Order Number 9108105

Fundamental domains of modular subgroups using isometric circles

Fung, Terry Y., Ph.D.

City University of New York, 1990

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

FUNDAMENTAL DOMAINS OF MODULAR SUBGROUPS USING ISOMETRIC CIRCLES

by

TERRY Y. FUNG

A dissertation submitted to the Graduate Faculty in
Mathematics in partial fulfillment of the requirements for the
Degree of Doctor of Philosophy
The City University of New York

1990

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

20 July 1990
Date

Harvey Cohn
Chair of Examining Committee

20 July 1990
Date

Rachel Silvestri
Executive Officer

Adam Kanigel

Supervisory Committee

The City University of New York

Abstract

Fundamental Domains of Modular Subgroups

Using Isometric Circles

by

Terry Y. Fung

Advisor: Professor Harvey Cohn

Let Γ denote the inhomogeneous modular group acting on the upper half plane $\mathcal{H}$ in this way :

$$z \longmapsto \frac{az+b}{cz+d},\ ad-bc=1,\ a,b,c,d \in \mathcal{Z}$$

Sometimes we denote the element of Γ by its matrix form $A = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

We consider the subgroup of Γ such as

$$\Gamma^{\circ}(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| b \equiv 0 \pmod{N} \right\}$$

We construct the fundamental domain for $\Gamma^{\circ}(N)$ using isometric circles in a manner based upon the divisibility of prime factor(s) of N. The use of isometric circles was Poincaré's original constructional and existential method for fundamental domains.

In this paper, we construct a fundamental domain of $\Gamma^{\circ}(N)$ for N which has at most four distinct prime factors. The fixed circle of $\Gamma^{\circ}(N)$ is the real axis and the cusps are zero and the multiples of the prime factors. We construct it by using isometric circles with the relation $(z-\frac{L}{Q})(z'-\frac{M}{Q}) = -\frac{1}{Q^2}$ provided that $LM \equiv -1 \pmod{QN}$ where $\frac{L}{Q}$, $\frac{M}{Q}$ are centers of circles with radius $r = \frac{1}{Q}$. The idea of the method is to find the matching circles by checking $LM \equiv -1 \pmod{QN}$. We found that for N with one prime factor, the isometric circles will have radius $r = 1$. If N has two distinct prime factors, then the isometric circles have radius $r \geq \frac{1}{2}$. If N has three distinct prime factors then the isometric circles have radius $r \geq \frac{1}{3}$ if N is odd, and $r \geq \frac{1}{4}$ if N is even. If N has four distinct prime factors, the isometric circles will have radius $r \geq \frac{1}{4}$ provided all the prime factors are greater than three, but if the prime factors are less than or equal to three, various special cases will occur leading to circles of radius $\frac{1}{7}$ as we shall demonstrate.

This work generalizes a result of Cohn [3] for two prime factors. The method will be shown to be applicable to any number of prime numbers.

ACKNOWLEDGEMENTS

First of all, I would like to thank my advisor Professor Cohn for his patience, encouragement and guidance. Without his assistance I would not be able to achieve this goal. In the past six years, many people helped me with different difficult crises. I would like to thank Elaine for her encouragement, and Dal, Debbie, Frank, Ron for their cheerful discussions. I would like to thank my friend Ming for her professional drawing. Also, I would like to thank my family for their support which makes this mission possible. Finally, my special thanks to Chi Ming who typed this manuscript and I appreciate his love and care through the years.

Contents

List of Tables

List of Figures

Chapter 1

Discontinuous Groups and Fundamental Domains

Let Ω be the group of all conformal homeomorphisms of the Riemann sphere C^*. Each element of Ω is a linear transformation

$$\Omega : z' = T(z) = \frac{az+b}{cz+d},\ ad-bc=1 \tag{1}$$

where a, b, c, d are complex numbers. Sometimes we use the matrix form $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to denote (1) and the matrices T and $-T$ give rise to the same transformation.

Let R denote the field of real numbers, C denote the field of complex numbers and C^* denote the Riemann sphere. Recall that (1)

$$T(z) = \frac{az+b}{cz+d},\ ad-bc=1$$

where $a, b, c, d \in C$. Equation (1) defines $T(z)$ for all z in the extended complex number system $C^* = C \cup \{\infty\}$ except for $z = -\frac{d}{c}$ and $z = \infty$. We extend the definition of T to all of C^* by defining

$$T(-\frac{d}{c}) = \infty,\ T(\infty) = \frac{a}{c}$$

with the usual convention that $z/0 = \infty$ if $z \neq 0$. First note that

$$T(w) - T(z) = \frac{(ad-bc)(w-z)}{(cw+d)(cz+d)} \tag{2}$$

which shows that T is constant if $ad - bc = 0$. To avoid this degenerate case we assume that $ad - bc \neq 0$. Further, T remains unchanged if we multiply all the coefficients a, b, c, d by the same nonzero constant. Therefore there is no loss of generality in assuming that $ad - bc = 1$ in (1). T is analytic everywhere on C^* except for a simple pole at $z = -\frac{d}{c}$.

Equation (1) shows that every linear transformation is one-to-one on C^*. Solving (1) for z in terms of $T(z)$, we have

$$z = \frac{dT(z) - b}{-cT(z) + a}$$

so T maps C^* onto C^*. This also shows that the inverse function T^{-1} is a linear transformation. We find the derivative of T, which is

$$T'(z) = \frac{ad - bc}{(cz + d)^2}$$

$T'(z) \neq 0$ except at the pole $z = -\frac{d}{c}$, thus T is conformal.

Linear transformations map circles onto circles(with straight lines being considered as circles with infinite radii).

For each linear transformation (1) we associate the 2×2 matrix $A = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $\det A = ad - bc = 1$. There is a one-to-one correspondence between linear transformations and matrices. It is easy to see that the linear transformations with $ad - bc = 1$ form a group. The operation is compostion $T \circ S$ where $(T \circ S)(z) = T(S(z))$. The identity transformation is $I(z) = \frac{1z+0}{0z+1}$. Therefore, the corresponding matrices will form a group under the operation of matrix product. The inverse elements for matrices and linear transformations are respectively $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ and $T^{-1} = \frac{dz-b}{-cz+a}$.

We now investigate the correspondence between the group of linear trans-

formations $\mathcal{L}$ and the group of matrices $\mathcal{A}$.

$$\varphi : \mathcal{A} \longrightarrow \bar{A},\ \varphi(A) = \frac{az+b}{cz+d} \tag{3}$$

where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $\det A = 1$. φ is a homomorphism with kernel $\{\pm I\}$. By the first isomorphism theorem $\mathcal{A}/\{\pm I\} \cong \bar{A}$.

Let Γ be a subgroup of Ω.

Definition 1 *The point α is called a limit point of Γ provided there is a point $z \in C^*$ and an infinite sequence $\{T_n\}$ of different elements of Γ such that $T_n(z) \longrightarrow \alpha$*

Definition 2 *If α is not a limit point, it is an ordinary point of Γ.*

Definition 3 *Γ is said to be discontinuous at α if α is an ordinary point of Γ. Γ is called a discontinuous group if it is discontinuous somewhere, i.e., Γ has at least one ordinary point.*

Definition 4 *It can be shown that the set of ordinary point of Γ is an open set which can be partitioned into countably many disjoint regions D_i. The D_i are called regions of discontinuity of Γ.*

Definition 5 *If Γ is a discontinuous group with $\{D_i, i = 1, 2, \cdots, n\}$, the regions of discontinuity of Γ. Γ is called a function group provided one of the regions D_j is mapped on itself by each element of Γ.*

Definition 6 *In a discontinuous function group, the region D_j is called a domain of existence of Γ.*

Definition 7 *A fixed circle(line) of a group is a circle(line) which is fixed by all element of the group.*

Definition 8 *A group is called principal circle group if each of its element preserves the interior of a fixed circle.*

Definition 9 *The fixed circle(or line) preserved by each element of the principal circle group is called the principal circle.*

Remark: Let $\mathcal{H}$ denote the upper half plane. In chapter 3 we shall limit ourselves to principal circle groups which leave the upper half plane $\mathcal{H}$ invariant, i.e., a, b, c, d are real and for which $\mathcal{H}$ is a region of discontinuity while the real axis is a principal circle.

There are at most 2 fixed points for the linear transformation (1), we can classify the linear transformation by the fixed points as follows:

Definition 10 *The transformation* $z' = \frac{az+b}{cz+d}$, *where* $ad - bc = 1$, *is of the type stated if and only if the following conditions on* $a + d$ *hold:*
Hyperbolic, if $a + d$ *is real and* $|a + d| > 2$.
Elliptic, if $a + d$ *is real and* $|a + d| < 2$.
Parabolic, if $a + d = \pm 2$.
Loxodromic, if $a + d$ *is complex.*

The major properties of these transformations can be found in Ford[4, p.18-23] (In the main result, loxodromic transformations do not occur).

Definition 11 *Two configurations (points, curves, regions, etc.) are said to be congruent with respect to a group if there is a transformation of the group other than the identical transformation which carries one configuration onto the other.*

Definition 12 *The fundamental domain of a principal circle group is a region R with the following properties:*

(i) Any point of $\mathcal{H}$ not in R is congruent to a point in R.

(ii) No two points interior to R are congruent.

(iii) Boundary points can be congruent only to other boundary points.

First notice that a fundamental domain of a group is not unique. There is a simple way to obtain a fundamental domain which involves the isometric circles of a group. We next define an isometric circle.

In an analytic transformation $z' = f(z)$, a lineal element dz connecting two points in an infinitesimal neighborhood of a point z is transformed into the lineal element dz' in a neighborhood of z'; hence, the length of the element is multiplied by $|f'(z)|$ and the element is rotated through an angle $\arg f'(z)$.

Consider dz and $|T'(z)| = |cz + d|^{-2}$ with regard to the transformation (1). An infinitesimal region is carried into a similar region with corresponding lengths multiplied by $|T'(z)|$; hence the area is multiplied by $|T'(z)|^2 = |cz + d|^{-4}$. We can see that lengths and areas are unaltered in magnitude if and only if $|cz + d| = 1$.

Definition 13 *The circle $I(T)$,*

$$I(T) : |cz + d| = 1, \ c \neq 0 \tag{4}$$

is called an isometric circle of the transformation (1)

Theorem 1 *Lengths and areas within the isometric circle are increased in magnitude and lengths and areas outside the isometric circle are decreased in magnitude, by the transformation (1).*

Proof. For the transformation $z' = T(z) = \frac{az+b}{cz+d}$, $ad - bc = 1$ the isometric circle is $I(T)$: $|cz + d| = 1$. When the transformation is applied, $|dz|$ is transformed into $|dz'| = |T'(z)dz| = |cz + d|^{-2}|dz|$. If z is within $I(T)$, that is, $|cz + d| < 1$ then $|T'(z)| = |cz + d|^{-2} > 1$, which is the region exterior to $I(T)$. If z is outside $I(T)$, i.e., $|cz + d| > 1$ then $|T'(z)| = |cz + d|^{-2} < 1$, which is the region interior to $I(T)$. A length or area within $I(T)$ is thus magnified by $|T'(z)| > 1$. A length or area outside $I(T)$ is diminished by $|T'(z)| < 1$. Q.E.D.

Theorem 2 *T maps $I(T)$ onto $I(T^{-1})$ and maps interior(exterior) of $I(T)$ into the exterior(interior) of $I(T^{-1})$.*

Proof. $z' = T(z) = \frac{az+b}{cz+d}$, $ad - bc = 1$. $I(T)$:$|cz + d| = 1$.
$T^{-1} = \frac{-dz+b}{cz-a}$, $I(T^{-1}) : |cz - a| = 1$.
If $z \in I(T)$, we have

$$|cz' - a|^{-2} = |cT(z) - a|^{-2} = |c\frac{az + b}{cz + d} - a|^{-2} = |\frac{1}{cz + d}|^{-2} = 1$$

hence, $T(z) \in I(T^{-1})$. Here "int" and "ext" are interior and exterior respectively.
If $z \in$int $I(T)$, then $|cz + d| < 1$ and so $|cT(z) - a|^{-2} > 1$, hence,
$T(z) \in$ext $I(T^{-1})$.
If $z \in$ext $I(T)$, then $|cz + d| > 1$ and so $|cT(z) - a|^{-2} < 1$, hence,
$T(z) \in$int $I(T^{-1})$. Q.E.D.

Note that a transformation carries its isometric circle into the isometric circle of the inverse transformation and gives the pairing of ext $|cz - a| = 1$ with int $|cz + d| = 1$. For each linear transformation of the group, there exists a corresponding isometric circle.

Theorem 3 *The region R consists of all the parts of the plane which is exterior to the isometric circles of all the transformations of the group and R constitutes a fundamental domain of the group.*

The complete proof can be found in Ford[4, p.44-45]. Theoretically, a fundamental domain can be obtained by the above method, but this is not always easy to do, especially when the group involved is large. Since a fundamental domain R is the exterior of all isometric circles of the group, it is clear that its boundary consists of circular arcs. We call the intersection point of two arcs a vertex of the fundamental domain. Let A_1 be a vertex. If either of the sides which meet in A_1 is carried into its congruent side, A_1 is carried into a vertex at the extremity of the latter arc. These congruent vertices may be carried into others, with the result that A_1 may be congruent to several of the vertices of R.

Definition 14 *A complete set of congruent vertices of a fundamental domain is called a cycle.*

There are two kinds of cycles, namely, parabolic cycles and ordinary cycles.

Definition 15 *If one of the points in the cycle is a limit point, we call the cycle parabolic.*

Remark: Consistent with earlier definitions "parabolic", "elliptic" refer to the nature of the vertex as a fixed point.

Definition 16 *If one of the points in the cycle is an ordinary point, we call the cycle ordinary. If one of the vertices of an ordinary cycle is a fixed point*

of a transformation, we call it an elliptic cycle. If none of the vertices is a fixed point, we call it an accidental cycle.

Theorem 4 *The sum of the angles at the vertices of an ordinary cycle of R is $\frac{2\pi}{l}$ if the cycle is elliptic of order l, and is 2π if the cycle is accidental. Conversely, if the angle sum at the vertices of an ordinary cycle of R is $\frac{2\pi}{l}$, the cycle is elliptic of order l when $l > 1$ and is accidental when $l = 1$.*

The complete proof of this theorem is quite long. For details, refer to Lehner[7, p.126]. We will sketch the proof by considering the following example. (see figure 1)

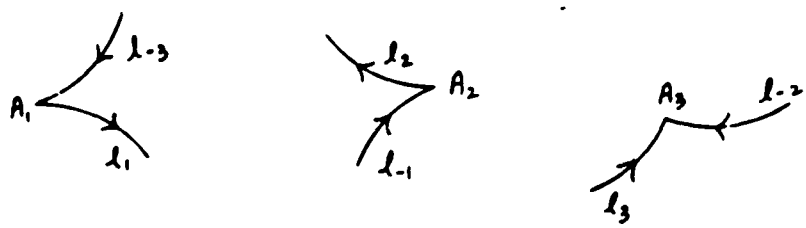

Figure 1: Ordinary cycle

Let A_1, A_2, A_3 constitute an ordinary cycle.

Let $T_1 : A_1 \longrightarrow A_2$ $\qquad T(l_1) = l_{-1}$

Let $T_2 : A_2 \longrightarrow A_3$ $\qquad T(l_2) = l_{-2}$

Let $T_3 : A_3 \longrightarrow A_1$ $\qquad T(l_3) = l_{-3}$

Let $E = T_3 \circ T_2 \circ T_1$, then E carries A_1 to itself. It may happen that E is the identical transformation. If not, E is an elliptic transformation since A_1 is a fixed point. For A_1 is a fixed point of E and the fixed points of hyperbolic or

loxodromic transformations lie within isometric circles and the fixed point of a parabolic transformation is a limit point of the group. Now, we can paste A_1, A_2 and A_3 together by applying E (see figure 2). The fact that E is elliptic of order l means $E^l = 1$. The sum of the angles at the vertices is $\frac{2\pi}{l}$. Applying E l times, the sum of the angles is 2π. On the other hand, we can consider accidental cycle as a special case of E, namely, $l = 1$. The sum of the angles is then 2π.

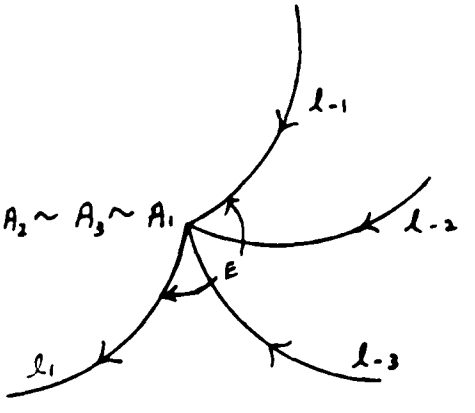

Figure 2: Pasting together the cycle

Chapter 2

Poincaré's Theorem

In 1880, a wide variety of groups could be constructed as free products, but no principal circle group with elliptic fixed points could be constructed by this method. Also, discontinuous groups could be defined as covering groups of Riemann surfaces, but these were groups without elliptic elements. So far, no information was obtained about the group presentation, namely, its generators or the coefficients of its matrix representation.

In 1882, Poincaré's [11] showed that the class of principal circle groups with finitely-sided fundamental domains is coextensive with the class of noneuclidean polygons satisfying certain conditions. Therefore, Poincaré's result is a characterization of the totality of principal circle groups that are associated with compact Riemann surfaces. We will state the theorem and sketch the proof. (We presuppose the elementary properties of Riemann surfaces since these properties do not arise directly. More details can be found in [9]).

Poincaré's Theorem

Let Q be a unit circle and U be the interior of Q. Let P_0 be a polygon bounded by a finite number of pairs of sides (S_i, S_i'), $i = 1, 2, \cdots, n$(arcs of circles orthogonal to Q). Let T_i be a linear transformation of Q mapping the outside of the circle determined by S_i on the inside of the circle determined

by S_i'. Let P_0 satisfies these conditions :

1) The boundary of P_0 consists of a finite number of pairs of sides (S_i, S_i'). There is a unique element $T_i \in \Gamma$ which maps S_i on S_i' and maps the exterior of the circle on which S_i lies on to the interior of the circle on which S_i' lies.

2) The sum of the angles at the vertices of an elliptic cycle of order l is $\frac{2\pi}{l}$.

3) The sum of the angles at the vertices of an accidental cycle lying in $\mathcal{U}$ is 2π.

4) P_0 can be chosen so that its boundary meets Q at most at a finite number of parabolic vertices.

Then the group Γ generated by $\{T_i, i = 1, 2, \cdots, n\}$ is a discontinuous function group with domain of existence $\mathcal{U}$ and P_0 is a fundamental domain for Γ.

We want to show that P_0 is a fundamental domain for Γ. The existence of a fundamental domain with inner point(s) will show that Γ is discontinuous. We start with a finitely-sided polygon. Conditions 2) to 4) guarantee that each vertex of P_0 belongs to a cycle. If two points are in the same cycle, there exists a transformation that maps one point to the other. So we can consider a point A_1 in a cycle as a representative of the cycle because we can map the other congruent points to A_1.

Let T_i be the transformation that maps A_i to A_1. Let P_i be the image of the sector of P_0 at vertex A_i under T_i (see figure 3). In order to show P_0 is a fundamental domain for Γ, it suffices to show

a. P_i, P_j are either disjoint or identical, where P_i, P_j are stated as above.

b. All P_i's cover $\mathcal{U}$.

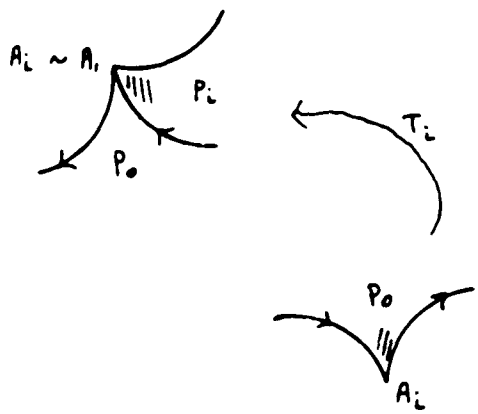

Figure 3: Illustration for Poincaré's Theorem: pasting process

We pick a vertex A_1 which lies on the side S_1. Applying the above process, we paste together all points congruent to A_1 and the images of the sectors will be around A_1. (see figure 4) We carry the process to the endpoint A_2 of S_1. We complete this process until we return to A_1.

Note that if A_1 is congruent to A_i, the P_i's around A_1 are the same as A_i (different in the order). After we have completed the process, we have a layer of P_i's around P_o. All P_i's will not intersect P_o since a transformation will map the outside of the circle determined by S_i on the inside of the circle determined by S_i'. Since P_o is outside of all circle, the P_i's must be in some circles, hence they do not intersect with P_o. Next we need to show that two polygons P_i, P_j are either disjoint or identical. Suppose P_i, P_j overlap, there exists at least a point α_k belonging to two different cycles. There exist two different transformations carrying two points to α_k, but condition 1) states that T_i is unique. Thus two transformations must be the same. Hence, P_i, P_j do not overlap. Next we pick an endpoint of a side of a polygon in the first

layer. Apply the same process to that endpoint to make the second layer of polygons . By the same argument, these polygons in the second layer are either disjoint or identical.

We keep making different layer of polygons and each layer is disjoint. Eventually, all polygons P_i's will cover $\mathcal{U}$, this is the most general construction for such a group Γ, further details see Lehner. [7]

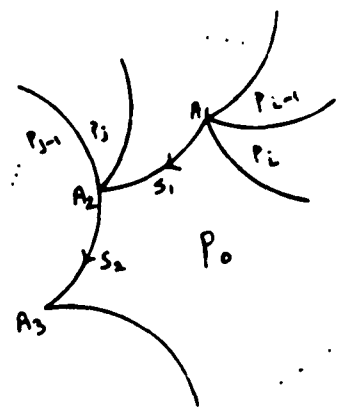

Figure 4: Illustration for Poincaré's Thorerm: completion of pasting process

Chapter 3

The Modular Group

We consider a historically significant subgroup Γ of Ω in equation (1) for which the region of discontinuity is $\mathcal{H}$ the upper half plane and the real axis $\Re$ is the principal circle.

Definition 17 *The group of* 2×2 *matrices with integer coefficients and determinant one is called the homogeneous modular group* Γ.

$$\Gamma = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| a, b, c, d \in Z,\ ad - bc = 1 \right\}$$

Definition 18 *The homomorphism* φ *in (3) leads to the inhomogeneous modular group* $\bar{\Gamma}$.

$$\bar{\Gamma} = \{\bar{A} | A \in \Gamma\}$$

where $\bar{A} : z \rightarrow \frac{az+b}{cz+d}$ *if* $A = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma$.

As maps they preserve the upper half plane $\mathcal{H}$, the real axis $\Re$ and the set of rational numbers Q. The relation between Γ and $\bar{\Gamma}$ is given by the isomorphism

$$\Gamma / \{\pm I\} \cong \bar{\Gamma}.$$

Next, we show some properties and theorems about homogeneous and inhomogeneous modular group. (Proofs will be only sketched or refered to standard textbooks, [4][7][13].)

Theorem 5 *The homogeneous modular group is generated by the elements* $S = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ *of order 3 and* $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *of order 2, where* $S^3 = T^2 = -1$.

Theorem 6 *The set* $\mathcal{D} = \{z | z \in \mathcal{H}, |Rez| < \frac{1}{2}, |z| > 1\} \cup \{i\infty\} \cup \{z | Rez = -\frac{1}{2}, |z| \geq 1\} \cup \{z | |z| = 1, -\frac{1}{2} \leq Rez \leq 0\}$ *is a fundamental domain of* Γ *for* $\mathcal{H}^*$ *where* $\mathcal{H}^*$ *denotes the extended upper half plane* $\mathcal{H} \cup \{i\infty\}$

The properties for homogeneous and inhomogeneous modular groups will be carried over to its subgroups. Later on we restrict ourselves to a special class of subgroups, the congruence subgroups. Let Γ_1 be a subgroup of the homogeneous modular group. The map $\varphi : A \longmapsto \bar{A}$ where

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \ \bar{A} = \frac{az + b}{cz + d}$$

induces a homomorphism of Γ_1 onto a subgroup $\bar{\Gamma}_1 = \varphi(\Gamma_1)$ of the inhomogeneous modular group $\bar{\Gamma}$. This homomorphism has the kernel $\{\pm I\}$ if $-I \in \Gamma_1$, and is an isomorphism if $-I \notin \Gamma_1$. The concepts of congruence and fundamental domain will hold for sugbroups as well. Instead of congruence under $\bar{\Gamma}$, we have congruence under Γ_1. The same definition for fundamental domain holds for $\bar{\Gamma}_1$.

Z is the ring of integers. For a natural number N, Z_N denotes the ring of all residue classes modulo N. Γ is isomorphic to the special linear group $SL(2, Z)$. We use the symbol Γ_N for the group $SL(2, Z_N)$.

Definition 19 *Let* Z_N *denote the ring of all residue classes modulo* N. $\sigma : Z \longrightarrow Z_N$ *induces a homomorphism by*

$$\sigma \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \sigma(a) & \sigma(b) \\ \sigma(c) & \sigma(d) \end{pmatrix}$$

The kernel

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

is called the principal congruence subgroup of Γ

Theorem 7 *The image of* Γ *under the homomorphism* σ *is isomorphic to the group* $\Gamma_N = SL(2, Z_N)$.

$$\sigma(\Gamma) \cong \Gamma/\Gamma(N) \cong \Gamma_N$$

We now determine the order $|\Gamma_N| = \mu(N)$. Equivalently, this is the number of noncongruent solutions of $ad - bc \equiv 1 \pmod{N}$. By the Chinese Remainder Theorem

$$\mu(N_1 N_2) = \mu(N_1)\mu(N_2)$$

for $(N_1, N_2) = 1$. Consequently, we may restrict ourselves to powers of a prime $N = p^\alpha$.

1. There are $\varphi(p^\alpha)$ residues classes $a \bmod p^\alpha$ with $a \not\equiv 0 \bmod p$ where $\varphi(n)$ denotes the Euler function, the number of residue classes mod n which are relatively prime to n. To each of these classes for a, the number b and c may be chosen arbitrarily modulo p^α. Then $d \bmod p^\alpha$ is uniquely determined. In this case there are altogether $\varphi(p^\alpha)p^{2\alpha}$ solutions.

2. There are $p^{\alpha-1}$ residue classes $a \bmod p^\alpha$ with $a \equiv 0 \bmod p$, and corresponding to each of these $d \bmod p^\alpha$ may be chosen arbitrarily. Since in this case $(p, b, c) = 1$, there are $\varphi(p^\alpha)$ possibilities for $b \bmod p^\alpha$ and $c \bmod p^\alpha$ are again uniquely determined. Hence there are $\varphi(p^\alpha)p^{2\alpha-1}$ additional solutions.

Adding these together, we obtain

$$\begin{aligned}\mu(p^\alpha) &= \varphi(p^\alpha)p^{2\alpha} + \varphi(p^\alpha)p^{2\alpha-1} \\ &= \varphi(p^\alpha)p^{2\alpha}(1+\frac{1}{p}) \\ &= p^{3\alpha}(1-\frac{1}{p^2})\end{aligned} \tag{5}$$

Hence for arbitrary N we arrive at the result:

$$|\Gamma_N| = \mu(N) = N^3 \prod_{p|N}(1-\frac{1}{p^2}) \tag{6}$$

where the product runs over prime divisors of N.

It is customary to give specific notations to the three congruence groups:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma | c \equiv 0 \pmod{N} \right\}$$

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma | b \equiv 0 \pmod{N} \right\}$$

$$\Gamma_0^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma | b \equiv c \equiv 0 \pmod{N} \right\}$$

Mainly we consider $\Gamma^0(N)$. The index of $\Gamma^0(N)$ in Γ is computed as follows:

We observe that the index

$$(\Gamma^0(N) : \Gamma(N)) = N\varphi(N)$$

because if $b \equiv 0 \pmod{N}$, the congruence

$$ad - bc \equiv 1 \pmod{N}$$

has exactly $N\varphi(N)$ noncongruent solutions. With the order of $|\Gamma_N| = \mu(N)$ as in equation (6) we obtain the index of $\Gamma^\circ(N)$:

$$(\Gamma : \Gamma^\circ(N)) = \frac{\mu(N)}{N\varphi(N)} = N \prod_{p|N} (1 + \frac{1}{p}) \tag{7}$$

A subgroup $\bar{\Gamma}_1$ of $\bar{\Gamma}$ is called an inhomogeneous congruence group if $\bar{\Gamma}_1$ is the homomorphic image of a homogeneous congruence group Γ_1 under the map

$$\varphi : A \longmapsto \bar{A}, \ A \in \Gamma_1$$

It contains the inhomogeneous principal congruence group $\Gamma(N_1)$. Now we assume that $\bar{\Gamma}_1$ is the homomorphic image under φ of the group Γ_1 which contains $-I$. We shall omit the bar in the designation of the inhomogeneous group and make no distinction between homogeneous and inhomogeneous modular groups and call them modular groups.

Chapter 4

Construction of the Fundamental Domain

Historical References

The theory of discontinuous groups and automorphic functions was first developed in early 1880. Poincaré introduced a construction of fundamental domains of discontinuous group using isometric circles. This is very good from the existence viewpoint but has been generally discarded particularly with modular subgroups because there are parabolic cycles which involve several different points of the z-plane belonging to the same parabolic cusp.

After his initial work, number theorists like Fricke and Klein were able to count the parabolic cusps and to find a fundamental domain which collects these cycles as one cusp. He presented a formula to do it, the idea is to construct out of certain tiles of the well-known modular tessellation. [5, p.349]. Even with the formula, this constuction is very inconvenient geometrically.

Since then, there is no major result to cite, except a few explicit examples. There is an explicit fundamental domain for $\Gamma^{\circ}(p)$ where p is a prime, [13, p.88] and for $\Gamma_{\circ}(p)$, [14, p.377] Nielsen constructed a fundamental domain for the subgroup of the triangle group $\Delta_{2,3,p}$ which uniformizes the surface $\Gamma(p)/H$ compactified by adjoining its cusps. This is done for $p > 5$ for which 2 is a primitive root , [10]. Cohn presented a simple construction of fundamental domain for $\Gamma^{\circ}(N)$ where N has at most two prime factors, [3, p.242].

Kulkarni attacked this problem in a new direction. He used partly geometric and partly arithmetic method to construct fundamental domains for $\Gamma(N)$ and $\Gamma_o(N)$ so that the side-pairing transformations form an independent set of generators [6]. This method applied to all subgroups of finite index in the modular group. It is a very big improvement on finding fundamental domains for $\Gamma(N)$ and $\Gamma_o(N)$.

In this paper, we construct a fundamental domain for $\Gamma^o(N)$ where N has at most four prime factors.

Construction

According to Cohn [3], a simple construction of the fundmental domain can be made when N has at most two prime factors. The construction is as follows:

1. We use the translation $z'=z+N$ to place $R(N)$ within the vertical line $|Rez| \leq N/2$. We call these the vertical limits for N.

2. We consider each interval $(m, m+\frac{1}{2})$ and $(m, m-\frac{1}{2})$ within the vertical limits, where m is an integer on the real axis.

3. m is a cusp (where the boundary touches $z = m > 1$ exactly) when $(m, N) > 1$

4. When $(m, N)=1$, We fill the interval $(m-\frac{1}{2}, m+\frac{1}{2})$ with the arc from $m-\frac{1+\sqrt{3}i}{2}$ to $m+\frac{1+\sqrt{3}i}{2}$ which have unit radius $|z-m| = 1$, $|Rez-m| \leq 1/2$.

5. When $(m, N) > 1$, we consider two cases:

a. If $(m+1, N)=1$ then we fill the interval $(m, m+\frac{1}{2})$ with the arc of unit radius $|z-m-1| = 1$, $0 \leq Re\ z-m-1 \leq 1/2$. (We make a symmetrical construction if $(m-1, N)=1$).

b. If $(m+1, N) > 1$ then we fill the interval $(m, m+1)$ with the arc of

radius $\frac{1}{2}$ joining the cusps m and $m+1$.

$$|z - m - \frac{1}{2}| = \frac{1}{2},\ m \leq Rez \leq m+1$$

In general, when N is a prime, only $m = 0$ is a cusp on the interval within the vertical limits. So the boundary consists of arcs with unit radius. When N has two distinct prime factors, the arcs with radius $\frac{1}{2}$ may occurs if $(m, N) > 1$ and $(m+1, N) > 1$.

Now, the identification of the boundary arcs of $R(N)$ are as follows:

1. If $(m, N) = 1$ and $(m_1, N) = 1$, where $mm_1 \equiv -1 \pmod{N}$, then the arc containing $m + i$ is mapped into the arc containing $m_1 + i$ by $(z - m)(z' - m_1) = -1$.

2. If $(m, N) > 1$ and $(m+1, N) > 1$ then the arc between m and $m+1$ is mapped into the arc containing m_1 and $m_1 + 1$ by

$$(z - \frac{2m+1}{2})(z' - \frac{2m_1+1}{2}) = -\frac{1}{4}$$

provided m and m_1 satisfy

$$(2m+1)(2m_1+1) \equiv -1 \pmod{2N}$$

We observe that

$$(z - m)(z' - m_1) = -1 \tag{8}$$

where $mm_1 \equiv -1 \pmod{N}$. The arc containing $m + i$ is on the circle centered at m with radius 1. Similarly for the arc containing $m_1 + i$

$$(z - \frac{2m+1}{2})(z' - \frac{2m_1+1}{2}) = -\frac{1}{4} \tag{9}$$

where $(2m+1)(2m_1+1) \equiv -1 \pmod{2N}$. The arc between m and $m+1$ is on the circle centered at $\frac{2m+1}{2}$ with radius $\frac{1}{2}$. Similarly for the arc between

m_1 and $m_1 + 1$. Now we have

$$(z - \frac{L}{Q})(z' - \frac{M}{Q}) = -\frac{1}{Q^2} \tag{10}$$

where $LM \equiv -1 \pmod{QN}$. The circle C_1 centered at $\frac{L}{Q}$ with radius $r = \frac{1}{Q}$ is mapped into the circle C_2 centered at $\frac{M}{Q}$ with radius $r = \frac{1}{Q}$ by (10) provided $LM \equiv -1 \pmod{QN}$.

In order to satisfy (10) L and M must each be relatively prime to N. Since $\frac{L}{Q}$, $\frac{M}{Q}$ are centers of C_1 and C_2, it suffices to consider the centers of various radii of circles which are relatively prime to N. Now, we can consider the above construction more generally. We consider each interval $(m, m+1)$ within the vertical limits. We try to find circles to cover the interval. If N has only one prime factor, say p_1, all m on the real axis except $m = 0$ and $m = p_1$ are relatively prime to N. They will form a circle centered at $\frac{m}{1}$ with radius 1. Suppose N has two distinct prime factors, say p_1 and p_2. Consider the interval $(m, m+1)$, $\frac{2m+1}{2}$ is the center of the circle which goes through m and $m+1$. If $(m, N) > 1, (m+1, N) > 1$ then $2m+1$ must be relatively prime to N. Thus we find a circle with radius $\frac{1}{2}$ which covers the interval. If N has 3 distinct prime factors, it may happen that $(m, N) > 1, (m+1, N) > 1, (2m+1) > 1$ which means no circle with radius $\frac{1}{2}$ in this interval. We need to find some smaller circles to cover the interval. The next type of circles we consider will be the circles with radius $\frac{1}{3}$. Its centers are at $\frac{3m+1}{3}$ and $\frac{3m+2}{3}$. We need to check $3m+1, 3m+2$ are relatively prime to N or not. If so, we can stop the process. If not, we consider the circles with radius $\frac{1}{4}$. We carry on the process until we find enough circles to cover the interval. Therefore, the question comes down to how many types of sets of circles will occur due to the various prime factors of N and m. Among these circles we must choose the ones with largest radii as the

boundary of the fundamental domain(i.e. if we have two sets of circles with centers $\frac{1}{6}, \frac{2}{5}, \frac{2}{3}$ and $\frac{1}{6}, \frac{2}{5}, \frac{3}{4}$, we choose $\frac{1}{6}, \frac{2}{5}, \frac{2}{3}$ since $\frac{2}{3}$ is bigger than $\frac{3}{4}$). For convenience, we say "*the circles centered at* $\frac{1}{3}$, $\frac{3}{4}$ *cover the interval*" which we mean the circles centered at $\frac{3m+1}{3}$ and $\frac{4m+3}{4}$ cover the interval $(m, m+1)$. It is abuse of the language by referring to the circles instead of the arcs on the upper half plane as the boundary. We will still use the term 'circle' but we mean the arcs on the upper half plane only.

We want to show there is always some lower limit to the isometric circles so that no cusp occurs except at integers m where $(m, N) > 1$. (i.e., no cusp occurs between m and $m+1$) Given an extra cusp, say $\frac{L}{Q}$ in reduced form, where $(L, N) > 1$ and $Q > 1$ then $\frac{L}{Q}$ is covered by a circle $|z - \frac{q}{s}| = \frac{1}{s}$ where $(q, N) = 1$. Recall that from equation (10),

$$(z - \frac{L}{Q})(z' - \frac{M}{Q}) = -\frac{1}{Q^2}$$

where $LM \equiv -1 \pmod{QN}$. The circle $|z - \frac{L}{Q}| = \frac{1}{Q}$ is mapped into $|z' - \frac{M}{Q}| = \frac{1}{Q}$. If $(L, N) = 1$ then $\frac{L}{Q}$ is a center and we are done. Suppose we have $(L, N) > 1$. Since $(L, Q) = 1$, there exist $q, s > 0$ such that $Ls - qQ = 1$. This implies that $(L, q) = 1$. We need the following result

Lemma 1 *Given any N and an arithmetic progression $q + tL, t = 0, 1, 2, \ldots$ where $(L, q) = 1$, there exists a t such that $(q + tL, N) = 1$.*

Proof. Let the primes $p_i | N$ then there is at most one solution in t to the congruence $q + tL \equiv 0 \pmod{p_i}$ (no solution if $p_i | L$ also). Hence for each p_i there is a value of $t \pmod{p_i}$ for which $q + tL \not\equiv 0 \pmod{p_i}$. Therefore there is a value of $t \pmod{M}$, where $M = \prod p_i$, for which $(q + tL, M) = (q + tL, N) = 1$, by the Chinese Remainder Theorem. Q.E.D.

By the lemma, choose such t and let $q' = q + tL$, $s' = s + tQ$. Then $(q', N) = 1$ and we still have $Ls' - q'Q = 1$. Now rename q', s' as q, s respectively. Then $(q, N) = (q, s) = 1$. Hence $\frac{q}{s}$ is a center. $Ls - qQ = 1$ imples that

$$\frac{q}{s} < \frac{L}{Q} = \frac{q}{s} + \frac{1}{sQ} < \frac{q}{s} + \frac{1}{s}$$

since $Q > 1$. So the circle $|z - \frac{q}{s}| = \frac{1}{s}$ covers the point $\frac{L}{Q}$.

Before proceeding, we notice that the total number of fundamental domains is the index of $\Gamma^0(N)$ in Γ which is $N \prod_{p|N}(1 + \frac{1}{p})$, where the product runs over all prime divisors of N. A diagram is given on the next page which shows how to count the number of fundamental domains. We list the figures occuring with at most three disinct prime factors in N, for Chapter 5, 6 and 7.

In general (with up to three prime factors in N) we have the following diagram (where each shaded region denotes the $\frac{1}{2}$ fundamental domain):

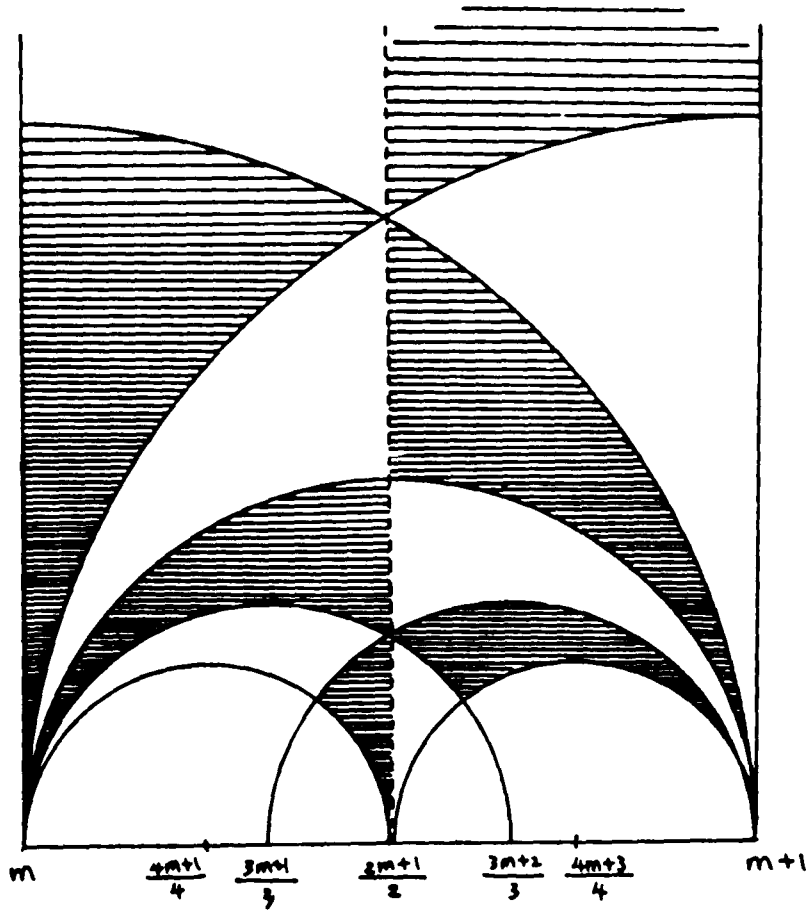

Figure 5: Illustration for counting fundamental domains

Due to the various factors of m, we have the following figures (where the solid line denotes the boundary) :

$s_1 : (m, N) = 1, (m+1, N) = 1$

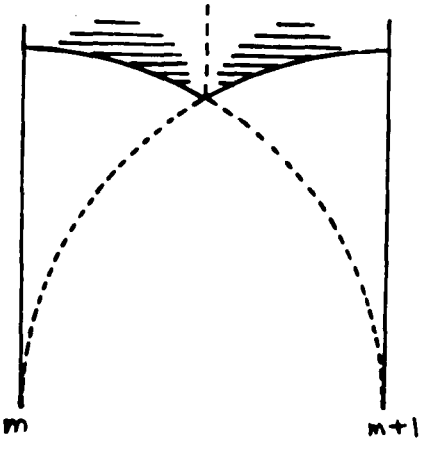

Figure 6: Configuration s_1 of area 1

$s_2 : (m, N) > 1, (m+1, N) = 1$

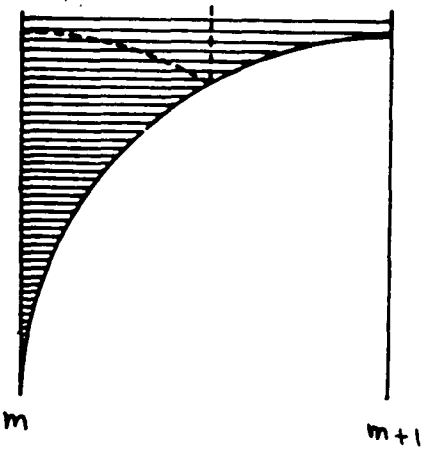

Figure 7: Configuration s_2 of area $\frac{3}{2}$

$s_3 : (m, N) = 1, (m+1, N) > 1$

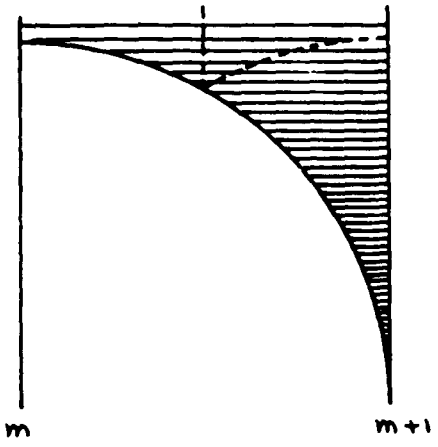

Figure 8: Configuration s_3 of area $\frac{3}{2}$

$s_4 : (m, N) > 1, (m+1, N) > 1, (2m+1, N) = 1$

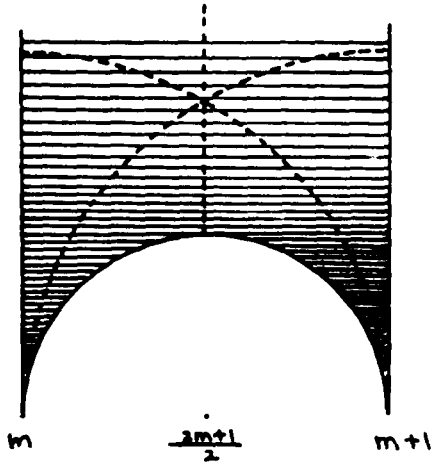

Figure 9: Configuration s_4 of area 3

$s_5 : (m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1, (3m+1, N) = 1, (3m+2, N) = 1$

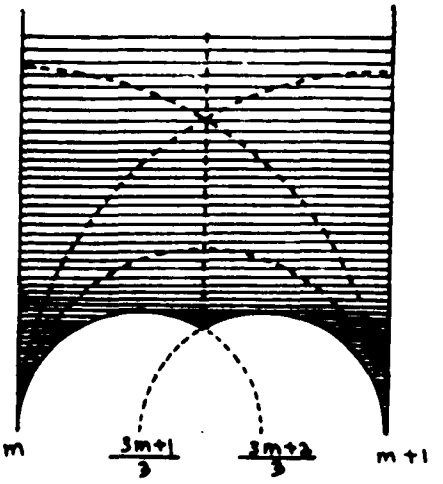

Figure 10: Configuration s_5 of area 4

$s_6 : (m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1, (3m+2, N) > 1, (3m+1, N) = (4m+3, N) = 1$

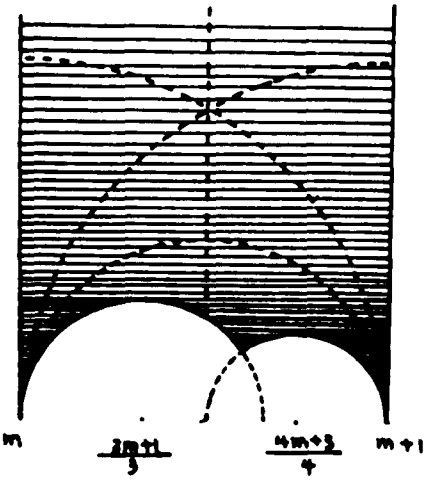

Figure 11: Configuration s_6 of area $\frac{9}{2}$

$s_7 : (m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1, (3m+1, N) > 1, (3m+2, N) = (4m+1, N) = 1$

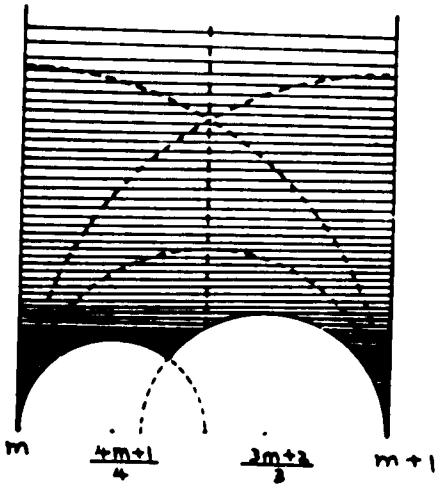

Figure 12: Configuration s_7 of area $\frac{9}{2}$

Chapter 5

The case $N = p_1^{e_1}$

Theorem 8 *If $N = p_1^{e_1}$, where p_1 is a positive prime and e_1 is a positive integer, then it is impossible for $(m, N) > 1$ and $(m+1, N) > 1$ where $|m| \leq \frac{N}{2}$. Hence circles can be found with radius $r = 1$.*

Proof. Recall that m is in integer on the real axis and only the cusps are zero and the multiples of p_1. It is clear that if N has only one prime factor p_1 and $(m, N) = p_1^{\alpha}$ where $1 \leq \alpha < e_1$, then it is impossible for $(m+1, N) = p_1^{\beta}$ where $1 \leq \beta < e_1$ since $(m, m+1) = 1$ thus $(m+1, N) = 1$. There are no two consecutive integers which are cusps. Therefore we may use only circles with radius $r = 1$. Q.E.D.

We have the following cases:

Case 1. $(m, N) = 1, (m+1, N) = 1$. s_1 will occur.

Case 2. $(m, N) > 1, (m+1, N) = 1$. s_2 will occur.

Case 3. $(m, N) = 1, (m+1, N) > 1$. s_3 will occur.

We need to examine the number of residue classes mod N for each class mod p and the total number of fundamental domains.

For s_1 we have

$$\begin{aligned} s_1 &= \#\{m \bmod N : (m, N) = (m+1, N) = 1\} \\ &= \#\{m \bmod N : m \not\equiv 0, -1 \bmod p\} \\ &= N(p-2)/p \end{aligned}$$

For s_2 we have

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m, N) > 1,\ (m+1, N) = 1\} \\ &= \#\{m \bmod N : m \equiv -1 \bmod p\} \\ &= N/p \end{aligned}$$

For s_3 we have

$$\begin{aligned} s_3 &= \#\{m \bmod N : (m, N) = 1,\ (m+1, N) > 1\} \\ &= \#\{m \bmod N : m \equiv -1 \bmod p\} \\ &= N/p \end{aligned}$$

We note that s_2 and s_3 are symmetrical and the total number of classes of $m \bmod N$ is as follows:

Total $\#\{m \bmod N\}$

$= s_1 + s_2 + s_3$

$= \frac{N}{p}(p-2) + \frac{N}{p} + \frac{N}{p}$

$= \frac{N}{p}(p)$

$= N$

Total # fundamental domains

$= s_1.1 + (s_2 + s_3)\frac{3}{2}$

$= \frac{N}{p}(p-2) + \frac{2N}{p}\frac{3}{2}$

$= N(p+1)/p$

$= N(1 + \frac{1}{p})$

Chapter 6

The case $N = p_1^{e_1} p_2^{e_2}$

Theorem 9 *If $N = p_1^{e_1} p_2^{e_2}$ where p_1, p_2 are distinct primes and e_1, e_2 are positive integers, then it is impossible that $(m, N) > 1$, $(m+1, N) > 1$, $(2m+1, N) > 1$ simultaneously, where $|m| \leq \frac{N}{2}$. Hence circles can be found with radius $r \geq \frac{1}{2}$.*

Proof. Assume $(m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1$ is possible. Since $(m, N) > 1$ and $(m, m+1) = 1$, we may assume $p_1 | (m, N)$ and $p_2 | (m+1, N)$. Since $(2m+1, N) > 1$, if $p_1 | (2m+1, N)$ then $p_1 | (m+1, N)$. But $p_1 \neq p_2$. If $p_2 | (2m+1, N)$ then $p_2 | (m, N)$. But $p_1 \neq p_2$. Thus $p_1, p_2 \nmid (2m+1, N)$, giving a contradiction.

The number of distinct prime factor(s) for (m, N), $(m+1, N)$ and $(2m+1, N)$ is either one or two. We have the following situation:

case	(m, N)	$(m+1, N)$	$(2m+1, N)$
1	$p_1 p_2$	1	1
2	1	$p_1 p_2$	1
3	1	1	$p_1 p_2$
4	p_1	p_2	1
5	1	p_1	p_2
6	p_2	1	p_1

Table 1: Cases for two primes

Notice that the order of p_1 and p_2 can be interchanged. Out of the six cases, only $p_1|(m,N)$, $p_2|(m+1,N)$ and $(2m+1,N)=1$ will yield a circle with radius $r=\frac{1}{2}$ beacause $m, m+1$ are two consecutive cusps, the other will give circles with radius $r=1$. Q.E.D.

To summarize, we have the following cases:

Case 1. $(m,N)=1$ and $(m+1,N)=1$ then s_1 will occur.

Case 2. $(m,N)>1$ and $(m+1,N)=1$ then s_2 will occur.

Case 3. $(m,N)=1$ and $(m+1,N)>1$ then s_3 will occur.

Case 4. $(m,N)>1$ and $(m+1,N)>1$ then s_4 will occur.

We need to examine the number of residue classes mod N for each class mod p_i, $i=1,2$.

For s_1 we have

$$\begin{aligned} s_1 &= \#\{m \bmod N : (m,N)=(m+1,N)=1\} \\ &= \#\{m \bmod N : m \not\equiv 0,-1 \bmod p_1p_2\} \\ &= N(p_1-2)(p_2-2)/p_1p_2 \end{aligned}$$

For s_2 we have

$$s_2 = \#\{m \bmod N : (m,N)>1,(m+1,N)=1\}$$

The following cases occur:

Case 1.

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m,N)=p_1p_2,(m+1,N)=1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_1p_2\} \\ &= N/p_1p_2 \end{aligned}$$

Case 2.

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m, N) = p_1, (m+1, N) = 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_1, m \not\equiv 0, -1 \bmod p_2\} \\ &= N(p_2 - 2)/p_1 p_2 \end{aligned}$$

Case 3.

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m, N) = p_2, (m+1, N) = 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_2, m \not\equiv 0, -1 \bmod p_1\} \\ &= N(p_1 - 2)/p_1 p_2 \end{aligned}$$

Adding up three cases, we have

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m, N) > 1, (m+1, N) = 1\} \\ &= N(1 + p_2 - 2 + p_1 - 2)/p_1 p_2 \\ &= N(p_1 + p_2 - 3)/p_1 p_2 \end{aligned}$$

For s_3 we have

$$s_3 = \#\{m \bmod N : (m, N) = 1, (m+1, N) > 1\}$$

The following cases occur:

Case 1.

$$\begin{aligned} s_3 &= \#\{m \bmod N : (m+1, N) = p_1 p_2, (m, N) = 1\} \\ &= \#\{m \bmod N : m \equiv -1 \bmod p_1 p_2\} \\ &= N/p_1 p_2 \end{aligned}$$

Case 2.

$$\begin{aligned} s_3 &= \#\{m \bmod N : (m+1, N) = p_1, (m, N) = 1\} \\ &= \#\{m \bmod N : m \equiv -1 \bmod p_1, m \not\equiv 0, -1 \bmod p_2\} \\ &= N(p_2 - 2)/p_1 p_2 \end{aligned}$$

Case 3.

$$\begin{aligned} s_3 &= \#\{m \bmod N : (m+1, N) = p_2, (m, N) = 1\} \\ &= \#\{m \bmod N : m \equiv -1 \bmod p_2, m \not\equiv 0, -1 \bmod p_1\} \\ &= N(p_1 - 2)/p_1 p_2 \end{aligned}$$

Adding up three cases, we have

$$\begin{aligned} s_3 &= \#\{m \bmod N : (m, N) = 1, (m+1, N) > 1\} \\ &= N(1 + p_2 - 2 + p_1 - 2)/p_1 p_2 \\ &= N(p_1 + p_2 - 3)/p_1 p_2 \end{aligned}$$

Notice that $s_2 = s_3$ by symmetry. From now on, we can compute s_2 only.

For s_4 we have

$$s_4 = \#\{m \bmod N : (m, N) > 1, (m+1, N) > 1\}$$

The following cases occur:

Case 1.

$$\begin{aligned} s_4 &= \#\{m \bmod N : (m, N) = p_1, (m+1, N) = p_2\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_1, m \equiv -1 \bmod p_2\} \\ &= N/p_1 p_2 \end{aligned}$$

Case 2.

$$\begin{aligned} s_4 &= \#\{m \bmod N : (m, N) = p_2, (m+1, N) = p_1\} \\ &= \#\{m \bmod N : m \equiv -1 \bmod p_1, m \equiv 0 \bmod p_2\} \\ &= N/p_1p_2 \end{aligned}$$

Adding up two cases, we have

$$\begin{aligned} s_4 &= N/p_1p_2 + N/p_1p_2 \\ &= 2N/p_1p_2 \end{aligned}$$

Total $\#\{m \bmod N\}$

$= s_1 + s_2 + s_3 + s_4$

$= \frac{N}{p_1p_2}(p_1 - 2)(p_2 - 2) + \frac{2N}{p_1p_2}(p_1 + p_2 - 3) + \frac{2N}{p_1p_2}$

$= \frac{N}{p_1p_2}(p_1p_2 - 2p_1 - 2p_2 + 4 + 2p_1 + 2p_2 - 6 + 2)$

$= \frac{N}{p_1p_2}(p_1p_2)$

$= N$

Total # of fundamental domains

$= 1 \cdot s_1 + \frac{3}{2}(s_2 + s_3) + 3s_4$

$= \frac{N}{p_1p_2}(p_1 - 2)(p_2 - 2) + \frac{3}{2}\frac{2N}{p_1p_2}(p_1 + p_2 - 3) + 3\frac{2N}{p_1p_2}$

$= \frac{N}{p_1p_2}(p_1p_2 + p_1 + p_2 + 1)$

$= N(1 + \frac{1}{p_1})(1 + \frac{1}{p_2})$

We call the circles with radius 1 and $\frac{1}{2}$ *standard.*

Chapter 7

The Case $N = p_1^{e_1} p_2^{e_2} p_3^{e_3}$

Recall that (10)

$$(z - \frac{L}{Q})(z' - \frac{M}{Q}) = -\frac{1}{Q^2}$$

provided $LM \equiv -1 \pmod{QN}$. In order to satisfy (10), L, M must each be relatively prime to N. When N has three distinct prime factors, the situation is slightly more complicated than the case when N has only two distinct prime factors. We divide it into two cases:

A. N is odd.

Theorem 10 *If $N = p_1^{e_1} p_2^{e_2} p_3^{e_3}$, where p_1, p_2, p_3 are distinct odd prime numbers and e_1, e_2, e_3 are positive integers, then it is impossible that $(m, N) > 1$, $(m+1, N) > 1$, $(2m+1, N) > 1$ and $(3m+1, N) > 1$ simultaneously, where $|m| \leq \frac{N}{2}$. Hence circles can be found with radius $r \geq \frac{1}{3}$.*

Proof. Assume $(m, N) > 1, (m+1. N) > 1, (2m+1, N) > 1, (3m+1, N) > 1$. Since $(m, N) > 1$ and $(m+1, N) > 1$, without loss of generality we may assume $p_1 | (m, N)$ and $p_2 | (m+1, N)$. Also, as $(2m+1, N) > 1$, then $p_3 | (2m+1, N)$ since $p_1 \nmid (2m+1, N)$ and $p_2 \nmid (2m+1, N)$. Now we claim that none of the p_i's divides $(3m+1, N)$, so this is a contradiction. First, $p_1 | m$ implies $p_1 | 3m$. So $p_1 \nmid 3m+1$. Next, $p_2 | m+1$ implies $p_2 | 3m+3$. If $p_2 | 3m+1$, then $p_2 | 3m+3-(3m+1) = 2$. But p_2 is odd, so $p_2 \nmid 3m+1$.

Finally, $p_3|2m+1$ implies $p_3|6m+3$. If $p_3|3m+1$ then $p_3|6m+2$, but this is not possible. Thus $(3m+1,N)=1$ as claimed and we get a contradiction. Therefore $(3m+1,N)=1$.

We want to investigate the number of prime divisors for (m,N), $(m+1,N)$, $(2m+1,N)$ and $(3m+1,N)$. With only at most one prime divisor, we consider the following cases:

case	(m,N)	$(m+1,N)$	$(2m+1,N)$	$(3m+1,N)$
1	p_1	p_2	p_3	1
2	1	p_1	p_2	p_3
3	p_3	1	p_1	p_2
4	p_2	p_3	1	p_1

Table 2: Cases for three primes, (part I)

Case 1. $(m,N)>1,(m+1,N)>1,(2m+1,N)>1,(3m+1,N)=1$
If in addition $(3m+2,N)=1$ then s_5 will occur. But this is true as in the proof above.

Case 2. $(m,N)=1,(m+1,N)>1,(2m+1,N)>1,(3m+1,N)>1$
s_3 will occur.

Case 3. $(m,N)>1,(m+1,N)=1,(2m+1,N)>1,(3m+1,N)>1$
s_2 will occur.

Case 4. $(m,N)>1,(m+1,N)>1,(2m+1,N)=1,(3m+1,N)>1$
s_4 will occur.

With two divisors, we consider the following cases:

case	(m, N)	$(m+1, N)$	$(2m+1, N)$	$(3m+1, N)$
1	p_1p_2	p_3	1	1
2	1	p_1p_2	p_3	1
3	1	1	p_1p_2	p_3
4	p_3	1	1	p_1p_2

Table 3: Cases for three primes, (part II)

Case 1. $(m, N) > 1, (m+1, N) > 1, (2m+1, N) = 1, (3m+1, N) = 1$

s_4 will occur.

Case 2. $(m, N) = 1, (m+1, N) > 1, (2m+1, N) > 1, (3m+1, N) = 1$

s_3 will occur.

Case 3. $(m, N) = 1, (m+1, N) = 1, (2m+1, N) > 1, (3m+1, N) > 1$

s_1 will occur.

Case 4. $(m, N) > 1, (m+1, N) = 1, (2m+1, N) = 1, (3m+1, N) > 1$

s_2 will occur.

Therefore, circles will be found with radius $r \geq \frac{1}{3}$. Q.E.D.

We want to examine the number of residue classes mod N for each class mod p_i, where $i = 1, 2, 3$.

For s_1, we have

$$\begin{aligned} s_1 &= \#\{m \bmod N : (m, N) = (m+1, N) = 1\} \\ &= \#\{m \bmod N : m \not\equiv 0, -1 \bmod p_1p_2p_3\} \\ &= \frac{N}{p_1p_2p_3}(p_1 - 2)(p_2 - 2)(p_3 - 2) \end{aligned} \tag{11}$$

For s_2, we have

$$s_2 = \#\{m \bmod N : (m, N) > 1, (m+1, N) = 1\}$$

The following cases occur:

Case 1.

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m, p_1) > 1, (m, p_2) > 1, (m, p_3) > 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_1 p_2 p_3\} \\ &= \frac{N}{p_1 p_2 p_3} \end{aligned}$$

Case 2.

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m, p_1) > 1, (m, p_2) > 1, (m, p_3) = 1, \\ &\quad (m+1, p_1 p_2 p_3) = 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_1 p_2, m \not\equiv 0, -1 \bmod p_3\} \\ &= \frac{N}{p_1 p_2 p_3}(p_3 - 2) \end{aligned}$$

By symmetry, we have from Case 2,

Case 3.

$$s_2 = \frac{N}{p_1 p_2 p_3}(p_2 - 2)$$

Case 4.

$$s_2 = \frac{N}{p_1 p_2 p_3}(p_1 - 2)$$

Case 5.

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m,p_1) > 1, (m,p_2) = 1, (m,p_3) = 1 \\ &\quad (m+1, p_1p_2p_3) = 1\} \\ &= \#\{m \bmod N : n_i \equiv 0 \bmod p_1, m \not\equiv 0, -1 \bmod p_2p_3\} \\ &= \frac{N}{p_1p_2p_3}(p_2-2)(p_3-2) \end{aligned}$$

By symmetry, we have from Case 5,

Case 6.

$$s_2 = \frac{N}{p_1p_2p_3}(p_1-2)(p_3-2)$$

Case 7.

$$s_2 = \frac{N}{p_1p_2p_3}(p_1-2)(p_2-2)$$

Add up all cases, we have

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m,N) > 1, (m+1,N) = 1\} \\ &= \frac{N}{p_1p_2p_3}[p_1+p_2+p_3-5+(p_2-2)(p_3-2) \\ &\quad +(p_1-2)(p_3-2)+(p_1-2)(p_2-2)] \end{aligned} \tag{12}$$

For s_3 we have

$$\begin{aligned} s_3 &= \#\{m \bmod N : (m,N) = 1, (m+1,N) > 1\} \\ &= \frac{N}{p_1p_2p_3}[p_1+p_2+p_3-5+(p_2-2)(p_3-2) \\ &\quad +(p_1-2)(p_3-2)+(p_1-2)(p_2-2)] \end{aligned}$$

since s_2 and s_3 are symmetrical.

For s_4 we have

$$s_4 = \#\{m \bmod N : (m, N) > 1, (m+1, N) > 1, (2m+1, N) = 1\}$$

The following cases occur:

Case 1.

$$\begin{aligned} & \#\{m \bmod N : (m, p_1) > 1, (m+1, p_2p_3) > 1\} \\ = \; & \#\{m \bmod N : m \equiv 0 \bmod p_1, m \equiv -1 \bmod p_2p_3\} \\ = \; & \frac{N}{p_1p_2p_3} \end{aligned}$$

By permutating the p_i's, we have two more terms. So we get $\frac{3N}{p_1p_2p_3}$. Interchanging the roles of m and $m+1$, we get three more terms. So in this case $s_4 = \frac{6N}{p_1p_2p_3}$

Case 2.

$$\begin{aligned} & \#\{m \bmod N : (m, p_1) > 1, (m+1, p_2) > 1 \\ & \quad (m, p_2p_3) = 1, (m+1, p_1p_3) = 1, (2m+1, p_1p_2p_3) = 1\} \\ = \; & \#\{m \bmod N : m \equiv 0 \bmod p_1, m \equiv -1 \bmod p_2 \\ & \quad m \not\equiv 0, -1 \bmod p_3, 2m \not\equiv -1 \bmod p_3\} \\ = \; & \frac{N}{p_1p_2p_3}(p_3 - 3) \end{aligned}$$

By permutating the p_i's, we get two more terms:

$$\frac{N}{p_1p_2p_3}(p_2 - 3), \; \frac{N}{p_1p_2p_3}(p_1 - 3)$$

By interchanging the roles of m and $m+1$, we get

$$\frac{2N}{p_1p_2p_3}[(p_1 - 3) + (p_2 - 3) + (p_3 - 3)]$$

Adding up all cases, we have

$$\begin{aligned} s_4 &= \frac{6N}{p_1p_2p_3} + \frac{2N}{p_1p_2p_3}[(p_1-3)+(p_2-3)+(p_3-3)] \\ &= \frac{2N}{p_1p_2p_3}(p_1+p_2+p_3-6) \end{aligned}$$

For s_5 we have

$$\begin{aligned} s_5 &= \#\{m \bmod N : (m,N)>1, (m+1,N)>1, (2m+1,N)>1, \\ &\quad (3m+1,N)=(3m+2,N)=1\} \end{aligned}$$

Consider

$$\#\{m \bmod N : m \equiv 0 \bmod p_1, m \equiv -1 \bmod p_2, 2m \equiv -1 \bmod p_3\}$$

$$= \frac{N}{p_1p_2p_3}$$

By permutating the p_i's, we have altogether 6 such terms. So

$$s_5 = \frac{6N}{p_1p_2p_3}$$

By direct computation, we have

Total $\#\{m \bmod N\}$

$= s_1 + s_2 + s_3 + s_4 + s_5$

$= N$

Total # fundamental domains

$= 1 \cdot s_1 + \frac{3}{2}(s_2 + s_3) + 3 \cdot s_4 + 4 \cdot s_5$

$= \frac{N}{p_1p_2p_3}(p_1+1)(p_2+1)(p_3+1)$

$= N(1+\frac{1}{p_1})(1+\frac{1}{p_2})(1+\frac{1}{p_3})$

B. N is even.

Theorem 11 *If $N = p_1^{e_1} p_2^{e_2} p_3^{e_3}$, where p_1, p_2, p_3 are distinct prime numbers and e_1, e_2, e_3 are positive integers, then it is impossible that $(m, N) > 1$ $(m+1, N) > 1, (2m+1, N) > 1, (4m+1, N) > 1, (4m+3, N) > 1$ simultaneously, where $|m| \leq \frac{N}{2}$. Hence circles can be found with $r \geq \frac{1}{4}$.*

Proof. Assume $(m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1, (4m+1, N) > 1$ $(4m+3, N) > 1$ is possible. Then $(m, N) > 1$ and $(m+1, N) > 1$. Without loss of generality, we may assume $p_1 | (m, N)$ and $p_2 | (m+1, N)$. By the same argument as in the previous case, $p_1 \nmid (2m+1, N)$ and $p_2 \nmid (2m+1, N)$. Thus $p_3 | (2m+1, N)$. Since $2m+1$ is odd, either p_1 or p_2 equals 2.

Case 1: $p_1 = 2$. Since $4m+3$ is odd, $p_1 \nmid 4m+3$. $p_2 | m+1$ implies $p_2 | 4m+4$. Thus $p_2 \nmid 4m+3$. $p_3 | 2m+1$ implies $p_3 | 4m+2$. Thus $p_3 \nmid 4m+3$. Therefore $(4m+3, N) = 1$, contradiction.

Case 2: $p_2 = 2$. $p_1 | m$ implies $p_1 | 4m$. Thus $p_1 \nmid 4m+1$. $4m+1$ is odd, so $p_2 \nmid 4m+1$. $p_3 | 2m+1$ implies $p_3 | 4m+2$. Thus $p_3 \nmid 4m+1$. Therefore $(4m+1, N) = 1$, contradiction.

We determine what type of circles will appear. First, we notice that if $p_1 | (m, N), p_2 | (m+1, N), p_3 | (2m+1, N)$ then either $(3m+1, N) > 1$ or $(3m+2, N) > 1$ but not both. The proof is similar to the proof above. So s_5 will not occur. We have the following cases:

Case 1. $(m, N) = 1, (m+1, N) = 1$ will not occur because $2 | N$.

Case 2. $(m, N) > 1, (m+1, N) = 1$. s_2 will occur.

Case 3. $(m, N) = 1, (m+1, N) > 1$. s_3 will occur.

Case 4. $(m, N) > 1, (m+1, N) > 1, (2m+1, N) = 1$. s_4 will occur.

Case 5. $(m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1,$
$(3m+1, N) = (3m+2, N) = 1$. s_5 will not occur since $2 | N$.

Case 6. $2|(m,N), p_2|(m+1,N), p_3|(2m+1,N), 2|(3m+2,N)$, $(3m+1,N) = (4m+3,N) = 1$. s_6 will occur.

Case 7. $p_1|(m,N), 2|(m+1,N), p_3|(2m+1,N), 2|(3m+1,N)$, $(3m+2,N) = (4m+1,N) = 1$. s_7 will occur. Q.E.D.

We want to compute the number of residue classes mod N for each class mod $p_i, i = 1,2,3$. Since $2|N$, we assume $p_1 = 2$.

For s_1, put $p_1 = 2$ in (11), we get $s_1 = 0$.

For s_2, put $p_1 = 2$ in (12), we get

$$s_2 = \frac{N}{p_1p_2p_3}(p_2p_3 - p_2 - p_3 + 1)$$

For s_3, by symmetry we have

$$s_3 = \frac{N}{p_1p_2p_3}(p_2p_3 - p_2 - p_3 + 1)$$

For s_4, we have

$$s_4 = \#\{m \bmod N : (m,N) > 1, (m+1,N) > 1, (2m+1,N) = 1\}$$

We are in the same situation as in the case when N is odd, except for those cases when the term $p_1 - 3$ appears. But actually these cases can never occur since $p_1 = 2$. We just set leave out the term $p_1 - 3$. So we get

$$\begin{aligned} s_4 &= \frac{6N}{p_1p_2p_3} + \frac{2N}{p_1p_2p_3}[(p_2-3)+(p_3-3)] \\ &= \frac{2N}{p_1p_2p_3}(p_2+p_3-3) \end{aligned}$$

$$s_5 = \#\{m \bmod N : (m,N) > 1, (m+1,N) > 1, (2m+1,N) > 1, (3m+1,N) = (3m+2,N) = 1\}.$$

It will not occur since $(3m+1,N) = (3m+2,N) = 1$ is impossible when N is even. So $s_5 = 0$.

$$s_6 = \#\{m \bmod N : (m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1,$$
$$(3m+2, N) > 1, (3m+1, N) = (4m+3, N) = 1\}.$$

The following cases occur:

Case 1.

$$\begin{aligned} s_6 &= \#\{m \bmod N : (m, p_1) > 1, (m+1, p_2) > 1, (2m+1, p_3) > 1, \\ &\quad (3m+2, 2) > 1, (3m+1, N) = (4m+3, N) = 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod 2, m \equiv -1 \bmod p_2, 2m \equiv -1 \bmod p_3\} \\ &= \frac{N}{p_1 p_2 p_3} \end{aligned}$$

Case 2.

$$\begin{aligned} s_6 &= \#\{m \bmod N : (m, p_1) > 1, (m+1, p_3) > 1, (2m+1, p_2) > 1, \\ &\quad (3m+2, 2) > 1, (3m+1, N) = (4m+3, N) = 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_2, m \equiv -1 \bmod p_3, 2m \equiv -1 \bmod p_2\} \\ &= \frac{N}{p_1 p_2 p_3} \end{aligned}$$

Adding up the two cases, we have $s_6 = \frac{2N}{p_1 p_2 p_3}$

$$\begin{aligned} s_7 &= \#\{m \bmod N : (m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1, \\ &\quad (3m+1, N) > 1, (3m+2, N) = (4m+1, N) = 1\} \end{aligned}$$

The following cases occur:

Case 1.

$$\begin{aligned} s_7 &= \#\{m \bmod N : (m, p_2) > 1, (m+1, p_1) > 1, (2m+1, p_3) > 1, \\ &\quad (3m+1, 2) > 1, (3m+2, N) = (4m+1, N) = 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod 2, m \equiv -1 \bmod p_2, 2m \equiv -1 \bmod p_3\} \\ &= \frac{N}{p_1 p_2 p_3} \end{aligned}$$

Case 2.

$$\begin{aligned} s_7 &= \#\{m \bmod N : (m, p_3) > 1, (m+1, p_1) > 1, (2m+1, p_2) > 1, \\ &\quad (3m+1, 2) > 1, (3m+2, N) = (4m+1, N) = 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_3, m \equiv -1 \bmod p_1, 2m \equiv -1 \bmod p_2\} \\ &= \frac{N}{p_1 p_2 p_3} \end{aligned}$$

Adding up the two cases, we have $s_7 = \frac{2N}{p_1 p_2 p_3}$

By direct computation, we have

Total $\#\{m \bmod N\}$

$= s_1 + s_2 + s_3 + s_4 + s_5 + s_6 + s_7$

$= \frac{N}{p_1 p_2 p_3}(p_1 p_2 p_3 - 2p_2 - 2p_3 + 2 + 2p_2 + 2p_3 - 6 + 2 + 2)$

$= N$

Total # fundamental domains

$= 1 \cdot s_1 + \frac{3}{2}(s_2 + s_3) + 3 \cdot s_4 + \frac{9}{2}s_6 + \frac{9}{2}s_7$

$= \frac{3N}{p_1 p_2 p_3}(p_2 p_3 + p_2 + p_3 + 1)$

$= \frac{3N}{p_1 p_2 p_3}(p_2 + 1)(p_3 + 1)$

$= \frac{3N}{p_1 p_2 p_3}(1 + \frac{1}{p_2})(1 + \frac{1}{p_3})$

$= N(1 + \frac{1}{p_1})(1 + \frac{1}{p_2})(1 + \frac{1}{p_3})$

since $p_1 = 2$.

We conclude that besides the standard circles, when N is odd, circles with radius $\frac{1}{3}$ can be found and when N is even, circles with radius $\frac{1}{3}$ and $\frac{1}{4}$ can be found.

Chapter 8

The Case $N = p_1^{e1} p_2^{e2} p_3^{e3} p_4^{e4}$

When N has four distinct prime factors, the cases become somewhat unwieldy due to the many possibilities for the divisors of m. We consider four cases, namely

A. $N = p_1^{e1} p_2^{e2} p_3^{e3} p_4^{e4}$ where $p_i > 3, i = 1, 2, 3, 4$.

B. $N = 2^{e1} p_2^{e2} p_3^{e3} p_4^{e4}$ where $p_i > 3, i = 2, 3, 4$.

C. $N = 3^{e1} p_2^{e2} p_3^{e3} p_4^{e4}$ where $p_i > 3, i = 2, 3, 4$.

D. $N = 2^{e1} 3^{e2} p_3^{e3} p_4^{e4}$ where $p_i > 3, i = 3, 4$.

In order for Poincaré's Theorem to work, the chosen circles must be of maximal radii. For example, in the interval $(0, 1)$ two sets of circles with radii, say $\frac{1}{6}, \frac{2}{5}, \frac{2}{3}$ and $\frac{1}{6}, \frac{2}{5}, \frac{3}{4}$ cover the interval as follows:

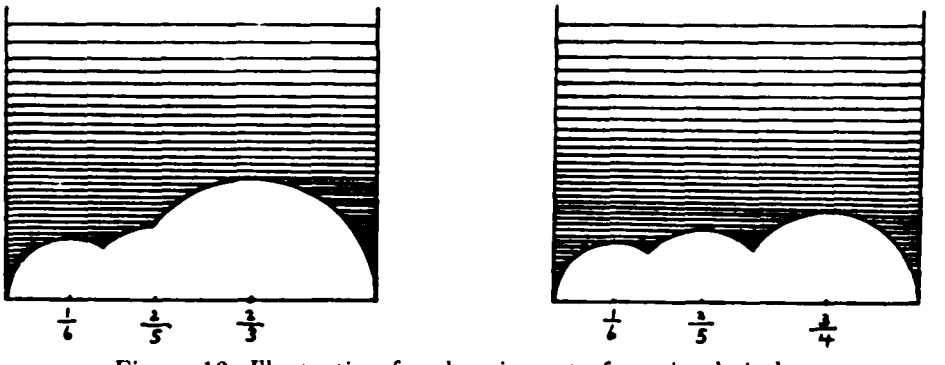

Figure 13: Illustration for choosing set of maximal circles

We choose $\frac{1}{6}, \frac{2}{5}, \frac{2}{3}$. We test different sets of circles which cover the interval.

We start with a circle with maximal radius and continue to choose the circles with maximal radii from the remaining circles until they cover the whole interval. Then we take the boundary of their union.

A. $N = p_1^{e_1}p_2^{e_2}p_3^{e_3}p_4^{e_4}$ where $p_i > 3, i = 1, 2, 3, 4$.

We call this case generic, since it works for all prime numbers greater than three. If $(m, N) = 1, (m+1, N) = 1$ then s_1 will occur. If $(m, N) > 1, (m+1, N) = 1$ then s_2 will occur. If $(m, N) = 1, (m+1, N) > 1$ then s_3 will occur. If $(m, N) > 1, (m+1, N) > 1, (2m+1, N) = 1$ then s_4 will occur. The only interesting case is when $m, m+1, 2m+1$ are not simultaneouly relatively prime to N.

Next we consider the following:

Theorem 12 *Let $N = p_1^{e_1}p_2^{e_2}p_3^{e_3}p_4^{e_4}$, where all p_i are distinct prime divisors greater than three and e_1, e_2, e_3, e_4 are positive integers. Suppose $|m| \leq \frac{N}{2}$ and $p_1|m, p_2|m+1, p_3|2m+1$ then either $(3m+1, N) = (4m+3, N) = 1$ or $(3m+2, N) = (4m+1, N) = 1$, hence, circles can be found with radius $r \geq \frac{1}{4}$.*

Proof. Clearly, either $p_4 \nmid 3m+1$ or $p_4 \nmid 3m+2$. Suppose $p_4 \nmid 3m+1$. Since $(m, 3m+1) = 1$ and $p_1|m$, therefore $p_1 \nmid 3m+1$. $p_2|m+1$ implies $p_2|3m+3$. Hence $p_2 \nmid 3m+1$ since $p_2 \neq 2$. Since $(2m+1, 3m+1) = 1$ and $p_3|2m+1$, therefore $p_3 \nmid 3m+1$. So $p_i \nmid 3m+1, \forall i = 1, 2, 3, 4$. Thus $(3m+1, N) = 1$. Similarly, $(m, 4m+3) = (2m+1, 4m+3) = 1$. Therefore $p_1 \nmid 4m+3$ and $p_3 \nmid 4m+3$. $p_2|m+1$ implies $p_2|4m+4$. So $p_2 \nmid 4m+3$. Therefore $(4m+3, N) = 1$. If we have $p_4 \nmid 3m+2$, then by the same argument we get $(4m+1, N) = (3m+2, N) = 1$.

We show that s_6 and s_7 will occur and the others will occur if $(m, N), (m+1, N), (2m+1, N)$ have more than one prime factor. Therefore, we can conclude that circles can be found with radius $r \geq \frac{1}{4}$. Q.E.D.

Let's examine the number of residue classes mod N for each class mod p_i where $p_i > 3, i = 1, 2, 3, 4$.

$$\begin{aligned} s_1 &= \#\{m \bmod N : (m, N) = (m+1, N) = 1\} \\ &= \#\{m \bmod N : m \not\equiv 0, -1 \bmod p_1p_2p_3p_4\} \\ &= \frac{N}{p_1p_2p_3p_4}(p_1 - 2)(p_2 - 2)(p_3 - 2)(p_4 - 2) \end{aligned}$$

$$s_2 = \#\{m \bmod N : (m, N) > 1, (m+1, N) = 1\}$$

The following cases occur:

Case 1.

$$\begin{aligned} s_2 &= \#\{m \bmod N : (m, p_1) > 1, (m, p_2) > 1, (m, p_3) > 1, (m, p_4) > 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_1p_2p_3p_4\} \\ &= \frac{N}{p_1p_2p_3p_4} \end{aligned}$$

Case 2.

$$\begin{aligned} &\#\{m \bmod N : (m, p_1) > 1, (m, p_2) > 1, (m, p_3) > 1, (m, p_4) = 1, \\ &\quad (m+1, p_1p_2p_3p_4) = 1\} \\ &= \#\{m \bmod N : m \equiv 0 \bmod p_1p_2p_3, m \not\equiv 0, -1 \bmod p_4\} \\ &= \frac{N}{p_1p_2p_3p_4}(p_4 - 2) \end{aligned}$$

By symmetry we have,

$$s_2 = \frac{N}{p_1p_2p_3p_4}[(p_1 - 2) + (p_2 - 2) + (p_3 - 2) + (p_4 - 2)]$$

Case 3.

$$\#\{m \bmod N : (m, p_1) > 1, (m, p_2) > 1, (m, p_3) = (m, p_4) = 1,$$
$$(m + 1, p_1p_2p_3p_4) = 1\}$$
$$= \#\{m \bmod N : m \equiv 0 \bmod p_1p_2, m \not\equiv 0, -1 \bmod p_3p_4\}$$
$$= \frac{N}{p_1p_2p_3p_4}(p_3 - 2)(p_4 - 2)$$

By symmetry, we have

$$s_2 = \frac{N}{p_1p_2p_3p_4} \sum_{1 \le i < j \le 4} (p_i - 2)(p_j - 2)$$

Case 4.

$$\#\{m \bmod N : (m, p_1) > 1, (m, p_2) = (m, p_3) = (m, p_4) = 1,$$
$$(m + 1, p_1p_2p_3p_4) = 1\}$$
$$= \#\{m \bmod N : m \equiv 0 \bmod p_1, m \not\equiv 0, -1 \bmod p_2p_3p_4\}$$
$$= \frac{N}{p_1p_2p_3p_4}(p_2 - 2)(p_3 - 2)(p_4 - 2)$$

By symmetry, we have

$$s_2 = \frac{N}{p_1p_2p_3p_4} \sum_{1 \le i < j < k \le 4} (p_i - 2)(p_j - 2)(p_k - 2)$$

Adding up all the cases, s_2= case 1 + case 2 + case 3 + case 4. Also by symmetry $s_3 = s_2$.

$$s_4 = \#\{m \bmod N : (m, N) > 1, (m+1, N) > 1, (2m+1, N) = 1\}$$

The following cases occur:

Case 1.

$$\#\{m \bmod N : (m, p_1) > 1, (m, p_2) > 1, (m, p_3) > 1, (m+1, p_4) > 1\}$$
$$= \#\{m \bmod N : m \equiv 0 \bmod p_1p_2p_3, m \equiv -1 \bmod p_4\}$$
$$= \frac{N}{p_1p_2p_3p_4}$$

By permutating the p_i's, we get $\frac{4N}{p_1p_2p_3p_4}$. Interchanging the roles of m and $m+1$, we get $\frac{8N}{p_1p_2p_3p_4}$ for this case.

Case 2.

$$\#\{m \bmod N : (m, p_1) > 1, (m, p_2) > 1, (m+1, p_3) > 1, (m+1, p_4) > 1\}$$
$$= \#\{m \bmod N : m \equiv 0 \bmod p_1p_2, m \equiv -1 \bmod p_3p_4\}$$
$$= \frac{N}{p_1p_2p_3p_4}$$

By permutating the p_i's, we get $\frac{6N}{p_1p_2p_3p_4}$ for this case.

Case 3.

$$\#\{m \bmod N : (m, p_1) > 1, (m, p_2) > 1, (m+1, p_3) > 1,$$
$$(m, p_3p_4) = (m+1, p_1p_2p_4) = (2m+1, p_1p_2p_3p_4) = 1\}$$
$$= \#\{m \bmod N : m \equiv 0 \bmod p_1p_2, m \equiv -1 \bmod p_3, m \not\equiv 0, -1 \bmod p_4,$$
$$2m \not\equiv -1 \bmod p_4\}$$
$$= \frac{N}{p_1p_2p_3p_4}(p_4 - 3)$$

By symmetry we have,

$$\frac{6N}{p_1p_2p_3p_4}[(p_1 - 3) + (p_2 - 3) + (p_3 - 3) + (p_4 - 3)]$$

for this case.

Case 4.

$$\#\{m \bmod N : (m,p_1) > 1, (m+1,p_2) > 1, (m,p_2p_3p_4) = (m+1,p_1p_3p_4) = (2m+1,p_1p_2p_3p_4) = 1\}$$

$$= \#\{m \bmod N : m \equiv 0 \bmod p_1, m \equiv -1 \bmod p_2, m \not\equiv 0,-1 \bmod p_3p_4, 2m \not\equiv -1 \bmod p_3p_4\}$$

$$= \frac{2N}{p_1p_2p_3p_4}(p_3-3)(p_4-3)$$

By symmetry, the total for this case is

$$\frac{2N}{p_1p_2p_3p_4} \sum_{1 \le i < j \le 4} (p_i-3)(p_j-3)$$

Adding up all the cases, s_4= case 1 + case 2 + case 3 + case 4.

$$s_5 = \#\{m \bmod N : (m,N) > 1, (m+1,N) > 1, (2m+1,N) > 1, (3m+1,N) = (3m+2,N) = 1\}$$

The following cases occur:

Case 1.

$$\#\{m \bmod N : (m,p_1) > 1, (m,p_2) > 1, (m+1,p_3) > 1, (2m+1,p_4) > 1\}$$

$$= \#\{m \bmod N : m \equiv 0 \bmod p_1p_2, m \equiv -1 \bmod p_3, 2m \equiv -1 \bmod p_4\}$$

$$= \frac{N}{p_1p_2p_3p_4}$$

By permutating the p_i's, we get $\frac{4!}{2!}\frac{N}{p_1p_2p_3p_4} = \frac{12N}{p_1p_2p_3p_4}$.

Interchanging the roles of $m, m+1, 2m+1$, we get $\frac{36N}{p_1p_2p_3p_4}$ as a total for this case.

Case 2.

$$\#\{m \bmod N : (m, p_1) > 1, (m+1, p_2) > 1, (2m+1, p_3) > 1, (m, p_2p_3p_4) = (m+1, p_1p_3p_4) = (2m+1, p_1p_2p_4) = (3m+1, p_1p_2p_3p_4) = (3m+2, p_1p_2p_3p_4) = 1\}$$

$$= \#\{m \bmod N : m \equiv 0 \bmod p_1, m \equiv -1 \bmod p_2, 2m \equiv -1 \bmod p_3, m \not\equiv 0, -1 \bmod p_4, 2m \not\equiv -1 \bmod p_4, 3m \not\equiv -1, -2 \bmod p_4.\}$$

$$= \frac{N}{p_1p_2p_3p_4}(p_4 - 5)$$

By permutation we have the total for this case,

$$\frac{6N}{p_1p_2p_3p_4}[(p_1 - 5) + (p_2 - 5) + (p_3 - 5) + (p_4 - 5)]$$

Adding up all the cases, we have s_5= case 1 + case 2.

$$s_6 = \#\{m \bmod N : (m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1, (3m+2, N) > 1, (3m+1, N) = (4m+3, N) = 1\}$$

Consider

$$\#\{m \bmod N : (m, p_1) > 1, (m+1, p_2) > 1, (2m+1, p_3) > 1, (3m+2, p_4) > 1, (3m+1, N) = (4m+3, N) = 1\}$$

$$= \#\{m \bmod N : m \equiv 0 \bmod p_1, m \equiv -1 \bmod p_2, 2m \equiv -1 \bmod p_3, 3m \equiv -1 \bmod p_4\}$$

$$= \frac{N}{p_1p_2p_3p_4}$$

By permutation, we have

$$s_6 = \frac{4!N}{p_1p_2p_3p_4} = \frac{24N}{p_1p_2p_3p_4}$$

$$s_7 = \#\{m \bmod N : (m,N) > 1, (m+1,N) > 1, (2m+1,N) > 1,$$
$$(3m+1,N) > 1, (3m+2,N) = (4m+1,N) = 1\}$$

Consider

$$\#\{m \bmod N : (m,p_1) > 1, (m+1,p_2) > 1, (2m+1,p_3) > 1,$$
$$(3m+1,p_4) > 1, (3m+2,N) = (4m+1,N) = 1\}$$
$$= \#\{m \bmod N : m \equiv 0 \bmod p_1, m \equiv -1 \bmod p_2, 2m \equiv -1 \bmod p_3,$$
$$3m \equiv -1 \bmod p_4\}$$
$$= \frac{N}{p_1p_2p_3p_4}$$

By permutation, we have

$$s_7 = \frac{4!N}{p_1p_2p_3p_4} = \frac{24N}{p_1p_2p_3p_4}$$

By direct calculation, we get

Total # of $\{m \bmod N\}$

$$= s_1 + s_2 + s_3 + s_4 + s_5 + s_6 + s_7$$
$$= N$$

Total # fundamental domains

$$= 1s_1 + \frac{3}{2}(s_2 + s_3) + 3s_4 + 4s_5 + \frac{9}{2}(s_6 + s_7)$$
$$= \frac{N}{p_1p_2p_3p_4}(p_1+1)(p_2+1)(p_3+1)(p_4+1)$$
$$= N(1+\frac{1}{p_1})(1+\frac{1}{p_2})(1+\frac{1}{p_3})(1+\frac{1}{p_4})$$

Recall that when N has 3 distinct prime factors, besides the standard circles, s_6 and s_7 will occur if N is even, only s_5 will occur if N is odd. Now for the generic case(i.e. $N = p_1^{e_1}p_2^{e_2}p_3^{e_3}p_4^{e_4}$, all $p_i > 3$) besides the standard circles, s_5, s_6, s_7 will occur.

B. $N = 2^{e_1} p_2^{e_2} p_3^{e_3} p_4^{e_4}$ where $p_i > 3, i = 2, 3, 4$.

This case is very unwieldy due to the fact with 2 as one of the prime factors which implies all even integers less than $\frac{N}{2}$ are cusps. We will have a lot of consecutive cusps which we might need circles with radii less than $\frac{1}{2}$. We consider this case in a slightly different way. We consider different sets of circles which are in desecending order of radii. We choose the largest possible set as the boundary arc.

Observe that since $2|N$, it is impossible for $(m, N) = (m + 1, N) = 1$. Therefore s_1 will not occur. If $(m, N) > 1, (m + 1, N) = 1$ then s_2 will occur. Of course s_3 will follow since s_2 and s_3 are symmetrical. If $(m, N) > 1, (m + 1, N) > 1$ then s_4 will occur if in addition $(2m + 1, N) = 1$. s_5 will not occur since $(3m + 1, N) = (3m + 2, N) = 1$ is impossible. From now on we assume $(m, N) > 1, (m + 1, N) > 1, (2m + 1, N) > 1$. We shall list the cases. We first insert a figure on the next page to help us visualize the situation.

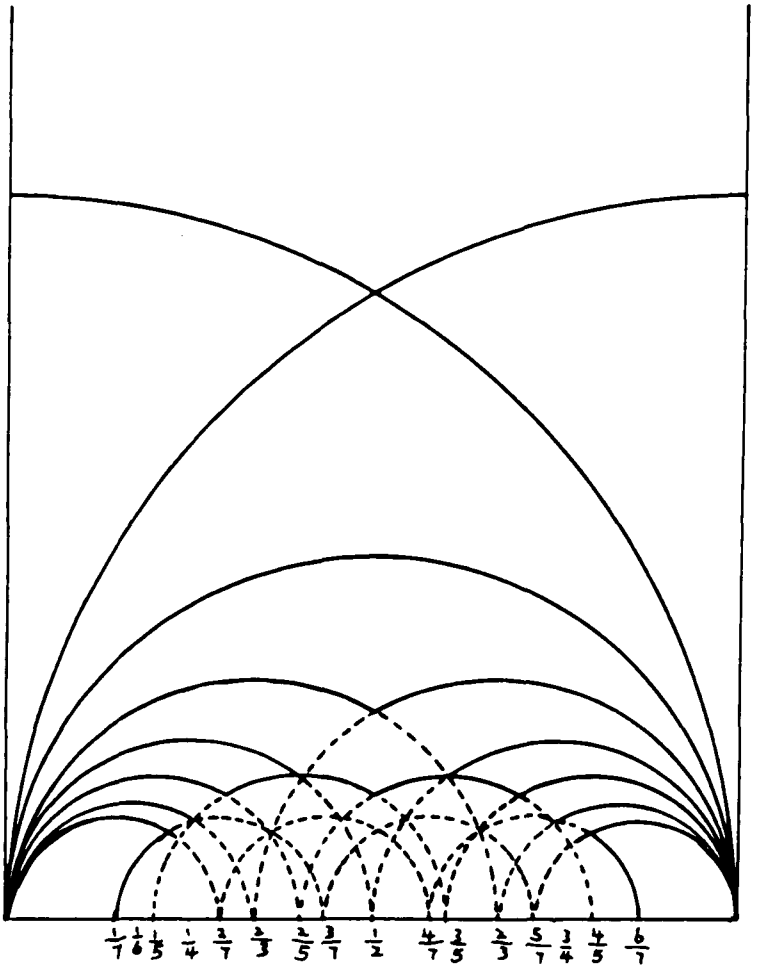

Figure 14: Circles with various radii in the interval $(m, m+1)$

Case 1. $(3m+1, N) = 1, (3m+2, N) > 1$.

If $(4m+3, N) = 1$, then s_7 will occur.

If $(4m+3, N) > 1$, we have:

1a. m is even. Without loss of generality, assume $p_2|m+1, p_3|2m+1$, $p_4|4m+3$. We check that $(3m+1, N) = (5m+3, N) = (6m+5, N) = 1$. Therefore the cirlces centered at $\frac{1}{3}, \frac{3}{5}, \frac{5}{6}$ can cover the interval. We denote them by s_8. We have a complete list of figures of s_i's in the appendix.

1b. m is odd. Observe that $m, m+1, 2m+1, 3m+2$ are pairwise relatively prime. So after reordering of the indices, we have $2|m+1, p_2|m, p_3|2m+1, p_4|3m+2$. Now $(4m+3, N) > 1$, but none of the p_i's can divide $4m+3$ since $p_i \neq 3$. So this case is impossible.

Case 2. $(3m+1, N) > 1, (3m+2, N) = 1$.

If $(4m+1, N) = 1$, then s_7 will occur.

If $(4m+1, N) > 1$, we have:

2a. m is even. Observe that $m, m+1, 2m+1, 3m+1, 4m+1$ are pairwise relatively prime or have common factor 3. By the same argument as in 1b., this is impossible.

2b. m is odd. We find that $(6m+1, N) = (5m+2, N) = (3m+2, N) = 1$, so the circles centered at $\frac{1}{6}, \frac{2}{5}, \frac{2}{3}$ can cover the interval. We denote them by s_9.

Case 3. $(3m+1, N) > 1, (3m+2, N) > 1$.

Assume first m is even.

3a. $(4m+3, N) = 1$. This implies the circles centered at $\frac{1}{4}, \frac{3}{5}, \frac{3}{4}$ can cover the interval. We denote them by s_{10}.

3b. $(4m+3, N) > 1$. Then the circles centered at $\frac{1}{4}, \frac{3}{5}, \frac{5}{6}$ cover the interval. We denote them by s_{11}.

The case when m is odd is symmetric.

3c. $(4m+1, N) = 1$. This implies the circles centered at $\frac{1}{4}, \frac{2}{5}, \frac{3}{4}$ can cover the interval. We denote them by s_{12}.

3d. $(4m+1, N) > 1$. Then the circles centered at $\frac{1}{6}, \frac{2}{5}, \frac{3}{4}$ cover the interval. We denote them by s_{13}.

Now we state the above results as

Theorem 13 *Let $N = 2^{e_1} p_2^{e_2} p_3^{e_3} p_4^{e_4}$, where $p_i > 3$ $i = 2,3,4$ are distinct prime numbers and e_1, e_2, e_3, e_4 are positive integers. Then circles can be found with radius $r \geq \frac{1}{6}$.*

C. $N = 3^{e_1}p_2^{e_2}p_3^{e_3}p_4^{e_4}$ where $p_i > 3, i = 2, 3, 4$.

It is possbible for $(m, N) = (m+1, N) = 1$, so s_1 can be found. Similarly s_2, s_3, s_4 can be found. From now on assume $(m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1$. If $(3m+1, N) = (3m+2, N) = 1$ then s_5 will occur. If not, we have:

Case 1. $(3m+1, N) > 1, (3m+2, N) = 1$.

1a. $3|m$. Without loss of generality we assume $p_2|m+1, p_3|2m+1, p_4|3m+1$. We find that $(4m+1, N) = 1$. So s_6 will occur.

1b. $3|m+1$. we find that $(4m+1, N) > 1, (5m+1, N) = 1$. Therefore the circles centered at $\frac{1}{5}, \frac{2}{3}$ can cover the interval. We denote them by s_{14}.

1c. $3|2m+1$. We find that $(4m+1, N) = 1$. So s_7 will occur.

Case 2. $(3m+1, N) = 1, (3m+2, N) > 1$.

2a. $3|2m+1$ or $3|m+1$. We find that $(4m+3, N) = 1$. So s_6 will occur.

2b. $3|m$. We find that $(4m+3, N) > 1, (5m+4, N) = 1$. Therefore the circles centered at $\frac{1}{3}, \frac{4}{5}$ can cover the interval. We denote them by s_{15}.

Case 3. $(3m+1, N) > 1, (3m+2, N) > 1$.

This is impossible, otherwise we would have too many prime divisors of N.

Now we state the above results as

Theorem 14 *Let $N = 3^{\epsilon_1}p_2^{\epsilon_2}p_3^{\epsilon_3}p_4^{\epsilon_4}$, where $p_i > 3, i = 2, 3, 4$ are distinct prime numbers and $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ are positive integers. Then circles can be found with radius $r \geq \frac{1}{5}$.*

D. $N = 2^{e_1}3^{e_2}p_3^{e_3}p_4^{e_4}$ where $p_i > 3, i = 3, 4$.

Since it is impossible for $(m, N) = (m+1, N) = 1$, s_1 does not occur. As usual, s_2, s_3, s_4 can occur. From now on assume $(m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1$.

Case 1. $(3m+1, N) = 1, (3m+2, N) > 1$.

m must be even. If $(4m+3, N) = 1$ then s_6 will occur.

If $(4m+3, N) > 1$, we subdivide this case:

1a. $3|m+1$ or $3|2m+1$. We find that $(5m+3, N) = (6m+5, N) = 1$. Therefore the circles centered at $\frac{1}{3}, \frac{3}{5}, \frac{5}{6}$ cover the interval. Note that this set is s_8.

1b. $3|4m+3$. We find that $(6m+5, N) = (7m+5, N) = 1$. Therefore the circles centered at $\frac{1}{3}, \frac{5}{7}, \frac{5}{6}$ cover the interval. We denote them by s_{16}.

Case 2. $(3m+1, N) > 1, (3m+2, N) = 1$.

m must be odd. If $(4m+1, N) = 1$, then s_7 can occur. If $(4m+1, N) > 1$ we subdivide this case:

2a. $3|m$ or $3|2m+1$. We find that $(5m+2, N) = (6m+1, N) = 1$. So the circles centered at $\frac{1}{6}, \frac{2}{5}, \frac{2}{3}$ cover the interval. Note that this set is s_9.

2b. $3|4m+1$. We find that $(6m+1, N) = (7m+2, N) = 1$. So the circles centered at $\frac{1}{6}, \frac{2}{7}, \frac{2}{3}$. We denote them by s_{17}.

Case 3. $(3m+1, N) > 1, (3m+2, N) > 1$.

Observe that in this case if m is even, we may assume that $p_2|m+1, p_3|2m+1, p_4|3m+1$ where either p_2 or p_3 is 3. If m is odd, then we may assume $p_2|m, p_3|2m+1, p_4|3m+2$ where either p_2 or p_3 is 3.

3a. $(4m+1, N) = (4m+3, N) = 1$. First assume m is even. Then $2 \nmid 5m+3$. $p_2|m+1$ implies $p_2|5m+5$. Hence $p_2 \nmid 5m+3$. Similarly we find that $p_3 \nmid 5m+3$ and $p_4 \nmid 5m+3$. Hence $(5m+3, N) = 1$. Therefore the circles

centered at $\frac{1}{4}, \frac{3}{5}, \frac{3}{4}$ will cover the interval if m is even. Note that this set is s_{10}. By the same argument the circles centered at $\frac{1}{4}, \frac{2}{5}, \frac{3}{4}$ will cover the interval if m is odd. Note that this set is s_{12}.

3b. $(4m+1, N) > 1, (4m+3, N) = 1$. When m is even, we check that the circles centered at $\frac{1}{5}, \frac{3}{7}, \frac{3}{5}, \frac{3}{4}$ will cover the interval. We denote them by s_{18}. When m is odd, $2|5m+1$ and $2|5m+3$. So we have to pick the circles centered at $\frac{1}{6}, \frac{2}{5}, \frac{3}{4}$. Note that this set is s_{13}.

3c. $(4m+1, N) = 1, (4m+3, N) > 1$. This case is symmetric to 3b. When m is odd, the circles centered at $\frac{1}{4}, \frac{2}{5}, \frac{4}{7}, \frac{4}{5}$ will cover the interval. We denote them by s_{19}. When m is even, we find that the circles centered at $\frac{1}{4}, \frac{3}{5}, \frac{5}{6}$ cover the interval. Note that this set is s_{11}.

3c. $(4m+1, N) > 1, (4m+3, N) > 1$. This case implies p_3 or p_4 is 5. We find that the circles centered at $\frac{1}{5}, \frac{3}{7}, \frac{3}{5}, \frac{5}{6}$ cover the interval if m is even. We denote them by s_{20}.

The circles centered at $\frac{1}{6}, \frac{2}{5}, \frac{4}{7}, \frac{4}{5}$ will cover the interval if m is odd. We denote them by s_{21}.

Now we state the above results as

Theorem 15 *Let $N = 2^{\epsilon_1} 3^{\epsilon_2} p_3^{\epsilon_3} p_4^{\epsilon_4}$, where $p_i > 3, i = 3, 4$, are distinct prime numbers and $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ are postive integers, then circles can be found with radius $r \geq \frac{1}{7}$.*

We have found sets of circles covering the interval $(m, m+1)$ where $|m| \leq \frac{N}{2}$. We take the arcs in the upper half plane as the boundary of the fundamental domain of $\Gamma^o(N)$ where N has four distinct prime factors. As we pointed out in chapter 4, when $(m, N) > 1, (m+1, N) > 1, (2m+1, N) > 1$, no circles with radius $\frac{1}{2}$ will be found. Therefore, we search various circles to cover the interval. If N has only 3 distinct prime factors, then $3m+1$ and

$3m+2$ must be relatively prime to N provided N is odd. If N is even then $2|m, 2|3m+2$ or $2|m+1, 2|3m+1$, the circles with radii $\frac{1}{3}$ is not enough to cover the interval. We consider $4m+1$ and $4m+3$ next. If N has 4 distinct prime factors and $(m, p_1p_2) > 1$, $(m+1, p_3) > 1, (2m+1, p_4) > 1$, this case will behave as if N has 3 prime factors. The most difficult case is when $(m, p_1) > 1, (m+1, p_2) > 1, (2m+1, p_3) > 1$. The last factor p_4 may divide various centers. In general, any circles within the interval $(m, m+1)$ have center at $\frac{rm+t}{r}$ and radius $\frac{1}{r}$, where $0 < t < r$ and $(t, r) = 1$. We observe that $p_i|m, p_i|m+p_i$ simultaneously, $p_i \not| rm+t$ where $t < p_i$. If p_i is big, we have a lot of $rm+t$ relatively prime to p_i. The situtation is more complicated when the p_i's are close to each others, for instance, $2|m, 2|3m+2, 3|m+1, 3|4m+1$ which mean a lot of circles cannot be found. Therefore, if the p_i's are greater than three, the above situtation will not occur and the case turns out to be very simple. Thus no matter which centers p_4 divides it will divide the multiples of the center. Therefore, the more prime factors we have, there are more common factors among the centers. This makes the process of finding the suitable circles more complicated. If N has 5 distinct prime factors and $(m, p_1) > 1, (m+1, p_2) > 1$, $(2m+1, p_3) > 1$, then p_4, p_5 may divide various centers. The number of choices seems to be very large. From past experience, we predict the case may reduce to a simplier form provided all $p_i > 5$. If 2 and 3 are one of the prime factors, then complicated situtation will be expected. Nevertheless, the number of different s_i is bounded by the numbers of primes p_i dividing N. Therefore, the numbers of s_i should be finite. In principle, it can be extended to the case where N is finite and arbitrary. We hope this can be done in the near future.

Appendix

We summarize the results in the following table.

N	Configurations	Centers
$p_1^{e_1}$	s_1	$m, m+1$
	s_2	$m+1$
	s_3	m
$p_1^{e_1}p_2^{e_2}$	s_1, s_2, s_3	as above
	s_4	$\frac{2m+1}{2}$
$p_1^{e_1}p_2^{e_2}p_3^{e_3}$ (odd)	s_1, s_2, s_3, s_4	as above
	s_5	$\frac{3m+1}{3}, \frac{3m+2}{3}$
$2^{e_1}p_2^{e_2}p_3^{e_3}$ (even)	$s_2, s_3, s_4,$	as above
	s_6	$\frac{3m+1}{3}, \frac{4m+3}{4}$
	s_7	$\frac{3m+2}{3}, \frac{4m+1}{4}$
$p_1^{e_1}p_2^{e_2}p_3^{e_3}p_4^{e_4}, p_i > 3$	$s_1, s_2, s_3, s_4, s_5, s_6, s_7$	as above
$2^{e_1}p_2^{e_2}p_3^{e_3}p_4^{e_4}$	s_2, s_3, s_4, s_6, s_7	as above
	s_8	$\frac{3m+1}{3}, \frac{5m+3}{5}, \frac{6m+5}{6}$
	s_9	$\frac{6m+1}{6}, \frac{5m+2}{5}, \frac{3m+2}{3}$
	s_{10}	$\frac{4m+1}{4}, \frac{5m+3}{5}, \frac{4m+3}{4}$
	s_{11}	$\frac{4m+1}{4}, \frac{5m+3}{5}, \frac{6m+5}{6}$
	s_{12}	$\frac{4m+1}{4}, \frac{5m+2}{5}, \frac{4m+3}{4}$
	s_{13}	$\frac{6m+1}{6}, \frac{5m+2}{5}, \frac{4m+3}{4}$
$3^{e_1}p_2^{e_2}p_3^{e_3}p_4^{e_4}$	$s_1, s_2, s_3, s_4, s_5, s_6, s_7$	as above
	s_{14}	$\frac{5m+1}{5}, \frac{3m+2}{3}$
	s_{15}	$\frac{3m+1}{3}, \frac{5m+4}{5}$
$2^{e_1}3^{e_2}p_3^{e_3}p_4^{e_4}$	$s_2, s_3, s_4, s_6, s_7, s_8$	as above
	$s_9, s_{10}, s_{11}, s_{12}, s_{13}$	as above
	s_{16}	$\frac{3m+1}{3}, \frac{7m+5}{7}, \frac{6m+5}{6}$
	s_{17}	$\frac{6m+1}{6}, \frac{7m+2}{7}, \frac{3m+2}{3}$
	s_{18}	$\frac{5m+1}{5}, \frac{7m+3}{7}, \frac{5m+3}{5}, \frac{4m+3}{4}$
	s_{19}	$\frac{4m+1}{4}, \frac{5m+2}{5}, \frac{7m+4}{7}, \frac{5m+4}{5}$
	s_{20}	$\frac{5m+1}{5}, \frac{7m+3}{7}, \frac{5m+3}{5}, \frac{6m+5}{6}$
	s_{21}	$\frac{6m+1}{6}, \frac{5m+2}{5}, \frac{7m+4}{7}, \frac{5m+4}{5}$

Table 4: Summary of results

We give a complete list of figures on the following pages.

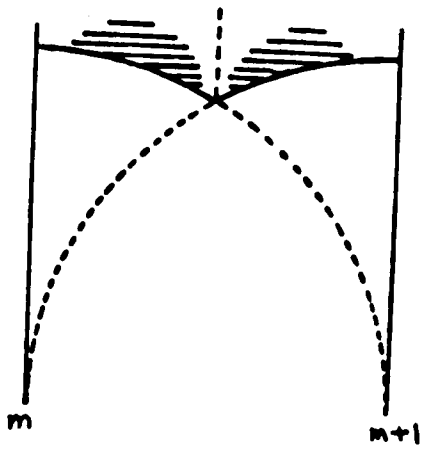

Figure 15: Configuration s_1

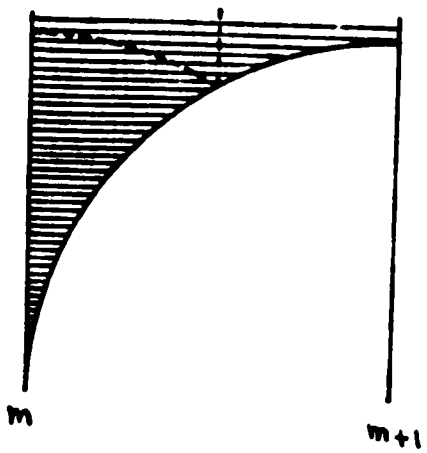

Figure 16: Configuration s_2

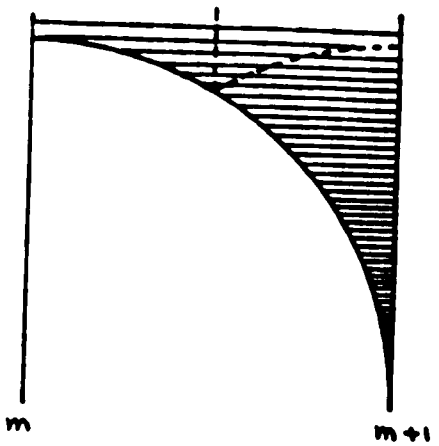

Figure 17: Configuration s_3

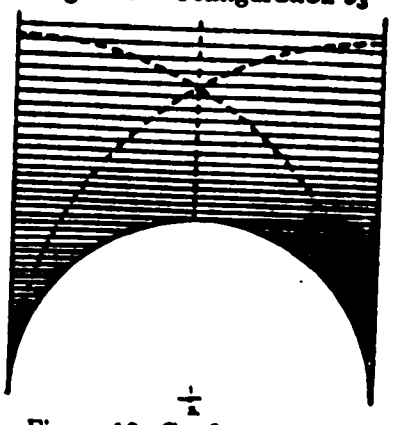

Figure 18: Configuration s_4

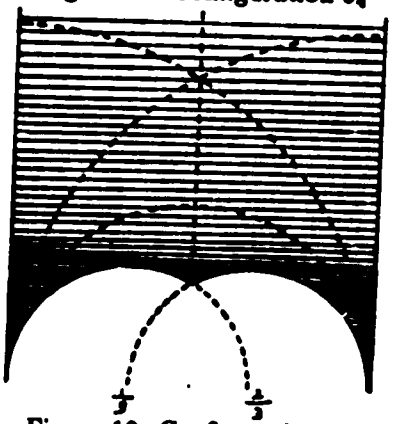

Figure 19: Configuration s_5

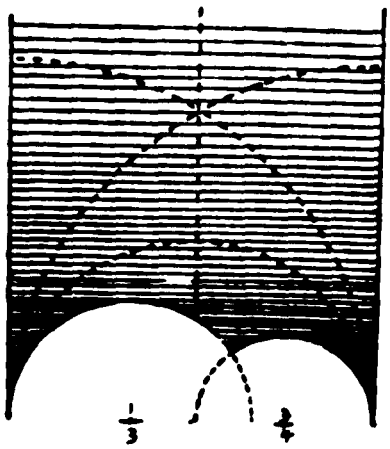

Figure 20: Configuration s_6

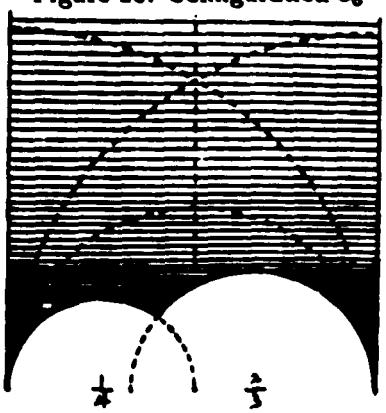

Figure 21: Configuration s_7

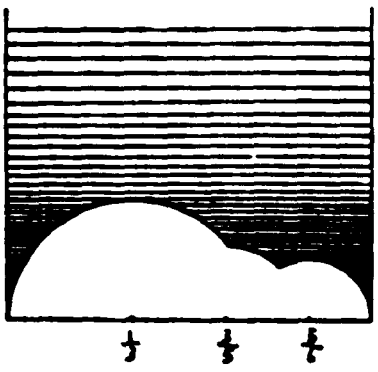

Figure 22: Configuration s_8

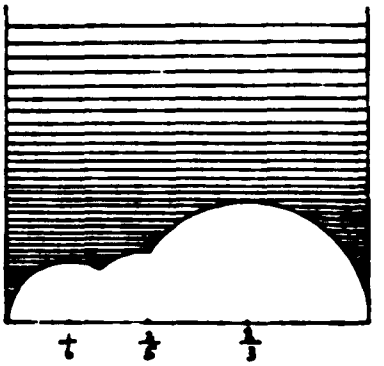

Figure 23: Configuration s_9

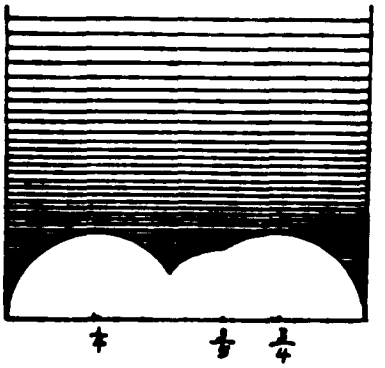

Figure 24: Configuration s_{10}

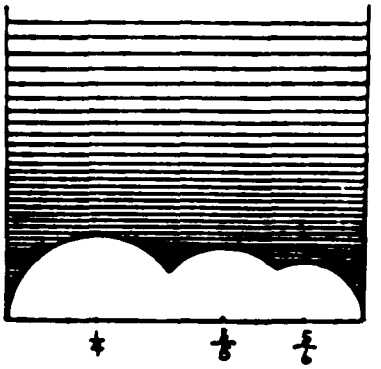

Figure 25: Configuration s_{11}

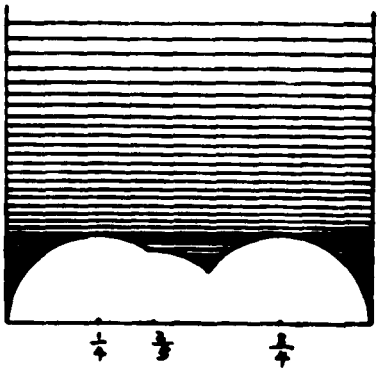

Figure 26: Configuration s_{12}

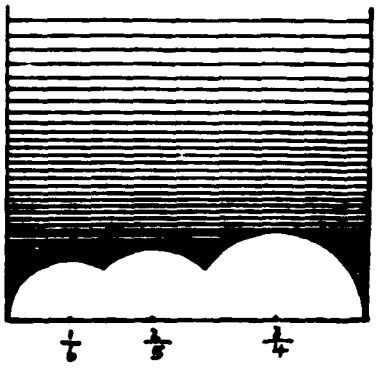

Figure 27: Configuration s_{13}

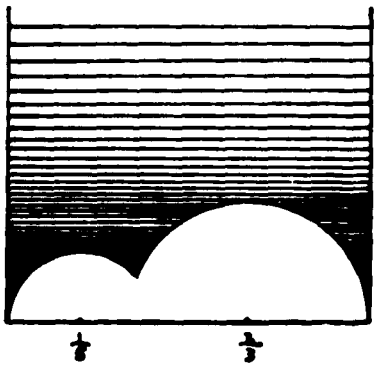

Figure 28: Configuration s_{14}

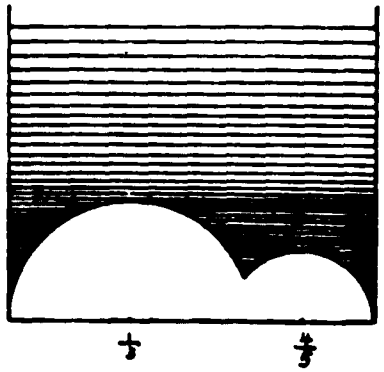

Figure 29: Configuration s_{15}

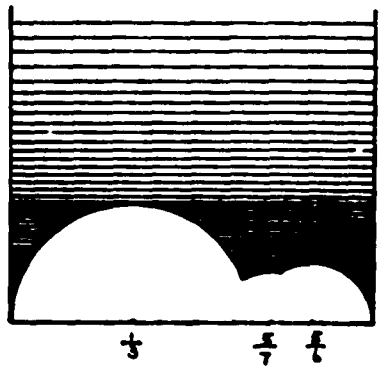

Figure 30: Configuration s_{16}

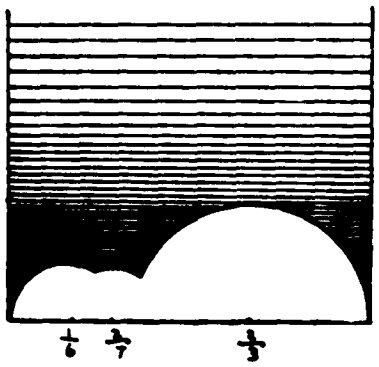

Figure 31: Configuration s_{17}

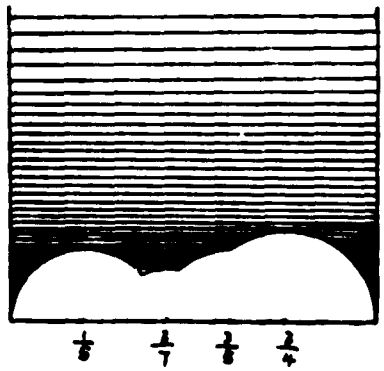

Figure 32: Configuration s_{18}

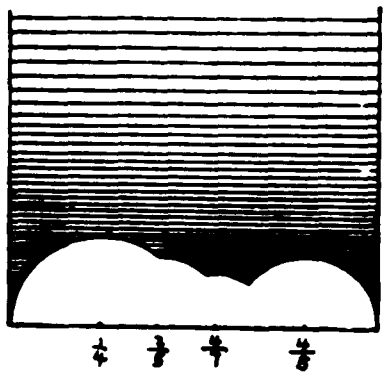

Figure 33: Configuration s_{19}

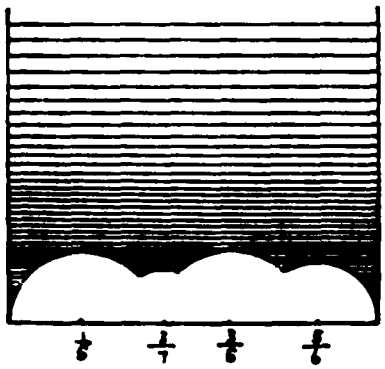

Figure 34: Configuration s_{20}

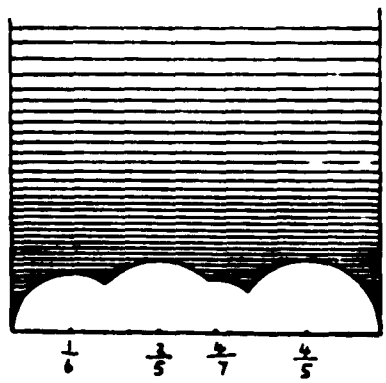

Figure 35: Configuration s_{21}

References

[1] A. Beardon, *The Geometry of Discrete Groups*, Grad. Texts in Math., Vol.91 Springer-Verlag, Berlin New York. (1983)

[2] H. Cohn, *Computation of Singular Moduli by Multi-valued Modular Equations*, to appear Proc. Conference, Debrecen. (1989)

[3] H. Cohn, *Singular Moduli and Modular Equations for Fricke's Cases*, Proceedings of Symposia in Pure Mathematics, Vol. 49, Part 2. (1989) 233-249

[4] L. Ford, *Automorphic Functions*, Chelsea Publishing Company, New York. (1951)

[5] R. Fricke, *Die Elliptischen Funktionen und ihre Anwendungen*, Part II, Teubner. (1922).

[6] R. Kulkarni, *An Arithmetic-Geometric Method in the Study of the Subgroups of the Modular Group*, Preprint.

[7] J. Lehner, *Discontinuous Groups and Automorphic Fuctions*, American Mathematical Society, Providence. (1964)

[8] J. Lehner, *A Short Course in Automorphic Functions*, Holt, Rinehart and Winston. New York. (1965)

[9] B. Maskit, *Kleinian groups*, Springer-Verlag. Berlin New York. (1988)

[10] J. Nielsen, *A Study Concerning the Congruence Subgroups of the Modular Group*, Danske Vid. Selsk, Mat. Phys. Medd. 25. (1950)

[11] H. Poincaré, *Oeuvres*, Vol. 2, Gauthiers-Villars, Paris. (1916)

[12] H. Poincaré, *Oeuvres*, Vol. 3, Gauthiers-Villars, Paris. (1934)

[13] B. Schoeneberg, *Elliptic Modular Functions*, Die Grundlehren der Math. Wissen., Vol.203, Springer-Verlag. Berlin New York. (1974)

[14] D. Zagier, *Modular Parametrizations of Elliptic Curves*, Canad. Math. Bull. 28 (1985) 372-384