Congruence subgroups, cusps and Manin symbols over number fields

J. E. Cremona and M. T. Aranés

Abstract We develop an explicit theory of congruence subgroups, their cusps, and Manin symbols for arbitrary number fields. While our motivation is in the application to the theory of modular symbols over imaginary quadratic fields, we give a general treatment which makes no special assumptions on the number field.

1 Introduction

Let K be a number field with ring of integers R. When $K = \mathbb{Q}$ or K is an imaginary quadratic field, spaces of cusp forms for $\mathrm{GL}(2, K)$ have been computed using methods based on modular symbols. These methods are well known for $K = \mathbb{Q}$: see the books of the first author [6] and Stein [11] for detailed accounts. In the case of imaginary quadratic fields with small class number, modular symbol methods have been developed by the first author and his students: see [4], [2] and [8], following earlier work of Manin, Mennicke and others. While modular symbols as such are not sufficient for explicit computation of more general automorphic forms (see the introduction to [7] for a discussion of this point), some of the algebraic background concerning congruence subgroups and the projective line over finite residue rings, whose elements are often called Manin symbols or M-symbols in this context, is relevant in more situations than computations with modular symbols over the rationals or imaginary quadratic fields.

J. E. Cremona
Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK.
e-mail: John.Cremona@gmail.com

M. T. Aranés
Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK.

In this paper we give a systematic treatment of the algebraic theory of congruence subgroups and Manin symbols over arbitrary number fields. For the most part, we only need assume that R is a Dedekind domain, and do not make use of any special properties enjoyed by the ring of integers of a number field; however we do give some counting formulas which rely on finiteness of the class group and of residue rings. This framework has already been useful in explicit computation of cusp forms over imaginary quadratic fields, which can be done using either the homology or the cohomology of Bianchi groups acting on hyperbolic 3-space, and we expect that our results will have wider application, though we will not discuss such applications (including the function field case) further here.

In a sequel to this paper, we will show how, in the case of imaginary quadratic fields, these ideas may be used in the explicit computation of automorphic forms over imaginary quadratic fields, giving connections to the adelic language in which such forms are normally defined, showing in particular how Hecke and Atkin-Lehner operators may be computed explicitly. See the contribution by A. Mohamed in this volume for related material about modular and Manin symbols over imaginary quadratic fields, including formulas for the action of Hecke operators on Manin symbols in the case of Euclidean imaginary quadratic fields, and also the work of Şengün ([9] and the survey article in this volume).

The main results of the paper are: criteria for cusp equivalence under the congruence subgroups $\Gamma_0(\mathfrak{n})$ (Theorem 6) and $\Gamma_1(\mathfrak{n})$ (Theorem 9), and the number of cusps for $\Gamma_0(\mathfrak{n})$ (Theorem 7). The cusp equivalence criteria are given in a form suitable for implementation, and algorithms based on the results of this paper, including tests for cusp equivalence and enumeration of Manin symbols over arbitrary number fields, have been implemented by the second author in the Sage open-source mathematical software system [12].

After setting basic notation, we define in Section 2 a special class of 2×2 matrices over a number field K called $(\mathfrak{a}, \mathfrak{b})$-matrices, which are used throughout the paper. They are used to generalise the definition of Manin symbols (also called M-symbols) to K in Section 3. In Section 4 we study cusps and cusp equivalence with respect to the standard congruence subgroups, giving criteria for equivalence and a result giving the number of cusps for congruence subgroups; the proofs here also use $(\mathfrak{a}, \mathfrak{b})$-matrices. These results, which depend critically on the class group of K, generalise classical results over $\mathbb{Q}$.

Notation and basic definitions

We denote by R a Dedekind Domain with field of fractions K. Let $\mathrm{Mat}_2(K)$ and $\mathrm{Mat}_2(R)$ be the algebras of 2×2 matrices with entries in K and R respectively, and $\mathrm{GL}(2, K)$ and $\Gamma = \mathrm{GL}(2, R)$ their multiplicative groups. Let R^* be the set of nonzero elements of R, and $R^\times$ the unit group.

Nonzero ideals of R will be denoted $\mathfrak{a}, \mathfrak{b}, \ldots, \mathfrak{n}$ and prime ideals by $\mathfrak{p}, \mathfrak{q}$. The norm of an ideal is $N(\mathfrak{a}) = \#(R/\mathfrak{a})$, which we assume throughout to be finite. We have $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ for all $\mathfrak{a}, \mathfrak{b}$, and $\#(R/\mathfrak{a})^\times = \varphi(\mathfrak{a})$, where

$$\varphi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - N(\mathfrak{p})^{-1}\right).$$

Associated to each nonzero integral ideal $\mathfrak{n}$ of R, we have the standard *congruence subgroups of level* $\mathfrak{n}$ of $\mathrm{GL}(2, R)$, denoted $\Gamma_0(\mathfrak{n})$, $\Gamma_1(\mathfrak{n})$ and $\Gamma(\mathfrak{n})$. We will mainly be concerned with $\Gamma_0(\mathfrak{n})$ and $\Gamma_1(\mathfrak{n})$ here:

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \in \mathfrak{n} \right\};$$
$$\Gamma_1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c, d-1 \in \mathfrak{n} \right\}.$$

Note that as we are using $\Gamma = \mathrm{GL}(2, R)$ as our base group, not $\mathrm{SL}(2, R)$, we define $\Gamma_0(\mathfrak{n})$ and $\Gamma_0(\mathfrak{n})$ accordingly. We have $[\Gamma : \Gamma_0(\mathfrak{n})] = \psi(\mathfrak{n})$, where

$$\psi(\mathfrak{n}) = N(\mathfrak{n}) \prod_{\mathfrak{p}|\mathfrak{n}} \left(1 + N(\mathfrak{p})^{-1}\right),$$

and $[\Gamma_0(\mathfrak{n}) : \Gamma_1(\mathfrak{n})] = \varphi(\mathfrak{n})$. Both φ and ψ are multiplicative in the sense that $\varphi(\mathfrak{mn}) = \varphi(\mathfrak{m})\varphi(\mathfrak{n})$ when $\mathfrak{m}, \mathfrak{n}$ are coprime, and similarly for ψ. This multiplicativity, and the index formulas, are proved exactly as for $K = \mathbb{Q}$.

We will use several standard facts about finitely generated modules over the Dedekind Domain R: a suitable reference for these, including many relevant algorithms, is the first chapter of Cohen's book [3]. Specifically we will be concerned with *R-lattices*, which we define to be projective (locally free) R-submodules of $K \oplus K$ of rank 2. Elements of R-lattices (and indeed all elements of $K \oplus K$) are row vectors, with matrices acting on the right.

The group Γ may be characterized through its action on R-lattices, as the set of all matrices $\gamma \in \mathrm{GL}(2, K)$ satisfying $(R \oplus R)\gamma = R \oplus R$. There is a similar characterization of $\Gamma_0(\mathfrak{n})$, whose proof is immediate.

Proposition 1.

$$\begin{aligned}\Gamma_0(\mathfrak{n}) &= \{\gamma \in \Gamma \mid (\mathfrak{n} \oplus R)\gamma = (\mathfrak{n} \oplus R)\} \\ &= \{\gamma \in \mathrm{GL}(2, K) \mid (R \oplus R)\gamma = R \oplus R \quad \textit{and} \quad (\mathfrak{n} \oplus R)\gamma = (\mathfrak{n} \oplus R)\}.\end{aligned}$$

In the above we could also replace $\mathfrak{n} \oplus R$ by $R \oplus \mathfrak{n}^{-1}$. Thus $\Gamma_0(\mathfrak{n})$ is the right stabilizer of the pair of lattices (L, L') where $L = R \oplus R$ and $L' = R \oplus \mathfrak{n}^{-1}$. A pair of lattices (L, L') satisfying $L' \supseteq L$ and $L'/L \cong R/\mathfrak{n}$ (as R-modules) is called a *modular point* for $\Gamma_0(\mathfrak{n})$; these will be studied in detail in the sequel to this paper.

To characterize $\Gamma_1(\mathfrak{n})$ in the same way, we need to rigidify the lattice pair (L, L') by fixing an R-module generator of the cyclic quotient L'/L, which is isomorphic to $R/\mathfrak{n}$. Let $n \in \mathfrak{n}^{-1}$ generate $\mathfrak{n}^{-1}/R$, so that $\mathfrak{n}^{-1} = R + Rn$, and let $\beta = (0, n) \in L'$. Then $L' = L + R\beta$, and $\Gamma_1(\mathfrak{n})$ is the subgroup of Γ fixing $\beta \pmod L$, since

$$\Gamma_1(\mathfrak{n}) = \{\gamma \in \mathrm{GL}(2, K) \mid (R \oplus R)\gamma = R \oplus R \quad \text{and} \quad \beta\gamma = \beta \pmod{R \oplus R}\};$$

this follows from $nx \in R \iff x \in \mathfrak{n}$, for $x \in R$. This characterization of $\Gamma_1(\mathfrak{n})$ is independent of the choice of β such that $L' = L + R\beta$. When $R = \mathbb{Z}$ and $\mathfrak{n} = N\mathbb{Z}$, one usually takes $n = \frac{1}{N}$.

For $a, b \in K$ we denote by $\langle a \rangle$ and $\langle a, b \rangle$ the (fractional) ideals aR and $aR + bR$. For an ideal or fractional ideal $\mathfrak{a}$ we denote its class in the class group $\mathrm{Cl}(K)$ by $[\mathfrak{a}]$. Among the elementary properties of Dedekind Domains we will use are the following.

- For any ideal $\mathfrak{a}$ and any nonzero $a \in \mathfrak{a}$ there exists $b \in \mathfrak{a}$ with $\mathfrak{a} = \langle a, b \rangle$;
- Every ideal class contains an ideal coprime to any given ideal.

2 $(\mathfrak{a}, \mathfrak{b})$-matrices

In our discussion of M-symbols and cusp equivalence later in this paper, and of Hecke and other operators in the sequel, certain matrices in $\mathrm{Mat}_2(R)$ will play an important role. Over $\mathbb{Q}$, or more generally when K has class number 1, these matrices are not visible, as their role is played by elements of $\Gamma = \mathrm{GL}(2, R)$ itself in discussions of cusp equivalence, while in Hecke theory their role is played by matrices in Hermite Normal Form. They will be used in the following section to define M-symbols; in the discussion of cusps and cusp equivalence in the final section, their use stems from the fact that every cusp has the form $M(\infty)$ for one of these matrices M.

We will define these special matrices below, after some preliminary remarks. They are associated with any pair of ideals $\mathfrak{a}, \mathfrak{b}$ which are in inverse ideal classes, *i.e.* with $[\mathfrak{b}] = [\mathfrak{a}]^{-1}$ in $\mathrm{Cl}(K)$, so that $\mathfrak{ab}$ is principal.

The following two results are well known from the structure theory of finitely generated projective R-modules [3, Lemma 1.2.20].

Proposition 2. *Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals of R. Then $\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{ab} \oplus R$ as R-modules.*

Corollary 1. *Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in inverse classes. Then $\mathfrak{a} \oplus \mathfrak{b} \cong R \oplus R$.*

We will need a very explicit and constructive form of this corollary. Observe that any R-module isomorphism $R \oplus R \to \mathfrak{a} \oplus \mathfrak{b}$ is necessarily given by a matrix $M \in \mathrm{Mat}_2(R)$ such that

$$(R \oplus R)M = \mathfrak{a} \oplus \mathfrak{b}.$$

We define an $(\mathfrak{a},\mathfrak{b})$-*matrix* to be a matrix $M \in \mathrm{GL}_2(R)$ satisfying this condition, and denote the set of all $(\mathfrak{a},\mathfrak{b})$-matrices by $X_{\mathfrak{a},\mathfrak{b}}$. Note that $(\mathfrak{a},\mathfrak{b})$-matrices are only defined when $\mathfrak{ab}$ is principal. We will now see how to to construct them.

Theorem 1. *Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in inverse classes. Write $\mathfrak{a} = \langle a_1, a_2\rangle$, let g be a generator of the principal ideal $\mathfrak{ab}$, and write $g = a_1b_2 - a_2b_1$ with $b_1, b_2 \in \mathfrak{b}$. Then $M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ is an $(\mathfrak{a},\mathfrak{b})$-matrix.*

Proof. Since each row of M lies in $\mathfrak{a}\oplus\mathfrak{b}$, clearly $(R\oplus R)M \subseteq \mathfrak{a}\oplus\mathfrak{b}$. Conversely, if $(a_3, b_3) \in \mathfrak{a} \oplus \mathfrak{b}$ then $(a_3, b_3) = (x, y)M$ where

$$(x, y) = (a_3, b_3)M^{-1} = g^{-1}(a_3b_2 - a_2b_3, a_1b_3 - a_3b_1) \in R \oplus R$$

since all $a_ib_j \in \mathfrak{ab} = \langle g\rangle$. $\square$

From the above proof we see that $(\mathfrak{a},\mathfrak{b})$-matrices exist whose first column is an arbitrary pair of generators of $\mathfrak{a}$. In particular, the lower left entry may be chosen to be any nonzero element of $\mathfrak{a}$. For an integral ideal $\mathfrak{n}$, we say that an $(\mathfrak{a},\mathfrak{b})$-matrix has *level* $\mathfrak{n}$ if its lower left entry lies in $\mathfrak{an}$.

In the case $\mathfrak{a} = \mathfrak{b} = R$, an $(\mathfrak{a},\mathfrak{b})$-matrix is simply an element of Γ and $(\mathfrak{a},\mathfrak{b})$-matrices of level $\mathfrak{n}$ are precisely elements of $\Gamma_0(\mathfrak{n})$. The preceding construction generalizes the familiar construction of a unimodular matrix with any prescribed first column of coprime elements.

Let

$$\Delta(\mathfrak{a},\mathfrak{b}) = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mid x, w \in R, y \in \mathfrak{a}^{-1}\mathfrak{b}, z \in \mathfrak{ab}^{-1}, xw - yz \in R^\times \right\}.$$

Note that $\Delta(\mathfrak{a},\mathfrak{b}) = \Gamma$ when $\mathfrak{a} = \mathfrak{b}$, and more generally that

$$\mathfrak{b} \mid \mathfrak{a} \implies \Delta(\mathfrak{a},\mathfrak{b}) \cap \Gamma = \Gamma_0(\mathfrak{ab}^{-1}).$$

Just as Γ is the stabilizer of the lattice $R \oplus R$, we have the following generalization, whose proof is straightforward. In some texts (for example [13]) the group $\Delta(\mathfrak{a},\mathfrak{b})$ is denoted $\mathrm{GL}(\mathfrak{a} \oplus \mathfrak{b})$; our notation is chosen in order to allow subscripts for certain subgroups to be defined shortly.

Proposition 3. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals (not necessarily in inverse ideal classes). Then for $\gamma \in \mathrm{GL}(2, K)$,*

$$(\mathfrak{a} \oplus \mathfrak{b})\gamma = \mathfrak{a} \oplus \mathfrak{b} \iff \gamma \in \Delta(\mathfrak{a},\mathfrak{b}),$$

and more generally,

$$(\mathfrak{a} \oplus \mathfrak{b})\gamma = (\mathfrak{a} \oplus \mathfrak{b})\gamma' \iff \gamma'\gamma^{-1} \in \Delta(\mathfrak{a},\mathfrak{b}).$$

We will need the following subgroups of $\Delta(\mathfrak{a},\mathfrak{b})$:

$$\Delta_0(\mathfrak{a},\mathfrak{b}) = \left\{ \begin{pmatrix} x & y \\ 0 & w \end{pmatrix} \mid x,w \in R, y \in \mathfrak{a}^{-1}\mathfrak{b}, xw \in R^\times \right\};$$
$$\Delta_1(\mathfrak{a},\mathfrak{b}) = \left\{ \begin{pmatrix} 1 & y \\ 0 & w \end{pmatrix} \in \Delta(\mathfrak{a},\mathfrak{b}) \right\};$$
$$\Delta_{1,1}(\mathfrak{a},\mathfrak{b}) = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in \Delta(\mathfrak{a},\mathfrak{b}) \right\} = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in \mathfrak{a}^{-1}\mathfrak{b} \right\};$$

these satisfy $\Delta_{1,1}(\mathfrak{a},\mathfrak{b}) \subseteq \Delta_1(\mathfrak{a},\mathfrak{b}) \subseteq \Delta_0(\mathfrak{a},\mathfrak{b}) \subseteq \Delta(\mathfrak{a},\mathfrak{b})$.

For each pair of ideals $\mathfrak{a},\mathfrak{b}$ in inverse classes, the set $X_{\mathfrak{a},\mathfrak{b}}$ is clearly closed under multiplication by elements of Γ on the left and by elements of $\Delta(\mathfrak{a},\mathfrak{b})$ on the right. Moreover, a simple calculation establishes that the resulting group actions are transitive, giving us the following description.

Theorem 2. *Let $M_0 \in X_{\mathfrak{a},\mathfrak{b}}$. Then*

$$X_{\mathfrak{a},\mathfrak{b}} = \Gamma M_0 = M_0\Delta(\mathfrak{a},\mathfrak{b}).$$

The orbit of M_0 under $\Delta_1(\mathfrak{a},\mathfrak{b})$ is the set of $(\mathfrak{a},\mathfrak{b})$-matrices with the same first column as M_0, while its orbit under $\Delta_{1,1}(\mathfrak{a},\mathfrak{b})$ is the set of those with same first column and same determinant.

If $\mathfrak{a}$ and $\mathfrak{b}$ are both principal, one choice for a representative $(\mathfrak{a},\mathfrak{b})$-matrix is a diagonal matrix.

A more general version of Proposition 3 is the following, whose proof is again straightforward.

Proposition 4. *M is an $(\mathfrak{a},\mathfrak{b})$-matrix of level $\mathfrak{n}$ if and only if*

$$(R\oplus R)M = \mathfrak{a}\oplus\mathfrak{b} \qquad \text{and} \qquad (\mathfrak{n}\oplus R)M = \mathfrak{a}\mathfrak{n}\oplus\mathfrak{b}.$$

We next consider the set of $(\mathfrak{a},\mathfrak{b})$-matrices under the action of $\Gamma_0(\mathfrak{n})$ on the left. The following is a generalization of [6, Lemma 2.2.1], which is the special case when $\mathfrak{a}=\mathfrak{b}=R=\mathbb{Z}$. When $\mathfrak{a}=\mathfrak{b}=R$ we obtain a criterion (see Proposition 6 below) for two elements of Γ to lie in the same right coset of $\Gamma_0(\mathfrak{n})$, which is used in computations with modular symbols. We will also use this rather technical result in the definition of Manin symbols in the next section (using the equivalence of statements (1)–(3)), and in the study of $\Gamma_0(\mathfrak{n})$-equivalence of cusps in the final section (using the equivalence of statements (1) and (4)).

Theorem 3. *Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in inverse classes, and let $M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ and $M' = \begin{pmatrix} a_1' & b_1' \\ a_2' & b_2' \end{pmatrix}$ be two $(\mathfrak{a},\mathfrak{b})$-matrices. Then the following statements* (1)–(3) *are equivalent:*

1. $M' = \gamma M$ *for some* $\gamma \in \Gamma_0(\mathfrak{n})$.
2. $a_2'b_2 \equiv a_2b_2' \pmod{\mathfrak{abn}}$.
3. There exists $u \in R$ *coprime to* $\mathfrak{n}$ *such that*

(a) $ua_2 \equiv a_2' \pmod{\mathfrak{an}}$, *and*
(b) $ub_2 \equiv b_2' \pmod{\mathfrak{bn}}$.

Each of the preceding statements also implies

4. There exist $u \in R$ *coprime to* $\mathfrak{n}$ *and* $v \in R^\times$ *and a divisor* $\mathfrak{d}$ *of* $\mathfrak{n}$ *such that the following hold:*

(a) $\langle a_2\rangle + \mathfrak{an} = \langle a_2'\rangle + \mathfrak{an} = \mathfrak{ad}$;
(b) $ua_2 \equiv a_2' \pmod{\mathfrak{an}}$;
(c) $va_1 \equiv ua_1' \pmod{\mathfrak{ad}}$.

Conversely, if (4) *holds, then there exists* $\gamma \in \Gamma_0(\mathfrak{n})$ *such that* $\gamma M = M'\begin{pmatrix}1 & w\\ 0 & 1\end{pmatrix}$ *with* $w \in \mathfrak{a}^{-1}\mathfrak{b}$, *so that* γM *is another* $(\mathfrak{a},\mathfrak{b})$*-matrix with the same first column and determinant as* M'.

Proof. Let $g = \det M$, so $\mathfrak{ab} = \langle g\rangle$ and $\det M' = vg$ with $v \in R^\times$, and let $\gamma = M'M^{-1}$, so $\det\gamma = v$ and $\gamma \in \Gamma$ by Theorem 2. Write $\gamma = \begin{pmatrix}w & x\\ y & u\end{pmatrix}$. Then

$$y = g^{-1}(a_2'b_2 - a_2b_2'),$$

so $\gamma \in \Gamma_0(\mathfrak{n}) \iff y \in \mathfrak{n} \iff$ (2) holds, showing that (1) and (2) are equivalent.

Now assume (1) and (2). The diagonal entries of γ are $w = g^{-1}(a_1'b_2 - b_1'a_2)$ and $u = g^{-1}(a_1b_2' - b_1a_2')$, so $uw \equiv v \pmod{\mathfrak{n}}$ and hence u is invertible modulo $\mathfrak{n}$. The bottom row of $M' = \gamma M$ now gives

$$(a_2', b_2') = (ya_1 + ua_2, yb_1 + ub_2)$$

and hence (3) holds. This also show that (1) implies (4b). Moreover, $a_2' = ya_1 + ua_2 \in \mathfrak{an} + \langle a_2\rangle$ implies $\mathfrak{an} + \langle a_2'\rangle \subseteq \mathfrak{an} + \langle a_2\rangle$, so by symmetry $\mathfrak{an} + \langle a_2\rangle = \mathfrak{an} + \langle a_2'\rangle = \mathfrak{ad}$ for some $\mathfrak{d} \mid \mathfrak{n}$, giving (4a). Finally, (4c) follows from

$$va_1 - ua_1' = (uw - xy)a_1 - u(wa_1 + xa_2) = -x(a_1y + ua_2) \in \mathfrak{an} + \langle a_2\rangle = \mathfrak{ad}.$$

Now assume (3). Then $ua_2b_2' \equiv a_2'b_2' \equiv ua_2'b_2 \pmod{\mathfrak{abn}}$, so $ua_2b_2'/g \equiv ua_2'b_2/g \pmod{\mathfrak{n}}$. Since u is coprime to $\mathfrak{n}$ we may divide by u on both sides and then multiply by g again to give (2).

Finally, assume (4). We first show that $ub_2 \equiv b_2' \pmod{\mathfrak{bd}}$:

$$\begin{aligned}(ub_2 - b_2')gv &= ub_2(a_1'b_2' - a_2'b_1') - vb_2'(a_1b_2 - a_2b_1)\\ &= b_2b_2'(ua_1' - va_1) + va_2b_1b_2' - ua_2'b_1'b_2 \in \mathfrak{dab}^2,\end{aligned}$$

since $ua_1' - va_1 \in \mathfrak{ad}$ and $a_2, a_2' \in \langle a_2\rangle + \mathfrak{an} = \mathfrak{ad}$. Dividing by gv gives $ub_2 - b_2' \in \mathfrak{bd}$ as required.

If we had $ub_2 - b_2' \in \mathfrak{bn}$ then the hypotheses of (3) would be satisfied and we could conclude. However, since

$$\mathfrak{bd} = \mathfrak{a}^{-1}\mathfrak{b}\mathfrak{ad} = \mathfrak{a}^{-1}\mathfrak{b}(\langle a_2'\rangle + \mathfrak{an}) = \mathfrak{a}^{-1}\mathfrak{b}\,\langle a_2'\rangle + \mathfrak{bn},$$

there exists $w \in \mathfrak{a}^{-1}\mathfrak{b}$ such that $ub_2 - (wa_2' + b_2') \in \mathfrak{bn}$. Setting $M'' = M'\begin{pmatrix}1 & w\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a_1' & b_1''\\ a_2' & b_2''\end{pmatrix}$ with $b_2'' = wa_2' + b_2'$, we have $ub_2 - b_2'' \in \mathfrak{bn}$, so (3) holds with M'' in place of M', as required. □

3 Manin symbols

We continue to work with pairs of ideals $\mathfrak{a}, \mathfrak{b}$ of R in inverse ideal classes.

We have seen that the first column of an $(\mathfrak{a}, \mathfrak{b})$-matrix can be any pair of elements which generate $\mathfrak{a}$. We next characterize which pairs $(a, b) \in \mathfrak{a} \oplus \mathfrak{b}$ occur as a row of an $(\mathfrak{a}, \mathfrak{b})$-matrix; equivalently, which elements of $\mathfrak{a} \oplus \mathfrak{b}$ form part of an R-basis for this free module.

Proposition 5. *Let $\mathfrak{a}, \mathfrak{b}$ be ideals in inverse classes. A pair $(a, b) \in \mathfrak{a} \oplus \mathfrak{b}$ occurs as a row of an $(\mathfrak{a}, \mathfrak{b})$-matrix if and only if*

$$a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1} = R;$$

that is, if and only if the integral ideals $a\mathfrak{a}^{-1}$ and $b\mathfrak{b}^{-1}$ are coprime.

Proof. The stated condition is equivalent to $a\mathfrak{b} + b\mathfrak{a} = \mathfrak{ab}$, and hence to $g \in a\mathfrak{b} + b\mathfrak{a}$, where g is generator of $\mathfrak{ab}$. If $\begin{pmatrix}a_1 & b_1\\ a_2 & b_2\end{pmatrix}$ is an $(\mathfrak{a}, \mathfrak{b})$-matrix with determinant g, then $g = a_1b_2 - b_1a_2 \in a_1\mathfrak{b} + b_1\mathfrak{a}$, so (a_1, b_1) satisfies the condition; similarly so does (a_2, b_2). Conversely, if $g \in a\mathfrak{b} + b\mathfrak{a}$, write $g = ab_2 - ba_2$ with $a_2 \in \mathfrak{a}$ and $b_2 \in \mathfrak{b}$, and then $\begin{pmatrix}a & b\\ a_2 & b_2\end{pmatrix}$ is an $(\mathfrak{a}, \mathfrak{b})$-matrix. □

Proposition 6. *Let $\gamma_i = \begin{pmatrix}a_i & b_i\\ c_i & d_i\end{pmatrix} \in \Gamma$ for $i = 1, 2$. Then*

$$\Gamma_0(\mathfrak{n})\gamma_1 = \Gamma_0(\mathfrak{n})\gamma_2 \iff c_1d_2 \equiv c_2d_1 \pmod{\mathfrak{n}}.$$

Proof. This follows from (1) $\iff$ (2) in Theorem 3, taking $\mathfrak{a} = \mathfrak{b} = R$ and $M_i = \gamma_i$. □

The set of coprime pairs $(c, d) \in R \oplus R$ modulo the equivalence relation

$$(c_1, d_1) \sim (c_2, d_2) \iff c_1d_2 \equiv c_2d_1 \pmod{\mathfrak{n}}$$

is simply $\mathbb{P}^1(R/\mathfrak{n})$. Its elements have been called M-symbols or $(c:d)$-symbols of level $\mathfrak{n}$, and have been extensively used in explicit computations with modular symbols: see [6] or [11], for example, for the case $K=\mathbb{Q}$, and [4] for when K is imaginary quadratic of class number one.

We now define, more generally, M-symbols of level $\mathfrak{n}$ and *type* $(\mathfrak{a},\mathfrak{b})$. In our applications we will always be free to choose ideals representing each ideal class, which simplifies the definition: thus we now restrict to the situation where $\mathfrak{ab}$ and $\mathfrak{n}$ are coprime. Assuming this, an *M-symbol of level* $\mathfrak{n}$ *and type* $(\mathfrak{a},\mathfrak{b})$ is defined to be an equivalence class of pairs $(a,b)\in\mathfrak{a}\oplus\mathfrak{b}$ satisfying $a\mathfrak{a}^{-1}+b\mathfrak{b}^{-1}=R$, modulo the equivalence relation

$$\begin{aligned}(a,b)\sim(a',b') &\iff ab'\equiv a'b \pmod{\mathfrak{n}}\\ &\iff \begin{cases}\text{there exists } u\in R \text{ coprime to } \mathfrak{n} \text{ such that}\\ ua\equiv a' \pmod{\mathfrak{n}}\\ ub\equiv b' \pmod{\mathfrak{n}}.\end{cases}\end{aligned}$$

Thus M-symbols of type (R,R) are just elements of $\mathbb{P}^1(R/\mathfrak{n})$; these will be called *principal* M-symbols.

In the more general situation where we do not assume that $\mathfrak{ab}$ and $\mathfrak{n}$ are coprime, the correct equivalence relation would be as follows.

$$\begin{aligned}(a,b)\sim(a',b') &\iff ab'\equiv a'b \pmod{\mathfrak{abn}}\\ &\iff \begin{cases}\text{there exists } u\in R \text{ coprime to } \mathfrak{n} \text{ such that}\\ ua\equiv a' \pmod{\mathfrak{an}}\\ ub\equiv b' \pmod{\mathfrak{bn}}.\end{cases}\end{aligned}$$

The set of M-symbols of level $\mathfrak{n}$ and type $(\mathfrak{a},\mathfrak{b})$ is in bijection with the orbit space $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}$, by Proposition 5 and Theorem 3. Since Γ acts transitively on $X_{\mathfrak{a},\mathfrak{b}}$ by Theorem 2, and $[\Gamma:\Gamma_0(\mathfrak{n})]=\psi(\mathfrak{n})$, we deduce the following.

Proposition 7. *For every pair of ideals* $\mathfrak{a},\mathfrak{b}$ *in inverse classes, the number of M-symbols of level* $\mathfrak{n}$ *and type* $(\mathfrak{a},\mathfrak{b})$ *is* $\psi(\mathfrak{n})$.

Below we will use M-symbols to count the number of $\Gamma_0(\mathfrak{n})$-orbits on cusps. For this it will be useful to able to normalize them in certain ways. The next result generalizes [2, Lemmas 24 and 25] for principal M-symbols and the special case for $K=\mathbb{Q}$ in [6].

Proposition 8. *Let* $\mathfrak{a}$, $\mathfrak{b}$ *be ideals in inverse classes which are both coprime to* $\mathfrak{n}$. *Given* $(a,b)\in\mathfrak{a}\oplus\mathfrak{b}$ *such that* $a\mathfrak{a}^{-1}+b\mathfrak{b}^{-1}+\mathfrak{n}=R$, *there exist* $(a',b')\in\mathfrak{a}\oplus\mathfrak{b}$ *such that* $a'\equiv a \pmod{\mathfrak{n}}$, $b'\equiv b \pmod{\mathfrak{n}}$ *and* $a'\mathfrak{a}^{-1}+b'\mathfrak{b}^{-1}=R$.

In other words, in the definition of M-symbols of type $(\mathfrak{a},\mathfrak{b})$ and level $\mathfrak{n}$ there is no harm in relaxing the condition that $a\mathfrak{a}^{-1}+b\mathfrak{b}^{-1}=R$ to the weaker condition that $a\mathfrak{a}^{-1}+b\mathfrak{b}^{-1}$ is coprime to $\mathfrak{n}$.

Proof. We follow the proof of [2, Lemma 25].

Assume that $b \neq 0$ (otherwise interchange the roles of a and b). We will take $b' = b$ and $a' = a + c$ where $c \in \mathfrak{an}$ is chosen appropriately.

Let $\mathfrak{q}$ be the product of the (finite) set of prime ideals which divide $b\mathfrak{b}^{-1}$ but not $a\mathfrak{a}^{-1}$. Choose $\mathfrak{r}$ coprime to $b\mathfrak{b}^{-1}$ in the inverse class to $\mathfrak{anq}$, so $\mathfrak{anqr} = \langle c\rangle$ with $c \in \mathfrak{an}$. It remains to show that $b\mathfrak{b}^{-1}$ and $a'\mathfrak{a}^{-1}$ are coprime. Let $\mathfrak{p}$ be a prime dividing $b\mathfrak{b}^{-1}$; we show that $\mathfrak{ap} \nmid a'$.

If $\mathfrak{p} \mid a\mathfrak{a}^{-1}$ then $\mathfrak{p} \nmid \mathfrak{q}$ (by construction of $\mathfrak{q}$), $\mathfrak{p} \nmid \mathfrak{n}$ (by hypothesis), and $\mathfrak{p} \nmid \mathfrak{r}$ (by construction of $\mathfrak{r}$), so $p \nmid c\mathfrak{a}^{-1} = \mathfrak{nqr}$. Hence $\mathfrak{ap} \nmid c$, but $\mathfrak{ap} \mid a$ so $\mathfrak{ap} \nmid a'$.

If $\mathfrak{p} \nmid a\mathfrak{a}^{-1}$ then $\mathfrak{p} \mid \mathfrak{q}$ and hence $\mathfrak{p} \mid c\mathfrak{a}^{-1} = \mathfrak{nqr}$, so $\mathfrak{ap} \mid c$. But $\mathfrak{ap} \nmid a$, so again $\mathfrak{ap} \nmid a'$. □

4 Cusps and cusp equivalence

Some of the material in this section appeared in [4, Lemma 2.2.7] for the case of trivial class group, and in the theses of Bygott [2, §1.5] and Lingham [8, §1.4–1.5] for the general case. The results for $\Gamma_1(\mathfrak{n})$ are from the second author's thesis [1]. Also, for K totally real (which makes no difference in our context) some of this material may be found in the literature on Hilbert Modular Forms and related matters: see [13], for example.

By a *cusp* of $\mathrm{GL}_2(K)$ (or simply, a cusp of K) we mean an element of $\mathbb{P}^1(K)$, identified as usual with $K \cup \{\infty\}$.

Over $\mathbb{Q}$, or a field K with trivial class group, we may represent cusps in the form a/b where $a, b \in R$ are coprime, and we allow $b = 0$ for the cusp ∞; this representation is unique up to multiplication of a and b by a unit of R. We may then regard the column vector $\begin{pmatrix} a \\ b \end{pmatrix}$ as the first column of a matrix in Γ, and study the action of Γ and its subgroups on the set $\mathbb{P}^1(K)$ via its action by left multiplication on Γ itself. In the general case we replace this action by left multiplication on $(\mathfrak{a}, \mathfrak{b})$-matrices.

Cusps may be always represented[1] in the form a/b with $a, b \in R$ not both zero, but this representation is far from unique. We do not attempt to normalize the representation of cusps, but instead we allow arbitrary representatives. To each representation $\alpha = a/b$, we may associate the ideal $\langle a, b\rangle$ and its class $[\langle a, b\rangle]$. Given two representatives a/b and a'/b' for the same cusp $\alpha \in \mathbb{P}^1(K)$, the ideals $\langle a, b\rangle$ and $\langle a', b'\rangle$ need not be equal but they have the same class:

Proposition 9. *If $a/b = a'/b' \in \mathbb{P}^1(K)$ then $[\langle a, b\rangle] = [\langle a', b'\rangle]$. Moreover, given any ideal $\mathfrak{a}$ in the class $[\langle a, b\rangle]$, there is a representative a'/b' of the cusp a/b whose ideal is $\langle a', b'\rangle = \mathfrak{a}$.*

[1] We avoid the common notation $(a : b)$ in order to avoid confusion with M-symbols.

Proof. From $a/b = a'/b'$ we have $ab' = a'b$. If $b = 0$ then $b' = 0$ and vice versa, and in this case both ideal classes are trivial. Otherwise we have $b' \langle a, b\rangle = \langle a', b'\rangle b$ so that $[\langle a, b\rangle] = [\langle a', b'\rangle]$.

If $[\mathfrak{a}] = [\langle a, b\rangle]$ then there exist nonzero $c, d \in R$ with $d\mathfrak{a} = c\langle a, b\rangle$, so $\mathfrak{a} = \langle a', b'\rangle$ with $a' = ca/d$, $b' = cb/d \in \mathfrak{a} \subseteq R$, and $a/b = a'/b' \in \mathbb{P}^1(K)$. □

Hence we have a well-defined *class* $[\alpha] \in \mathrm{Cl}(K)$ for each cusp $\alpha \in \mathbb{P}^1(K)$, and for every ideal $\mathfrak{a} \in [\alpha]$, there is a representative $\alpha = a/b$ with $\langle a, b\rangle = \mathfrak{a}$. If two representatives a/b, a'/b' have the same ideal $\mathfrak{a} = \langle a, b\rangle = \langle a', b'\rangle$ then there is a unit $u \in R^\times$ with $a' = ua$, $b' = ub$; for we may define $u = a'/a = b'/b$ (omitting one of these if $a = a' = 0$ or $b = b' = 0$), and then $u\mathfrak{a} = \mathfrak{a}$ so $u \in R^\times$.

We now consider the actions of Γ, $\Gamma_0(\mathfrak{n})$ and $\Gamma_1(\mathfrak{n})$ on the set of cusps (by linear fractional transformations), and on the set of representatives $\begin{pmatrix} a \\ b \end{pmatrix} \in R^2 \setminus \{0\}$ (by left multiplication). The natural map $\pi : R^2 \setminus \{0\} \to \mathbb{P}^1(K)$ sending $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto a/b$ is clearly Γ-equivariant.

Cusp equivalence under Γ

Theorem 4. *The ideal $\langle a, b\rangle$ associated to $\begin{pmatrix} a \\ b \end{pmatrix}$ is Γ-invariant. Conversely, if $\langle a, b\rangle = \langle a', b'\rangle$ then there exists $\gamma \in \Gamma$ such that $\gamma \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a' \\ b' \end{pmatrix}$.*

Proof. If $\begin{pmatrix} a' \\ b' \end{pmatrix} = \gamma \begin{pmatrix} a \\ b \end{pmatrix}$ with $\gamma \in \Gamma$, then $a', b' \in \langle a, b\rangle$, so $\langle a', b'\rangle \subseteq \langle a, b\rangle$, and the situation is symmetric so $\langle a', b'\rangle = \langle a, b\rangle$.

For the second part, let $\mathfrak{a} = \langle a, b\rangle = \langle a', b'\rangle$, let $\mathfrak{b}$ be an ideal in the inverse class to $\mathfrak{a}$, and let g be a generator of $\mathfrak{ab}$. Let M_1 and M_2 be $(\mathfrak{a}, \mathfrak{b})$-matrices with determinant g and first columns $\begin{pmatrix} a \\ b \end{pmatrix}$ and $\begin{pmatrix} a' \\ b' \end{pmatrix}$ respectively. Then $\gamma = M_2 M_1^{-1} \in \Gamma$ and from $\gamma M_1 = M_2$ we have $\gamma \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a' \\ b' \end{pmatrix}$. □

The following result is classical and was certainly known in the 19th century to Hurwitz, Humbert, Bianchi and others. It also appears in the literature on Bianchi and Hilbert modular forms (see Proposition 1.1 in van der Geer [13]).

Theorem 5. *The association $\alpha \mapsto [\alpha]$ defines a bijection $\Gamma\backslash\mathbb{P}^1(K) \to \mathrm{Cl}(K)$.*

Proof. The map $\alpha = a/b \mapsto [\langle a, b\rangle]$ induces a well-defined map $\Gamma\backslash\mathbb{P}^1(K) \to \mathrm{Cl}(K)$ by Proposition 9, which is obviously surjective. It is injective since if a/b and a'/b' have the same class then by Proposition 9 we may assume

they have the same ideal, and then Theorem 4 says that they are in the same Γ-orbit. □

When the class group is trivial one normally chooses representatives for cusps "in lowest terms", *i.e.*, as a/b with $\langle a, b\rangle = \langle 1\rangle = R$. In any case, we can always choose representatives whose ideal is coprime to any given ideal, such as the level.

For $\alpha = a/b \in \mathbb{P}^1(K)$, we define the *denominator ideal* of α, denoted $\mathfrak{d}(\alpha)$, to be the ideal $\langle b\rangle / \langle a, b\rangle$. The denominator ideal is independent of the representation $\alpha = a/b$. For $\alpha \neq 0, \infty$ we may write the principal fractional ideal αR uniquely as $\alpha R = \mathfrak{a}\mathfrak{b}^{-1}$ with $\mathfrak{a}, \mathfrak{b}$ coprime integral ideals, and then $\mathfrak{d}(\alpha) = \mathfrak{b}$. In this notation we have $[\mathfrak{a}] = [\mathfrak{b}] = [\langle a, b\rangle]^{-1}$. $\mathfrak{b}\,\langle a, b\rangle = \langle b\rangle$. If $\alpha \neq \infty$, then $\mathfrak{d}(\alpha) = \{b \in R \mid b\alpha \in R\} = R \cap \alpha^{-1}R$, so $\mathfrak{d}(\alpha)$ is the set of all denominators of representatives of α.

Cusp equivalence under $\Gamma_0(\mathfrak{n})$

Fix a nonzero ideal $\mathfrak{n}$. We now describe the orbits of $\mathbb{P}^1(K)$ under $\Gamma_0(\mathfrak{n})$.

To each cusp α, we assign the ideal $\mathfrak{d}_\mathfrak{n}(\alpha) = \mathfrak{d}(\alpha) + \mathfrak{n}$, a divisor of $\mathfrak{n}$. We will see in Theorem 6 below that this is well-defined and $\Gamma_0(\mathfrak{n})$-invariant. Thus, two necessary conditions for cusps α, α' to be $\Gamma_0(\mathfrak{n})$-equivalent are that $[\alpha] = [\alpha']$ and $\mathfrak{d}_\mathfrak{n}(\alpha) = \mathfrak{d}_\mathfrak{n}(\alpha')$. It remains to see how to distinguish cusps in the same class and with same value of $\mathfrak{d}_\mathfrak{n}(\alpha)$, and to count them.

The following condition for cusps in the same class to be $\Gamma_0(\mathfrak{n})$-equivalent is a generalization of [6, Lemma 2.2.3]; most of the work has already been done in Theorem 3.

Theorem 6. *Let α, α' be two cusps in the same ideal class. Choose representatives $\alpha = a_1/a_2$ and $\alpha' = a_1'/a_2'$ with the same ideal $\mathfrak{a} = \langle a_1, a_2\rangle = \langle a_1', a_2'\rangle$. Then the following are equivalent:*

1. *There exists $\gamma \in \Gamma_0(\mathfrak{n})$ such that $\gamma(\alpha) = \alpha'$;*
2. *There exist $u \in R$ coprime to $\mathfrak{n}$ and $v \in R^\times$ and a divisor $\mathfrak{d}$ of $\mathfrak{n}$ such that*
   - *a. $\mathfrak{d}_\mathfrak{n}(\alpha) = \mathfrak{d}_\mathfrak{n}(\alpha') = \mathfrak{d}$.*
   - *b. $a_2' \equiv u a_2 \pmod{\mathfrak{n}\mathfrak{a}}$.*
   - *c. $u a_1' \equiv v a_1 \pmod{\mathfrak{d}\mathfrak{a}}$.*

In case $\mathfrak{a}$ and $\mathfrak{n}$ are coprime we can replace the moduli in conditions 2(b), 2(c) by $\mathfrak{n}$ and $\mathfrak{d}$ respectively.

Proof. The existence of $\gamma \in \Gamma_0(\mathfrak{n})$ with $\gamma(\alpha) = \alpha'$ is equivalent to the existence of $\gamma \in \Gamma_0(\mathfrak{n})$ with $\gamma \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a_1' \\ a_2' \end{pmatrix}$, since we are free to multiply γ by a unit times the identity matrix. Hence if $\gamma(\alpha) = \alpha'$ with $\gamma \in \Gamma_0(\mathfrak{n})$, we

may assume that $\gamma \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a_1' \\ a_2' \end{pmatrix}$. Let M be an $(\mathfrak{a}, \mathfrak{b})$-matrix with first column $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$, and $M' = \gamma M$, which is an $(\mathfrak{a}, \mathfrak{b})$-matrix with first column $\begin{pmatrix} a_1' \\ a_2' \end{pmatrix}$. Now (2) follows from Theorem 3.

For the converse, assume that (2) holds. Again, using Theorem 3 we see that there exist $(\mathfrak{a}, \mathfrak{b})$-matrices M and $M' = \gamma M$ with $\gamma \in \Gamma_0(\mathfrak{n})$ and first columns $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ and $\begin{pmatrix} a_1' \\ a_2' \end{pmatrix}$, so $\gamma \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a_1' \\ a_2' \end{pmatrix}$ as required.

For the last part, when $\mathfrak{a} + \mathfrak{n} = \langle 1 \rangle$ we have first $\mathfrak{d}_{\mathfrak{n}}(\alpha) = \langle a_2 \rangle / \mathfrak{a} + \mathfrak{n} = \langle a_2 \rangle + \mathfrak{n}$; then $a_2' - u a_2 \in \mathfrak{n} \iff a_2' - u a_2 \in \mathfrak{a}\mathfrak{n}$ since certainly $a_2' - u a_2 \in \mathfrak{a}$, and similarly $u a_1' - v a_1 \in \mathfrak{a}\mathfrak{d} \iff u a_1' - v a_1 \in \mathfrak{d}$. $\square$

We also give the following criterion, generalizing [6, Prop. 2.2.3(3)]. This is more convenient when it comes to testing two cusps for $\Gamma_0(\mathfrak{n})$-equivalence.

Corollary 2. *Let α, α' be cusps with $[\alpha] = [\alpha']$, let $\mathfrak{a}$ be an ideal in the class $[\alpha]$ which is coprime to $\mathfrak{n}$, and let $\mathfrak{b}$ be an ideal in the inverse class. Write the two cusps as $\alpha = a_1/a_2$ and $\alpha' = a_1'/a_2'$ with $\langle a_1, a_2 \rangle = \langle a_1', a_2' \rangle = \mathfrak{a}$. Form $(\mathfrak{a}, \mathfrak{b})$-matrices $M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ and $M' = \begin{pmatrix} a_1' & b_1' \\ a_2' & b_2' \end{pmatrix}$. Then α and α' are $\Gamma_0(\mathfrak{n})$-equivalent if and only if $\mathfrak{d}_{\mathfrak{n}}(\alpha) = \mathfrak{d}_{\mathfrak{n}}(\alpha')$ and there exists $v \in R^\times$ such that*

$$a_2' b_2 \equiv v a_2 b_2' \pmod{\mathfrak{a}\mathfrak{b}\mathfrak{d}^2}$$

where $\mathfrak{d} = \mathfrak{d}_{\mathfrak{n}}(\alpha)$.

Proof. If $\gamma \in \Gamma_0(\mathfrak{n})$ satisfies $\gamma(\alpha) = \alpha'$ then (after multiplying γ by a unit if necessary), $\gamma M = M''$ where M'' has the same first column as M'. Thus $M'' = \begin{pmatrix} a_1' & b_1'' \\ a_2' & b_2'' \end{pmatrix} = M' \begin{pmatrix} 1 & w \\ 0 & v \end{pmatrix}$ where $w \in \mathfrak{a}^{-1}\mathfrak{b}$ and $v = \det \gamma \det M \det M'^{-1} \in R^\times$. Now Theorem 3 implies that $a_2' b_2 - a_2 b_2'' \in \mathfrak{a}\mathfrak{b}\mathfrak{n}$, so $a_2' b_2 - v a_2 b_2' \in \mathfrak{a}^{-1}\mathfrak{b} \langle a_2 a_2' \rangle + \mathfrak{a}\mathfrak{b}\mathfrak{n}$. The latter ideal can be seen to equal $\mathfrak{a}\mathfrak{b}\mathfrak{d}^2$, where $\mathfrak{d} = \mathfrak{d}_{\mathfrak{n}}(\alpha) = \mathfrak{d}_{\mathfrak{n}}(\alpha')$, these being equal by the Proposition.

Conversely, suppose that $\mathfrak{d} = \mathfrak{d}_{\mathfrak{n}}(\alpha) = \mathfrak{d}_{\mathfrak{n}}(\alpha')$ and the congruence $a_2' b_2 \equiv v a_2 b_2' \pmod{\mathfrak{a}\mathfrak{b}\mathfrak{d}^2}$ holds. Noting again that $\mathfrak{a}\mathfrak{b}\mathfrak{d}^2 = \mathfrak{a}^{-1}\mathfrak{b} \langle a_2 a_2' \rangle + \mathfrak{a}\mathfrak{b}\mathfrak{n}$, this implies the existence of $w \in \mathfrak{a}^{-1}\mathfrak{b}$ such that $a_2' b_2 - a_2 b_2'' \in \mathfrak{a}\mathfrak{b}\mathfrak{n}$ where $b_2'' = w a_2' + v b_2'$. Then $\gamma = M'' M^{-1} = M' \begin{pmatrix} 1 & w \\ 0 & v \end{pmatrix} M^{-1} \in \Gamma_0(\mathfrak{n})$ so $\gamma M = M''$ and hence $\gamma(\alpha) = \alpha'$. $\square$

Finally we will find a formula for the number of $\Gamma_0(\mathfrak{n})$-equivalence classes. In the case $\mathfrak{n} = R$ we have seen that the number is the class number of R.

There are two different approaches to this enumeration, which we call the "vertical" and "horizontal" approaches. First of all, from general principles

of group actions, each Γ-orbit of cusps splits into a finite union of $\Gamma_0(\mathfrak{n})$-sub-orbits, in bijection with the set of double cosets $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$, where α is any cusp in the orbit and $\Gamma_\alpha \leq \Gamma$ is its stabilizer.

The vertical approach, which is more direct, is to first consider the coset space Γ/Γ_α, which is in bijection with the cusps in the orbit $\Gamma\alpha$, and then consider how $\Gamma_0(\mathfrak{n})$ acts on this. We call this approach "vertical" since in the case $\alpha = \infty$ we are essentially looking at the action of $\Gamma_0(\mathfrak{n})$ on column vectors, the first columns of elements of Γ. In general this approach would require considering one cusp α in each class, which would be complicated since the stabilizer Γ_α is not so simple in general as when $\alpha = \infty$.

A variation on the vertical approach is possible using $(\mathfrak{a}, \mathfrak{b})$-matrices. Fix an ideal class, an ideal $\mathfrak{a}$ in that class and an ideal $\mathfrak{b}$ in the inverse class. Cusps in class $[\mathfrak{a}]$ all have representations with ideal $\mathfrak{a}$, and so are of the form $\alpha = M(\infty)$ where M is an $(\mathfrak{a}, \mathfrak{b})$-matrix. Now the $\Gamma_0(\mathfrak{n})$-sub-orbits of $\Gamma\alpha$ are also in bijection with double cosets $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}/\Delta_0(\mathfrak{a}, \mathfrak{b})$. The equivalence may be seen by fixing one $M_0 \in X_{\mathfrak{a},\mathfrak{b}}$ and observing that $X_{\mathfrak{a},\mathfrak{b}} = \Gamma M_0$ by Theorem 2, and $M_0\Delta_0(\mathfrak{a}, \mathfrak{b})M_0^{-1} = \Gamma_\alpha$ where $\alpha = M_0(\infty)$, since $\Delta_0(\mathfrak{a}, \mathfrak{b}) = \{M \in \Delta(\mathfrak{a}, \mathfrak{b}) \mid M(\infty) = \infty\}$. Hence from a double coset decomposition

$$\Gamma = \bigsqcup_i \Gamma_0(\mathfrak{n})\gamma_i\Gamma_\alpha$$

with γ_i in a set of representatives of $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$, we obtain

$$X_{\mathfrak{a},\mathfrak{b}} = \Gamma M_0 = \bigsqcup_i \Gamma_0(\mathfrak{n})\gamma_i\Gamma_\alpha M_0 = \bigsqcup_i \Gamma_0(\mathfrak{n})M_i\Delta_0(\mathfrak{a}, \mathfrak{b}) = \bigsqcup_i \Gamma_0(\mathfrak{n})M_i\Delta_1(\mathfrak{a}, \mathfrak{b})$$

with $M_i = \gamma_i M_0$ in a set of representatives of $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}/\Delta_1(\mathfrak{a}, \mathfrak{b})$; the last equality follows from $\Delta_0(\mathfrak{a}, \mathfrak{b}) = R^\times\Delta_1(\mathfrak{a}, \mathfrak{b})$ and the unit scalars may be absorbed in $\Gamma_0(\mathfrak{n})$. Viewing $X_{\mathfrak{a},\mathfrak{b}}/\Delta_1(\mathfrak{a}, \mathfrak{b})$ as the set of first columns of $(\mathfrak{a}, \mathfrak{b})$-matrices, and considering the left action of $\Gamma_0(\mathfrak{n})$ on this set, gives the vertical approach used in Theorem 6 to determine $\Gamma_0(\mathfrak{n})$-equivalence of cusps.

The horizontal approach proceeds instead as follows. For the principal class, we may enumerate $\Gamma_0(\mathfrak{n})\backslash\Gamma/\Gamma_\alpha$ by first taking the coset space $\Gamma_0(\mathfrak{n})\backslash\Gamma$, which is represented by the set of principal M-symbols $(c : d)$, and then considering the right action of Γ_α on this set, for any principal cusp α. In the case $K = \mathbb{Q}$ this is the approach used[2] by Shimura in [10, Prop. 1.43(4)], using $\alpha = 0$.

In our situation we would need to consider the action of more general stabilizers Γ_α on the set of M-symbols, which is not very convenient. However, the alternative formulation in terms of $(\mathfrak{a}, \mathfrak{b})$-matrices works instead. We may enumerate $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}/\Delta_1(\mathfrak{a}, \mathfrak{b})$ by considering the action of $\Delta_1(\mathfrak{a}, \mathfrak{b})$ on the

[2] Note that the definition marked (*) on [10, p. 25] is not quite correct as stated: in each residue class modulo N/d one must take a representative c which is coprime to d, if one exists, but one cannot restrict to the range $0 < c \leq N/d$.

set $\Gamma_0(\mathfrak{n})\backslash X_{\mathfrak{a},\mathfrak{b}}$ of M-symbols of type $(\mathfrak{a},\mathfrak{b})$. This leads to the following result, which generalizes the classical formula when $R=\mathbb{Z}$. Here, $\varphi_u(\mathfrak{m})$ is defined by

$$\varphi_u(\mathfrak{m}) = \#((R/\mathfrak{m})^\times/R^\times).$$

Theorem 7. *Each Γ-orbit on $\mathbb{P}^1(K)$ splits into $\sum_{\mathfrak{d}|\mathfrak{n}} \varphi_u(\mathfrak{d}+\mathfrak{n}\mathfrak{d}^{-1})$ disjoint $\Gamma_0(\mathfrak{n})$-orbits. Hence the total number of $\Gamma_0(\mathfrak{n})$-orbits of cusps is*

$$h\sum_{\mathfrak{d}|\mathfrak{n}} \varphi_u(\mathfrak{d}+\mathfrak{n}\mathfrak{d}^{-1})$$

where h is the class number of R.

Proof (using vertical approach). For each ideal class we choose an ideal $\mathfrak{a}$ in that class and a divisor $\mathfrak{d}$ of $\mathfrak{n}$, and count $\Gamma_0(\mathfrak{n})$-orbits of cusps in the class represented as $\alpha=a_1/a_2$ with $\langle a_1,a_2\rangle=\mathfrak{a}$ and $\mathfrak{d}_\mathfrak{n}(\alpha)=\mathfrak{d}$. To see that there is at least one such cusp, let $\mathfrak{b}$ be an ideal coprime to $\mathfrak{n}$ in the class inverse to $\mathfrak{d}\mathfrak{a}$, so that $\mathfrak{d}\mathfrak{a}\mathfrak{b}=\langle a_2\rangle$ for some $a_2\in R$. Now $a_2\in\mathfrak{a}$, so $\mathfrak{a}=\langle a_1,a_2\rangle$ for some $a_1\in R$, and we take $\alpha=a_1/a_2$. Now $\mathfrak{d}_\mathfrak{n}(\alpha)=\langle a_2\rangle+\mathfrak{n}=\mathfrak{d}\mathfrak{a}\mathfrak{b}+\mathfrak{n}=\mathfrak{d}$, since $\mathfrak{a}\mathfrak{b}$ is coprime to $\mathfrak{n}$. This argument, together with condition (2) of Theorem 6, shows that every $\Gamma_0(\mathfrak{n})$-orbit of cusps α with this class and this denominator ideal $\mathfrak{d}_\mathfrak{n}(\alpha)$ has a representative with this specific denominator a_2. It remains to examine when a_1/a_2 and a_1'/a_2 with $\mathfrak{a}=\langle a_1,a_2\rangle=\langle a_1',a_2\rangle$ are $\Gamma_0(\mathfrak{n})$-equivalent; one finds (though we omit the details) that the number of such cusps, up to $\Gamma_0(\mathfrak{n})$-equivalence, is $\varphi_u(\mathfrak{d}+\mathfrak{n}\mathfrak{d}^{-1})$. □

Proof (using horizontal approach). Let $\mathfrak{a}$ and $\mathfrak{b}$ be as in the first proof; again we show that the number of orbits of cusps in class $[\mathfrak{a}]$ is $\sum_{\mathfrak{d}|\mathfrak{n}} \varphi_u(\mathfrak{d}+\mathfrak{n}\mathfrak{d}^{-1})$, independent of the class of $\mathfrak{a}$.

The action of $\Delta_1(\mathfrak{a},\mathfrak{b})$ on the set of all M-symbols of type $(\mathfrak{a},\mathfrak{b})$ is given by

$$(a:b)\begin{pmatrix}1 & y\\ 0 & w\end{pmatrix} = (a: ya+wb).$$

We saw earlier that this number of orbits of cusps in class $[\mathfrak{a}]$ is the same as the number of right $\Delta_1(\mathfrak{a},\mathfrak{b})$-orbits under this action.

We first classify M-symbols by the possible values of a. To each $(a:b)$ we associate the divisor $\mathfrak{d}=\langle a\rangle+\mathfrak{n}=a\mathfrak{a}^{-1}+\mathfrak{n}$ of $\mathfrak{n}$. This is well-defined since if $(a:b)=(a':b')$ then there exists $u\in R$ coprime to $\mathfrak{n}$ such that $a\equiv ua'$ (mod $\mathfrak{n}$) which implies that $\langle a\rangle+\mathfrak{n}=\langle a'\rangle+\mathfrak{n}$.

Fix a divisor $\mathfrak{d}$ of $\mathfrak{n}$. Choose $\mathfrak{d}'$ coprime to $\mathfrak{n}$ such that $\mathfrak{d}\mathfrak{d}'\mathfrak{a}=\langle a\rangle$ is principal. Then $\langle a\rangle+\mathfrak{n}=\mathfrak{d}$ (since $\mathfrak{a}\mathfrak{d}'$ is coprime to $\mathfrak{n}$). Now for any M-symbol $(a':b')$ with $\langle a'\rangle+\mathfrak{n}=\mathfrak{d}=\langle a\rangle+\mathfrak{n}$, there exists u coprime to $\mathfrak{n}$ such that $a\equiv ua'$ (mod $\mathfrak{n}$); then $(a':b')=(ua':ub')=(a:b)$ with $b=ub'$. This shows that every M-symbol associated with the fixed divisor $\mathfrak{d}$ has the form $(a:b)$ with this fixed value of a and some $b\in\mathfrak{b}$. Note that for this step we required

the validity of M-symbols of the form $(a : b)$ where $a\mathfrak{a}^{-1}$ and $b\mathfrak{b}^{-1}$ are not necessarily coprime but such that $a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1}$ is coprime to $\mathfrak{n}$.

For fixed a, consider M-symbols of the form $(a : b)$ under M-symbol equivalence and the action of $\Delta_1(\mathfrak{a}, \mathfrak{b})$ as above. For such a symbol we have

$$\langle b \rangle + \mathfrak{d} + \mathfrak{n}/\mathfrak{d} = b\mathfrak{b}^{-1} + a\mathfrak{a}^{-1} + \mathfrak{n}/\mathfrak{d} = \langle 1 \rangle .$$

Also,

$$(a : b) = (a : b') \iff b \equiv b' \pmod{\mathfrak{n}/\mathfrak{d}}$$

since

$$\begin{aligned} (a : b) = (a : b') &\iff \mathfrak{n} \mid a(b - b') = \mathfrak{d}\mathfrak{d}'\mathfrak{a}(b - b') \\ &\iff \mathfrak{n} \mid \mathfrak{d}(b - b') \\ &\iff \mathfrak{n}/\mathfrak{d} \mid b - b'. \end{aligned}$$

Moreover, under the $\Delta_1(\mathfrak{a}, \mathfrak{b})$-action, we have

$$(a : b) \mapsto (a : b') = (a : b) \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = (a : ay + b) \qquad \text{for all} \quad y \in \mathfrak{a}^{-1}\mathfrak{b},$$

so this action identifies $(a : b)$ and $(a : b')$ whenever $b - b' \in \langle a \rangle\, \mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{d}\mathfrak{d}'\mathfrak{b}$. Since $\mathfrak{n}/\mathfrak{d} + \mathfrak{d}\mathfrak{d}'\mathfrak{b} = \mathfrak{n}/\mathfrak{d} + \mathfrak{d}$, we may identify $(a : b)$ and $(a : b')$ whenever $b \equiv b' \pmod{\mathfrak{d} + \mathfrak{n}/\mathfrak{d}}$. So the number of orbits of the smaller group $\Delta_{1,1}(\mathfrak{a}, \mathfrak{b})$ is exactly $\varphi(\mathfrak{d} + \mathfrak{n}/\mathfrak{d})$. Taking into account the units we find the (possibly) smaller number $\varphi_u(\mathfrak{d} + \mathfrak{n}/\mathfrak{d})$, and this gives the result as stated. □

Cusp equivalence under $\Gamma_1(\mathfrak{n})$

We can adapt our results about M-symbols and cusp equivalence for the congruence subgroup $\Gamma_0(\mathfrak{n})$ to obtain similar results for $\Gamma_1(\mathfrak{n})$. Over $\mathbb{Q}$, this was done by the first author in [5]; see also [11, Chap. 8]. The proofs are similar to those for $\Gamma_0(\mathfrak{n})$, and can be found in the second author's thesis [1], so will be omitted.

We start by studying the left action of $\Gamma_1(\mathfrak{n})$ on the set of $(\mathfrak{a}, \mathfrak{b})$-matrices, with a result analogous to Theorem 3.

Theorem 8. *Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in inverse classes, and let $M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ and $M' = \begin{pmatrix} a_1' & b_1' \\ a_2' & b_2' \end{pmatrix}$ be any two $(\mathfrak{a}, \mathfrak{b})$-matrices. Then the following statements are equivalent:*

1. $M' = \gamma M$ with $\gamma \in \Gamma_1(\mathfrak{n})$.
2. The following congruences hold:

a. $a_2'b_2 \equiv a_2b_2' \pmod{\mathfrak{abn}}$,
b. $a_2 \equiv a_2' \pmod{\mathfrak{n}}$,
c. $b_2 \equiv b_2' \pmod{\mathfrak{m}}$.

3. There exists $u \in 1+\mathfrak{n}$ *such that:*

a. $a_2' = ua_2 \pmod{\mathfrak{an}}$,
b. $b_2' = ub_2 \pmod{\mathfrak{bn}}$.

If any of these equivalent statements holds, then there exist $v \in R^\times$, $u \in 1+\mathfrak{n}$ *and* $\mathfrak{d} \mid \mathfrak{n}$ *such that:*

1. $\langle a_2\rangle + \mathfrak{an} = \langle a_2\rangle + \mathfrak{an} = \mathfrak{ad}$,
2. $a_2' \equiv ua_2 \pmod{\mathfrak{an}}$,
3. $ua_1' \equiv va_1 \pmod{\mathfrak{ad}}$.

Conversely, if these conditions hold, there exists $\gamma \in \Gamma_1(\mathfrak{n})$ *such that*

$$\gamma M = M'' = M' \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix} \qquad \text{with} \qquad w \in \mathfrak{a}^{-1}\mathfrak{b}.$$

Proof. Similar to Theorem 3: see [1, p. 34] for details. □

Now we can adapt the definition of M-symbols for $\Gamma_0(\mathfrak{n})$ to obtain a set of symbols in bijection with the cosets of $\Gamma_0(\mathfrak{n})$ in Γ. As before, we assume, as we may, that $\mathfrak{ab}$ and $\mathfrak{n}$ are coprime. Then an *M-symbol of level* $\mathfrak{n}$ *and type* $(\mathfrak{a},\mathfrak{b})$ *for* $\Gamma_1(\mathfrak{n})$ is an equivalence class of

$$\left\{(a,b) \in \mathfrak{a}\oplus\mathfrak{b} :\ a\mathfrak{a}^{-1} + b\mathfrak{b}^{-1} = R\right\} / \sim,$$

where:

$$(a,b) \sim (a',b') \iff \begin{cases} a \equiv a' \pmod{\mathfrak{n}} \\ b \equiv b' \pmod{\mathfrak{n}}. \end{cases}$$

We refer to M-symbols of type (R,R) and level $\mathfrak{n}$ as *principal M-symbols of level* $\mathfrak{n}$ *for* $\Gamma_1(\mathfrak{n})$, and note that principal M-symbols are a direct generalization of the M-symbols for $\Gamma_1(N)$ introduced in [5].

If $(\mathfrak{a},\mathfrak{b})$ and $\mathfrak{n}$ are not coprime, then the appropriate equivalence relation to use is more complicated:

$$\begin{aligned}(a,b) \sim (a',b') &\iff ab' \equiv a'b \pmod{\mathfrak{abn}} \text{ and } \begin{cases} a \equiv a' \pmod{\mathfrak{an}} \\ b \equiv b' \pmod{\mathfrak{bn}} \end{cases} \\ &\iff \text{there exists } u \in R \text{ such that } u-1 \in \mathfrak{n} \text{ and} \\ &\qquad \begin{cases} ua \equiv a' \pmod{\mathfrak{an}} \\ ub \equiv b' \pmod{\mathfrak{bn}}. \end{cases}\end{aligned}$$

It is clear from the definition that we have a bijection between M-symbols of type $(\mathfrak{a},\mathfrak{b})$ and level $\mathfrak{n}$ for $\Gamma_1(\mathfrak{n})$ and orbits of $(\mathfrak{a},\mathfrak{b})$-matrices under the action of $\Gamma_1(\mathfrak{n})$. We also have an analogue to Proposition 7.

Proposition 10. *For every pair of ideals $\mathfrak{a}, \mathfrak{b}$ in inverse classes, the number of M-symbols of level $\mathfrak{n}$ and type $(\mathfrak{a}, \mathfrak{b})$ for $\Gamma_1(\mathfrak{n})$ is $[\Gamma : \Gamma_1(\mathfrak{n})]$.*

Our final result gives a test for $\Gamma_1(\mathfrak{n})$-equivalence of cusps.

Let α, α' be two cusps in the same ideal class, and choose representatives $\alpha = a_1/a_2$ and $\alpha' = a_1'/a_2'$ with the same ideal $\mathfrak{a} = \langle a_1, a_2\rangle = \langle a_1', a_2'\rangle$. In our study of $\Gamma_0(\mathfrak{n})$-orbits of cusps, we used the equivalence between the existence of an element $\gamma \in \Gamma_0(\mathfrak{n})$ with $\gamma(\alpha) = \alpha'$ and the existence of $\gamma \in \Gamma_0(\mathfrak{n})$ such that $\gamma \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a_1' \\ a_2' \end{pmatrix}$. This equivalence holds because $\Gamma_0(\mathfrak{n})$ contains all matrices of the form wI, where $w \in R^\times$ and I is the 2×2 identity matrix. This is not true for $\Gamma_1(\mathfrak{n})$ in general (it holds only if $w - 1 \in \mathfrak{n}$). Instead, we have the following, whose proof is straightforward:

Lemma 1. *Let α, α' be two cusps in the same ideal class. Choose representatives $\alpha = a_1/a_2$ and $\alpha' = a_1'/a_2'$ with the same ideal $\mathfrak{a} = \langle a_1, a_2\rangle = \langle a_1', a_2'\rangle$. Then the following are equivalent:*

1. *There exists $\gamma \in \Gamma_1(\mathfrak{n})$ such that $\gamma\alpha = \alpha'$.*
2. *There exist $\gamma \in \Gamma_1(\mathfrak{n})$ and $w \in R^\times$ such that*

$$\gamma \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a_1' \\ wa_2' \end{pmatrix}.$$

Theorem 9. *Let α, α' be two cusps in the same ideal class. Choose representatives $\alpha = a_1/a_2$ and $\alpha' = a_1'/a_2'$ with the same ideal $\mathfrak{a} = \langle a_1, a_2\rangle = \langle a_1', a_2'\rangle$. Then the following are equivalent:*

1. *α and α' are $\Gamma_1(\mathfrak{n})$-equivalent;*
2. *there exist $u \in R$ such that $u \in 1 + \mathfrak{n}$, $v, w \in R^\times$ and $\mathfrak{d} \mid \mathfrak{n}$ such that:*
   a. $\mathfrak{d}_\mathfrak{n}(\alpha) = \mathfrak{d}_\mathfrak{n}(\alpha') = \mathfrak{d}$,
   b. $wa_2' \equiv ua_2 \pmod{\mathfrak{a}\mathfrak{n}}$,
   c. $ua_1' \equiv va_1 \pmod{\mathfrak{a}\mathfrak{d}}$.

In case $\mathfrak{a}$ and $\mathfrak{n}$ are coprime, we can replace the moduli in conditions 2(b), 2(c) by $\mathfrak{n}$ and $\mathfrak{d}$ respectively.

Proof. See [1].

References

1. M. T. Aranés. *Modular symbols over number fields.* PhD thesis, University of Warwick, 2011. See `http://wrap.warwick.ac.uk/35128/`.
2. J. S. Bygott. *Modular forms and elliptic curves over imaginary quadratic number fields.* PhD thesis, University of Exeter, 1998. See `http://www.warwick.ac.uk/staff/J.E.Cremona/theses/bygott.pdf`.

3. H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
4. J. E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Mathematica*, 51:275–323, 1984.
5. J. E. Cremona. Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction. *Math. Proc. Cambridge Philos. Soc.*, 111(2):199–218, 1992.
6. J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, second edition, 1997. available from `http://www.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/index.html`.
7. M. Greenberg and J. Voight. Computing systems of Hecke eigenvalues associated to Hilbert modular forms. *Math. Comp.*, 80(274):1071–1092, 2011.
8. M. P. Lingham. *Modular forms and elliptic curves over imaginary quadratic fields*. PhD thesis, University of Nottingham, 2005. See `http://etheses.nottingham.ac.uk/archive/00000138/`.
9. M. H. Şengün. On the integral cohomology of Bianchi groups. *Exp. Math.*, 20(4):487–505, 2011.
10. G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.
11. W. Stein. *Modular Forms, a Computational Approach*. Number 79 in Graduate Studies in Mathematics. American Mathematical Society, 2007.
12. W. Stein et al. *Sage Mathematics Software (Version 5.2)*. The Sage Development Team, 2012. `http://www.sagemath.org`.
13. G. van der Geer. *Hilbert Modular Surfaces*. Springer, 1988.