}{2^{2(d-1)}}\mathrm{N}(I)^2 - 3\right) \qquad (9.3) \\ &\geq 2\log\left(\frac{1}{2^{2(d-1)}}\left[\frac{4\pi}{\Lambda_{D,Q}\cdot \mathrm{area}(X_1)}\left(g(X_I) - 1\right)\right]^{\frac{2}{3}} - 3\right). \end{aligned}$$

Expanding the argument under the logarithm as a series in g, we find that the coefficient of the highest term $g^{2/3}$ is $\left[\frac{1}{2^{3(d-1)}}\frac{4\pi}{\Lambda_{D,Q}\cdot \mathrm{area}(X_1)}\right]^{\frac{2}{3}}$. When this coefficient is strictly greater than 1, for sufficiently large g we have that
$$\mathrm{sys}(X_I) > \frac{4}{3}\log\left(g(X_I)\right). \qquad \square$$

A closer inspection of (9.3) enables us to provide an explicit bound on the genera g for which the inequality of Proposition 9.1 holds.

Remark 9.2. We have that
$$2\log\left(\frac{1}{2^{2(d-1)}}\left[\frac{4\pi}{\Lambda_{D,Q}\cdot \mathrm{area}(X_1)}\left(g - 1\right)\right]^{\frac{2}{3}} - 3\right) > \frac{4}{3}\log(g)$$
if and only if
$$\frac{\left(1 + \frac{3}{g^{2/3}}\right)^{3/2}}{1 - \frac{1}{g}} \leq \frac{4\pi}{2^{3(d-1)}\Lambda_{D,Q}\cdot \mathrm{area}(X_1)}.$$

Since
$$\frac{\left(1 + \frac{3}{g^{2/3}}\right)^{3/2}}{1 - \frac{1}{g}} \leq 1 + \frac{6}{g^{2/3}}$$

for every $g \geq 13$, we conclude that if $2^{3(d-1)}\Lambda_{D,Q} < \frac{4\pi}{\mathrm{area}(X_1)}$, then $\mathrm{sys} > \frac{4}{3}\log g$ provided that

$$g \geq \max\left\{13, \left(\frac{6}{\frac{4\pi}{2^{3(d-1)}\Lambda_{D,Q}\mathrm{area}(X_1)}-1}\right)^{3/2}\right\}.$$

Corollary 9.3. *Principal congruence covers of the Bolza order satisfy the bound* $\mathrm{sys} > \frac{4}{3}\log g$ *provided that* $g \geq 15$.

Proof. Since the order $\mathcal{Q}_B$ is maximal, it follows (e.g. by [19, Corollary 6.2.8]) that all localisations are maximal as well. Therefore the set T_2 is empty (see material around [13, formula 4.10]), while T_1 consists of a single nonarchimedean place $\sqrt{2}$ with norm 2 (see Remark 5.2). Therefore $\Lambda_{D_B,\mathcal{Q}_B} = \frac{3}{2}$.

Moreover, since $\mathcal{Q}_B^1/\{\pm 1\}$ is the triangle group $(3,3,4)$, we have

$$\mathrm{area}(X_1) = 2\left(\pi - \left(\frac{\pi}{3} + \frac{\pi}{3} + \frac{\pi}{4}\right)\right) = \frac{\pi}{6},$$

so $\frac{4\pi}{\mathrm{area}(X_1)} = 24$. Finally the dimension of the invariant trace field over $\mathbb{Q}$ is $d = 2$, so the condition $2^{3(d-1)}\Lambda_{D_B,\mathcal{Q}_B} < \frac{4\pi}{\mathrm{area}(X_1)}$ of Proposition 9.1 holds since $12 < 24$.

In order to obtain the explicit lower bound on g, we substitute in Remark 9.2, using the numerical value $6^{3/2} \approx 14.697$. □

10. The Fuchsian group of the Bolza surface

In this section we give an explicit presentation of the Fuchsian group of the Bolza surface in terms of the quaternion algebra $\mathcal{Q}_B$. We start with a geometric lemma that will motivate the introduction of the special element exploited in Lemma 10.2.

Lemma 10.1. *Let* $\bar{A}$ *and* $\bar{B}$ *be antipodal points on a systolic loop of a hyperbolic surface* M. *Let* A *and* B *be their lifts to the universal cover such that* $d(A,B) = \frac{1}{2}\mathrm{sys}(M)$. *Let* τ_A *and* τ_B *be the involutions of the universal cover with centers at* A *and* B. *Then the composition* $\tau_B \circ \tau_A$ *belongs to a conjugacy class in the fundamental group defined by the systolic loop.*

Proof. A composition of two involutions gives a translation by twice the distance between the fixed points of the involutions. Thus, consider the hyperbolic line ρ in the universal cover passing through A and B. Then the composition $\tau_B \circ \tau_A$ is a hyperbolic translation along ρ with displacement distance precisely $\mathrm{sys}(M)$. The image of the projection of ρ back to M is the systolic loop. □

We now apply Lemma 10.1 in a situation where the points A and B are lifts of Weierstrass points on the Bolza surface (see Section 4 for details). The composition of the involutions $(\alpha\beta)^2$ and $(\beta\alpha)^2$ yields the desired element. This element was obtained through a detailed geometric analysis of the action in the upperhalf plane which we will not reproduce (`magma` was not used here).

Lemma 10.2. *The element* $(\alpha\beta)^2(\beta\alpha)^{-2}$ *is in the congruence subgroup* $\mathcal{Q}^1_B(\sqrt{2})$.

Proof. One has $(\alpha\beta)^2(\beta\alpha)^2 = 1 + \sqrt{2}(1 + (1 + \sqrt{2})(\alpha - \beta))$. □

Proposition 10.3. *The normal subgroup of the* $(3, 3, 4)$ *triangle group generated by the element* $(\alpha\beta)^2(\beta\alpha)^{-2}$ *has index* 24. *The normal subgroup is generated by the following four elements:*

- $c_1 = \alpha^{-1}\beta\alpha\beta^{-1}\alpha\beta$,
- $c_2 = \alpha\beta^{-1}\alpha\beta\alpha^{-1}\beta$,
- $c_3 = \alpha\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta^{-1}$,
- $c_4 = \beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha$,

*which satisfy a single length-*8 *relation* $c_4^{-1}c_3^{-1}c_2c_4c_1c_2^{-1}c_1^{-1}c_3 = 1$. *The reduced traces are*

$$\mathrm{tr}(c_1) = \mathrm{tr}(c_2) = \mathrm{tr}(c_3) = \mathrm{tr}(c_4) = -2(1 + \sqrt{2}).$$

This was checked directly using the `magma` package.

Corollary 10.4. *The normal subgroup of* $\mathcal{Q}^1_B$ *generated by the element* $(\alpha\beta)^2(\beta\alpha)^{-2}$ *generates the Fuchsian group of the Bolza surface.*

Proof. The presentation of the Fuchsian group given in Proposition 10.3 implies that the surface has genus 2. This identifies it as the Bolza surface which is the unique genus-2 surface admitting a tiling of type $(3, 3, 4)$ or (2,3,8); see Bujalance & Singerman (1985 [6, p. 518]). This surface is known to have the largest systole in genus 2, or equivalently largest trace $2(1+\sqrt{2})$ (see e.g., Bavard [5, p. 6], Katz & Sabourau [11], Schmutz [23]). Therefore all 4 generators specified in Proposition 10.3 correspond to systolic loops. □

11. An elliptic element of order 2

The principal congruence subgroup $\mathcal{Q}^1_B(\sqrt{2})$ contains the Fuchsian group of the Bolza surface (see Lemma 10.2), but it also contains torsion elements. The element

$$\varpi = 1 + \sqrt{2}\alpha\beta \tag{11.1}$$

in $\mathcal{Q}_B^1(\sqrt{2})$ defines an elliptic (torsion) element of order 2 in the Fuchsian group. Indeed, applying the relations given in Theorem 7.1, we have $(\alpha\beta)^2 = -1 - \sqrt{2}\alpha\beta$. Hence

$$\varpi^2 = (1 + \sqrt{2}\alpha\beta)^2 = 1 + 2\sqrt{2}\alpha\beta + 2(\alpha\beta)^2 = -1$$

and therefore ϖ is of order 2 in the Fuchsian group.

By the above, $\varpi = -(\alpha\beta)^2$. The fixed point of ϖ can be taken to be the vertex of a $(3, 3, 4)$ triangle where the angle is $\pi/4$. The element $\alpha\beta$ gives a rotation by $\pi/2$ around this vertex, and therefore ϖ gives the rotation by π around the vertex of the $(3, 3, 4)$ triangle where the angle is $\pi/4$.

Lemma 11.1. *The action of ϖ descends to the Bolza surface and coincides with the hyperelliptic involution of the surface.*

Proof. The involution ϖ is a rotation by π around a Weierstrass point (see Section 4), namely the vertex of the $(3, 3, 4)$ triangle where the angle is $\pi/4$. Therefore ϖ descends to the identity on the Riemann sphere. Thus ϖ lifts to the hyperelliptic involution of M. □

12. Quotients of the Bolza order

In the next section we compare the Bolza group with some principal congruence subgroups of the Bolza order. To this end, we need to compute quotients of the Bolza order $\mathcal{Q}_B$.

Remark 12.1. In Theorem 7.1 we obtained the presentation

$$\mathcal{Q}_B = O_K\big[\alpha, \beta \,|\, \alpha^2 = -1+\alpha,\ \beta^2 = -1+\beta,\ \beta\alpha = (-1-\sqrt{2})+\alpha+\beta-\alpha\beta\big].$$

The symplectic involution $z \mapsto z^*$ on the quaternion algebra D (of (5.1)) is defined by $i^* = -i$ and $j^* = -j$. It follows from the definition of α, β in (6.1) and (7.1) that

$$\alpha^* = 1 - \alpha, \qquad \beta^* = 1 - \beta; \tag{12.1}$$

so in particular the order $\mathcal{Q}_B$ is preserved under the involution. This is particularly useful for the computation of the groups, because the norm is defined by $N(x) = xx^*$ for every $x \in D$.

12.1. **The Bolza order modulo 2.** Let us compute the ring $\overline{\mathcal{Q}_B} = \mathcal{Q}_B/2\mathcal{Q}_B$, which will be used below to compute the index of $\mathcal{Q}_B^1(2)$ in $\mathcal{Q}_B^1$.

Notice that $O_K/2O_K = \mathbb{Z}[\sqrt{2}]/2\mathbb{Z}[\sqrt{2}] = \mathbb{F}_2[\epsilon \,|\, \epsilon^2 = 0]$, where ϵ stands for the image of $\sqrt{2}$ in the quotient ring.

Proposition 12.2. $\overline{\mathcal{Q}_B} = \mathcal{Q}_B/2\mathcal{Q}_B$ *is a local noncommutative ring with* 256 *elements, whose residue field has order* 4*, and whose maximal ideal J has nilpotency index* 4*. Moreover each of the quotients J/J^2, J^2/J^3 and $J^3 = J^3/J^4$ is one-dimensional over $\overline{\mathcal{Q}_B}/J \cong \mathbb{F}_4$.*

Proof. Replacing β by $\beta' = \beta + \alpha + 1 + \epsilon$ in the presentation of Remark 12.1, we obtain the quotient

$$\overline{\mathcal{Q}_B} = \mathbb{F}_2[\epsilon \,|\, \epsilon^2 = 0][\alpha, \beta' \,|\, \alpha^2 = 1 + \alpha,\ \beta'^2 = \epsilon,\ \beta'\alpha + \alpha\beta' = \beta'],$$

where ϵ is understood to be central (which actually follows from the relations).

This ring has a maximal ideal $J = \beta'\overline{\mathcal{Q}_B}$, with $J^2 = \epsilon\overline{\mathcal{Q}_B}$ and $J^3 = \epsilon\beta'\overline{\mathcal{Q}_B}$, and with a quotient ring

$$\overline{\mathcal{Q}_B}/J = \mathbb{F}_2[\alpha \,|\, \alpha^2 = 1 + \alpha] \cong \mathbb{F}_4.$$

Taking $\mathbb{F}_4 = \mathbb{F}_2[\alpha] = \mathbb{F}_2 + \mathbb{F}_2\alpha$, we obtain

$$\overline{\mathcal{Q}_B} = \mathbb{F}_4 \oplus \mathbb{F}_4\beta' \oplus \mathbb{F}_4\epsilon \oplus \mathbb{F}_4\epsilon\beta',$$

where β' acts on $\mathbb{F}_4$ by $\beta'\alpha = (\alpha+1)\beta'$, $\beta'^2 = \epsilon$ and $\epsilon^2 = 0$, so the ring has 256 elements. ☐

12.2. **The quotients $\widetilde{\mathcal{Q}_B} = \mathcal{Q}_B/\sqrt{2}\mathcal{Q}_B$.** Since ϵ stands for the image of $\sqrt{2}$ in $\overline{\mathcal{Q}_B}$, we immediately obtain the quotient $\mathcal{Q}_B/\sqrt{2}\mathcal{Q}_B = \overline{\mathcal{Q}_B}/\epsilon\,\overline{\mathcal{Q}_B}$:

Proposition 12.3. $\widetilde{\mathcal{Q}_B} = \mathcal{Q}_B/\sqrt{2}\mathcal{Q}_B$ *is a local noncommutative ring with a maximal ideal with* 4 *elements and a quotient field of order* 4*.*

Proof. Taking $\epsilon = 0$ in the presentation of $\overline{\mathcal{Q}_B} = \mathcal{Q}_B/2\mathcal{Q}_B$ obtained above, we get

$$\widetilde{\mathcal{Q}_B} = \mathbb{F}_2[\alpha, \beta' \,|\, \alpha^2 = 1 + \alpha,\ \beta'^2 = 0,\ \beta'\alpha + \alpha\beta' = \beta'],$$

which can be written as

$$\widetilde{\mathcal{Q}_B} = \mathbb{F}_4 \oplus \mathbb{F}_4\beta';$$

this quotient of $\overline{\mathcal{Q}_B} = \mathcal{Q}_B/2\mathcal{Q}_B$ has 16 elements. The ideal

$$\beta'\widetilde{\mathcal{Q}_B} = \mathbb{F}_2\beta' + \mathbb{F}_2\alpha\beta'$$

has four elements, and $(\beta'\widetilde{\mathcal{Q}_B})^2 = 0$. ☐

12.3. **Involution and norm.** The involution defined on $\mathcal{Q}_B$ clearly preserves $2\mathcal{Q}_B$, so it induces an involution on the quotient $\overline{\mathcal{Q}_B}$. Using (12.1), we conveniently have that $\beta'^* = \beta^* + \alpha^* + 1 + \epsilon = \beta'$.

The subring $\mathbb{F}_2[\epsilon, \alpha]$ of $\overline{\mathcal{Q}_B}$ is commutative, and the involution induces the automorphism σ of $\mathbb{F}_2[\epsilon, \alpha]$ defined by $\sigma(\alpha) = \alpha + 1$ and $\sigma(\epsilon) = \epsilon$. The norm defined above coincides with the Galois norm,

$$N(x_0 + x_1\alpha) = (x_0 + x_1\alpha)(x_0 + x_1(\alpha + 1)) = x_0^2 + x_0x_1 + x_1^2$$

for $x_0, x_1 \in \mathbb{F}_2[\epsilon]$. Furthermore, writing

$$\overline{\mathcal{Q}_B} = \mathbb{F}_2[\epsilon, \alpha] \oplus \mathbb{F}_2[\epsilon, \alpha]\beta',$$

we have for $y_0, y_1 \in \mathbb{F}_2[\epsilon, \alpha]$ that $(y_0 + y_1\beta')^* = y_0^* + \beta' y_1^* = y_0^* + y_1\beta'$. Therefore, for every $y_0, y_1 \in \mathbb{F}_2[\epsilon, \alpha]$,

$$N(y_0 + y_1\beta') = (y_0 + y_1\beta')(y_0^* + y_1\beta') = N(y_0) + N(y_1)\epsilon \in \mathbb{F}_2[\epsilon].$$

Together, we have

$$N(x_{00}+x_{01}\alpha+x_{10}\beta'+x_{11}\alpha\beta') = (x_{00}^2+x_{00}x_{01}+x_{11}^2)+(x_{10}^2+x_{10}x_{11}+x_{11}^2)\epsilon$$

for every $x_{00}, x_{01}, x_{10}, x_{11} \in \mathbb{F}_2[\epsilon]$.

Clearly, an element is invertible if and only if its norm is invertible. There are two invertible elements in $\mathbb{F}_2[\epsilon]$, namely 1 and $1 + \epsilon$, and $1 + \epsilon = N(1 + \epsilon\alpha)$ is obtained as a norm, so we conclude:

Corollary 12.4. *The subgroup* $\overline{\mathcal{Q}_B}^1 = \left\{x \in \overline{\mathcal{Q}_B} : N(x) = 1\right\}$ *has index* 2 *in the group of invertible elements* $\overline{\mathcal{Q}_B}^\times$.

In contrast, when we reduce further to the quotient $\widetilde{\mathcal{Q}_B} = \mathcal{Q}_B/\sqrt{2}\mathcal{Q}_B$, which is equal to $\overline{\mathcal{Q}_B}/\epsilon\overline{\mathcal{Q}_B}$, the induced norm function takes values in $\mathbb{F}_2[\epsilon]/\epsilon\mathbb{F}_2[\epsilon] = \mathbb{F}_2$, where only the identity is invertible. We therefore obtain the following corollary.

Corollary 12.5. *The subgroup* $\widetilde{\mathcal{Q}_B}^1 = \left\{x \in \widetilde{\mathcal{Q}_B} : N(x) = 1\right\}$ *is equal to* $\widetilde{\mathcal{Q}_B}^\times$.

12.4. **Subgroups of $\overline{\mathcal{Q}_B}^\times$.** The ring $\overline{\mathcal{Q}_B} = \mathcal{Q}_B/2\mathcal{Q}_B$ has a unique maximal ideal $J = \beta'\overline{\mathcal{Q}_B}$, and its powers are

$$0 = J^4 \subset J^3 = \epsilon\beta'\overline{\mathcal{Q}_B} \subset J^2 = \epsilon\overline{\mathcal{Q}_B} \subset J = \beta'\overline{\mathcal{Q}_B}.$$

Similarly to congruence subgroup of $\mathcal{Q}_B$, for every ideal $I \lhd \overline{\mathcal{Q}_B}$ which is stable under the involution (so that the involution and thus the norm are well defined on the quotient $\overline{\mathcal{Q}_B}/I$), we have the subgroups

$$\overline{\mathcal{Q}_B}^1(I) = \overline{\mathcal{Q}_B}^1 \cap (1 + I)$$

and

$$\overline{\mathcal{Q}_B}^{\times}(I) = \overline{\mathcal{Q}_B}^{\times} \cap (1+I);$$

when $I = x\overline{\mathcal{Q}_B}$, we write $\overline{\mathcal{Q}_B}^{1}(x)$ and $\overline{\mathcal{Q}_B}^{\times}(x)$ for $\overline{\mathcal{Q}_B}^{1}(x\overline{\mathcal{Q}_B})$ and $\overline{\mathcal{Q}_B}^{\times}(x\overline{\mathcal{Q}_B})$, respectively.

Proposition 12.6. *The numbers along edges in Figure 12.1 are the relative indices of the depicted subgroups.*

Proof. The argument leading to Corollary 12.4 also implies that

$$[\overline{\mathcal{Q}_B}^{\times}(\beta') : \overline{\mathcal{Q}_B}^{1}(\beta')] = [\overline{\mathcal{Q}_B}^{\times}(\epsilon) : \overline{\mathcal{Q}_B}^{1}(\epsilon)] = 2,$$

because the invertible element $1+\epsilon\alpha$, whose norm is $1+\epsilon$ and not 1, is in $\overline{\mathcal{Q}_B}^{\times}(\epsilon)$. However,

$$\overline{\mathcal{Q}_B}^{\times}(\epsilon\beta') = \overline{\mathcal{Q}_B}^{1}(\epsilon\beta')$$

because $N(1+x_3\epsilon\beta') = 1$ for every $x_3 \in \mathbb{F}_2[\alpha]$. Moreover, since $\overline{\mathcal{Q}_B}$ is explicitly known, it is easy to compute the quotients

$$\overline{\mathcal{Q}_B}^{\times} / \overline{\mathcal{Q}_B}^{\times}(\beta') \cong \mathbb{F}_4^{\times}$$

and

$$\overline{\mathcal{Q}_B}^{\times}(J^i) / \overline{\mathcal{Q}_B}^{\times}(J^{i+1}) \cong \mathbb{F}_4^{+}, \qquad (i = 1,2,3);$$

together, we have all the indices of the subgroups as depicted in the diagram. ☐

Since we encounter several small classical groups, let us record their interactions.

Remark 12.7. The group A_4 of even permutation on 4 letters is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_3)$, and $S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$. The group A_4 has two central extensions by $\mathbb{Z}/2\mathbb{Z}$: the trivial one, namely $A_4 \times \mathbb{Z}/2\mathbb{Z}$, and the group $\mathrm{SL}_2(\mathbb{F}_3)$. Likewise $\mathrm{GL}_2(\mathbb{F}_3)$ is a central extension of S_4 by $\mathbb{Z}/2\mathbb{Z}$, and we have the short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_3) & \longrightarrow & \mathrm{PGL}_2(\mathbb{F}_3) \cong S_4 & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathrm{SL}_2(\mathbb{F}_3) & \longrightarrow & \mathrm{PSL}_2(\mathbb{F}_3) \cong A_4 & \longrightarrow & 1 \end{array}$$

where the image of $\mathbb{Z}/2\mathbb{Z}$ in both groups is central.

Since A_4 has the triangle group presentation

$$\Delta_{(3,3,2)} \cong \langle x, y \mid x^3 = y^3 = (xy)^2 = 1 \rangle,$$

it follows that $\mathrm{SL}_2(\mathbb{F}_3)$ can be presented as

$$\langle x, y \mid x^3 = y^3 = (xy)^4 = 1,\ [x,(xy)^2] = 1 \rangle.$$

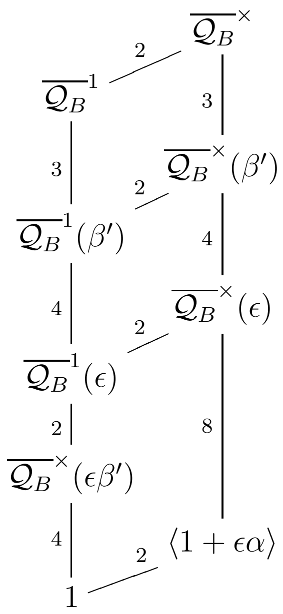

FIGURE 12.1. Subgroups of $\overline{\mathcal{Q}_B}^\times$, with relative indices

Proposition 12.8. *The following holds for the quotients of* $\overline{\mathcal{Q}_B}^1$*:*

$$\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon\beta') \cong \mathrm{SL}_2(\mathbb{F}_3), \tag{12.2}$$

$$\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon) \cong A_4. \tag{12.3}$$

Proof. The elements $\alpha, \beta \in \mathcal{Q}_B^1$, which satisfy $\alpha^3 = \beta^3 = -1$, map to their images $\alpha, \beta \in \overline{\mathcal{Q}_B}^1$. In $\overline{\mathcal{Q}_B}^1$ we have the relations $\alpha^3 = \beta^3 = 1$ (noting that $-1 = 1$ in $\overline{\mathcal{Q}_B} = \mathcal{Q}_B/2\mathcal{Q}_B$), and also, by computation, $(\alpha\beta)^2 = 1 + \epsilon + \epsilon\alpha\beta'$. Passing to the quotient $\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon\beta')$, we have that

$$\alpha^3 = \beta^3 = (\alpha\beta)^4 = [\alpha, (\alpha\beta)^2] = [\beta, (\alpha\beta)^2] = 1$$

since in this quotient $(\alpha\beta)^2 = 1 + \epsilon$, which is central of order 2. By Remark 12.7, the group with this presentation is $\mathrm{SL}_2(\mathbb{F}_3)$, of order 24. To complete the proof, it remains to show that the image of $\langle\alpha, \beta\rangle$ in $\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon\beta')$ has order 24. This can be done by computing in each quotient separately:

- α generates $\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\beta') \cong \mathbb{Z}/3\mathbb{Z}$;
- $\alpha\beta = 1 + \epsilon\alpha + \alpha\beta' \equiv 1 + \alpha\beta' \pmod{\overline{\mathcal{Q}_B}^1(\epsilon)}$, and $\beta\alpha = 1 + \epsilon\alpha + (1+\alpha)\beta' \equiv 1 + (1+\alpha)\beta'$, which together generate $\overline{\mathcal{Q}_B}^1(\beta')/\overline{\mathcal{Q}_B}^1(\epsilon)$, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

- and $(\alpha\beta)^2$ generates $\overline{\mathcal{Q}_B}^1(\epsilon)/\overline{\mathcal{Q}_B}^1(\epsilon\beta') \cong \mathbb{Z}/2\mathbb{Z}$ as we have seen.

As for the second isomorphism, passing with the previous item to the quotient $\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon)$, we have that

$$\alpha^3 = \beta^3 = (\alpha\beta)^2 = 1,$$

so we get the triangle group $\Delta_{(3,3,2)} \cong A_4$. (An explicit isomorphism is obtained by $\alpha \mapsto (123)$ and $\beta \mapsto (124)$). □

Remark 12.9. The following quotients decompose as direct products:

$$\overline{\mathcal{Q}_B}^\times/\overline{\mathcal{Q}_B}^\times(\epsilon\beta') \cong \mathrm{SL}_2(\mathbb{F}_3) \times (\mathbb{Z}/2\mathbb{Z}),$$
$$\overline{\mathcal{Q}_B}^\times/\overline{\mathcal{Q}_B}^1(\epsilon) \cong A_4 \times (\mathbb{Z}/2\mathbb{Z}).$$

Proof. The element $1+\epsilon\alpha$, which has order 2, is not in $\overline{\mathcal{Q}_B}^1$ because it has norm $1+\epsilon$. To prove the first isomorphism, it suffices to note that $1+\epsilon\alpha$ commutes with the generators α, $\beta = 1+\epsilon+\alpha+\beta'$ of $\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon\beta')$, because

$$(1+\epsilon\alpha)(1+\alpha+\epsilon+\beta')(1+\epsilon\alpha)^{-1} = 1+\alpha+\epsilon+\beta'+\epsilon\beta' \equiv 1+\alpha+\epsilon+\beta'.$$

The second isomorphism follows by taking the first one modulo $\overline{\mathcal{Q}_B}^1(\epsilon)$, giving the quotient $\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon)$, which is isomorphic to A_4 by Proposition 12.8. □

Remark 12.10. The group $\overline{\mathcal{Q}_B}^\times(\epsilon)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$.

Proof. By definition, $\overline{\mathcal{Q}_B}^\times(\epsilon) = 1+\mathbb{F}_2[\alpha]\epsilon+\mathbb{F}_2[\alpha]\beta'\epsilon$ has order 16. But for every $f \in \overline{\mathcal{Q}_B}$, $(1+f\epsilon)^2 = 1+2f\epsilon+f^2\epsilon^2 = 1$. This shows that the group has exponent 2, so it is abelian. □

13. The Bolza group as a congruence subgroup

Our goal is to compare the Fuchsian group B, corresponding to the Bolza surface, to congruence subgroups of $\mathcal{Q}_B^1$ modulo $\{\pm 1\}$. To simplify notation, we write

$$\mathbb{P}\mathcal{Q}_B^1 = \mathcal{Q}_B^1/\{\pm 1\}$$

and

$$\mathbb{P}\mathcal{Q}_B^1(I) = \left\langle -1, \mathcal{Q}_B^1(I)\right\rangle/\{\pm 1\} \tag{13.1}$$

for any ideal $I \lhd \mathbb{Z}[\sqrt{2}]$.

By Lemma 10.2, the group $B \subseteq \mathbb{P}\mathcal{Q}_B^1$ is generated, as a normal subgroup, by the element $\delta = (\alpha\beta)^2(\alpha^2\beta^2)^2 = 1+\sqrt{2}(1+(1+\sqrt{2})(\alpha-\beta))$.

Proposition 13.1. *The map $\mathcal{Q}_B^1/\mathcal{Q}_B^1(\sqrt{2}) \to \overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon)$, induced by the projection $\mathcal{Q}_B \to \overline{\mathcal{Q}_B}$, is an isomorphism.*

Proof. The projection modulo $\sqrt{2}$ provides an injection

$$\mathcal{Q}_B^1/\mathcal{Q}_B^1(\sqrt{2}) \to \overline{\mathcal{Q}_B}^\times/\overline{\mathcal{Q}_B}^1(\epsilon),$$

which a priori need not be onto $\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon)$, even taking into account that every element of $(\mathcal{Q}_B/2\mathcal{Q}_B)^\times$ has norm 1. But in Proposition 12.8 we observed that the images of $\alpha, \beta \in \mathcal{Q}_B^1$ generate $\overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon)$. □

Theorem 13.2. *The Bolza group B satisfies $\mathbb{P}\mathcal{Q}_B^1(2) \subset B \subset \mathbb{P}\mathcal{Q}_B^1(\sqrt{2})$, and*

$$\mathbb{P}\mathcal{Q}_B^1/B \cong \overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon\beta').$$

Proof. Noting that $-1 \in \mathcal{Q}_B^1(2)$, we investigate the chain of groups

$$\mathbb{P}\mathcal{Q}_B^1(2) \subseteq B\mathbb{P}\mathcal{Q}_B^1(2) \subseteq \mathbb{P}\mathcal{Q}_B^1(\sqrt{2}) \subseteq \mathbb{P}\mathcal{Q}_B^1.$$

Let $\phi : \mathcal{Q}_B^1 \to \overline{\mathcal{Q}_B}^1$ be the map induced by the projection $\mathcal{Q}_B \to \overline{\mathcal{Q}_B} = \mathcal{Q}_B/2\mathcal{Q}_B$. This homomorphism, whose kernel is $\mathcal{Q}_B^1(2)$, is well defined on $\mathbb{P}\mathcal{Q}_B^1 = \mathcal{Q}_B^1/\{\pm 1\}$, since $-1 \in \mathcal{Q}_B^1(2)$. Furthermore, ϕ carries $\mathbb{P}\mathcal{Q}_B^1$ onto $\overline{\mathcal{Q}_B}^1$, and the subgroup $\mathbb{P}\mathcal{Q}_B^1(\sqrt{2})$ onto $\overline{\mathcal{Q}_B}^1(\epsilon)$, by Proposition 13.1.

At the same time, because $\phi(\delta) = 1 + \epsilon\beta' \in \overline{\mathcal{Q}_B}^1(\epsilon\beta')$, the normal subgroup it generates is mapped into $\overline{\mathcal{Q}_B}^1(\epsilon\beta')$. This proves that

$$[\mathbb{P}\mathcal{Q}_B^1 : B \cdot \mathbb{P}\mathcal{Q}_B^1(2)] = [\overline{\mathcal{Q}_B}^1 : \overline{\mathcal{Q}_B}^1(\epsilon\beta')] = 24.$$

But since $\mathbb{P}\mathcal{Q}_B^1$ is isomorphic to $\Delta_{(3,3,4)}$, we have by Proposition 10.3 that

$$[\mathbb{P}\mathcal{Q}_B^1 : B] = 24$$

as well. This proves that $B = B\mathbb{P}\mathcal{Q}_B^1(2)$, so that $\mathbb{P}\mathcal{Q}_B^1(2) \subseteq B$. It follows that the injection of $\mathcal{Q}_B^1/\mathcal{Q}_B^1(2)$ into $\overline{\mathcal{Q}_B}^1$ sends δ to $1 + \epsilon\beta'$, and the normal subgroup B generated by the former, to the normal subgroup $\overline{\mathcal{Q}_B}^1(\epsilon\beta')$ generated by the latter. □

Let $\mathrm{Sym}_{(3,3,4)}(B)$ denote the quotient $\mathbb{P}\mathcal{Q}_B^1/B$, which is the group of orientation preserving symmetries of the Bolza surface stemming from the $(3, 3, 4)$ tiling.

Corollary 13.3. *The symmetry group $\mathrm{Sym}_{(3,3,4)}(B)$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$.*

Proof. Indeed, the automorphism group $\mathbb{P}\mathcal{Q}_B^1/B \cong \overline{\mathcal{Q}_B}^1/\overline{\mathcal{Q}_B}^1(\epsilon\beta')$ was computed in Proposition 12.8.(12.2). □

Let us add this result to the observations made in Section 3, where we embedded

$$\Delta_{(3,3,4)} = \big\langle \alpha, \beta \,|\, \alpha^3 = \beta^3 = (\alpha\beta)^4 = 1 \big\rangle$$

as a subgroup of index 2 in

$$\Delta_{(2,3,8)} = \big\langle x, y \,|\, x^2 = y^3 = (xy)^8 = 1 \big\rangle$$

via the map $\alpha \mapsto y$ and $\beta \mapsto xyx$. Since $B \subseteq \Delta_{(3,3,4)}$ is the normal subgroup generated by $(\alpha\beta)^2(\alpha^2\beta^2)^{-2}$ by Lemma 10.2, its image in $\Delta_{(2,3,8)}$ is $\langle (yx)^4(y^{-1}x)^4 \rangle^{\langle y, xyx \rangle}$, which happens to be normal in $\Delta_{(2,3,8)}$, and the quotient group is

$$\big\langle x, y \,|\, x^2 = y^3 = (xy)^8 = (yx)^4(y^{-1}x)^4 = 1 \big\rangle.$$

This quotient is isomorphic to $\mathrm{GL}_2(\mathbb{F}_3)$ by taking $x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $y \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Corollary 13.4. *The symmetry group* $\mathrm{Sym}_{(2,3,8)}(B) = \Delta_{(2,3,8)}/B$ *is isomorphic to* $\mathrm{GL}_2(\mathbb{F}_3)$*.*

We can also compute the quotient of B modulo the principal congruence subgroup it contains:

Remark 13.5. We have that $B/\mathbb{P}\mathcal{Q}_B^1(2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Indeed, $\overline{\mathcal{Q}_B}^1(\epsilon\beta')$ has order 4, and as a subgroup of $\overline{\mathcal{Q}_B}^\times(\epsilon)$, which is of exponent 2 by Proposition 12.10, we obtain

$$B/\mathbb{P}\mathcal{Q}_B^1(2) \cong \overline{\mathcal{Q}_B}^1(\epsilon\beta') \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

as claimed. □

Corollary 13.6. $\mathbb{P}\mathcal{Q}_B^1(\sqrt{2})$ *is generated by* B *and the torsion element* ϖ *of* (11.1)*.*

Proof. As we have seen before, B is torsion free, so $\varpi \notin B$, and $\langle B, \varpi \rangle$ strictly contains B, so the result follows from $[\mathcal{Q}_B^1(\sqrt{2}) : \mathcal{Q}_B^1(2)] = 8$. □

14. Computations in the Bolza twins

In this section and the ones that follow, we will present some explicit computations with the "twin" surfaces corresponding to the algebraic primes factoring rational primes in $K = \mathbb{Q}(\sqrt{2})$. Recall that $O_K = \mathbb{Z}[\sqrt{2}]$. We first state a result on quotients co-prime to 6, which follows from the definition of ramification (and splitting) in a quaternion algebra.

Lemma 14.1. *Let $I \lhd O_K$ be a prime ideal. If 2 and 3 are invertible modulo I, then $\mathcal{Q}_B/I\mathcal{Q}_B \cong \mathrm{M}_2(O_K/I)$.*

Proof. It is convenient to make the substitution

$$\alpha = \alpha' + \frac{1}{2}, \quad \beta = \beta' + \frac{1+2\sqrt{2}}{3}\alpha' + \frac{1}{2}.$$

Then α' and β' anticommute, and we obtain a standard presentation

$$\mathcal{Q}_B/I\mathcal{Q}_B = (O_K/I)\left[\alpha', \beta' \,\middle|\, \alpha'^2 = -\tfrac{3}{4},\ \beta'^2 = \tfrac{\sqrt{2}}{3},\ \beta'\alpha' = -\alpha'\beta'\right].$$

Since α'^2 and β'^2 are invertible, the quotient $\mathcal{Q}_B/I\mathcal{Q}_B$ is a quaternion algebra over O_K/I. But as a finite integral domain, O_K/I is a field, so by Wedderburn's little theorem (that the only finite division algebras are fields), $\mathcal{Q}_B/I\mathcal{Q}_B$ is necessarily isomorphic to $\mathrm{M}_2(O_K/I)$. □

Corollary 14.2. *Let $I \lhd O_K$ be a prime ideal such that 6 is invertible modulo I. Then*

$$\mathbb{P}\mathcal{Q}_B^1/\mathbb{P}\mathcal{Q}_B^1(I) \cong \mathrm{PSL}_2(O_K/I).$$

Proof. By Lemma 14.1 and strong approximation we have $\mathcal{Q}_B^1/\mathcal{Q}_B^1(I) \cong \mathrm{SL}_2(O_K/I)$. □

Lemma 14.3. *Let p be a rational prime that splits in K, so that $pO_K = I_1 I_2$ for distinct prime ideals $I_1, I_2 \lhd O_K$. There are exactly two normal subgroups $H \lhd \mathbb{P}\mathcal{Q}_B^1$ such that $\mathbb{P}\mathcal{Q}_B^1/H \cong \mathrm{PSL}_2(\mathbb{F}_p)$, namely $\mathbb{P}\mathcal{Q}_B^1(I_1)$ and $\mathbb{P}\mathcal{Q}_B^1(I_2)$.*

Proof. Recall that the rational primes p splitting in K are precisely those satisfying $p \equiv \pm 1 \bmod 8$. Let $H \lhd \mathbb{P}\mathcal{Q}_B^1$ be a normal subgroup such that $\mathbb{P}\mathcal{Q}_B^1/H \cong \mathrm{PSL}_2(\mathbb{F}_p)$ and choose a surjection $\varphi : \mathbb{P}\mathcal{Q}_B^1 \to \mathrm{PSL}_2(\mathbb{F}_p)$ such that $\ker(\varphi) = H$. Clearly φ is determined by the triple $(\varphi(\alpha), \varphi(\beta), \varphi(\alpha\beta)^{-1}) \in (\mathrm{PSL}_2(\mathbb{F}_p))^3$, where we use α, β to denote the images of these elements in $\mathbb{P}\mathcal{Q}_B^1$. Note that $\varphi(\alpha)$ must have order 3; otherwise it would be trivial and $\varphi(\mathbb{P}\mathcal{Q}_B^1)$ would be abelian, contradicting surjectivity. Similarly, $\varphi(\beta)$ has order 3. Since $\alpha\beta$ has order 4 in $\mathbb{P}\mathcal{Q}_B^1$, the order of $\varphi(\alpha\beta)$ must divide 4. If $\varphi(\alpha\beta)$ is trivial, then again we get that $\varphi(\mathbb{P}\mathcal{Q}_B^1)$ is abelian. If $\varphi(\alpha\beta)^2$ is trivial, then it is easy to show that $\langle \varphi(\alpha\beta), \varphi(\beta\alpha) \rangle \subseteq \mathrm{PSL}_2(\mathbb{F}_p)$ is a normal subgroup and hence all of $\mathrm{PSL}_2(\mathbb{F}_p)$ since the latter is a simple group. However, this is again absurd because a finite group generated by two involutions must be dihedral. Thus the order of $\varphi(\alpha\beta)$ is 4.

We have thus shown that $(\varphi(\alpha), \varphi(\beta), \varphi(\alpha\beta)^{-1})$ is a non-exceptional group triple in the sense of [9, Section 8]. Moreover, since none of these three elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ can be a scalar matrix, it follows that if $(g_1, g_2, g_3) \in (\mathrm{PSL}_2(\mathbb{F}_p))^3$ is any triple such that $g_1g_2g_3 = 1$ and $(\mathrm{tr}(g_1), \mathrm{tr}(g_2), \mathrm{tr}(g_3)) = (\mathrm{tr}\varphi(\alpha), \mathrm{tr}\varphi(\beta), \mathrm{tr}\varphi(\beta^{-1}\alpha^{-1}))$, then the orders of g_1, g_2, g_3 are $3, 3, 4$, respectively. In particular, the subgroup $\langle g_1, g_2, g_3\rangle$ is never abelian. Hence the trace triple

$$(\mathrm{tr}\varphi(\alpha), \mathrm{tr}\varphi(\beta), \mathrm{tr}\varphi(\beta^{-1}\alpha^{-1}))$$

is not commutative, and so it must be projective by [17, Theorem 4]. Since $p \notin \{2, 3\}$, all the hypotheses of [9, Proposition 8.10] hold. By that proposition, there are at most two normal subgroups H such that $\mathbb{P}\mathcal{Q}^1_B/H \cong \mathrm{PSL}_2(\mathbb{F}_p)$. On the other hand, $\mathbb{P}\mathcal{Q}^1_B(I_1)$ and $\mathbb{P}\mathcal{Q}^1_B(I_2)$ are clearly distinct and satisfy this condition by Corollary 14.2. We are grateful to J. Voight for directing us to the reference [9]. □

Remark 14.4. For every p splitting in K, we obtain a pair of Bolza twin surfaces M of genus $g(M) = \frac{p(p^2-1)}{48} + 1$, i.e., Euler characteristic $\chi(M) = -\frac{p(p^2-1)}{24}$, and area $\frac{\pi p(p^2-1)}{12}$. Since the area of the (3,3,4) triangle is $\frac{\pi}{12}$ and its double is $\frac{\pi}{6}$, the automorphism group generated by orientation-preserving elements of the triangle group has order $\frac{p(p^2-1)}{2}$, namely that of $\mathrm{PSL}_2(\mathbb{F}_p)$.

15. Bolza twins of genus 8

We now apply the results of Section 14 to the pair $(1+2\sqrt{2})O_K$ and $(1-2\sqrt{2})O_K$. Both of these have norm 7, and therefore their principal congruence quotients are isomorphic to the group $\mathrm{PSL}_2(\mathbb{F}_7)$ of order 168. These ideals give rise to twin surfaces analogous to the Hurwitz triplets (see [14]), namely non-isometric surfaces with the same automorphism group. Note that by estimate (9.2), these Fuchsian groups contain no elliptic elements.

The normal subgroup of the triangle group generated by each of these in `magma` produces a presentation with 16 generators and a single relation of length 32, corresponding to Fuchsian groups of a Riemann surface of genus 8. Therefore it coincides with the corresponding congruence subgroup, since it gives the correct order of the symmetry group (i.e., index in the (3,3,4) triangle group), namely order 168.

To find these groups, we searched for subgroups of index 168 using `magma`, and looked for the simplest generator whose normal closure is the entire group. The results are summarized in Lemmas 15.1 and 15.3 below.

The numerical values reproduced below suggest that the systole of the surface corresponding to the ideal $(1+2\sqrt{2})O_K$ should be smaller than the systole of the surface corresponding to the ideal $(1-2\sqrt{2})O_K$.

Lemma 15.1. *The element $-(\alpha\beta^{-1})^4$ is in $\mathcal{Q}_B^1(1+2\sqrt{2})$. Its normal closure is the full congruence subgroup corresponding to the ideal generated by $1+2\sqrt{2}$.*

Proof. With respect to the module basis we have

$$(\alpha\beta^{-1})^4 = (5+3\sqrt{2})(\alpha-\alpha\beta)-(2+2\sqrt{2}),$$

which is congruent to -1 modulo the ideal $(1+2\sqrt{2})$. On the other hand,

$$\langle \alpha,\beta \mid \alpha^3=\beta^3=(\alpha\beta)^4=(\alpha\beta^{-1})^4=1\rangle$$

has order 168, showing that the normal closure of $(\alpha\beta^{-1})^4$ is the full congruence subgroup. □

Remark 15.2. The element $(\alpha\beta^{-1})^4$ has trace $7+4\sqrt{2}=12.656\ldots$ Of the 16 generators produced by `magma`, 14 have this trace (up to sign), and the remaining two generators have trace $19+13\sqrt{2}=37.384\ldots$ (up to sign). The smaller value $7+4\sqrt{2}=12.656\ldots$ is a good candidate for the least trace of a nontrivial element for this Fuchsian group.

Lemma 15.3. *The element $-(\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha)^2$ is in $\mathcal{Q}_B^1(1-2\sqrt{2})$. Its normal closure is the full congruence subgroup corresponding to the ideal generated by $1-2\sqrt{2}$.*

Proof. A calculation shows that

$$(\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha)^2 = (7+5\sqrt{2})+(5+4\sqrt{2})\alpha-(8+5\sqrt{2})\beta+(3+\sqrt{2})\alpha\beta.$$

Adding 1, the coefficients $8+5\sqrt{2}$, $5+4\sqrt{2}$ and $3+\sqrt{2}$ are divisible by $1-2\sqrt{2}$, so $(\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha)^2$ is congruent to -1 modulo $1-2\sqrt{2}$ in the Bolza order. Again, the normal closure is the full congruence subgroup because the group

$$\langle \alpha,\beta \mid \alpha^3=\beta^3=(\alpha\beta)^4=(\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha)^2=1\rangle$$

has order 168 as well. □

Remark 15.4. The trace of $(\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha)^2$ is $9+6\sqrt{2}=17.485\ldots$ Of the 16 generators of the Fuchsian group produced by `magma`, 13 have this trace (up to sign), and the remaining three have trace $14+11\sqrt{2}=29.556\ldots$ The smaller value $9+6\sqrt{2}=17.485\ldots$ is a good candidate for the least trace of a nontrivial element for this Fuchsian group.

The traces in Remarks 15.2 and 15.4 can be compared to the trace bound of [13, Theorem 2.3], cf. (9.2), which, since $\mathcal{Q}_B\subseteq\frac{1}{6}O_K[i,j]$, gives for any ideal $I\lhd\mathbb{Z}[\sqrt{2}]$ and any $\pm1\neq x\in\mathcal{Q}_B^1(I)$ that $|\mathrm{Tr}_D(x)|>\frac{1}{4}\mathrm{N}(I)^2-2$. In particular since $\mathrm{N}(1+2\sqrt{2})=\mathrm{N}(1-2\sqrt{2})=7$, we have for both congruence subgroups mentioned in this section the trace lower bound $\frac{41}{4} = 10.25$. Note that the trace appearing in Remark 15.2 exceeds the theoretical bound by less than 25%.

Remark 15.5. It would be interesting to explore possible algorithms for the computation of the systole of an explicitly given Fuchsian group, possibly exploiting its fundamental domain using Voight [28].

16. Bolza twins of higher genus

In this section we collect explicit computations, performed in `magma`, of Bolza twins for some primes $p > 7$ that split in $K = \mathbb{Q}(\sqrt{2})$. We briefly sketch the method. Let I_1 and I_2 be the two places of K dividing p. We first obtain presentations of the congruence subgroups $\mathbb{P}\mathcal{Q}_B^1(I_1)$ and $\mathbb{P}\mathcal{Q}_B^1(I_2)$. By Lemma 14.3, these are the only two normal subgroups of $\mathbb{P}\mathcal{Q}_B^1$ such that the corresponding quotients are isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p)$.

The most efficient way to find such subgroups in practice is randomly to generate a homomorphism from the triangle group onto $\mathrm{PSL}_2(\mathbb{F}_p)$. Thus, we generate pairs (A_1, A_2) of random elements of $\mathrm{SL}_2(\mathbb{F}_p)$ by means of the Product Replacement Algorithm and search for pairs that generate $\mathrm{SL}_2(\mathbb{F}_p)$ and such that the projective orders of A_1, A_2, A_1A_2 are $3, 3, 4$, respectively. Each such pair corresponds to a surjection $\varphi : \mathbb{P}\mathcal{Q}_B^1 \to \mathrm{PSL}_2(\mathbb{F}_p)$ determined by $\varphi(\alpha) = \overline{A_1}$ and $\varphi(\beta) = \overline{A_2}$; here the bars denote images in $\mathrm{PSL}_2(\mathbb{F}_p)$. We search for two pairs such that the kernels of the corresponding surjections are distinct; by Lemma 14.3, these kernels are our two congruence subgroups.

This random search is far faster than any known deterministic algorithm. Finding suitable pairs (A_1, A_2) is very quick: for $p = 71$, for instance, a search through one million random pairs produced twenty suitable ones and took only a few seconds.

We then rewrite the presentations of these kernels by means of the Reidemeister-Schreier algorithm, as implemented in `magma`; this is time-consuming, taking a few hours to run on a MacBook for $p = 71$. It may be necessary to treat more than two surjections φ before two different kernels are found.

In all cases that we have investigated, the Reidemeister-Schreier algortihm produces presentations with $2g_p$ generators and a single relation of length $4g_p$; here $g_p = p(p^2 - 1)/48 + 1$. We search through this list for elements of minimal trace and for generators whose normal closure in $\mathbb{P}\mathcal{Q}_B^1$ is the full congruence subgroup and present our results below. In some cases, none of the elements of minimal trace normally generate the entire congruence subgroup, and for one of the primes dividing 71 we were unable to find any single element that normally generates the associated congruence subgroup.

16.1. **Bolza twins of genus** 103**.** Factoring the rational prime $p = 17$ as $-(1-3\sqrt{2})(1+3\sqrt{2})$, we obtain a pair of Bolza twins of genus 103, with automorphism group $\mathrm{PSL}_2(\mathbb{F}_{17})$. The order of $\mathrm{PSL}_2(\mathbb{F}_p)$ is $(p^2-1)p/2$. This is 2448 for $p = 17$. The element

$$\alpha\beta\alpha^{-1}\beta^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta^{-1}\alpha^{-1}\beta\alpha\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha\beta$$

is congruent to 1 modulo $(1-3\sqrt{2})$ and normally generates the corresponding congruence subgroup. Its trace is $75+53\sqrt{2} \approx 149.953\ldots$, which is the least trace (in absolute value) among the 206 generators (with a single relation of length 412). For the "twin" normal subgroup, we find a generator of the form

$$(\alpha\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta^{-1}\alpha\beta)^2,$$

equal to -1 mod $(1+3\sqrt{2})$. It generates the full congruence subgroup, and gives the least trace, namely $79+56\sqrt{2} \approx 158.195\ldots$, among all the generators.

16.2. **Bolza twins of genus** 254**.** For $p = 23$, there are two normal subgroups of the triangle group whose quotient is $\mathrm{PSL}_2(\mathbb{F}_{23})$. The order of $\mathrm{PSL}_2(\mathbb{F}_p)$ is $(p^2-1)p/2$. This is 6072 for $p = 23$. One obtains a generator

$$\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha$$

with minimal trace of $91+65\sqrt{2}$, whose normal closure is a group with 508 generators and a single relation of length 1016. This generator is congruent to $+1$ modulo $5-\sqrt{2}$.

For its Bolza twin, the lowest trace appears to be $119+84\sqrt{2}$. An element that normally generates the congruence subgroup of $5+\sqrt{2}$ is

$$\alpha\beta\alpha\beta^{-1}\alpha\beta^{-1}\alpha\beta^{-1}\alpha\beta\alpha^2\beta^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\alpha\beta^{-1}\alpha\beta^{-1}$$

This generator is congruent to -1 modulo $5+\sqrt{2}$.

By Lemma 14.3, for each prime p satisfying $p \equiv \pm 1 \pmod 8$, there are precisely two normal subgroups of our triangle group with quotient isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p)$, which are congruence subgroups corresponding to the two algebraic primes factoring p.

16.3. **Bolza twins of genus 621.** Consider the decomposition $31 = (9-5\sqrt{2})(9+5\sqrt{2})$. The generator

$$\beta\alpha\beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha\beta^{-1}\alpha\beta\alpha^{-1}\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha\beta^{-1}\alpha^{-1}$$

is equivalent to 1 modulo $9-5\sqrt{2}$ and normally generates the corresponding principal congruence subgroup, producing a surface of genus $g = 621 = 31(31^2-1)/48+1$. This element has trace $153+109\sqrt{2}$, which is the smallest among the $2g$ generators.

For the Bolza twin, the element

$$(\beta^{-1}\alpha\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta\alpha)^2$$

equals -1 mod $(9+5\sqrt{2})$, with normal closure with the same properties, the least trace being $129+90\sqrt{2}$.

16.4. **Bolza twins of genus 1436.** Let $41 = (7-2\sqrt{2})(7+2\sqrt{2})$. For both $\mathbb{P}\mathcal{Q}^1_B(7-2\sqrt{2})$ and $\mathbb{P}\mathcal{Q}^1_B(7+2\sqrt{2})$, `magma` found presentations with $2g$ generators and a single relation of length $4g$, where $g = 1436 = 41(41^2-1)/48+1$. The generator

$$\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta\alpha\beta^{-1}\alpha\beta\alpha^{-1}$$

is congruent to -1 mod $(7-2\sqrt{2})$ and has trace $208\sqrt{2}+295$. Its normal closure is the full congruence subgroup $\mathbb{P}\mathcal{Q}^1_B(7-2\sqrt{2})$.

The pair of generators

$$(\beta^{-1}\alpha)^{10}$$

and

$$\beta\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta\alpha^{-1}$$

are congruent to -1 and 1 mod $(7+2\sqrt{2})$, respectively, and they have traces $281+198\sqrt{2}$ and $-(281+198\sqrt{2})$, respectively. The normal closure of this pair is the congruence subgroup $\mathbb{P}\mathcal{Q}^1_B(7+2\sqrt{2})$. While $281+198\sqrt{2}$ is the minimal trace among the $2g = 2872$ generators of $\mathbb{P}\mathcal{Q}^1_B(7+2\sqrt{2})$ found by `magma`, no single generator of this trace normally generates $\mathbb{P}\mathcal{Q}^1_B(7+2\sqrt{2})$. It is, however, normally generated by the element

$$\beta\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1},$$

which is congruent to 1 mod $(7+2\sqrt{2})$ and has trace $681+481\sqrt{2}$.

16.5. **Bolza twins of genus 2163.** Let $p = 47 = (7-\sqrt{2})(7+\sqrt{2})$. The generator

$$(\beta^{-1}\alpha\beta\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha)^2$$

has trace $529+374\sqrt{2}$ and equals $-1 \bmod (7-\sqrt{2})$, while the generator

$$\beta\alpha\beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}$$

has trace $499 + 353\sqrt{2}$ and equals $1 \bmod (7+\sqrt{2})$. In both cases, normal closures are subgroups with $2g$ generators and a single relation of length $4g$, for $g = 2163$.

16.6. **Bolza twins of genus 7456.** Consider $p = 71 = (11+5\sqrt{2})(11-5\sqrt{2})$. The two elements

$$\beta\alpha\beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}$$

and

$$\beta\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1}$$

are each congruent to 1 modulo $(11+5\sqrt{2})$, and they each have trace $-(951 + 672\sqrt{2})$. The normal closure of this pair of elements is the corresponding congruence subgroup $\mathbb{P}\mathcal{Q}^1_B(11+5\sqrt{2})$. This congruence subgroup can also be generated by a single element; however, the minimal trace that we have found of such a generator is $2299 + 1625\sqrt{2}$, for instance for the generator

$$\beta\alpha\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}.$$

The congruence subgroup has a presentation with $2g$ generators and a single relation of length $4g$, for the expected $g = 7456 = 47(47^2 - 1)/48 + 1$.

For its Bolza twin, we were unable to find any element whose normal closure is the entire congruence subgroup $\mathbb{P}\mathcal{Q}^1_B(11-5\sqrt{2})$. This congruence subgroup again has a presentation with $2g$ generators and a single relation of length $4g$; however, the normal closure of each of these generators have index at least 3 in $\mathbb{P}\mathcal{Q}^1_B(11-5\sqrt{2})$. The smallest trace among the $2g = 14912$ generators is $\pm(633 + 449\sqrt{2})$, which is obtained for eighteen of them. We note that `magma` was unable the determine the index in $\mathbb{P}\mathcal{Q}^1_B(11-5\sqrt{2})$ of the normal closure of all eighteen of these generators; this index is likely to be very large or infinite. However, the congruence subgroup can be normally generated by the two elements

$$\beta\alpha\beta\alpha^{-1}\beta\alpha\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta\alpha\beta\alpha^{-1}\beta\alpha^{-1}$$

and

$\beta\alpha\beta\alpha^{-1}\beta\alpha^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha\beta^{-1}\alpha^{-1}\beta^{-1}\alpha\beta\alpha^{-1}\beta^{-1}\alpha\beta\alpha\beta^{-1}\alpha\beta\alpha^{-1}\beta\alpha^{-1}$,

which are congruent to 1 modulo $(11 - 5\sqrt{2})$ and have traces $633 + 449\sqrt{2}$ and the next smallest $-(1527 + 1080\sqrt{2})$, respectively.

16.7. **Summary of results.** To summarize, we collect some of the results presented above in a table. Each line of the table corresponds to a prime ideal $I \lhd O_K = \mathbb{Z}[\sqrt{2}]$ dividing a rational prime p that splits in $K = \mathbb{Q}(\sqrt{2})$. We present the lowest trace discovered by our `magma` computations of a non-trivial element in the congruence subgroup $\mathbb{P}\mathcal{Q}^1_B(I)$, as well as the decimal expansion of this candidate for the lowest trace, rounded to the nearest thousandth. For comparison, the rightmost column displays the theoretical lower bound $N(I)^2/4 - 2$ for the trace.

For some ideals, such as $I = (11 - 5\sqrt{2})$, we find elements whose traces are remarkably close to the theoretical bound. For other ideals, our experimental results are not as close to the theoretical bound; we ask whether elements of lower trace exist that could be discovered by other methods.

I	$N(I)$	lowest trace		$N(I)^2/4 - 2$
$(1 + 2\sqrt{2})$	7	$7 + 4\sqrt{2}$	12.657	10.25
$(1 - 2\sqrt{2})$	7	$9 + 6\sqrt{2}$	17.485	10.25
$(1 - 3\sqrt{2})$	17	$75 + 53\sqrt{2}$	149.953	70.25
$(1 + 3\sqrt{2})$	17	$79 + 56\sqrt{2}$	158.196	70.25
$(5 - \sqrt{2})$	23	$91 + 65\sqrt{2}$	182.924	130.25
$(5 + \sqrt{2})$	23	$119 + 84\sqrt{2}$	237.794	130.25
$(9 + 5\sqrt{2})$	31	$129 + 90\sqrt{2}$	256.279	238.25
$(9 - 5\sqrt{2})$	31	$153 + 109\sqrt{2}$	307.149	238.25
$(7 + 2\sqrt{2})$	41	$281 + 198\sqrt{2}$	561.014	418.25
$(7 - 2\sqrt{2})$	41	$295 + 208\sqrt{2}$	589.156	418.25
$(7 + \sqrt{2})$	47	$499 + 353\sqrt{2}$	998.217	550.25
$(7 - \sqrt{2})$	47	$529 + 374\sqrt{2}$	1057.916	550.25
$(11 - 5\sqrt{2})$	71	$633 + 449\sqrt{2}$	1267.982	1258.25
$(11 + 5\sqrt{2})$	71	$951 + 672\sqrt{2}$	1901.352	1258.25

Acknowledgments

We are grateful to M. Belolipetsky and J. Voight for helpful comments. M. Katz is partially supported by ISF grant 1517/12. M. M. Schein is partially supported by GIF grant 1246/2014. U. Vishne is partially supported by a BSF grant 206940 and an ISF grant 1207/12.

References

[1] Akrout, H.; Muetzel, B. "Construction of hyperbolic Riemann surfaces with large systoles." See http://arxiv.org/abs/1305.5510

[2] Akrout, H.; Muetzel, B. "Construction of surfaces with large systolic ratio." See http://arxiv.org/abs/1311.1449

[3] Babenko, I.; Balacheff, F. "Systolic volume of homology classes." *Algebr. Geom. Topol.* **15** (2015), no. 2, 733–767.

[4] Balacheff, F.; Makover, E.; Parlier, H. "Systole growth for finite area hyperbolic surfaces." *Ann. Fac. Sci. Toulouse Math. (6)* **23** (2014), no. 1, 175--180.

[5] Bavard, C. "La systole des surfaces hyperelliptiques." *Prepubl. Ec. Norm. Sup. Lyon* **71** (1992).

[6] Bujalance, E.; Singerman, D. "The symmetry type of a Riemann surface." *Proc. London Math. Soc. (3)* **51** (1985), no. 3, 501–519.

[7] Bulteau, G. "Systolic geometry and regularization technique." See http://arxiv.org/abs/1506.07848

[8] Buser, P.; Sarnak, P. "On the period matrix of a Riemann surface of large genus." With an appendix by J. H. Conway N. J. A. Sloane. *Invent. Math.* **117** (1994), no. 1, 27-56.

[9] Clark, P.; Voight, J. "Algebraic curves uniformized by congruence subgroups of triangle groups." Preprint, 2015; see `http://arxiv.org/abs/1506.01371`.

[10] Katok, S. *Fuchsian groups.* Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992.

[11] Katz, M.; Sabourau, S. "An optimal systolic inequality for CAT(0) metrics in genus two." *Pacific J. Math.* **227** (2006), no. 1, 95--107.

[12] Katz, M.; Sabourau, S. "Dyck's surfaces, systoles, and capacities." *Trans. Amer. Math. Soc.* **367** (2015), no. 6, 4483–4504.

[13] Katz, M.; Schaps, M.; Vishne, U. "Logarithmic growth of systole of arithmetic Riemann surfaces along congruence subgroups." *J. Differential Geom.* **76** (2007), no. 3, 399–422.

[14] Katz, M.; Schaps, M.; Vishne, U. "Hurwitz quaternion order and arithmetic Riemann surfaces." *Geometriae Dedicata* **155** (2011), no. 1, 151-161. See `http://dx.doi.org/10.1007/s10711-011-9582-3` and `http://arxiv.org/abs/math/0701137`

[15] Kowalick R; Lafont, J.-F.; Minemyer, B. Combinatorial systolic inequalities. See http://arxiv.org/abs/1506.07121

[16] Linowitz, B.; Meyer, J. "Systolic Surfaces of Arithmetic Hyperbolic 3-Manifolds." See http://arxiv.org/abs/1506.08341

[17] Macbeath, A. "Generators of the linear fractional groups." Number Theory (Proc. Sympos. Pure Math., Vol. XII), Amer. Math. Soc., Providence, 14-32.

[18] Macbeath, A. "Automorphisms of Riemann Surfaces." *Contemp. Math.* **109** (1990), 107–112.

[19] Maclachlan, C.; Reid, A. *The arithmetic of hyperbolic 3-manifolds.* Springer, 2003.

[20] Makisumi S. "A note on Riemann surfaces of large systole." *J. Ramanujan Math. Soc.* **28** (2013), no. 3, 359–377. See `http://arxiv.org/abs/1206.2965`.

[21] Marcus, D.A. *Number fields.* Springer-Verlag, New York Heidelberg Berlin, 1977.

[22] Reiner, I. *Maximal orders.* Academic Press, 1975.
[23] Schmutz, P. "Riemann surfaces with shortest geodesic of maximal length." *Geom. Funct. Anal.* **3** (1993), no. 6, 564–631.
[24] Schmutz Schaller, P. "Geometry of Riemann surfaces based on closed geodesics." *Bull. Amer. Math. Soc. (N.S.)* **35** (1998), no. 3, 193–214.
[25] Takeuchi, K. "Commensurability classes of arithmetic triangle groups." *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **24** (1977), no. 1, 201–212.
[26] Vignéras, M.-F. *Arithmétique des algèbres de quaternions.* Lecture Notes in Mathematics, vol. 800. Springer, Berlin, 1980.
[27] Vinberg, E. "Discrete groups generated by reflections in Lobacevskii spaces." (Russian) *Mat. Sb. (N.S.)* **72** (114) (1967), 471-488; correction, ibid. **73** (115) (1967), 303.
[28] Voight, J. "Computing fundamental domains for Fuchsian groups." *J. Théor. Nombres Bordeaux* **21** (2009), no. 2, 469–491.

Department of Mathematics, Bar Ilan University