

# A DIOPHANTINE PROPERTY OF THE FUCHSIAN GROUPS

JOSEPH LEHNER

1. **Introduction.** A central result in diophantine analysis is the following [4]:

For every irrational real number  $\alpha$  and every positive constant  $h \leq \sqrt{5}/2$  there exists an infinite sequence of reduced fractions  $p_i/q_i$  such that

$$(1) \quad \left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{2h q_i^2} \quad (i = 1, 2, 3, \dots).$$

The property obviously fails if  $\alpha$  is rational.

This result can be related to the theory of the (elliptic) modular group [3]. We sketch the proof for a smaller value of  $h$ . The fundamental regions of the modular group lie in the upper half-plane and have cusps or vertices at every real rational point. Thus the fractions  $p_i/q_i$  are the parabolic vertices of the modular group, while  $\alpha$  is a limit point of vertices which is not itself a vertex. To establish (1), take a vertical line  $L$  in the upper half-plane ending at  $\alpha$ . Then  $L$  cuts infinitely many fundamental regions. Select a point  $z_k = \alpha_k + iy_k$  lying on  $L$  in the region  $R_k$  ( $k = 1, 2, 3, \dots$ ); there is a unique modular substitution

$$zV_k = \frac{q'_k z - p'_k}{q_k z - p_k}$$

which carries  $R_k$  and therefore  $z_k$  into the standard fundamental region  $R_0$ :

$$(|z| \geq 1, |\Re z| \leq 1/2).$$

We have  $z'_k = z_k V_k = x'_k + iy'_k$  and  $y'_k = y_k/Q$ , where

$$Q = (q_k \alpha - p_k)^2 + q_k^2 y_k^2.$$

Now  $y'_k > \sqrt{3}/2$ , since this is true for every point in  $R_0$ ; equality is attained only for points with rational abscissae. Since the arithmetic mean is not less than the geometric, we have

$$(2/\sqrt{3}) y_k > Q \geq 2 |q_k y_k| |q_k \alpha - p_k|,$$

---

Received December 3, 1951.

*Pacific J. Math.* 2 (1952), 327-333

which is (1) with  $h = \sqrt{3}/2$ . This result was first obtained by Hermite [2]; he used algebraic methods.

The above proof depends only on the circumstance that there is a fundamental region of the modular group which is at a positive distance from the real axis. This suggests a generalization to Fuchsian groups whose fundamental regions have the same property. But the result can be proved for more general groups. We are not particularly interested in the best possible value of  $h$ , but only in the existence of a constant  $h$  depending only on the group and not on  $\alpha$ .

First, let us note that in a Fuchsian group with a finite number of generators and with real axis as principal circle, the set of parabolic points (which we shall assume includes the point  $\infty$ ) consists of real numbers, of the form  $p/q$ ,  $p$  real,  $q > 0$ . Moreover,  $p$  and  $q$  have distinguishable identities; that is, they cannot be replaced by  $\lambda p$ ,  $\lambda q$ . For the number of inequivalent parabolic vertices of the group is finite;  $p/q$  must be equivalent to one of them, say  $\infty$ . Then the group contains a substitution carrying  $p/q$  to  $\infty$ ; that is, the first but in general not the second of the substitutions

$$\begin{pmatrix} * & * \\ q & -p \end{pmatrix} \text{ and } \begin{pmatrix} * & * \\ \lambda q & -\lambda p \end{pmatrix},$$

belongs to the group. Thus the statement that (1) is satisfied by infinitely many of the parabolic points  $p_i/q_i$  of a Fuchsian group has a nontrivial content.

Our result is now as follows:

**THEOREM.** *Let  $G$  be a Fuchsian group, with real axis as principal circle, which is generated by a finite number of substitutions. Let  $P$ , the set of parabolic points of  $G$ , be an infinite set including the point  $\infty$ . Let  $\alpha \in \bar{P} - P$ . Then there exist  $p_i/q_i$  ( $i = 1, 2, \dots$ ) for which (1) is true, where  $p_i/q_i \in P$ , and  $h = h(G)$  is a geometrical constant depending only on the group  $G$ .*

That  $\infty$  is a parabolic point of  $G$  is no real restriction since the group can always be transformed by a linear transformation ( $G \rightarrow T^{-1}GT$ ) to secure this.

We intend to develop further arithmetic properties of the Fuchsian groups in future investigations. A generalization of the semi-regular continued fractions is indicated.

**2. Preliminaries.** In this section we gather together some known facts concerning the fundamental regions of Fuchsian groups which will be needed in §3. Reference may be made to Ford [1].

We shall find it convenient to transform  $G$  into  $\Gamma = S^{-1}GS$ , choosing  $S$  so that no substitution  $V$  of  $\Gamma$  has infinity as a fixed point, and so that the real axis and upper half-plane are mapped into the unit circle ( $Q$ ) plus its interior.

Then every substitution

$$V = \frac{\alpha z + \beta}{\gamma z + \delta}$$

has  $\gamma \neq 0$  and possesses the isometric circle  $|\gamma z + \delta| = 1$ , which is orthogonal to  $Q$ . Furthermore, in any infinite sequence of isometric circles, the radii ( $= \gamma_n^{-1}$ ) tend to zero.

The fundamental region  $R_0$  of  $\Gamma$  is that part of the interior of  $Q$  which is exterior to all isometric circles; it is a simply connected region, bounded by arcs of isometric circles, which are called sides. Two sides intersect if at all in a single point (vertex) which may lie in the interior of  $Q$  or on  $Q$ ; in the latter case the sides must be tangent. The boundary of  $R_0$  on  $Q$  consists entirely of vertices if  $\Gamma$  is a Fuchsian group of the first kind; in a group of the second kind, it contains arcs of  $Q$ ; it may also contain vertices. These arcs are not sides of  $R_0$ ; they will be called bounding arcs. A side which, together with its endpoints, lies entirely inside  $Q$  is called an open side.

The transformations  $V_i$  of  $\Gamma$  map  $R_0$  into fundamental regions  $R_i$ , which in their entirety, fill the interior of  $Q$  completely and without overlapping, and cluster in infinite number about each parabolic vertex.

The sides of  $R_0$  are arranged in conjugate pairs  $(l_j, l_j')$ ; that is, there is a substitution  $T_j$  of  $\Gamma$  carrying  $l_j$  into  $l_j'$ . (If a side is followed immediately by its conjugate, the two sides are part of the same isometric circle.) Starting with any particular vertex in  $R_0$ , we label the sides and bounding arcs  $1, 2, 3, \dots$ , in counterclockwise order; as the conjugate of a side appears, it is labelled with the corresponding primed integer. (The bounding arcs are not considered to have conjugates.) As an example, the usual fundamental region for the modular group would be labelled  $1, 2, 2', 1'$ , if we start from the vertex corresponding to infinity in the upper half-plane.

Since each region  $R_i$  is a directly conformal image of  $R_0$ , the sides are described in the same order in both. The side of  $R_i$  which is the image of the side  $k$  in  $R_0$  is written  $\bar{k}$ . When two regions abut, the common side bears two labels, one for each region.

Suppose two regions  $R_i, R_j$  abut along a side  $\bar{l}$  in  $R_i$ . The substitution carrying  $R_i$  into  $R_j$  carries some side, evidently  $\bar{l}$ , into  $\bar{l}'$ . Therefore, the side of  $R_j$  common to  $R_i$ , being the image of  $\bar{l}$  in  $R_i$ , is labelled  $\bar{l}$  in  $R_j$  and, as we have seen, is labelled  $\bar{l}'$  in  $R_i$ . When two regions abut, then, the common side bears labels in the two regions which are conjugate to each other.

We are now able to define a quantity  $\eta = \eta(\Gamma)$  which in §4 will be related to  $h(G)$  of (1). If  $l$  is any side of  $R_0$ , let  $d_l$  be the maximum of the distances

of points of  $l$  from  $Q$ . If  $l$  is a bounding arc, construct the unique circle orthogonal to  $Q$  which passes through the endpoints of  $l$ ; then  $d_l$  is the largest distance from  $Q$  of points of the arc of this circle lying in  $Q$ . Now we define

$$(2) \quad \eta(\Gamma) = \min_l d_l,$$

where  $l$  runs over the (finite number) of sides and bounding arcs of  $R_0$ . Obviously

$$(3) \quad \eta(\Gamma) > 0.$$

**3. Lemma.** Denote by  $P_1$  the set of parabolic vertices of  $\Gamma$ , and let  $\beta \in \overline{P_1} - P_1$ ;  $\beta$ , and therefore  $\beta$ , lies on  $Q$ . Denote by  $\pi$  the image of  $\infty$  on  $Q$  under the transformation  $S$  (§2). Let  $\lambda$  be the unique orthogonal arc connecting  $\pi$  and  $\beta$ . Since  $\beta$  is not in  $P_1$ ,  $\lambda$  crosses infinitely many regions, say  $R_1, R_2, \dots$ , in that order. Let  $\lambda_i$  be the closed arc of  $\lambda$  lying in  $R_i$ . The substitution  $V_i^{-1}$  maps  $R_i$  on  $R_0$  and  $\lambda_i$  on an arc  $\lambda_i' = \lambda_i V_i^{-1}$  lying in  $R_0$ . Our object is to prove the following:

**LEMMA.** *For each  $\beta$  there exist infinitely many values of  $j$ , and corresponding points  $t_j$  on  $\lambda_j$  whose images  $t_j'$  on  $\lambda_j'$  are at a distance from  $Q$  greater than  $\eta(\Gamma)$ . Further,  $t_j \rightarrow \beta$ .*

To this end let us study the sequence of sides of the fundamental regions crossed in turn as  $\lambda$  is traversed from  $\pi$  to  $\beta$ . We may just as well consider the maps of these sides in  $R_0$  and thus write the sequence as

$$k_1; k_1', k_2; k_2', k_3; \dots$$

(It is understood that all letters appearing stand for either unprimed or primed integers, and  $(n')' = n$ .) Since the first side in each pair is merely the conjugate of the last side in the preceding pair, we may abbreviate the above to

$$(4) \quad k_1, k_2, k_3, \dots,$$

where only the *last* side crossed in each region is written down. This sequence, which is uniquely determined by  $\beta$ , will be denoted by  $(\beta)$ .

It is clear that  $(\beta)$  must contain some pair  $(k, l)$  infinitely often, for  $R_0$  has only a finite number of sides and arcs. The appearance of  $k$  in the  $(j-1)$ th place of  $(\beta)$  followed by  $l$  means that, in  $R_j$ ,  $\lambda_j$  starts from the side  $\overline{k'}$  and ends in the side  $\overline{l}$ . Then  $\lambda_j'$  starts from the side  $k'$  of  $R_0$  and ends in the side  $l$  of  $R_0$  and is orthogonal to  $Q$ .

Suppose first that  $k'$  and  $l$  are not consecutive sides of  $R_0$  in the labelling already adopted, so that there is at least one side or bounding arc  $m$  following

$k'$  and preceding  $l$ . Then  $\lambda'_j$ , being orthogonal to  $Q$  and cutting only  $k'$  and  $l$ , must lie between  $m$  and the center of  $Q$ . There is a point  $t'_j$  on  $\lambda'_j$  whose distance from  $Q$  exceeds  $d_m$ ; and hence exceeds  $\eta(\Gamma)$ . This is obvious if  $m$  is not a bounding arc. Otherwise, the circle which determines  $d_m$  lies completely interior to  $\lambda'_j$ . Hence, in all cases, the image of  $t'_j$  is a point  $t_j$  in  $\lambda_j$  with the desired properties. Since  $j$  assumes infinitely many values, the lemma is proved under the above mentioned supposition.

According to this result, the lemma may be established by demonstrating the existence of a pair  $(x, y)$  occurring indefinitely often in the sequence  $(\beta)$  such that  $x', y$  are not consecutive sides of  $R_0$ . This we proceed to do.

We divide the discussion into two cases:

A.  $R_0$  has all vertices on  $Q$ . Let  $(k, x)$  be an infinitely recurring pair in  $(\beta)$ . If there is an  $x$  such that  $k', x$  are not consecutive, apply the previous result. Otherwise, from a certain point on in  $(\beta)$ ,  $k$  occurs followed always by  $l$  where  $k', l$  are consecutive. Now consider infinitely recurring triples  $(k, l, x)$ . If an  $x$  exists for which  $l', x$  are not consecutive, there is nothing further to prove. If not, all late triples in  $(\beta)$  involving  $k, l$  are  $(k, l, m)$ , where  $l', m$  are consecutive.

In the continuation of this process, two possible situations can arise. We may find a block  $(k, l, \dots, r, s)$  occurring infinitely often in  $(\beta)$  with  $r', s$  not consecutive. If this does not happen, then we arrive at an infinitely recurring block  $(k, l, \dots, u, v)$  with  $k', l$  consecutive,  $\dots, u', v$  consecutive, and  $v', k$  consecutive. This block may contain all or only some of the vertices of  $R_0$ . But now these blocks must occur in succession with no entries in between in  $(\beta)$ . For if we assume  $z \neq k$  follows  $v$  infinitely often in  $(\beta)$ , we have the recurring pair  $(v, z)$ , and  $(v', z)$  are not consecutive since  $v', k$  are.

The sequence  $(\beta)$  now looks like this:

$$\dots a_1, a_2, \dots, a_{N-1}, B, B, B, \dots,$$

where  $B$  is the block  $(k, l, \dots, u, v)$ . The sides  $\bar{k}', \bar{l}$  of the first block  $B$  lie in  $R_{N+1}$ . Let the vertex at the intersection of these sides be  $K$ . Then  $K$  lies on  $Q$ , and  $\bar{k}'$  and  $\bar{l}$  issue from  $K$ . The next side cut by  $\lambda$  is  $\bar{m}$ . Since  $l'$  and  $m$  are consecutive in  $R_0$ , it follows that  $\bar{l}'$  and  $\bar{m}$  issue from  $K$ . Continuing in this way, we see that from a certain point on all the sides cut by  $\lambda$  issue from  $K$ . Let  $\bar{k}$  be one of these sides;  $\bar{k}$  is an arc of an isometric circle which cuts  $Q$  in two points,  $K$  and another point  $K_1$ ; and  $\beta$  lies in the interior of the arc  $KK_1$ . In fact,  $\beta$  lies inside all such arcs formed from the sides of all regions cut by  $\lambda$ . Since the radii of the isometric circles tend to zero, the distance from  $\beta$  to  $K$  is arbitrarily

small. This contradicts the hypothesis that  $\beta$  is not in  $P_1$ .

B.  $R_0$  has some vertices not on  $Q$ . Let  $k', l$  be sides of  $R_0$  meeting at a vertex  $K$  which lies on  $Q$ . Suppose  $(k', l)$  recurs indefinitely in  $(\beta)$ . We continue the argument as in case A. The side  $l$  is not open since it meets  $k'$  at  $K$ . Hence,  $l'$  is not open. The side  $m$  consecutive to  $l'$  is thus not open. Therefore, the block  $(k, l, m, \dots, u, v)$  consists entirely of sides which are not open. Then we are in case A.

If  $(k', l)$  does not occur infinitely often for any nonopen  $k'$ , then all pairs  $(x, y)$  which do recur indefinitely consist of open sides. Then the argument is similar to that of case A except that the vertex  $K$  lies in the interior of  $Q$ . Infinitely many sides cut by  $\lambda$  issue from  $K$ . This is known to be an impossibility: since  $K$  is a vertex in the interior of  $Q$ , only a finite number of sides of fundamental regions can end at  $K$ . Hence the possibility envisaged cannot actually occur.

This completes the proof of the lemma.

**4. Proof of the theorem.** Let  $Q^*$  be an interior circle concentric with  $Q$  and at a distance  $\eta(\Gamma)$  from  $Q$ . The content of the lemma is that on the arc connecting the fixed vertex  $\pi$  to any point  $\beta \in \bar{P}_1 - P_1$  there exists a sequence of points  $t_1, t_2, \dots \rightarrow \beta$  whose transforms  $t_1', t_2', \dots$  in  $R_0$  lie inside  $Q^*$ .

Recalling that  $\Gamma = S^{-1}GS$ , we map  $Q$  back onto the real axis  $E$  by means of  $S$ . Then the interior of  $Q$  is mapped onto the upper half-plane  $H$  and  $\pi$  is carried to infinity,  $P_1$  to  $P$ , and  $\beta \in \bar{P}_1 - P_1$  to  $\alpha \in \bar{P} - P$ . The sides of  $R_0$  in  $Q$  are mapped into sides of  $R_0'$  in  $H$ , some of which may extend to infinity. The bounding arcs become intervals of  $E$  of finite length. The image of  $\lambda$  is a vertical line  $L$  ending at  $\alpha$ , and  $Q^*$  is carried into a circle  $E^*$  whose lowest point is at a distance  $h(G)$  above  $E$ ; we use this to define  $h(G)$ .

The sequence  $t_n \rightarrow \beta$  is mapped into a sequence  $z_n \rightarrow \alpha$ ,  $z_n$  on  $L$ . The lemma then states that the sequence  $z_n$  has transforms  $z_n'$  in  $R_0$  which lie inside  $E^*$ . The distance of  $z_n'$  from  $E$  is therefore greater than  $h$ ; that is,

$$(5) \quad \Im z_n' > h \quad (n = 1, 2, 3, \dots).$$

Let  $\begin{pmatrix} * & * \\ q_n & -q_n \end{pmatrix}$  be the substitution of  $G$  carrying  $R_n$  into  $R_0$ ; then  $p_n/q_n$  is carried to infinity, and  $p_n/q_n$  is thus a parabolic vertex.

Now applying the argument in §1, we see that  $p_i/q_i$  ( $i = 1, 2, 3, \dots$ ) satisfies (1) with  $h = h(G)$ .

A geometrical definition of  $h$  can be given. For each side  $l$  of  $R_0$ , set  $d_l$  ( $\leq +\infty$ ) equal to the maximum height of points on  $l$ . If  $l$  is a bounding arc, set  $d_l$  equal to half the length of  $l$ . Then

$$(6) \quad h(G) = \min_l d_l > 0,$$

where  $l$  varies over the sides and bounding arcs of  $R_0'$ .

#### REFERENCES

1. L. R. Ford, *Automorphic Functions*, McGraw-Hill, New York, 1929.
2. C. Hermite, *Sur l'introduction des variables continues dans la théorie des nombres*, J. Reine Angew. Math. **41** (1851), 191-216.
3. G. Humbert, *Sur la méthode d'approximation d'Hermite*, J. Math. Pures Appl. (7) **2** (1916), 79-103.
4. A. Hurwitz, *Über die Angenäherte Darstellung der Irrationalzahlen durch rationale Brüche*, Math. Ann. **39** (1891), 279-285.

UNIVERSITY OF PENNSYLVANIA

