Hyperbolic uniformizations through computations on ternary quadratic forms

Montserrat Alsina
Universitat Politècnica de Catalunya BarcelonaTech

montserrat.alsina@upc.edu

Abstract

Orders in indefinite quaternion algebras provide Fuchsian groups acting on the Poincare half-plane, used to construct the associated Shimura curves.

We explain how, by using embedding theory, the elements of those Fuchsian groups depend on representations of integers by suitable ternary quadratic forms. Thus the explicit computation of those representations leads to explicit presentations and fundamental domains of those Fuchsian groups, the computation of CM points, and a rich interpretation of the points in the complex upper half-plane.

Keywords
Fuchsian groups, quaternion algebras, quadratic forms, embeddings

1 Introduction

Let D, N be natural numbers such that $\gcd(D, N) = 1$ and D is the product of an even number of different primes. Then there exists an indefinite quaternion algebra H over $\mathbb{Q}$, unique up to isomorphism, with discriminant D, given by a $\mathbb{Q}$-basis $\{1, i, j, ij\}$ satisfying the relations $i^2 = a$, $j^2 = b$ and $ij = -ji$ (plus the associative property) for some $a, b \in \mathbb{Q}^*$, $a > 0$. As usual, we write $H = \left(\frac{a,b}{\mathbb{Q}}\right)$. Since H is indefinite, we can fix an embedding $\Phi : H \hookrightarrow \mathrm{M}(2, \mathbb{R})$.

Let us consider an Eichler order of level N, $\mathcal{O}(D, N)$, that is, a $\mathbb{Z}$-module of rank 4, subring of H, intersection of two maximal orders, unique up to conjugation. Basics on quaternion algebras and orders can be found at [7], [9].

Consider $\Gamma(D, N) := \Phi(\{\alpha \in \mathcal{O}(D, N) : n(\alpha) = 1\})$, the image of the group of units of positive norm. Then $\Gamma(D, N) \subseteq \mathrm{SL}(2, \mathbb{R})$ is a Fuchsian group of the first kind acting on the Poincare half-plane $\mathcal{H} = \{x + \iota y \mid y > 0\}$, and the quotient $\Gamma(D, N) \setminus \mathcal{H}$ yields a Riemann surface. If $D = 1$, then $H = \mathrm{M}(2, \mathbb{Q})$, $\Gamma(D, N) = \Gamma_0(N)$ and this construction leads to the modular curves usually denoted by $X_0(N)$. Otherwise, if $D > 1$, these Riemann surfaces are already compact and Shimura's work (cf. [8]) provides a canonical model for $\Gamma(D, N) \setminus \mathcal{H}$ with nice properties, that will be denoted by $X(D, N)$, and a modular interpretation. $X(D, N)$ are called Shimura curves associated to the subgroups $\Gamma(D, N)$, and they are involved in some spectacular results as the proof of Taniyama-Shimura-Weil modularity conjecture (cf. [5], [10]).

By construction, it is not so easy to make explicit these groups $\Gamma(D, N)$ and to compute, for example, the hyperbolic uniformization of the associated Shimura curves. In particular the lack of cusps in these groups makes a big difference with the well-known modular case. Anyway, the fundamental domains of theses curves allows a rich interpretation of the points in the complex upper half-plane, which can be elliptic, CM-points, etc. and even binary quadratic forms show up (cf. [3]).

The goal of this paper is to make explicit the relationship between the Fuchsian group $\Gamma(D, N)$ and representations of integers by suitable ternary quadratic forms, in such a way that computational results on quadratic forms can be applied to this arithmetic and geometric setting.

2 The group of quaternion transformations via embeddings

We deal with embeddings of quadratic fields into quaternion algebras, taking into account the arithmetic of orders in both algebraic structures.

From now on consider a quadratic field $F = \mathbb{Q}(\sqrt{d})$, and $\Lambda = \Lambda(d, m) \subset F$ the quadratic order of conductor m. It is well-known that $\Lambda(d, m) = \mathbb{Z}[1, mw]$, where $w = \sqrt{d}$ if $d \equiv 2, 3 \mod 4$, and $w = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \mod 4$. For $m = 1$, Λ is the integer ring of F.

We denote by $\mathcal{E}(H, F)$ the set of embeddings of the quadratic field F in the quaternion algebra H. If it is non empty, we consider the restriction to the orders

$$\mathcal{E}(\mathcal{O}, \Lambda) := \{\varphi : \varphi \in \mathcal{E}(H, F), \varphi(\Lambda) \subset \mathcal{O}\}.$$

An embedding is called optimal if $\varphi(F) \cap \mathcal{O} = \varphi(\Lambda)$, and $\mathcal{E}^*(\mathcal{O}, \Lambda)$ will denote the set of optimal embeddings.

The group $\operatorname{Nor}\mathcal{O}$ acts on $\mathcal{E}^*(\mathcal{O}, \Lambda)$, and we can consider the quotient $\mathcal{E}^*(\mathcal{O}, \Lambda)/\operatorname{Nor}\mathcal{O}$. In the case $\mathcal{O} = \mathcal{O}(D, N)$, its class number can be computed following results by Eichler (cf. [1], [6]).

In our setting, those embeddings will be very interesting because, by using fundamental units in quadratic orders, they allow to compute elements in the Fuchsian group $\Gamma(D, N)$. They are also relevant to compute the fundamental domain of the Shimura curves $X(D, N)$ and the corresponding tessellation of $\mathcal{H}$, and interesting points as elliptic and complex multiplication ones. Note that, because of the lack of cusps, a lot of information is concentrated on those points.

Remark 2.1 *Let ε be a fundamental unit in the quadratic order $\Lambda(d, m)$. Put $\xi := \varepsilon$ if $\mathrm{n}(\varepsilon) = 1$ and $\xi := \varepsilon^2$ if $\mathrm{n}(\varepsilon) = -1$. Then:*

$$\varphi \in \mathcal{E}(\mathcal{O}(D, N), \Lambda(d, m)) \Longrightarrow \Phi(\varphi(\xi^n)) \in \Gamma(D, N), \quad \forall n \in \mathbb{Z}.$$

Conversely, every quaternion transformation can be obtained from embeddings of quadratic orders in the quaternion order as above, as it is shown in the following theorem, proved at [1].

Theorem 2.2 *Let $\gamma \in \Gamma(D, N)$, $D > 1$.*
Then there exists a quadratic order $\Lambda(d, m)$, a number $n \in \mathbb{Z} - \{0\}$ and an optimal embedding $\varphi \in \mathcal{E}^*(\mathcal{O}(D, N), \Lambda(d, m))$ such that $\Phi(\varphi(\varepsilon^n)) = \gamma$, where ε is the fundamental unit of $\Lambda(d, m)$. Moreover, elliptic transformations come from imaginary quadratic fields, and hyperbolic transformations come from real quadratic fields.

In the proof of that theorem the involved quadratic field $\mathbb{Q}(\sqrt{d})$ is explicit: given $\gamma \in \Gamma(D, N)$, then $d = \operatorname{tr}(\gamma)^2 - 4$.

As a consequence of the theorem, all elements in $\Gamma(D, N)$ can be computed from the explicit computation of embeddings by using the fundamental units in quadratic fields, which can be computed algorithmically (cf. [4]). Actually it can be done by using computer algebra systems as *Magma*.

3 Computations via quadratic forms

Next, we shall use quadratic forms to construct those embeddings. Mainly we will use the ternary quadratic form $n_{\mathcal{O},3}$, induced by the reduced norm in a quaternion order $\mathcal{O}$, when we restrict to pure quaternions. To get an expression of the quadratic form, up to $\mathbb{Z}$ equivalence, a basis of the order need to be fixed. We will use normalized basis $\{1, v_2, v_3, v_4\}$ satisfying $\operatorname{tr}(v_2) = \operatorname{tr}(v_3) = 0$, $\operatorname{tr}(v_4) \in \{0, 1\}$ (cf. [1]).

Remark 3.1 *Consider the family of quaternion algebras of discriminant $D = 2p$, $p \equiv 3 \mod 4$, $H_A(p) = \left(\frac{p,-1}{\mathbb{Q}}\right)$, called small ramified algebras of type A. Then a family of Eichler orders is given by $\mathcal{O}_A(2p, N) := \mathbb{Z}\left[1, i, Nj, \frac{1+i+j+ij}{2}\right]$, $N|\frac{p-1}{2}$ square-free. The corresponding ternary normic forms are: $n_{H,3}(Y, Z, T) = -pY^2+Z^2-pT^2$ and $n_{\mathcal{O},3} = (1-2p)X^2-pY^2+N^2Z^2+2pXY-2NXZ$.*

Given a quadratic form f in n variables and $A(f)$ the associated matrix, consider the set of integer representations of a number δ:

$$\mathcal{R}(f, \delta; \mathbb{Z}) := \{\alpha \in \mathbb{Z}^n \,:\, f(\alpha) = \delta\} = \{\alpha \in \mathbb{Z}^n \,:\, \alpha^t A(f) \alpha = \delta\}.$$

We denote by $\mathcal{R}^*(f,\delta;\mathbb{Z})$ those satisfying the condition $\gcd(\alpha_1,\ldots,\alpha_n)=1$, called primitive representations.

The following result is proved in [1] (cf. Theorem 4.26, Corollary 4.27). Note that $n_{\mathbb{Z}+2\mathcal{O},3}$ needs to be used instead of $n_{\mathcal{O},3}$.

Theorem 3.2 *Let $\mathcal{O}\subseteq H$ an Eichler order given by a normalized basis $\mathcal{B}=\{1,v_2,v_3,v_4\}$. Let $\Lambda=\Lambda(d,m)\subseteq\mathbb{Q}(\sqrt{d})$ a quadratic order of conductor m and denote D_Λ its discriminant. Then there is a bijective mapping*

$$\begin{array}{ccc}\sigma:\mathcal{R}\left(n_{\mathbb{Z}+2\mathcal{O},3},-D_\Lambda;\mathbb{Z}\right) & \longrightarrow & \mathcal{E}(\mathcal{O},\Lambda)\\ (x,y,z) & \mapsto & \varphi\,,\end{array}$$

where φ is the embedding defined by $\varphi(mw)=\left(\frac{rm-z\,\mathrm{tr}(v_4)}{2},x,y,z\right)_{\mathcal{B}}$, for $r=0$ if $d\equiv 2,3 \mod 4$, and $r=1$ if $d\equiv 1 \mod 4$. Namely,

$$\varphi(\sqrt{d})=\begin{cases}\left(\dfrac{-z\,\mathrm{tr}(v_4)}{2m},\dfrac{x}{m},\dfrac{y}{m},\dfrac{z}{m}\right)_{\mathcal{B}} & \text{if } d\equiv 2,3 \mod 4,\\[2ex] \left(\dfrac{-z\,\mathrm{tr}(v_4)}{m},\dfrac{2x}{m},\dfrac{2y}{m},\dfrac{2z}{m}\right)_{\mathcal{B}} & \text{if } d\equiv 1 \mod 4.\end{cases}$$

Moreover, primitive representations are in bijection with optimal embeddings.

Example 3.3 *Consider a maximal order in a small ramified quaternion algebra of type A, $\mathcal{O}_A(14,1)=\mathbb{Z}[1,i,j,\frac{1+i+j+ij}{2}]\subseteq H_A(7)=\left(\frac{7,-1}{\mathbb{Q}}\right)$.*
Consider the quadratic orders $\Lambda(-1,1)$, $\Lambda(-1,3)$ and $\Lambda(-1,15)$, in $\mathbb{Q}(\sqrt{-1})$.
Computing representations of 1, 9 and 225 by the ternary normic form

$$n_{\mathbb{Z}+2\mathcal{O}_A(14,1),3}(X,Y,Z)=-28X^2+4Y^2-13Z^2-28XZ+4YZ,$$

we obtain the embeddings $\varphi_s\in\mathcal{E}(H_A(7),F)$, given by $\varphi_s(w)=\omega_s$, $1\le s\le 4$,
where $\omega_1:=j$, $\omega_2:=3i+8j$, $\omega_3:=1/3i+4/3j$, and $\omega_4:=1/15i+22/15j+2/5ij$.

Bullets in next table shows which embeddings are on each set, optimal or not.

	φ_1	φ_2	φ_3	φ_4
$\mathcal{E}(\mathcal{O}_A(7,1),\Lambda(-1,1))$	•	•	–	–
$\mathcal{E}^*(\mathcal{O}_A(7,1),\Lambda(-1,1))$	•	•	–	–
$\mathcal{E}(\mathcal{O}_A(7,1),\Lambda(-1,3))$	•	•	•	–
$\mathcal{E}^*(\mathcal{O}_A(7,1),\Lambda(-1,3))$	–	–	•	–
$\mathcal{E}(\mathcal{O}_A(7,1),\Lambda(-1,15))$	•	•	•	•
$\mathcal{E}^*(\mathcal{O}_A(7,1),\Lambda(-1,15))$	–	–	–	•

Considering the class groups of optimal embeddings and primitive representation, it is proved that the map σ induce a bijection between the class groups. Thus, the class number of equivalent representations can be computed too, using the classification of optimal embeddings quoted in previous section. At the example above, the integer 1 has two inequivalent representations by the ternary form $n_{\mathbb{Z}+2\mathcal{O}_A(14,1),3}$; however, the integer 9 has four inequivalent ones.

As a consequence of the Theorems 2.2 and 3.2, the elements in the group $\Gamma(D,N)$ can be found explicitly by computing representations by ternary quadratic forms.

Next, we show explicit expressions depending only on representations of integers by ternary quadratic forms the small ramified parametric case presented in Remark 3.1. They are applied to the computation of the elliptic elements in $\Gamma(2p,N)$ and its corresponding points, and to the computation of the complex multiplication (CM) points. Both are the interesting points in this context of hyperbolic uniformization of Shimura curves in the Poincaré half-plane.

We use the explicit embedding $\Phi:\left(\frac{p,-1}{\mathbb{Q}}\right)\hookrightarrow \mathrm{M}(2,\mathbb{Q}(\sqrt{p}))\subset\mathrm{M}(2,\mathbb{R})$ given by

$$\Phi(x+y\sqrt{p}+z\sqrt{-1}+t\sqrt{-p})=\begin{pmatrix}x+y\sqrt{p} & z+t\sqrt{p}\\ -(z-t\sqrt{p}) & x-y\sqrt{p}\end{pmatrix}.$$

Proposition 3.4 *Let $p \equiv 3 \mod 4$ and $N|\frac{p-1}{2}$ square-free. Fix the quaternion algebra $H_A(p)$, the Eichler order $\mathcal{O}_A(2p,N) = \mathbb{Z}[1, i, Nj, \frac{1+i+j+ij}{2}]$, and the group of quaternion transformations $\Gamma(2p,N)$ defining the Shimura curve $X(2p,N)$. Then:*

i) $\gamma \in \Gamma(2p,N)$ is an elliptic linear fractional transformation on $\mathcal{H}$ of order 2 if, and only if, $\gamma = \frac{1}{2}\begin{pmatrix} (2x+z)\sqrt{p} & (2Ny+z)+z\sqrt{p} \\ -(2Ny+z)+z\sqrt{p} & -(2x+z)\sqrt{p} \end{pmatrix}$, where $(x,y,z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O},3}, 4; \mathbb{Z})$.

In this case, the corresponding elliptic point is $\tau = \dfrac{(2x+z)\sqrt{p} \pm 2\iota}{-(2Ny+z)+z\sqrt{p}} \in \mathcal{H}$.

ii) The complex points of $X(D,N)$ with complex multiplication by a quadratic order Λ are

$$\left\{ \frac{(2x+z)\sqrt{p} \pm \sqrt{-D_\Lambda}\iota}{-(2Ny+z)+z\sqrt{p}} \in \mathcal{H} \,:\, (x,y,z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O},3}, -D_\Lambda; \mathbb{Z}) \right\}.$$

We can conclude that from a fine study of the algorithms to compute representations of integers by ternary quadratic forms, new results for the complexity of computations related to the Shimura curves $X(D,N)$ can be drawn. They would be of great interest not only in the area of Number Theory but in applications to other areas as Coding Theory or Cryptography.

References

[1] M. Alsina and P. Bayer, *Quaternion Orders, Quadratic Forms and Shimura Curves*, CRM Monograph Series vol. 22, AMS (2004).

[2] M. Alsina, *Fundamental domains of the upper half plane by the action of matrix groups*, Meeting on matrix analysis and applications, Dept. Mat. Apl. I, Fac. Informática y Estadística, Univ. de Sevilla (1997), 10–17.

[3] M. Alsina, *Binary quadratic forms and Eichler orders*, J. de Théorie des Nombres de Bordeaux **17** (2005), 13–23.

[4] H. Cohen, *Number Theory*, Graduate Texts in Mathematics, vol. 239, Springer (2007).

[5] G. Cornell, J. H. Silverman, and G. Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer, (1997), Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston MA (1995).

[6] A.P. Ogg, *Real points on Shimura curves*, Progress in mathematics, no. 35, Birkhäuser (1983), 277–303.

[7] I. Reiner, *Maximal Orders*, Academic Press (1975).

[8] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Annals of Math. **85** (1967), 58–159.

[9] M.F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., no. 800, Springer (1980).

[10] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.