

THE SHAPE OF THE FORD DOMAINS FOR $\Gamma_0(N)$

ANTONIO LASCURAIN ORIVE

ABSTRACT. This is a second paper on the Ford domains for the Hecke congruence subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}.$$

The author establishes techniques to calculate the number of sides of these domains; in the process the shape of such polygons becomes apparent in many cases. Explicit formulas are given for numbers which have no more than four prime factors. The main result (**Theorem 1**) exhibits the existence of a *universal* symmetric polynomial which evaluated at p_1, p_2, \dots, p_r yields the number of finite vertices of the Ford polygon for $\Gamma_0(N)$, for all numbers $N = p_1 p_2 \cdots p_r$ whose prime factors are larger than a constant which depends only on r . In all cases the formulas are in terms of symmetric polynomials which generalize the Euler ϕ function. The techniques developed to count the number of *visible* isometric circles show that the study of these circles might also be a useful tool to simplify or solve problems in number theory.

1. INTRODUCTION

The classical modular group $SL(2, \mathbb{Z})$ and its subgroups of finite index play an important role in many branches of mathematics, especially in number theory. A particularly important class consists of the Hecke congruence subgroups of level N

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}.$$

These subgroups might also be useful in the study of the structure of the rings \mathbb{Z}_N .

Hyperbolic geometry provides a great deal of information about these groups, for instance, in the construction of fundamental domains. In the specific case of $\Gamma_0(N)$, these regions were first studied in the simplest cases, that is when N is a prime number, by Fricke [4] and later by Zagier [9]. Recently, a more general study was developed independently by Kulkarni [5] and the author [6], [7]. Kulkarni constructed fundamental domains which have the least number of sides, though they are not Ford polygons. In [7] the Ford domains are studied; one of the main results (Theorem 3) is that given N , if \bar{N} denotes the square free part of N and $\rho = \frac{N}{\bar{N}}$, then the Ford polygon for $\Gamma_0(N)$ is basically ρ copies of the Ford polygon for $\Gamma_0(\bar{N})$. Some other statements are about parabolic and elliptic vertices and cycles.

This paper describes some aspects of the combinatorial structure of the Ford polygons for $\Gamma_0(N)$, principally the calculation of the number of sides of these

Received by the editors February 1, 1998 and, in revised form, November 23, 1998.
1991 *Mathematics Subject Classification*. Primary 11F06, 20H10, 22E40, 30F35, 51M10.

©1999 American Mathematical Society

domains (**Corollaries** 2 and 3). The main result (**Theorem** 1) exhibits the existence of a *universal* symmetric polynomial which evaluated at p_1, p_2, \dots, p_r yields the number of finite vertices of the Ford polygon for $\Gamma_0(N)$, for all numbers $N = p_1 p_2 \cdots p_r$ whose prime factors are larger than a constant which depends only on r . More results on the number of different kinds of sides obtained by symmetric polynomials are given in **Propositions** 1, 3, 4 and 5. All these statements can be generalized to non-square free numbers (see Theorem 3 in [7]).

These symmetric polynomials, which are generalizations of the Euler ϕ function, are not only very useful to describe the different kinds of isometric circles, they are also interesting from an algebraic viewpoint (**Lemmas** 1, 2, 3 and **Proposition** 6). The methods developed show an intrinsic relation between the isometric circles for $\Gamma_0(N)$ and a family of circles which is in a one to one correspondence with the rational numbers in the unit interval (see Figures 3, 4 and 5 in Section 2). In the last section a definition of a *distance* between any two of these circles is introduced; this apparently geometric concept is actually rather algebraic in character and can be used to compare the prime decompositions of arithmetic progressions (see **Proposition** 7 and the proof of **Theorem** 1).

The general spirit of the paper is that number theory provides a lot of information about the isometric circles and consequently the Ford polygons, and conversely that geometry appears as a powerful tool to study number theoretical problems.

I would like to thank Troels Jørgensen for encouraging me to work on this beautiful part of mathematics.

2. PRELIMINARIES

Let $\bar{\Gamma}_0(N)$ be the group of transformations determined by $\Gamma_0(N)$; we will write $\bar{g} \in \bar{\Gamma}_0(N)$ whenever $g \in \Gamma_0(N)$. These Fuchsian groups act in

$$\mathbb{H}^2 = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$$

as hyperbolic isometries. Moreover, for all numbers N , $\bar{\Gamma}_0(N)$ contains as a subgroup, the translation group generated by the transformation $z \mapsto z + 1$. This subgroup has as a fundamental region the infinite rectangle

$$R_\infty = \{z \in \mathbb{H}^2 \mid 0 < \text{Re } z < 1\}.$$

Given \bar{g} a Möbius transformation, which is not a Euclidean similarity, there exists a unique circle in the complex plane where the action of \bar{g} is Euclidean. This circle is called the isometric circle of \bar{g} (it is also called the isometric circle of g , where $g \in SL(2, \mathbb{C})$ determines \bar{g}). Analytically, this circle which we will denote by $I(\bar{g})$ or $I(g)$ is determined by

$$\{z \in \mathbb{C} \mid |\bar{g}'(z)| = 1\}.$$

Let $\text{ext } I(\bar{g})$ denote the unbounded component of $\mathbb{C} - I(\bar{g})$ and $\text{int } I(\bar{g})$ the bounded component. The chain rule implies that $\bar{g}(\text{ext } I(\bar{g})) = \text{int } I(\bar{g}^{-1})$. Certainly, one also has that $\bar{g}(\text{int } I(\bar{g})) = \text{ext } I(\bar{g}^{-1})$. On the other hand, the derivative formula shows that if

$$g \in SL(2, \mathbb{Z}), \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

$I(g)$ has Euclidean center at $\frac{-d}{c}$ and Euclidean radius $\frac{1}{|c|}$. In particular, if $g \in SL(2, \mathbb{R})$, the isometric circle of g is orthogonal to the real axis; so it determines a geodesic in \mathbb{H}^2 , which is also called the isometric circle of g . To avoid a cumbersome notation $I(\bar{g})$ (or $I(g)$) will also denote this geodesic.

Definition. Let Γ be a discrete subgroup of $SL(2, \mathbb{R})$ such that $\bar{\Gamma}$ contains as a subgroup the group of translations generated by $z \mapsto z + 1$. Then the Ford polygon for Γ is the set

$$R_\infty \cap \bigcap_{g \in \Gamma} \text{ext } I(g).$$

This is a fundamental region for the action of $\bar{\Gamma}$ in \mathbb{H}^2 . If Γ is finitely generated, this is a finite sided convex hyperbolic polygon, bounded by two vertical lines and a finite number of geodesic arcs (see [1] or [2]). Our groups of interest $\Gamma_0(N)$ are certainly finitely generated (see [3], [8] or [9]). We will denote by R_N their Ford polygons.

Since

$$\begin{pmatrix} * & * \\ kN & -t \end{pmatrix} \in \Gamma_0(N) \iff \begin{pmatrix} * & * \\ kN & -(kN - t) \end{pmatrix} \in \Gamma_0(N),$$

R_N is symmetric with respect to the line

$$\left\{ z \in \mathbb{H}^2 \mid \text{Re } z = \frac{1}{2} \right\}.$$

We will be using certain properties of the polygons R_N that are derived in [7]; principally, Theorem 3 states that: given N any natural number, if \bar{N} denotes its square free part and $\rho = \frac{N}{\bar{N}}$, then one has that

$$\bar{R}_N = \bigcup_{m=0}^{\rho-1} \bar{M}_{\frac{1}{\rho}} \bar{T}^m(\bar{R}_{\bar{N}}),$$

where $\bar{T}(z) = z + 1$, $\bar{M}_{\frac{1}{\rho}}(z) = \frac{z}{\rho}$ and $\bar{R}_{\bar{N}}$, \bar{R}_N denote the Euclidean closures in the complex plane of $R_{\bar{N}}$ and R_N respectively. This result will allow us to work exclusively with square free numbers, since the combinatorial structure of R_N (number of sides, vertices, etc.) is basically that one of $R_{\bar{N}}$ repeated ρ times. In Figure 1, one sees that R_9 is R_3 repeated 3 times.

Elliptic and parabolic vertices of R_N are also discussed in [7]. It is proved that the parabolic vertices of R_N are 0, the point at infinity and the points of the form $\frac{t}{N}$, $(t, N) > 1$, where $t \in \{1, 2, 3, \dots, N\}$. Therefore R_N has $N - \phi(N) + 2$ parabolic vertices, where ϕ denotes the Euler function. In particular, if $N = p_1 p_2 \cdots p_r$, the number of parabolic vertices is given by

$$p_1 p_2 \cdots p_r - \prod_{j=1}^r (p_j - 1) + 2.$$

Observe that this expression may be thought of as a symmetric polynomial in r variables. Another result in [7] says that $\frac{t_1}{N}$, $\frac{t_2}{N}$ are $\bar{\Gamma}_0(N)$ -equivalent parabolic vertices if and only if

- i) $(t_1, N) = (t_2, N) = d$,
- ii) $\frac{t_1}{d} \equiv \frac{t_2}{d} \pmod{\left(d, \frac{N}{d}\right)}$.

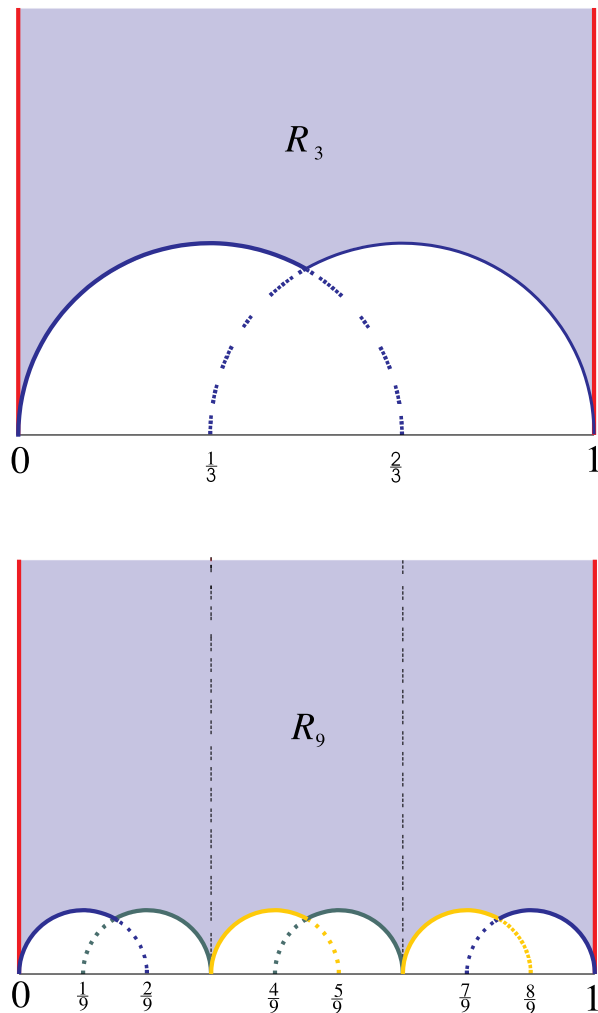


FIGURE 1. The Ford polygons for $\Gamma_0(3)$ and $\Gamma_0(9)$.

These methods also imply the formula for the number of cusps (equivalence classes of the action of $\bar{\Gamma}_0(N)$ in the Riemann sphere)

$$\sum_{d|N, d>0} \phi\left(\left(d, \frac{N}{d}\right)\right).$$

In relation to finite fixed points, it is proved in [7] that each elliptic cycle of order two of R_N is represented by a single vertex with coordinates

$$\frac{t}{N} + \frac{i}{N}, \quad 1 < t < N, \quad t^2 \equiv -1 \pmod{N}.$$

And vice versa, for each solution of the previous equation in \mathbb{Z}_N there is an elliptic vertex of order two. Since these fixed points belong to exactly one arc of R_N , one may not count them as vertices; in the present paper it will be convenient to do so. Elliptic vertices of order three will also appear in cycles of length one, and there

are as many as the square roots of -3 in the ring \mathbb{Z}_N . In fact they are the points

$$\frac{2t+1}{2N} + \frac{\sqrt{-3}}{2N}i, \quad t(t+1) = -1 \quad \text{in } \mathbb{Z}_N, \quad 1 < t < N$$

(see [7], Lemma 2 and Proposition 2). In this paper, we will consider these fixed points as any other vertices of R_N . The formulas to be exhibited will give the number of all vertices, either if they are fixed points (not of order two), or if they are accidental.

It is well known that if $N = 2^r p_1^{r_1} \cdots p_m^{r_m}$, where $p_j \equiv 1 \pmod{4}$, $j = 1, 2, \dots, m$, the number of conjugacy classes of subgroups of order two in $\bar{\Gamma}_0(N)$ is 2^m , and that for other numbers with a different prime decomposition there are no elements of order two (see for example [8] or [9]). A similar result holds for elements of order three, however, as we have just mentioned, we will not use these estimates.

The isometric circles defined by $\Gamma_0(N)$ have Euclidean radii of the form $\frac{1}{nN}$, $n \in \mathbb{N}$, we will call them *n-circles*; in particular, when they are visible (that is, if they contain an arc of positive length which is also a subset of ∂R_N), the corresponding arcs will be called *n-sides*. Hence, a side of R_N is either a vertical line or an *n-side*.

We make some other remarks about the isometric circles defined by $\Gamma_0(N)$.

1) *Points of the form $\frac{t}{N}$, $t \in \mathbb{Z}$, are not the Euclidean centers of n-circles, $n > 1$.* This follows because given a matrix

$$\begin{pmatrix} * & * \\ nN & s \end{pmatrix} \in \Gamma_0(N),$$

the center of $I(g)$ is $\frac{-s}{nN}$. Hence, if $\frac{t}{N} = \frac{-s}{nN}$, n is a factor of s , but $(n, s) = 1$, so $n = 1$.

2) *The center of any n-circle C lies in the closure of the non-bounded component of $\mathbb{C} - D$, for any other n-circle D.* Rescaling and translating, this remark is clear from Figures 3, 4 and 5.

3) *A rational point of the form $\frac{t}{N}$, $t \in \mathbb{Z}$, lies in the closure of the non-bounded component of $\mathbb{C} - D$, for any n-circle D, $n > 1$.* This follows from remarks 1) and 2).

4) *n-circles are contained in the region $\{z \in \mathbb{C} \mid \text{Im } z \leq \frac{1}{2N}\}$.* Rescaling and translating, this is clear from Figures 3, 4 and 5.

5) *∂R_N intersects the subrectangles*

$$S_t = \left\{ z \in \mathbb{H}^2 \mid \frac{t}{N} \leq \text{Re } z \leq \frac{t+1}{N} \right\}, \quad t \in \{0, 1, \dots, N-1\},$$

in four different ways:

- a) *In two 1-sides with Euclidean centers at $\frac{t}{N}$, $\frac{t+1}{N}$ respectively.*
- b) *In a 1-side with Euclidean center at $\frac{t}{N}$ or at $\frac{t+1}{N}$.*
- c) *In a 2-side with Euclidean center at $\frac{2t+1}{2N}$.*
- d) *In a collection of arcs contained in isometric circles of radius smaller than $\frac{1}{2N}$.*

This last remark follows from the previous four (see also Figure 2). Observe that since

$$\begin{pmatrix} * & * \\ N & -1 \end{pmatrix} \in \Gamma_0(N),$$

1-sides always exist.

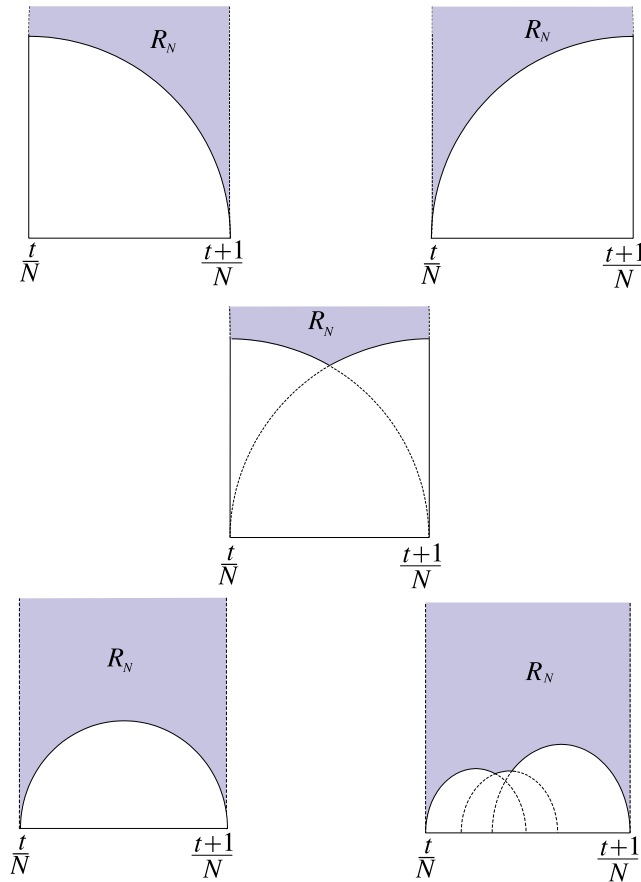


FIGURE 2. The different ways R_N intersects the rectangles S_t according to remark 5.

The location of parabolic vertices and the way that isometric circles appear, as described in the previous remarks, show that the geometric structure of the polygons R_N is determined by a parameter $t \in \{0, 1, \dots, N-1\}$ which subdivides the region R_∞ into N subrectangles. Cases a), b) and c) (1-sides, 2-sides) are the simplest and are fully described in the next section. Case d) is more complex, in fact it only arises when N is divisible by more than two primes. This follows because a prime number can only be a divisor of no more than one of the integers t , $t+1$, $2t+1$, where $t \in \mathbb{N}$; and consequently if $N = p_1 p_2$, one of the matrices

$$\begin{pmatrix} * & * \\ N & -t \end{pmatrix}, \quad \begin{pmatrix} * & * \\ N & -(t+1) \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} * & * \\ 2N & -(2t+1) \end{pmatrix}$$

belong to $\Gamma_0(N)$. Certainly, numbers with many prime factors in their decomposition define more complex polygons than others with less prime factors.

In order to study more carefully the collection of isometric circles for $\Gamma_0(N)$, we define another family of semicircles. Given $m \in \mathbb{N}$ or $m = 0$ and $n \in \mathbb{N}$, H_n^m will denote the semicircle in \mathbb{H}^2 of radius $\frac{1}{n}$ and center at $\frac{m}{n}$. We choose some of

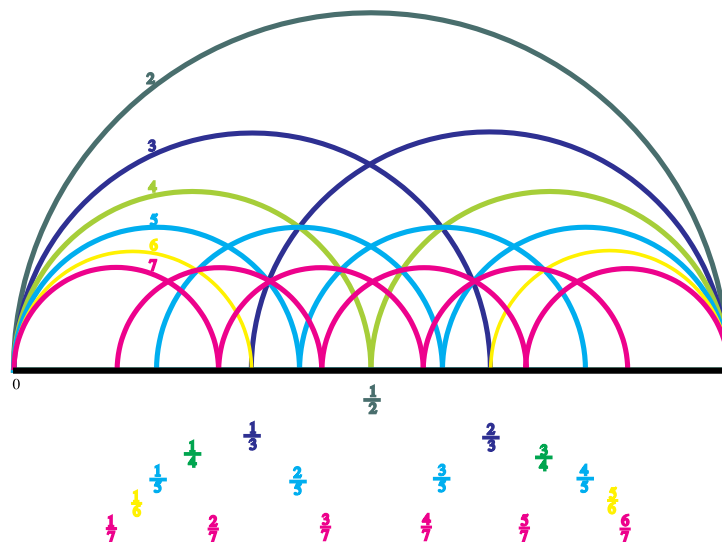


FIGURE 3. The subset of G defined by the semicircles in the family Φ of radius $1/2, 1/3, 1/4, 1/5, 1/6, 1/7$.

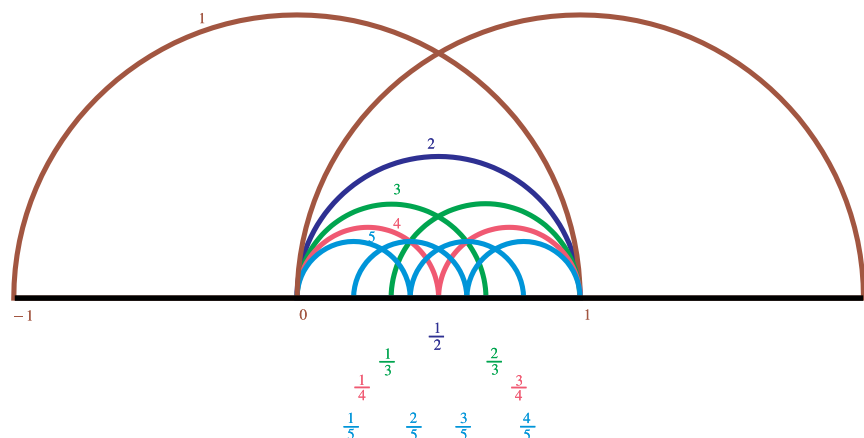


FIGURE 4. The subset of G defined by the semicircles in the family Φ of radius $1, 1/2, 1/3, 1/4, 1/5$.

these semicircles to define a family Φ consisting of all semicircles H_n^m satisfying the following two conditions:

- i) $1 \leq m < n, \quad (m, n) = 1.$
- ii) $m = 0$ and $n = 1$, or $m = 1$ and $n = 1$.

The underlying space of the family Φ in \mathbb{H}^2 will be denoted by G (see Figures 3, 4 and 5).

Remarks 1) through 5) show that given any matrix

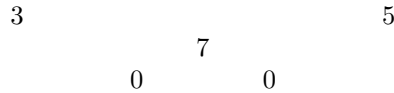
$$\begin{pmatrix} * & * \\ nN & -u \end{pmatrix} \in \Gamma_0(N),$$

The relevance of this array is due to the fact that $(nt + m, N) = 1$ if and only if

$$\begin{pmatrix} * & * \\ nN & -(nt + m) \end{pmatrix} \in \Gamma_0(N),$$

where $(n, m) = 1$. This remark means that the circle with center at $\frac{t}{N} + \frac{m}{nN}$ and radius $\frac{1}{nN}$ is isometric for $\Gamma_0(N)$ if and only if the prime factors of N do not appear in the prime decomposition of $nt + m$. However, this definition does not depend on N .

When working with an specific number N , we will replace the labels $nt + m$ in the S_t -*diagram* and put instead the prime divisors of N , together with the symbol 0, signifying the existence of an isometric circle in that spot; for example, if $N = 3 \cdot 5 \cdot 7$ and $t = 24$, one has that $3 \mid t$, $5 \mid t + 1$ and $7 \mid 2t + 1$, but $((3t + 1)(3t + 2), N) = 1$. This data implies that ∂R_N intersects S_t in two *3-sides* (see Figure 6). To establish this distribution of isometric circles we define the following diagram:



It will mean that for a number $t \in \{0, 1, \dots, N - 1\}$, there are no isometric circles centered at $\frac{t}{N}$, $\frac{t+1}{N}$ and $\frac{2t+1}{2N}$, because 3, 5 and 7 are divisors of t , $t + 1$ and $2t + 1$ respectively; but since $((3t + 1)(3t + 2), N) = 1$, there are two *3-sides* in the rectangle S_t , and all other *n-circles*, $n > 3$ in that rectangle are non-visible (see

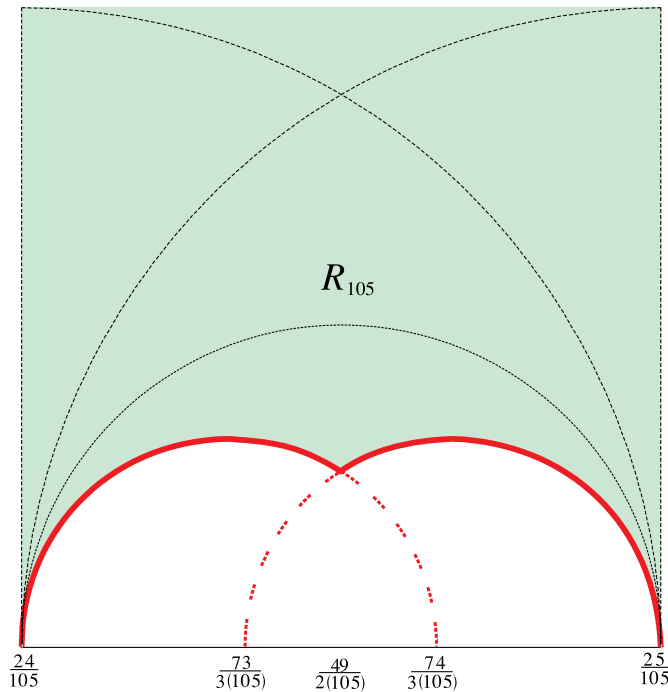


FIGURE 6. The intersection of the Ford polygon defined by $\Gamma_0(105)$ and the rectangle determined by $24/105$, $25/105$ and the point at infinity.

Figures 3, 4 and 5). An S_t -diagram with this modification will be called an *adapted S_t -diagram*.

3. 1-SIDES, 2-SIDES

From now on, all the numbers N to be discussed in relation with $\Gamma_0(N)$ will be square free. As we mentioned before, all our results can be generalized to non-square free numbers. We begin this section with a lemma which might be well known, however, as a reference was not found, we include a proof.

Lemma 1. *Let $N = p_1 p_2 \cdots p_r$ and a_2, a_3, \dots, a_m be such that $0, a_2, a_3, \dots, a_m$ represent different classes in \mathbb{Z}_{p_i} for all $i \in \{1, 2, \dots, r\}$, then the number of integers t , strictly between 0 and N , relatively prime to N , for which also $t + a_j$ is relatively prime to N , $j = 2, 3, \dots, m$ equals*

$$\prod_{i=1}^r (p_i - m).$$

We may think of this expression as a polynomial on r variables; it will be denoted by $\sigma_m(p_1, p_2, \dots, p_r)$, or $\sigma_m(N)$, or simply σ_m .

Proof. The proof is by induction on the number of prime divisors of N . If N is a prime number, say $N = p$, one writes the following array of classes in \mathbb{Z}_p

$$\begin{array}{cccc} \overline{0} & \overline{0 + a_2} & \cdot & \overline{0 + a_m} \\ \overline{1} & \overline{1 + a_2} & \cdot & \overline{1 + a_m} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \hline \overline{p-1} & \overline{p-1 + a_2} & \cdot & \overline{p-1 + a_m}. \end{array}$$

Each column has exactly one class which is zero, moreover, since each row is made up of different classes, $p - m$ rows do not contain the zero class, and the lemma follows for this case.

For the general case let $M = p_1 p_2 \cdots p_{r-1}$, by induction there are

$$\prod_{j=1}^{r-1} (p_j - m)$$

integers t in $\{1, 2, \dots, M\}$ such that $(t(t + a_2) \cdots (t + a_m), M) = 1$. For such integers t one considers the following array of classes, now in \mathbb{Z}_{p_r}

$$\begin{array}{cccc} \overline{t} & \overline{t + a_2} & \cdot & \overline{t + a_m} \\ \overline{t + M} & \overline{t + M + a_2} & \cdot & \overline{t + M + a_m} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \hline \overline{t + (p_r - 1)M} & \overline{t + (p_r - 1)M + a_2} & \cdot & \overline{t + (p_r - 1)M + a_m}. \end{array}$$

Again, since each column has exactly one class which is zero and the rows are made up of different classes, there are $p_r - m$ rows which do not contain the zero

class. The lemma follows now from the following two facts:

i) Any number $u \in \{1, 2, \dots, N - 1\}$ such that $u, u + a_2, \dots, u + a_m$ are coprime with N , can be written as $t + kM$, where t is as above.

ii) For all $k_1, k_2 \in \mathbb{Z}$,

$$t_1 \equiv t_2 \pmod{M} \iff t_1 + k_1M \equiv t_2 + k_2M \pmod{M}.$$

□

Some of the techniques used in this paper will arise from this lemma. Now we discuss 1-sides. Observe that since $(t, N) = 1$ if and only if

$$\begin{pmatrix} * & * \\ N & -t \end{pmatrix} \in \Gamma_0(N),$$

R_N has $\phi(N)$ 1-sides.

Definition. A 1-side is called of type 0, 1 or 2, if it contains 0, 1 or 2 parabolic vertices.

Remark 1) in the preliminaries implies that these cases arise precisely when there are 3, 2 or 1 consecutive integers relatively prime with N . In particular, when N is even all 1-sides are of type 2, because $(t, N) = 1$ implies that $t - 1$ and $t + 1$ are even. Moreover, the number of 1-sides is precisely σ_1 (see Figure 7).

Proposition 1. If N is odd, the number of 1-sides of R_N of type 0, 1 or 2 is given by $\sigma_3, 2(\sigma_2 - \sigma_3)$ and $\sigma_1 - 2\sigma_2 + \sigma_3$, respectively.

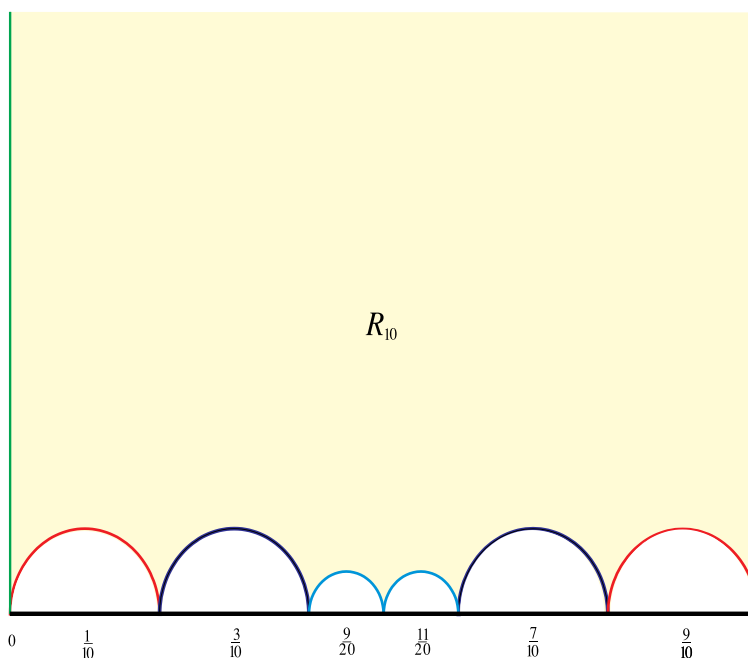


FIGURE 7. The Ford polygon for $\Gamma_0(10)$.

Proof. We calculate the number of 1-sides of type 2, the other cases may be calculated in a similar way. The result follows from **Lemma 1**, because the number $\sigma_1 - 2\sigma_2 + \sigma_3$ may be interpreted as follows:

$$\begin{aligned} & \# \{t \in \{1, 2, 3, \dots, N-1\} \mid (t, N) = 1\} \text{ minus} \\ & \# \{t \in \{1, 2, 3, \dots, N-1\} \mid (t, N) = 1, (t+1, N) = 1\} \text{ minus} \\ & \# \{t \in \{1, 2, 3, \dots, N-1\} \mid (t, N) = 1, (t-1, N) = 1\} \text{ plus} \\ & \# \{t \in \{1, 2, 3, \dots, N-1\} \mid (t, N) = 1, (t-1, N) = 1, (t+1, N) = 1\}. \quad \square \end{aligned}$$

Corollary 1. *The number of finite vertices of R_N contained in 1-sides is given by $\sigma_2(N)$.*

Proof. It follows from the remarks in the preliminaries that these vertices have imaginary part $\frac{\sqrt{3}}{2N}$ and belong to exactly two 1-sides. To calculate the number of these vertices we count the number of 1-sides which appear on the right of them, those of type 0 are σ_3 and those of type 1 are $\sigma_2 - \sigma_3$. \square

In order to get a more detailed description of 1-sides, we introduce the following definition which describes the way in which they are distributed.

Definition. An m -block is a collection of m 1-sides determined by a fixed number $t \in \{0, 1, 2, \dots, N-1\}$ such that

- i) the Euclidean centers of their corresponding isometric circles are $\frac{t+k}{N}$, $k \in \{1, 2, \dots, m\}$,
- ii) $\frac{t}{N}$ and $\frac{t+m+1}{N}$ are parabolic vertices of R_N .

When N is a prime number, R_N consists precisely of two vertical lines and an $(N-1)$ -block. In Figure 1 this situation is described for $N = 3$. Moreover, for numbers which are powers of prime numbers the blocks are repeated, as one sees in Figure 1 for $N = 9$. The general case is described in the following result.

Proposition 2. *Let $N = p_1 p_2 \cdots p_r$, $p_1 < p_2 < \cdots < p_r$, then R_N has the following number of m -blocks:*

$$\begin{array}{ll} 0 & \text{if } m \geq p_1, \\ \sigma_m & \text{if } m = p_1 - 1, \\ \sigma_m - 2\sigma_{m+1} & \text{if } 1 \leq m = p_1 - 2, \\ \sigma_m - 2\sigma_{m+1} + \sigma_{m+2} & \text{if } 1 \leq m < p_1 - 2. \end{array}$$

Proof. The first case is clear; the second is a direct application of **Lemma 1**, and the other cases are proved by induction on $p_1 - m$. The basic idea is that one may count the number of m -blocks knowing the number of larger blocks, for instance, for each $m+1$ -block there are two m -blocks, etc. For this purpose one writes

$$\begin{aligned} \sigma_m = & \begin{array}{l} (p_1 - 1 - m) \quad (\sigma_{p_1-1}) \\ + (p_1 - 2 - m) \quad (\sigma_{p_1-2} - 2\sigma_{p_1-1}) \\ + (p_1 - 3 - m) \quad (\sigma_{p_1-3} - 2\sigma_{p_1-2} + \sigma_{p_1-1}) \\ + (p_1 - 4 - m) \quad (\sigma_{p_1-4} - 2\sigma_{p_1-3} + \sigma_{p_1-2}) \\ \cdot \\ \cdot \\ \cdot \\ +4 \quad (\sigma_{m+3} - 2\sigma_{m+4} + \sigma_{m+5}) \\ +3 \quad (\sigma_{m+2} - 2\sigma_{m+3} + \sigma_{m+4}) \\ +2 \quad (\sigma_{m+1} - 2\sigma_{m+2} + \sigma_{m+3}) \\ + \quad \text{The number of } m\text{-blocks.} \end{array} \end{aligned}$$

Using the relation $t - 2(t - 1) + (t - 2) = 0$, one solves the above equation for the number of m -blocks to get the result. \square

2-sides also play a special role. It follows from remark 5) in the preliminaries that these sides do not intersect other sides, in particular they always contain two parabolic vertices.

Proposition 3. *The number of 2-sides of R_N equals*

$$\begin{array}{ll} \sigma_1(N) - 2\sigma_2(N) + \sigma_3(N) & \text{if } N \text{ is odd.} \\ 2(\sigma_1(\frac{N}{2}) - \sigma_2(\frac{N}{2})) & \text{if } N \text{ is even.} \end{array}$$

Proof. R_N has a 2-side whenever there is a $t \in \{1, 2, \dots, N-1\}$ for which $(t, N) > 1$, $(t + 1, N) > 1$ and $(2t + 1, 2N) = 1$.

If N is odd, these conditions are equivalent to $(2t, N) > 1$, $(2t + 2, N) > 1$ and $(2t + 1, N) = 1$. Putting $s = 2t + 1$, we seek the odd numbers $s \in \{1, 2, \dots, 2N - 1\}$ such that $(s, N) = 1$, $(s - 1, N) > 1$ and $(s + 1, N) > 1$. Using **Lemma 1**, we get the result for this case.

If N is even, we consider two subcases depending if t is even or odd. If t is even, there is a 2-side with parabolic vertices $\frac{t}{N}, \frac{t+1}{N}$ whenever $(t + 1, N) > 1$ and $(2t + 1, 2N) = 1$. Writing $s = 2t + 1$, we need to compute the number of integers $s \in \{1, 2, \dots, 2N - 1\}$ such that $(s, \frac{N}{2}) = 1$, $(s + 1, \frac{N}{2}) > 1$ and $s \equiv 1 \pmod{4}$. It follows from **Lemma 1** that this number is given by $\sigma_1(\frac{N}{2}) - \sigma_2(\frac{N}{2})$. The proof of the other subcase is similar. \square

4. SIDES CONTAINING PARABOLIC VERTICES

In this section we develop the previous techniques in order to compute and describe the sides of R_N with infinite hyperbolic length, this machinery will also lead to the main results.

Proposition 4. *Let $N = p_1 p_2 \cdots p_r$, then the number of sides of R_N which contain parabolic vertices is given by*

$$\begin{array}{ll} 2N - 5\sigma_1(\frac{N}{2}) + 2\sigma_2(\frac{N}{2}) + 2 & \text{if } N \text{ is even,} \\ 2N - 4\sigma_1(N) + 4\sigma_2(N) - 2\sigma_3(N) + 2 & \text{if } N \text{ is odd.} \end{array}$$

Proof. **Propositions 1** and **3** together with remark 5) in the preliminaries imply that one may know the number of sides containing parabolic vertices by counting the different contributions in each rectangle S_t , $t \in \{0, 1, \dots, N - 1\}$ (see Figure 2).

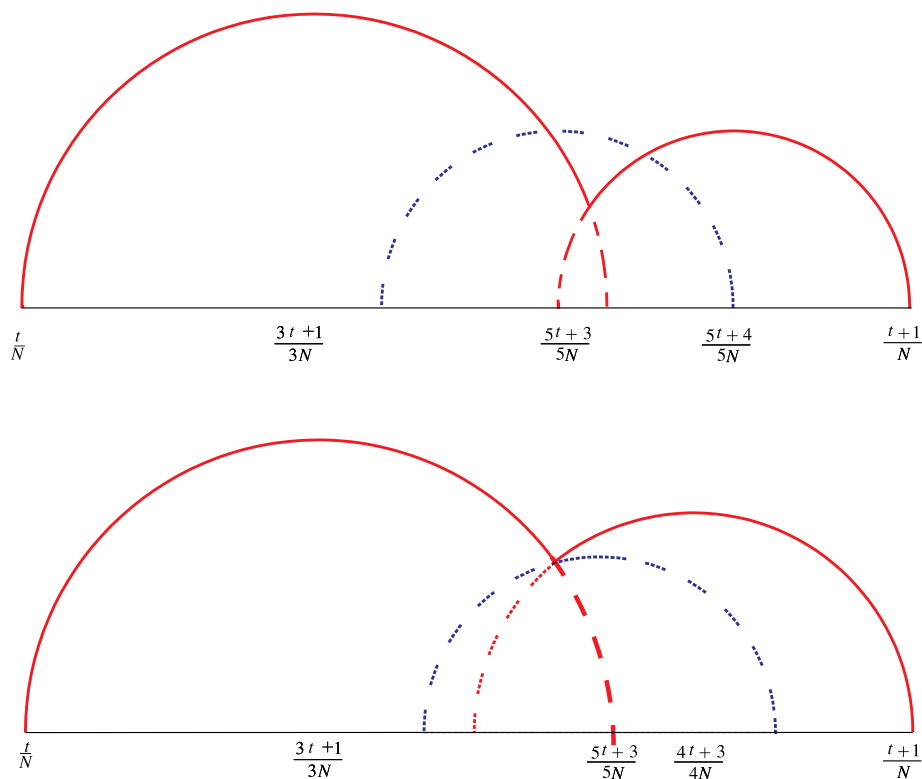
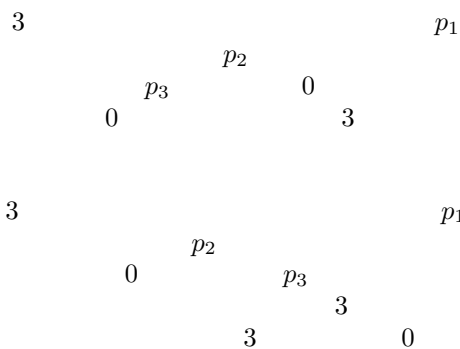


FIGURE 8. Some of the cases in the proof of Corollaries 2 and 3.

or a similar one with the primes permuted, or other symmetrical diagrams. In all cases the intersection of S_t with ∂R_N consists of a 3-side together with a 4-side, both containing parabolic vertices (see Figure 8).

Case 2. $N = 3p_1p_2p_3$. There are three subcases, depending on 3 being a divisor of t , $t + 1$, or $2t + 1$. In the first case, up to a permutation, one gets one of the next two adapted S_t -diagrams:



Again, in all these cases S_t intersects ∂R_N in two sides which contain parabolic vertices: either a 3-side together with a 4-side, or a 3-side with a 5-side (see Figure 8).

The case $3 \mid t + 1$ produces symmetrical situations to the previous case. Finally, when $3 \mid 2t + 1$, up to symmetry and permutation of p_1, p_2, p_3 , one gets the following adapted S_t -diagram:

$$\begin{array}{ccccc}
 & p_1 & & & p_2 \\
 & & & 3 & \\
 & & & 0 & p_3 \\
 & & & & 0
 \end{array}$$

□

In order to establish one of the more general polynomials which count the number of sides of the Ford Polygons for $\Gamma_0(N)$, we need the following result:

Lemma 2. *Given $N = p_1 p_2 \cdots p_r$, let a_2, a_3, \dots, a_{k+m} be integers such that $0, a_2, a_3, \dots, a_{k+m}$ represent different classes in Z_{p_i} for all $i \in \{1, 2, \dots, r\}$, then the number of integers $t \in \{1, 2, \dots, N - 1\}$ which satisfy the next two conditions*

- i) $(t(t + a_2) \cdots (t + a_m), N) = 1$,
- ii) $(t + a_{m+1}, N) > 1, \dots, (t + a_{m+k}, N) > 1$,

equals $f_k^m(p_1, p_2, \dots, p_r)$, where

$$(1) \quad f_k^m = \sum_{j=m}^{m+k} (-1)^{j-m} \binom{k}{j-m} \sigma_j,$$

$\binom{k}{j-m}$ being the binomial coefficient $\frac{k!}{(j-m)!(k-(j-m))!}$.

Proof. Using **Lemma 1**, the summation on the right member of the equality (1) may be interpreted as follows:

The first summand $\binom{k}{0} \sigma_m$ may be thought of as the cardinality of the set

$$(*) \quad \{t \in \{1, 2, \dots, N\} \mid (t(t + a_2)(t + a_3) \cdots (t + a_m), N) = 1\}.$$

Subtracting those t in $(*)$, which also satisfy $(t + a_{m+j}, N) = 1$, where $j \in \{1, 2, \dots, k\}$ yields the second summand $-\binom{k}{1} \sigma_{m+1}$. Here we are counting with multiplicity; the same integer t may be counted more than once. This suggests a third summand, where we add the contributions of those t in $(*)$ which also accomplish the condition $((t + a_{m+i})(t + a_{m+j}), N) = 1, i \neq j, i, j \in \{1, 2, \dots, k\}$; counting with multiplicities one gets $\binom{k}{2} \sigma_{m+2}$. We proceed in the same way with the other summands.

Under this interpretation, a number $t \in \{1, 2, \dots, N\}$ satisfying the hypothesis of the lemma will be counted only in the first summand of (1).

On the other hand, if another number t in the set defined by $(*)$ also satisfies the condition

$$((t + a_{j_1})(t + a_{j_2}) \cdots (t + a_{j_r}), N) = 1,$$

where $\{j_1, j_2, \dots, j_r\}$ are r different integers in $\{m+1, \dots, m+k\}$; it will be counted in (1) as follows:

$$\begin{array}{ll} (-1)^0 \binom{r}{0} & \text{times in the first summand,} \\ (-1)^1 \binom{r}{1} & \text{times in the second summand,} \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ (-1)^r \binom{r}{r} & \text{times in the } r\text{th summand.} \end{array}$$

Since $\sum_{j=0}^r (-1)^j \binom{r}{j} = 0$, the lemma follows. □

The symmetric polynomials f_k^m defined in **Lemma 2** are very useful to count sides and vertices of R_N . As a first application we get a formula for the number of k -sides containing parabolic vertices when the prime divisors of N are larger than k .

Proposition 5. *Given an integer k , $k > 2$, and $N = p_1 p_2 \cdots p_r$ such that $p_j > k$, $j \in \{1, 2, \dots, r\}$, then R_N has $2 f_k^1(p_1, p_2, \dots, p_r)$ k -sides containing parabolic vertices.*

Proof. By the symmetry of R_N we may consider only those sides which contain a parabolic vertex on the left. Now, it follows from the remarks in the preliminaries that R_N has a k -side containing a parabolic vertex on the left whenever there is a $t \in \{0, 1, \dots, N-1\}$, for which the Euclideanly larger isometric circle containing $\frac{t}{N}$ (as a point on the circle or within its interior) is a circle of radius $\frac{1}{kN}$. Analytically, this fact may be expressed as follows:

- i) $(t, N) > 1$ and $(ht + 1, hN) > 1$ for $1 \leq h < k$,
- ii) $(kt + 1, kN) = 1$.

The hypothesis of the proposition allows us to replace these conditions in order to apply **Lemma 2**, namely i) may be rewritten as

- a) $(k!t, N) > 1$ and $(k!t + \frac{k!}{h}, N) > 1$, $1 \leq h < k$.

And ii) as

- b) $(k!t + (k-1)!, N) = 1$.

Finally, writing $s = k!t + (k-1)!$, the number of $t \in \{0, 1, \dots, N-1\}$ satisfying a) and b) equals the number of $s \in \{0, 1, \dots, k!(N-1)\}$ accomplishing the following:

- 1) $(s, N) = 1$,
- 2) $(s - (k-1)!, N) > 1$,
- 3) $(s - (k-1)! + \frac{k!}{h}, N) > 1$, $1 \leq h < k$,
- 4) $s \equiv (k-1)! \pmod{k!}$.

Lemma 2 states that this number is f_k^1 . □

5. SYMMETRIC POLYNOMIALS

The symmetric polynomial

$$\sigma_1(x_1, x_2, \dots, x_r) = \prod_{i=1}^r (x_i - 1)$$

evaluated at p_1, p_2, \dots, p_r is precisely the Euler function applied to the square free number $N = p_1 p_2 \cdots p_r$. Hence, the other polynomials σ_j generalize this function. On the other hand, the symmetric polynomials f_k^m , obtained from the σ_j , turn

out to be very useful to count and describe the different kinds of sides of R_N (see **Propositions** 5 and 6 and the proof of **Theorem** 1). Thereby, it will be convenient to describe the coefficients of these polynomials, in order to get some basic estimates.

First we define certain numbers, denoted by μ_u^k , which will turn out to be the coefficients of the terms of degree $r-u$ in the polynomial f_k^0 thought of as a function in r variables (see the proof of **Proposition** 6).

Definition. Given $u, k \in \mathbb{N}$, the number μ_u^k is defined inductively by

- i) 1 if $k = 1$,
- ii) $\sum_{i=1}^{u-(k-1)} \binom{u}{i} \mu_{u-i}^{k-1}$ if $u \geq k > 1$,
- iii) 0 if $k > u$.

There is an alternative expression for these numbers.

Lemma 3. *The numbers μ_u^k can also be expressed as the following sum*

$$\sum_{j=0}^{k-1} (-1)^j \binom{k}{j} (k-j)^u.$$

Proof. We use induction on k . The cases $k = 1, 2$ are straightforward. Assuming the lemma for numbers smaller than $k+1$, we have two cases:

Case 1. $u \geq k+1$.

Since $\mu_{k-t}^k = 0 \forall t \in \mathbb{N}$

$$\mu_u^{k+1} = \sum_{i=1}^{u-k} \binom{u}{i} \mu_{u-i}^k = \sum_{i=1}^{u-1} \binom{u}{i} \mu_{u-i}^k.$$

The induction hypothesis also implies that the last summand may be written as

$$\sum_{i=0}^u \binom{u}{i} \sum_{j=0}^{k-1} (-1)^j \binom{k}{j} (k-j)^{u-i} - \binom{u}{0} \mu_u^k - \sum_{j=0}^{k-1} (-1)^j \binom{k}{j}.$$

Interchanging the double sums, this becomes

$$\sum_{j=0}^{k-1} (-1)^j \binom{k}{j} (k-j+1)^u + \sum_{j=0}^{k-1} (-1)^j \binom{k}{j} (k-j)^u + (-1)^k.$$

Finally, replacing j by $j-1$ in the second summand and collecting terms, one gets the result.

Case 2. $u < k+1$.

Working the argument backwards in the first case, one gets that

$$\sum_{j=1}^k (-1)^j \binom{k+1}{j} (k+1-j)^u = \sum_{i=1}^{u-1} \binom{u}{i} \mu_{u-i}^k$$

and therefore again by induction $\mu_u^{k+1} = 0$. □

Since $\mu_k^k = k \mu_{k-1}^{k-1}$ and $\mu_1^1 = 1$, one has that $\mu_k^k = k!$; hence the numbers μ_u^k are extensions of the factorial function. Now we can describe the polynomials f_k^m in more detail.

Proposition 6. *As a polynomial on r variables, f_k^m has the following properties:*

- i) *if $k > r$, f_k^m is identically zero,*
- ii) *the degree of f_k^m ($k \leq r$) is $r - k$, and the coefficients of all terms of degree $r - k$ are given by $k!$.*

Proof. Changing the indexes j by $j - 1$ in the expression

$$f_k^{m+1}(x_1, x_2, \dots, x_r) = \sum_{j=m+1}^{m+1+k} (-1)^{j-(m+1)} \binom{k}{j-(m+1)} \sigma_j(x_1, x_2, \dots, x_r),$$

one gets that

$$f_k^{m+1}(x_1, x_2, \dots, x_r) = f_k^m(x_1 - 1, x_2 - 1, \dots, x_r - 1).$$

Consequently, it is enough to prove the proposition for the case $m = 0$. Since the assertions hold simultaneously for f_k^{m+1} and f_k^m .

In this case,

$$f_k^0(x_1, x_2, \dots, x_r) = \sum_{j=0}^k (-1)^j \binom{k}{j} \prod_{i=1}^r (x_i - j),$$

and the coefficients of all the terms of degree $r - u$, $r \geq u > 0$ are given by

$$(-1)^u \sum_{j=1}^k (-1)^j \binom{k}{j} j^u,$$

writing $j = k - t$, the summation becomes

$$(-1)^u \sum_{t=0}^{k-1} (-1)^{k-t} \binom{k}{k-t} (k-t)^u.$$

Since $\binom{k}{k-t} = \binom{k}{t}$, **Lemma 3** implies that all the coefficients of the terms of degree $r - u$ in $f_k^0(x_1, x_2, \dots, x_r)$ are given by $(-1)^{u+k} \mu_u^k$. In particular, when $k > r$ one has $k > u$ and therefore $\mu_u^k = 0$, hence f_k^0 is the null polynomial.

It remains to prove the last part of the proposition. From the first part we may assume that $k \leq r$. Now, since the coefficients of the terms of degree $r - u$ are given by $(-1)^{u+k} \mu_u^k$ and $\mu_u^k = 0$ when $u < k$, the degree of f_k^0 is $r - k$ and the coefficients of the terms of highest degree are precisely $(-1)^{2k} \mu_k^k = k!$. \square

Another feature of these polynomials is given by the relation

$$f_k^m - f_{k+1}^m = f_k^{m+1}.$$

This equality is a consequence of the binomial coefficients properties.

The last proposition yields more information on the conclusions of **Proposition 5**. Specifically, under the hypothesis of this theorem one has:

- i) *If $k < r$, there are no k -sides containing parabolic vertices.*
- ii) *If $k = r$, there are $2k!$ k -sides containing parabolic vertices.*

6. NUMBER OF SIDES OF R_N

In this last section we prove the existence of a formula, in terms of symmetric polynomials, which yields the number of finite vertices of R_N , for all numbers N whose prime factors are big in a sense to be described.

In some cases, one can deduce that the circle C of radius $\frac{1}{nN}$ and center at $\frac{t}{N} + \frac{m}{nN}$ is isometric for $\Gamma_0(N)$, $N = p_1 p_2 \dots p_r$, if one knows that other circles are not; namely it may happen that the conditions $(p_j, n_j t + m_j) > 1$, $j = 1, 2, \dots, r$ imply that $(nt + m, N) = 1$ and therefore C is isometric. The following definition is the necessary tool to make this idea useful as we will see in the proof of **Theorem 1**.

Definition. Given two semicircles $H_{n_1}^{m_1}$ and $H_{n_2}^{m_2}$ in the family Φ , the *distance* between them, denoted by $\|H_{n_1}^{m_1}, H_{n_2}^{m_2}\|$, is defined to be

$$\max \{ s \in \mathbb{N} \mid s \mid n_1 t + m_1, \quad s \mid n_2 t + m_2, \quad t \in \mathbb{N} \}.$$

This number is clearly bounded by $|n_2 m_1 - n_1 m_2|$. In fact, there is a better estimate of the *distance*.

Proposition 7. *Given $H_{n_1}^{m_1}$ and $H_{n_2}^{m_2}$ in the family Φ , one has that*

$$\|H_{n_1}^{m_1}, H_{n_2}^{m_2}\| \leq \frac{|n_2 m_1 - n_1 m_2|}{(n_1, n_2)}.$$

Equality is achieved if and only if

$$\left(\frac{n_2 m_1 - n_1 m_2}{(n_1, n_2)}, n_1 n_2 \right) = 1.$$

In particular, if $(n_1, n_2) = 1$, then equality holds.

Proof. The inequality follows from the definition, because given s a common divisor of $n_1 t + m_1$ and $n_2 t + m_2$ for some $t \in \mathbb{N}$, a prime divisor of s is not a divisor of n_1 (or of n_2), since $(m_i, n_i) = 1$, $i = 1, 2$.

For the second part let

$$\frac{|n_2 m_1 - n_1 m_2|}{(n_1, n_2)}$$

be denoted by b and suppose that $(b, n_1 n_2) = 1$, then for fixed i , ($i = 1, 2$), the collection $n_i d + m_i$, $0 < d \leq b$, forms a complete set of residues in the ring \mathbb{Z}_b , so there exist $0 < d_1, d_2 \leq b$ such that $n_i d_i + m_i = c_i b$, $i = 1, 2$, and therefore

$$n_1 n_2 (d_1 - d_2) + n_2 m_1 - n_1 m_2 = b(c_1 n_2 - c_2 n_1).$$

Hence $b \mid d_1 - d_2$, so $d_1 = d_2$ and b is a common divisor of $n_1 d + m_1$ and $n_2 d + m_2$. This means

$$b = \|H_{n_1}^{m_1}, H_{n_2}^{m_2}\|.$$

Vice versa, if $b = \|H_{n_1}^{m_1}, H_{n_2}^{m_2}\|$, there exist $d \in \mathbb{N}$ such that $b \mid n_i d + m_i$, $i = 1, 2$. Therefore $(b, n_i) = 1$, otherwise $(m_i, n_i) > 1$. \square

In the same way that we classify isometric circles defined by $\Gamma_0(N)$, one may do so for finite points which are intersections of them, specifically if α is the point of intersection of isometric circles of type $H_{n_1}^{m_1}, H_{n_2}^{m_2}, \dots, H_{n_k}^{m_k}$ respectively, then we say that α is of type $\tau = H_{n_1}^{m_1} \vee H_{n_2}^{m_2} \vee \dots \vee H_{n_k}^{m_k}$. In particular, this definition applies to the finite vertices of the polygon R_N .

We will associate to a point α of type τ the point

$$\bar{\alpha} = \bigcap_{j=1}^k H_{n_j}^{m_j}.$$

Furthermore, to this point α we associate a subfamily of Φ , which we will denote by Φ_τ , namely

$$\Phi_\tau = \left\{ H_n^m \in \Phi \mid \left| \bar{\alpha} - \frac{m}{n} \right| \leq \frac{1}{n} \right\}.$$

This family consists of those semicircles that contain the point $\bar{\alpha}$ in the closure of their interiors. We still need one more definition to prove the main result.

Definition. Given $r \in \mathbb{N}$, $\beta(r)$ is defined to be

$$\max \left\{ \sup \| H_{n_1}^{m_1}, H_{n_2}^{m_2} \|, r \right\},$$

where the supremum is taken over all the semicircles in the family Φ which intersect the region

$$\left\{ z \in \mathbb{H}^2 \mid \text{Im } z \geq \frac{\sqrt{3}}{2r} \right\}.$$

Since this collection of semicircles is finite, this number is well defined (see Figures 3, 4 and 5).

Theorem 1. *Given $r \in \mathbb{N}$, there exists a symmetric polynomial in r variables Ψ such that for all numbers $N = p_1 p_2 \cdots p_r$, for which $p_j > \beta(r)$, $j = 1, 2, \dots, r$, the number of finite vertices of R_N is given by*

$$\Psi(p_1, p_2, \dots, p_r).$$

Proof. We remark that for all such numbers N , the polygons R_N have no vertices below the line $\text{Im } z = \frac{\sqrt{3}}{2rN}$. To prove this, observe that if α were a vertex of R_N with $\text{Im } \alpha < \frac{\sqrt{3}}{2rN}$, $\frac{t}{N} < \text{Re } \alpha < \frac{t+1}{N}$, then there would be at least $r + 1$ semicircles in the family Φ , of radius greater or equal to $\frac{1}{r}$, say $H_1^0, H_1^1, H_2^1, \dots, H_r^{m_r}$ such that $\bar{\alpha}$ is contained in their interiors (see Figures 3, 4 and 5). This would mean that the corresponding semicircles in the rectangle S_t are not isometric and therefore

$$(t, N) > 1, (t + 1, N) > 1, (2t + 1, N) > 1, \dots, (rt + m_r, N) > 1.$$

However, the assumptions on the *distances* between these semicircles and on the prime factors being larger than $\beta(r)$ imply that one needs at least $r + 1$ different primes to accomplish these conditions; hence such vertex does not exist.

Other types of vertices, which are contained in the region $\left\{ z \in \mathbb{H}^2 \mid \text{Im } z \geq \frac{\sqrt{3}}{2rN} \right\}$, may be counted as follows:

First we look for the number of vertices of type

$$\tau = H_{n_1}^{m_1} v H_{n_2}^{m_2} v \cdots v H_{n_k}^{m_k},$$

this is given by the number of integers $t \in \{0, 1, \dots, N - 1\}$, that accomplish the following conditions:

- 1) $(n_j t + m_j, N) = 1, j = 1, 2, \dots, k,$
- 2) $(h_i t + k_i, N) > 1, i = 1, 2, \dots, u,$

where the semicircles $H_{h_1}^{k_1}, H_{h_2}^{k_2}, \dots, H_{h_u}^{k_u}$ are those semicircles in the family Φ_τ different from $H_{n_1}^{m_1}, H_{n_2}^{m_2}, \dots, H_{n_k}^{m_k}$.

The number of such integers t is in a one to one correspondence with the numbers $t \in \{0, 1, \dots, N-1\}$ that satisfy

- a) $\left(r!t + \frac{r!m_j}{n_j}, N\right) = 1, \quad j = 1, 2, \dots, k,$
 b) $\left(r!t + \frac{r!k_i}{h_i}, N\right) > 1, \quad i = 1, 2, \dots, u.$

This follows because $p_i > r$ for all $i = 1, 2, \dots, r$.

Now, if we write $s = r!t + \frac{r!m_1}{n_1}$, it is not hard to prove that the number of integers t for which the conditions 1) and 2) are valid equals the number of integers $s \in \{0, 1, \dots, r!(N) - 1\}$ that accomplish the following:

- i) $(s, N) = 1,$
 ii) $\left(s + \left(\frac{n_j}{m_j} - \frac{n_1}{m_1}\right)r!, N\right) = 1, \quad j = 2, 3, \dots, k,$
 iii) $\left(s + \left(\frac{k_i}{h_i} - \frac{n_1}{m_1}\right)r!, N\right) > 1, \quad i = 1, 2, \dots, u,$
 iv) $s \equiv \frac{r!m_1}{n_1} \pmod{r!}.$

Moreover, 0 and the numbers $\left(\frac{k_i}{h_i} - \frac{n_1}{m_1}\right)r!, \quad i = 1, 2, \dots, u,$ $\left(\frac{n_j}{m_j} - \frac{n_1}{m_1}\right)r!, \quad j = 1, 2, \dots, k,$ represent different classes in the ring \mathbb{Z}_N . This follows because $p_i > r$ for all $i = 1, 2, \dots, r$, and by hypothesis these prime numbers are also larger than the *distance* between any two semicircles in the family Φ_α . At this point we may apply **Lemma 2** and deduce that there are $f_u^k(p_1, p_2, \dots, p_r)$ numbers in $\{0, 1, 2, \dots, N-1\}$ satisfying conditions i), ii) and iii). Hence there are $r!f_u^k(p_1, p_2, \dots, p_r)$ integers $s \in \{0, 1, \dots, r!(N) - 1\}$ satisfying conditions i), ii) and iii); however each solution in $\{0, 1, 2, \dots, N-1\}$ generates only one solution in $\{0, 1, \dots, r!(N) - 1\}$, that is congruent with $\frac{r!m_1}{n_1} \pmod{r!}$.

Consequently, there are $f_u^k(p_1, p_2, \dots, p_r)$ vertices of type τ ; considering all the other types of vertices whose imaginary parts are above the line $\frac{\sqrt{3}}{2rN}$, one gets the required symmetric polynomial. Observe that this polynomial does not depend on N but only on r and the result is valid for all numbers $N = p_1 p_2 \cdots p_r$, for which $p_j > \beta(r)$, $j = 1, 2, \dots, r$. \square

Since the number of parabolic vertices in R_N is known for all numbers N , and it is given by a symmetric polynomial (see [7]); it follows from **Theorem 1** that there exists a symmetric polynomial on r variables which evaluated at p_1, p_2, \dots, p_r yields the number of sides of R_N , for all $N = p_1 p_2 \cdots p_r$, such that $p_j > \beta(r)$, $j = 1, 2, \dots, r$.

We finally remark that although the Ford polygons are not in general invariant under conjugation, our results have their counterparts for the groups

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \mid b \equiv 0 \pmod{N} \right\}.$$

REFERENCES

- [1] A.F. Beardon, *The Geometry of Discrete Groups*, Springer Verlag, 1983. MR **85d**:22026
- [2] A.F. Beardon and T. Jørgensen, *Fundamental Domains for Finitely Generated Kleinian Groups*, *Mathematica Scandinavica*, **36** (1975), 21–26. MR **52**:8415
- [3] Y. Chuman, *Generators and Relations of $\Gamma_0(N)$* , *J. Math. Kyoto Univ.*, **13** (1973), 381–390. MR **50**:499
- [4] R. Fricke, *Die Elliptischen Funktionen und ihre Anwendungen*, part II. ch. 3, p. 349, Teubner, 1922.

- [5] R. Kulkarni, *An Arithmetic-Geometric Method in the Study of the Subgroups of the Modular Group*, American Journal of Mathematics, **113** (1991), 1053–1133. MR **92i**:11046
- [6] A. Lascurain, *Fundamental Domains for the Hecke Congruence Subgroups*, Columbia University, Ph.D. thesis, 1989.
- [7] A. Lascurain, *Ford Polygons for $\Gamma_0(N)$* , Boletín de la Sociedad Matemática Mexicana, Vol. **39**, p. 1-18, 1994.
- [8] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Tokyo Iwanami Shoten and Princeton University Press, 1971. MR **47**:3318
- [9] B. Schoeneberg, *Elliptic Modular Functions*, Springer Verlag, 1974. MR **54**:236
- [10] D. Zagier, *Modular Parametrizations of Elliptic Curves*, Canadian Mathematical Bulletin, **28** (1985), 372–384. MR **86m**:11041

HAVRE 101, COLONIA VILLA VERDUN, MEXICO D. F. 01810 MEXICO

E-mail address: `lasc@hardy.fciencias.unam.mx`