

Fundamental Domains for Shimura Curves

David R. Kohel and Helena A. Verrill

Abstract

We describe a process for defining and computing a fundamental domain in the upper half plane $\mathcal{H}$ of a Shimura curve $X_0^D(N)$ associated to an order in a quaternion algebra $A/\mathbf{Q}$. A fundamental domain for $X_0^D(N)$ realizes a finite presentation of the quaternion unit group, modulo units of its center. We give explicit examples of domains for the curves $X_0^6(1)$, $X_0^{15}(1)$, and $X_0^{35}(1)$. The first example is a classical example of a triangle group and the second is a corrected version of that appearing in the book of Vignéras [13], due to Michon. These examples are also treated in the thesis of Alsina [1]. The final example is new and provides a demonstration of methods to apply when the group action has no elliptic points.

1 Introduction to Shimura curves

Let $A/\mathbf{Q}$ be a quaternion algebra, and let $\mathcal{O}/\mathbf{Z}$ be a maximal order in A . We say that A is indefinite if $A \otimes_{\mathbf{Q}} \mathbf{R}$ is isomorphic to the matrix algebra $\mathbf{M}_2(\mathbf{R})$. By fixing an isomorphism, we obtain an exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathcal{O}_+^* \longrightarrow \mathrm{PSL}_2(\mathbf{R}),$$

where $\mathcal{O}_+^*$ is the subgroup of units of positive norm, such that the image of $\mathcal{O}_+^*/\{\pm 1\}$ is a discrete subgroup of $\mathrm{PSL}_2(\mathbf{R})$. We define $\mathcal{H}$ to be the upper half complex plane, on which we identify $\mathrm{PSL}_2(\mathbf{R})$ with $\mathrm{Aut}(\mathcal{H})$ via the standard action by linear fractional transformations. We denote the image of $\mathcal{O}_+^*/\{\pm 1\}$ in $\mathrm{PSL}_2(\mathbf{R})$ by $\Gamma_0^D(1)$, where D is the discriminant of the algebra $A/\mathbf{Q}$, and define the Shimura curve $X_0^D(1)$ to be an algebraic model for the compactification of the quotient $\Gamma_0^D(1)\backslash\mathcal{H}$. An Eichler order of index N in $\mathcal{O}$ defines a subgroup of $\Gamma_0^D(1)$ which we denote by $\Gamma_0^D(N)$, with corresponding Shimura curve $X_0^D(N)$.

In the case of the split quaternion algebra $A = \mathbf{M}_2(\mathbf{Q})$ of discriminant $D = 1$, and maximal order $\mathcal{O} = \mathbf{M}_2(\mathbf{Z})$ we have the identification $\mathcal{O}_+^*/\{\pm 1\} = \mathrm{PSL}_2(\mathbf{Z})$. The compactification of $\Gamma_0^D(1)\backslash\mathcal{H}$ is obtained by adjoining the cusps of $\mathcal{H}$, and the Shimura curve $X_0^1(1)$ can be identified with the classical modular curve $X(1)$. An Eichler order of index N in $\mathbf{M}_2(\mathbf{Z})$ is conjugate to the ring of matrices upper triangular modulo N , and the family of curves $X_0^1(N)$ can be identified with the classical family of modular curves $X_0(N)$.

When the algebra A is nonsplit, the quotient $\Gamma_0^D(M)\backslash\mathcal{H}$ is already compact and the Shimura curves $X_0^D(M)$ provide a new class of curves whose Jacobians are related to those of the modular curves $X_0(N)$, where $N = DM$. While the structure of the groups $\Gamma_0(N)$ and the fundamental domains for their actions on $\mathcal{H}$ can be inferred from the group structure of $\mathrm{PSL}_2(\mathbf{Z})$ and the computation of cosets for the quotient $\mathrm{PSL}_2(\mathbf{Z})/\Gamma_0(N)$, for each discriminant D it is necessary to first compute anew the group structure and a fundamental domain for the base group $\Gamma_0^D(1)$ associated to a maximal order of discriminant D .

We note that the above construction depends explicitly on the choice of Eichler order and the choice of embedding in $\mathrm{PSL}_2(\mathbf{R})$. The former choice has minimal significance—every maximal order in an indefinite algebra is isomorphic, so we are free to choose one which is conveniently represented for computation. The embedding in $\mathrm{PSL}_2(\mathbf{R})$ is subject to uncountably many isomorphisms given by conjugation. We reduce the latter choice however to a choice of a real quadratic subfield K of A and a K -basis for A , by which we obtain an isomorphism $A \otimes_{\mathbf{Q}} K \cong \mathbf{M}_2(K)$. Choosing a real place v of K , the isomorphism $K_v \cong \mathbf{R}$, gives an isomorphism $A \otimes_{\mathbf{Q}} K_v \cong \mathbf{M}_2(\mathbf{R})$.

In the sequel we present computations of fundamental domains for several Shimura curves, with a description of the methods used. In the next section we discuss representations of quaternion algebras and the structure of units which we use for our computations. We follow with a review of hyperbolic geometry and group actions, sufficient to prove the correctness of our results. In the final section we give fundamental domains for the Shimura curves $X_0^6(1)$, $X_0^{15}(1)$, $X_0^{35}(1)$, of genera 0, 1, and 3, respectively, in terms of an explicit representation. The example $X_0^{35}(1)$ presents the initial obstacle that neither $\mathbf{Q}(\sqrt{-3})$ nor $\mathbf{Q}(\sqrt{-1})$ embeds in the algebra ramified at 5 and 7, so there exist no torsion elements in $\Gamma_0^{35}(N)$, hence no elliptic points to serve as base vertices for a fundamental domain.

The background material for this work follows closely the comprehensive book of Vignéras [13], to which we refer the reader for further information. In addition we note a strong overlap with the recent work of Alsina [1], who, in particular, computes fundamental domains for $X_0^6(1)$, $X_0^{10}(1)$, $X_0^{15}(1)$, and classifies certain CM points and other invariants of Shimura curves.

2 Representations of quaternion algebras

One defines a quaternion algebra A over a field K to be a central simple algebra of dimension four over K . The definition is often replaced by a constructive one, setting $A = K\langle x, y \rangle$, where x and y are generators satisfying relations $x^2 = a \neq 0$, $y^2 = b \neq 0$, and $xy + yx = 0$. In this study we restrict to the case of $K = \mathbf{Q}$, although much of what is said here for Shimura curves generalizes to totally real number fields.

As a first example, we consider the split quaternion algebra defined by $a = b = 1$. There exists an isomorphism:

$$\begin{aligned} K\langle x, y \rangle &\longrightarrow M_2(K) \\ x, y &\longmapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \end{aligned}$$

We say that a quaternion algebra isomorphic to a 2×2 matrix algebra is split.

A field L such that $A \otimes_K L \cong \mathbf{M}_2(L)$ is said to be a *splitting field* for a quaternion algebra A over K . A field extension L/K is a splitting field for A if and only if it contains a quadratic subfield which embeds in A . For any number

field K and quaternion algebra A over K there exist infinitely many quadratic splitting fields L/K of A up to isomorphism.

As a second example, we consider the quaternion algebra over K defined as above with a nonsquare in K , and take the splitting field $L = \mathbf{Q}(t)$, where $t^2 = a$. Then we obtain the splitting:

$$\begin{array}{ccc} A \otimes_K L = L\langle x, y \rangle & \xrightarrow{\quad\quad\quad} & M_2(L) \\ x, y \mapsto & \xrightarrow{\quad\quad\quad} & \begin{bmatrix} t & 0 \\ 0 & -t \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}. \end{array}$$

In the sequel we work with quaternion algebras over $\mathbf{Q}$ defined by such a presentation and choose a matrix representation of this form.

In the study of quaternion algebras A over a number field K , the splitting behaviour of A at the completions of K at the finite and infinite places serves to classify the algebra up to isomorphism. We say that A is split at a place v if $A_v = A \otimes_K K_v$ is isomorphic to a matrix algebra, and otherwise say that A is ramified at v . A nonsplit quaternion algebra over a local field is a division algebra which is unique up to isomorphism. A classical result for Brauer groups of number fields says that A is ramified at a finite, even number of places.

We define the reduced discriminant of a quaternion algebra over $\mathbf{Q}$ to be the product of the finite primes which ramify and say that A is indefinite or definite according to whether the prime at infinity is split or ramified.

3 Structure of units

We define the reduced trace $\text{Tr}(x)$ and reduced norm $N(x)$, respectively, of an element x of a quaternion algebra A to be the trace and determinant under any matrix representation of A . One easily verifies that these are elements of the center K , and that x satisfies a characteristic polynomial $x^2 - \text{Tr}(x)x + N(x) = 0$. Hereafter we omit the adjective reduced and refer to the trace, norm, and discriminant associated to A .

The existence of a quadratic characteristic polynomial for quaternion elements immediately implies that any element of a quaternion algebra $A/\mathbf{Q}$ not in the center must necessarily generate a quadratic extension. We can therefore classify the units in $\mathcal{O}_+^*$ as either torsion units, existing in some cyclotomic extension, or as lying in the free unit group of a real quadratic suborder of $\mathcal{O}$. In terms of the matrix representation of elements, it is standard to classify elements γ of $\text{PSL}_2(\mathbf{R})$ in terms of their trace as *elliptic* ($|\text{Tr}(\gamma)| < 2$), *parabolic* ($|\text{Tr}(\gamma)| = 2$), or *hyperbolic* ($|\text{Tr}(\gamma)| > 2$).

According to this classification, the elliptic elements have one fixed point in $\mathcal{H}$, while parabolic and hyperbolic elements have one and two fixed points, respectively, which are cuspidal—that is, in the boundary $\mathbb{P}^1(\mathbf{R})$ of $\mathcal{H}$. In the case of nonsplit quaternion unit groups $\mathcal{O}_+^*$, we find that nontrivial parabolic elements do not exist, and the distinction between elliptic and hyperbolic elements is precisely that of cyclotomic and real quadratic units. In particular we

note that in a quaternion algebra over $\mathbf{Q}$ the only cyclotomic units are those coming from embeddings of the fields $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(\sqrt{-1})$.

In addition to the units in $\mathcal{O}_+^*/\{\pm 1\}$ we introduce elements of the normalizer group $\mathcal{N}(\Gamma_0^D(1))$ of $\Gamma_0^D(1)$ in $\mathrm{PSL}_2(\mathbf{R})$. We can find nontrivial elements of $\mathcal{N}(\Gamma_0^D(1))$ using the following lemma.

Lemma 3.1. *Let p be a prime divisor of $D = \mathrm{disc}(A)$. If π_p is an element of $\mathcal{O}$ of norm p then $\pi_p \mathcal{O} \pi_p^{-1} = \mathcal{O}$, and the image of π_p is in $\mathcal{N}(\Gamma_0^D(1))$.*

Proof. For a prime $\ell \neq p$ we have $\pi_p \mathcal{O}_\ell \pi_p^{-1} = \mathcal{O}_\ell$ since π_p is a unit in $\mathcal{O}_\ell$, so the result holds locally at such primes. At the ramified prime p , the order $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ is the unique maximal order, defined by

$$\mathcal{O}_p = \{\alpha \in A_p \mid v_p(N(\alpha)) \geq 0\}.$$

Since the norm is multiplicative, it follows that $\pi_p x \pi_p^{-1} \in \mathcal{O}_p$ for all x in $\mathcal{O}_p$. The local-global correspondence for lattices in A implies that the result holds globally. $\square$

More generally the quotient $\mathcal{N}(\Gamma_0^D(1))/\Gamma_0^D(1)$ is known to be an elementary 2-abelian group, generated precisely by elements of this form.

Lemma 3.2. *The group $\mathcal{N}(\Gamma_0^D(1))/\Gamma_0^D(1)$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^m$, where m is the number of prime divisors of D , and is generated by any set of elements $\{\pi_{p_i} \in \mathcal{O} \mid N(\pi_{p_i}) = p_i\}$, where $p_1, \dots, p_m$ are the prime divisors of D .*

Proof. See Michon [10] or Vignéras [13, Ch IV.B] $\square$

If the trace of an element π_p is zero then we obtain a new elliptic element in $\mathcal{N}(\Gamma_0^D(1))$. Thus when $\Gamma_0^D(1)$ fails to have elliptic elements we may exploit the existence of elliptic points of the normalizer to build a fundamental domain for the group $\Gamma_0^D(1)$ such that the vertices are distinguished points of the curve $X_0^D(1)$.

As our computational model, we make an explicit identification of $\mathrm{PGL}_2^+(\mathbf{R})$ with $\mathrm{PSL}_2(\mathbf{R})$ so that for a fixed quadratic splitting field $K/\mathbf{Q}$, we may represent an element π of the normalizer by an element of $\mathrm{PGL}_2^+(K)$, without extending K to by the square roots $\sqrt{p_i}$.

We are able to generate “random” units in $\mathcal{O}_+^*$ by searching for fundamental units of real quadratic suborders, which may have norm 1 or -1 . The search for elements π_p of norm p in $\mathcal{O}$ is facilitated by taking the product of an element of norm $-p$ with any unit in $\mathcal{O}^*$ of norm -1 , whose existence is proved by the following lemma.

Lemma 3.3. *An Eichler order in a indefinite quaternion algebra over $\mathbf{Q}$ contains a unit of norm -1 .*

Proof. We define the *discriminant form* to be the form $\mathrm{Tr}(x)^2 - 4N(x)$ on $\mathcal{O}/\mathbf{Z}$. This form is a ternary quadratic form of discriminant $4\mathrm{disc}(\mathcal{O})$, which represents the discriminants of the quadratic subrings $\mathbf{Z}[x]$ in $\mathcal{O}$ (see Chapter 6

of Kohel [5]). It suffices to show that the discriminant form represents a prime p congruent to 1 mod 4, since then $\mathcal{O}$ contains a real quadratic order of discriminant p , whose fundamental unit has norm -1 . Since $\mathcal{O}$ is an Eichler order it is either ramified and maximal or locally isomorphic an upper triangular matrix algebra at each finite prime. In both cases, the discriminant form is not zero modulo any prime p , in particular represents the class of 1 mod 4, and by the assumption that $\mathcal{O}$ is indefinite, represents both 1 and -1 at infinity. It follows that the discriminant form admits a representation of a primitive indefinite quadratic form which represents 1 mod 4. By the Chebotarev density theorem, this latter form represents a positive density of primes 1 mod 4, and the result holds. $\square$

We note that the lemma is false if $\mathcal{O}$ is not an Eichler order. For example, if $\mathcal{O}$ is nonmaximal at a ramified prime $p \equiv 3 \pmod{4}$, then the discriminant form is not primitive, as it represents only integers congruent to 0 mod p , and no quadratic order of this discriminant contains a unit of norm -1 . The lemma also fails for a quaternion order of the form $\mathbf{Z} + 4\mathcal{O}$, whose norm form represents only integers congruent to 0 or 1 mod 4.

4 Hyperbolic geometry and group action

The metric on $\mathcal{H}$ defines a volume measure which permits the effective computation of volumes of hyperbolic polygons (see Vignéras [13, Ch. IV]). We define the arithmetic volume of such a region to be $1/(2\pi)$ times its hyperbolic volume. If the region is a fundamental domain of any discrete group acting on $\mathcal{H}$ such that $\Gamma \backslash \mathcal{H}^*$ is compact then the arithmetic volume is a rational number. In particular we have the following formula for this quantity when $\Gamma = \Gamma_0^D(1)$.

Lemma 4.1. *The arithmetic volume of $\Gamma_0^D(1)$ is given by*

$$|\text{vol}(\mathcal{F})| = \frac{1}{6} \prod_{p|D} (p-1).$$

Proof. See Vignéras [13], Lemme IV.3.1. $\square$

Let Γ be an discrete co-compact subgroup of $\text{PSL}_2(\mathbf{R})$ and let $e_n(\Gamma)$ be the number of elliptic points $\bar{z}$ of $\Gamma \backslash \mathcal{H}$ such that $|\{\gamma \in \Gamma \mid \gamma(z) = z\}| = n$ where z is any representative of $\bar{z}$ in $\mathcal{H}$.

Lemma 4.2. *The arithmetic volume of a fundamental domain $\mathcal{F}$ for Γ satisfies the following relation:*

$$|\text{vol}(\mathcal{F})| = 2g(\Gamma) - 2 + \sum_{n \geq 1} \frac{n-1}{n} e_n(\Gamma),$$

where $g(\Gamma)$ is the genus of the Riemann surface $\Gamma \backslash \mathcal{H}$.

Proof. See Vignéras [13], Proposition IV.2.10. $\square$

Lemma 4.3. *The numbers e_n of elliptic elements for $\Gamma_0^D(1)$ satisfy the identities:*

$$e_2 = \prod_{p|D} \left(1 - \left(\frac{-4}{p}\right)\right), \quad e_3 = \prod_{p|D} \left(1 - \left(\frac{-3}{p}\right)\right),$$

and $e_n = 0$ for all n greater than 3. The numbers e_n for $\mathcal{N}(\Gamma_0^D(1))$ are zero except for n in $\{1, 2, 3, 4, 6, 8, 12\}$.

Proof. See Vignéras [13, Ch. IV.A-B]. $\square$

We now generalize the formulas for the numbers of elliptic points to include their normalizers.

Lemma 4.4. *Let γ be an elliptic element of order $n > 1$ in $\mathcal{N}(\Gamma_0^D(1))$, and identify γ with a representative in $\mathcal{O} \cap A_+^*$ of square-free integral norm m . Then m divides D and the possible combinations for the subring $R = \mathbf{Z}[\gamma] \subset \mathcal{O}$, the minimal polynomial $f(x)$ of γ , and the integers m and n are given in the following table.*

R	$f(x)$	m	n
$\mathbf{Z}[\sqrt{-m}]$	$x^2 + m$		2
$\mathbf{Z}[\sqrt{-1}]$	$x^2 + 1$	$m \neq 2$	2
	$x^2 + 2x + 2$	$m = 2$	4
$\mathbf{Z}[(1 + \sqrt{-3})/2]$	$x^2 \pm x + 1$	$m \neq 3$	3
	$x^2 \pm 3x + 3$	$m = 3$	6

Proof. The projective normalization $\mu = \gamma/\sqrt{m}$ in $A \otimes_{\mathbf{Q}} \mathbf{R}$ of an elliptic element γ in $\mathcal{N}(\Gamma_0^D(1))$ of norm m is a root of unity. On the other hand, the square of this element is an element of $\mathcal{O}_+^* = \Gamma_0^D(1)$ and so is quadratic over $\mathbf{Z}$. Therefore the normalized element μ is contained in the biquadratic extension $\mathbf{Q}[\sqrt{m}, \alpha]$. The possible roots of unity are those of order 1, 2, 3, 4, 6 or 12, giving rise to elliptic elements of projective order 1, 2, 3, or 6. It follows that the possible rings and minimal polynomials for γ are those specified. $\square$

For a prime p dividing the discriminant of A , a p -orientation on a maximal order $\mathcal{O}$ is a homomorphism $\mathcal{O} \rightarrow \mathbf{F}_{p^2}$. An embedding $R \subset \mathcal{O}$ is said to be optimal if $\mathcal{O}/R$ is torsion free, and an orientation distinguishes two embeddings of R into $\mathcal{O}$ which do not commute with a collection of p -orientations on $\mathcal{O}$ for each prime p dividing the discriminant D . As a special case of Corollaire III.5.12 in Vignéras [13], the number $r_n(\mathcal{O}, R)$ of optimal, oriented embeddings of a quadratic subring R in $\mathcal{O}$ is given by

$$r_n(\mathcal{O}, R) = h(R) \prod_{p|D} \left(1 - \left(\frac{d_R}{p}\right)\right),$$

where d_R is the discriminant of R . We can now express the number of elliptic points for a group $\mathcal{N}(\Gamma_0^D(1)) < G < \Gamma_0^D(1)$ in terms of these invariants.

Theorem 4.5. *Let G be an extension of $\Gamma = \Gamma_0^D(1)$ contained in $\mathcal{N}(\Gamma_0^D(1))$. Then the invariants $e_n(G)$ are given by the following formula:*

$$e_n(G) = \frac{1}{[G : \Gamma]} \sum_R \delta_n(G, R) r_n(\mathcal{O}, R)$$

where the sum is over all imaginary quadratic orders and where

$$\begin{aligned} \delta_2(G, R) &= \begin{cases} 2 & \text{if } -3, -4 \neq d_R \in \{-m, -4m\} \text{ and } \pi_m \in G, \\ 1 & \text{if } d_R = -4 \text{ and } \pi_2 \notin G, \\ 0 & \text{otherwise;} \end{cases} \\ \delta_3(G, R) &= \begin{cases} 1 & \text{if } d_R = -3 \text{ and } \pi_3 \notin G, \\ 0 & \text{otherwise;} \end{cases} \\ \delta_4(G, R) &= \begin{cases} 2 & \text{if } d_R = -4 \text{ and } \pi_2 \in G, \\ 0 & \text{otherwise;} \end{cases} \\ \delta_6(G, R) &= \begin{cases} 2 & \text{if } d_R = -3 \text{ and } \pi_3 \in G, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Proof. This follows from the classification of elliptic elements in Lemma 4.4 and consideration of the ramification of the cover $\Gamma_0^D(1) \backslash \mathcal{H} \rightarrow G \backslash \mathcal{H}$. $\square$

5 Examples

We present here examples of fundamental domains for $\Gamma_0^6(1)$, $\Gamma_0^{15}(1)$, and $\Gamma_0^{35}(1)$. This provides the base case from which domains for the families of subgroups $\Gamma_0^D(N)$ can be studied. We note, however, that even within the collection of groups $\Gamma_0^D(1)$ associated to the maximal orders in rational quaternion algebras the genus of the Shimura curve $X_0^D(1)$ may be arbitrarily large. For reference we display in Figure 1 the initial genera of the Shimura curves of discriminant D and index 1.

5.1 Fundamental domain for $\Gamma_0^6(1)$.

The group $\Gamma_0^6(1)$ is a well-known triangle group in the literature. This group is treated in Alsina [1], where one also finds an explicit description of a fundamental domain. Ihara proved that, as an abstract curve, $X_0^6(1)$ is isomorphic to the conic $X^2 + Y^2 + 3Z^2 = 0$, as reported in Kurihara [9]. Elkies [4] determines equations for the quotient curve associated to the normalizer, and also treats several examples of the subgroups $\mathcal{N}(\Gamma_0^6(\ell))$ for small primes ℓ .

We apply Lemma 4.5 to compute the elliptic invariants for each of the extensions groups G with image W in $\mathcal{N}(\Gamma_0^6(1))/\Gamma_0^6(1) = \langle \bar{\pi}_2, \bar{\pi}_3 \rangle$, and present this information with the genus and volume data in the following table. The elliptic points will be explicitly determined as part of the fundamental domain computation.

D	$g_0^D(1)$	D	$g_0^D(1)$	D	$g_0^D(1)$	D	$g_0^D(1)$	D	$g_0^D(1)$
6	0	46	1	87	5	129	7	166	6
10	0	51	3	91	7	133	9	177	9
14	1	55	3	93	5	134	6	178	7
15	1	57	3	94	3	141	7	183	11
21	1	58	2	95	7	142	5	185	13
22	0	62	3	106	4	143	11	187	13
26	2	65	5	111	7	145	9	194	9
33	1	69	3	115	7	146	7	201	11
34	1	74	4	118	4	155	11	202	8
35	3	82	3	119	9	158	7	203	15
38	2	85	5	122	6	159	9	205	13
39	3	86	4	123	7	161	11	206	9

Table 1: Genera of Shimura groups $\Gamma_0^D(1)$.

W	$g_0^6(1)$	e_2	e_3	e_4	e_6	$ \text{vol}(\mathcal{F}) $
$\langle 1 \rangle$	0	2	2	0	0	1/3
$\langle \pi_2 \rangle$	0	0	1	2	0	1/6
$\langle \pi_3 \rangle$	0	1	0	0	2	1/6
$\langle \pi_6 \rangle$	0	3	1	0	0	1/6
$\langle \pi_2, \pi_3 \rangle$	0	1	0	1	1	1/12

Figure 1: Genus and invariant data for extensions of $\Gamma_0^6(1)$.

We define a presentation of the quaternion algebra $A = \mathbf{Q}\langle x, y \rangle$ of discriminant 6 by the relations $x^2 = 2$, $y^2 = -3$, and $xy = -yx$, and let $\mathcal{O}$ be the $\mathbf{Z}$ -module with basis $\{1, (x+z)/2, (1+y)/2, z\}$. The module $\mathcal{O}$ is immediately verified to be closed under multiplication and forms a maximal order of A since the discriminant of its norm form is 6^2 (see Lemme I.4.7 and Corollaire I.4.8 of Vigneras [13] for the computational construction and Corollaire III.5.3 for its value). We introduce a representation $A \rightarrow \mathbf{M}_2(\mathbf{R})$ given by

$$x \mapsto \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ -3 & 0 \end{pmatrix}, \quad z \mapsto \begin{pmatrix} 0 & \sqrt{2} \\ 3\sqrt{2} & 0 \end{pmatrix},$$

under which $\Gamma_0^6(1)$ acts on $\mathcal{H}$.

Without further ado, we begin by writing down a system of units in $\Gamma_0^6(1)$:

$$\begin{aligned} \gamma_1 &= (x + 2y - z)/2, & \gamma_3 &= (1 + y)/2, \\ \gamma_2 &= (x - 2y + z)/2, & \gamma_4 &= (1 + 3y - 2z)/2. \end{aligned} \tag{1}$$

and note that they satisfy the elementary relations:

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^3 = \gamma_4 \gamma_2 \gamma_3 \gamma_1 = 1. \tag{2}$$

We moreover define the elements π_2 , π_3 , and π_6 of the normalizer $\mathcal{N}(\Gamma_0^6(1))$ by:

$$\pi_2 = (-2 + x + 2y - z)/2, \quad \pi_3 = (3 + y)/2, \quad \pi_6 = 2y - z. \quad (3)$$

Together with the identity, these elements form a set of coset representatives for the quotient $\mathcal{N}(\Gamma_0^6(1))/\Gamma_0^6(1)$, and satisfy the additional projective relations:

$$\pi_2^2 = \gamma_1, \quad \pi_3^2 = \gamma_3, \quad \pi_6^2 = 1 \text{ and } \pi_2 = \pi_6\pi_3. \quad (4)$$

Here by projective relation we mean that the relation holds up to some element of $\mathbf{Q}^*$. We note that all of the above relations are verified by elementary means and are independent of any matrix representation or embedding in $\text{PSL}_2(\mathbf{R})$.

With respect to the chosen representation we define the points a , b , and c to be the fixed points of the elements γ_4 , $\gamma_2\pi_3^2\pi_6$, and γ_2 , respectively—specifically these are the points:

$$a = \frac{(-2\sqrt{2} + 3)\sqrt{-3}}{3}, \quad b = \frac{(4\sqrt{2} - 5)(3 + 2\sqrt{-3})}{21}, \quad c = \frac{(\sqrt{2} - 1)(1 + \sqrt{-2})}{3}.$$

From these points we define $b' = -\bar{b}$ and $c' = -\bar{c}$ to be the reflections around the imaginary axis, and define elements d , d' , and e by $d' = \pi_6b$, $d = \pi_6b'$, and $e = \pi_6a$.

Theorem 5.1. *The hyperbolic polygon $\mathcal{F}$ with vertices $(a, b, c, d, e, d', c', b', a)$ is a fundamental domain for $\Gamma_0^6(1)$. The polygon $\mathcal{F}_0$ with vertices (a, b, c, t) , where $t = (\sqrt{2} - 1)\sqrt{-3}/3$ is a fixed point of the elliptic element π_6 , is a fundamental domain for $\mathcal{N}(\Gamma_0^6(1))$.*

Proof. The edge gluing relations for the domains $\mathcal{F}$ and $\mathcal{F}_0$ are determined by the equations (1) and (3), as can be directly verified. A volume computation shows that the volumes ~ 0.3333 and ~ 0.08333 agree with the known values of $1/3$ and $1/12$ for $\Gamma_0^6(1)$ and $\mathcal{N}(\Gamma_0^6(1))$ in Figure 1, from which it follows that the polygons are not the union of multiple domains. $\square$

From the gluing relations on the edges of the fundamental domains we obtain the following corollary. We note that essentially the same presentation for $\mathcal{N}(\Gamma_0^6(1))$, describing $\mathcal{N}(\Gamma_0^6(1))$ as a triangle group, appears in Elkies [4].

Corollary 5.2. *The generators (1) with relations (2) give a finite presentation for the group $\Gamma_0^6(1)$. The generators π_3 and π_6 with relations*

$$\pi_3^6 = \pi_6^2 = (\pi_6\pi_3)^4 = 1$$

give a finite presentation for the group $\mathcal{N}(\Gamma_0^6(1))$.

The content of the previous theorem is summarized graphically in Figure 2, which shows a fundamental domain $\mathcal{F}$ for $\Gamma_0^6(1)$. The subdivisions define four constituent fundamental domains $\mathcal{F}_0$, $\pi_2\mathcal{F}_0$, $\pi_3\mathcal{F}_0$, and $\pi_6\mathcal{F}_0$ for the normalizer $\mathcal{N}(\Gamma_0^6(1))$, with boundary geodesics formed by the imaginary axis and a bisecting arc stabilized by π_2 . The edge gluing relations are indicated by the arrows, and the actions of the π_m are determined by their relations (4) and the indicated mapping on the constituent subdomains of $\mathcal{F}$.

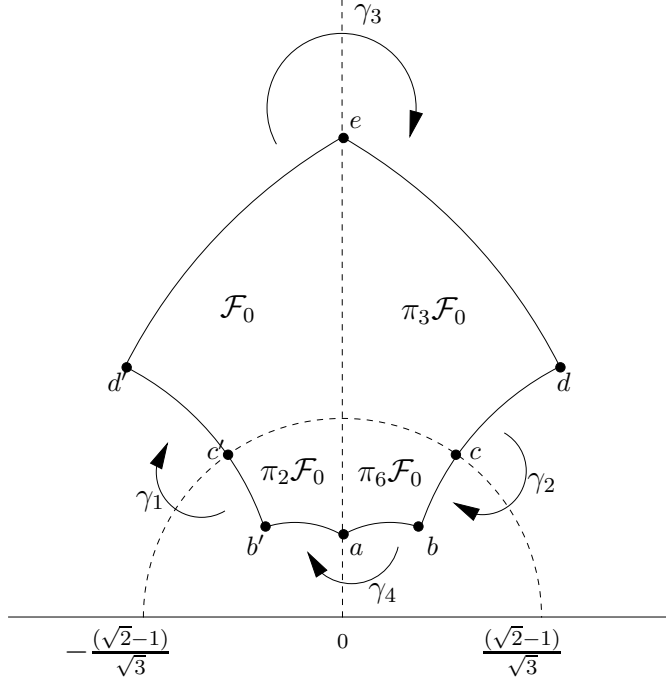


Figure 2: Fundamental domain for $\Gamma_0^6(1)$.

5.2 Fundamental domain for $\Gamma_0^{15}(1)$.

A fundamental domain for $\Gamma_0^{15}(1)$ and $\mathcal{N}(\Gamma_0^{15}(1))$, due to Michon, appears Vignéras [13], IV.3.C. The domain given below is normalized to be defined over the splitting field $\mathbf{Q}(\sqrt{3})$, to be computationally more effective than the biquadratic field $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ of Michon, and corrects errors in the book of Vignéras. A similar corrected example also appears in the thesis of Alsina [1], also over the splitting field $\mathbf{Q}(\sqrt{3})$.

We take the quaternion algebra of discriminant 15 presented by $A = \mathbf{Q}\langle x, y \rangle$ with the relations $x^2 = 3$, $y^2 = 5$, and $xy = -yx$, and choose the maximal order $\mathcal{O}$ having basis $\{1, x, (1+y)/2, (x+z)/2\}$. As with the previous example the maximality of $\mathcal{O}$ is verified by showing that the discriminant of the associated norm form is 15^2 . We embed A in $\mathbf{M}_2(\mathbf{R})$ by taking

$$x \mapsto \begin{pmatrix} \sqrt{3} & 0 \\ 0 & -\sqrt{3} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 5 & 0 \end{pmatrix}, \quad z \mapsto \begin{pmatrix} 0 & \sqrt{3} \\ -5\sqrt{3} & 0 \end{pmatrix}.$$

The elliptic invariants and genus are given by Lemmas 4.2 and 4.5 for each of the extensions groups G with image W in $\mathcal{N}(\Gamma_0^{15}(1))/\Gamma_0^{15}(1) = \langle \bar{\pi}_3, \bar{\pi}_5 \rangle$, and present this information with the genus and volume data in Figure 3. With respect to this embedding, we obtain a fundamental domain $\mathcal{F}$ for $\Gamma_0^{15}(1)$, pictured in Figure 4.

W	$g_0^{15}(1)$	e_2	e_3	e_4	e_6	$ \text{vol}(\mathcal{F}) $
$\langle 1 \rangle$	1	2	0	0	0	$4/3$
$\langle \bar{\pi}_3 \rangle$	0	2	0	0	2	$2/3$
$\langle \bar{\pi}_5 \rangle$	1	0	1	0	0	$2/3$
$\langle \bar{\pi}_{15} \rangle$	0	4	1	0	0	$2/3$
$\langle \bar{\pi}_3, \bar{\pi}_5 \rangle$	0	3	0	0	1	$1/3$

Figure 3: Genus and invariant data for extensions of $\Gamma_0^{15}(1)$.

In the figure, points a, b, c are given by

$$a = \frac{(t+3)(-5+\sqrt{-5})}{30}, \quad b = \frac{(t+2)(-2+\sqrt{-1})}{5}, \quad c = \frac{(t+2)(2+\sqrt{-1})}{5}.$$

All the other vertices of the domain can be given in terms of these points, and in clockwise order around the domain, the vertices of $\mathcal{F}$ are given by

$$\{a, b, c, \gamma_2 a, \gamma_3^{-1} \gamma_2 a, \gamma_1 c, \gamma_1 b, \gamma_2^{-1} \gamma_3^{-1} \gamma_2 a\}.$$

Theorem 5.3. *The region $\mathcal{F}$ is a fundamental domain for $\Gamma_0^{15}(1)$ associated to the generators*

$$\begin{aligned} \gamma_1 &= 2 - x, & \gamma_3 &= (4 + 3x - z)/2, \\ \gamma_2 &= (3 + y)/2, & \gamma_4 &= (4 + 3x + z)/2, \end{aligned}$$

which provides $\Gamma_0^{15}(1)$ with the presentation

$$\Gamma_0^{15}(1) \cong \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4 \mid (\gamma_3 \gamma_1)^3 = (\gamma_4 \gamma_1)^3 = \gamma_3 \gamma_2 \gamma_4^{-1} \gamma_2^{-1} = 1 \rangle.$$

Proof. The relations can be verified directly. The points b and c are taken to be the fixed points of $\gamma_4 \gamma_1$ and $\gamma_3 \gamma_1$ respectively, and with this choice it can then be seen that all the edge identifications of $\mathcal{F}$ are given by $\gamma_1, \gamma_2, \gamma_3, \gamma_4$, as indicated in the figure. We compute the volume of the region to be ~ 1.3333 , which agrees with the expected value of $2/3$. The verification of the relations, together with the computation of the volume shows that the region given is indeed a fundamental domain for $\Gamma_0^{15}(1)$. $\square$

A set of coset representatives for $\mathcal{N}(\Gamma_0^{15}(1))/\Gamma_0^{15}(1)$ is given by 1 and

$$\pi_3 = (x + z)/2, \quad \pi_5 = (5 + y)/2, \quad \pi_{15} = z,$$

which satisfy the projective relations:

$$\pi_3^2 = \pi_{15}^2 = 1, \quad \pi_5 \pi_3 = \pi_{15}.$$

Theorem 5.4. *A fundamental domain for $\mathcal{N}(\Gamma_0^{15}(1))$ can be given by a region $\mathcal{F}_0$ having vertices*

$$\{b, \gamma_1^{-1} \pi_3 a, \pi_3 a, \gamma_1 b\}.$$

Moreover $\mathcal{N}(\Gamma_0^{15}(1))$ is generated by the γ_1, π_3 , and π_{15} , and has a presentation

$$\mathcal{N}(\Gamma_0^{15}(1)) \cong \langle \gamma_1, \pi_3, \pi_{15} \mid \pi_{15}^2 = \pi_3^2 = (\gamma_1 \pi_{15})^2 = (\gamma_1 \pi_3)^6 = 1 \rangle.$$

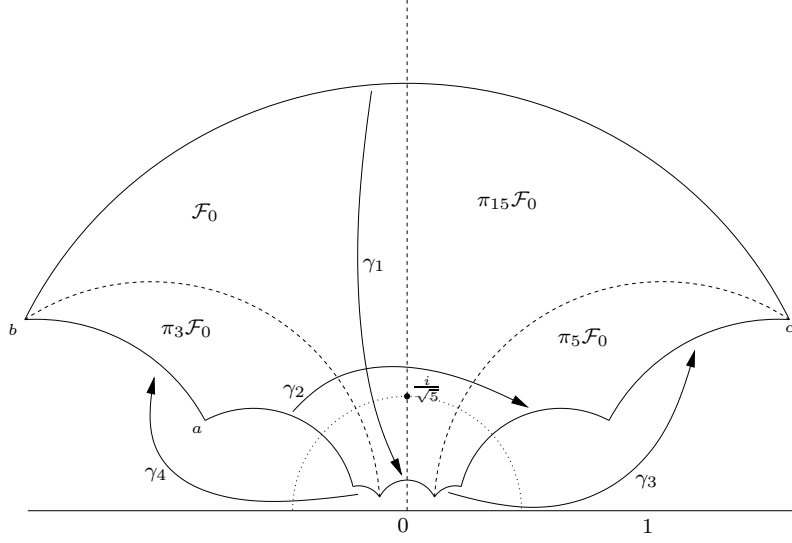


Figure 4: Fundamental domain for $\Gamma_0^{15}(1)$ and its normalizer.

Proof. To verify that $\mathcal{F}_0$ is a fundamental domain for the normaliser we simply note that the edges are identified by elements in the normaliser, and that precisely four copies of this domain give the domain for $\Gamma_0^{35}(1)$, which means this is a domain for a subgroup of the normalizer containing $\Gamma_0^{35}(1)$ with index 4, but we know that 4 is the index of $\Gamma_0^{35}(1)$ in $\mathcal{N}(\Gamma_0^{35}(1))$. Here we are using the fact that a is the fixed point of $\pi_3\pi_{15}^{-1}\gamma_1^{-1}\pi_3^{-1}$, in addition to the choices of b and c as being elliptic points for $\Gamma_0^{35}(1)$. $\square$

Figure 4 shows the domain $\mathcal{F}$ for $\Gamma_0^{35}(1)$ divided by the dashed lines into four fundamental domains for $\mathcal{N}(\Gamma_0^{35}(1))$. These dividing lines are lines from vertices b to $\gamma_1 b$, and from c to $\gamma_1 c$, which are lines stabilised by π_3 and $\gamma_2\pi_3$ respectively, and the imaginary axis.

6 The fundamental domain for $\Gamma_0^{35}(1)$.

For the case of $D = 35$, we take the quaternion algebra of discriminant 35 presented by $A = \mathbf{Q}\langle x, y \rangle$, with the relations $x^2 = 5$, $y^2 = 7$, and $xy = -yx$, and choose the maximal order $\mathcal{O}$ having basis $\{1, (1+x)/2, (y+z)/2, z\}$. As in the previous examples, the maximality of this order is proved by verifying that the discriminant is 35^2 . We embed A in $\mathbf{M}_2(\mathbf{R})$ by taking

$$x \mapsto \begin{pmatrix} \sqrt{5} & 0 \\ 0 & -\sqrt{5} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 7 & 0 \end{pmatrix}, \quad z \mapsto \begin{pmatrix} 0 & \sqrt{5} \\ -7\sqrt{5} & 0 \end{pmatrix}.$$

The elliptic invariants and genus are given by Lemmas 4.2 and 4.5 for each of the extensions groups G with image W in $\mathcal{N}(\Gamma_0^{35}(1))/\Gamma_0^{35}(1) = \langle \bar{\pi}_5, \bar{\pi}_7 \rangle$, and present the genus and volume data in Figure 5. Figure 6 shows a fundamental

W	g	e_2	e_3	e_4	e_6	$ \text{vol}(\mathcal{F}) $
$\langle 1 \rangle$	3	0	0	0	0	4
$\langle \bar{\pi}_5 \rangle$	2	0	0	0	0	2
$\langle \bar{\pi}_7 \rangle$	1	4	0	0	0	2
$\langle \bar{\pi}_{35} \rangle$	0	8	0	0	0	2
$\langle \bar{\pi}_5, \bar{\pi}_7 \rangle$	0	6	0	0	0	1

Figure 5: Genus and invariant data for extensions of $\Gamma_0^{35}(1)$.

domain for $\Gamma_0^{35}(1)$ with respect to this embedding. In much the same way as in the previous examples, we have the following theorem:

Theorem 6.1. *The group $\Gamma_0^{35}(1)$ is generated by elements*

$$\begin{aligned} \gamma_1 &= 7 + 2x - 2y & \gamma_3 &= (11 + x - 4y)/2 & \gamma_5 &= (12 + 5y + z)/2 \\ \gamma_2 &= 7 - 2x - 2y & \gamma_4 &= (11 - x - 4y)/2 & \gamma_6 &= (12 + 5y - z)/2 \\ & & \gamma_7 &= (3 - x)/2 \end{aligned}$$

and has a presentation

$$\Gamma_0^{35}(1) \cong \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6, \gamma_7 \mid \gamma_7 \gamma_1 \gamma_6 \gamma_2 = \gamma_2 \gamma_5 \gamma_1 \gamma_7, \gamma_4 \gamma_5 \gamma_3 = \gamma_3 \gamma_6 \gamma_4 \rangle.$$

This presentation corresponds to a fundamental domain $\mathcal{F}$ for $\Gamma_0^{35}(1)$ given by a region in $\mathcal{H}$ with vertices

$$\begin{aligned} \{a, \gamma_5 \gamma_1 \gamma_7 a, \gamma_5 \gamma_3 b, b, \gamma_6 \gamma_4 b, \gamma_6 \gamma_2 a, \gamma_7 a, \gamma_7 \gamma_1 \gamma_6 \gamma_2 a, \\ \gamma_2 a, \gamma_4 b, \gamma_3 \gamma_6 \gamma_4 b, \gamma_3 b, \gamma_1 \gamma_7 a, \gamma_1 \gamma_6 \gamma_2 a\}, \end{aligned}$$

where

$$a = \frac{(t+3)(21+\sqrt{-7})}{112}, \quad b = \frac{21+\sqrt{-7}}{56}.$$

and a is the unique point in the upper half plane fixed by $\pi_{35} \gamma_7 \gamma_1 \gamma_6 \gamma_2$, where $\pi_{35} = z$, and $b = \pi_{35} \pi_7 a$, where $\pi_7 = (y+z)/2$.

Proof. The proof of this theorem is similar to the other examples. The relations can easily be verified, and one can check that the γ_i identify the edges of the domain. Then we compute the volume and show that up to a very small error we obtain the expected value of 4. $\square$

The elements

$$\pi_5 = (5-x)/2, \quad \pi_7 = (y+z)/2, \quad \pi_{35} = z,$$

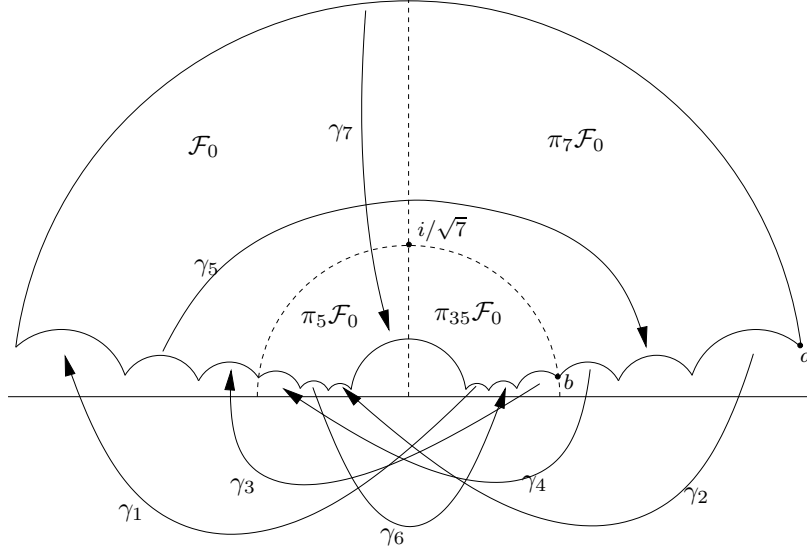


Figure 6: Fundamental domain for $\Gamma_0^{35}(1)$ and its normalizer.

together with 1, give the equivalence classes of $\mathcal{N}(\Gamma_0^{35}(1))/\Gamma_0^{35}(1)$. Projectively, these elements satisfy the relations:

$$\pi_{35}^2 = \pi_7^2 = 1, \quad \pi_5\pi_7 = \pi_{35}, \quad \pi_5^2\gamma_7 = 1$$

Note that these relationships only hold up to multiplication by some scalar.

The dashed lines in the diagram divide the fundamental domain into four regions, each of which is a fundamental domain for the normalizer. Four copies of the domain $\mathcal{F}_0$ form a fundamental domain for $\Gamma_0^{35}(1)$ as shown. The vertices of $\mathcal{F}_0$ are given by

$$\{c, \pi_5^{-1}c, \pi_{35}\pi_5b, \gamma_1\gamma_7a, \gamma_3b, \pi_{35}b\},$$

where c is the fixed point of π_{35} .

In the diagram the edge identifications obtained from these elements are indicated.

7 Algorithmic considerations

In the construction of fundamental domains, it has proved possible to find units by ad hoc search, which can be structured by first searching for real quadratic suborders of small discriminant, followed by a fundamental unit computation in that order. To find a provably deterministic algorithm, one needs to design a search algorithm which guarantees that a system of generators will be found.

For this purpose we invert the following standard lemma (see Vignéras [13], p. 116) to compute units in hyperbolic neighborhoods.

Lemma 7.1. *Let Γ be a discrete subgroup of $\mathrm{PSL}_2(\mathbf{R})$ and let z be a point in $\mathcal{H}$ which is not an elliptic point of Γ . Then the set*

$$\mathcal{F}_z = \{z_1 \in \mathcal{H} \mid d(z, z_1) \leq d(z, \gamma z_1) \text{ for all } \gamma \in \Gamma\},$$

is a convex fundamental domain for Γ .

We invert this construction by letting $T_z(\gamma) = \gamma z$, for fixed z , define a map $\Gamma \rightarrow \mathcal{H}$, and searching for elements of the finite sets $T_z^{-1}(B(z, r))$, where $B(z, r)$ is the hyperbolic disc of radius r about z . A complete set of group generators is provided by the elements mapping $\mathcal{F}_z$ to an adjacent domain, so the search region is sufficient as soon as the search radius r is sufficiently large so that $B(z, r)$ includes the midpoints of all adjacent domains.

We illustrate this argument for $D = 6$ in Figure (7). The dashed circles are discs of various radii, centered at $z = (\sqrt{2}-1)\sqrt{-3}/3$, the fixed point of π_6 . The circle of radius 3, for which the lower boundary is drawn, contains the domain $\mathcal{F} = \mathcal{F}_z$ and all of its neighbors. In particular, it contains points γz for γ any of the generators $\gamma_1, \gamma_2, \gamma_3$, or γ_4 for $\Gamma_0^6(1)$.

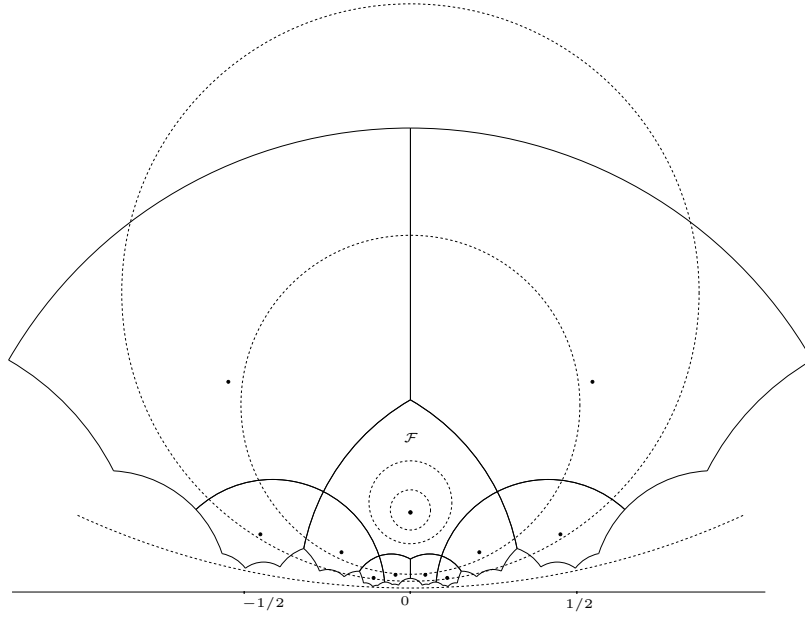


Figure 7: Fundamental domains for $\Gamma_0^6(1)$, and hyperbolic neighborhoods.

As a final computational note we sketch the following reduction algorithm used to reduce of a new generator with respect to a current system of generators

for a group Γ . Let z be a fixed point, which is not elliptic point for the group Γ and fix a radius $r > 0$. Suppose we have found units $\gamma_1, \dots, \gamma_m$ such that $|\gamma_i z - z| < r$ for each i . Then if we can find another element σ with $|\sigma z - z| < r$, we then apply the γ_i to minimize $|\gamma \sigma z - z|$, where γ is a product of the γ_i and their inverses. To do this, construct $\sigma_0 = \sigma, \sigma_1, \dots, \sigma_n = \gamma \sigma$ as follows. Given σ_i , let $\sigma_{i+1} = \gamma_j^e \sigma_i$ such that $|\gamma_j^e \sigma_i z - z|$ is minimal among all generators γ_j and $e = \pm 1$. This process either terminates with $|\gamma \sigma_i z - z| = 0$, in which case σ is not a new generator, or else at some other minimum value, in which case we set $\gamma_{m+1} = \gamma \sigma$.

The computations involved in this work were carried out with algorithms developed in the Magma language [2]. The authors' packages for actions of congruence subgroups on the upper half hyperbolic plane [12] and quaternion algebras [8] were modified for this study.

8 Future work

The authors envisage this study as part of a program to compute invariants of Shimura curves, extending approaches through quaternion ideals and supersingular constructions (see Kohel [6] and [7]) and analogous to the undertakings of Cremona [3]. A complementary project to that discussed here is the development of algorithms for computing modular forms, by means of their Fourier expansions along the minimal geodesic of a hyperbolic element. Such a study should allow the effective determination of models for $X_0^D(N)$. Further, by integration along paths $(z, \gamma z)$, one could determine the period lattice of a curve as a step towards experimentally testing and verifying analogues of the Birch and Swinnerton–Dyer conjectures for Shimura curves.

References

- [1] Alsina, Montserrat. *Aritmetica d'ordres quaternionics i uniformitzacio hiperbolica de corbes de Shimura*, PhD Thesis, Universitat de Barcelona 2000, Publicacions Universitat de Barcelona, ISBN: 84-475-2491-4, 2001.
- [2] W. Bosma and J. Cannon, eds. *The Magma Handbook*, <http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm>, The University of Sydney, 2002.
- [3] J. Cremona, *Algorithms for modular elliptic curves*, Second edition. Cambridge University Press, Cambridge, 1997.
- [4] N. Elkies, Shimura Curve Computations. *Algorithmic Number Theory*, LNCS **1423**, J. Buhler, ed, Springer (1998), 1–47.
- [5] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Thesis, University of California, Berkeley, 1996.

- [6] D. Kohel. Hecke module structure of quaternions. *Class field theory—its centenary and prospect (Tokyo, 1998)*, K. Miyake, ed, Adv. Stud. Pure Math., **30**, Math. Soc. Japan, Tokyo (2001), 177–195.
- [7] D. Kohel. *Brandt modules*. Chapter in *The Magma Handbook*, Volume 7, J. Cannon, W. Bosma Eds., (2001), 343–354.
- [8] D. Kohel. *Quaternion Algebras*. Chapter in *The Magma Handbook*, Volume 6, J. Cannon, W. Bosma Eds., (2001), 237–256.
- [9] A. Kurihara. On some examples of equations defining Shimura curves and the Mumford uniformization. *J. Fac. Sci. Univ. Tokyo*, **25** (1979), 277–301.
- [10] Michon, J.-F. Courbes de Shimura hyperelliptiques. *Bull. Soc. Math. France* **109** (1981), no. 2, 217–225.
- [11] D. Roberts. *Shimura curves analogous to $X_0(N)$* . Ph.D. thesis, Harvard, 1989.
- [12] H. Verrill. *Subgroups of $\mathrm{PSL}_2(\mathbf{R})$* , Chapter in *The Magma Handbook*, Volume 2, J. Cannon, W. Bosma Eds., (2001), 233–254.
- [13] M.-F. Vignéras. *Arithmétiques des Algèbres de Quaternions*, LNM 800, Springer–Verlag, 1980.

David R. Kohel
 School of Mathematics and Statistics
 University of Sydney
 Sydney, NSW 2006, Australia

Helena A. Verrill
 Department of Mathematics
 Louisiana State University
 Baton Rouge, Louisiana 70803-4918, USA