Werk

Titel: Arithmetic Fuchsian groups and the number of systoles.

Autor: Schmutz, Paul

Jahr: 1996

PURL: https://resolver.sub.uni-goettingen.de/purl?266833020_0223|log8

Math. Z. 223, 13–25 (1996)

Mathematische Zeitschrift

Arithmetic Fuchsian groups and the number of systoles

Paul Schmutz

Institut de Mathématiques, Université de Lausanne CH-1015 Lausanne, Switzerland
(e-mail: Paul.Schmutz@ima.unil.ch)

Received 2 September 1994; in final form 10 March 1995

1 Introduction

The kissing number problem for lattice spheres consists of finding the lattice sphere packing with the biggest possible number of spheres touching one sphere. In Euclidean spaces this is a well known problem with a developed theory, see for example [2] and the references there. Here, I consider a non-Euclidean analogue in dimension two. The problem is to find the Riemann surface of a fixed signature (g,n) (g the genus, n the number of cusps being the unique boundary components) such that the number (called kissing number) of the systoles (shortest closed geodesic) is maximal. As in the Euclidean case, such surfaces are supposed to have many important properties.

The kissing number problem is related to the best lattice sphere packing problem. Its non-Euclidean analogue in dimension two is the problem to find the Riemann surface of a given signature with the systole of maximal length. I called them *maximal surfaces*, see [6] and [7]. I proved the following theorem about them.

Theorem[6] *A maximal surface M has at least $dim(T(M))+1$ different systoles where $T(M)$ denotes the Teichmüller space of M.*

The number dim $T(M)+1$ is thus a lower bound for the maximal kissing number, and maximal surfaces are the first candidates for being the best kissing number surfaces.

The next idea for finding the best kissing number surface is to look for surfaces with big automorphism groups. By the action of this group the systoles are separated in isometry classes. A generic surface has of course only one isometry class of systoles. In this case the number of systoles is bounded from above by $K \cdot \dim(T(M))$, K a constant, since the order of the automorphism group is bounded like that.

Certainly the best candidates for the best kissing number surface are those surfaces which not only have a big automorphism group, but also many different isometry classes of systoles. In fact, there exist surfaces with an arbitrarely big number of different isometry classes of systoles. Such surfaces can be constructed by arithmetic groups. The most simple examples are the principal congruence subgroups of $PSL,(2,\mathbf{Z})$, but we will see other congruence subgroups with the same property. I shall prove the following main result.

Theorem *There exists a Riemann surface M_K corresponding to a congruence subgroup of $PSL(2,\mathbf{Z})$ such that the number of systoles is bigger than $K \cdot dim(T(M))$ for every given integer K.*

This is a new example which shows the great *geometric* importance of congruence subgroups of arithmetic Fuchsian groups.

The main theorem is certainly not optimum. Its proof and the calculation of examples give strong reasons that the following conjecture is true.

Conjecture *(i) For every positive integer K there exists an integer $Q(K)$ such that for every $N > Q(K)$ the surface $C(N)$ corresponding to the principal congruence subgroup $\Gamma(N)$ of $PSL(2,\mathbf{Z})$ has more than $K \cdot dim(T(C(N)))$ different systoles.*

(ii) There are infinite many different integers N_i such that $C(N_i)$ has more than $(dim(T(C(N_i))))^{7/6}$ different systoles.

The paper is organized like follows. Section 2 defines and describes some congruence subgroups of $PSL(2,\mathbf{Z})$. Section 3 introduces the degree of a systole which is a geometric measure and indicates the "minimal" distance between a given systole and the set of the cusps. Systoles with different degree are in different isometry classes, the degree thus allows the classification of the isometry classes of systoles. It is shown that there exist congruence surfaces with systoles of each prescripted degree hence with an arbitrarely big number of different isometry classes of systoles. In the same time it is shown that these isometry classes are big enough to prove the main theorem. Finally, I give in Section 4 some concrete examples for the calculation of the degree of the systoles which justify part (i) of the conjecture above.

Some remarks on the bibliography. For counting the systoles of the surfaces corresponding to the congruence subgroups other methods have been described, see [10], [4], [3], [1]. Concerning the kissing number problem I already noted [2]. For congruence subgroups there is a lot of literature, I only cite [8], [5], [9].

2 Some congruence subgroups of $PSL(2,\mathbf{Z})$

Definition Let A and N be positive integers with $AN > 3$. Let

$$\Gamma_A(N) = \left\{ \begin{bmatrix} 1+aAN & bAN \\ cN & 1+dAN \end{bmatrix} \in SL(2,\mathbf{Z}) \middle| a,b,c,d \in \mathbf{Z} \right\}.$$

Elements of $\Gamma_A(N)$ are also written as $U(a,b,c,d)$ instead of

$$\begin{bmatrix} 1+aAN & bAN \\ cN & 1+dAN \end{bmatrix}.$$

Let

$$\Gamma^0(A) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PSL(2,\mathbf{Z}) \,\middle|\, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} \star & 0 \\ \star & \star \end{bmatrix} \bmod (\mathbf{A}) \right\}.$$

If $A = 1$, than I also write $\Gamma(N)$ instead of $\Gamma_A(N)$. Γ denotes the modular group $PSL(2,\mathbf{Z})$.

Remark. By $AN > 3$ it follows that $\Gamma_A(N)$ has no elliptic element.

Theorem 1 *(i) $\Gamma(N)$ is a normal subgroup of Γ of index*

$$N^3/2\prod_{p|N}(1-1/p^2)$$

where the product runs over every prime of N.
(ii) $\Gamma^0(A)$ is a subgroup of Γ of index

$$A\prod_{p|A}(1+1/p).$$

(iii) $\Gamma(AN)$ is a normal subgroup of $\Gamma_A(N)$ of index A.
(iv) $\Gamma_A(N)$ is a normal subgroup of $\Gamma^0(A)$ of index

$$\frac{AN^3\prod_{p|AN}(1-1/p^2)}{2\prod_{p|A}(1+1/p)}.$$

Proof. (i) is well known. For (ii) see for example [3].

(iii) It is clear that $\Gamma(AN)$ is a normal subgroup of $\Gamma_A(N)$. Let

$$Z = \begin{bmatrix} 1 & 0 \\ N & 1 \end{bmatrix}.$$

Then $\Gamma_A(N) = \bigcup_{k=0}^{A-1} Z^k\Gamma(AN)$ as it is easy to verify. Therefore, the index is A.

(iv) Again, it is clear that $\Gamma_A(N)$ is a normal subgroup of $\Gamma^0(A)$. By (i) and (iii) the index of $\Gamma_A(N)$ in Γ is

$$A^2N^3/2\prod_{p|AN}(1-1/p^2).$$

This together with (ii) proves (iv). □

Definition (i) The Riemann surface which corresponds to $\Gamma_A(N)$ is denoted by $C_A(N)$.
(ii) $T(M)$ denotes the Teichmüller space of the Riemann surface M.
(iii) The signature (g,n) of a Riemann surface indicates the genus g and the number n of boundary components which are by convention simple closed geodesics or cusps.

Corollary 1 *Let $\delta_A(N)$ be the dimension of the Teichmüller space of $C_A(N)$. Let $\Sigma_A(N)$ be the index of $\Gamma_A(N)$ in $\Gamma^0(A)$. Then*

$$\delta_A(N)/\Sigma_A(N) < A/2\prod_{p|A}(1+1/p)$$

and $\delta_A(N)/\Sigma_A(N)$ is bounded from above independently from N.

Proof. This follows by (ii) and (iv) of Theorem 1. □

3 The degree of a systole

Definition Let u be a non-oriented closed geodesic in $C_A(N)$. I denote by $M(u)$ the two conjugacy classes (which may coincide) of matrices U in $\Gamma_A(N)$ which corresponds to u (such that we have $|tr(U)|/2 = \cosh(L(u)/2)$ where $L(u)$ stands for the length of u). I also say for a matrix $U \in M(u)$ that it *corresponds* to u. If u is a cusp, then $M(u)$ may contain more than 2 conjugacy classes of matrices.

Definition (i) The *systole* of a Riemann surface M is the shortest simple closed geodesic which is not a boundary geodesic.
(iv) The *automorphism group* of a Riemann surface consists of the *orientation preserving* automorphisms. The *restricted automorphism group of $C_A(N)$* contains the automorphisms induced by

$$\Gamma_A(N) \to X\Gamma_A(N)X^{-1}$$

with $X \in \Gamma^0(A)$.
(iii) The *isometry class* of a systole u of $C_A(N)$ contains all systoles u' of $C_A(N)$ such that there exists an automorphism ϕ of the restricted automorphism group of $C_A(N)$ with $\phi(u) = u'$.

Lemma 1 *Let $2x$ be the length of the systole of $C_A(N)$. Then*

$$2\cosh x = AN^2 - 2.$$

Proof. Let $U = U(a,b,c,d) \in \Gamma_A(N)$. Then for the trace of U we have $tr(U) = 2 + (a+d)AN$. Since $det(U) = 1$ we have $a + d \equiv 0 \bmod (N)$. It follows that

$$2\cosh x \geq AN^2 - 2.$$

On the other hand the matrix

$$\begin{bmatrix} 1 & AN \\ -N & 1 - AN^2 \end{bmatrix}$$

has the desired trace. □

Definition For integers x and y the greatest common positive factor is denoted by (x,y).

Definition (i) $U = U(a,b,c), a,b,c \in \mathbf{Z}$, defines the following matrix.

$$U = \begin{bmatrix} 1+aAN & bAN \\ cN & 1-aAN-AN^2 \end{bmatrix}.$$

(ii) $V = V(a',b',c'), a',b',c' \in \mathbf{Z}$, defines the following matrix.

$$V = \begin{bmatrix} 1+a'AN & b'AN \\ c'N & 1-a'AN \end{bmatrix}.$$

Lemma 2 *In the notation of the preceeding definition we have*

(i) $U(a,b,c)$ corresponds to a systole of $C_A(N)$ if and only if $a^2A + aAN + bc + 1 = 0$ and all matrices corresponding to a systole of $C_A(N)$ can be written like that.

(ii) $V(a',b',c')$ corresponds to a cusp of $C_A(N)$ if and only if $a'^2A + b'c' = 0$ and all matrices corresponding to a cusp of $C_A(N)$ can be written like that.

(iii) If $U(a,b,c)$ corresponds to a systole of $C_A(N)$, then $b \neq 0$, $c \neq 0$ and $(c,A) = (b,A) = 1$.

Proof. (i) and (ii) follow since the determinants of U and of V must be one 1 and since the trace of a matrix corresponding to a systole must be $2 - AN^2$ by Lemma 1. (iii) follows by (i). □

Lemma 3 *Let u be a systole of $C_A(N)$ and v a cusp. Let $U(a,b,c)$ correspond to u and $V(a',b',c')$ correspond to v. Let $W = UV$. Then*

$$tr(W) = [(2a+N)Aa' + cb' + bc' - 1]AN^2 + 2.$$

Proof. By calculation. □

Definition (i) I denote by v_0 the cusp in $C_A(N)$ which corresponds to the matrix $V(0,1,0)$. This matrix is denoted by V_0.
(ii) The subset $\mathscr{V}$ of the cusps of $C_A(N)$ contains a cusp v if there exists an element ϕ of the restricted automorphism group of $C_A(N)$ with $\phi(v_0) = v$.
(iii) Let u be a systole and v a cusp of $C_A(N)$, let $U = U(a,b,c) \in M(u)$ and $V = V(a',b',c') \in M(v)$. Set $D(U,V) = |(2a+N)Aa' + cb' + bc'|$.
(iv) I call $D(u) = \min\{D(U,V) | V \in M(v), v \in \mathscr{V}\}$ the *degree* of u.
(v) A *canonical representative* of an isometry class $\bar{u}$ of systoles of $C_A(N)$ is a matrix $U = U(a,b,c)$ corresponding to a systole u of $\bar{u}$ with $c = D(u)$.

Lemma 4 *(i) The degree of a systole is invariant with respect to the restricted automorphism group of $C_A(N)$.*

(ii) Every isometry class of systoles has a canonical representative.

Proof. (i) Let u be a systole, $v \in \mathscr{V}$ a cusp, $U \in M(u)$ and $V \in M(v)$ such that $D(U,V) = D(u)$. Then the lengths of the two geodesics corresponding to $W = UV$ and $W' = UV^{-1}$, respectively, are well defined by Lemma 3 and part (i) of the lemma follows.

(ii) By (i), there exists a systole u' in the isometry class of u and a $U' \in M(u')$ such that $D(u') = D(U, V_0)$. This implies $D(u) = \pm c$ and since we can replace U' by its inverse, we can assume $D(u) = c$. □

Remark In the notation of Lemma 4, W (or W') corresponds to the shortest geodesic with the property that the geodesics corresponding to U, V and W (or W') are the boundary geodesics of a surface of signature $(0,3)$. Therefore, the degree of a systole has a precise geometric meaning.

If in a surface of signature $(0,3)$ two boundary geodesics x and y are fixed while the length of the third increases, then also the length of the common orthogonal between x and y increases. In this sense, the degree of a systole is a measure for its shortest distance to a cusp of $\mathscr{V}$. A canonical respresentative corresponds to a systole such that the "nearest" cusp of $\mathscr{V}$ is v_0.

Proposition 1 *Let $V = V(a', b', c'), c' \leq 0$, correspond to a cusp $v \in \mathscr{V}$ of $C_A(N)$ such that there exist a systole u and a corresponding matrix U with $D(u) = D(U, V)$. Then there exists integers x and y with $(x, Ay) = 1$, and $a' = -xy$, $b' = x^2$, $c' = -Ay^2$.*

Proof. By definition there exists an $X \in \Gamma^0(A)$ and an integer k such that $V = XV_0^k X^{-1}$. Let

$$X = \begin{bmatrix} \alpha & A\beta \\ \gamma & \delta \end{bmatrix}.$$

Then

$$XV_0^k X^{-1} = \begin{bmatrix} 1 - k\alpha\gamma AN & k\alpha^2 AN \\ -k\gamma^2 AN & 1 + k\alpha\gamma AN \end{bmatrix}.$$

Since $D(U, V) = D(u)$, it follows that $|k| = 1$, and since $(\alpha, A\gamma) = 1$, the proposition follows. □

Corollary 2 *Let $U = U(a, b, c)$ correspond to a systole u of $C_A(N)$. Then $D(u)$ corresponds to the smallest (with respect to the absolute value) non-zero integer D which is represented by the quadratic form*

$$cx^2 - (2a + N)Axy - bAy^2.$$

Proof. Clear by Proposition 1 ($D(u) = 0$ is excluded by Lemma 2(iii) and Lemma 4(ii)). □

Lemma 5 *Let $U = U(a, b, c)$ correspond to a systole u of $C_A(N)$. Let $m \neq 0$, s, t be integers such that*

$$cs^2 - (2a + N)Ast - bAt^2 = m.$$

Let $(x_0, y_0) = (cs - aAt, t)$.

(i) (x_0, y_0) is an integer solution of the equation

$$x^2 - ANxy + Ay^2 = cm.$$

(ii) Put

$$X = \begin{bmatrix} -1 & AN \\ 0 & 1 \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & 0 \\ N & -1 \end{bmatrix}.$$

Let $[x_0, y_0]$ *denote a column vector. Then* $X[x_0, y_0]$ *and* $Y[x_0, y_0]$ *are also integer solutions of*

$$x^2 - ANxy + Ay^2 = cm.$$

Proof. I will prove the claim for $X[x_0, y_0]$. The other claims are proved by similar calculations using the equation (see Lemma 2)

$$a^2A + aAN + bc + 1 = 0.$$

$X[x_0, y_0] = [-cs + aAt + ANt, t]$.

$$(-cs + aAt + ANt)^2 - AN(-cs + aAt + ANt)t + At^2 =$$

$$= c(cs^2 - (2a+N)Ast) + At^2(a^2A + aAN + 1) = c(cs^2 - (2a+N)Ast) - bcAt^2 = cm.$$

□

Proposition 2 *Let* $U = U(a, b, c)$ *correspond to a systole* u *of* $C_A(N)$, $N > 1$. *Assume that* $c^2 < AN + A + 1$. *Then* $D(u) = |c|$.

Proof. Let $m = D(u)$. By Corollary 2 we have $m \leq |c|$.

(i) Assume firstly that there are integers s, t, x_1, y_1 with $x_1 = cs - aAt, y_1 = t$ and

$$cs^2 - (2a + N)Ast - bAt^2 = m, \qquad x_1^2 - ANx_1y_1 + Ay_1^2 = |c|m.$$

It then follows by Lemma 5 (compare Fig. 1) that there exist integers x_0 and y_0 with

$$x_0^2 - ANx_0y_0 + Ay_0^2 = |c|m$$

and $x_0^2 \leq |c|m$ and $y_0^2 \leq |c|m/A$. If

$$z^2 + ANz^2 + Az^2 = |c|m$$

then $|z| < 1$ by hypothesis. Since

$$x^2 - ANxy + Ay^2 = |c|m$$

describes a hyperbola with asymptotics passing through the origin, it follows that (x_0, y_0) must lie on the axes.

Assume that $(x_0, y_0) = (\pm\sqrt{|c|m}, 0)$. This implies by Lemma 5 that $x_1 \equiv y_1 \equiv 0 \bmod (\sqrt{|c|m})$ and therefore, $cs \equiv t \equiv 0 \bmod (\sqrt{|c|m})$. By the equation

$$cs^2 - (2a + N)Ast - bAt^2 = m$$

we conclude $m \equiv 0 \bmod (\sqrt{|c|m})$, thus $m = |c|$.

If $(x_0, y_0) = (0, \pm\sqrt{|c|m/A})$, then it follows by the same argument that $m \equiv \bmod(\sqrt{|c|m/A})$ and hence $m = |c|$ since $(c, A) = 1$ by Lemma 2. This implies moreover that this second case is only possible for $A = 1$.

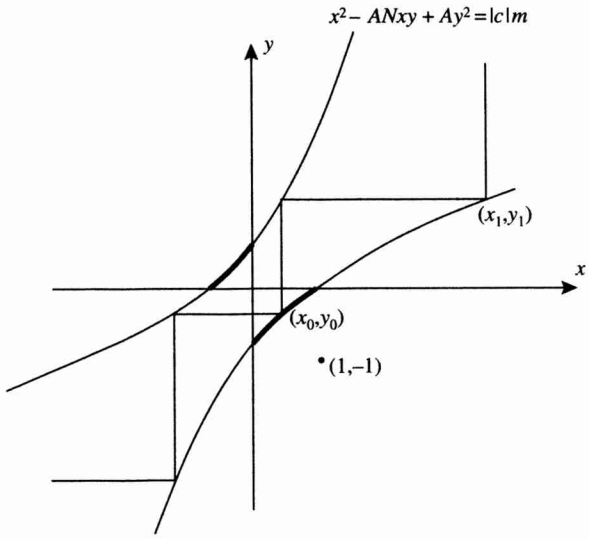

Fig. 1. To every integer solution (x_1, y_1) of $x^2 - ANxy + Ay^2 = |c|m$ corresponds an integer solution (x_0, y_0) on the thick region of the picture. If the points $(-1, 1)$ and $(1, -1)$ are on the "outside" of the hyperbola as in the picture, then (x_0, y_0) must be a point on the axes

(ii) Let $y_{min} > 0$ be defined by $(A^2N^2 - 4A)y_{min}^2 - 4|c|m = 0$. Let $x_y = ANy_{min}/2$. Then (x_y, y_{min}) is the real solution of

$$x^2 - ANxy + Ay^2 = -|c|m$$

with minimal positive y.

Let $x_{min} > 0$ be defined by $(A^2N^2 - 4A)x_{min}^2 - 4A|c|m = 0$. Let $y_x = Nx_{min}/2$. Then (x_{min}, y_x) is the real solution of

$$x^2 - ANxy + Ay^2 = -|c|m$$

with minimal positive x.

Assume now that there exist positive integers x_1 and y_1 with

$$x_1^2 - ANx_1y_1 + Ay_1^2 = -|c|m.$$

By an analogous argument as above (compare Fig. 2) there exist integers x_0 and y_0 with

$$x_0^2 - ANx_0y_0 + Ay_0^2 = -|c|m$$

and $x_{min} \leq x_0 \leq x_y$ and $y_{min} \leq y_0 \leq y_x$.

But since $x_y/y_{min} > 1$ and $y_x/x_{min} > 1$ and

$$z^2 - ANz^2 + Az^2 = -|c|m$$

for $|z| < 1$ by hypothesis, there cannot exist such integers x_0 and y_0 which contradicts the assumption that

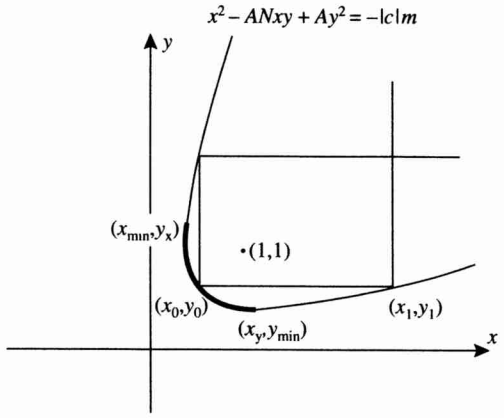

Fig. 2. To every integer solution $(x_1, y_1), x_1 > 0, y_1 > 0$, of $x^2 - ANxy + Ay^2 = -|c|m$ corresponds an integer solution (x_0, y_0) on the thick region of the picture. If the point $(1, 1)$ is on the "outside" of the hyperbola as in the picture, then (x_0, y_0) cannot exist

$$x_1^2 - ANx_1y_1 + Ay_1^2 = -|c|m.$$

□

Theorem 2 *Let K be an integer. Then for every A there exists an N such that $C_A(N)$ has (at least) K different isometry classes of systoles.*

Proof. Let $N = \prod_{j=1}^{K}(Aj^2 + 1)$, $a_n = n$, $c_n = An^2 + 1$ and $b_n = -1 - nAN/c_n$, $n \leq K$ a positive integer. Then b_n is an integer and $a_n^2A + a_nAN + b_nc_n + 1 = 0$ and therefore, by Lemma 2, $U_n = U_n(a_n, b_n, c_n)$ corresponds to a systole u_n of $C_A(N)$ for every integer n with $1 \leq n \leq K$. Moreover, $n^2 < AN + A + 1$ for every $n \leq K$ if $K > 4$, say. It follows by Proposition 2 that $D(u_n) = c_n = An^2 + 1$, $1 \leq n \leq K$. The theorem now follows by Lemma 4. □

Theorem 3 *Let K be an integer. Then for every A there exists an N such that the number of systoles of $C_A(N)$ is bigger than $K \cdot dim(T(C_A(N)))$.*

Proof. (i) Let N, a_n, b_n, c_n, u_n, U_n be defined as in the proof of Theorem 2 and let $K > 4$. Let $v_n \in \mathscr{V}$ be a cusp and $V_n = V_n(a_n', b_n', c_n')$ a corresponding matrix with $D(U_n, V_n) = D(u_n)$, $1 \leq n \leq K$. By Proposition 1 we can write $a_n' = -x_ny_n$, $b_n' = x_n^2$, $c_n' = -Ay_n^2$.

Let $V_n' = U_nV_nU_n^{-1}$. Then $tr(U_nV_n') = tr(U_nV_n)$, hence $D(U_n, V_n') = D(u_n)$ and V_n' can be described by x_n' and y_n' as in Proposition 1. By calculation we obtain

$$x_n' = (1 + a_nAN)x_n + b_nANy_n$$

and

$$y_n' = c_nNx_n + (1 - a_nAN - AN^2)y_n.$$

(x_n, y_n) is a solution of one of the two equations

$$c_nx^2 - (2a_n + N)Axy - Ab_ny^2 = \pm c_n.$$

(ii) Assume firstly that (x_n, y_n) is a solution of

$$c_n x^2 - (2a_n + N)Axy - Ab_n y^2 = c_n.$$

Then, by Lemma 5, $(c_n x_n - a_n A y_n, y_n)$ and $YX[c_n x_n - a_n A y_n, y_n] =: [w_n, z_n]$ are solutions of

$$x^2 - ANxy + Ay^2 = c_n^2$$

where X, Y and the symbol $[,]$ are defined as in Lemma 5.

Going back we obtain a solution $((w_n + a_n A z_n)/c_n, z_n) =: (r_n, z_n)$ of

$$c_n x^2 - (2a_n + N)Axy - Ab_n y^2 = c_n.$$

By calculation we obtain

$$r_n = -x_n - a_n x_n AN + (1 + a_n^2 A + a_n AN)ANy_n/c_n$$

$$z_n = -Nc_n x_n + a_n ANy_n + (AN^2 - 1)y_n$$

and it follows by the equation $a_n^2 A + a_n AN + b_n c_n + 1 = 0$ (see Lemma 2) that

$$(r_n, z_n) = (-x_n', -y_n').$$

We can repeat the hole procedure and it follows as in the proof of Proposition 2 that v_n has a corresponding matrix $W_n = W_n(-\xi_n \eta_n, \xi_n^2, -A\eta_n^2)$ with $\eta_n^2 \leq c_n^2/A$ (compare Fig. 1). By the proof of Proposition 2, $\eta_n = 0$ or, if $A = 1$, $\eta_n = \pm c_n$. In the first case we have $v_n = v_0$, in the second case v_n corresponds to a different cusp.

(iii) Assume now that (x_n, y_n) is a solution of

$$c_n x^2 - (2a_n + N)Axy - Ab_n y^2 = -c_n.$$

The same argument as in (ii) is possible and we obtain a contradiction as in the proof of Proposition 2.

(iv) We have proved that there exist at most two different cusps which are "nearest" to the systole u_n, $1 \leq n \leq K$. More precisely, we have proved that there exists at most one non-trivial element ϕ of the restricted automorphism group of $C_A(N)$ such that $\phi(u_n) = u_n$. It follows that the order of the isometry class of u_n is at least half of the order of the restricted automorphism group of $C_A(N)$. Corollary 1 and Theorem 2 now imply the theorem. □

4 Examples for the degree of systoles

We calculate the degree of the systoles for some examples. By Lemma 2, we have to look how the integers $f(a) = Aa^2 + aAN + 1$ can be parted into two factors b and c. It can be shown that it is sufficient to analyse the possibilities for $-AN/2 \leq a < 0$.

I firstly give some examples for $A = 1$.

(a) $N = 21$. In this case all numbers $f(a) = a^2 + Na + 1, -N/2 \leq a < 0$, are primes and $C(21)$ has only systoles of degree 1. The same is true for $N = 9$. I conjecture that these are the unique surfaces $C(N), N > 5$, which have only systoles of degree 1 (which are the separating systoles).

(b) $N = 24$. In this case all numbers $f(a) = a^2 + Na + 1, -N/2 \leq a < 0$, are primes or twice a prime with the unique exeption $|f(-12)| = 143 = 11 \cdot 13$. It is obvious that the corresponding systole has degree 2. Therefore, $C(24)$ has only systoles of degree 1 and 2.

Since all surfaces $C(N), N \geq 6$, N even, have systoles of degree 1 and 2, this is an extremal example. Also the surfaces $C(6)$, $C(8)$ and $C(12)$ have only systoles of degree 1 and 2. I conjecture that these are all such exceptions with N even, $N \geq 6$.

These examples justify the following conjecture.

Conjecture *For every positive integer K there exists an integer $Q(K)$ such that for every $N > Q(K)$, $C(N)$ has more than $K \cdot dim(T(C(N)))$ different systoles.*

(c) $N = 22$. I give the list of the numbers $|f(a)|, -N/2 \leq a < 0$.

$|f(-11)| = 120 = 2 \cdot 60 = 3 \cdot 40 = 4 \cdot 30 = 5 \cdot 24 = 6 \cdot 20 = 8 \cdot 15 = 10 \cdot 12$
$|f(-10)| = 119 = 7 \cdot 19$
$|f(-9)| = 116 = 2 \cdot 58 = 4 \cdot 29$
$|f(-8)| = 111 = 3 \cdot 37$
$|f(-7)| = 104 = 2 \cdot 52 = 4 \cdot 26 = 8 \cdot 13$
$|f(-6)| = 95 = 5 \cdot 19$
$|f(-5)| = 84 = 2 \cdot 42 = 3 \cdot 28 = 4 \cdot 21 = 6 \cdot 14 = 7 \cdot 12$
$|f(-4)| = 71$ prime
$|f(-3)| = 56 = 2 \cdot 28 = 4 \cdot 14 = 7 \cdot 8$
$|f(-2)| = 39 = 3 \cdot 13$
$|f(-1)| = 20 = 2 \cdot 10 = 4 \cdot 5$

We have possibly systoles of degree 1,2,3,4 (two isometry classes), 7 for $C(22)$. Since $4 \cdot 4 + 2 < 22$, it follows by Proposition 2 that there are systoles of degree 1,2,3,4.

There are also systoles of degree 7 since

$$x^2 - 22xy + y^2 = 7D$$

has no integer solution for $|D| < 7$ (compare Lemma 5).

It follows that $C(22)$ has six different isometry classes of systoles. In contrast to the exaples (a) and (b), this is an example with many isometry classes with respect to N.

In view of Proposition 2, we can expect that there exist integers N such that $C(N)$ has systoles of degree $1, 2, 3, \ldots, m$ with

$$\sqrt{N-2} > m \geq -1 + \sqrt{N-2}.$$

Since $dim(T(C(N)))$ grows with N^3, I conjecture

Conjecture *There are infinitely many different integers N_i such that $C(N_i)$ has more than $(dim(T(C(N_i))))^{7/6}$ different systoles.*

d) I finally calculate the example $C_5(2)$. This is a small surface (genus 1 with 12 cusps) which already has three different isometry classes of systoles, compare Fig. 3.

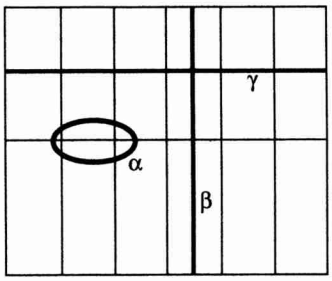

Fig. 3. The surface $C_A(N)$ drawn as a Euclidean torus where opposite sides must be identified. The vertices of the quadrilaterals are however cusps. The systoles of type α have degree 1, those of type β have degree 2 and those of type γ have degree 4. We can also see that a bigger degree means a bigger "distance" from the next cusp of $\mathscr{V}$ (which here contains six cusps)

I give the possible factorizations $|f(a)| = bc$ with $-5 \leq a < 0$.
$|f(-5)| = 76 = 2 \cdot 38 = 4 \cdot 19$
$|f(-4)| = 41$
$|f(-3)| = 16 = 2 \cdot 8 = 4 \cdot 4$
$|f(-2)| = 1$
$|f(-1)| = 4 = 2 \cdot 2$

By Proposition 2, $C_5(2)$ has systoles of degree 1 and 2. The surface also has systoles of degree 4 since, for $a = -3, b = -4, c = 4$, the equation

$$cx^2 - (2a + N)Axy - bAy^2$$

gives

$$4x^2 + 20xy + 20y^2$$

which is a multiple of 4.

References

[1] Z. Arad; M. Herzog (editors). *Products of Conjugacy Classes in Groups.* Lecture Notes 1112, Springer Berlin Heidelberg New York Tokyo (1985).

[2] J. Conway; N. Sloane. *Sphere packings, lattices and groups.* Second ed. Springer Berlin Heidelberg New York Tokyo (1993).

[3] M. Huxley. *Conjugacy Classes in Congruence Subgroups.* in: *Automorphic forms and analytic number theory*, Proc. Conf., Montréal 1989, ed. R. Murty; Montréal Publications CRM (1990), 65-88.

[4] S. Katok. *Fuchsian Groups.* University of Chicago Press Chicago London (1992).

[5] R. Rankin. *Modular forms and functions.* Cambridge University Press London New York Melbourne (1977).

[6] P. Schmutz. *Riemann surfaces with shortest geodesic of maximal length.* Geometric and Functional Analysis GAFA **3** (1993), 564-631.

[7] P. Schmutz. *Congruence subgroups and maximal Riemann surfaces.* The Journal of Geometric Analysis **4** (1994), 207-218.

[8] B. Schoeneberg. *Elliptic modular Functions.* Springer Berlin Heidelberg New York (1974).

[9] G. Shimura. *Introduction of the arithmetic theory of automorphic functions.* Iwanami Shoten Publishers and Princeton University Press (1971).

[10] M.F. Vignéras. *Arithmétique des Algèbres de Quaternions.* Lecture Notes 800, Springer Berlin Heidelberg New York (1980).