A LEVEL N REDUCTION THEORY OF INDEFINITE BINARY QUADRATIC FORMS

CARLOS CASTAÑO-BERNARD

Abstract. In this paper we study a geometric coding algorithm for indefinite binary quadratic forms \( Q \) for the congruence subgroup \( \Gamma^0(N) \), with respect to the usual fundamental domain \( \mathcal{F}_N \), where \( N \) is assumed prime. The cycles \( Q_1, \ldots, Q_n \) that this algorithm produces are such that the the corresponding paths \( \gamma_1, \ldots, \gamma_n \) in the Riemann surface \( X_0(N)(\mathbb{C}) \) have a nice behaviour around the elliptic points of order 2.

Contents

1. Introduction 1
2. The level 1 case 2
2.1. Preliminaries 2
2.2. Indefinite forms 4
2.3. Regular path attached to an indefinite form 10
2.4. Geometric coding algorithm I 15
3. Higher levels 17
3.1. Reduction algorithms 17
3.2. Geometric coding algorithm II 20
References 24

1. Introduction

In this paper we study a geometric coding algorithm for indefinite binary quadratic forms \( Q \) for the congruence subgroup \( \Gamma^0(N) \), with respect to the usual fundamental domain \( \mathcal{F}_N \), where \( N \) is assumed prime. (Cf. Schoeneberg book [8].) Following Ogg [6] let us call \( E \)-points the elliptic points of order 2 with respect to the action of \( \Gamma^0(N) \) on the upper half-plane

\[ \mathcal{H} = \{ \tau \in \mathbb{C} : \Im(\tau) > 0 \}. \]

The cycle

\[ Q_1, \ldots, Q_n \]

that this algorithm attaches to \( Q \) deals with the \( E \)-points is such that the corresponding paths

\[ \gamma_1, \ldots, \gamma_n \]
define in a natural way a regular path on the Riemann surface $X_0(N)(\mathbb{C})$.

The motivation to write this paper was mostly utilitarian. In a forthcoming paper of the author this algorithm is applied to the computation of the homology class of each of the connected components of the real locus of the Atkin-Lehner quotient $X_0^+(N)$ of $X_0(N)$ associated to the Fricke involution $w_N$.

2. THE LEVEL 1 CASE

2.1. Preliminaries. Let $[A, B, C](X, Y) = AX^2 + BXY + CY^2$ denote a binary quadratic forms with real coefficients $A$, $B$, and $C$. Note that for any real numbers $\alpha, \beta, \gamma$ and $\delta$ we have

$$[A, B, C](\alpha X + \beta Y, \gamma X + \delta Y) = \begin{pmatrix} \alpha^2 & \alpha\gamma & \gamma^2 \\ 2\alpha\beta & \alpha\delta + \beta\gamma & 2\gamma\delta \\ \beta^2 & \beta\delta & \delta^2 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix}.$$ 

Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{GL}_2(\mathbb{R})$ and define

$$\sigma_M = \det(M) \begin{pmatrix} \alpha^2 & \alpha\gamma & \gamma^2 \\ 2\alpha\beta & \alpha\delta + \beta\gamma & 2\gamma\delta \\ \beta^2 & \beta\delta & \delta^2 \end{pmatrix}^{-1}. $$

Let $Q$ denote the set of binary quadratic forms. Note that

$$\langle Q, Q' \rangle = BB' - 2(AC' + A'C).$$

makes $Q$ a quadratic space and $M \mapsto \sigma_M$ defines a group homomorphism

$$\sigma : \text{GL}_2(\mathbb{R}) \longrightarrow O^+(Q)$$

of the general linear group $\text{GL}_2(\mathbb{R})$ into the group of orientation preserving automorphisms $O^+(Q)$ of the ternary quadratic form $|Q|^2 = \langle Q, Q \rangle$ on $Q$.\footnote{In fact the homomorphism $\sigma_M$ restricted to $\text{SL}_2(\mathbb{R}) = \{m \in \text{GL}_2(\mathbb{R}) : \det m = \pm 1\}$ is a degree 2 cover of $\text{SL}_2(\mathbb{R})$ known as the spin representation attached to the ternary quadratic form $|Q|^2 = \langle Q, Q \rangle$.}

For each matrix $M \in \text{GL}_2(\mathbb{R})$ and each binary quadratic form $Q \in Q$ we write $M \circ Q = \sigma_M Q$. The ternary quadratic form $|Q|^2 = \langle Q, Q \rangle$ is called the discriminant of the binary quadratic form $Q = [A, B, C]$. We say $Q$ is definite (resp. indefinite) if $|Q|^2 > 0$ (resp. $|Q|^2 < 0$). If $Q$ is definite and $A > 0$ then we say $Q$ is positive definite.

**Definition 2.1.** Two binary quadratic forms $Q_1$ and $Q_2$ are called equivalent if there exists $M \in \text{SL}_2(\mathbb{Z})$ such that $M \circ Q_1 = Q_2$.

**Example 2.2.** Any form $Q = [A, B, C]$ is equivalent to

$$S \circ Q = [C, -B, A],$$

where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$.\footnote{In fact the homomorphism $\sigma_M$ restricted to $\text{SL}_2(\mathbb{R}) = \{m \in \text{GL}_2(\mathbb{R}) : \det m = \pm 1\}$ is a degree 2 cover of $\text{SL}_2(\mathbb{R})$ known as the spin representation attached to the ternary quadratic form $|Q|^2 = \langle Q, Q \rangle$.}
Example 2.3. Any form $Q = [A, B, C]$ is equivalent to
\[ T^t \circ Q = [A, -2tA + B, t^2A - tB + C], \]
where $T = (\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}) \in \text{SL}_2(\mathbb{Z})$, for each $t \in \mathbb{Z}$.

Definition 2.4. We say a positive definite binary quadratic form $Q = [A, B, C]$ is normal if $-A \leq -B < A$.

Every positive definite form $Q$ is equivalent to a normal form, namely $Q^{\text{norm}} = T^t \circ Q$, where
\[ t = \left\lfloor \frac{A - B}{2A} \right\rfloor \]
and $\lfloor x \rfloor$ denotes the floor of a real number $x$. The form $Q^{\text{norm}}$ is known as the normalisation of $Q$.

Definition 2.5. We say a positive definite binary quadratic form $Q = [A, B, C]$ is reduced if $Q$ is normal and if any of the following two conditions is true.

1. $A < C$
2. $A = C$ and $-B \leq 0$

Algorithm 1: The reduction of a positive definite form $Q$

Data: any positive definite binary quadratic form $Q$

Result: a reduced form $Q^{\text{red}}$ equivalent to $Q$

1. $Q \leftarrow Q^{\text{norm}}$;
2. while not reduced do
3. \hspace{1em} $Q \leftarrow (S \circ Q)^{\text{norm}}$;
4. end

The definition of reduced form may be rephrased in geometric terms as follows. To each positive definite form $Q$ attach the point $\pi_Q \in \mathcal{H}$ defined by
\[ \pi_Q = \frac{-B + |Q|}{2A}, \]
where $|Q|$ denotes the square root of $|Q|^2$ such that $\Im(|Q|) > 0$. So $Q$ is reduced if and only if $\pi_Q \in \mathcal{F}'$, where
\[ \mathcal{F}' = \left\{ \tau \in \mathcal{H}: -\frac{1}{2} \leq \Re(\tau) < \frac{1}{2} \right\} \cap \left\{ \tau \in \mathcal{H}: |\tau| > 1 \text{ or } (|\tau| = 1 \text{ and } \Re(\tau) \leq 0) \right\}, \]
which is depicted by Figure 2.1. If we define $\tau \mapsto M\tau$ for each $M = (\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}) \in \text{SL}_2(\mathbb{R})$ by the Möbius transformation
\[ M\tau = \frac{\alpha \tau + \beta}{\gamma \tau + \delta}, \]
then we have an action of $\text{SL}_2(\mathbb{R})$ on $\mathcal{H}$ such that $M\pi_Q = \pi_{MQ}$. 


While performing Algorithm 1 on a given positive definite form $Q$ we may obtain a product of matrices

$$R_Q = T^n S \cdots S T^{n_2} S T^{n_1} \in SL_2(\mathbb{Z})$$

such that $R_Q \circ Q$ is reduced, where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Note that in terms of the above geometric setting we have $R_Q \pi_Q \in \mathcal{F}$. So given any $\tau \in \mathcal{H}$ there is a matrix $R_\tau \in SL_2(\mathbb{Z})$ such that $R_\tau \tau \in \mathcal{F}$.

In fact $R_\tau$ is uniquely determined by $\tau$, except when $\tau$ is equivalent to either $i = \sqrt{-1}$, with stabiliser of order 2 or $\rho^{-1} = \frac{1 + \sqrt{-3}}{2}$, with stabiliser of order 3.

Remark 2.6. Later, in connection with the coding algorithm we will find convenient to use the closure $\mathcal{F}_N = (\mathcal{F}')^{\text{cl}}$ of the fundamental set $\mathcal{F}'_N$. In the literature the closed set $\mathcal{F} \subset \mathcal{H}$ is known as a fundamental region.

2.2. Indefinite forms. Let $\text{sign}(x)$ denote the sign of a real number $x$. We will find convenient to assume the somewhat non-standard convention that $\text{sign}(0) = 1$, as opposed to the usual $\text{sign}(0) = 0$.

Definition 2.7. We say an indefinite binary quadratic form $Q = [A, B, C]$ is reduced\(^2\) if $B > 0$ and if any of the following two conditions is satisfied.

- **R1**: $2|A + C| < B$
- **R2**: $2(A + C) = -\text{sign}(A)B$

\(^2\)A closely related definition of reduced indefinite form may be found in Choie and Parson’s article [3], where $Q = [A, B, C]$ is called reduced if $A > 0$, $C > 0$, and $A + C < B$. 
From now on let us assume $Q = [A, B, C]$ is an indefinite binary quadratic form with $A$, $B$ and $C$ in $\mathbb{Z}$. We shall give a geometric interpretation of the concept of reduced indefinite form. Provide the upper half-plane $\mathcal{H}$ with the hyperbolic metric

$$ds = \frac{|d\tau|}{y},$$

where $\tau = x + iy$, with $x$ and $y$ the usual (real-valued) coordinate functions of $\mathbb{C}$. Let $\{\tau_1, \tau_2\}$ denote the (oriented) geodesic that joins a given point $\tau_1 \in \mathcal{H}^*$ to a given point $\tau_2 \in \mathcal{H}^*$. The geodesic $\gamma_Q$ attached to an indefinite form $Q$ is

$$\gamma_Q = \begin{cases} \{\frac{-B-Q}{2A}, \frac{-B+Q}{2A}\} & \text{if } A \neq 0 \\ \{i\infty, -\frac{C}{A}\} & \text{if } A = 0 \text{ and } B > 0 \\ \{-\frac{C}{A}, i\infty\} & \text{if } A = 0 \text{ and } B < 0 \end{cases}$$

where $|Q|$ denotes the positive square root of $|Q|^2$. We also write $\sqrt{D} = |Q|$, where $D = B^2 - 4AC$. The intersection number $I(\gamma_1, \gamma_2)$ of given (oriented) geodesics arcs $\gamma_1$ and $\gamma_2$ on the upper half-plane $\mathcal{H}^*$ is defined by

$$I(\gamma_1, \gamma_2) = \begin{cases} 1, & \text{if } \#(\gamma_1 \cap \gamma_2) = 1 \text{ and } \{\gamma_1'(P), \gamma_2'(P)\} \text{ has positive orientation} \\ -1, & \text{if } \#(\gamma_1 \cap \gamma_2) = 1 \text{ and } \{\gamma_1'(P), \gamma_2'(P)\} \text{ has negative orientation} \\ 0, & \text{otherwise} \end{cases}$$

where $\gamma'(P)$ denotes the unit tangent vector of a geodesic $\gamma$ at a point $P \in \gamma$.

**Example 2.8.** Suppose $Q = [0, 1, 0]$ and $U = [1, 0, -1]$. In fact $\gamma_Q = \{i\infty, 0\}$ and $\gamma_U = \{-1, 1\}$. Clearly $\gamma_Q$ and $\gamma_U$ meet at $P = \pi_{[1,0,1]} = i$ (and no other point). In particular $I(\gamma_Q, \gamma_U) = \pm 1$. To determine the sign we note that the tangent vector of $\gamma_Q$ at $P$ is given by $\gamma'_Q(P) = (0, -1)$, and the tangent vector of $\gamma_U$ at $P$ is given by $\gamma'_U(P) = (1, 0)$. Since the determinant

$$\begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix} > 0$$

we have $I(\gamma_Q, \gamma_U) = 1$.

Put $\sigma = \{\rho_-1, \rho_{+1}\}$, where as before $\rho_{\pm 1} = \frac{\pm 1 + \sqrt{-3}}{2}$. Note $\sigma \subset \gamma_U$, where $U = [1, 0, -1]$. To simplify our exposition assume from now on that $D$ is not a perfect square.

**Lemma 2.9.** An indefinite form $Q$ is reduced if and only if $I(\gamma_Q, \sigma) = 1$ and $\gamma_Q \cap \mathcal{F}^{\text{int}} \neq \emptyset$.

**Proof.** First note that given two binary quadratic forms $Q_1$ and $Q_2$, where $Q_1$ is positive definite and $Q_2$ is indefinite, the condition that the point $\pi_{Q_1}$ lies on the geodesic $\gamma_{Q_2}$ is equivalent to $\langle Q_1, Q_2 \rangle = 0$. So $\gamma_Q \cap \gamma_U \neq \emptyset$ means there is a positive definite form $Q'$ such that
(1) $\langle Q', U \rangle = 0$
(2) $\langle Q', Q \rangle = 0$

Write $Q' = [A', B', C']$. Clearly (1) and (2) hold if and only if

$$A' = C' \quad \text{and} \quad B'B - 2(AA' + A'C') = 0.$$ 

This means that $B'B - 2(AA' + A'C') = 0$. In other words

$$\frac{B'}{2A'} = \frac{A + C}{B}.$$ 

Thus $\gamma_Q$ meets $\gamma_U$ at a point $\pi_{Q'}$ on the geodesic arc $\sigma = \{\rho_{-1}, \rho_{+1}\}$ if and only if

$$2|A + C| \leq |B|.$$ 

Now we split the proof in two cases according as $\pi_{Q'}$ is an endpoint of $\sigma$ or not.

**Case I:** Suppose

$$2(A + C) = \mp B.$$ 

This condition is equivalent to $\rho_{\pm 1} \in \gamma_Q$. So $\gamma_Q \cap \mathcal{F}^\text{int} \neq \emptyset$ if and only if

$$\mp \frac{B}{2A} < 0,$$ 

and $I(\gamma_Q, \sigma) = 1$ if and only if $\pm A > 0$. In other words, $2(A + C) = -\text{sign}(A)B$ and $B > 0$.

**Case II:** Now suppose

$$2|A + C| < |B|.$$ 

Since the point $\pi_{Q'}$ is not an endpoint of $\sigma$, we have $\gamma_Q \cap \mathcal{F}^\text{int} \neq \emptyset$. Moreover, the condition $B > 0$ is equivalent to $I(\gamma_Q, \sigma) = 1$. The lemma follows. \hfill \Box

We will shortly introduce Algorithm 2, which is a reduction algorithm of indefinite binary quadratic forms that we will use in connection with Algorithm 3. The latter algorithm is a variant on the geometric coding algorithm of Katok [4].

We call an indefinite form $Q = [A, B, C]$ nearly reduced if $3A^2 \leq D$, where $D = B^2 - 4AC$ is the discriminant of $Q$. To each nearly reduced indefinite form $Q$ we attach the interval

$$J_Q = \begin{cases} 
[t_{-1}', t_{+1}'], & \text{if } D > 4A^2 \\
[t_{-\text{sign}(A)}', t_{-\text{sign}(A)}'], & \text{if } D < 4A^2
\end{cases}$$

where

$$t_{\pm 1} = \pm \frac{1}{2} + \frac{B + \sqrt{D - 3A^2}}{2A}, \quad \text{and} \quad t_{\pm 1}' = \pm \frac{1}{2} + \frac{B - \sqrt{D - 3A^2}}{2A}.$$ 

\textsuperscript{3}The author owes the main ideas underlying this algorithm to a talk given by Richard Pinch.
Proof. First we define an auxiliary function \( f_Q \) attached to the nearly reduced form \( Q = [A, B, C] \) by letting

\[
f_Q(t) = \left| \frac{A_t + C_t}{B_t} \right|,
\]

where

\[
A_t = A, \\
B_t = B - 2At, \\
C_t = At^2 - Bt + C,
\]

with \( t \in \mathbb{R} \). Note that \( \gamma_{T^*Q} \) has non-trivial intersection with the geodesic arc \( \sigma = \{\rho_-, \rho_+\} \) if and only if \( t \in \mathbb{R} \) is such that

\[
f_Q(t) \leq \frac{1}{2}.
\]

We will see that the set of such \( t \) may be expressed as a union of two closed intervals. Our first step will be to find the endpoints of these intervals, i.e. the solutions \( t \in \mathbb{R} \) of \( f_Q(t) = \frac{1}{2} \). The latter is equivalent to any of the following equations

\[
2|A_t + C_t| = |B_t|, \\
2|At^2 - Bt + A + C| = |B - 2At|, \\
2(At^2 - Bt + A + C) = \pm(B - 2At).
\]

A straightforward calculation shows that the four real numbers \( t_+, t_-^1, t_-^1, \) and \( t_-' \), defined above are all the solutions of \( f_Q(t) = \frac{1}{2} \). Now the proof splits in two cases.

**Case I:** Suppose \( D > 4A^2 \). This condition means that the intervals \([t_-, t_+]\) and \([t_-', t_+']\) are disjoint. It is straightforward to see that \( f_Q(t) \leq \frac{1}{2} \), if and only if \( t \in [t_-, t_+] \cup [t_-', t_+'] \), with \( f_Q(t) = \frac{1}{2} \) exactly at the endpoints. Clearly \( I(\gamma_{T^*Q}, \sigma) = 1 \) if and only if

\[
t \in [t_-', t_+]^1.
\]

**Case II:** Suppose \( D < 4A^2 \). This condition means that the intervals \([t_-, t_+]\) and \([t_-', t_+']\) are disjoint. Again it is straightforward to see that \( f_Q(t) \leq \frac{1}{2} \), if and only if \( t \in [t_-, t_-'] \cup [t_+', t_+] \), with \( f_Q(t) = \frac{1}{2} \) exactly at the endpoints. Note that \( I(\gamma_{T^*Q}, \sigma) = 1 \) if and only if

\[
(2.1) \quad \left| \rho_{-\text{sign}(A)} - t + \frac{B}{2A} \right| \leq \frac{\sqrt{D}}{2|A|}.
\]

By squaring the left-hand side of Inequality 2.1 we get

\[
\left| \rho_{-\text{sign}(A)} - t + \frac{B}{2A} \right|^2 = \left( \rho_{-\text{sign}(A)} - t + \frac{B}{2A} \right) \left( \bar{\rho}_{-\text{sign}(A)} - t + \frac{B}{2A} \right) =
\]
\[ \rho_{-\text{sign}(A)} \rho_{-\text{sign}(A)} + (\rho_{-\text{sign}(A)} + \rho_{+\text{sign}(A)}) \left( -t + \frac{B}{2A} \right) + t^2 - \frac{B}{A}t + \frac{B^2}{4A^2} = \\
1 - \text{sign}(A) \left( -t + \frac{B}{2A} \right) + t^2 - \frac{B}{A}t + \frac{B^2}{4A^2} \]

So Inequality 2.1 is equivalent to

\[ t^2 + \left( \text{sign}(A) - \frac{B}{A} \right) t - \text{sign}(A) \frac{B}{2A} + \frac{B^2}{4A^2} - \frac{D}{4A^2} + 1 \leq 0. \]

After a straightforward calculation we may see that \( t \in \mathbb{R} \) satisfies Inequality 2.1 if and only if \( t \in [t_{-\text{sign}(A)}, t'_{+\text{sign}(A)}] \), and the lemma follows. □

**Corollary 2.11.** If \( Q = [A, B, C] \) is an indefinite form such that \( \gamma_Q \cap F \neq \emptyset \), then there is exactly one \( t \in \mathbb{Z} \) such that \( T^t \circ Q \) is reduced, unless \( D < 4A^2 \) and either \( \rho_{-1} \) or \( \rho_{+1} \) lies in \( \gamma_Q \).

**Proof.** We split the proof splits in two cases as follows.

**Case I** Suppose \( Q = [A, B, C] \) is an indefinite form such that \( D > 4A^2 \). Note that the closed interval \( J_Q \) has length 1. Now we consider two sub-cases.

**Sub-case I:** There is exactly one point \( t \in J_Q \cap \mathbb{Z} \). Note that \( \gamma_{T^t \circ Q} \cap F^{\text{int}} \neq \emptyset \). Thus by Lemma 2.10 we may see \( T^t \circ Q \) is reduced.

**Sub-case II:** The endpoints \( t'_{-1} \) and \( t'_{+1} \) are integral. Clearly \( t = t'_{+\text{sign}(A)} \) is the only point such that \( \gamma_{T^t \circ Q} \cap F^{\text{int}} \neq \emptyset \), and again by applying Lemma 2.10 we may see that \( T^t \circ Q \) is reduced.

**Case II** Suppose \( Q = [A, B, C] \) is such that \( D < 4A^2 \), but neither \( \rho_{-1} \) nor \( \rho_{+1} \) lies in \( \gamma_Q \). Clearly \( \gamma_{T^t \circ Q} \cap F^{\text{int}} \neq \emptyset \). Now using the Lemma 2.10 we may see that \( T^t \circ Q \) is reduced.

**Proof.** On the one hand note that the assumption \( \rho_{\pm 1} \in \gamma_Q \) is equivalent to

\[ (2.2) \quad 2(A + C) = \mp B, \]

where \( Q = [A, B, C] \). On the other hand note \( \gamma_Q \cap F^{\text{int}} = \emptyset \) is equivalent to

\[ (2.3) \quad -\frac{B}{2A} \in (0, \pm 1). \]

Using Equation 2.2 we may see Inclusion 2.3 is equivalent to

\[ \frac{C}{A} \in (0, -1). \]
An immediate consequence of the latter is that the form

\[ Q' = S \circ Q = [C, -B, A] \]

satisfies \( \gamma_{Q'} \cap \mathcal{F}^{int} \neq \emptyset \). The converse is clearly true and the lemma follows.

**Definition 2.13.** We say an indefinite form \( Q \) is *normalisable* if there is \( \delta(Q) \in \mathbb{Z} \) such that \( T^{\delta(Q)} \circ Q \) is reduced. Such form \( Q^{\text{nrm}} = T^{\delta(Q)} \circ Q \) is called its *normalisation*.

**Definition 2.14.** The *tip* \( \hat{\gamma} \) of a geodesic \( \gamma \subset \mathcal{H} \) is the point

\[ \hat{\gamma} = \frac{x + y}{2} + \left| \frac{x - y}{2} \right| i \in \gamma \]

where \( \gamma = \{x, y\} \) and \( x \) and \( y \) in \( \mathbb{R} \). We define the *tip* \( \hat{Q} \) of an indefinite form \( Q \) as the positive definite binary quadratic form \( P \) such that \( \pi_P = \hat{\gamma}_Q \). If \( Q \) is integral we assume \( \hat{Q} \) is primitive.

We will find it convenient to consider pointed spaces \((\gamma_Q, \tau_0)\), with \( \tau_0 \in \gamma_Q \), e.g. \( \tau_0 = \hat{\gamma}_Q \). By a slight abuse of notation we sometimes write \((Q, \tau_0)\) instead of \((\gamma_Q, \tau_0)\).

**Algorithm 2:** The reduction of \( Q \)

**Data:** \((Q, \tau_0)\) with \( \tau_0 \gamma_Q \)

**Result:** reduced form \( Q^{\text{red}} \) equivalent to \( Q \)

1. \( Q \leftarrow R_{\tau_0} \circ Q \);
2. if \( \gamma_Q \cap \mathcal{F}^{int} \neq \emptyset \) then
3. \( Q \leftarrow Q^{\text{nrm}} \)
4. else
5. \( Q \leftarrow (S \circ Q)^{\text{nrm}} \)
6. end

Now we prove that Algorithm 2 is correct. First note that the correctness of Algorithm 1 (due to Gauß) implies that after Step 1 the geodesic \( \gamma_Q \) and the (closed) fundamental region \( \mathcal{F} \) share at least one point. If also the interior \( \mathcal{F}^{int} \) and \( \gamma_Q \) have non-trivial intersection, then Corollary 2.11 implies that the normalisation \( Q^{\text{nrm}} \) of \( Q \) is reduced. However, it may sometimes happen that \( \mathcal{F}^{int} \cap \gamma_Q = \emptyset \), which means that \( \gamma_Q \) contains one of the lower vertices of the fundamental region \( \mathcal{F} \). But Lemma 2.12 tells us that the transformed form \( S \circ Q \) now belongs to the above case, and thus \((S \circ Q)^{\text{nrm}}\) is reduced. Therefore Algorithm 2 is correct.
2.3. **Regular path attached to an indefinite form.** As before let \( Q = [A, B, C] \) be primitive indefinite form with non-square discriminant \( D = B^2 - 4AC \) and define

\[
M_Q = \begin{pmatrix}
x - By & -2Cy \\
2Ay & x + By
\end{pmatrix} \in \Gamma(1),
\]

where \((x, y) \in \mathbb{Z} \times \mathbb{Z}\) is the fundamental solution to Pell’s equation

\[
(2.4) 
X^2 - DY^2 = 1
\]

such that both, \( x > 0 \) and \( y > 0 \), so that the eigenvalue \( \lambda_Q = x + y \sqrt{D} \in \mathcal{O}_D \) of \( M_Q \) satisfies \( \lambda_Q > 1 \). Note that \( M_Q \) is an automorphism of the quadratic form \( Q \). So given a base-point \( \tau_0 \in \gamma_Q \), the geodesic segment \( \{\tau_0, M_Q\tau_0\} \) is a subset of the geodesic

\[
\gamma_Q = \left\{ \frac{-B - \sqrt{D}}{2A}, \frac{-B + \sqrt{D}}{2A} \right\}
\]

Now, by standard results of hyperbolic geometry as in Beardon’s book [2], we may see that the arc-length parametrisation of the (oriented) geodesic segment \( \{\tau_0, M_Q\tau_0\} \) is the restriction of the arc-length parametrisation of the (oriented) geodesic \( \gamma_Q \) with base point \( \tau_0 \) to the closed interval \([0, l(Q)] \subset \mathbb{R}\), where \( l(Q) = 2 \log(\lambda_Q) \) is the hyperbolic length of \( \{\tau_0, M_Q\tau_0\} \). Now let

\[
g_{Q,\tau_0} : [0, l(Q)] \longrightarrow X(1).
\]

be the parametrisation induced in the quotient \( X(1) \) by the above restriction. Note that \((\gamma_Q)_{\Gamma(1)} = \{\tau_0, M_Q\tau_0\}_{\Gamma(1)}\), where \( X_{\Gamma(1)} \) denotes the image of a subset \( X \subset \mathcal{H}^* \) in the quotient \( X(1) = \Gamma(1) \backslash \mathcal{H}^* \). Since \( Q \) is primitive, the assumption that \((x, y)\) is a fundamental solution to Equation 2.4 is equivalent to the assertion that \( M_Q \) is not a non-trivial power of an element in the modular group \( \Gamma(1) \). So essentially \( g_{Q,\tau_0} \) traces out its image \((\gamma_Q)_{\Gamma(1)} = \{\tau_0, M_Q\tau_0\}_{\Gamma(1)}\) only once. We call \( g_{Q,\tau} \) the **closed geodesic** associated to the form \( Q \) and the point \( \tau_0 \in \gamma_Q \).

Let \( X \) be any differentiable manifold and let \( T \) be a positive real number. A differentiable path \( g : [0, T] \longrightarrow X \) is called **regular** if the derivative \( g'(t) \neq 0 \), for each \( t \in [0, T] \).

**Lemma 2.15.** Again let \( Q \) be an indefinite form and \( \tau \) a point of \( \gamma_Q \). If the image of the path \( \gamma_Q \subset \mathcal{H} \) contains an elliptic point, then the path \( g_{Q,\tau} \subset \mathcal{H} \) is not regular, else the path \( g_{Q,\tau} \subset \mathcal{H} \) is regular.

**Proof.** It is well-known that the complex-analytic structure of the affine modular curve \( Y(1) = \Gamma(1) \backslash \mathcal{H} \) is induced by the map \( j : \mathcal{H} \mapsto \mathbb{C} \), where

---

In the literature the closed geodesic \( g_{Q,\tau_0} \) is also known as a **prime geodesic**. By the Prime Geodesic Theorem of Sarnak [7] we know that the distribution of the lengths \( l(Q) \) is similar to the distribution of prime numbers.
\[ j(\tau) = \frac{1}{q} + 744 + 196884q + \ldots, \]

(See Knapp's book [5].) Moreover, given any point \( b \in \mathcal{H} \) there is a sufficiently small neighbourhood \( U \) (resp. \( V \)) of \( b \) (resp. \( j(b) \)) together with an holomorphic identification \( \phi: U \to \mathbb{D} \) (resp. \( \psi: V \to \mathbb{D} \)) with the unit disk

\[ \mathbb{D} = \{ z \in \mathbb{C}: |z| < 1 \} \]

such that the diagram

\[
\begin{array}{ccc}
U & \xrightarrow{j} & V \\
\downarrow{\phi} & & \downarrow{\psi} \\
\mathbb{D} & \rightarrow & \mathbb{D}
\end{array}
\]

commutes, where

\[
n = \begin{cases} 
3, & \text{if } b \text{ is an elliptic point of order } 3, \\
2, & \text{if } b \text{ is an elliptic point of order } 2, \\
1, & \text{otherwise.}
\end{cases}
\]

So there is \( t_0 \in [0, l(Q)] \) such that \( g_{Q,\tau_0}(t_0) \) is an elliptic point then if and only if the derivative \( g'_{Q,\tau_0}(t_0) = 0 \). The lemma follows. \( \square \)

For the rest of the subsection suppose \( g_{Q,\tau_0} \) fails to be regular at a point \( t_0 \in [0, T] \), i.e. \( g_{Q,\tau_0}(t_0) = \tau_e \), where \( \tau_e \) is (the image in \( X(1) \) of) an elliptic point of order \( e = 2 \) or \( 3 \). Shortly we shall see how, under certain mild conditions, a suitable restriction of the path \( g_{Q,\tau_0} \) may be extended in a natural way to produce an analytic regular path. But first we need to prove the following two elementary lemmas on square roots of certain elements of the group \( \text{SL}_2(\mathbb{R}) \), and also introduce a basic definition immediately after the lemmas. The mentioned regular path is actually constructed in the proof of Theorem 2.19.

**Lemma 2.16.** Let \( Q \) and \( M_Q \) be as above. Also let \( \epsilon = x' + y'\sqrt{D} \in \mathcal{O}_D^\times \) (with \( x' \) and \( y' \) in \( \frac{1}{2}\mathbb{Z} \)) be a fundamental unit of the real quadratic order \( \mathcal{O}_D \) of discriminant \( D \). Assume that \( \epsilon \) has negative norm \( N(\epsilon) = -1 \) and also that \( \epsilon > 1 \). Then

\[
M_Q^{\frac{1}{2}} = \frac{1}{\sqrt{D}} \begin{pmatrix} Dy' - Bx' & -2Cx' \\ 2Ax' & Dy' + Bx' \end{pmatrix} \in \text{SL}_2(K)
\]

is a square root of \( M_Q \) such that the arc-length parametrisation of the geodesic segment \( \{ \tau_0, M_Q^{\frac{1}{2}}\tau_0 \} \) is the restriction of the arc-length parametrisation of the geodesic segment \( \{ \tau_0, M_Q\tau_0 \} \) to the interval \([0, \frac{1}{2}l(Q)]\).
Proof. Consider the matrix
\[ M = \begin{pmatrix} \frac{-B + \sqrt{D}c}{2A} & \frac{-B - \sqrt{D}d}{2A} \\ c & d \end{pmatrix} \in \text{SL}_2(K) \]
where \( c \) and \( d \) are integers such that \( cd = \frac{A}{\sqrt{D}} \). It is plain that the matrix \( M \) maps the elements 0 and \( \infty \) as follows:
\[ \begin{align*}
0 & \mapsto \frac{-B - \sqrt{D}}{2A}, \\
\infty & \mapsto \frac{-B + \sqrt{D}}{2A}.
\end{align*} \]
Now recall that the solution \((x, y) \in \mathbb{Z} \times \mathbb{Z}\) of Equation 2.4 is minimal subject to the conditions \( x > 0 \) and \( y > 0 \). In particular the eigenvalue \( \lambda_Q = x + y\sqrt{D} \) of \( M_Q \) is the generator of the cyclic subgroup \( \{z \in O_D^\times : \mathcal{N}(z) = 1 \text{ and } z > 1\} \).

Now consider that the fundamental unit \( \epsilon = x' + y'\sqrt{D} \) has negative norm \( \mathcal{N}(\epsilon) = -1 \). Thus \( \epsilon^2 = \lambda_Q \) (since both, \( \lambda_Q > 1 \) and \( \epsilon > 1 \)). Hence \( M \left( \begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{smallmatrix} \right) M^{-1} \in \text{SL}_2(K) \) is a square root of \( M_Q \). It is plain that
\[ M \left( \begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{smallmatrix} \right) M^{-1} = \frac{1}{\sqrt{D}} \begin{pmatrix} Dy' - Bx' & -2Cx' \\ 2Ax' & Dy' + Bx' \end{pmatrix}, \]
and the equality in the lemma follows. Now using (once more) that \( \epsilon > 1 \), the latter part of the lemma follows. \( \square \)

**Lemma 2.17.** The matrix
\[ S^{\frac{1}{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \]
is the square root of \( S = \left( \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \right) \); it fixes \( i \) and induces the \( z \mapsto iz \) map in the tangent space of \( \mathcal{H} \) at \( i \).

**Proof.** The lemma follows after a couple of straightforward calculations. \( \square \)

**Definition 2.18.** Let \( X \) be a topological space and let \( T_1 \) and \( T_2 \) be positive real numbers. Suppose we have paths \( f_1 : [0, T_1] \rightarrow X \) and \( f_2 : [0, T_2] \rightarrow X \) such that \( f_1(T_1) = f_2(0) \). The *concatenation* \( f_1 * f_2 \) of \( f_1 \) and \( f_2 \) is the path
\[ f_1 * f_2 : [0, T_1 + T_2] \rightarrow X, \]
where
\[ (f_1 * f_2)(t) = \begin{cases} f_1(t) & \text{if } 0 \leq t < T_1, \\ f_2(t - T_1) & \text{if } T_1 \leq t \leq T_1 + T_2, \end{cases} \]
for each \( t \in [0, T_1 + T_2] \).
Theorem 2.19. Assume that the base point \( \tau_0 \) of \( g_{\mathcal{Q},\tau_0} \) is not an elliptic point of order \( e = 2 \). Also, if \( g_{\mathcal{Q},\tau_0} \) contains an elliptic point of degree \( e = 2 \), further assume that the fundamental unit \( \epsilon \) of \( \mathcal{O}_D \) has norm \( N(\epsilon) = -1 \). Then there is a regular analytic path \( \rho_{\mathcal{Q},\tau_0} \) on \( X(1) \) such that, up to a continuous reparametrisation of \( g_{\mathcal{Q},\tau_0} \), the restrictions of \( \rho_{\mathcal{Q},\tau_0} \) and \( g_{\mathcal{Q},\tau_0} \) to \( I = [0, t_0) \) coincide

\[
\rho_{\mathcal{Q},\tau_0}|_I = g_{\mathcal{Q},\tau_0}|_I,
\]

for \( t_0 \in \mathbb{R}_{>0} \) sufficiently small. Moreover, up to a regular (analytic) reparametrisation of \( \rho_{\mathcal{Q},\tau_0} \), the path \( \rho_{\mathcal{Q},\tau_0} \) is uniquely determined by \( g_{\mathcal{Q},\tau_0} \).

Proof. Suppose \( \gamma_Q \) contains an elliptic point \( \tau_e \) of order \( e = 3 \). By the commutative diagram in the proof of Lemma 2.15 we may see that for a small enough open neighbourhood \( U \) of \( \tau_e \) there is a continuous reparametrisation of the restriction \( g_{\mathcal{Q},\tau_0}|_U \) of \( g_{\mathcal{Q},\tau_0} \) to the preimage \( V = g_{\mathcal{Q},\tau_0}^{-1} U \), such that \( g_{\mathcal{Q},\tau_0}|_V \) is both, analytic and regular. Now suppose \( \gamma_Q \) contains an elliptic point \( \tau_e \) of order \( e = 2 \). Without loss of generality we may assume \( \tau_e = \sqrt{-1} \in \mathcal{H} \). The proof splits in two steps as follows.

Step 1. We claim that the path \( g_{\mathcal{Q},\tau_0} \) may be decomposed as

\[
g_{\mathcal{Q},\tau_0} = \{\tau_0, b\}_{\Gamma(1)} \ast \{b, \tau_0\}_{\Gamma(1)} \ast \{\tau_0, b'\}_{\Gamma(1)} \ast \{b', \tau_0\}_{\Gamma(1)},
\]

for suitably chosen elliptic points \( b \) and \( b' \) in \( \mathcal{H} \) of order 2. Indeed, put \( b = \tau_e \) and \( b' = M_Q^{-\frac{1}{2}} b \). Now it suffices to prove that \( b' \) is an imaginary quadratic number of discriminant \( \Delta = -4 \). If we consider the positive definite form \( P = [1, 0, 1] \), our claim follows if we prove that \( P' = M_Q^{-\frac{1}{2}} \circ P \) is integral, primitive, and has discriminant \( \Delta = -4 \). From Definition 2.1 and Lemma 2.16 we get

\[
P' = [1 + 2x^2 - 2Bxy, 8Axy, 1 + 2x^2 + 2Bxy],
\]

where \( x + y\sqrt{D} \in \mathcal{O}_D^* \) is a fundamental unit (of negative norm) of the real quadratic order \( \mathcal{O}_D \), and \( D \) is the discriminant of \( Q \). So \( x \) and \( y \) both lie in \( \frac{1}{2}\mathbb{Z} \). (By a slight abuse of notation we have written \( x \) and \( y \) instead of \( x' \) and \( y' \).) In particular we may see \( P' \) is integral.

Now suppose \( P' \) is not primitive. So \( M_Q^{-\frac{1}{2}} \circ P' = (\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) \circ P \) is not primitive, but \( P = [1, 0, 1] \) is obviously primitive. We have reached a contradiction. Therefore \( P' \) must be primitive. Since it is plain that \( P' \) has discriminant \( \Delta = -4 \), our claim follows. A consequence of our claim is that the path \( g_{\mathcal{Q},\tau_0} \) not only fails to be regular at the points \( b \) and \( b' \); these points are cusps (in the sense of differential geometry) of the path \( g_{\mathcal{Q},\tau_0} \).

Step 2. Now we “remove” the cusps of \( g_{\mathcal{Q},\tau_0} \) by replacing in the above decomposition the components

\[
\{b, \tau_0\}_{\Gamma(1)} \ast \{\tau_0, b'\}_{\Gamma(1)} \ast \{b', \tau_0\}_{\Gamma(1)}
\]
by a certain concatenation of paths that meet at an angle of $\frac{\pi}{2}$ at elliptic points of degree $e = 2$. More precisely, we claim that a suitable continuous reparametrisation of the concatenation

$$p = \{\tau_0, b\}_{\Gamma(1)} \ast \{b, b'\}_{\Gamma(1)} \ast \{b'', \tau_0\}_{\Gamma(1)},$$

is the desired regular path, where $b' = M_{S^{\frac{1}{2}} \circ Q} b$ with $a = \text{sign}(A)$, and $b'' = M_{Q}^{-\frac{1}{2}} b$. Since we assumed that $\tau_0 \neq b$, the length $t_0 = l(\tau_0, b) > 0$. So $p|I = g_{Q, \tau_0}|I$, where $I = [0, t_0)$. Again by the commutative diagram in the proof of Lemma 2.15, the fact that the ramification degree $e = 2$ implies that the path $p$ is both, regular and analytic at the point $b$, after a continuous reparametrisation of $p$. Clearly the same is true for $p$ at $b'$ (considering $b'$ and $b''$ are the same point in $X(1)$). Denote $\rho_{Q, \tau_0}$ any such continuous reparametrisation of $p$. It is clear that $\rho_{Q, \tau_0}$ is unique up to a regular analytic parametrisation and the theorem follows. \(\square\)

**Example 2.20.** Consider the indefinite form $Q = [1, 4, -1]$ of discriminant $D = 20$, and let $\tau_0$ be the imaginary quadratic number $\tau_0 = \frac{-3 + \sqrt{-19}}{2} \in \gamma_Q$. Clearly $b = i$, $b' = i - 4$, and $b'' = i + 1$, as depicted in Figure 2.2. Note the restriction $g_{Q, \tau_0}|I$ of $g_{Q, \tau_0}$ to $I = [0, T)$ is regular, where $T = l(\{\tau_0, b\}) = 1.216185939 \cdots > 0$.\(^5\) Note $g_{Q, \tau_0}$ fails to be regular at $b$. Moreover, the path $g_{Q, \tau_0}$ clearly has a cusp (in the sense of differential geometry) at $b$. Since the geodesics $\gamma_Q$ and $\gamma_{S^{\frac{1}{2}} \circ Q}$ meet at an angle of $\frac{\pi}{2}$, and locally the function $j(\tau)$ at $b$ is the map

\(\\)

\(^5\)It is a curious fact that

$$e^{l((\tau_0, b))} = \sqrt{\frac{218 + 96\sqrt{5}}{38}},$$

which obviously lies in a quadratic extension of the field $\mathbb{Q}(\sqrt{5})$.\(/\)

![Figure 2.2. The path \(\{\tau_0, b\} \ast \{b, b'\} \ast \{b'', \tau_0\}\).](image-url)
A level \( N \) reduction theory of indefinite binary quadratic forms

\[ z \mapsto z^2, \] it is plain that the path \( \{b', b\} \ast \{b, b''\} \) is analytic and regular at \( b \), if \( \{b', b\} \ast \{b, b''\} \) is suitably reparametrised.

**Remark 2.21.** As before suppose that \( \gamma_Q \) contains an elliptic point \( \tau_e \) of order \( e = 2 \). Note that the path \( g_{Q, \tau_0} \) is generically 2 : 1 onto its image, whereas the path \( \rho_{Q, \tau_0} \) is generically 1 : 1 onto its image. This explains the italics in the word “essentially” by the beginning of this subsection, when describing how \( g_{Q, \tau_0} \) traces out its image.

### 2.4. Geometric coding algorithm I.

Let \( Q \) be an indefinite form and let \( \rho_{Q, \tau_0} \) be the closed regular path we attached to \( Q \) and \( \tau_0 \in \gamma_Q \) in the above subsection. Here our main result is Algorithm 3, which produces the (geometric) code of \( \rho_{Q, \tau_0} \) with respect to the fundamental region \( \mathcal{F} \) of the modular group \( \Gamma(1) \). So our algorithm may be regarded as a variant on the geometric coding algorithm of Katok [4].

We need to introduce some preliminaries and notations. Let

\[
S_Q = \begin{cases} (S^\frac{1}{2})^a, & \text{if } A + C = 0, \text{ where } a = \text{sign}(A) \\ S_{\pm 1}, & \text{if } 2(A + C) = \pm B \neq 0 \\ S, & \text{otherwise}, \end{cases}
\]

where

\[
S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad S_{\pm 1} = \begin{pmatrix} \pm 1 & 0 \\ 1 & \pm 1 \end{pmatrix}, \quad \text{and} \quad S^\frac{1}{2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.
\]

Note

\[
\sigma_{S^{\pm \frac{1}{2}}} = \frac{1}{2} \begin{pmatrix} 1 & \pm 1 & 1 \\ -2 & 0 & 2 \\ 1 & -1 & 1 \end{pmatrix},
\]

where \( M \mapsto \sigma_M \) is the homomorphism defined by the beginning of this chapter. So we have

\[
S^{\pm \frac{1}{2}} \circ [A, B, -A] = \left[ \pm \frac{1}{2} B, \mp 2A, \mp \frac{1}{2} B \right]
\]

In particular, \( S^{\pm \frac{1}{2}} \circ Q \) may be non-primitive—and even non-integral. Given any form \( Q \) with coefficients in \( \mathbb{Q} \), we define \( \nu_Q \in \mathbb{Q}_{>0} \) to be such that \( \nu_Q Q \) is integral and primitive.

**Definition 2.22.** If \( (Q) = (Q_0, Q_1, \ldots, Q_{l-1}) \) is the cycle of \( (Q, \tau_0) \) produced by Algorithm 3, the code of the path \( \rho_{Q, \tau_0} \) is the sequence of matrices \( (M_0, M_1, \ldots, M_{l-1}) \) such that \( Q_{n+1} = M_n \circ Q_n \), obtained while performing Algorithm 3.
Algorithm 3: The cycle of $Q$

Data: a pair $(Q, \tau_0)$ with $\tau_0 \gamma_Q$ as above

Result: the cycle $(Q) = (Q_0, Q_1, \ldots, Q_l)$ of $Q$

1. $Q \leftarrow Q^\text{red}$;
2. $Q_0 \leftarrow Q$;
3. $n \leftarrow 0$;
4. while $Q \neq Q_n$ or $n = 0$ do
5. $Q_{n+1} \leftarrow (\nu_{Q_n} S_{Q_n} \circ Q_n)^\text{nrm}$;
6. $n \leftarrow n + 1$;
7. end

Example 2.23. Consider the reduced form $Q = [1, 12, -1]$ of discriminant $D = 2^2 \cdot 37$. The cycle and code of $Q$ are as follows.

| $n$ | $Q_n$      | $M_n$        |
|-----|------------|--------------|
| 0   | [1, 12, -1]| $\begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix}$ |
| 1   | [3, 5, -1] | $\begin{pmatrix} 5 & -1 \\ 1 & 0 \end{pmatrix}$ |
| 2   | [-1, 5, 3] | $\begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}$ |
| 3   | [3, 1, -3] | $\begin{pmatrix} 13 & -11 \\ -1 & 1 \end{pmatrix}$ |

Note there is a “jump” in the discriminant after we encounter a symmetric form. This is a consequence of the fact that the path $\gamma_Q$ contains an elliptic point of order $e = 2$.

Again let $Q$ be an indefinite form of discriminant $D$ (which we assume non-square). It is seems likely that the condition $N(\epsilon) = -1$ on the fundamental unit $\epsilon$ of $O_D$ in our construction of the regular path $\rho_{Q,\tau_0}$ may be dropped. In fact, Algorithm 3 makes perfect sense for any indefinite form $Q$ (with non-square, positive discriminant). So one possible approach might be to (1) define $\rho_{Q,\tau_0}$ as the image in $X(1)$ of a path constructed in some way out of the code $(M_0, M_1, \ldots, M_{l-1})$ of $(Q, \tau_0)$ produced with the help of Algorithm 3, and then (2) prove that $\rho'_{Q,\tau_0}$ (after a suitable continuous reparametrisation) has the desired properties. But we have not explored this approach any further in this dissertation. (In the applications we have in mind next chapter it is possible to prove that $N(\epsilon) = -1$.)

Example 2.24. Consider the reduced form $Q = [5, 9, -7]$ of discriminant $D = 221$. The cycle of the form $Q$ is as follows.

| $n$ | $Q_n$      | $M_n$        |
|-----|------------|--------------|
| 0   | [5, 9, -7] | $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ |
| 1   | [-7, 5, 7] | $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ |
| 2   | [-5, 32, -7]| $\begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix}$ |
| 3   | [-7, 24, 11]| $\begin{pmatrix} -2 & 0 \\ 1 & 1 \end{pmatrix}$ |
| 4   | [11, 20, -11]| $\begin{pmatrix} 3 & -1 \\ -1 & 1 \end{pmatrix}$ |

It is well-known that the fundamental unit of $O_D$ has positive norm.
3. Higher levels

3.1. Reduction algorithms. Let $\Gamma$ be a group acting on a Riemann surface $X$. A fundamental domain for $\Gamma$ is a connected open subset $D$ of $X$ such that the following two properties hold.

$\text{FD 1:}$ No two points on $D$ lie in the same orbit of $\Gamma$.

$\text{FD 2:}$ The closure $D^{\text{clo}}$ of $D$ contains at least one element from each orbit.

The fundamental region associated to a fundamental domain $D$ is the closure $D^{\text{clo}}$ of $D$. A fundamental set may be defined as a set $D \subset S \subset D^{\text{clo}}$ such that the canonical map from $S$ into $\Gamma \setminus X$ is a bijection.

**Definition 3.1.** Suppose $S$ is a fundamental set for the action of $\Gamma_0(N)$ on $H$. We say a positive definite form $Q$ is $S$-reduced if $\pi Q \in F_N$.

We shall now describe a fundamental set for $\Gamma_0(N)$. As before assume that $N$ is an odd prime. Define

$$R(N) = \left\{-\frac{N-1}{2}, \ldots, -2, -1\right\} \cup \left\{1, 2, \ldots, \frac{N-1}{2}\right\}$$

and let $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ be the standard generators of $\text{SL}_2(\mathbb{Z})$. It is well-known that the union $F_N = \{SF^{\text{clo}}\} \cup \{T^rF^{\text{clo}} : r \in R(N)\}$, is a fundamental region for $\Gamma_0(N)$ with an even number of sides which are identified by the generators of $\Gamma_0(N)$

$$T^N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}, \text{ and } M_s = \begin{pmatrix} s' & -ss' - 1 \\ 1 & -s \end{pmatrix}, \in \Gamma_0(N),$$

with $s, s' \in R(N)$ such that $r'r \equiv -1 \pmod{N}$. (See e.g. Apostol [1], p. 76).

Now we briefly review a construction of a fundamental set $F_N'$ such that $F_N = (F_N')^{\text{clo}}$. First note that for each point $\tau \in \partial(F_N) = F_N - F_N^{\text{int}}$ the orbit $\Gamma^0(N)\tau$ consists of at most 3 points, say, $\tau_1, \tau_2,$ and $\tau_3$. Clearly $\Re(\tau_i) \neq \Re(\tau_j)$ if $i \neq j$, for each $i, j = 1, 2, 3$. So it makes sense to define the left most point $l(\tau)$ of the orbit $\Gamma^0(N)\tau$ as the point $\tau_i$ with the least real part $\Re(l(\tau)) \leq \Re(\tau_i), i = 1, 2, 3$. Then we may define $F_N'$ as

$$F_N' = F_N^{\text{int}} \cup \{l(\tau) : \tau \in \partial(F_N)\}$$

which is by construction a fundamental set for $\Gamma^0(N)$ such that $F_N = (F_N')^{\text{clo}}$.

So given any positive definite form $Q$ there is an element $R_{Q,N} \in \Gamma^0(N)$ such that $R_{Q,N} \circ Q$ is $F_N$-reduced. Such element may be computed as follows. Using Algorithm 1 we may find a matrix $M_1 \in \text{SL}_2(\mathbb{Z})$ such that $Q$ is $F$-reduced. Now by trial and error we may pick a matrix $M_2$ among the elements of the (finite) set of coset representatives $\{S\} \cup \{T^n : n \in R(N)\}$ of $\Gamma^0(N)$ in $\text{SL}_2(\mathbb{Z})$ such that
$M = M_2 M_1 \in \Gamma^0(N)$. Note that the imaginary quadratic $\tau = \pi_{Q'}$ attached to $Q' = M \circ Q$ clearly lies in the fundamental region $\mathcal{F}_N$. If $\tau \in \mathcal{F}^\text{int}_N$ then $R_{Q,N} = M$ has required property. So we suppose $\tau \in \partial(\mathcal{F}_N)$. If $\tau \notin \mathcal{F}'_N$ then for suitable choice among the generators $G$ of $\Gamma^0(N)$ introduced above we have $G\tau$ lies in the fundamental set $\mathcal{F}'_N$. So $R_{Q,N} = G M$ has the required property and we are done.

Now we turn to the $D > 0$ case. Let $Q = [A, B, C]$ be an indefinite binary quadratic form of discriminant $D = B^2 - 4AC > 0$. As before we assume $D$ is non-square, to avoid forms $Q$ such that the geodesic $\gamma_Q$ contains a side of the fundamental region $\mathcal{F}_N$, e.g. $Q = [1, 2, 0], [1, 4, 3], [1, 6, 8], \ldots$. Here we discuss an extension of the definition of normalisation and reduction of $Q$ for the group $\Gamma^0(N)$.

**Lemma 3.2.** Pick a base point $\tau_0$ of $\gamma_Q$, e.g. $\tau_0 = \hat{\gamma}_Q$. The form $Q$ is $\Gamma^0(N)$-equivalent to a form, we denote $Q^{\text{mt}}$, such that $\gamma_{Q^{\text{mt}}} \cap \mathcal{F}^\text{int}_N \neq \emptyset$.

**Proof.** Now let $R_{\tau_0,N}$ denote the matrix in $\Gamma^0(N)$ such that $\tau'_0 = R_{\tau_0,N} \circ \tau_0$ is $\mathcal{F}_N$-reduced. Clearly the geodesic $\gamma_{Q_1}$ attached to $Q_1 = R_{\tau_0,N} \circ Q$ is such that

$$\gamma_{Q_1} \cap \mathcal{F}^\text{int}_N \neq \emptyset,$$

except possibly when $\tau'_0 = \rho_{\pm 1} \pm r$, with $r \in \{1, 2, \ldots, \frac{N-1}{2}\}$, i.e. when the point $\tau'_0$ is one of the non-cusp vertices of the fundamental region $\mathcal{F}_N$. So let us suppose $\rho_{\pm 1} \pm r \in \gamma_{Q_1}$ and $\gamma_{Q_1} \cap \mathcal{F}^\text{int}_N = \emptyset$.\footnote{This case occurs very seldom in practice. For example, fix $b \in \mathbb{R}_{> 0}$ moderately large, and also fix a positive (non-square) discriminant $D$. Experimental evidence suggests that the probability that a form $Q = [A, B, C]$ picked randomly in the set $\{Q = [A, B, C] \in \mathbb{Z}^3 : |A| < b, |B| < b, |C| < b, B^2 - 4AC = D, \text{and } Q \text{ primitive}\}$}$
A LEVEL $N$ REDUCTION THEORY OF INDEFINITE BINARY QUADRATIC FORMS

$Q_2 = T^{-s} \circ Q_1$, where $s = \pm r$ and note that $\gamma_{Q_2}$ contains the point $\rho_{\pm 1}$. Now by Lemma 2.12 we know that

$$Q_3 = S \circ Q_2 = [C_2, -B_2, A_2]$$

is such that $\gamma_{Q_3}$ has non-trivial intersection with the open set $F^{\text{int}}$. Therefore $Q_4 = T^{s'} \circ Q_3$ is such that $\gamma_{Q_4}$ has non-trivial intersection with $T^{s'} F^{\text{int}} \subset F^{\text{int}}$, for each $s' \in \mathcal{R}(N)$. In particular if $ss' \equiv -1$ (mod $N$) then the form

$$Q_4 = (T^{s'} ST^{-s}) \circ Q_1 = (T^{s'} ST^{-s} \hat{R}_{Q,N}) \circ Q$$

is clearly $\Gamma^0(N)$-equivalent to $Q$, and it is plain that $\gamma_{Q_4} \cap F^{\text{int}} \neq \emptyset$. □

Given a geodesic segment $\gamma = \{\alpha, \beta\}$ let $\gamma^{\text{int}}$ be the open geodesic segment obtained by removing the endpoints $\alpha$ and $\beta$ of $\gamma$. So let $\sigma_{\pm, \infty} \subset \partial(F_N)$ be the open geodesic segment defined by

$$\sigma_{-1, \infty} = \left\{ \infty, \rho_{-1} - \frac{N - 1}{2} \right\}^{\text{int}}$$

$$\sigma_{1, \infty} = \left\{ \rho_{+1}, \infty, \frac{N - 1}{2} \right\}^{\text{int}}$$

In a similar way let us define the open geodesic segment $\sigma_{\pm, 0} \subset \partial(F_N)$ by

$$\sigma_{-1, 0} = \{\rho_{-1}, 0\}^{\text{int}}$$

$$\sigma_{1, 0} = \{0, \rho_{+1}\}^{\text{int}}$$

Now for the rest of this paragraph let us restrict the discussion only to forms $Q$ such that $\gamma_{Q} \cap F^{\text{int}} \neq \emptyset$. We say $Q$ is close to the cusp $\infty$ if $I(\gamma_Q, \sigma_{\text{sign}(A), \infty}) = 1$. This is equivalent to the condition

$$3|A| + \text{sign}(A)(4C + N^2A) + 2NB < 0.$$ 

The $N$-normalisation $Q^{N,\text{nrm}}$ of a form $Q$ close to the cusp $\infty$ is the $\Gamma^0(N)$-equivalent form $Q^{N,\text{nrm}} = T^{\left[\frac{4Q}{N}\right]} \circ Q$, where $[\cdot]$ is the nearest integer function. We say $Q$ is close to the cusp $0$ if $I(\gamma_Q, \sigma_{\text{sign}(A), 0}) = 1$. This means that

$$3|C| + \text{sign}(C)(4A + C) - 2B < 0.$$ 

The $N$-normalisation $Q^{N,\text{nrm}}$ of a form $Q$ close to the cusp $0$ is the $\Gamma^0(N)$-equivalent form $Q^{N,\text{nrm}} = (ST^{\delta(S\pi Q)} S) \circ Q$, where $\delta$ is as in Definition 2.13. For completeness, if $Q$ is neither close to the cusp $\infty$ nor close to the cusp $0$ we define the $N$-normalisation $Q^{N,\text{nrm}}$ of $Q$ to be $Q$ itself. Finally, the $N$-reduction $Q^{N,\text{red}}$ of an arbitrarily given indefinite form $Q$ (with non-square discriminant) is the normalisation $Q^{N,\text{red}} = (Q^{mt})^{N,\text{nrm}}$ of $Q^{mt}$, where $Q^{mt}$ is the form defined in

falls in this case is small.
Figure 3.2. The $N$-reduction of $Q = [-13, 108, -213]$, with $N = 13$.

Lemma 3.2. If a form $Q_1$ is the $N$-reduction of a form $Q_0$ then we say $Q_1$ is $N$-reduced.

Example 3.3. Let $N = 13$ and consider the primitive indefinite form

$$Q = [-13, 108, -213]$$

of discriminant $D = 588$. Note $\gamma_Q \cap F_{N}^{mt} = \emptyset$. Also $\rho_{+1} + r \in \gamma_Q$ for $r = 4$. So by the proof of Lemma 3.2 we may see that $Q^{mt} = (T^3ST^{-4}) \circ Q$ is a $\Gamma^0(N)$-equivalent form such that $\gamma_{Q^{mt}}$ meets the open set $F_{N}^{mt}$. Now since $Q^{mt}$ is neither close to the cusp $\infty$ nor close to the cusp $0$, then by definition $Q^{N-reduced} = Q^{mt}$, as depicted in Figure 3.2.

3.2. Geometric coding algorithm II. Note that $\Gamma^0(N) = S^{-1}\Gamma_0(N)S$, where $S = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. By a slight abuse of notation we write $X_0(N) = \Gamma^0(N) \backslash \mathcal{H}^*$.

As before let $Q = [A, B, C]$ be primitive indefinite form with non-square discriminant $D = B^2 - 4AC$. Now define $M_{N,Q} = M_Q^n$, where

$$M_Q = \begin{pmatrix} u - Bv & -2Cv \\ 2Av & u + Bv \end{pmatrix} \in \Gamma(1),$$

and $(u, v) \in \mathbb{Z}$ is a fundamental solution of the ordinary Pell equation

$$X^2 - DX^2 = 1,$$

and $n$ is the smallest positive integer such that $M_Q^n \in \Gamma_0(N)$. Now pick a base point $\tau_0$ of $\gamma_Q$ and let $g_{N,Q,\tau_0}$ denote the image of the path $\{\tau_0, M_{N,Q}\tau_0\}$ in the modular curve $X_0(N)$. The construction of the regular path in the proof of Theorem 2.19 carries over to $X_0(N)$ as follows. It is well-known that the elliptic points $\tau_e \in \mathcal{H}$ for the action

\footnote{It is more customary to write $X^0(N) = \Gamma^0(N) \backslash \mathcal{H}^*$. But we want to avoid writing non-standard expressions such as $X^0_0(N)$ (or $X^{0+}(N)$) when considering the Atkin-Lehner quotient defined by the Fricke involution $w_N$.}
of $\Gamma^0(N)$ in the upper half plane $\mathcal{H}$ are precisely the ones attached to primitive forms $P = [A, B, C]$ with $N \mid C$ and discriminant $\Delta = -3$, if the degree of the point is $e = 3$ and discriminant $\Delta = -4$, if the degree of the point is $e = 2$. Assume there is an elliptic point $\tau_e$ of degree $e = 2$, e.g. $\tau_e = r + \sqrt{-1} \in \mathcal{H}$ with $r \in \mathbb{Z}$ such that

$$r^2 \equiv -1 \pmod{N},$$

and that $\gamma_Q$ contains such elliptic point $\tau_e$. The matrix $S_{\frac{3}{2}}$ in the said construction is to be replaced by $T^a S_{\frac{3}{2}} T^{-r}$, where and $T = \left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right)$. Again let $n$ be the smallest positive integer such that $M^a_Q$ lies in $\Gamma^0(N)$. Further assume that the fundamental unit $\epsilon$ of the real quadratic order $\mathcal{O}_D$ has norm $N(\epsilon) = -1$. The matrix $M^1_Q$ is to be replaced by $M^n_{N,Q} = (M^1_Q)^n$, so that $(M^1_{N,Q})^2 = M_{N,Q}$. Let $\rho_{N,Q,n}$ be the regular analytic path thus obtained and call it the regular path of level $N$ attached to $Q$. This path is unique up to a regular analytic reparametrisation.

Now we need to extend Definition 2.13 to include some indefinite forms $Q$ that arise in Algorithm 4. As before put $\sigma = \{ \rho_{-1}, \rho_{+1} \}$. Let $\delta(Q)$ be just as in Definition 2.13, if $D > 4A^2$ and let $\delta(Q)$ be the integer such that the intersection number $I(\gamma_Q + \delta(Q), \sigma) = 1$ (whenever it exists), if $3A^2D < 4A^2$. Assume that $Q$ is $N$-reduced and that $Q$ is neither close to cusp $\infty$ nor close to cusp 0. Now put $a = \text{sign}(A)$, $d = \delta(Q)$, and define the matrix

$$S_{N,Q} = \begin{cases} 
T^a S T^{-a}, & \text{if } d = 0, \text{ i.e. } \rho_a \in \gamma_Q \\
T^{-a} S^{\frac{1}{2}} T^{-2a}, & \text{if } \rho_a \in \gamma_Q - a \\
T^{(d-a)} S^{\frac{1}{2}} T^{d-a}, & \text{if } \rho_a \in \gamma_Q + d \text{ and } |d| \neq 1 \\
T^d S^{\frac{1}{2}} T^d, & \text{if } i_N \in \gamma_Q \\
T^d S^{\frac{1}{2}} T^d, & \text{otherwise},
\end{cases} \quad (3.1)$$

where $i_N = i + k$ and $k \in C(N)$ is such that $k^2 \equiv -1 \pmod{N}$, whenever $N \equiv 1 \pmod{4}$, and $s^*$ is the element of $C(N)$ such that $ss^* \equiv 1 \pmod{N}$, given $s \in \mathbb{Z}$ with $s \neq 0 \pmod{N}$.

Now we shall consider some examples of $N$-cycles $(Q)_N = (Q_0, \ldots, Q_{l-1})$ that may help to clarify the above ideas. In the tables below the last column encodes the steps followed while executing the algorithm, using the the convention that a number from 1 to 5 indicates one of the five cases of the definition of matrix $S_{N,Q}$, while 0 (resp. $\infty$) indicates the normalisation step associated to a form close to the cusp 0 (resp. the cusp $\infty$).

**Example 3.4.** Suppose $N = 13$. Consider the indefinite form $Q = [-13, 108, -213]$ of discriminant $D = 7^2 \cdot 12$. The $N$-reduction of
Algorithm 4: The $N$-cycle of $Q$

Data: a primitive indefinite binary quadratic form $Q$
Result: the $N$-cycle $(Q)_N = (Q_0, Q_1, \ldots, Q_{l-1})$ of $Q$

1 $Q \leftarrow Q^{N\text{-red}}$;
2 $Q_0 \leftarrow Q$;
3 $n \leftarrow 0$;
4 while $Q \neq Q_n$ or $n = 0$ do
5 
6 
7 
8 
9 end
10 $n \leftarrow n + 1$;
11 end

$Q^{N\text{-red}} = [11, -70, 98]$ of $Q$ has the following $N$-cycle.

| $n$ | $Q_n$          | $M_n$   | Case |
|-----|----------------|---------|------|
| 0   | $[11, -70, 98]$ | $\begin{pmatrix} 3 & -13 \\ -4 & 1 \end{pmatrix}$ | 5    |
| 1   | $[-6, 18, 11]$  | $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ | 0    |
| 2   | $[-13, -4, 11]$ | $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ | 5    |
| 3   | $[2, -26, 11]$  | $\begin{pmatrix} 0 & 13 \\ 0 & 1 \end{pmatrix}$ | $\infty$ |
| 4   | $[2, 26, 11]$   | $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ | 5    |
| 5   | $[-13, 4, 11]$  | $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ | 0    |
| 6   | $[-6, -18, 11]$ | $\begin{pmatrix} -4 & -13 \\ -6 & -13 \end{pmatrix}$ | 5    |
| 7   | $[11, 70, 98]$  | $\begin{pmatrix} 1 & 2 \\ -3 & -1 \end{pmatrix}$ | 3    |
| 8   | $[2, -2, -73]$  | $\begin{pmatrix} -2 & 13 \\ 1 & -7 \end{pmatrix}$ | 3    |
| 9   | $[11, 18, -6]$  | $\begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}$ | 0    |
| 10  | $[11, -18, -6]$ | $\begin{pmatrix} -7 & -2 \\ 1 & -6 \end{pmatrix}$ | 2    |
| 11  | $[2, 2, -73]$   | $\begin{pmatrix} 2 & -13 \\ 1 & -6 \end{pmatrix}$ | 3    |

Figure 3.3 depicts the intersection of the geodesics $\gamma_{Q_n}$, with the fundamental domain $\mathcal{F}_N$, for $n = 0, 1, 2$ and 3. Similarly, Figure 3.4 depicts the intersection of the geodesics $\gamma_{Q_n}$, with the fundamental domain $\mathcal{F}_N$, for $n = 9, 10$ and 11. Note that instance (4) of $S_{N,Q}$ in Equation 3.1 does not take place. This means that the geodesic $\gamma_Q$ does not contain an elliptic point $\tau_e$ of degree $e = 2$. 
Example 3.5. Now suppose $N = 5$ and consider the $N$-reduced form $Q = [1, -1, -3]$ of discriminant $D = 13$. The $N$-cycle of $Q$ is as follows.

| $n$ | $Q_n$          | $M_n$         | Case |
|-----|----------------|---------------|------|
| 0   | $[1, -1, -3]$  | $\begin{pmatrix} -1 & 5 \\ 3 & -1 \end{pmatrix}$ | 4    |
| 1   | $[3, -16, 17]$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\infty$ |
| 2   | $[3, 14, 12]$  | $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ | 3    |
| 3   | $[1, -10, 12]$ | $\begin{pmatrix} 1 & -10 \\ 0 & 1 \end{pmatrix}$ | $\infty$ |
| 4   | $[1, 10, 12]$  | $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ | 3    |
| 5   | $[3, -14, 12]$ | $\begin{pmatrix} 1 & -5 \\ 0 & 1 \end{pmatrix}$ | $\infty$ |
| 6   | $[3, 16, 17]$  | $\begin{pmatrix} 3 & 5 \\ -1 & -1 \end{pmatrix}$ | 4    |
| 7   | $[1, 1, -3]$   | $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ | 5    |
| 8   | $[-1, -5, -3]$ | $\begin{pmatrix} 5 \\ 0 \end{pmatrix}$ | $\infty$ |
| 9   | $[-1, 5, -3]$  | $\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$ | 5    |
Figure 3.5. Beginning of the $N$-cycle of $Q = [1, -1, -3]$, with $N = 5$.

Figure 3.5 depicts the intersections of the geodesics $\gamma_{Q_n}$ with the fundamental domain $\mathcal{F}_N$, for $n = 1, 2, \text{and } 3$. Note that $Q_n$ falls in case (4), for $n = 0$ and 6. This means that $\gamma_Q$ contains an elliptic point $\tau_e$ of order $e = 2$.

Remark 3.6. It is not hard to see that for each prime $N > 1$, the $N$-cycle of the indefinite form $Q = [2, 2N, -1]$ is given by

$$
\begin{array}{ccc}
n & Q_n & M_n \\
0 & [2, 2N, -1] & \left( \begin{array}{cc} 1 & 0 \\ -2N & 1 \end{array} \right) \\
1 & [2, -2N, -1] & \left( \begin{array}{cc} 1 & -N \\ 0 & 1 \end{array} \right)
\end{array}
$$

Note that the matrices $M_0 = \left( \begin{array}{cc} 1 & 0 \\ -2N & 1 \end{array} \right)$ and $M_0 = \left( \begin{array}{cc} 1 & -N \\ 0 & 1 \end{array} \right)$ are parabolic. So the code $(M_0, M_1, \ldots)$ of some indefinite forms $Q$ may consist of parabolic elements only.

Definition 3.7. The $N$-code of $Q$ is the sequence of matrices $(M_0, M_1, \ldots)$ defined by $Q_{n+1} = M_n \circ Q_n$, where the matrices $M_n$ come from the computation of the $N$-cycle $(Q)_N = (Q_0, Q_1, \ldots Q_l)$ of $Q$ using Algorithm 4.

References

1. T. M. Apostol, *Modular functions and Dirichlet series in number theory*, Springer-Verlag, New York, 1976, Graduate Texts in Mathematics, No. 41.
2. A. F. Beardon, *The geometry of discrete groups*, Graduate Texts in Mathematics, vol. 91, Springer-Verlag, New York, 1995, Corrected reprint of the 1983 original.
3. Y. Choie and L. A. Parson, *Rational period functions and indefinite binary quadratic forms. II*, Illinois J. Math. 35 (1991), no. 3, 374–400.
4. S. Katok, *Coding of closed geodesics after Gauss and Morse*, Geom. Dedicata 63 (1996), no. 2, 123–145.
5. A. W. Knapp, *Elliptic curves*, Princeton University Press, Princeton, NJ, 1992.
6. A. P. Ogg, *Real points on Shimura curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 277–307.
7. P. C. Sarnak, *Prime geodesic theorems*, Stanford Ph.D. thesis (1980).
8. S. Schoeneberg, *Elliptic modular functions: an introduction*, Springer-Verlag, New York-Heidelberg, 1974.

E-mail address: ccastanobernard@gmail.com
URL: http://sarva.no-ip.info/ccb/index.html