J. DIFFERENTIAL GEOMETRY
76 (2007) 399-422

LOGARITHMIC GROWTH OF SYSTOLE OF ARITHMETIC RIEMANN SURFACES ALONG CONGRUENCE SUBGROUPS

Mikhail G. Katz, Mary Schaps & Uzi Vishne

Abstract

We apply a study of orders in quaternion algebras, to the differential geometry of Riemann surfaces. The least length of a closed geodesic on a hyperbolic surface is called its systole, and denoted $\mathrm{sys}\pi_1$. P. Buser and P. Sarnak constructed Riemann surfaces X whose systole behaves logarithmically in the genus $g(X)$. The Fuchsian groups in their examples are principal congruence subgroups of a fixed arithmetic group with rational trace field. We generalize their construction to principal congruence subgroups of arbitrary arithmetic surfaces. The key tool is a new trace estimate valid for an arbitrary ideal in a quaternion algebra. We obtain a particularly sharp bound for a principal congruence tower of Hurwitz surfaces (PCH), namely the 4/3-bound $\mathrm{sys}\pi_1(X_{\mathrm{PCH}}) \geq \frac{4}{3}\log(g(X_{\mathrm{PCH}}))$. Similar results are obtained for the systole of hyperbolic 3-manifolds, relative to their simplicial volume.

1. Orders in quaternion algebras and Riemann surfaces

Arithmetic lattices, besides their own intrinsic interest, have traditionally provided a rich source of examples in geometry. One striking application is the construction of isospectral, non-isometric hyperbolic surfaces by M.-F. Vigneras [**Vig80**]. A survey of arithmeticity as applied in geometry and dynamics may be found in [**Pa95**]. See [**Lub94**] for an application of congruence subgroups and the literature on girth in graph theory initiated by W. Tutte [**Tu47**]. See also [**ChW06**] for a recent geometric application of congruence subgroups.

While the simplest definition of arithmeticity, in analogy with $\mathrm{SL}_2(\mathbb{Z})$, can be presented in terms of n-dimensional representations by matrices defined over the integers, for many purposes it is convenient to work with

The first author was supported by the Israel Science Foundation (grants no. 84/03 and 1294/06), the third author was supported by the EU research and training network HPRN-CT-2002-00287, ISF Center of Excellence grant 1405/05, and BSF grant no. 2004-083.
Received 09/02/2005.

a definition in terms of quaternion algebras. The latter is equivalent to the former; cf. Definition 1.3. We start by recalling the relevant material on quaternion algebras.

Let $a, b \in \overline{\mathbb{Q}}$, and let

$$D = \mathbb{Q}[i, j \mid i^2 = a,\ j^2 = b,\ ji = -ij] \tag{1.1}$$

be an (associative) division algebra. If a and b are positive integers, we have $D \otimes \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$, cf. [**K92**, Theorem 5.2.1(i)]. Consider the group Γ, by definition composed of the elements of norm one in $\mathbb{Z}[i, j] \subseteq D$. Then Γ is a co-compact lattice in $\mathrm{SL}_2(\mathbb{R})$, see [**PR94**, Theorem 5.5].

P. Buser and P. Sarnak [**BS94**, p. 44] showed that in such a case, the principal congruence subgroups of the Fuchsian group Γ exhibit near-optimal asymptotic behavior with regard to their systole. (A more general construction, but still over $\mathbb{Z}$, was briefly described by M. Gromov [**Gr96**, 3.C.6].) Namely, there is a constant c independent of m such that the compact hyperbolic Riemann surfaces defined as the quotients $X_m = \Gamma(m) \backslash \mathcal{H}^2$ satisfy the bound

$$\mathrm{sys}\pi_1(X_m) \geq \frac{4}{3} \log g(X_m) - c,$$

where $\mathcal{H}^2$ is the Poincaré upper half plane, $\Gamma(m)$ are the principal congruence subgroups of Γ, $g(X)$ denotes the genus of X, and the systole (or girth) $\mathrm{sys}\pi_1(X)$ is defined as follows.

Definition 1.1. The homotopy 1-systole, denoted $\mathrm{sys}\pi_1(\mathcal{G})$, of a Riemannian manifold $(X, \mathcal{G})$ is the least length of a noncontractible loop for the metric $\mathcal{G}$.

Remark 1.2. The calculation of [**BS94**] relies upon a lower bound for the (integer) trace resulting from a congruence relation modulo a rational prime p. Such a congruence argument does not go over directly to a case when the structure constants a, b of the quaternion algebra (1.1) are algebraic integers of a proper extension of $\mathbb{Q}$, since the latter are dense in $\mathbb{R}$. In particular, the results of [**BS94**] do not apply to Hurwitz surfaces. Thus a new type of trace estimate is needed, see Theorem 2.3 below.

Riemann surfaces with such logarithmic asymptotic behavior of the systole were exploited by M. Freedman in his construction of $(1, 2)$-systolic freedom, in the context of quantum computer error correction [**Fr99**]. For additional background on quaternion algebras and arithmetic Fuchsian groups, see [**GP69**, Appendix to chapter 1], [**K92**, Section 5.2] and [**MR03**]. See also the recent monograph [**Ka07**] for an overview of systolic problems, as well as [**CrK03**].

Definition 1.3. Let F denote one of the fields $\mathbb{R}$ or $\mathbb{C}$. An *arithmetic lattice* $G \subset \mathrm{SL}_2(F)$ is a finite co-volume discrete subgroup, which is commensurable with the group of elements of norm one in an order of a central quaternion division algebra D over a number field K (which has at least one dense embedding in F).

Remark 1.4. By a result of K. Takeuchi [**Ta75**], a lattice G is arithmetic if and only if the lattice $G^{(2)}$ (the subgroup generated by the squares in G) is contained in an order of a division algebra.

Such a lattice $\Gamma \subset D$ is cocompact if and only if the algebra D as in (1.1) splits in a single Archimedean place of the center K of D (real or complex depending on F), and remains a division algebra in all other Archimedean places.

In particular if $F = \mathbb{R}$ then K is totally real, and if $F = \mathbb{C}$ then K has one complex place and $[K:\mathbb{Q}]-2$ real ones. Denote by $O_K \subset K$ its ring of algebraic integers. Given an ideal $I \subset O_K$, consider the associated congruence subgroup $\Gamma(I) \subset \Gamma$ (see Definition 2.1 for more details).

In the Fuchsian case, we have the following theorem.

Theorem 1.5. *Let Γ be an arithmetic cocompact subgroup of $\mathrm{SL}_2(\mathbb{R})$. Then for a suitable constant $c = c(\Gamma)$, the principal congruence subgroups of Γ satisfy*

$$\mathrm{sys}\pi_1(X_I) \geq \frac{4}{3}\log g(X_I) - c,$$

for every ideal $I \lhd O_K$, where $X_I = \Gamma(I)\backslash\mathcal{H}^2$ is the associated hyperbolic Riemann surface.

The Buser-Sarnak result mentioned above corresponds to the case where D is a division algebra defined over $\mathbb{Q}$, while $I = \langle m\rangle \lhd \mathbb{Z}$.

The proof of Theorem 1.5 is given in Section 6, where we provide additional details concerning the constant c, cf. Theorem 6.1.

When $\Gamma(I)$ is torsion free, the area of X_I is equal to $4\pi(g(X_I)-1)$. We can therefore rephrase the bound in terms of the systolic ratio, as follows.

Definition 1.6. The *systolic ratio*, $\mathrm{SR}(X,\mathcal{G})$, of a metric $\mathcal{G}$ on an n-manifold X is

$$\mathrm{SR}(X,\mathcal{G}) = \frac{\mathrm{sys}\pi_1(\mathcal{G})^n}{\mathrm{vol}_n(\mathcal{G})}.$$

Corollary 1.7. *The hyperbolic surfaces $X_I = \Gamma(I)\backslash\mathcal{H}^2$ satisfy the bound*

$$\mathrm{SR}(X_I) \geq \frac{4}{9\pi}\frac{(\log g(X_I) - c)^2}{g(X_I)},$$

where c only depends on Γ.

Note that an asymptotic *upper* bound of $\frac{1}{\pi}\frac{(\log g)^2}{g}$ was obtained by the first author in collaboration with S. Sabourau in [**KS05**], for the systolic ratio of arbitrary (not necessarily hyperbolic) metrics on a genus g

surface. The asymptotic multiplicative constant therefore lies in the interval

$$\limsup_{g\to\infty} \frac{g\,\mathrm{SR}(\Sigma_g)}{\log(g)^2} \in \left[\tfrac{4}{9\pi}, \tfrac{1}{\pi}\right], \tag{1.2}$$

where Σ_g denotes a surface of genus g. The question of the precise asymptotic constant in (1.2) remains open. Note that R. Brooks and E. Makover [**BrM04**, p. 124] opine that the Platonic surfaces of [**Br99**] have systole on the order of $C \log g$. However, the text of [**Br99**] seems to contain no explicit statement to that effect. The result may be obtainable by applying the techniques of [**Br99**] so as to compare the systole of compact Platonic surfaces, and the systole of their noncompact prototypes, namely the finite area surfaces of the congruence subgroups of the modular group, studied by P. Schmutz [**Sc94**].

The expected value of the systole of a random Riemann surface turns out to be independent of the genus [**MM05**] (in particular, it does not increase with the genus), indicating that one does not often come across surfaces constructed in the present paper.

Another asymptotic problem associated with surfaces is Gromov's filling area conjecture, when the circle is filled by a surface of an arbitrary genus g. The case $g = 1$ was recently settled [**BCIK05**].

Similarly, in the Kleinian case we have the following. The simplicial volume $\|X\|$, a topological invariant of a manifold X, was defined in [**Gr81**].

Theorem 1.8. *Let Γ be an arithmetic cocompact torsion free subgroup of $\mathrm{SL}_2(\mathbb{C})$. Then for a suitable constant $c = c(\Gamma)$, the congruence subgroups of Γ satisfy*

$$\mathrm{sys}\pi_1(X_I) \geq \frac{2}{3} \log \|X_I\| - c$$

for every ideal $I \lhd O_K$, where $X_I = \Gamma(I)\backslash\mathcal{H}^3$, while $\mathcal{H}^3$ is the hyperbolic 3-space.

As a consequence, we obtain the following lower bound for the systolic ratio of the hyperbolic 3-manifolds X_I. This bound should be compared to Gromov's similar *upper* bound, cf. [**Gr83**, 6.4.D$''$] (note the missing exponent n over the log), [**Gr96**, 3.C.3(1)], [**Gr99**, p. 269].

Corollary 1.9. *Let Γ be an arithmetic cocompact subgroup of $\mathrm{SL}_2(\mathbb{C})$. The 3-manifolds $X_I = \Gamma(I)\backslash\mathcal{H}^3$ satisfy the bound*

$$\mathrm{SR}(X_I) \geq C_1 \frac{(\log \|X_I\| - c)^3}{\|X_I\|},$$

where c and C_1 only depend on Γ. In fact, if Γ is torsion free, then one can take $C_1 = \frac{8}{27} v_3^{-1}$, where v_3 is the volume of a regular ideal 3-simplex in $\mathcal{H}^3$.

Theorem 1.8 and Corollary 1.9 are proved in Section 6. These bounds are shown in [**Vis07**] to be exact if K has only one Archimedean place.

Asymptotic lower bounds for the systolic ratio in terms of the Betti number are studied in [**BB05**]. Analogous asymptotic estimates for the conformal 2-systole of 4-manifolds are studied in [**Ka03**, **Ha06**]. See [**BKSS06**] for a recent study of the 4-systole.

In a direction somewhat opposite to ours, hyperbolic 4-manifolds of arbitrarily short 1-systole are constructed by I. Agol [**Ag06**].

Returning the the 2-dimensional case, recall that the order of the automorphism group of a Riemann surface of genus g cannot exceed the bound $84(g-1)$. Of particular interest are surfaces attaining this bound, which are termed Hurwitz surfaces, cf. [**El98**, **El99**]. Consider the geodesic triangle with angles $\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{7}$, which is the least area triangle capable of tiling the hyperbolic plane. Let Δ_H be the group of even products of reflections in the sides of this triangle. The area of $\Delta_H \backslash \mathcal{H}^2$, namely $\pi/21$, is the smallest possible for any Fuchsian group. The Fuchsian group N of a Hurwitz surface is a normal torsion free subgroup of Δ_H. The automorphism group of the surface is the quotient group Δ_H/N. The geometry of Hurwitz surfaces was recently studied in [**Vo04**].

We specialize to Hurwitz surfaces in Section 7. Following N. Elkies [**El98**], we choose an order in a suitable quaternion algebra, as well as a realization of the $\mathbb{Z}/2\mathbb{Z}$-central extension $\tilde{\Delta}_H$ of Δ_H as a group of 2×2 matrices. We then obtain the following sharpening of Theorem 1.5.

Theorem 1.10. *For infinitely many congruence subgroups $\Delta_H(I) \triangleleft \tilde{\Delta}_H$, the Hurwitz surfaces $X_I = \Delta_H(I) \backslash \mathcal{H}^2$ satisfy the bound*

$$\mathrm{sys}\pi_1(X_I) \geq \frac{4}{3} \log g(X_I).$$

With the explicit realization of $\tilde{\Delta}_H$ described in Section 7, the bound holds for all the principal congruence subgroups.

Riemannian geometers have long felt that surfaces which are optimal for the systolic problem should have the highest degree of symmetry; see, for example, the last paragraph of the introduction to [**HK02**, p. 250]. This sentiment is indeed borne out by our Theorem 1.10 (though in principle there could exist surfaces with even better asymptotic systolic behavior).

In Section 2, we present the key trace estimate which allows us to generalize the results of Buser and Sarnak to quaternion algebras over an arbitrary number field. In Section 3, we prove the trace estimate. Section 4 contains a detailed study of congruence subgroups. We comment on torsion elements in Section 5. Section 6 contains the proofs of the main theorems. Section 7 focuses on the Hurwitz case.

Acknowledgments. We are grateful to Misha Belolipetsky, Amiram Braun, Dima Kazhdan, Alan Reid, David Saltman, and Roger Vogeler for helpful discussions.

2. Trace estimate

Fix $F = \mathbb{R}$ or $F = \mathbb{C}$, and let K be a number field of dimension d over $\mathbb{Q}$, as in Definition 1.3. Namely, K is a totally real field in the former case, or a field with exactly one complex Archimedean place, in the latter. We view K as a subfield of F, where the other real embeddings are denoted by $\sigma : K \hookrightarrow \mathbb{R}$ for $\sigma \neq 1$. Let D be a quaternion division algebra with center K. We assume that D is split by the distinguished embedding $K \subseteq F$, and remains a division algebra under any other embedding.

Recall that an *order* $\mathcal{Q}$ of D is a subring (with unit), which is a finite module over $\mathbb{Z}$, and such that its (central) ring of fractions is D. Every maximal order contains O_K, the ring of algebraic integers in K (since $O_K \cdot \mathcal{Q}$ is an order), so in the sequel we will only deal with orders containing O_K.

Let $D^1 \subseteq D^\times$ denote the group of elements of norm 1 in D. Similarly, for an order $\mathcal{Q} \subset D$, let $\mathcal{Q}^1$ denote the group of elements of norm one in $\mathcal{Q}$. By assumption the inclusion $K \subseteq F$ splits D, so we have the natural inclusion

$$\mathcal{Q} \subseteq D \subseteq D \otimes_K F \cong \mathrm{M}_2(F). \tag{2.1}$$

Thus $\mathcal{Q}^1$ is a subgroup of $(D \otimes F)^1 = \mathrm{SL}_2(F)$.

Since $\mathcal{Q}$ is an order over O_K, in particular it contains O_K (as its center). An ideal I of the center defines an ideal $I\mathcal{Q}$ of $\mathcal{Q}$, yielding a finite quotient ring $\mathcal{Q}/I\mathcal{Q}$. The *principal congruence subgroup* of $\mathcal{Q}^1$ with respect to an ideal $I \lhd O_K$ is by definition the kernel of the homomorphism $\mathcal{Q}^1 \to (\mathcal{Q}/I\mathcal{Q})^\times$ induced by the natural projection $\mathcal{Q} \to \mathcal{Q}/I\mathcal{Q}$. A *congruence subgroup* is any subgroup of $\mathcal{Q}^1$ containing a principal congruence subgroup.

Definition 2.1. The kernel of $\mathcal{Q}^1 \to (\mathcal{Q}/I\mathcal{Q})^\times$ induced by the natural projection $\mathcal{Q} \to \mathcal{Q}/I\mathcal{Q}$, will be denoted by $\Gamma(I) = \mathcal{Q}^1(I)$, where

$$\mathcal{Q}^1(I) = \ker\left(\mathcal{Q}^1 \to (\mathcal{Q}/I\mathcal{Q})^\times\right). \tag{2.2}$$

Since $D \otimes_\sigma \mathbb{R}$ is, by hypothesis, a division algebra for $\sigma \neq 1$, the associated groups $(D \otimes_\sigma \mathbb{R})^1$ are compact. Moreover, the ring O_K is discrete in the product $F \times \prod_{\sigma \neq 1} \sigma(\mathbb{R})$, making $\mathcal{Q}^1$ discrete in the product

$$(D \otimes F)^1 \times \prod (D \otimes_\sigma \mathbb{R})^1,$$

and therefore discrete in $(D \otimes F)^1 = \mathrm{SL}_2(F)$. In fact $\mathcal{Q}^1$ is cocompact there, by [**PR94**, Theorem 5.5].

Since all orders of D are commensurable, the groups of elements of norm 1 in orders are commensurable to each other, i.e., the intersection of two such groups is of finite index in each of the groups [**MR03**, p. 56]. Our computations are based on a specific order, arising naturally from the presentation of D.

A quaternion algebra can always be presented in the form

$$D = (a,b)_K = K[i,j \mid i^2 = a,\, j^2 = b,\, ji = -ij] \tag{2.3}$$

for suitable elements $a, b \in K$. If $\sigma : K \hookrightarrow \mathbb{R}$ is an embedding, then with this presentation, the algebra $D \otimes_\sigma \mathbb{R}$ is a division algebra if and only if we have both $\sigma(a) < 0$ and $\sigma(b) < 0$. Another convenient feature is that the matrix trace in the embedding $D \subseteq \mathrm{M}_2(F)$ is equal to the reduced trace Tr_D, which for non-central elements is the negative of the linear coefficient in the minimal polynomial. This can be read off the presentation of an element:

$$\mathrm{Tr}_D(x_0 + x_1 i + x_2 j + x_3 ij) = 2x_0$$

for any $x_0, x_1, x_2, x_3 \in K$.

Lemma 2.2. *The defining constants a and b of the algebra D can be taken to be algebraic integers in K.*

Proof. It is clear from the presentation (2.3) that the isomorphism class of D depends only the class of a and b in $K^\times / K^{\times 2}$. q.e.d.

Let O_K be the ring of algebraic integers in K, and fix the order

$$\mathcal{O} = O_K \oplus O_K i \oplus O_K j \oplus O_K ij. \tag{2.4}$$

Since all elements of an order are algebraic integers, $\mathcal{Q}$ is contained in $\frac{1}{\kappa}\mathcal{O}$ for a suitable $\kappa \in O_K$ (in fact one can take $\kappa \mid 2ab$, cf. Lemma 2.2). Denote by $\mathrm{N}(k)$ the number field norm of $k \in K$ along the extension $K/\mathbb{Q}$. Similarly, we denote by $\mathrm{N}(I)$ the norm of an ideal $I \lhd O_K$, namely the cardinality of the quotient ring O_K/I. The two norms coincide for principal ideals, so in particular, we have $\mathrm{N}(m) = m^d$ for $m \in \mathbb{Z}$.

Theorem 2.3. *Let $I \lhd O_K$ be an ideal. If $F = \mathbb{R}$ then for every $x \neq \pm 1$ in $\mathcal{Q}^1(I)$, we have the following estimates:*

$$\left|\mathrm{Tr}_D(x)\right| > \frac{1}{2^{d-2}\mathrm{N}(\langle 2 \rangle + \kappa I)} \mathrm{N}(I)^2 - 2 \tag{2.5}$$

and therefore

$$\left|\mathrm{Tr}_D(x)\right| > \frac{1}{2^{2d-2}} \mathrm{N}(I)^2 - 2. \tag{2.6}$$

If $F = \mathbb{C}$, then

$$\begin{aligned}\left|\mathrm{Tr}_D(x)\right| &> \frac{1}{2^{d/2-2}\mathrm{N}(\langle 2\rangle + \kappa I)^{1/2}}\mathrm{N}(I) - 2 \\ &\geq \frac{1}{2^{d-2}}\left|\mathrm{N}(I)\right| - 2.\end{aligned}$$

The estimates are proved in the next section.

3. Proof of trace estimate

The first step towards a proof of Theorem 2.3 is a bound on $\sigma(x_0)$ for $\sigma \neq 1$, where $x \in D$ is an arbitrary element of norm 1.

Proposition 3.1. *Let $x = x_0 + x_1 i + x_2 j + x_3 ij$, where $x \neq \pm 1$, be any element of norm one in D. Then $|\sigma(x_0)| < 1$ for every non-trivial embedding $\sigma : K \hookrightarrow \mathbb{R}$. Writing $x_0 = 1 + y_0$, we obtain*

$$-2 < \sigma(y_0) < 0. \tag{3.1}$$

Proof. The norm condition is that

$$x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 = 1 \tag{3.2}$$

in K, where a, b are the structure constants from (2.3). Applying any $\sigma \neq 1$, we obtain

$$\begin{aligned}\sigma(x_0)^2 &\leq \sigma(x_0)^2 + \sigma(-a)\sigma(x_1)^2 + \sigma(-b)\sigma(x_2)^2 + \sigma(ab)\sigma(x_3)^2 \\ &= 1,\end{aligned} \tag{3.3}$$

since $\sigma(a) < 0$ and $\sigma(b) < 0$ by assumption. In particular, equality in (3.3) implies that $x_1 = x_2 = x_3 = 0$. Writing $x_0 = 1 + y_0$, we obtain the inequality $|1 + \sigma(y_0)| < 1$, proving (3.1). q.e.d.

Recall that for any ideal $J \lhd O_K$, the fractional ideal

$$J^{-1} = \{u \in K : \ uJ \subseteq O_K\}$$

is the inverse of J in the group of fractional ideals of K.

Recall that the symplectic involution on D is, by definition, the unique involution under which only central elements are symmetric. It is often called the 'standard' involution.

Lemma 3.2. *The symplectic involution preserves any order in D.*

Proof. Let $w \mapsto w^*$ denote the involution. The reduced trace and norm may be defined by $\mathrm{Tr}_D(w) = w + w^*$ and $\mathrm{N}_D(w) = ww^*$, which implies the characteristic equation

$$w^2 - \mathrm{Tr}_D(w)w + \mathrm{N}_D(w) = 0$$

for every $w \in D$. Moreover, if $\mathcal{Q}$ is an order and we have $w \in \mathcal{Q}$, it follows that $\mathrm{Tr}_D(w), \mathrm{N}_D(w) \in O_K$, as $O_K[w] \subseteq \mathcal{Q}$ is a finite module. In particular, we have $w^* = \mathrm{Tr}_D(w) - w \in \mathcal{Q}$ for every $w \in \mathcal{Q}$. q.e.d.

Lemma 3.3. *Let $I \lhd O_K$. If $z \in I\mathcal{Q}$ then $\mathrm{Tr}_D(z) \in I$ and $\mathrm{N}_D(z) \in I^2$.*

Proof. Let $\alpha_1, \ldots, \alpha_t \in I$ be generators of I as an O_K-module (in fact we may assume $t \leq 2$, as O_K is a Dedekind domain [**Coh61**, Section VII.10]).

Let $z = \sum \alpha_r w_r$, $w_r \in \mathcal{Q}$, be an arbitrary element of $I\mathcal{Q}$. Then we have $w_r w_s^* \in \mathcal{Q}$ by Lemma 3.2, so that

$$\mathrm{Tr}_D(z) = \sum \alpha_r \, \mathrm{Tr}_D(w_r) \in I$$

since $\mathrm{Tr}_D(w_r) \in O_K$, and

$$\begin{aligned} \mathrm{N}_D(z) = zz^* &= \sum_{r,s} \alpha_r \alpha_s w_r w_s^* \\ &= \sum_r \alpha_r^2 w_r w_r^* + \sum_{r<s} \alpha_r \alpha_s (w_r w_s^* + w_s w_r^*) \\ &= \sum_r \alpha_r^2 \mathrm{N}_D(w_r) + \sum_{r<s} \alpha_r \alpha_s \, \mathrm{Tr}_D(w_r w_s^*) \in I^2 \end{aligned}$$

since $\mathrm{N}_D(w_r), \mathrm{Tr}_D(w_r w_s^*) \in O_K$. q.e.d.

Lemma 3.4. *Let $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{Q}^1(I)$, where $\mathcal{Q} \subseteq \frac{1}{\kappa}\mathcal{O}$, and $\mathcal{O}$ is the standard order of* (2.4)*. Then*

$$x_0 - 1 \in (\langle 2 \rangle + \kappa I)^{-1} I^2. \tag{3.4}$$

Proof. By assumption, we have $x - 1 \in I\mathcal{Q} \subseteq \frac{1}{\kappa} I\mathcal{O}$. In particular, the element $y_0 = x_0 - 1$ satisfies $y_0 \in \frac{1}{\kappa} I$. Substituting $x_0 = 1 + y_0$ in (3.2), we obtain

$$2y_0 = -(y_0^2 - ax_1^2 - bx_2^2 + abx_3^2) = -\mathrm{N}_D(x-1) \in I^2, \tag{3.5}$$

by the previous lemma. Using the decomposition of fractional ideals in the Dedekind domain O_K, which implies that $(J_1 + J_2)(J_1 \cap J_2) = J_1 J_2$, we obtain

$$y_0 \in \frac{1}{\kappa} I \cap \frac{1}{2} I^2 = \frac{1}{2\kappa}(2O_K \cap \kappa I) I = (2O_K + \kappa I)^{-1} I^2, \tag{3.6}$$

proving the lemma. q.e.d.

Proof of Theorem 2.3. We write $x = x_0 + x_1 i + x_2 j + x_3 ij$, and we set $y_0 = x_0 - 1$. By the lemma, we have $\mathrm{N}(y_0) \in \frac{\mathrm{N}(I)^2}{\mathrm{N}(\langle 2 \rangle + \kappa I)} \mathbb{Z}$, but we also have $y_0 \neq 0$ (Proposition 3.1). When $F = \mathbb{R}$, this shows

$$\frac{\mathrm{N}(I)^2}{\mathrm{N}(\langle 2 \rangle + \kappa I)} \leq |\mathrm{N}(y_0)| \quad = \quad |y_0| \prod_{\sigma \neq 1} |\sigma(y_0)| < 2^{d-1} |y_0| \,,$$

by inequality (3.1). The inclusion $\langle 2 \rangle \subseteq \langle 2 \rangle + \kappa I$ implies

$$\mathrm{N}(\langle 2 \rangle + \kappa I) \leq \mathrm{N}(\langle 2 \rangle) = \mathrm{N}(2) = 2^d.$$

Plugging the norm bound on y_0 back in $x_0 = y_0 + 1$, we obtain

$$\begin{aligned} |x_0| &= |1 + y_0| \\ &\geq |y_0| - 1 \\ &> \frac{1}{2^{d-1}\mathrm{N}(\langle 2\rangle + \kappa I)}\mathrm{N}(I)^2 - 1, \\ &\geq \frac{1}{2^{2d-1}}\mathrm{N}(I)^2 - 1, \end{aligned}$$

from which the case $F = \mathbb{R}$ of Theorem 2.3 follows immediately in view of the fact that $\mathrm{Tr}_D(x) = 2x_0$.

In the case $F = \mathbb{C}$, we repeat the same argument, noting that $|\mathrm{N}(y_0)| = |y_0|^2 \prod_{\sigma\neq 1} |\sigma(y_0)|$ so that $\frac{|\mathrm{N}(I)|^2}{\mathrm{N}(\langle 2\rangle+\kappa I)} < 2^{d-2} |y_0|^2$. q.e.d.

4. Congruence subgroups of $\mathcal{Q}^1$ in the prime power case

Some of the calculations in this section are related to A. Borel's volume formula [**Bo81**]; see also [**Jo98**, **Be04**].

Let F be $\mathbb{R}$ or $\mathbb{C}$ as above, and let $\Gamma = \mathcal{Q}^1$ be the group defined by an order $\mathcal{Q}$ in a division quaternion algebra D over a number field K, as in Sections 2 and 3.

Let $I \lhd O_K$ be an arbitrary ideal. In order to estimate the topological invariants of $\Gamma(I)\backslash\mathcal{H}^2$ or $\Gamma(I)\backslash\mathcal{H}^3$ (namely, the genus and simplicial volume, respectively), we need to bound the index $[\Gamma : \Gamma(I)]$ in terms of I. We will construct below a norm map

$$\nu : (\mathcal{Q}/I\mathcal{Q})^\times \to (O_K/I)^\times. \tag{4.1}$$

Let $(\mathcal{Q}/I\mathcal{Q})^1 = \nu^{-1}(1)$, where 1 denotes the multiplicative neutral element in the finite ring O_K/I.

Lemma 4.1. *We have the bound*

$$[\Gamma : \Gamma(I)] \leq (\mathcal{Q}/I\mathcal{Q})^1. \tag{4.2}$$

Proof. The reduced norm N_D on D may be defined by setting $N(x) = xx^*$, where $x \mapsto x^*$ is the unique symplectic involution of D. Note that every element with zero trace is anti-symmetric under the involution. After tensoring with a splitting field, the involution becomes the familiar adjoint map, which exchanges the two diagonal elements and multiplies the off diagonal elements by -1. Note that orders are closed under involution, as $x^* = \mathrm{tr}(x) - x$.

Note that the symplectic involution descends to the quotient $\mathcal{Q}/I\mathcal{Q}$. Indeed, the involution acts trivially on $I \lhd O_K$ and preserves the order $\mathcal{Q} \subset D$ by Lemma 3.2. Hence an ideal of the form $I\mathcal{Q}$ is also closed under the involution. Thus we may define the involution on a coset $(x + I\mathcal{Q})$ by setting $(x + I\mathcal{Q})^* = x^* + I\mathcal{Q}$, which is independent of the representative. The involution can then be used to define a norm map ν of (4.1). Let $\pi : \mathcal{Q} \to \mathcal{Q}/I\mathcal{Q}$ and $\pi_0 : O_K \to O_K/I$ denote the natural projections; then $\pi_0 \mathrm{N}(x) = \pi_0(xx^*) = \nu(\pi(x))$, and in particular $\pi(x) \in (\mathcal{Q}/I\mathcal{Q})^1$ for every $x \in \mathcal{Q}^1 = \Gamma$.

By definition, $\mathrm{Ker}(\pi) \cap \Gamma = \Gamma(I) = \mathcal{Q}^1(I)$, and so

$$\Gamma/\Gamma(I) \cong \pi(\mathcal{Q}^1) \leq (\mathcal{Q}/I\mathcal{Q})^1,$$

proving the claim. q.e.d.

Since K is an algebraic number field, O_K is a Dedekind domain, so that every ideal factors as an intersection of powers of prime ideals. Suppose $I = \mathfrak{p}^t$ where $\mathfrak{p} \lhd O_K$ is a prime ideal. To find an upper bound for the right-hand side of (4.2), we pass to the local situation, via standard techniques in algebraic number theory, as follows.

Let $K_{\mathfrak{p}}$ be the completion of K with respect to the $\mathfrak{p}$-adic valuation, and $O_{\mathfrak{p}}$ the valuation ring. We consider an $O_{\mathfrak{p}}$-order in $D_{\mathfrak{p}} = D \otimes_K K_{\mathfrak{p}}$, defined by setting $\mathcal{Q}_{\mathfrak{p}} = \mathcal{Q} \otimes_{O_K} O_{\mathfrak{p}}$.

Lemma 4.2. *We have an isomorphism* $\mathcal{Q}/I\mathcal{Q} = \mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}}$.

Proof. Let $S = O_K - \mathfrak{p}$, the complement of $\mathfrak{p}$ in O_K. Since $\mathfrak{p}$ is a maximal ideal, localization (in which elements of S are forced into being invertible) gives

$$\mathcal{Q}/\mathfrak{p}^t \mathcal{Q} \cong S^{-1}\mathcal{Q}/\mathfrak{p}^t S^{-1}\mathcal{Q},$$

which is isomorphic to $\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}}$ [**Re75**, Exercise 5.7]. q.e.d.

It follows that

$$[\Gamma : \Gamma(\mathfrak{p}^t)] \leq \left|(\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}})^1\right|. \tag{4.3}$$

In one common situation, we can compute $\left|(\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}})^1\right|$ explicitly. To put things in perspective, it is worth noting that for all but finitely many primes $\mathfrak{p}$, the algebra $D_{\mathfrak{p}}$ is a matrix algebra, and $\mathcal{Q}_{\mathfrak{p}}$ is maximal, i.e., not contained in a larger order. Let $q = \mathrm{N}(\mathfrak{p}) = \left|O_K/\mathfrak{p}\right|$.

Lemma 4.3. *Suppose $\mathcal{Q}_{\mathfrak{p}}$ is a maximal order of $D_{\mathfrak{p}}$. If $D_{\mathfrak{p}}$ is a division algebra, then $\mathcal{Q}/\mathfrak{p}^t\mathcal{Q}$ is a local* (*non-commutative*) *ring with residue field of order q^2 and radical whose nilpotency index is $2t$; in such a case, we have $\left|(\mathcal{Q}/\mathfrak{p}^t\mathcal{Q})^1\right| = q^{3t}(1 + \frac{1}{q})$. Otherwise, we have $\mathcal{Q}/\mathfrak{p}^t\mathcal{Q} \cong \mathrm{M}_2(O_{\mathfrak{p}}/\mathfrak{p}^t)$, and $\left|(\mathcal{Q}/\mathfrak{p}^t\mathcal{Q})^1\right| = q^{3t}(1 - \frac{1}{q^2})$.*

Proof. Let $\varpi \in O_{\mathfrak{p}}$ be a uniformizer (i.e., generator of the unique maximal ideal). Central simple algebras over local fields are cyclic [**Pi82**, Chapter 17]. Therefore, there is an unramified maximal subfield L, satisfying

$$K_{\mathfrak{p}} \subseteq L \subseteq D_{\mathfrak{p}}, \tag{4.4}$$

and an element $z \in D_{\mathfrak{p}}$, such that $z\ell z^{-1} = \sigma(\ell)$ for $\ell \in L$ (where σ is the non-trivial automorphism of $L/K_{\mathfrak{p}}$), and moreover $D_{\mathfrak{p}} = L[z]$. Furthermore if $D_{\mathfrak{p}}$ is a division algebra then we may assume $z^2 = \varpi$. If $D_{\mathfrak{p}}$ splits, then being a matrix algebra it can be presented in a similar manner, with $z^2 = 1$.

In both cases, $D_{\mathfrak{p}}$ has, up to conjugation, a unique maximal order [**Re75**, Section 17], namely $O_L[z]$ where O_L is the valuation ring of L. We may therefore assume $\mathcal{Q}_{\mathfrak{p}} = O_L[z]$.

To finish the proof, we note that $O_L[z]/\varpi^t O_L[z]$ is a local ring, so its invertible elements are those invertible modulo the maximal ideal. First assume $D_{\mathfrak{p}}$ is split, so that $z^2 = 1$. Then

$$O_L[z]/\varpi^t O_L[z] = (O_L/\varpi^t O_L)[\bar{z} \mid \bar{z}^2 = 1]$$

is isomorphic to $\mathrm{M}_2(O_{\mathfrak{p}}/\varpi^t O_{\mathfrak{p}})$, noting that $O_L/\varpi^t O_L$ is a finite local ring, which modulo the maximal ideal is the residue field $O_{\mathfrak{p}}/\varpi O_{\mathfrak{p}} = \bar{K}$, of order q. The group of elements of norm 1 is $\mathrm{SL}_2(O_{\mathfrak{p}}/\varpi^t O_{\mathfrak{p}})$, of order $(q^3 - q)q^{3(t-1)}$.

Finally, assume $D_{\mathfrak{p}}$ does not split, so $z^2 = \varpi$. Then the ring

$$O_L[z]/\varpi^t O_L[z] = O_L[z]/z^{2t} O_L[z]$$

is a local (non-commutative) ring, which modulo the maximal ideal is

$$O_L[z]/zO_L[z] \cong \bar{L},$$

the residue field of L, of order q^2. Thus there are $(q^2 - 1)q^{2(2t-1)}$ invertible elements. The norm map

$$(O_L[z]/z^{2t} O_L[z])^\times \to (O_{\mathfrak{p}}/\varpi^t)^\times$$

is onto (since the norm $O_L^\times \to O_{\mathfrak{p}}^\times$ is), and since $\left|(O_{\mathfrak{p}}/\varpi^t)^\times\right| = (q-1)q^{t-1}$, there are precisely

$$\frac{(q^2 - 1)q^{2(2t-1)}}{(q - 1)q^{t-1}} = (q + 1)q^{3t-1}$$

elements of norm 1. q.e.d.

Our next goal is to bound $(\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}})^1$ in the general case. Consider the exact sequence induced by the norm map, namely

$$(\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}})^1 \hookrightarrow (\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}})^\times \xrightarrow{N} (O_K/\mathfrak{p}^t)^\times, \tag{4.5}$$

which shows that

$$\left|(\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}})^1\right| \leq \frac{\left|(\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t \mathcal{Q}_{\mathfrak{p}})^\times\right|}{|\mathrm{Im}(N)|}. \tag{4.6}$$

Here, $\mathrm{Im}(N)$ stands for the image of the norm map in (4.5). We will first treat the numerator, then the denominator.

Since $\mathfrak{p}\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t\mathcal{Q}_{\mathfrak{p}}$ is a nilpotent ideal of $\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t\mathcal{Q}_{\mathfrak{p}}$, the invertible elements in this finite ring are those invertible modulo $\mathfrak{p}\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t\mathcal{Q}_{\mathfrak{p}}$; namely, in the quotient ring $\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}\mathcal{Q}_{\mathfrak{p}}$. Let $u = |(\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}\mathcal{Q}_{\mathfrak{p}})^\times|$, then

$$\left|(\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t\mathcal{Q}_{\mathfrak{p}})^\times\right| = \left|\mathfrak{p}\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}^t\mathcal{Q}_{\mathfrak{p}}\right|u \leq q^{4(t-1)}u.$$

By Wedderburn's decomposition theorem, we can decompose the $O_K/\mathfrak{p}$-algebra $\mathcal{Q}_{\mathfrak{p}}/\mathfrak{p}\mathcal{Q}_{\mathfrak{p}}$ as $T \oplus J$, where T is a semisimple algebra and J is the radical. Again, the invertible elements are those invertible modulo J, namely in T.

Proposition 4.4. *Let $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ denote the finite fields of orders q and q^2, respectively. Then T is isomorphic to one of the following six algebras:*

$$\mathbb{F}_q,\ \mathbb{F}_{q^2},\ \mathrm{M}_2(\mathbb{F}_q),\ \mathbb{F}_q \times \mathbb{F}_q,\ \mathbb{F}_q \times \mathbb{F}_{q^2},\ \textit{or}\quad \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}.$$

Furthermore, only the first three options are possible if $D_{\mathfrak{p}}$ is a division algebra.

Proof. By construction, T is a semisimple algebra over $\mathbb{F}_q$. The classification follows from two facts: every element satisfies a quadratic equation; and the maximal number of mutually orthogonal idempotents is no larger than the corresponding number for $\mathcal{Q}_{\mathfrak{p}}$ (as Hensel's lemma allows lifting idempotents from $\mathcal{Q}/\mathfrak{p}\mathcal{Q}$ to $\mathcal{Q}$). q.e.d.

By inspection of the various cases, the number u of invertible elements satisfies

$$u \leq \begin{cases} q(q-1)(q^2-1) & \text{if } D_{\mathfrak{p}} \text{ is a division algebra,} \\ q^2(q-1)^2 & \text{otherwise.} \end{cases} \tag{4.7}$$

It remains to give a lower bound for the size of $\mathrm{Im}(N)$. Since $O_{\mathfrak{p}} \subseteq \mathcal{Q}$, every square in $(O_{\mathfrak{p}}/\mathfrak{p}^t)^\times$ is a norm.

Lemma 4.5. *If $\mathfrak{p}$ is non-diadic (namely $\mathfrak{p}$ is prime to 2, and q is odd), then $\left|(O_K/\mathfrak{p}^t)^{\times 2}\right| = \frac{q-1}{2}q^{t-1}$.*

On the other hand if $\mathfrak{p}$ is diadic and $2O_{\mathfrak{p}} = \mathfrak{p}^e$ for $e \geq 1$, then we have the bound $\left|(O_K/\mathfrak{p}^t)^{\times 2}\right| \geq \frac{1}{2}q^{t-e}$ (with equality if $t \geq 2e+1$).

Proof. Note that an element $a \in O_{\mathfrak{p}}^\times$ is a square if and only if a is a square modulo $4\mathfrak{p}$ [**OM62**, Chapter 63]. Furthermore, we have $y^2 \equiv x^2 \pmod{4\mathfrak{p}}$ if and only if $y \equiv \pm x \pmod{2\mathfrak{p}}$, proving the lemma. q.e.d.

Combining Equations (4.6) and (4.7) with Lemma 4.5, we have the following bounds for non-maximal orders:

(4.8)

$$\frac{(\mathcal{Q}/\mathfrak{p}^t\mathcal{Q})^1}{q^{3t}} \leq \begin{cases} 2(1-q^{-2}) & \text{if } D_\mathfrak{p} \text{ is a division algebra, } \mathfrak{p} \text{ non-diadic,} \\ 2(1-q^{-1})(1-q^{-2})q^e & \text{if } D_\mathfrak{p} \text{ is a division algebra, } \mathfrak{p} \text{ diadic,} \\ 2(1-q^{-1}) & \text{if } D_\mathfrak{p} \text{ is a matrix algebra, } \mathfrak{p} \text{ non-diadic,} \\ 2(1-q^{-1})^2q^e & \text{if } D_\mathfrak{p} \text{ is a matrix algebra, } \mathfrak{p} \text{ diadic,} \end{cases}$$

where

$$2O_\mathfrak{p} = \mathfrak{p}^e \tag{4.9}$$

in the diadic cases.

Given an order $\mathcal{Q}$ of a quaternion algebra D over K, let T_1 denote the set of finite primes $\mathfrak{p}$ for which $D_\mathfrak{p}$ is a division algebra, and let T_2 denote the set of finite primes for which $\mathcal{Q}_\mathfrak{p}$ is non-maximal. It is well known that T_1 and T_2 are finite.

We denote

$$\lambda_{D,\mathcal{Q}} = \prod_{\mathfrak{p}\in T_1-T_2}\left(1+\frac{1}{\mathrm{N}(\mathfrak{p})}\right)\cdot\prod_{\mathfrak{p}\in T_2} 2\cdot\prod_{\mathfrak{p}\in T_2,\,\mathfrak{p}\,|\,2}\mathrm{N}(\mathfrak{p})^{e(\mathfrak{p})}, \tag{4.10}$$

where for a diadic prime, $e(\mathfrak{p})$ denotes the ramification index of 2, as defined in (4.9). The third product is bounded from above by

$$\prod_{\mathfrak{p}\,|\,2}\mathrm{N}(\mathfrak{p})^{e(\mathfrak{p})} = \mathrm{N}(2) = 2^d.$$

Factoring an arbitrary ideal $I \lhd O_K$ into prime factors $I = \prod \mathfrak{p}_i^{t_i}$, we have by the Chinese remainder theorem that $\mathcal{Q}/I\mathcal{Q} \cong \prod \mathcal{Q}/\mathfrak{p}_i^{t_i}\mathcal{Q}$, where the projection onto each component preserves the norm (as the norm can be defined in terms of the involution). The results of Lemma 4.3 and (4.10) imply the bound

$$\left|(\mathcal{Q}/I\mathcal{Q})^1\right| \leq \lambda_{D,\mathcal{Q}}\prod\mathrm{N}(\mathfrak{p}_i^{t_i})^3 = \lambda_{D,\mathcal{Q}}\mathrm{N}(I)^3.$$

Together with Equation (4.3), we obtain the following corollary.

Corollary 4.6. *We have the bound* $[\Gamma:\Gamma(I)] \leq \left|(\mathcal{Q}/I\mathcal{Q})^1\right| \leq \lambda_{D,\mathcal{Q}}\mathrm{N}(I)^3$. *In fact, the products in* (4.10) *can be taken over the primes* $\mathfrak{p}\,|\,I$*; in particular if* $\mathcal{Q}$ *is maximal and no ramification primes of* D *divide* I*, then* $[\Gamma:\Gamma(I)] < \mathrm{N}(I)^3$.

5. Torsion elements

A comment about torsion elements in $\mathcal{Q}^1$ is in order. If $x \in D$ is a root of unity, then $K[x]$ is a quadratic field extension of K, and with K fixed, there are of course only finitely many roots of unity with this property. Moreover if $x \in \mathcal{Q}^1$ then $\mathrm{N}(x) = 1$ forces $x + x^{-1} \in K$. Now, if $x \in \mathcal{Q}^1(I)$ for an ideal $I \lhd O_K$, then we have

$$0 = x^2 - (x + x^{-1})x + 1 \equiv 2 - (x + x^{-1}) = -x^{-1}(x-1)^2 \pmod{I},$$

so $I \supseteq \left\langle x^{-1}(x-1)^2 \right\rangle$. These are the ideals to be avoided if we want $\mathcal{Q}^1(I)$ to be torsion free:

Corollary 5.1. *If $\mathcal{Q}^1(I)$ is not torsion free, then I divides an ideal of the form*

$$\left\langle x^{-1}(x-1)^2 \right\rangle = \left\langle x + x^{-1} - 2 \right\rangle,$$

when x a root of unity for which $K[x]/K$ is a quadratic extension. Moreover if I contains a principal ideal I_0, then $I_0^2 \mid \left\langle x^{-1}(x-1)^2 \right\rangle$.

Proof. Only the final statement was not proved. Suppose $x \in \mathcal{Q}^1(I)$ is a root of unity; then $K[x]/K$ is a quadratic extension, and $x^2 - (x + x^{-1})x + 1 = 0$. Thus $\mathrm{Tr}_D(x) = x + x^{-1} \in O_K$, and $\mathrm{N}(x) = 1$.

Suppose $I_0 \subseteq I$ and $I_0 = \langle i \rangle$ is principal. Write $x = 1 + ia$ for $a \in \mathcal{Q}$. Then

$$x + x^{-1} = \mathrm{Tr}_D(x) = 2 + i\,\mathrm{Tr}_D(a),$$

so that $\mathrm{Tr}_D(a) = \frac{x+x^{-1}-2}{i}$, and

$$1 = \mathrm{N}(x) = (1 + ia)(1 + ia^*) = 1 + i(a + a^*) + i^2 aa^*,$$

where a^* is the quaternion conjugate. Therefore,

$$\mathrm{N}(a) = aa^* = -\frac{1}{i}(a + a^*) = \frac{2 - x + x^{-1}}{i^2}.$$

But as an element of an order, the norm of a is an algebraic integer, implying that i^2 divides $(x + x^{-1}) - 2$. q.e.d.

6. Proof of the main theorems

In this section we prove Theorems 1.5 and 1.8. First, we recall the relation between the length of closed geodesics and traces. Let $\Gamma \leq \mathrm{SL}_2(F)$ be an arbitrary discrete subgroup, and set $X = \Gamma\backslash\mathcal{H}^2$ (or $X = \Gamma\backslash\mathcal{H}^3$ when $F = \mathbb{C}$). Let $x \in \Gamma$ be a semisimple element. Then x is conjugate (in $\mathrm{SL}_2(F)$) to a matrix of the form $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, and

$$|\lambda| = e^{\ell_x/2},$$

where $\ell_x > 0$ is the translation length of x, which is the length of the closed geodesic corresponding to x on the manifold X. Note that if $F=\mathbb{R}$, then in fact $\lambda = e^{\ell_x/2}$. In the Kleinian case $F=\mathbb{C}$, there is a rotation of the loxodromic element, as well. In either case, we have

$$\left|\mathrm{Tr}_{\mathrm{M}_2(F)}(x)\right| = \left|\lambda+\lambda^{-1}\right| \le |\lambda| + |\lambda|^{-1} < |\lambda|+1,$$

and

$$\ell_x > 2\log(\left|\mathrm{Tr}_{\mathrm{M}_2(F)}(x)\right| - 1). \tag{6.1}$$

Because of the undetermined constant in Theorems 1.5 and 1.8, it is enough to treat the co-compact lattice Γ of $\mathrm{SL}_2(F)$ up to commensurability. However, since subgroups defined by orders form an important class of examples, we do give an explicit bound for the principal congruence subgroups of Γ, depending on the volume of the cocompact quotient, as well as some numerical characteristics of the order defining Γ. Therefore, assume $\Gamma = \mathcal{Q}^1$ where $\mathcal{Q}$ is an order in a division algebra D over K, as before.

Now assume $F=\mathbb{R}$, and let $X_I = \Gamma(I)\backslash\mathcal{H}^2$ where $I \lhd O_K$ is a given ideal. Let μ denote the hyperbolic measure on $\mathcal{H}^2$.

Theorem 6.1. *Let K be a totally real number field of dimension d over $\mathbb{Q}$, and let D be a quaternion division algebra as in* (2.3)*. Let $\Gamma = \mathcal{Q}^1$ where $\mathcal{Q}$ is an order in D. Let $\nu = \mu(X_1)$ where $X_1 = \Gamma\backslash\mathcal{H}^2$. Then the surfaces $X_I = \Gamma(I)\backslash\mathcal{H}^2$, where $I\lhd O_K$, satisfy*

$$\mathrm{sys}\pi_1(X_I) \ge \frac{4}{3}\left[\log(g(X_I)) - \left(\log(2^{3d-5}\pi^{-1}\nu\lambda_{D,\mathcal{Q}}) + o(1)\right)\right],$$

where $\lambda_{D,\mathcal{Q}}$ is defined as in (4.10)*, ranging over the primes of $T_1\cup T_2$ which divide I.*

Let $R(D,\mathcal{Q}) = 8^d\nu(\mathcal{Q})\lambda_{D,\mathcal{Q}}$, where $d=[K:\mathbb{Q}]$. Theorem 6.1 can be restated as follows.

Corollary 6.2. *We have*

$$\mathrm{sys}\pi_1(X_I) \ge \tfrac{4}{3}\log(g(X_I)) + \tfrac{4}{3}\log(32\pi) - \tfrac{4}{3}\log R(D,\mathcal{Q}) + o(1).$$

Thus, finding a family of principal congruence subgroups with the best systolic lower bound amounts to minimizing the expression $R(D,\mathcal{Q})$ over all orders.

Proof of Theorem 6.1. Clearly X_I is a cover of degree $[\Gamma\!:\!\Gamma(I)]$ of X_1, hence we have from Corollary 4.6 that

$$\begin{aligned} 4\pi(g(X_I)-1) &\le \mu(\Gamma(I)\backslash\mathcal{H}^2) \\ &= [\Gamma\!:\!\Gamma(I)]\cdot\nu \\ &\le \nu\lambda_{D,\mathcal{Q}}\cdot \mathrm{N}(I)^3 \end{aligned} \tag{6.2}$$

and so $\mathrm{N}(I) \ge \left(\frac{4\pi(g-1)}{\nu\lambda_{D,\mathcal{Q}}}\right)^{1/3}$ where $g=g(X_I)$ is the genus. Note that the first line in (6.2) is an equality if $\Gamma(I)$ is torsion free. Let $\pm1 \ne x\in\Gamma(I)$.

By (6.1) and Theorem 2.3, we have

$$\begin{aligned}
\ell_x &> 2\log\left(\left|\mathrm{Tr}_{\mathrm{M}_2(\mathbb{R})}\right|(x) - 1\right) \\
&> 2\log\left(\frac{1}{2^{2d-2}}\mathrm{N}(I)^2 - 3\right) \\
&> 2\log\left(\frac{1}{2^{2d-2}}\left(\frac{4\pi(g-1)}{\nu\lambda_{D,\mathcal{Q}}}\right)^{2/3} - 3\right) \\
&> 2\log\left(\frac{1}{2^{2d-2}}\left(\frac{4\pi g}{\nu\lambda_{D,\mathcal{Q}}}\right)^{2/3}\right) + o(1) \\
&= \frac{4}{3}\left[\log(g) - \left(\log(2^{3d-5}\pi^{-1}\nu\lambda_{D,\mathcal{Q}}) + o(1)\right)\right].
\end{aligned}$$

The constant can be somewhat improved by taking the stronger version of Theorem 2.3 into account. q.e.d.

Theorem 1.5 now follows immediately, since every arithmetic cocompact lattice of $\mathrm{SL}_2(\mathbb{R})$ is by definition commensurable to one of the lattices treated in Theorem 6.1.

To prove Theorem 1.8, let $F = \mathbb{C}$. Let K be a number field with one complex embedding and $d-2$ real ones, where $d = [K:\mathbb{Q}]$. As before, let

$$D = (a,b)_{2,K}$$

be a quaternion division algebra over K, and define $\mathcal{O}$, $\mathcal{Q}$ and κ as in Theorem 6.1. Let $\Gamma = \mathcal{Q}^1$, and set $X_1 = \Gamma\backslash\mathcal{H}^3$.

Theorem 6.3. *Let K be a number field of dimension d over $\mathbb{Q}$ with a single complex place, and let D, $\mathcal{O}$, $\mathcal{Q}$ and κ be as in Theorem 6.1. As before, let $\Gamma = \mathcal{Q}^1$. Let $I_0 \lhd O_K$ be an ideal such that $\Gamma(I_0)$ is torsion free (see Corollary 5.1), and set $X_1 = \Gamma(I_0)\backslash\mathcal{H}^3$.*

Then, the 3-manifolds $X_I = \Gamma(I)\backslash\mathcal{H}^3$, where $I \subseteq I_0$, satisfy

$$\mathrm{sys}\pi_1(X_I) \geq \frac{2}{3}\left[\log(\|X_I\|) - \left(\log(2^{3d-6}\|X_1\|\lambda_{D,\mathcal{Q}}) + o(1)\right)\right],$$

where $\lambda_{D,\mathcal{Q}}$ are defined as in (4.10), ranging over the primes of $T_1 \cup T_2$ which divide I.

Proof. We proceed as in the proof of Theorem 6.1. Since the simplicial volume is multiplicative under covers where the covered space is smooth, we have from Corollary 4.6 that

$$\begin{aligned}
\|X_I\| &= [\Gamma(I_0):\Gamma(I)]\cdot\|X_1\| \\
&\leq [\Gamma:\Gamma(I)]\cdot\|X_1\| \\
&\leq \|X_1\|\lambda_{D,\mathcal{Q}}\cdot\mathrm{N}(I)^3
\end{aligned}$$

and so $\mathrm{N}(I) \geq \left(\frac{\|X_I\|}{\|X_1\|\lambda_{D,\mathcal{Q}}}\right)^{1/3}$. Let $\pm 1 \neq x \in \Gamma(I)$. By (6.1) and Theorem 2.3, we have

$$\begin{aligned}
\ell_x &> 2\log\left(\left|\mathrm{Tr}_{\mathrm{M}_2(\mathbb{C})}\right|(x) - 1\right) \\
&> 2\log\left(\frac{1}{2^{d-2}}\mathrm{N}(I) - 3\right) \\
&> 2\log\left(\frac{1}{2^{d-2}}\left(\frac{\|X_I\|}{\|X_1\|\lambda_{D,\mathcal{Q}}}\right)^{1/3} - 3\right) \\
&> 2\log\left(\frac{1}{2^{d-2}}\left(\frac{\|X_I\|}{\|X_1\|\lambda_{D,\mathcal{Q}}}\right)^{1/3}\right) + o(1) \\
&= \frac{2}{3}\left[\log(\|X_I\|) - \left(\log(2^{3d-6}\|X_1\|\lambda_{D,\mathcal{Q}}) + o(1)\right)\right],
\end{aligned}$$

and again the constant may be improved by taking the stronger version of Theorem 2.3 into account. q.e.d.

Theorem 1.8 now follows, by the same argument as for Theorem 1.5. Corollary 1.9 follows from the fact that for a closed hyperbolic 3-manifold M, we have $\|M\| = \frac{\mathrm{vol}(M)}{v_3}$ where v_3 is the volume of a regular ideal simplex in $\mathcal{H}^3$.

7. The systole of Hurwitz surfaces

In this section, we specialize the results of Section 2 to the lattice Δ_H, defined as the even part of the group of reflections in the sides of the $(2,3,7)$ hyperbolic triangle. We follow the concrete realization of the $\mathbb{Z}/2\mathbb{Z}$-central extension $\tilde{\Delta}_H$ of Δ_H as the group of norm one elements in an order of a quaternion algebra, given by N. Elkies in [**El98**, p. 39] and in [**El99**, Subsection 4.4]. The $(2,3,7)$ case is is also considered in detail in [**MR03**, pp. 159–160].

Let K denote the real subfield of $\mathbb{Q}[\rho]$, where ρ is a primitive 7^{th} root of unity. Thus $K = \mathbb{Q}[\eta]$, where $\eta = \rho+\rho^{-1}$ has minimal polynomial $\eta^3+\eta^2-2\eta-1=0$. There are three embeddings of K into $\mathbb{R}$, defined by sending η to any of the numbers

$$2\cos\left(\tfrac{2\pi}{7}\right), 2\cos\left(\tfrac{4\pi}{7}\right), 2\cos\left(\tfrac{6\pi}{7}\right).$$

We view the first embedding as the 'natural' one, and denote the others by $\sigma_1, \sigma_2 : K \to \mathbb{R}$.

Now let D denote the quaternion K-algebra

$$(\eta,\eta)_K = K[i,j \mid i^2 = j^2 = \eta,\ ji = -ij].$$

The ring of integers of K is $O_K = \mathbb{Z}[\eta]$, and so this presentation satisfies the condition of Lemma 2.2.

Proposition 7.1. *The only two ramification places of D are the real embeddings σ_1 and σ_2.*

Proof. This fact is mentioned without proof in [**El99**, p. 96], and we provide the easy argument for the sake of completeness. The behavior of D over a real place is determined by the sign of η. Since $2\cos(2\pi/7)$ is positive, the algebra $D\otimes\mathbb{R}$ is a matrix algebra. On the other hand, the two conjugates $\sigma_1(\eta) = \eta^2 - 2 = 2\cos(4\pi/7)$ and $\sigma_2(\eta) = 2\cos(8\pi/7)$ are negative, and so $D\otimes_{\sigma_1}\mathbb{R}$ and $D\otimes_{\sigma_2}\mathbb{R}$ are division algebras.

Now let $\mathfrak{p}$ be a prime of K. If $\mathfrak{p}$ is odd, then the norm form

$$\lambda_1^2 - \eta\lambda_2^2 - \eta\lambda_3^2 + \eta^2\lambda_4^2$$

is a four dimensional form over the field $O_K/\mathfrak{p}$, so it represents zero non-trivially over $O_K/\mathfrak{p}$ [**Se73**, Prop. IV.4]. By Hensel's lemma, such a representation can be lifted to a representation over the completion $K_\mathfrak{p}$, and so $D\otimes K_\mathfrak{p}$ has elements of zero norm, which are clearly zero divisors; thus $D\otimes K_\mathfrak{p} \cong \mathrm{M}_2(K_\mathfrak{p})$.

A similar argument works for $\mathfrak{p} = \langle 2\rangle$. We note that the latter is the only even prime, since $O_K/\langle 2\rangle \cong \mathbb{F}_8$ is a field. The only refinement necessary for Hensel's lemma to apply is the fact that the form represents 0 modulo $\mathfrak{p}^3 = 8$:

$$1 - \eta(1+3\eta+\eta^2)^2 - \eta(\eta)^2 + \eta^2(0)^2 = -8(1+3\eta+\eta^2) \equiv 0 \pmod 8.$$

As an alternative to the computation modulo 8, one can deduce the behavior at $\mathfrak{p} = 2$ from the other places, via the quadratic reciprocity, which forces an even number of ramification places. q.e.d.

Let $\mathcal{O} \subseteq D$ be the order defined by (2.4), namely $\mathcal{O} = \mathbb{Z}[\eta][i,j]$. Fix the element $\tau = 1 + \eta + \eta^2$, and let

$$j' = \frac{1}{2}(1 + \eta i + \tau j).$$

Notice that j' is an algebraic integer of D, since the reduced trace is 1 while the reduced norm is

$$\frac{1}{4}(1 - \eta\cdot\eta^2 - \eta\cdot\tau^2 + \eta^2\cdot 0) = -1 - 3\eta,$$

so that both are in O_K. In particular

$$j'^2 = j' + (1 + 3\eta). \tag{7.1}$$

Definition 7.2. We define the Hurwitz quaternion order $\mathcal{Q}_{\mathrm{Hur}}$ by setting

$$\mathcal{Q}_{\mathrm{Hur}} = \mathbb{Z}[\eta][i,j,j']. \tag{7.2}$$

There is a discrepancy between the descriptions of a maximal order in [**El98**, p. 39] and in [**El99**, Subsection 4.4]. The maximal order according to [**El98**, p. 39] is $\mathbb{Z}[\eta][i,j,j']$. Meanwhile, in [**El99**, Subsection 4.4], the maximal order is claimed to be the order $\mathbb{Z}[\eta][i, j']$, described as $\mathbb{Z}[\eta]$-linear combinations of the elements 1, i, j', and ij' on the last line of page 94. The correct answer is the former, i.e., (7.2). More details may be found in [**KSV07**].

Obviously $\mathcal{Q}_{\mathrm{Hur}} \subseteq \frac{1}{2}\mathcal{O}$. Moreover since $\mathrm{Tr}_D(j') = 1$, this is the best possible choice for κ.

Lemma 7.3. *In the Hurwitz case, one has* $\lambda_{D,\mathcal{Q}_{\mathrm{Hur}}} = 1$.

Proof. Indeed, in (4.10), we have $T_1 = \emptyset$ since D has no finite ramification points by Proposition 7.1, while $T_2 = \emptyset$ since the Hurwitz order $\mathcal{Q}_{\mathrm{Hur}}$ is maximal. q.e.d.

Lemma 7.4. *The group* $\mathcal{Q}^1_{\mathrm{Hur}}(I)$ *is torsion-free for every proper ideal* $I \lhd O_K$.

Proof. Let $I \lhd O_K$ be a proper non-zero ideal, and assume $\mathcal{Q}^1_{\mathrm{Hur}}(I)$ is not torsion free. Taking into account the fact that O_K is a principal ideal domain, we have by Corollary 5.1 that I^2 divides an ideal of the form

$$\langle x^{-1}(x-1)^2 \rangle = \langle x + x^{-1} - 2 \rangle,$$

where x a root of unity for which $K[x]/K$ is a quadratic extension. For our field K, we must have $x^{14} = 1$, namely $x = \pm\rho^j$, $j = 1, \ldots, 6$. Now, the element

$$2 + (\rho + \rho^{-1}) = 2 + \eta,$$

as well as its Galois conjugates, is invertible in $\mathbb{Z}[\eta]$ (as $\eta(\eta-1)(\eta+2) = 1$), ruling out the cases $x = -\rho^j$. In all the remaining cases $I = \langle 2 - \eta \rangle$, since this ideal is stable under the Galois action (as $\sigma_1 : 2 - \eta \mapsto (2 - \eta)(2+\eta)$). However $\langle 2 - \eta \rangle$ is prime (of norm 7), so it cannot be divisible by I^2. q.e.d.

Proof of Theorem 1.10. For low genus, e.g., $g \leq 100$, one can verify directly that the Hurwitz surfaces satisfy the 4/3-bound. The Hurwitz surfaces with automorphism group of order up to a million were classified by M. Conder [**Con87**] using group theoretic arguments. The few surfaces of genus below 100 can be dealt with on a case by case basis. We list them in Table 7.1, together with their systoles and the bound $\frac{4}{3} \log g(X)$. Here a surface is called *simple* if its automorphism group is. A surface is called *real* if it admits an antiholomorphic involution. Thus, if a surface is non-real, then there are two distinct Riemann surfaces which are isometric as Riemannian manifolds. The systoles given in the table were calculated by R. Vogeler [**Vo03**, Appendix C], cf. [**Vo04**].

A comparison of the values in the last two columns, together with Lemma 7.4, verifies the validity of the 4/3-bound for these surfaces. The general case is treated below. q.e.d.

g	Automorphism Group	Type	Reality	Systole	Bound
3	PSL(2, 7)	simple	real	3.936	1.465
7	PSL(2, 8)	simple	real	5.796	2.595
14	PSL(2, 13)	simple	real	5.903	3.519
14	PSL(2, 13)	simple	real	6.887	3.519
14	PSL(2, 13)	simple	real	6.393	3.519
17	$(C_2)^3$.PSL(2, 7)	non-simple	non-real	7.609	3.778

Table 7.1. Hurwitz surfaces of genus ≤ 65.

Theorem 2.3 specializes to the following result.

Theorem 7.5. *Let $I \lhd \mathbb{Z}[\eta]$. For every $x \neq \pm 1$ in $\Delta_H(I)$ we have*

$$\left|\mathrm{Tr}_D(x)\right| > \frac{1}{16}\mathrm{N}(I)^2 - 2.$$

To complete the proof of Theorem 1.10, we let $X_I = \Delta_H(I) \backslash \mathcal{H}^2$. Combining this bound with (6.1) and (6.2), the fact that $\nu = \pi/21$, and applying Lemma 7.3, we obtain

$$\mathrm{sys}\pi_1(X_I) \quad > \quad 2\log\left(\left(\tfrac{21(g-1)}{16}\right)^{2/3} - 3\right),$$

which implies

$$\mathrm{sys}\pi_1(X_I) \geq \frac{4}{3}\log g(X_I)$$

if $g(X_I) \geq 65$.

References

[Ag06] I. Agol, *Systoles of hyperbolic 4-manifolds*, arXiv:math.DG/0612290.

[BB05] I. Babenko & F. Balacheff, *Géométrie systolique des sommes connexes et des revêtements cycliques*, Mathematische Annalen **333**(**1**) (2005) 157–180, MR 2169832.

[BCIK05] V. Bangert, C. Croke, S. Ivanov, & M. Katz, *Filling area conjecture and ovalless real hyperelliptic surfaces*, Geometric and Functional Analysis (GAFA) **15**(**3**) (2005) 577–597; see arXiv:math.DG/0405583, MR 2221144, Zbl 1082.53033.

[BaK03] V. Bangert & M. Katz, *Stable systolic inequalities and cohomology products*, Comm. Pure Appl. Math. **56** (2003) 979–997; available at the site arXiv:math.DG/0204181, MR 1990484, Zbl 1038.53031.

[BKSS06] V. Bangert, M. Katz, S. Shnider, & S. Weinberger, *E_7, Wirtinger inequalities, Cayley 4-form, and homotopy*, see arXiv:math.DG/0608006.

[Be04] M. Belolipetsky, *On volumes of arithmetic quotients of* $\mathrm{SO}(1,n)$, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **3**(**4**) (2004) 749–770; Addendum: preprint arXiv:math.NT/0610177, MR 2124587.

[Bo81] A. Borel, *Commensurability classes and volumes of hyperbolic* 3*-manifolds*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **8**(**1**) (1981) 1–33, MR 0616899, Zbl 0473.57003.

[Br99] R. Brooks, *Platonic surfaces*, Comment. Math. Helv. **74**(**1**) (1999) 156–170, MR 1677565, Zbl 0920.30037.

[BrM04] B. Brooks & E. Makover, *Random construction of Riemann surfaces*, J. Differential Geom. **68** (2004) 121–157, MR 2152911.

[BS94] P. Buser & P. Sarnak, *On the period matrix of a Riemann surface of large genus*, With an appendix by J. Conway and N. Sloane, Invent. Math. **117**(**1**) (1994) 27–56, MR 1269424, Zbl 0814.14033.

[ChW06] S. Chang & S. Weinberger, *Topological nonrigidity of nonuniform lattices*, Communications on Pure and Applied Mathematics **59** (2006).

[Coh61] H. Cohn, *Advanced number theory*, Reprint of A second course in number theory, 1962, Dover Books on Advanced Mathematics, Dover Publications, Inc., New York, 1980, MR 0594936, Zbl 0474.12002.

[Con87] M. Conder, *The genus of compact Riemann surfaces with maximal automorphism group*, Jour. of Alg. **108** (1987) 204–247, MR 0887205, Zbl 0614.20035.

[CrK03] C. Croke & M. Katz, *Universal volume bounds in Riemannian manifolds*, Surveys in Differential Geometry, **8**, Lectures on Geometry and Topology held in honor of Calabi, Lawson, Siu, and Uhlenbeck at Harvard University, May 3- 5, 2002, edited by S.-T. Yau (Somerville, MA: International Press, 2003), 109–137; see arXiv:math.DG/0302248, MR 2039987, Zbl 1051.53026.

[El98] N. Elkies, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), 1–47, Lecture Notes in Comput. Sci., **1423**, Springer, Berlin, 1998; see arXiv:math.NT/0005160, MR 1726059, Zbl 1010.11030.

[El99] ———, *The Klein quartic in number theory*, The eightfold way, 51–101, Math. Sci. Res. Inst. Publ., **35**, Cambridge Univ. Press, Cambridge, 1999, MR 1722413, Zbl 0991.11032.

[Fr99] M. Freedman, $\boldsymbol{Z}_2$*-Systolic-Freedom*, Geometry and Topology Monographs, **2**, Proceedings of the Kirbyfest (J. Hass, M. Scharlemann, eds.), 113–123, Geometry & Topology, Coventry, 1999, MR 1734404, Zbl 1024.53029.

[GP69] I. Gelfand, M. Graev, & I. Pyatetskii-Shapiro, *Representation theory and automorphic functions*, Reprint of the 1969 edition, Generalized Functions, **6**, Academic Press, Inc., Boston, MA, 1990, MR 1071179, Zbl 0718.11022.

[Gr81] M. Gromov, *Volume and bounded cohomology*, Publ. IHES. **56** (1981) 213–307, MR 0686042, Zbl 0516.53046.

[Gr83] ———, *Filling Riemannian manifolds*, J. Differential Geom. **18** (1983) 1–147, MR 0697984, Zbl 0515.53037.

[Gr96] ———, *Systoles and intersystolic inequalities*, Actes de la Table Ronde de Géométrie Différentielle (Luminy, 1992), 291–362, Sémin. Congr., **1**, Soc. Math. France, Paris, 1996; www.emis.de/journals/SC/1996/1/ps/smf_sem-cong_1_291-362.ps.gz, MR 1427763, Zbl 0877.53002.

[Gr99] ———, *Metric structures for Riemannian and non-Riemannian spaces*, Progr. in Mathematics, **152**, Birkhäuser, Boston, 1999, MR 1699320, Zbl 0953.53002.

[Ha06] M. Hamilton, *On the conformal systoles of four-manifolds*, Manuscripta Math. **121** (2006) 417–424; see arXiv:math.DG/0512127.

[HK02] U. Hamenstädt & R. Koch, *Systoles of a family of triangle surfaces*, Experiment. Math. **11**(**2**) (2002) 249–270, MR 1959267.

[Jo98] S. Johansson, *Genera of arithmetic Fuchsian groups*, Acta Arith. **86**(**2**) (1998) 171–191, MR 1654474, Zbl 0923.11067.

[K92] S. Katok, *Fuchsian groups*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1992, MR 1177168, Zbl 0753.30001.

[Ka03] M. Katz, *Four-manifold systoles and surjectivity of period map*, Comment. Math. Helv. **78** (2003) 772–786; see arXiv:math.DG/0302306, MR 2016695, Zbl 1048.53031.

[Ka06] ———, *Systolic inequalities and Massey products in simply-connected manifolds*, Israel J. Math., to appear; see arXiv:math.DG/0604012.

[Ka07] ———, *Systolic geometry and topology*, With an abstract by J. Solomon, Mathematical Surveys and Monographs **137** (2007), American Mathematical Society, Providence, RI.

[KS05] M. Katz & S. Sabourau, *Entropy of systolically extremal surfaces and asymptotic bounds*, Ergo. Th. Dynam. Sys. **25**(**4**) (2005) 1209–1220; available at arXiv:math.DG/0410312, MR 2158402.

[KSV07] M. Katz, M. Schaps, & U. Vishne, *Explicit computations in the Hurwitz quaternion order*, see arXiv:math.RA/0701137.

[Lub94] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, With an appendix by Jonathan D. Rogawski, Progress in Mathematics, **125**, Birkhäuser Verlag, Basel, 1994, MR 1308046, Zbl 0826.22012.

[MM05] E. Makover & J. McGowan, *The length of closed geodesics on random Riemann surfaces*, see arXiv:math.DG/0504175.

[MR03] C. Maclachlan & A. Reid, *The Arithmetic of Hyperbolic* 3*-Manifolds*, Graduate Texts in Math., **219**, Springer, 2003, MR 1937957, Zbl 1025.57001.

[OM62] T. O'Meara, *Introduction to quadratic forms*, Classics in Math., Springer, 1962, MR 0152507, Zbl 0107.03301.

[Pa95] P. Pansu, *Sous-groupes discrets des groupes de Lie: rigidité, arithméticité*, Séminaire Bourbaki, Vol. 1993/94, Astérisque **227** (1995), Exp. **778**(**3**) 69–105, MR 1321644, Zbl 0835.22011.

[Pi82] R. Pierce, *Associative Algebras*, Graduate Texts in Math., **88**, Springer, 1982, MR 0674652, Zbl 0497.16001.

[PR94] V. Platonov & A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure and Applied Math., **139**, Academic Press, 1994, MR 1278263, Zbl 0841.20046.

[Re75] I. Reiner, *Maximal Orders*, Academic Press, 1975, MR 0393100, Zbl 0305.16001.

[Sc94] P. Schmutz, *Congruence subgroups and maximal Riemann surfaces*, J. Geom. Anal. **4**(**2**) (1994) 207–218, MR 1277506, Zbl 0804.32010.

[Se73] J.-P. Serre, *A Course in Arithmetic*, Lecture Notes in Mathematics, **7**, 1973, MR 0344216, Zbl 0256.12001.

[Ta75] K. Takeuchi, *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan **27**(**4**) (1975) 600–612, MR 0398991, Zbl 0311.20030.

[Tu47] W. Tutte, *A family of cubical graphs*, Proc. Cambridge Philos. Soc. **43** (1947) 459–474, MR 0021678, Zbl 0029.42401.

[Vig80] M.-F. Vignéras, *Variétés riemanniennes isospectrales et non isométriques*, Ann. of Math. (2) **112**(**1**) (1980) 21–32, MR 0584073, Zbl 0445.53026.

[Vis07] U. Vishne, *Traces in congruence subgroups of arithmetic groups, and girth of Riemannian manifolds*, in preparation.

[Vo03] R. Vogeler, *On the geometry of Hurwitz surfaces*, Thesis, Florida State University, 2003.

[Vo04] ______, *Combinatorics of curves on Hurwitz surfaces*, Dissertation, University of Helsinki, Helsinki, 2004, Ann. Acad. Sci. Fenn. Math. Diss., **137**, 2004, MR 2061398, Zbl 1062.30050.

Department of Mathematics
Bar Ilan University
Ramat Gan 52900
Israel

E-mail address: katzmik@math.biu.ac.il

E-mail address: mschaps@math.biu.ac.il

E-mail address: vishne@math.biu.ac.il