THE GROUP OF AUTOMORPHISMS OF THE HEISENBERG CURVE

JANNIS A. ANTONIADIS AND ARISTIDES KONTOGEORGIS

ABSTRACT. The Heisenberg curve is defined to be the curve corresponding to an extension of the projective line by the Heisenberg group modulo n, ramified above three points. This curve is related to the Fermat curve and its group of automorphisms is studied. Also we give an explicit equation for the curve C_3.

1. INTRODUCTION

Probably the most famous curve in number theory is the Fermat curve given by affine equation

$$F_n : x^n + y^n = 1.$$

This curve can be seen as ramified Galois cover of the projective line with Galois group $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with action given by $\sigma_{a,b} : (x, y) \mapsto (\zeta^a x, \zeta^b y)$ where $(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The ramified cover

$$\pi : F_n \to \mathbb{P}^1$$

has three ramified points and the cover

$$F_n^0 := F_n - \pi^{-1}(\{0, 1, \infty\}) \xrightarrow{\pi} \left(\mathbb{P}^1 - \{0, 1, \infty\}\right),$$

is a Galois topological cover. We can see the hyperbolic space $\mathbb{H}$ as the universal covering space of $\mathbb{P}^1 - \{0, 1, \infty\}$. The Galois group of the above cover is isomorphic to the free group F_2 in two generators, and a suitable realization of this group in our setting is the group Δ which is the subgroup of $\mathrm{SL}(2, \mathbb{Z}) \subseteq \mathrm{PSL}(2, \mathbb{R})$ generated by the elements $a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ and $\pi(\mathbb{P}^1 - \{0, 1, \infty\}, x_0) \cong \Delta$. Related to the group Δ is the modular group

$$\Gamma(2) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) : \gamma \equiv 1_2 \bmod 2 \right\},$$

which is isomorphic to $\{\pm I\}\Delta$ while $\Gamma(2)\backslash\mathbb{H} \cong \left(\mathbb{P}^1 - \{0, 1, \infty\}\right)$. The groups Δ and $\Gamma(2)$ act in exactly the same way on the hyperbolic plane $\mathbb{H}$.

Remark 1. Covers of the projective line minus three points are very important in number theory because of the Belyi theorem [3],[4] that asserts that all algebraic curves defined over $\bar{\mathbb{Q}}$ fall into this category. It seems that the idea of studying algebraic curves as "modular curves" goes back to S. Lang and to D. Rohrlich [22].

For every finitely generated group G generated by two elements there is a homomorphism

$$\Gamma(2) \to G.$$

Notice that $\Gamma(2)^{\mathrm{ab}} \cong \mathbb{Z} \times \mathbb{Z}$ so using the projection

$$\psi : \Delta \to \Delta^{\mathrm{ab}} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Date: December 1, 2019.

keywords: Automorphisms, Curves, Differentials, Numerical Semigroups. **AMS subject classification** 14H37.

we can write the open Fermat curve F_n^0 as the quotient

$$F_n^0 = \ker \psi \backslash \mathbb{H}.$$

In the theory of modular curves [20], the hyperbolic space $\mathbb{H}$ is extented to $\bar{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, where $\mathbb{P}^1(\mathbb{Q})$ is the set of cusps so that subgroups Γ of $\mathrm{SL}(2, \mathbb{Z})$ give rise to compact quotients. The orbits of $\mathbb{P}^1(\mathbb{Q})$ under the action of Γ are the cusps of the curve $\Gamma \backslash \mathbb{H}$. In this setting the cusps of the Fermat curve F_n are the points $F_n - F_n^0$.

Aim of this article is to initialize the study of the curve C_n, which is defined in the following way: Consider the Heisenberg group modulo n:

$$H_n = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z}/n\mathbb{Z} \right\}.$$

It is a finite group generated by the elements

$$a_H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } b_H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{1}$$

Notice that

$$[a_H, b_H] = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2}$$

and

$$H_n^{\mathrm{ab}} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

We have the short exact sequence

$$1 \to \mathbb{Z}/n\mathbb{Z} \cong Z_n \to H_n \longrightarrow H_n^{\mathrm{ab}} \to 1, \tag{3}$$

where

$$Z_n := \left\{ \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : z \in \mathbb{Z}/n\mathbb{Z} \right\}.$$

Observe that there is an epimorphism: $\phi : \Gamma(2) \to H_n$ sending each generator of $\Gamma(2)$ to the elements $a_H, b_H \in H_n$. This way an open curve C_n^0 is defined as $\ker \phi \backslash \mathbb{H}$ that can be compactified to a compact Riemann surface C_n.

We have the following diagram:

$$\begin{tikzcd}
\mathbb{H} \arrow[d, "\ker \phi"] \arrow[dd, bend left=60, "\ker \psi"] \arrow[ddd, bend right=60, "\Gamma(2)"'] \\
C_n \arrow[d, "Z_n"] \arrow[dd, bend right, "H_n"'] \\
F_n \arrow[d, "\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}"] \\
\mathbb{P}^1
\end{tikzcd} \tag{4}$$

Definition 2. Let X be a curve that comes as a compactification by adding some cusps of the open curve $\Gamma \backslash \mathbb{H}$ where Γ is a subgroup of finite index of $\mathrm{SL}(2, \mathbb{Z})$. The group of *modular automorphisms* is the group

$$\mathrm{Aut}^{\mathrm{m}}(X) = N_{\mathrm{SL}(2,\mathbb{R})}(\Gamma)/\Gamma,$$

where $\mathrm{SL}(2, \mathbb{R})$ is the group of automorphisms of $\mathbb{H}$ and $N_{\mathrm{SL}(2,\mathbb{R})}(\Gamma)$ is the normalizer of Γ in $\mathrm{SL}(2, \mathbb{R})$.

Remark 3. An automorphism σ of a complete curve X which comes out from an open curve $\Gamma\backslash\mathbb{H}$ by adding the set of cusps $\mathbb{P}^1(\mathbb{Q})$ is modular if and only if σ sends cusps to cusps and non-cusps to non-cusps.

Remark 4. Deciding if there are extra non-modular automorphism is a difficult classical question for the case of modular and Shimura curves, see [1], [13], [12], [8], [16], [21], [17] for some related results.

Acknowledgement: The authors would like to thank Professor Dinakar Ramakrishnan for proposing the study of Heisenberg curves to them.

2. THE TRIANGLE GROUP APPROACH

A Fuchsian group Γ is a finitely generated discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$. It is known that a Fuchsian group has a set of $2g$ hyperbolic generators $\{a_1, b_1, \ldots, a_g, b_g\}$, a set of elliptic generators $x_1, \ldots, x_r$ and parabolic generators $p_1, \ldots, p_s$ and some hyperbolic boundary elements $h_1, \ldots, h_t$, see [25]. The relations are given by

$$x_1^{m_1} = x_2^{m_2} = \cdots = x_r^{m_r} = 1$$

$$\prod_{i=1}^{g} [a_i, b_i] \prod_{j=1}^{r} x_j \prod_{k=1}^{s} p_k \prod_{i=1}^{t} h_t = 1.$$

The signature of Γ is

$$(g; m_1, \ldots, m_r; s; t),$$

where $m_1, \ldots, m_r$ are natural numbers ≥ 2 and are called the periods of Γ.

Triangle groups: A triangle group $\Delta(\ell, m, n)$ is a group with signature $[0; \ell, m, n]$. We also thing parabolic elements as elliptic elements of infinite period and in this point of view , the group $\Gamma(2)$ can also be considered as the triangle group $\Gamma(\infty, \infty, \infty)$.

The Fermat curve can be uniformized in terms of triangle groups. This is a quite different uniformization than the uniformization given in (4). Namely we have the following diagramm of curves and groups

(5)

$$\begin{tikzcd}
\mathbb{H} \arrow[d] \arrow[dd, bend left=50, "\Delta(n,n,n)'"] \arrow[ddd, bend right=70, "\Delta(n,n,n)"'] \\
C_n \arrow[d, "Z_n"] \arrow[dd, bend right=50, "H_n"'] \\
F_n \cong \Delta(n,n,n)'\backslash\mathbb{H} \arrow[d, "\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}"] \\
\mathbb{P}^1 \cong \Delta(n,n,n)\backslash\mathbb{H}
\end{tikzcd}$$

$\Delta(n,n,n)'$ is the commutator of the triangle group $\Delta(n,n,n)$. For $n > 3$ it is known that $\Delta(n,n,n)'$ is the universal covering group of the Fermat curve see [31].

We will show in lemma 11 that if $(n, 2) = 1$, then $C_n \to F_n$ is unramified. In this case, if $D(n)$ denotes the universal covering group of the Heisenberg curve then $D(n)$ is a normal subgroup of $\Delta(n,n,n)'$ and $\Delta(n,n,n)'/D(n) \cong \mathbb{Z}/n\mathbb{Z}$.

The presentation of a Riemann surface in terms of a co-compact triangle group has several advantages. Concerning automorphism groups, the advantage is that if Π is the funtamental group of the curve, which is a normal torsion free subgroup of the triangle group $\Delta(a, b, c)$, then the group $N_{\mathrm{PSL}(2,\mathbb{R})}(\Pi)/\Pi$ is the whole automorphism group not only the group of modular automorphisms, see [11]. The computation of the automorphism group is then simplified, as we will see for the case of Heisenberg and Fermat curves, since $N_{\mathrm{PSL}(2,\mathbb{R})}(\Pi)$ is known to be also a triangle curve which contains $\Delta(\ell, m, n)$, and these groups are fully classified [7], [25], [11, table 2]. This approach has the disadvantage that does not provide explicitly the automorphisms acting on the curve.

Remark 5. The automorphism group of the Fermat curve can be computed by using the classification of the triangle groups which contain $\Delta(n, n, n)$ as a normal subgroup [7], [25], [11, table 2]. Indeed, the only such group is $\Delta(2, 3, 2n)$ and this computation provides and alternative method for proving:

$$\mathrm{Aut}(F_n) = \Delta(2, 3, 2n)/\Delta(n, n, n) = (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \rtimes S_3.$$

Notice that the triangle curve $\Delta(2, 3, 2n)$ is compatible with the ramification diagram given in figure 1.

Remark 6. In addition to the above proof, the authors are aware of the following different methods for computing the automorphisms group of the Fermat curve: there are proofs using the Riemann-Hurwitz formula [28], [18] and proofs using the embedding of the Fermat curve in $\mathbb{P}^2$ and projective duality [23], [15].

3. Restriction and Lifting of automorphisms in covers

In this section we will study the following:

Question 7. Assume that $X \to Y$ is a Galois cover of curves. How are the groups $\mathrm{Aut}(X)$ and $\mathrm{Aut}(Y)$ related? When can an automorphism in $\mathrm{Aut}(Y)$ lift to an automorphism of $\mathrm{Aut}(X)$?

Assume that $X^0 = \Gamma_X\backslash\mathbb{H}, Y^0 = \Gamma_Y\backslash\mathbb{H}$ are either open curves corresponding to certain subgroups Γ_X, Γ_Y of $\mathrm{SL}(2, \mathbb{Z})$ or complete curves uniformized by cocompact groups Γ_X, Γ_Y. In the first case the complete curves X, Y are obtained by adding the cusps and in the second case $X^0 = X$ and $Y^0 = Y$.

Proposition 8. *Let* $\{1\} < \Gamma_X \lhd \Gamma_Y$ *and consider the sequence of Galois covers*

$$\mathbb{H} \to \Gamma_X\backslash\mathbb{H} \to \Gamma_Y\backslash\mathbb{H}$$

and $G = \mathrm{Gal}(X/Y)$. *If* Γ_X, Γ_Y *are both normal subgroups of* $\mathrm{SL}(2, \mathbb{Z})$ *then a modular automorphism* σ *of* Y *lifts to* $|G|$ *automorphisms of* X*, if and only if* $\sigma\Gamma_X\sigma^{-1} \subset \Gamma_X$. *A modular automorphism* τ *of* X *restricts to a modular automorphism of* Y *if and only if* $\tau G\tau^{-1} \subset G$*, i.e. if and only if* $\tau^{-1}\Gamma_Y\tau \subset \Gamma_Y$.

Similarly if Γ_X, Γ_Y *are cocompact subgroups of* $\mathrm{SL}(2, \mathbb{R})$ *uniformizing the compact curves* X, Y*, then an automorphism* σ *of* Y *lifts to* G *automorphisms of* X*, if and only if* $\sigma\Gamma_X\sigma^{-1} \subset \Gamma_X$. *An automorphism* τ *of* X *restricts to a modular automorphism of* Y *if and only if* $\tau G\tau^{-1} \subset G$*, i.e. if and only if* $\tau^{-1}\Gamma_Y\tau \subset \Gamma_Y$.

Proof. We will prove the first case, where Γ_X, Γ_Y are subgroups of $\mathrm{SL}(2, \mathbb{Z})$ uniformizing the open curves X^0, Y^0. The second case has a similar proof.

By definition, a modular automorphism of Y, is represented by element in the normalizer $N_{\mathrm{SL}(2,\mathbb{R})}\Gamma_Y$. This element has to normalize Γ_X as well in order to extend to an automorphism of Γ_X.

$$\begin{tikzcd}
X \arrow[d, "G"'] \arrow[dd, bend left, "N"] \\
Y \arrow[d, "N/G"'] \\
N\backslash X
\end{tikzcd}$$

For restricting an automorphism from X to Y. Set $G = \mathrm{Gal}(X/Y) = \Gamma_Y/\Gamma_X$ and let N be the subgroup of $\mathrm{Aut}^0(X)$ which restrict to automorphisms of Y. We have the tower of fields shown on the right. The group N has to normalize G so that N/G is group acting on Y. Since G is a subgroup of the modular automorphism group, there is a conjugation action of every automorphism of X on G. In particular a modular automorphism $\tau \cdot \Gamma_X$ of X acts by conjugation on an element $\gamma \cdot \Gamma_X \in G$:

$$(\tau \cdot \Gamma_X)(\gamma \cdot \Gamma_X)(\tau \cdot \Gamma_X)^{-1} = \tau\gamma\tau^{-1} \cdot \Gamma_X,$$

and the later element is in G if an only if $\tau\gamma\tau^{-1} \in \Gamma_Y$. ☐

4. THE FERMAT CURVE

In this section we will collect some known results about the Fermat curve and its automorphism group.

We will use the coorespondence of functions fields of one variable to curves and of points to places, see [27]. In particular we will use that coverings of curves correspond to algebraic extensions of their function fields.

Lemma 9. *For $n \geq 4$ the automorphism group of the Fermat curve is isomorphic to the semidirect product $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \rtimes S_3$. In the cover $F_n \rightarrow F_n/\mathrm{Aut}(F_n) \cong \mathbb{P}^1$, three points are ramified with ramification indices $2n, 3, 3$ respectively.*

Proof. For the automorphism group of the Fermat curve see [28],[18]. In characteristic zero the automorphism group can be also studied as in remark 5.

The curves F_2 and F_3 are rational and elliptic respectively and so they have infinite automorphism group. The Fermat curve can be seen as a Kummer cover, i.e. the function field $\mathbb{C}(F_n) = \mathbb{C}(x)[\sqrt[n]{x^n - 1}]$ is a Kummer extension of the rational function field $\mathbb{C}(x)$ and the ramification places in this Kummer extension correspond to the irreducible polynomials $x - \zeta^i$, $i = 0, \ldots, n-1$, where ζ is a primitive n-th root of unity. We have the following picture of function fields and ramification of places.

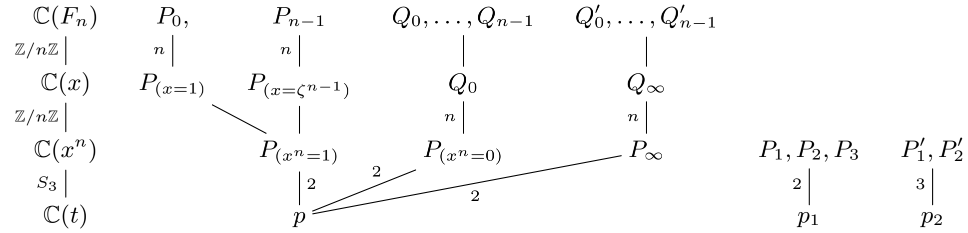

FIGURE 1. Ramification diagram for the Fermat Curve

□

Let us now consider the cover $F_n \rightarrow F_n^{\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{P}^1$. Consider the function field $\mathbb{C}(x^n) = \mathbb{C}(F_n)^{\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}}$. In the extension $\mathbb{C}(F_n)/\mathbb{C}(x^n)$ three places are ramified $P_{(x^n=0)}, P_{(x^n=1)}, P_\infty$. We will describe now the places of $\mathbb{C}(F_n)$ which restrict to the three points ramified above. For this we need the projective form of the Fermat curve given by

$$X^n + Y^n = Z^n.$$

The n places $P_0, \ldots, P_{n-1}$ which restrict to $P_{(x^n=1)}$ correspond to points with projective coordinates $P_k = (\zeta^k : 0 : 1)$ for $k = 0, \ldots, n-1$. We have also the n places $Q_0, \ldots, Q_{n-1}$ which restrict to $P_{x^n=0}$ which correspond to points with projective coordinates $Q_k = (0 : \zeta^k : 1)$ and the n places $Q'_0, \ldots, Q'_{n-1}$ that restrict to P_∞ and correspond to points with projective coordinates $Q'_k = (\epsilon\zeta^k : 1 : 0)$, $k = 0, \ldots, n-1$, $\epsilon^2 = \zeta$. An element $\sigma_{a,b} \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is acting on coordinates $(X : Y : Z)$ by the following rule:

$$\sigma_{a,b} : (X, Y, Z) \mapsto (\zeta^a X, \zeta^b Y, Z).$$

We will compute the stabilizers of the places $P_0, \ldots, P_{n-1}, Q_0, \ldots, Q_{n-1}, Q'_0, \ldots, Q'_{n-1}$ ramified in $\mathbb{C}(F_n)/\mathbb{C}(x^n)$:

Lemma 10. *The points $(\zeta^k : 0 : 1)$ for $k = 0, \ldots, n-1$ are fixed by the cyclic group of order n generated by $\sigma_{0,1}$. The points $(0 : \zeta^k : 1)$, $k = 0, \ldots, n-1$ are fixed by the cyclic group of order n generated by $\sigma_{1,0}$. Finaly the points $(\zeta^k : 1 : 0)$ for $k = 0, \ldots, n-1$ are fixed by the cyclic group of order n generated by $\sigma_{1,1}$.*

Proof. By computation. □

5. AUTOMORPHISM GROUP OF THE HEISENBERG CURVE

Lemma 11. *If $(n,2)=1$, then the cover $C_n \to F_n$ is unramified.*

Proof. Notice first that

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^{\nu} = \begin{pmatrix} 1 & \nu x & \nu z + \frac{\nu(\nu-1)}{2} xy \\ 0 & 1 & \nu y \\ 0 & 0 & 1 \end{pmatrix}. \tag{6}$$

If $(n,2)=1$ then by eq. (6) every element in H_n has order at most n. Notice that the top right corner element is $\nu z + \frac{\nu(\nu-1)}{2} xy$ and $2 \mid (n-1)$.

Also the only points that can ramify in $C_n \to F_n$ are the points of the Fermat curve, which lie above $\{0,1,\infty\}$ since outside this set the cover is unramified. But if such a point P of the Heisenberg curve was ramified in $C_n \to F_n$, then its stabilizer $H_n(P)$ should be a cyclic group of order greater that n and no such group exist. □

Assume now that $(n,2)=2$. Consider the map $\pi : H_n \to H_n^{\mathrm{ab}} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ defined in equation (3). Let $\sigma_{a,b} \in H_n^{\mathrm{ab}}$ be the automorphism corresponding to the pair $(a,b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $a, b \in \mathbb{Z}/n\mathbb{Z}$.

Select an element $\alpha_{a,b}$ such that $\pi(\alpha) = \sigma_{a,b}$. Such an element has the following matrix form for some $z \in \mathbb{Z}/n\mathbb{Z}$:

$$\alpha_{a,b} = \begin{pmatrix} 1 & a & z \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}.$$

By eq. (6) if $ab = 0$ and $a = 1$ or $b = 1$ then the order $\mathrm{ord}(\alpha_{a,b})$ is at most n. So $\mathrm{ord}(\alpha_{1,0}) = n$ and $\mathrm{ord}(\alpha_{0,1}) = n$. Using again (6) we see that $\mathrm{ord}(\alpha_{1,1}) = 2n$.

This fact, combined to the computation of the stabilizers given in lemma 10 gives the following:

Lemma 12. *If $(n,2)=2$ in the cover $C_n \to F_n$ only the points $(\zeta^k : 1 : 0)$ above P_∞ can ramify with ramification index at most* 2.

In order to understand the even n case we will treat first the $n=2$ case.

Lemma 13. *The Heisenberg curve C_2 is rational and in $C_2 \to F_2$ only two points of F_2 are branched in the cover $C_2 \to F_2$, namely $(1:1:0)$ and $(-1:1:0)$.*

Proof. The case $n=2$ is special since the Fermat curve F_2 is rational. In this case the Heisenberg group H_2 has order 8 and is isomorphic to the dihedral group D_4 generated by the elements

$$a_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \bmod 2 \text{ and } a_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \bmod 2,$$

where the order of a_1 is 4 and the order of a_2 is 2. From the classification of finite subgroups of the projective line [29], we have the following: The curve F_2 has the group $D_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ inside its automorphism group, while in the cover $F_2 \to F_2/D_2$ three points $\{0,1,\infty\}$ are ramified with ramification indices 2. At least one point should ramify in the cover $C_2 \to F_2$ since F_2 is simply connected, this should be a cusp and the only cusps that are permitted by lemma 12 are $(1:1:0)$, $(-1:1:0)$ and both should ramifify. The genus of C_2 is zero by Riemann-Hurwitz formula. The ramification indices in the intermediate extensions are shown in the following table:

$$\begin{tikzcd}
C_2 \arrow[d, "\mathbb{Z}/2\mathbb{Z}"] \arrow[dd, bend right=60, "D_4"'] & & & Q_1 \arrow[d, dash, "2"] & Q_2 \arrow[d, dash, "2"] \\
F_2 \arrow[d, "D_2"] & P_1, P_2 \arrow[d, dash, "2"'] & P_3, P_4 \arrow[d, dash, "2"'] & P_5 \arrow[d, dash, "2"'] & P_6 \arrow[dl, dash, "2"'] \\
D_2\backslash F_2 & 1 & 0 & \infty &
\end{tikzcd}$$

Notice that the ramification type of D_4 acting on the rational function field is $(2,2,4)$, which is in accordance to the classification in [29]. ☐

Lemma 14. *If $2 \mid n$ then the cusps of C_n of the form $(\zeta^k : 1 : 0)$ are ramified in the cover $C_n \to F_n$ with ramification index equal to two.*

Proof. Observe now that the elements of order $2n$

$$\sigma_j := \begin{pmatrix} 1 & 1 & j \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

all restrict to $\sigma_{1,1} \in \mathrm{Aut}(F_n)$. Consider the points $Q'_1, \ldots, Q'_n$ of F_n that are above ∞ and for a fixed point Q'_{ν_0} consider the set of elements $\bar{Q}_{\nu_0,j}$ $j = 1, \ldots, t$ extending Q'_{ν_0} for $i = 1, \ldots, n$. Select now a point $\bar{Q}_{\nu_0,\mu_0}$ among them. If σ_0 does not fix $\bar{Q}_{\nu_0,\mu_0}$ the it moves it to the point $\bar{Q}_{\nu_0,j}$. But then there is an element $\tau \in \mathrm{Gal}(C_n, F_n) = Z_n$ moving $\bar{Q}_{\nu_0,\mu_0}$. Therefore its fixed by a matrix σ_j for an appropriate j. We compute

$$\sigma_j^n = \begin{pmatrix} 1 & 1 & j \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 & -n/2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in Z_n.$$

This means that in the cover $C_n \to (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})\backslash F_n$ the point $\bar{Q}_{\nu_0,\mu_0}$ is ramified with ramification index $2n$.

☐

Lemma 15. *The genus g_{C_n} of the curve C_n equals:*

$$g_{C_n} = \begin{cases} \frac{n^2(n-3)}{2} + 1 & \text{if } (n,2) = 1 \\ \frac{n^2(n-3)}{2} + \frac{n^2}{4} + 1 & \text{if } 2 \mid n \end{cases}$$

Proof. If $(n,2) = 1$, then the cover $C_n \to F_n$ is unramified with Galois group $Z_n = \mathbb{Z}/n\mathbb{Z}$ and Riemann-Hurwitz formula implies that

$$2g_{C_n} - 2 = n(2g_{F_n} - 2).$$

We know that $g_{F_n} = \frac{(n-1)(n-2)}{2}$ and this gives the result in this case.

If $2 \mid n$ then in the cover $C_n \to F_n$ n cusps of the Fermat curve are ramified with ramification index 2. These cusps have $\frac{n^2}{2}$ points in total above them, so Riemann-Hurwitz in this case gives

$$2g_{C_n} - 2 = n(2g_{F_n} - 2) + \frac{n^2}{2}, \tag{7}$$

and the desired result follows. ☐

We have the following diagram:

$$\begin{tikzcd}
C_n \arrow[d] & P_{1,j},\dots P_{n,j} \arrow[d, dash] & Q_{1,j},\dots Q_{n,j} \arrow[d, dash] & Q'_{1,j},\dots Q'_{n/e,j} \arrow[d, dash, "e=1 \text{ or } 2"] \\
F_n \arrow[d] & P_j \arrow[d, dash] & Q_j \arrow[d, dash] & Q'_j \arrow[d, dash] \\
\mathbb{P}^1 \cong \frac{F_n}{\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}} & 0 & 1 & \infty
\end{tikzcd}$$

where $j = 0, \dots, n-1$ and e is 1 or 2 according to the value of $n \bmod 2$.

6. MODULAR AUTOMORPHISMS

6.1. **The Fermat curve.**

The open Fermat curve is the curve $F_n^0 := \ker\psi\backslash\mathbb{H}$, where

$$\ker\psi := \langle a^n, b^n, [a,b]\rangle \subset \langle a, b\rangle = \Gamma(2).$$

Notice that the above group differs from the universal covering group $\Delta(n,n,n)'$ given in section 2 which correspond to the closed Fermat curve.

Every automorphism of the Fermat curve is modular. Indeed, the generators $\sigma_{1,0}$, $\sigma_{0,1}$ of the $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$ part of the automorphism group, are coming from the deck transformations $a, b \in \pi^1(\mathbb{P}^1\backslash\{0,1,\infty\}) = \Delta \subset \mathrm{SL}(2,\mathbb{Z}) \subset \mathrm{SL}(2,\mathbb{R})$. On the other hand it is known [32, exer. 3 p. 32] that $S_3 = \mathrm{SL}(2,\mathbb{Z})/\Gamma(2)$ and the action is given by lifts of elements of S_3 to $\mathrm{SL}(2,\mathbb{Z})$. The fact that all automorphisms are indeed modular comes from the fact that $\mathrm{SL}(2,\mathbb{Z})$ leaves both the set $\mathbb{H}$ and the cusps $\mathbb{P}^1$ invariant.

Let $\mathbf{F}_n$ denote the free group in n generators. Notice that the group S_3 acts by conjugation on Δ so it can be seen as a subgroup of the group of outer automorphisms of Δ. It is known [5, exam. 1 p. 117], [6, th. 3.1.7 p. 125] that the epimorphism

$$\mathbf{F}_2 \to \mathbf{F}_2^{\mathrm{ab}} \cong \mathbb{Z}\times\mathbb{Z}$$

induces an isomorphism of

$$\mathrm{Out}(\mathbf{F}_2)/\mathrm{In}(\mathbf{F}_2) = \mathrm{Aut}(\mathbf{F}_2) \to \mathrm{GL}(2,\mathbb{Z}).$$

The group S_3 is generated by the folowing automorphisms of the free group $\mathbf{F}_2 = \langle a, b\rangle$:

$$i_1 : a \leftrightarrow b \qquad i_2 : \begin{array}{l} a \mapsto b^{-1}a^{-1} \\ b \mapsto b \end{array} \tag{8}$$

The above generators i_1, i_2 of S_3 keep the group $\ker\psi$ invariant.

On the other hand, an arbitrary element of S_3 reduces to an action on the Fermat curve F_n by permutation of the variables X, Y, Z in the projective model of the curve. The automorphism intechanging X, Y coressponds to the involution interchanging a, b. Let us now consider the automorphism $\bar{\tau}$ interchanging X, Z in the projective model the Fermat curve.

Denote by $\sigma_{i,j}$ the automorphism of the Fermat curve sending

$$\sigma_{i,j} : (X : Y : Z) \mapsto (\zeta^i X : \zeta^j Y : Z).$$

By computation we have

$$\bar{\tau}\sigma_{i,j}\bar{\tau}^{-1} : (X : Y : Z) \mapsto (X : \zeta^j Y : \zeta^i Z) = (\zeta^{-i}X : \zeta^{-i+j}Y : Z).$$

Therefore, the conjugation action of $\bar{\tau}$ on $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z})$ is given by the matrix $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$.

6.2. **The Heisenberg curve.** We will now describe the automorphisms of the Fermat curves F_n that can be lifted to automorphisms of C_n. Every representative $\sigma \in \mathrm{Aut}(\mathbb{H})$ of an element $\bar{\sigma} \in \mathrm{Aut}(F_n) = N_{\mathrm{SL}(2,\mathbb{R})}(\ker\psi)/\ker\psi$ should keep the group $\ker\psi$ invariant when acting by conjugation. The subgroup of the automorphism group of F_n should also keep the group

$$\ker(\phi) = \langle a^n, b^n, [a,b]^n \rangle$$

invariant, in order to extend to an automorphism of C_n.

The elements a, b generating $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ modulo $\ker\psi$ keep both groups $\ker\phi, \ker\psi$ invariant, so $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} < \mathrm{Aut}(F_n)$ is lifted to a subgroup of automorphisms of C_n.

Let $\sigma \in \Gamma$ be a representative of an element $\bar{\sigma} \in S_3 \subset \mathrm{Aut}(F_n)$. This element is lifted to an automorphism of the group C_n if and only if the conjugation action of σ keeps the defining group $\ker\phi$ invariant.

Let i_1, i_2 be the involutions generating S_3 as defined in eq. (8). Checking that the involution i_1 keeps $\ker\phi$ invariant is trivial.

We will now check the involution i_2: It is clear that $(b^n)^{i_2} = b^{i_2}$ and $[a,b]^{i_2} = [b^{-1}, a^{-1}]$ so $([a,b]^n)^{i_2} = [b^{-1}, a^{-1}]^n$.

Let a_H, b_H be the generators of the Heisenberg group, seen as elements in $F_2 = \langle a_H, b_H \rangle / \ker\phi$ as given in eq. (1). In order to check whether the generator a^n of $\ker\phi$ are sent to $\ker\phi$ under the action of i_2 it is enough to prove that its image modulo $\ker\phi$ is the zero element in the Heisenberg group. We compute

$$a_H^{i_2} = b_H^{-1} a_H^{-1} \text{ and } b_H^{i_2} = b_H.$$

Therefore

$$a_H^{i_2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

so by eq. (6) we have

$$\left(a_H^{i_2}\right)^n = \begin{cases} \begin{pmatrix} 1 & 0 & -\frac{n}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \text{if } n \equiv 0 \bmod 2 \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \text{if } (n,2) = 1 \end{cases}$$

and this gives the identity matrix if and only if $(n,2) = 1$. Therefore in the case $2 \mid n$ the element $(a^n)^{i_2}$ does not belong to the group $\ker\phi$.

Lemma 16. *The modular automorphism group for the Heisenberg curve is given by an extension*

$$1 \to \mathbb{Z}/n\mathbb{Z} \to \mathrm{Aut}^{\mathrm{m}}(C_n) \to G_n \to 1$$

where G_n is the group

$$G_n = \begin{cases} \mathrm{Aut}(F_n) & \textit{if } (n,2) = 1 \\ (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z} & \textit{otherwise} \end{cases}$$

Proof. The Heisenberg group is already in the automorphism group, fitting in the short exact sequence

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & \mathrm{Aut}^{\mathrm{m}}(C_n) \arrow[r] & G_n \arrow[r] & 1 \\
1 \arrow[r] & \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[u, equal] & H_n \arrow[r] \arrow[u, hook] & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

We have computed the part of $\mathrm{Aut}(F_n)$ which lifts to automorphisms of C_n according to the value of n modulo 2.

We will now prove that every modular automorphism of C_n restricts to an automorphism of F_n. Indeed, using proposition 8 we have to show that every automorphism σ that fixes by conjugation elements of $\langle a^n, b^n, [a,b]^n\rangle$ fixes elements of $\langle a^n, b^n, [a,b]\rangle$ as well.

Assume that σ fixes the group $\langle a^n, b^n, [a,b]^n\rangle$. If $(a^n)^\sigma$ is a word in $a^n, b^n, [a,b]^n$ then it is obviously a word in $a^n, b^n, [a,b]$. For the commutator we will use the following result due to Nielsen [19, th. 3.9]

$$[a,b]^\sigma = T[a,b]^{\pm 1}T^{-1},$$

where T is a word in a, b. So the invariance of the commutator $[a,b]$ under the action of the outer automorphism σ follows since $\langle a^n, b^n, [a,b]\rangle$ is a normal subgroup of $\langle a, b\rangle$. □

Lemma 17. *For* $2 \mid n$ *three points are ramified in* $C_n \mapsto \mathrm{Aut}^{\mathrm{m}}(C_n)$*, with ramification indices* $4n, n, 2$*.*

Proof. In the cover $C_n \rightarrow F_n \rightarrow (\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z})\backslash F_n \cong \mathbb{P}^1$ we have ramification on the points $P_{x=0}, P_{x=1}$ and P_∞, with ramification indices $n, n, 2n$.

Consider the group S_3 acting on $(\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z})\backslash F_n$ and generated by the automorphisms $x \mapsto f(x)$, where

$$f(x) \in \left\{x, 1-x, \frac{1}{x}, \frac{1}{1-x}, \frac{x}{x-1}, \frac{x-1}{x}\right\}.$$

The involution $i_1 : a \leftrightarrow b$ in terms of generators of the free group, corresponds to the involution $x \mapsto 1-x$, which sends $1 \leftrightarrow 0$ and keeps $\infty, 1/2$ invariant. Therefore, the three ramified points have ramification indices $2, n, 4n$. □

Theorem 18. *Every automorphism of* C_n *is modular, i.e., sends the cusps to the cusps. In particular the automorphism group of the curve* C_n *in this case equals:*

$$\mathrm{Aut}(C_n) = N_{\mathrm{SL}(2,\mathbb{R})}(\ker\phi)/\ker\phi.$$

Proof. If $(n,2)=1$ then the group $D(n)$ corresponding to the Heisenberg curve in the triangle uniformization given in eq. (5) is a normal subgroup of $\Delta(n,n,n)$. The normalizer $N_{\mathrm{PSL}(2,\mathbb{R})}(D(n))$ contains the trigonal curve $\Delta(n,n,n)$ and since every group containing a triangle group with finite index is also triangle [2, th. 10.6.5 p.279] the normalizer is also a triangle group. By the computation of the modular automorphism group and the classification given in [11, table 2] we have that $N_{\mathrm{PSL}(2,\mathbb{R})}(D(n)) = D(2,n,2n)$, which gives us

$$\mathrm{Aut}(C_n) = \frac{N_{\mathrm{PSL}(2,\mathbb{R})}(D(n))}{D(n)} = \mathrm{Aut}^{\mathrm{m}}(C_n).$$

For the $2 \mid n$ case we will employ the Riemann-Hurwitz formula. Let G be the automorphism group, $|G| = 2n^3 m$, where $m = [G : \mathrm{Aut}^{\mathrm{m}}(C_n)]$. Let $Y = C_n^G$. Since $\mathbb{C}(Y) \subset C_n^{H_n}$ we have that $g_Y = 0$. By eq. (7) $2g_{C_n} - 2 = n^2(n-3) + n^2/2$ and Riemann-Hurwitz theorem [9, ex. IV.2.5] gives us that

$$n^2(n-3) + n^2/2 = n^3 2m(-2 + \sum_{i=1}^{r}(1 - 1/e_i))$$

where $e_i \geq 2$ are the ramification indices of the r-points of $\mathbb{P}^1$ ramified in extension $C_n \rightarrow G\backslash C_n = \mathbb{P}^1$. Set $\Omega_n = -2 + \sum_{i=1}^{r}(1 - 1/e_i)$. Then the Riemann-Hurwitz formula can be written as

$$n - 5/2 = 2mn\Omega_n.$$

Observe that $\Omega_n \geq 0$ and $m \geq 1$. So for $n > 3$ we must have $\Omega_n > 0$. If $\Omega_n \geq 1/4$, then it is obvious that $m = 1$. Indeed, we should have

$$1 \leq m = \frac{2n-5}{4n\Omega_n} \leq 2 - 5/n < 2. \tag{9}$$

In the above formula we have that for $n \leq 4$ the term $2-5/n < 1$, which is not compatible with the $1 \leq m$ inequality. This means that for $n = 4$ the inequality $\Omega_n \geq 1/4$ is not possible so $\Omega_n < 1/4$. For Ω_4 the ramification index index for one point is at least $16 = 4n$.

$$\Omega_4 = -2 + \left(1 - \frac{1}{16e}\right) + \sum_{i=2}^{r} \left(1 - \frac{1}{e_i}\right) \geq -\frac{17}{16} + \frac{r-1}{2}.$$

The above value for Ω_4 is negative for $r \leq 3$ and $1/4$ for $r = 4$. So we need less than 3 ramification points, which we assume that have ramification indices $16e, \kappa, \lambda$. In this case we have

$$\Omega_4 = 1 - \frac{1}{16e} - \frac{1}{\ell} - \frac{1}{\kappa}.$$

Since this value has to be smaller than $1/4$ the values for e, λ, κ can not take very big values. If both $\kappa, \ell \geq 3$ then

$$\Omega_4 \geq 1 - \frac{1}{16} - \frac{2}{3} > \frac{1}{4}$$

which is impossible. So $\kappa = 2$ and $\lambda = 3$ is the only possible case. For this case $\Omega_4 \geq 5/48$ and eq. (9) implies that $m \leq 9/5 < 2$.

Now we consider the $n > 4$ case and we will show that $\Omega_n \geq 1/4$. If three or more points, other than the one with $e_1 = 4ne$, are ramified in the cover $C_n \to Y$, then

$$\Omega_n = -2 + 1 - \frac{1}{4ne} + \sum_{i=2}^{r} \left(1 - \frac{1}{e_i}\right) \geq \frac{1}{2} - \frac{1}{4ne} \geq \frac{1}{4}.$$

Consider now that exactly three points are ramified in $C_n \to Y$. If two of them are ramified with ramification index 2 then $\Omega_n = -1/4n$ and this is not allowed since $\Omega_n \geq 0$.

Assume now that we have exactly 3 ramification points with ramification $(4ne, \kappa, \ell)$. In this case

$$\Omega_n \geq -2 + \left(1 - \frac{1}{4n}\right) + \left(1 - \frac{1}{\ell}\right) + \left(1 - \frac{1}{\kappa}\right) = 1 - \frac{1}{4n} - \frac{1}{\ell} - \frac{1}{k}.$$

If $n > 4$ then $n \geq 6$ (n is even) so

$$\Omega_n \geq \frac{23}{24} - \frac{1}{\ell} - \frac{1}{k}.$$

It is clear that the above quantity is bigger than $1/4$ if ℓ and κ are big enough. For instance if $\ell, \kappa \geq 3$ then $23/24 - 2/3 = 7/24$ and $\Omega_n \geq 1/4$. We have to check the case $\kappa = 2$ and in this case $\Omega_n = 23/24 - 1/2 - 1/\ell = 11/24 - 1/\ell$ so the inequality $\Omega_n \geq 1/4$ holds provided $\ell \geq 5$.

The cases $\ell = 3, 4$ give the corresponding bounds $B_\ell = (2n-5)\Omega_\ell/(4n)$,

$$B_3 = \frac{3(2n-5)}{n(3n+2)}, \qquad B_4 = \frac{2n-5}{n^2+n},$$

All the above values are < 1 and can not bound the quantity m, hence they can't occur. □

7. THE CURVE C_3

The Fermat curve $F_3 : x^3 + y^3 = 1$ is elliptic and it has the projective cannonical Weierstrass form $zy^2 = x^3 - 432z^3$, see [14, p. 50-52] and [10, ex. 3 p.32]. Its torsion 3-points are the flexes which can be computed as the zeros of the Hessian determinant:

$$\mathrm{Hess}(y^2z - x^3 + 432z^3) = \det \begin{pmatrix} -6x & 0 & 0 \\ 0 & 2z & 2y \\ 0 & 2y & 2592y \end{pmatrix} = 24(y^2 - 1296z^2)x.$$

- If $x = 0$, then $zy^2 = -432z^3$ which gives the solutions

$$(0 : 1 : 0), (0 : 12\sqrt{-3} : 1), (0 : -12\sqrt{-3} : 1).$$

- If $x \neq 0$, then $y^2 = 1296z^2$, which gives the solutions $(1:0:0)$, which does not satisfy the equation of the elliptic curve. We also have the solution $y = \pm\sqrt{1296}z$, which we plug into the equation of the elliptic curve to obtain:
  $$z^3 1296 = x^3 - 432z^3,$$
  so for $z = 1$ we obtain $x^3 = 1728$ so $x = 12\zeta_3^i$, and $\zeta_3 = (-1+\sqrt{-3})/2$ is a primitive third root of unity. We therefore have 6-more 3-torsion points namelly
  $$(12\zeta_3^i : \pm 36 : 1).$$

The curve C_3 is by Riemann-Hurwitz formula also an elliptic curve and the covering map

$$C_3 \to F_3$$

is an isogeny. For each point of order 3 computed above Vélu method [30] can be applied and using sage [26] we compute the following table:

point of order 3	Equation of isogenus curve	j-invariant
$(0 : \pm 12\sqrt{-3} : 1)$	$y^2 = x^3 + 11664$	0
$(-6(1+\sqrt{-3}) : \pm 36 : 1)$	$y^2 = x^3 + 2160(1-\sqrt{-3})x - 109296$	-12288000
$(6(1-\sqrt{-3}) : \pm 36 : 1)$	$y^2 = x^3 + 2160(1+\sqrt{-3})x - 109296$	-12288000
$(12 : \pm 36 : 1)$	$y^2 = x^3 - 4320x - 109296$	-12288000

The three last curves have the same j-invariant and are isomorphic (they are quadratic twists of each other). The first one has j-invariant zero and therefore the automorphism group $\mathrm{Aut}^0(E)$ of E, consisted of automorphisms $E \to E$ which fix the identity, is a cyclic group of order 6, see [24, ch. III. par. 10.1]. This is compatible with the structure of the Heisenberg curve C_3, since the neutral element of C_3 is fixed by a group of order 6.

On the other hand the other 3 isomorphic curves of the above table have j-invariant $\neq 0, 1728$ so $\mathrm{Aut}^0(E)$ is a cyclic group of order 2. Therefore the equation of C_3 is given by

$$C_3 : y^2 = x^3 + 2^4 \cdot 3^6.$$

REFERENCES

1. Matthew Baker and Yuji Hasegawa, *Automorphisms of $X_0^*(p)$*, J. Number Theory **100** (2003), no. 1, 72–87. MR 1971247
2. A.F. Beardon, *The geometry of discrete groups*, Graduate Texts in Mathematics, Springer New York, 1995.
3. G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479. MR MR534593 (80f:12008)
4. ———, *A new proof of the three-point theorem*, Mat. Sb. **193** (2002), no. 3, 21–24. MR 1913596 (2003b:14030)
5. Joan S. Birman, *Braids, Links, and Mapping class Groups*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1974, Annals of Mathematics Studies, No. 82. MR 0375281
6. Oleg Bogopolski, *Introduction to Group Theory*, EMS Textbooks in Mathematics, European Mathematical Society (EMS), Zürich, 2008, Translated, revised and expanded from the 2002 Russian original. MR 2396717
7. Leon Greenberg, *Maximal Fuchsian Groups*, Bull. Am. Math. Soc. **69** (1963), no. 4, 569–573.
8. Michael Corin Harrison, *A new automorphism of $X_0(108)$*, (2011).
9. Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.
10. Dale Husemöller, *Elliptic Curves*, second ed., Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004, With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. MR 2024529
11. Sadok Kallel and Denis Sjerve, *On the group of Automorphisms of cyclic covers of the Riemann sphere*, Math. Proc. Cambridge Philos. Soc. **138** (2005), no. 2, 267–287.
12. S Kamienny, *On the automorphism groups of some modular curves*, Math. Proc. Cambridge Philos. Soc. **134** (2003), no. 01, 61–64.
13. M A Kenku and Fumiyuki Momose, *Automorphism groups of the modular curves $X_0(n)$*, Compos. Math. **65** (1988), no. 1, 51–80.
14. Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR 1193029
15. Aristides Kontogeorgis, *Automorphisms of Fermat-like varieties*, Manuscripta Math. **107** (2002), no. 2, 187–205.

16. Aristides Kontogeorgis and Victor Rotger, *On the non-existence of exceptional automorphisms on Shimura curves*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 363–374. MR 2418792 (2009c:11089)
17. Aristides Kontogeorgis and Yifan Yang, *Automorphisms of hyperelliptic modular curves $X_0(N)$ in positive characteristic*, LMS J. Comput. Math. **13** (2010), 144–163. MR 2638986
18. Heinrich-Wolfgang Leopoldt, *Über die Automorphismengruppe des Fermatkörpers*, J. Number Theory **56** (1996), no. 2, 256–282.
19. Wilhelm Magnus, Abraham Karrass, and Donald Solitar, *Combinatorial group theory*, second ed., Dover Publications, Inc., Mineola, NY, 2004, Presentations of groups in terms of generators and relations. MR 2109550
20. James S. Milne, *Modular functions and modular forms (v1.31)*, 2017, Available at www.jmilne.org/math/, p. 134.
21. Santiago Molina and Victor Rotger, *Automorphisms and reduction of Heegner points on Shimura curves at Cerednik-Drinfeld primes*, Proc. Am. Math. Soc. **142** (2013), no. 2.
22. David Ephraim Rohrlich, *Modular Functions and the Fermat Curves*, ProQuest LLC, Ann Arbor, MI, 1976, Thesis (Ph.D.)–Yale University. MR 2626317
23. Tetsuji Shioda, *Arithmetic and geometry of Fermat curves*, Algebraic Geometry Seminar (Singapore, 1987), World Sci. Publishing, Singapore, 1988, pp. 95–102.
24. Joseph H. Silverman, *The arithmetic of Elliptic Curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094
25. David Singerman, *Finitely maximal Fuchsian groups*, J. Lond. Math. Soc. **s2-6** (1972), no. 1, 29–38.
26. W. A. Stein et al., *Sage Mathematics Software (Version 8.9)*, The Sage Development Team, 2019, `http://www.sagemath.org`.
27. Henning Stichtenoth, *Algebraic Function Fields and Codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR 2464941 (2010d:14034)
28. Pavlos Tzermias, *The group of automorphisms of the Fermat curve*, J. Number Theory **53** (1995), no. 1, 173–178.
29. Robert C. Valentini and Manohar L. Madan, *A hauptsatz of L. E. Dickson and Artin-Schreier extensions*, J. Reine Angew. Math. **318** (1980), 156–177. MR 82e:12030
30. Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. MR 294345
31. Jürgen Wolfart, *The "obvious" part of Belyi's theorem and Riemann surfaces with many automorphisms*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 97–112. MR 1483112
32. Masaaki Yoshida, *Hypergeometric functions, my love*, Aspects of Mathematics, E32, Friedr. Vieweg & Sohn, Braunschweig, 1997, Modular interpretations of configuration spaces. MR 1453580

DEPARTMENT OF MATHEMATCIS, UNIVERSITY OF CRETE, HERAKLEION CRETE GREECE 71409
Email address: `antoniad@uoc.gr`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ATHENS, PANEPISTIMIOUPOLIS, 15784 ATHENS, GREECE
Email address: `kontogar@math.uoa.gr`