Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

A FUNDAMENTAL DOMAIN FOR THE FERMAT CURVES AND THEIR QUOTIENTS¹

(Fermat curves/uniformization)

J. Guàrdia

Dept. Àlgebra i Geometria. Univesitat de Barcelona. Gran Via de les Corts Catalanes, 585. E-08007 Barcelona. E-mail: guardia@mat.ub.es

ABSTRACT

Usando técnicas básicas de geometría hiperbólica, construimos un dominio fundamental de las curvas de Fermat y sus cocientes. A partir de éste, calculamos una base del grupo de homología singular $H_1(F_N, \mathbb{Z})$ y determinamos el apareamiento de intersección respecto de esta base.

We construct a fundamental domain for the Fermat curves $F_N: X^N + Y^N = 1$, and their quotients, using basic facts from hyperbolic geometry. We use it to give a basis for the singular homology group $H_1(F_N, \mathbb{Z})$. We also determine the intersection pairing with respect to this basis.

1. INTRODUCTION

Let $F_N: X^N + Y^N = 1$ be the Fermat curve of Nth degree, with $N \ge 4$. The period lattice of F_N is well known ([3], [1]). In order to compute this lattice, one needs a family of generators for the singular homology group $H_1(F_N, \mathbb{Z})$. In the references mentioned, this family is constructed by lifting some paths in the complex plane to the curve, and computing the action of the automorphisms of F_N in these liftings. But no basis for $H_1(F_N, \mathbb{Z})$ is given, and it is hard to calculate the intersection product of the generators. In particular, finding a symplectic basis for $H_1(F_N, \mathbb{Z})$ is rather messy. A symplectic basis is necessary, for instance, to compute the theta functions associated to the curves.

We present a construction that allows easy specification of both a basis and the intersection product in $H_1(F_N, \mathbb{Z})$. Using basic facts from hyperbolic geometry, we build a fundamental domain for F_N , as a polygon with some sides and vertices identified. By elementary topology

methods, we extract a basis for $H_1(F_N, \mathbb{Z})$ from this polygon, for which the intersection product is trivially computed. We also develop these computations for the quotient curves of the Fermat curves of prime exponent.

2. CONSTRUCTION OF CURVES OF GENUS 0

Let us denote by \mathbb{D} the complex unity disk, with centre a given point A in the complex plane. Let $N \ge 4$ be an integer. Since $\frac{1}{N} + \frac{1}{N} + \frac{1}{N} < 1$, we can construct inside of \mathbb{D} an hyperbolic triangle with interior angles π/N , π/N , π/N , and with one vertex on A. Call the other vertices B, C. Let ABC' be the symmetric triangle with respect to the side AB.

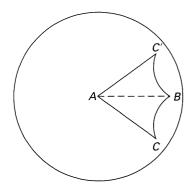


Figure 1

Let α (resp. β) be the hyperbolic rotation of centre A (resp. B) and angle $2\pi/N$. Both rotations are elliptic linear transformations and they operate on $\mathbb D$ and on its boundary. Thus, the discrete group

$$\Gamma = \langle \alpha, \beta; \alpha^N = \beta^N = 1 \rangle$$

is a fuchsian group of the first kind. It is a general fact ([2]) that the quadrilateral Q = ACBC' is a fundamental

¹ Partially supported by DGES:PB-96-0166.

domain for the action of Γ on \mathbb{D} . As none of the vertices of Q is on the boundary of \mathbb{D} , the quotient $\mathcal{C} = \Gamma \backslash \mathbb{D}$ is a compact and connected Riemann surface. On \mathcal{C} , the orientated sides of Q are identified in the following way:

$$AC \stackrel{\alpha}{\sim} AC', BC \stackrel{\beta}{\sim} BC'.$$

We have 2 inequivalent sides, and 3 inequivalent vertices. Hence

$$\chi(\mathcal{C}) = 1 - 2 + 3 = 2, \quad g(\mathcal{C}) = 0.$$

We now construct two new curves of genus 0, as coverings of \mathcal{C} . Consider the group homomorphism

$$\Gamma \xrightarrow{\phi_A} \mathbb{Z}/N\mathbb{Z}$$

$$\alpha \longrightarrow 1$$

$$\beta \longrightarrow 0.$$

The kernel of ϕ_A is $\Gamma_A = \langle \beta, D\Gamma \rangle$, where $D\Gamma$ is the commutator subgroup of Γ . A fundamental domain for the action of Γ_A on $\mathbb D$ is

$$P_A = \bigcup_{i=0}^{N-1} \alpha^i(Q),$$

which is a hyperbolic regular polygon with 2N sides and interior angles equal to π/N . The vertices of this polygon are the points $B_i = \alpha^i(B)$ and $C_i = \alpha^i(C)$. We enumerate the sides of the polygon from 0 to 2N-1 counterclockwise, starting from C_0B_0 .

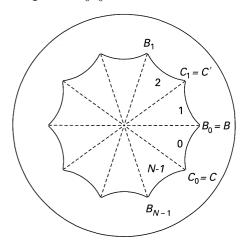


Figure 2

We will denote by β_i the rotation of center B_i and angle $2\pi/N$, $\beta_i = \alpha^i \beta \alpha^{-i}$. Since $\beta_i \in \ker \phi_A$, every even side on the quotient curve $\mathcal{C}_A = \Gamma_A \setminus \mathbb{D}$ is identified with the next odd side and all the vertices C_i are identified:

$$2i \sim 2i + 1, \quad i = 0, ..., N - 1,$$

 $C_0 \sim C_1 \sim \cdots \sim C_{N-1}.$

Hence

$$\chi(\mathcal{C}_A)=1-N+(N+1)=2, \quad g(\mathcal{C}_A)=0.$$

The curve \mathcal{C}_A is a covering of degree N of \mathcal{C} , ramified over the points A, C. The natural projection $\mathcal{C}_A \to \mathcal{C}$ maps every quadrilateral $Q_i = \alpha^i(Q)$ onto the original quadrilateral Q. The group of automorphisms of \mathcal{C}_A over \mathcal{C} is $H_A = \Gamma/\Gamma_A = \langle \overline{x} \rangle$, which is cyclic of order N.

We can mimic the construction of \mathcal{C}_A , interchanging the roles of α and β . We obtain a new curve \mathcal{C}_B of genus 0, corresponding to the fuchsian group $\Gamma_B = \langle \alpha, D\Gamma \rangle$. A fundamental domain is composed by the quadrilaterals $Q^j = \beta^j(Q)$. The group of automorphisms of \mathcal{C}_B over \mathcal{C} is $H_B = \Gamma/\Gamma_B = \langle \overline{\beta} \rangle$.

Since the genus of \mathcal{C}_A is 0, there exists a Γ_A -automorphic function establishing an analytic isomorphism between \mathcal{C}_A and $\mathbb{P}^1(\mathbb{C})$. Let us call this function X. We assume X normalized to satisfy X(A)=0, X(B)=1, $X(C)=\infty$. We have an isomorphism between the function field of \mathcal{C}_A , $\mathbb{C}(\mathcal{C}_A)$, and $\mathbb{C}(X)$. Similarly, we can find a Γ_B -automorphic function Y establishing an analytic isomorphism between \mathcal{C}_B and $\mathbb{P}^1(\mathbb{C})$, with Y(A)=1, Y(B)=0, $Y(C)=\infty$ and $\mathbb{C}(\mathcal{C}_B)\simeq \mathbb{C}(Y)$.

Proposition 2.1. For some $r, s \in \mathbb{Z}$ coprime with N, we have

$$X \circ \alpha = e^{2\pi r/N} X$$
, $Y \circ \alpha = e^{2\pi s/N} Y$.

Proof. The zeroes and poles of $X \circ \alpha$ coincide with those of X, because $\alpha(A) = A$ and $\alpha(C) = C'$, which are identified on \mathcal{C}_A . Hence, \mathcal{C}_A being compact, the quotient $X(\alpha(z))/X(z)$ is a constant function k. We obtain

$$X(\alpha^i(z)) = k^i X(z).$$

For i = N the last inequality tells us that k is a N-root of unity. If $k^j = 1$ for some j < N, we would have $X \circ \alpha^j = X$. As X is bijective, that would imply that $\alpha^j = 1$, which is not possible. The second equality is proved in the same way.

Corollary 2.2.
$$\mathbb{C}(\mathcal{C}_A) = \mathbb{C}(X^N) = \mathbb{C}(Y^N).$$

Proof. We have

$$X^N \circ \alpha = X^N, \quad Y^N \circ \beta = Y^N,$$

and hence both functions are invariant under the action of Γ . Thus, $\mathbb{C}(X^N) \subseteq \mathbb{C}(\mathcal{C}) \subseteq \mathbb{C}(\mathcal{C}_A) = \mathbb{C}(X)$, $\mathbb{C}(Y^N) \subseteq \mathbb{C}(\mathcal{C}) \subseteq \mathbb{C}(\mathcal{C}) \subseteq \mathbb{C}(\mathcal{C}_B) = \mathbb{C}(Y)$. Counting degrees, we obtain the equalities.

Proposition 2.3. For any $z \in \mathcal{C}$,

$$X^{N}(z) + Y^{N}(z) = 1.$$

Proof. The functions X^N and $1 - Y^N$ have the same zeroes and the same poles over \mathcal{C} , and therefore their quotient is constant. Evaluating this quotient on the point B we see that its value is equal to 1.

3. UNIFORMIZATION OF THE FERMAT CURVES

We define the group homomorphism

$$\Gamma \xrightarrow{\phi} \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

$$\alpha \longrightarrow (1, 0)$$

$$\beta \longrightarrow (0, 1),$$

whose kernel is $\Gamma_N = D\Gamma$. We will see that the quotient curve, $\mathcal{C}_N = D\Gamma \backslash \mathbb{D}$ is a model for the Fermat curve of degree N. Let $H_N = \Gamma/D\Gamma$ be the group of automorphisms of \mathcal{C}_N over \mathcal{C} . We can take as representatives of the classes in H_N the elements $\{\beta_i^j \alpha^i\}_{i,j=1}^N$. With this selection, the polygon

$$P = \bigcup_{i, i=0}^{N-1} (\beta^{i} \alpha^{i})(Q)$$

is a fundamental domain for the Riemann surface \mathcal{C}_N .

We will now introduce some notation. From now on, we will consider all indices as integers modulus N. Put $Q_{i,j} = \beta_i^j \alpha_i(Q) = \beta_i^j(Q_i) = \alpha^i(Q^j)$. For every $i \in \{0, 1, ..., N-1\}$, the quadrilaterals $Q_{i,0}, Q_{i,1}, ..., Q_{i,N-1}$ form a 2N-sided regular polygon T_i , centered on the point B_i . We label its vertices $C_{i,j}$, starting from the point A and moving counterclockwise, so that $C_{i,2j} = \beta_i^j(A)$, $C_{i,2j+1} = \beta_i^j(C_i)$. Note that, under the natural projection $\mathcal{C}_N \to \mathcal{C}$, the points $C_{i,2j}$ map to the point A, and the points $C_{i,2j+1}$ map to C. Finally, we denote by $b_{i,j}$ the side of Q^i which goes from the point $C_{i,j}$ to the point $C_{i,j+1}$. With this notation, the boundary of the polygon P is described by the sides $b_{0,1},b_{0,2},...,b_{0,N-2},b_{1,1},...,b_{N-1,N-2}$. The case N=5 is sketched in figure 3.

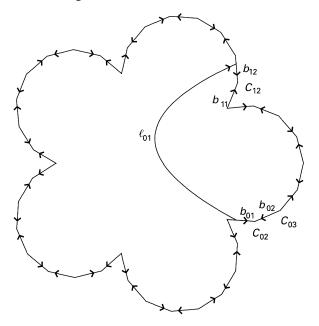


Figure 3

Proposition 3.1. The genus of C_N is (N-1)(N-2)/2.

Proof. Let us analyze the identifications of the sides and vertices of P on \mathcal{C}_N . We have

$$\alpha\beta_i^j\alpha^{-1}\beta_i^{-j}(b_{i,\,2j-1})=\beta_{i+1}^j\beta_i^{-j}(b_{i,\,2j-1})=\beta_{i+1}^j(b_{i+1,\,0})=b_{i+1,\,2j}^{-1}.$$

Hence

$$b_{i,2i-1} \sim b_{i+1,2i}^{-1}, \quad i = 0, ..., N-1, \quad j = 1, ..., N-2.$$

In the same way,

$$C_{0,2j} \sim C_{2,2j} \sim \cdots \sim C_{N-1,2j}, \quad j = 1, \dots, N-1$$

 $C_{i,1} \sim C_{i+1,3} \sim C_{i+2,5} \sim \cdots C_{i+N-1,2N-3}, \quad i = 0, \dots, N-1.$

Therefore

$$\chi(\mathcal{C}_N) = 1 - N(N-1) + 2N - 1 = -N^2 - 3N,$$

and
$$g(\mathcal{C}_N) = (N-1)(N-2)/2$$
.

Proposition 3.2. The curve C_N is a model of the Fermat curve of degree N.

Proof. By proposition 2.3, it is enough to see that $\mathbb{C}(\mathcal{C}_N) = \mathbb{C}(X, Y)$. The functions X and Y are Γ_N -automorphic, because $\Gamma_N \subset \Gamma_A \cap \Gamma_B$. This gives the inclusion $\mathbb{C}(X,Y) \subset \mathbb{C}(\mathcal{C}_N)$. The polynomial $Y^N + (X^N - 1)$ is irreducible in $\mathbb{C}[X][Y]$ (because it is (X - 1)-Eisenstein), and thus $[\mathbb{C}(X, Y) : \mathbb{C}(X)] = \mathbb{N}$, which implies the desired equality.

4. A BASIS FOR $H_1(F_N, \mathbb{Z})$

In this section we will find a basis for $H_1(F_N, \mathbb{Z})$. For every i, j, choose a path $\ell_{i, 2j+1}$ joining the middle points of the sides $b_{i, 2j+1}$, $b_{i+1, 2j+2}$ of the fundamental domain we have found for F_N in the last section. Our result is based on the following lemma:

Lemma 4.1. Assume that S is a compact connected surface, given as a polygon P, with 2r-sides identified by pairs $\{a_i, b_i\}$, but with vertices not necessarily identified. Let l_i be a path joining the middle points of the sides a_i and b_i , passing through the interior of the polygon. Then, the first homology group $H_1(S, \mathbb{Z})$ is generated by the classes of l_1, \ldots, l_r .

Proof. It is very well-known that with a finite number of elementary transformations, we can pass from the original polygon P to a new polygon Q with all vertices identified and the border given by

$$c_1c_2c_1^{-1}c_2^{-1} \cdots c_g c_{g+1}c_g^{-1}c_{g+1}^{-1}b_1b_1 \cdots b_nb_n$$

In order to prove the lemma, we will see that:

- a) The result is true for the polygon P if and only if it is true for the polygon Q.
- b) The result is true for the polygon Q.

We begin by part b). It is well-known that the classes of the sides $\langle c_1, \ldots, c_g, b_1, \ldots, b_n \rangle$ of the polygon Q generate $H_1(S, \mathbb{Z})$. Let us consider the path l_1 (resp. l_2) joining the middle points of c_1 and c_1^{-1} (resp. c_2 and c_2^{-1}). It is evident that l_1 is homotopic to c_2 and that l_2 is homotopic to c_1 , so that we can replace c_1 , c_2 by l_1 , l_2 in the list of generators of $H_1(S, \mathbb{Z})$. In the same way, the path l_i' joining the middle points of the consecutive sides b_i and b_i is homotopic to any of these sides, so that we can also replace b_i by l_i' .

Let us now proof part a). We know that the classes of the sides of the polygon P generate the full homology group $H_1(S, \mathbb{Z})$. In passing from P to the polygon Q we make a finite number of elementary transformation of one of the following four types:

- a1) Cancel two consecutive sides of the first kind (i.e., of type aa^{-1}).
- *a2*) Transform two different vertices into equivalent vertices.
- a3) Transform two sides of the second kind (i.e., of type aa) into consecutive sides.
- a4) Transform a couple of pairs of sides of the first kind

$$\cdots \ a_i \cdots a_j \cdots a_i^{-1} \cdots a_j^{-1} \cdots$$
 into consecutive sides
$$\cdots \ a_i a_j a_i^{-1} a_j^{-1} \cdots .$$

In each of these transformations, we pass from a polygon P_k to a new polygon P_{k+1} . We denote by l_i^k the paths joining the middle points of the sides of the polygon P_k . One can check that after each of these transformation, the subspaces $\langle l_1^k, \ldots, l_t^k \rangle$ and $\langle l_1^{k+1}, \ldots, l_s^{k+1} \rangle$ of $H_1(S, \mathbb{Z})$ coincide, so that the lemma is true for P_k if and only if it is true for P_{k+1} . This proves a.

Theorem 4.2.

a) A basis for $H_1(F_N, \mathbb{Z})$ is

$$\{\ell_{0,1}, \ell_{0,3}, \ldots, \ell_{0,2N-3}, \ell_{1,1}, \ldots, \ell_{N-3,2N-3}\}.$$

b) The intersection product in $H_1(F_N, \mathbb{Z})$ is given by

$$\begin{split} &(\ell_{i,2j-1},\,\ell_{i,2k-1}) = +\,1 \quad k > j, \\ &(\ell_{i,2j-1},\,\ell_{i+1,\,1}) = (\ell_{i,2j-1},\,\ell_{i+1,\,3}) = \cdots = (\ell_{i,2j-1},\,\ell_{i+1,\,2j-1}) = 1 \\ &(\ell_{i,2j-1},\,\ell_{i+1,\,2j+1}) = \cdots = (\ell_{i,\,2j-1},\,\ell_{i+1,\,2N-3}) = 0 \\ &(\ell_{i,\,2i-1},\,\ell_{i+r,\,2k-1}) = 0 \quad r = 2,\,\ldots,\,N-2,\,k = 0,\,\ldots,\,N-1. \end{split}$$

c) $H_1(F_N, \mathbb{Z})$ is a cyclic $\mathbb{Z}[\alpha, \beta]$ -module, generated by any of the paths $\ell_{i, 2i+1}$.

Proof. If we apply lemma lemma 4.1 to our case, we obtain

$$H_1(F_N, \mathbb{Z}) = \langle \ell_{0,1}, \ell_{0,3}, ..., \ell_{N-1,2N-3} \rangle.$$
 (1)

Of course, this family of generators cannot be free, because it has N(N-1) elements, while the rank of $H_1(F_N, \mathbb{Z})$ is (N-1)(N-2). But one can check easily that the cycles

$$\sum_{k=0}^{N-1} \alpha^k(\ell_{0,2j+1}) \quad j=0,\,...,\,N-2,$$

$$\sum_{k=0}^{N-1} (\ell_{k, 2j+1+k}) \quad j = 0, ..., N-2,$$

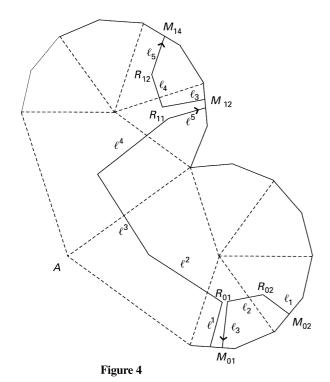
are homotopic to zero, and so we can eliminate the paths $\ell_{N-1,2j+1}$, $\ell_{N-2,2j+1}$, $j=0,\ldots,N-2$, from the generators (1). As the number of remaining generators coincides with the rank of $H_1(F_N, \mathbb{Z})$, they form a basis.

The second assertion is immediate. We will prove c) only for the path $\ell_{0,1}$ but during the proof it will become evident that it is also true for any $\ell_{i,2j+1}$. It is evident that $\alpha(\ell_{0,1}) = \ell_{1,2}$. Let us compute $\beta(\ell_{0,1})$. Denote by $M_{i,j}$ the middle point of the side $b_{i,j}$, and by $R_{i,j}$ the center of the quadrilateral $Q_{i,j}$. We deform $\ell_{0,1}$ to the homologous path $\ell^1 + \ell^2 + \ell^3 + \ell^4 + \ell^5$, where:

- $-\ell^1$ goes from M_{01} to R_{01} ;
- $-\ell^2$ goes from R_{01} to R_{00} ;
- $-\ell^3$ goes from R_{00} to R_{10} ;
- $-\ell^4$ goes from R_{10} to R_{11} ;
- $-\ell^5$ goes from R_{11} to M_{12} .

Taking into account the identifications in the boundary of the polygon P, we see that $\beta(Q_{1,0}) = Q_{1,1}$. We apply β to the five preceding paths:

- $-\ell_1 = \beta(\ell^1)$ goes from M_{02} to R_{02} ;
- $-\ell_2 = \beta(\ell^2)$ goes from R_{02} to R_{01} ;
- $-\ell_3 = \beta(\ell^3)$ goes from R_{01} to M_{01} , which is identified with M_{12} , and then continues from this point to R_{11} ;
- $-\ell_4 = \beta(\ell^4)$ goes from R_{11} to R_{12} ;
- $-\ell_5 = \beta(\ell^5)$ goes from R_{12} to M_{14} .



With this description of $\beta(\ell_{0,1})$, we can compute its intersections with the rest of the $\ell_{i,2j+1}$ using a) and b). From these calculations one sees that

$$\beta(\ell_{0,1}) = \ell_{1,3} - \ell_{1,1},$$

$$\beta^{2}(\ell_{0,1}) = \ell_{1,5} - \ell_{1,3},$$

$$\vdots$$

$$\beta^{N-2}(\ell_{0,1}) = \ell_{1,2N-3} - \ell_{1,2N-5},$$

$$\beta^{N-1}(\ell_{0,1}) = -\ell_{0,1}.$$
(2)

Using that $\alpha^i(\ell_{0,2j+1}) = \ell_{i,2j+1}$, we obtain c).

Remark 4.3. Combining equations (2) and theorem 4.2 we find that the paths

$$\alpha^{i}\beta^{j}(\ell_{0,1}), \quad i=0,\ldots,N-3, \quad j=0,\ldots,N-2,$$

form also a basis for $H_1(F_N, \mathbb{Z})$.

Remark 4.4. With the preceding result, the computation of a symplectic basis for $H_1(F_N, \mathbb{Z})$ for a concrete value of N can be easily performed using the Gram-Schmidt orthogonalization process.

5. QUOTIENTS OF THE FERMAT CURVE

We have given a presentation of the Fermat curve \mathcal{C}_N as a covering of a curve \mathcal{C} of genus 0. We now study subcoverings $\mathcal{C}_N \to \mathcal{C}' \to \mathcal{C}$. As $\operatorname{Aut}(\mathcal{C}_N/\mathcal{C}) = \Gamma/D\Gamma$, these

subcoverings correspond to subgroups $\Gamma \supset \Gamma' \supset D\Gamma$. We know that $\Gamma/D\Gamma = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, so that these subgroups Γ' must be of the form $\Gamma_{r,s} := \langle a^r \beta^s, D\Gamma \rangle$. For instance, the subgroups $\Gamma_{1,0}$ and $\Gamma_{0,1}$ give rise respectively to the curves \mathcal{C}_B and \mathcal{C}_A of section 2.

In order to simplify the exposition, from now on we will suppose that N=p is a prime number. In this case, every subgroup $\Gamma_{r,s}$ is conjugate to a subgroup $\Gamma_{r,1}$, so that we can confine our attention to the subgroups $\Gamma_r := \langle \alpha^r \beta, D\Gamma \rangle, \ r \not\equiv 0, -1 \pmod{p}$. We call $\mathcal{C}_r := \Gamma_r \backslash \mathbb{D}$ the subcovering of $\mathcal{C}_p / \mathcal{C}$ corresponding to the subgroup Γ_r .

The subgroup Γ_r is normal, since it is the kernel of the surjective map

$$\Gamma \xrightarrow{\phi_r} \mathbb{Z}/p\mathbb{Z}$$

$$\alpha \longrightarrow r'$$

$$\beta \longrightarrow 1,$$

where r' is such that $rr' \equiv -1 \pmod{p}$. Let us write $\overline{\Gamma}_r := \Gamma_r/D\Gamma$. From proposition 2.1 and the fact that $[\Gamma/D\Gamma : \overline{\Gamma}_r] = p$, we deduce that $\mathbb{C}(X, Y)^{\Gamma_r} = \mathbb{C}(X^p, X^rY)$. We see thus:

Proposition 5.1. The curve $C_r = \Gamma_r \backslash \mathbb{D}$ is given by the equation

$$V^p = U^r(1-U),$$

where $U = X^N$, $V = X^r Y$.

These are exactly the quotients of the Fermat curve built in ([1]). We now proceed to build a fundamental domain and a basis for the homology group of these curves.

As $\Gamma/\Gamma_r = \langle \overline{\alpha} \rangle$, the hyperbolic polygon $P_r = \bigcup_{i=0}^{p-1} \alpha^i(Q)$ gives a fundamental domain for the curve \mathcal{C}_r . This coincides with the polygon P_A of section 2, but the sides and vertices of P_r are identified in a different way. One finds easily that (following the notation of section 2):

$$2i + 1 \sim 2i + 2r + 2, \quad i = 0, ..., p - 1,$$

$$B_0 \sim B_1 \sim \cdots B_{p-1}, \qquad (3)$$

$$C_0 \sim C_1 \sim \cdots C_{p-1}.$$

Corollary 5.2. The genus of the curve C_r is $\frac{p-1}{2}$.

Let m_i denote the path on P_r which joins the middle points of the sides 2i + 1, 2i + 2r + 2. The same type of reasoning applied to the Fermat curve on section 4 gives now:

Theorem 5.3.

- a) A basis for $H_1(\mathcal{C}_r, \mathbb{Z})$ is $\{m_1, ..., m_{p-1}\}$.
- b) The intersection product in $H_1(\mathcal{C}_r, \mathbb{Z})$ is given by $(m_k, m_{k+1}) = (m_k, m_{k+2}) = \dots = (m_k, m_{k+r-1}) = 1,$ $(m_k, m_{k-1}) = (m_k, m_{k-2}) = \dots = (m_k, m_{k-r}) = -1,$ $(m_k, m_k) = 0$ in any other case.
- $c) \quad H_1(\mathcal{C}_r,\,\mathbb{Z})=\mathbb{Z}[\alpha]\;\langle m_1\rangle.$

REFERENCES

- 1. [La-82] Lang, S. (1982), *Introduction to algebraic and abelian functions*, Graduate Text in Mathematics, Vol. 89, Ed.: Springer.
- [Le-64] Lehner, J. (1964), Discontinuous groups and automorphic functions, AMS Mathematical Surveys, Vol. 8.
- 3. [Rho-78] Rhorlich, D. (1978), The periods of the Fermat curve, apéndice a Gross, B. (1978), On the periods of abelian integrals and a formula of Chowla and Selberg, *Inventiones Mathematicae*, 45, pp 193-211.