

THE HEISENBERG COVERING OF THE FERMAT CURVE

DEBARGHA BANERJEE AND LOÏC MEREL

ABSTRACT. For N integer ≥ 1 , K. Murty and D. Ramakrishnan defined the N -th Heisenberg curve, as the compactified quotient X'_N of the upper half-plane by a certain non-congruence subgroup of the modular group. They ask whether the Manin-Drinfeld principle holds, namely if the divisors supported on the cusps of those curves are torsion in the Jacobian. We give a model over $\mathbf{Z}[\mu_N, 1/N]$ of the N -th Heisenberg curve as covering of the N -th Fermat curve. We show that the Manin-Drinfeld principle holds for $N = 3$, but not for $N = 5$. We show that the description by generator and relations due to Rohrlich of the cuspidal subgroup of the Fermat curve is explained by the Heisenberg covering, together with a higher covering of a similar nature. The curves X_N and the classical modular curves $X(n)$, for n even integer, both dominate $X(2)$, which produces a morphism between jacobians $J_N \rightarrow J(n)$. We prove that the latter has image 0 or an elliptic curve of j -invariant 0. In passing, we give a description of the homology of X'_N .

CONTENTS

1. Introduction	1
2. Heisenberg Groups and the lower central series of $\bar{\Gamma}(2)$	4
3. The associated Riemann surfaces	11
4. The Heisenberg covering and its models	18
References	28

1. INTRODUCTION

Let Γ be a subgroup of finite index of $SL_2(\mathbb{Z})$. This subgroup acts by homographies on the complex upper half-plane \mathfrak{H} . Consider the corresponding modular curve $Y_\Gamma = \Gamma \backslash \mathfrak{H}$, and

2010 *Mathematics Subject Classification*. Primary: 11D11, Secondary: 11F11, 11G05, 11G30.

Key words and phrases. Fermat's curves, Modular symbols, Heisenberg curves.

The author was partially supported by the SERB grant MTR/2017/000357 and CRG/2020/000223. The first named author is deeply indebted to Professor Yuri Manin for several stimulating conversation at the MPIM. The authors are deeply indebted to the anonymous referees for careful reading of the paper. We are sincerely grateful to the anonymous referee for drawing our attention to [1].

its compactification obtained by adding the cusps X_Γ . We say that X_Γ satisfies the Manin-Drinfeld principle if any cuspidal (i.e. supported on the cusps) divisor of degree 0 is torsion in the Jacobian of X_Γ . Manin and Drinfeld proved that it is the case when Γ is a congruence subgroup.

For a subgroup of finite index (not necessarily a congruence subgroup), K. Murty and Ramakrishnan [13] give an analytic criterion for the Manin-Drinfeld principle to be satisfied. As an illustrative example, Murty and Ramakrishnan consider modular curves attached to certain subgroups of $\Gamma(2)$: Fermat curves, and what they propose to call Heisenberg curves. We revisit those examples. In [2], we reconsider this question and give an analytic criterion of a different nature, but also based on Eisenstein series; this is unconnected to the present work, which is purely algebraic in nature.

The Heisenberg curves are defined as follows from the complex analytic point of view. Let A and B be the classes of the matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ respectively in $\bar{\Gamma}(2) = \Gamma(2)/\{\pm 1\}$. These matrices generate freely the group $\bar{\Gamma}(2)$. Let $C = ABA^{-1}B^{-1}$.

Let N be an integer > 0 . Denote by Φ_N the kernel of the morphism $\bar{\Gamma}(2) \rightarrow (\mathbb{Z}/N\mathbb{Z})^2$ which to A associates $(1, 0)$ and to B associates $(0, 1)$. The corresponding modular curve is the Fermat modular curve and is denoted by X_N . It can be identified with the complex points of the Fermat curve F_N (see for instance [17], [7]). Let Φ'_N be the subgroup of Φ_N generated by A^N, B^N, C^N and the third term $[\bar{\Gamma}(2), [\bar{\Gamma}(2), \bar{\Gamma}(2)]]$ in the descending central series of $\bar{\Gamma}(2)$. An exact sequence of groups follows

$$1 \rightarrow \Phi'_N \rightarrow \bar{\Gamma}(2) \rightarrow H_N \rightarrow 1,$$

where H_N is a central extension of $(\mathbb{Z}/N\mathbb{Z})^2$ by $\mathbb{Z}/N\mathbb{Z}$ (coinciding with the $\mathbb{Z}/N\mathbb{Z}$ -points of the Heisenberg group). The N -th Heisenberg modular curve, in the sense of Murty and Ramakrishnan, is $X'_N = X_{\Phi'_N}$.

Let $\mathbb{Q}(\mu_N)$ be a cyclotomic extension of \mathbb{Q} generated by N -th roots of unity. Denote by $\mathbb{Z}[\mu_N]$ its ring of integers. The covering $X'_N \rightarrow X_N$ extends to a morphism $F'_N \rightarrow F_N$ of curves over $\mathbb{Q}(\mu_N)$ that we call the Heisenberg covering of the Fermat curve.

Theorem 1. *Suppose N is an odd integer. The Heisenberg modular curve X'_N extends to a smooth projective scheme \mathcal{F}'_N of relative dimension one over $\text{Spec}(\mathbb{Z}[\mu_N, 1/N])$ given by the following model:*

$$X^N + Y^N = Z^N$$

and, for every primitive N -th root of unity ζ in $\mathbb{Q}(\mu_N)$

$$\prod_{j=1}^{(N-1)/2} (Y - \zeta^{-j}Z)^j T_\zeta^N = \prod_{j=1}^{(N-1)/2} (Y - \zeta^j Z)^j U_\zeta^N.$$

It seems to have been known to Deligne (see a comment in [13]) that the generic fiber F'_N of \mathcal{F}'_N can be defined over \mathbb{Q} , an assertion for which we provide a proof.

Rohrlich [17] (see also Vélú [18]) has determined the cuspidal subgroup of F_N . In particular, he has shown that any cuspidal divisor on F_N is of order dividing N . This description plays a key role in justifying the existence of the Heisenberg covering. We show that, by going further in the descending central series of $\Gamma(2)$, X'_N is covered by a modular curve X''_N , in such a way that X''_N is still an abelian covering of the Fermat curve X_N . We do not describe algebraically X''_N .

We note that there has been a considerable interest in the cuspidal group of the Fermat curve. For instance, in [10], p. 39, Mazur draws (or rather “stretches”) an analogy between Fermat curves and modular curves. Such an analogy is somewhat strengthened by the fact that the Heisenberg covering is analogous to the familiar Shimura covering $X_1(N) \rightarrow X_0(N)$ between modular curves.

Like Murty and Ramakrishnan, our goal had been to illustrate our study of non-congruence subgroups by examining Heisenberg curves. We can not determine in general whether such curves satisfy the Manin-Drinfeld principle. But we can show easily that the principle holds for $N = 3$. Furthermore, for $N = 3$, we study the connection between F'_3 and various modular curves. By contrast, for $N = 5$:

Theorem 2. *There exists a cuspidal divisor on X'_5 whose class in the jacobian of X'_5 is of infinite order.*

Let $\bar{\Gamma}'(2)$ be the subgroup of index 3 of $\bar{\Gamma}(2)$ obtained by pulling back the 2-Sylow subgroup of $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z})$. Let Γ be a congruence subgroup of $\bar{\Gamma}(2)$. Consider the correspondence $X'_N \rightarrow X_\Gamma$ obtained by combining pulling back to the modular curve $X_{\Gamma \cap \Phi'_N}$ with pushing to X_Γ . It produces a morphism of abelian varieties between the jacobians or Riemann surfaces $\theta_{N,\Gamma}: J'_N \rightarrow J_\Gamma$. In view of the following statement, we can hardly have any hope of establishing a limited form of the Manin-Drinfeld principle for Heisenberg curves using the classical Manin-Drinfeld theorem for congruence subgroups.

Theorem 3. *The morphism $\theta_{N,\Gamma}$ is zero if and only if either $3 \nmid N$ or Γ is not contained in $\bar{\Gamma}'(2)$. If $3 \mid N$ and Γ is contained in $\bar{\Gamma}'(2)$, the image of $\theta_{N,\Gamma}$ is isogenous to an elliptic curve with j -invariant 0. Furthermore, when Γ is contained in $\bar{\Gamma}'(2)$, $\theta_{3,\Gamma}$ has finite kernel.*

The proof of theorem 3 is a translation of a group theoretic statement: any term of the lower central series of $\bar{\Gamma}(2)$ is essentially dense in adelic completions of $\bar{\Gamma}(2)$ (see Proposition 13). In addition to these results of algebraic nature, we give a combinatorial description of the homology of the Riemann surface X'_N , by a method similar to Manin’s presentation, but following the variant introduced in [12]. This might have an interest of its own. But it does not help us for establishing our other results.

One of the referees noted connections to the work of Anderson and Ihara [1], as well as unpublished computations of Deligne. We hope that all this will be made explicit in the future.

2. HEISENBERG GROUPS AND THE LOWER CENTRAL SERIES OF $\bar{\Gamma}(2)$

2.1. The Heisenberg group. The Heisenberg group is the algebraic group of 3×3 unipotent

upper triangular matrices. Set: $x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ and $z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Those elements satisfy the relations $xz = zx$, $yz = zy$ and $z = xyx^{-1}y^{-1} = [x, y]$. Thus one obtains a presentation of the Heisenberg group over the integers. Note the formula, for $a, b, c \in \mathbf{Z}$

$$x^a z^b y^c = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

From that perspective, the group law is given by

$$x^a z^b y^c x^{a'} z^{b'} y^{c'} = x^{a+a'} z^{b+b'+a'c} y^{c+c'}.$$

The Heisenberg group $H_{\mathbf{Z}}$ over \mathbf{Z} can be identified with \mathbf{Z}^3 with the previous group law. The abelianization of $H_{\mathbf{Z}}$ is freely generated by the images of x and y and is thus isomorphic to \mathbf{Z}^2 . Thus $H_{\mathbf{Z}}$ is a central extension of \mathbf{Z}^2 by \mathbf{Z} .

Let M and N be natural integers. Let L be a common divisor of M and N . Let $H_{M,N,L}$ be the quotient group of $H_{\mathbf{Z}}$ spanned by x and y with relations $xz = zx$, $yz = zy$, $z = xyx^{-1}y^{-1}$ and $x^M = y^N = z^L = 1$. Such a group can be identified (as a set) with $\mathbf{Z}/M\mathbf{Z} \times \mathbf{Z}/L\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ via the inverse of the map $(a, b, c) \mapsto x^a z^b y^c$.

Note the map $H_{M,N,L} \rightarrow \mathbf{Z}/M\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ is coming from the abelianization.

Let M', N' and L' be integer ≥ 1 such that $M|M'$, $N|N'$, and $L|L'$. The canonical group homomorphism $H_{M',N',L'} \rightarrow H_{M,N,L}$ is surjective. Its kernel is generated by $\{x^M, y^N\}$. Since $[x^M, y^N] = z^{NM}$, this kernel is abelian if and only if $L'|NM$.

Proposition 4. *Let T be the lower common multiple of M and N . The group $H_{M,N,L}$ is of exponent T if T is odd or T/L is even. It is of exponent $2T$ otherwise. In particular $H_{N,N,N}$, for N odd, and $H_{N,N,N/2}$, for N even, are of exponent N .*

Proof. Let $\alpha, \beta \in H_{M,N,L}$ in the subgroups generated by x and y respectively. Let $e = T$ if T is odd or T/L is even. Let $e = 2T$ otherwise. Since $[\alpha, \beta]$ belongs to the center of $H_{M,N,L}$, it is of order dividing L . Moreover, one has $(\alpha\beta)^n = \alpha^n [\alpha, \beta]^{n(n-1)/2} \beta^n$, which vanishes if $n = e$. By this calculation, one has $(xy)^n = x^n z^{n(n-1)/2} y^n$, which shows that xy is of order T . \square

Since the group $\bar{\Gamma}(2) = \Gamma(2)/\{\pm 1\}$ is freely generated by A and B , one gets a surjective group homomorphism $\bar{\Gamma}(2) \rightarrow H_{\mathbb{Z}}$ which sends A and B to x and y respectively. Its kernel is $[\bar{\Gamma}(2), [\bar{\Gamma}(2), \bar{\Gamma}(2)]]$. Every (necessarily nilpotent) finite quotient group of $\bar{\Gamma}(2)$ which factorizes through $\bar{\Gamma}(2)/[\bar{\Gamma}(2), [\bar{\Gamma}(2), \bar{\Gamma}(2)]]$ is isomorphic to one of the groups $H_{M,N,L}$.

Denote by $\Gamma_{M,N,L}$ the kernel of the map $:\bar{\Gamma}(2) \rightarrow H_{\mathbb{Z}} \rightarrow H_{M,N,L}$.

2.2. The lower central series. Recall that the lower central series $(G_k)_{k \geq 1}$ of a group G is defined recursively by $G_1 = G$ and $G_{k+1} = [G_k, G]$. The quotient G_k/G_{k+1} is then an abelian group. When G is a free group generated by the family $(t_i)_{i \in I}$, G_k/G_{k+1} is a free abelian group generated (not freely) by the classes of the commutators of weight k on the generators, i.e. by the $[t_{i_1}, \dots, t_{i_k}]$, where the indices run through any sequence $\{1, 2, \dots, k\} \rightarrow I$ [6, Theorem 10.2.3]. When, furthermore, I is finite of cardinality m , the rank r_k of G_k/G_{k+1} is given by Witt's formula, involving the necklace polynomial,

$$r_k(G) = \frac{1}{k} \sum_{d|k} \mu(d) m^{k/d},$$

where μ is the Möbius function. In particular the lower central series $(\bar{\Gamma}(2)_k)_{k \geq 1}$ of $\bar{\Gamma}(2)$ satisfies $r_1(\bar{\Gamma}(2)) = 2$, $r_2(\bar{\Gamma}(2)) = 1$, $r_3(\bar{\Gamma}(2)) = 2$ and $r_4(\bar{\Gamma}(2)) = 3$. The corresponding generators of $\bar{\Gamma}(2)_k/\bar{\Gamma}(2)_{k+1}$ for $k = 1, 2, 3$ are the classes of $\{A, B\}$, $\{C\}$, and $\{[C, A], [C, B]\}$ respectively. Therefore one has a surjective group morphism $\phi_1 : \bar{\Gamma}(2) \rightarrow \mathbb{Z}^2$ such that $\phi_1(A) = (1, 0)$ and $\phi_1(B) = (0, 1)$. Its kernel is $\bar{\Gamma}(2)_2$. Moreover, one gets a group isomorphism: $\bar{\Gamma}(2)_1/\bar{\Gamma}(2)_3 \simeq H_{\mathbb{Z}}$.

Next we have the surjective group morphism $\phi_2 : \bar{\Gamma}(2)_2 \rightarrow \mathbb{Z}$, such that $\phi_2(C) = 1$. Its kernel is $\bar{\Gamma}(2)_3$. We can now describe $\phi_3 : \bar{\Gamma}(2)_3 \rightarrow \mathbb{Z}^2$ such that $\phi_3([C, A]) = (1, 0)$ and $\phi_3([C, B]) = (0, 1)$. Something interesting happens at that stage.

For k integer ≥ 2 , the extension $1 \rightarrow G_k/G_{k+1} \rightarrow G_{k-1}/G_{k+1} \rightarrow G_{k-1}/G_k \rightarrow 1$ is central. Consequently, since $r_2(\bar{\Gamma}(2)) = 1$, the group $\bar{\Gamma}(2)_2/\bar{\Gamma}(2)_4$ is abelian, and free of rank 3. Of course, the extension $1 \rightarrow \bar{\Gamma}(2)_2/\bar{\Gamma}(2)_4 \rightarrow \bar{\Gamma}(2)_1/\bar{\Gamma}(2)_4 \rightarrow \bar{\Gamma}(2)_1/\bar{\Gamma}(2)_2 \rightarrow 1$ is not central.

Proposition 5. *There exists a group isomorphism $\psi : \bar{\Gamma}(2)_2/\bar{\Gamma}(2)_4 \simeq \mathbb{Z}^3$ given by $C \mapsto (0, 0, 1)$, $[C, A] \mapsto (1, 0, 0)$, and $[C, B] \mapsto (0, 1, 0)$. One has, for $\gamma \in \bar{\Gamma}(2)$ and $\delta \in \bar{\Gamma}(2)_2$, the formula*

$$\psi(\gamma\delta\gamma^{-1}) = (-\phi_1(\gamma)\phi_2(\delta), 0) + \psi(\delta).$$

or equivalently

$$\psi([\delta, \gamma]) = (\phi_1(\gamma)\phi_2(\delta), 0).$$

In particular, one has, for $i, j \in \mathbb{Z}$, the formula $\psi(A^i B^j C^k B^{-j} A^{-i}) = (-ki, -kj, k)$.

Proof. Given that $\{[C, A], [C, B]\}$ is basis of the \mathbb{Z} -module $\bar{\Gamma}(2)_3/\bar{\Gamma}(2)_4$, and C is a basis of the \mathbb{Z} module $\bar{\Gamma}(2)_2/\bar{\Gamma}(2)_3$, any lifting of C modulo $\bar{\Gamma}(2)_3$, to a class C' modulo $\bar{\Gamma}(2)_4$ gives a basis

$\{[C, A], [C, B], C'\}$ of $\bar{\Gamma}(2)_2/\bar{\Gamma}(2)_4$. The choice $C = C'$ is evidently suitable, but is somewhat arbitrary.

One has

$$\psi(\gamma\delta\gamma^{-1}) = \psi(\gamma\delta C^{-\phi_2(\delta)}\gamma^{-1}C^{\phi_2(\delta)}\delta^{-1}\delta C^{-\phi_2(\delta)}\gamma C^{\phi_2(\delta)}\gamma^{-1}).$$

Since $\delta C^{-\phi_2(\delta)} \in \bar{\Gamma}(2)_3$, the factor $\gamma\delta C^{-\phi_2(\delta)}\gamma^{-1}C^{\phi_2(\delta)}\delta^{-1}$ belongs to $\bar{\Gamma}(2)_4$; hence its image by ψ vanishes. So we get

$$(2.1) \quad \psi(\gamma\delta\gamma^{-1}) = \psi(\delta) - \phi_2(\delta)\psi(C) + \phi_2(\delta)\psi(\gamma C\gamma^{-1}),$$

which translates into

$$\psi([\delta, \gamma]) = \phi_2(\delta)\psi([C, \gamma]).$$

It remains to determine $\psi([C, \gamma])$. Let $\gamma_1, \gamma_2 \in \bar{\Gamma}(2)$. One has

$$(2.2) \quad (\gamma_1\gamma_2)\delta(\gamma_1\gamma_2)^{-1} = [\gamma_1, \gamma_2][\gamma_2, [\gamma_1, \delta]][\gamma_1, \delta][\gamma_2, \delta]\delta[\gamma_2, \gamma_1].$$

Since $[\gamma_2, [\gamma_1, \delta]]$ is a commutator of degree 4, it is in the kernel of ψ . It follows that the map $\gamma \mapsto \psi(\gamma\delta\gamma^{-1})$ is a group homomorphism from $\bar{\Gamma}(2)$ to \mathbb{Z}^2 . For $\delta = C, \gamma = A$ (resp. $\gamma = B$), one has $\psi(\gamma\delta\gamma^{-1}) = -(\psi_1(\gamma), 0)$, hence the latter equality is true for all $\gamma \in \bar{\Gamma}(2)$. Thus one gets

$$\psi([C, \gamma]) = (\phi_1(\gamma), 0),$$

which gives the main formula. It remains to apply this to $\gamma = A^i B^j$ and $\delta = C^k$ to obtain the final formula. □

The exact sequence $1 \rightarrow \bar{\Gamma}(2)_3/\bar{\Gamma}(2)_4 \rightarrow \bar{\Gamma}(2)_1/\bar{\Gamma}(2)_4 \rightarrow \bar{\Gamma}(2)_1/\bar{\Gamma}(2)_3 \rightarrow 1$ identifies to a central group extension

$$0 \rightarrow \mathbb{Z}^2 \rightarrow H'_\mathbb{Z} \rightarrow H_\mathbb{Z} \rightarrow 1.$$

2.3. The groups Φ_N, Φ'_N and Φ''_N . We denote the group $\Gamma_{N,N,1}$ by Φ_N . It is the kernel of the group homomorphism $\bar{\phi}_1 : \bar{\Gamma}(2) \rightarrow (\mathbb{Z}/N\mathbb{Z})^2$, which maps A to $(1, 0)$ and B to $(0, 1)$ (and thus C to $(0, 0)$). A system of representatives for the cosets $\Phi_N \backslash \bar{\Gamma}(2)$ is given by $A^i B^j$ with $i, j \in \{0, 1, \dots, (N-1)\}$. The structure of Φ_N is probably well known, but we could not find a complete reference for a presentation Φ_N .

Proposition 6. *The group Φ_N is generated by $U = \{A^N, B^N, A^i B^j C B^{-j} A^{-i} / 0 \leq i, j \leq N-1\}$. Moreover Φ_N has presentation*

$$\langle A^N, B^N, T_{i,j}, 0 \leq i, j \leq N-1 \mid [A^N, B^N] = \prod_{i=0}^{N-1} \prod_{j=0}^{N-1} T_{N-1-i,j} \rangle.$$

Proof. The group Φ_N is generated by $U = \{A^N, B^N, A^i B^j C B^{-j} A^{-i} / 0 \leq i, j \leq N - 1\}$ [7], [17]. By the Nielsen-Schreier theorem, Φ_N , being a free subgroup of index N^2 of a free group on two generators, is free on $N^2 + 1$ generators. A relation between the $N^2 + 2$ exhibited generators in U presents itself :

$$(2.3) \quad A^N B^N A^{-N} B^{-N} = \prod_{i=0}^{N-1} \prod_{j=0}^{N-1} A^{N-1-i} B^j C B^{-j} A^{i+1-N}.$$

One of the exhibited generators in U can be expressed in terms of the $N^2 + 1$ remaining elements of U . Thus we get a presentation by generators and relations of Φ_N . \square

Set $N' = N$ if N is odd, and $N' = N/2$ if N is even.

We set $\Phi'_N = \Gamma_{N,N,N'}$. It is the subgroup of Φ_N obtained as the kernel of the morphism $\bar{\phi}_2 : \Phi_N \rightarrow \mathbb{Z}/N'\mathbb{Z}$ which vanishes on A^N and B^N and takes the value 1 on $A^i B^j C B^{-j} A^{-i}$ for i, j integers.

Alternately, Φ'_N is the kernel of the composed map $\bar{\Gamma}(2) \rightarrow H_{\mathbf{Z}} \rightarrow H_{N,N,N'}$. Thus the composed map $[\bar{\Gamma}(2), \bar{\Gamma}(2)] \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}/N'\mathbb{Z}$ extends to a map $\bar{\phi}_2 : \Phi_N \rightarrow \mathbb{Z}/N'\mathbb{Z}$, with kernel Φ'_N . It vanishes on A^N and B^N .

Proposition 7. *The composed map $[\bar{\Gamma}(2), \bar{\Gamma}(2)] \rightarrow \mathbb{Z}^3 \rightarrow (\mathbb{Z}/N'\mathbb{Z})^3$ extends to a group homomorphism*

$$\bar{\psi} : \Phi_N \rightarrow (\mathbb{Z}/N'\mathbb{Z})^3$$

which vanishes on A^N and B^N and, for $\gamma \in \bar{\Gamma}(2)$ and $\delta \in \Phi_N$, satisfies

$$(2.4) \quad \bar{\psi}(\gamma \delta \gamma^{-1}) = (-\bar{\phi}_1(\gamma) \bar{\phi}_2(\delta), 0) + \bar{\psi}(\delta).$$

In particular, for $i, j, k \in \mathbb{Z}$, one has

$$(2.5) \quad \bar{\psi}(A^i B^j C^k B^{-j} A^{-i}) = (-ik, -jk, k).$$

Proof. It follows from the presentation of Φ_N that formula 2.5 defines a morphism $\Phi_N \rightarrow (\mathbb{Z}/N'\mathbb{Z})^3$ (it vanishes on the exhibited relation 2.3 between the generators). Such a morphism coincides with the composed map $[\bar{\Gamma}(2), \bar{\Gamma}(2)] \rightarrow \mathbb{Z}^3 \rightarrow (\mathbb{Z}/N'\mathbb{Z})^3$, by the formula we established on ψ .

The formula 2.4 is valid whenever $\delta \in \bar{\Gamma}(2)_2$, by 2.1. Since Φ_N is generated by $\bar{\Gamma}(2)_2$ together with A^N and B^N , it remains to prove 2.4 for $\delta = A^N$ and $\delta = B^N$. Consider the case $\delta = B^N$ for instance (the other case is similar). Let us use the formula 2.2 again. We get, for $\gamma_1, \gamma_2 \in \bar{\Gamma}(2)$, (leaving out opposite terms)

$$\bar{\psi}(\gamma_1 \gamma_2 B^N \gamma_2^{-1} \gamma_1^{-1}) = \bar{\psi}([\gamma_2, [\gamma_1, B^N]]) + \bar{\psi}([\gamma_1, B^N]) + \bar{\psi}([\gamma_2, B^N]) + \bar{\psi}(B^N).$$

We have $\bar{\psi}(B^N) = 0$, and $\bar{\psi}([\gamma_2, [\gamma_1, B^N]])$ is the reduction modulo N of $\psi([\gamma_2, [\gamma_1, B^N]])$. One has $\psi([\gamma_2, [\gamma_1, B^N]]) = -(\phi_1(\gamma_2) \phi_2([\gamma_1, B^N]), 0)$. But $\phi_2([\gamma_1, B^N]) \in N\mathbb{Z}$. So we have proved

that the map $\gamma \mapsto \bar{\psi}(\gamma B^N \gamma^{-1})$ is a group homomorphism. It remains to prove that the formula 2.4 holds for $\gamma = A$ and $\gamma = B$ (still in the configuration where $\delta = B^N$). Only the case $\gamma = A$ is of interest. We have

$$\bar{\psi}(AB^N A^{-1}) = \bar{\psi}(AB^N A^{-1} B^{-N}).$$

As $AB^N A^{-1} B^{-N} \in \bar{\Gamma}(2)_2$, $\bar{\psi}(AB^N A^{-1} B^{-N})$ is the reduction modulo N of $\psi(AB^N A^{-1} B^{-N})$. We use the identity

$$AB^N A^{-1} B^{-N} = (ABA^{-1})^N B^{-N} = (ABA^{-1} B^{-1} B)^N B^{-N} = C B C B^{-1} B^2 C B^{-2} \dots B^{N-1} C B^{1-N}.$$

The right-hand side is a product of generators of Φ_N . We can apply 2.5

$$\psi(AB^N A^{-1} B^{-N}) = \sum_{i=0}^{N-1} \psi(B^i C B^{-i}) = \sum_{i=0}^{N-1} (0, -i, 0) = (0, N(N-1)/2, 0).$$

Since $N' = \gcd(N, N(N-1)/2)$, we have indeed that $\bar{\psi}(AB^N A^{-1} B^{-N}) = 0$. \square

Remark 8. Let $N'' = N'$ if N is prime to 3, and $N'' = N'/3$ otherwise. The appearance of the denominator 2 (for N') and now 3 (for N'') is related to Bernoulli numbers. We suspect that ultimately it is related to the mixed Tate motives that have been discovered by Deligne in his study of the nilpotent completion of the fundamental group of the projective line deprived of three points [4].

We define Φ''_N as the kernel of the composed map $\Phi_N \rightarrow (\mathbb{Z}/N'\mathbb{Z})^2 \times (\mathbb{Z}/N'\mathbb{Z}) \rightarrow (\mathbb{Z}/N''\mathbb{Z})^2 \times (\mathbb{Z}/N'\mathbb{Z})$.

Corollary 9. *The exact sequence*

$$0 \rightarrow \Phi'_N / \Phi''_N \rightarrow \bar{\Gamma}(2) / \Phi''_N \rightarrow \bar{\Gamma}(2) / \Phi'_N \rightarrow 0$$

makes of the group $\bar{\Gamma}(2) / \Phi''_N$ a central extension of the Heisenberg group $H_{N,N,N'}$ by $(\mathbb{Z}/N''\mathbb{Z})^2$.

Proof. It follows from formula 2.4, as $\bar{\phi}_2$ vanishes on Φ'_N . \square

We denote by $H'_{\mathbb{Z}/N\mathbb{Z}}$ the group $\bar{\Gamma}(2) / \Phi''_N$.

Proposition 10. *The group $H'_{\mathbb{Z}/N\mathbb{Z}}$ is of exponent N . In other words, for every $\gamma \in \bar{\Gamma}(2)$, one has $\gamma^N \in \Phi''_N$.*

Proof. It relies on relations for commutators, that, we presume, are well known. Let G be a group. Suppose G_4 is trivial. Then G_3 is contained in the center of G . Let $\alpha, \beta \in G$. Set $\gamma = [\alpha, \beta]$, $\alpha' = [\gamma^{-1}, \alpha]$ and $\beta' = [\gamma^{-1}, \beta]$. Let $n \in \mathbb{N} \cup \{0\}$ be an integer. One has the relation

$$(2.6) \quad \beta^n \alpha = \alpha \gamma^{-n} \beta^n \alpha'^n \beta'^{-\frac{n(n-1)}{2}}.$$

We prove it by induction on n . Indeed, it holds for $n = 0$. Suppose it holds for some value of n . We have

$$\beta^{n+1}\alpha = \beta\alpha\gamma^{-n}\beta^n\alpha'^n\beta'^{-n(n-1)/2} = \gamma^{-1}\alpha\beta\gamma^{-n}\beta^n\alpha'^n\beta'^{-\frac{n(n-1)}{2}}.$$

We use the relations $\gamma^{-1}\beta = [\gamma^{-1}, \beta]\beta\gamma^{-1} = \beta'\beta\gamma^{-1}$, $\gamma^{-1}\alpha = [\gamma^{-1}, \alpha]\alpha\gamma^{-1} = \alpha'\alpha\gamma^{-1}$ and $\beta\gamma^{-n} = \beta'^{-n}\gamma^{-n}\beta$. Using the fact that $\alpha', \beta' \in Z(G)$, we get

$$\begin{aligned} \beta^{n+1}\alpha &= \gamma^{-1}\alpha\beta\gamma^{-n}\beta^n\alpha'^n\beta'^{-\frac{n(n-1)}{2}} \\ &= \alpha'\alpha\gamma^{-1}\beta\gamma^{-n}\beta^n\alpha'^n\beta'^{-\frac{n(n-1)}{2}} \\ &= \alpha\gamma^{-n-1}\beta^{n+1}\alpha'^{n+1}\beta'^{-n-n(n-1)/2} \end{aligned}$$

which is the desired formula. We pass to the next step. We now claim that

$$(2.7) \quad (\alpha\beta)^n = \alpha^n\gamma^{-\binom{n}{2}}\beta^n\alpha'^{\binom{n+1}{3}}\beta'^{-\binom{n}{3}}.$$

We proceed again by induction on n . This is true for $n = 1$. We suppose the formula holds for a certain value of n . We get

$$(\alpha\beta)^{n+1} = (\alpha\beta)^n \cdot (\alpha\beta) = \alpha^n\gamma^{-\binom{n}{2}}\beta^n \cdot (\alpha\beta)\alpha'^{\binom{n+1}{3}}\beta'^{-\binom{n}{3}}.$$

Using the formula 2.6, we get

$$(\alpha\beta)^{n+1} = \alpha^n\gamma^{-\binom{n}{2}}\alpha\gamma^{-n}\beta^n\alpha'^n\beta'^{-\binom{n}{2}}\beta\alpha'^{\binom{n+1}{3}}\beta'^{-\binom{n}{3}}.$$

We now use the formula $\gamma^{-\binom{n}{2}}\alpha = \alpha'^{\binom{n}{2}}\alpha\gamma^{-\binom{n}{2}}$ and the centrality of α' and β' to get

$$(\alpha\beta)^{n+1} = \alpha^n\gamma^{-\binom{n}{2}-n}\beta^n\alpha'^{\binom{n+1}{3}+\binom{n}{2}+n}\beta'^{-\binom{n}{3}-\binom{n}{2}} = \alpha^n\gamma^{-\binom{n+1}{2}}\beta^n\alpha'^{\binom{n+2}{3}}\beta'^{-\binom{n+1}{3}}$$

which establishes 2.7.

The N -th powers of both A and B belong to Φ''_N (Proposition 7). The N' -th, and therefore the $\binom{N}{2}$, power of any commutator belongs to Φ''_N , since Φ'_N contains $\bar{\Gamma}(2)_2$. Similarly the N'' -th power, and therefore the $\binom{N}{3}$ and $\binom{N+1}{3}$ powers, of an element of $\bar{\Gamma}(2)_3$ belongs to Φ''_N . We can combine these remarks with the formula 2.7 for $n = N$, to establish that, if the N -th powers of α and β both belong to Φ''_N , one has $(\alpha\beta)^N \in \Phi''_N$. The proposition follows, since $\{A, B\}$ generates $\bar{\Gamma}(2)$. □

Remark 11. Let p be prime number. Stallings introduced the lower p -central series $(S_k)_{k \geq 1}$ as a particular case for $N = p$ of the following construction. One has $S_1 = G$, and, for $k \geq 2$, $S_{k+1} = [G, S_k](S_k)^N$, where the latter expression is the subgroup of G generated by $[G, S_k]$ and $(S_k)^N$. Note that, when $G = \bar{\Gamma}(2)$, one has $S_2 = [\bar{\Gamma}(2), \bar{\Gamma}(2)]\bar{\Gamma}(2)^N = \Phi_N$ and $S_3 = [\bar{\Gamma}(2), \Phi_N]\Phi_N^N$. Note that $S_3 \subset \Phi'_N \subset S_2$. Since A^N and B^N do not belong to S_3 , the groups S_3 and Φ'_N do not coincide.

2.4. Odd adelic completions. Recall that, for $k \geq 1$, $\bar{\Gamma}(2)_k$ is the k -th term in the lower central series of $\bar{\Gamma}(2)$. Let $D_3 = \{\pm \text{Id}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\}$ in $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ be the index 3, 2-Sylow subgroup of $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$. It is isomorphic to the Klein group.

Recall that the derived subgroup of $\text{PSL}_2(\mathbb{Z})$ is the projective congruence subgroup of level 6 whose image in $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ is D_3 , and whose image in $\text{PSL}_2(\mathbb{Z}/2\mathbb{Z})$ is cyclic of order 3.

Let

$$\hat{\mathbb{Z}}_{\text{odd}} = \varprojlim_{n \text{ odd}} \mathbb{Z}/n\mathbb{Z} \simeq \prod_{p \neq 2} \mathbb{Z}_p$$

be the profinite completion of \mathbb{Z} away from the prime 2. Let \hat{D}_{odd} be the inverse image of D_3 in $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$.

Proposition 12. *The image of $\bar{\Gamma}(2)_2$ in $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ is equal to D_3 . For p prime, $p > 3$, its image modulo p is $\text{PSL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Proof. Indeed, the images of $\bar{\Gamma}(2)$ and $\text{PSL}_2(\mathbb{Z})$ in $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ coincide by weak approximation. Thus $\bar{\Gamma}(2)_2$ modulo 3 coincides with the derived subgroup of $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$, which in turn is the reduction modulo 3 of the derived subgroup of $\text{PSL}_2(\mathbb{Z})$. The second assertion is proved similarly. □

Proposition 13. *Let k be an integer ≥ 2 . The closure of $\bar{\Gamma}(2)_k$ in $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$ is equal to \hat{D}_{odd} .*

Proof. We prove this first for $k = 2$. Let n be an odd integer divisible by 3. Let D_n be the inverse image of D_3 in $\text{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. The image of $\bar{\Gamma}(2)_2$ modulo n coincide with the image of the derived subgroup of $\text{PSL}_2(\mathbb{Z})$ modulo n , which is a subgroup of index 3 of $\text{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. Such a subgroup can only be D_n . Thus we obtain the proposition for $k = 2$.

We prove the proposition for $k = 3$. Let I_n be the image of $\bar{\Gamma}(2)_3$ in $\text{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. Note that we have an exact sequence

$$1 \rightarrow K_n \rightarrow I_n \rightarrow D_3 \rightarrow 1.$$

Since we have an exact sequence

$$1 \rightarrow \pm 1 + 3M_2(\mathbb{Z}/\frac{n}{3}\mathbb{Z})_0 \rightarrow \text{PSL}_2(\mathbb{Z}/n\mathbb{Z}) \rightarrow \text{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \rightarrow 1$$

where $M_2(\mathbb{Z}/\frac{n}{3}\mathbb{Z})_0$ is the subgroup of $M_2(\mathbb{Z}/\frac{n}{3}\mathbb{Z})$ made of matrices of trace 0, the equality $I_n = D_n$ would follow from the inclusion $1 + 3M_2(\mathbb{Z}/\frac{n}{3}\mathbb{Z})_0 \subset K_n$. It remains to establish the latter inclusion. Since $\text{PSL}_2(\mathbb{Z}/n\mathbb{Z})$ is equal to its derived subgroup when n is prime to 6, by the Chinese remainder theorem, it is enough to prove it when n is a power of 3.

It follows from the equality $[(1 + pM_2(\mathbb{Z}_p))_0, \text{SL}_2(\mathbb{Z}_p)] = (1 + pM_2(\mathbb{Z}_p))_0$, valid for any prime p , and the fact that the closure of $\bar{\Gamma}(2)_2$ in $\text{PSL}_2(\mathbb{Z}_3)$ contains $[(1 + 3M_2(\mathbb{Z}_3))_0$.

The general case $k \geq 3$ of the proposition is now immediate. Indeed, since $\bar{\Gamma}(2)_3$ and $\bar{\Gamma}(2)_2$ have the same image modulo n , those images are the second and third respectively derived subgroups of $\text{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. Thus the lower central series of $\text{PSL}_2(\mathbb{Z}/n\mathbb{Z})$ stabilizes to the image modulo n of $\bar{\Gamma}(2)_k$ for any $k \geq 3$. \square

Proposition 14. *The closure of Φ_N in $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$ is $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$ if 3 does not divide N . It is \hat{D}_{odd} if 3 divides N .*

Proof. If 3 does not divide N , Φ_N contains a non-zero upper triangular matrix (for instance A'^N) which is not the identity modulo 3. Its closure in $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$ contains a maximal proper subgroup of index 3, namely \hat{D}_{odd} , and an element which is not in that subgroup. Therefore the closure is $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$. If 3 divides N , since both A^{3N} and B^{3N} vanish modulo 3, the images of Φ_N and $\bar{\Gamma}(2)_2$ coincide in $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$. Hence the result. \square

Proposition 15. *The closure of Φ'_N in $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$ is $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$ if 3 does not divide N . It is \hat{D}_{odd} if 3 divides N .*

Proof. The closure of $\bar{\Gamma}(2)_2$ and $\bar{\Gamma}(2)_3$ coincide modulo n for every n divisible by 3, as we have just established. Thus the closure of Φ'_N in $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$ contains $\bar{\Gamma}(2)_2$. Since the group Φ'_N contains the matrices A^N and B^N , its closure contains Φ_N . Thus the closure of Φ'_N in $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$ is equal to the closure of Φ_N in $\text{PSL}_2(\hat{\mathbb{Z}}_{\text{odd}})$. \square

Let $\bar{\Gamma}'(2) = \bar{\Gamma}(2) \cap \hat{D}_{\text{odd}}$. It is a subgroup of index 3 of $\bar{\Gamma}(2)$.

Corollary 16. *Let Γ be a congruence subgroup of $\bar{\Gamma}(2)$. One has $\Gamma\Phi'_N = \bar{\Gamma}'(2)$ if $\Gamma \subset \bar{\Gamma}'(2)$ and 3 divides N . One has $\Gamma\Phi'_N = \bar{\Gamma}(2)$ otherwise.*

Let n be an even integer. In particular, one has $\Gamma(n)\Phi'_N = \bar{\Gamma}(2)$ if 3 does not divide either n or N . One has $\Gamma(n)\Phi'_N = \bar{\Gamma}'(2)$ if 3 divides both n and N .

3. THE ASSOCIATED RIEMANN SURFACES

3.1. The Riemann surface $X_{M,N,L}$. Denote by $X_{M,N,L}$ the compactified modular curve defined by $\Gamma_{M,N,L}$.

Proposition 17. *The genus $g_{M,N,L}$ of the curve $X_{M,N,L}$ is given by the following formulas. Denote by T the lowest common multiple of M and N . Suppose T is even and T/L is odd, then one has*

$$g_{M,N,L} := g(X_{M,N,L}) = (NML - NL - ML - NML/2T)/2 + 1.$$

Suppose T is odd or T/L is even, then one has

$$g_{M,N,L} := g(X_{M,N,L}) = (NML - NL - ML - NML/T)/2 + 1.$$

Proof. We use Riemann-Hurwitz formula for the morphism $X_{N,M,L} \rightarrow X(2)$. Since $\Gamma(2)$ has no elliptic elements, the ramification points of this morphism reside entirely among the cusps.

Concerning the cusps above 0 (resp. ∞), note that the stabilizer of the rational number 0 (resp. ∞) in $P\Gamma(2)$ is generated by B (resp. A). As the morphism $X_{N,M,L} \rightarrow X(2)$ is Galois, the ramification index is independent of the chosen cusp, and is the order of the orbit of B (resp. of A) acting on $\Gamma_{M,N,L} \backslash \Gamma(2)$. This is N (resp. M) by definition of $\Gamma_{M,N,L}$. Concerning the cusps above 1, the stabilizer in $P\Gamma(2)$ of the rational number -1 is generated by $A^{-1}B$. It remains to determine the order of $A^{-1}B$ in $\Gamma_{M,N,L} \backslash \Gamma(2) = H_{M,N,L}$.

The abelianization provides a map $: H_{M,N,L} \rightarrow \mathbf{Z}/M\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ which sends $A^{-1}B$ to $(1, -1)$. The latter element is of order T , which leads us to examine the order of $(A^{-1}B)^T$ in $H_{M,N,L}$. Denote by $D = [A^{-1}, B]$. It belongs to and generates the center of $H_{M,N,L}$. It is of order L . Note the formula $A^{-1}B = DBA^{-1}$. Thus one has $(A^{-1}B)^T = D^k A^{-T} B^T$ in $H_{M,N,L}$, where k is the number of factors A^{-1} to the right of a factor B in the $(A^{-1}B)^T$ written as a product of $2T$ factors. One has $k = 1 + 2 + \dots + (T - 1) = T(T - 1)/2$. This is why the order of $(A^{-1}B)^T$ is 1 if L is odd or if T/L is even. This order is 2 otherwise.

Thus the ramification index e of any cusp above 1 is equal to T if L is odd or if T/L is even. It is $2T$ otherwise. We can now apply the Riemann-Hurwitz formula for the dominant morphism $X_{M,N,L} \rightarrow X(2)$:

$$2g_{M,N,L} - 2 = -2d + \sum_{x \in X_{M,N,L}} (e_x - 1).$$

We have $d = |H_{M,N,L}| = MNL$. One gets

$$2g_{M,N,L} - 2 = -2MNL + NL(M - 1) + ML(N - 1) + NML(1 - 1/e)$$

and

$$g_{M,N,L} = NML - NL - ML - NML/e + 1$$

The lemma follows from the calculation of e . □

3.2. The Riemann surfaces X_N, X'_N and X''_N . All three groups Φ_N, Φ'_N and Φ''_N act on the upper half-plane \mathbb{H} . We denote respectively by X_N, X'_N and X''_N the corresponding completed modular curves.

Proposition 18. *Both morphisms $X'_N \rightarrow X_N$ and $X''_N \rightarrow X'_N$ (and therefore $X''_N \rightarrow X_N$ as well) are unramified. The covering $X'_N \rightarrow X_N$ is cyclic of degree N' . The covering $X''_N \rightarrow X'_N$ is Galois with group $(\mathbb{Z}/N''\mathbb{Z})^2$. The covering $X''_N \rightarrow X_N$ is abelian with Galois group $(\mathbb{Z}/N''\mathbb{Z})^2 \times (\mathbb{Z}/N'\mathbb{Z})$.*

Proof. The first statement needs only to be established for the morphism $X''_N \rightarrow X_N$. The ramification points can only reside at the cusps. To show that those cusps are unramified, we

need only to show that their width in X''_N is equal to their width, equal to N , in X_N . Since the covering $X''_N \rightarrow X_1$ is Galois, the width of a cusp of X''_N depends only on its image in the set of cusps $\{0, 1, \infty\}$ of X_1 . We just need to look at the order of A, B and $A^{-1}B$ in $\bar{\Gamma}(2)/\Phi''_N$. All three are of order N in the latter quotient.

The other assertions follow immediately from the properties of the groups Φ_N, Φ'_N and Φ''_N . □

The Riemann surface X_N is isomorphic to the Riemann surface obtained from the complex points of the Fermat curve. The covering $X'_N \rightarrow X_N$ is obtained from what we call *Heisenberg covering of the Fermat curve* by passing to the complex numbers.

We obtain the genus g_N and g'_N of the curves X_N and X'_N by our formulas for the genus of $X_{N,M,L}$. One has $g_N = g_{N,N,1} = (N - 1)(N - 2)/2$. Furthermore, if N is odd, one has $g'_N = g_{N,N,N} = (N^3 - 3N^2 + 2)/2 = (N - 1)(N^2 - 2N - 2)/2$. If N is even, one gets $g'_N = g_{N,N,N'} = (2N^3 - 5N^2 + 4)/4 = (N - 2)(2N^2 - N - 2)/4$.

The genus of g''_N of the curve X''_N can be deduced from the Riemann-Hurwitz formula. Since we have a covering $X''_N \rightarrow X'_N$ of degree N''^2 , one has

$$g''_N = N''^2 g'_N - N^2 + 1.$$

The curve X'_N possesses NN' cusps above each of the cusps $0, 1$ and ∞ of $X(2)$.

3.3. Some cases of small genus.

Proposition 19. *The genus g of the curve $X_{M,N,L}$ is equal to 0 for the following values of (N, M, L) , and only for those values : $(N, 1, 1), (1, M, 1), (2, 2, 1), (2, 2, 2)$.*

Proof. The formula just established gives : $2 - 2g = -L(MN - N - M - MN/e)$. Thus $g = 0$ implies that $L = 1$ or 2 .

If $g = 0$ and $L = 1$, then one has $MN - N - M - MN/e = -2$ and $e = \text{lcm}(M, N)$. Thus $\text{gcd}(M, N)$ divides 2. If $\text{gcd}(M, N) = 1$, then one has $MN - N - M - 1 = -2$, and thus $(M - 1)(N - 1) = 0$ that is $M = 1$ or $N = 1$. If $\text{gcd}(M, N) = 2$, one has $MN - N - M - 2 = -2$ and thus $(M - 1)(N - 1) = 1$; therefore one has $(M, N) = (2, 2)$.

If $g = 0$ and $L = 2$, then one has $MN - N - M - MN/e = -1$. If 4 divides neither M nor N , one has $e = 2\text{lcm}(M, N)$. Then $\text{gcd}(M, N)$ divides 2, and is equal to 2. Then one has $MN - N - M - 1 = -2$, as above. As $L = 2$, the cases $M = 1$ and $N = 1$ are excluded; thus one has $(M, N) = (2, 2)$. □

Proposition 20. *The genus g of the curve $X_{M,N,L}$ is equal to 1 for the following values of (N, M, L) , and only for those values (up to permutation of N and M) : $(3, 2, 1), (4, 2, 1), (4, 2, 2), (3, 3, 1), (3, 3, 3)$.*

The Jacobian varieties of those curves are elliptic curves endowed with automorphisms of order 3, 4, 4, 3 and 3 respectively. Consequently the j -invariants of those curves are 0, 1728, 1728, 0 and 0 respectively.

Proof. Consider again the formula : $2 - 2g = -L(MN - N - M - MN/e)$. Thus $g = 1$ amounts to $MN - N - M - MN/e = 0$. One has $MN - N - M - MN/e = (N - 2)(M - 1) - 2 + M(1 - N/e)$. We can suppose that $N > 1$ and $M > 1$ (otherwise $g = 0$).

If $N = 2$, one gets $M(1 - 2/e) = 2$. If $L = 1$, then $e = \text{lcm}(M, 2)$. Thus $M - 1 = 2$ or $M - 2 = 2$. One has $(N, M, L) = (2, 3, 1)$ or $(N, M, L) = (2, 4, 1)$.

If $N = 2$ and $L = 2$, then $e = 2M$ or $e = M$. If $e = M$, then $M - 2 = 2$. If $e = 2M$, then $M - 1 = 2$ (absurd since $L|M$). One has $(N, M, L) = (2, 4, 2)$ or $(N, M, L) = (2, 4, 1)$.

If $N = 3$, then one has $M - 3 + M(1 - 3/e) = 0$ and $e = \text{lcm}(M, 3)$. One can suppose that $M > 2$. Thus one has $M = 3$ and $L = 1$ or $L = 3$. One has $(N, M, L) = (3, 3, 1)$ or $(N, M, L) = (3, 3, 3)$.

The case where $M = 2$ or $M = 3$ are treated similarly. If $N > 3$ and $M > 3$, one has $(N - 2)(M - 1) - 2 + M(1 - N/e) > 0$, which precludes $g = 1$.

The automorphisms come from the action of the image of A in $H_{N,M,L}$ which stabilizes a cusp and therefore is an automorphism of an elliptic curve. □

We can derive some information on the Manin-Drinfeld principle in the genus 1 cases.

Proposition 21. Divisors of the form $(CP) - (P)$, where P is any point (in particular a cusp) of $X_{3,3,3}$ (resp. $X_{4,2,2}$) and C acts via the map $\bar{\Gamma}(2) \rightarrow H_{N,M,L}$, are of order dividing 3 (resp. 2).

Proof. The canonical morphism $X_{3,3,3} \rightarrow X_{3,3,1}$ is of degree 3. It gives rise to an isogeny of degree 3 on the Jacobians by Albanese functoriality. Thus the kernel of this isogeny is of order 3. Moreover any divisor of the form $(CP) - (P)$ is in the kernel of the isogeny. □

3.4. The curve $X'(2)$. Recall that the group $\bar{\Gamma}'(2)$ is the subgroup of index 3 of $\bar{\Gamma}(2)$ that is the inverse image of the 2-Sylow subgroup of $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$. Denote by $X'(2) = X_{\bar{\Gamma}'(2)}$ the corresponding modular curve.

Proposition 22. The curve $X'(2)$ is of genus 1 and its j -invariant is 0.

Proof. Consider the morphism of degree $d = 3 : X'(2) \rightarrow X(2)$. Since none of the matrices A (generator of the stabilizer of the cusp ∞), B (generator of the stabilizer of the cusp 0), and AB^{-1} (generator of the stabilizer of the cusp 1) are not in $\bar{\Gamma}'(2)$, the morphism is totally ramified at each of the three cusps of $X(2)$, and ramified only over those points. The Riemann-Hurwitz formula expresses the genus g of $X'(2)$ as $(2g - 2) = -2d + \sum_P (e_P - 1) = 6 - 6 = 0$ (where

P runs through points of ramification and e_P designates the ramification index at that point), hence $g = 1$.

The curve $X'(2)$ has an automorphism (the class of A in $\bar{\Gamma}(2)/\bar{\Gamma}'(2)$) of order 3 which leaves fixed the cusp ∞ . Since it is of genus 1, it is an elliptic curve of with an automorphism of order 3. It has necessarily j -invariant 0. □

Remark 23. Since $\Gamma_{3,3,3} = \Phi'_3$ is a subgroup of index 3 of $\Gamma'(2)$. One has a morphism $X_{3,3,3} \rightarrow X'(2)$ of degree 3. Both curves involved are of genus 1, so we have an isogeny of degree 3. Note that $\bar{\Gamma}'(2)$ is a congruence subgroup of level 12 and a subgroup of index 3 of the derived subgroup $\tilde{\Gamma}$ of $\text{PSL}_2(\mathbb{Z})$. The latter subgroup defined a modular curve $X_{\tilde{\Gamma}}$ of genus 1, which happens to have j -invariant 0. Thus we get an isogeny $X'(2) \rightarrow X_{\tilde{\Gamma}}$ of degree 3.

We now prove theorem 3.

Proof. The correspondence is obtained by composing pushing to X_{Γ, Φ'_d} and pulling back to X_Γ . By Proposition 15, one has $\Gamma \cdot \Phi'_d = \bar{\Gamma}(2)$ except if 3 divides N and Γ is contained in $\bar{\Gamma}'(2)$. In the latter case, $\theta_{N,\Gamma}$ factorizes through the jacobian of $X(2)$, which is 0. Otherwise, namely if 3 divides N and Γ is contained in $\bar{\Gamma}'(2)$, $\theta_{N,\Gamma}$ factorizes through the surjective map $J'_N \rightarrow J'(2)$. Since $J'(2)$ is the jacobian of a curve of genus 1, and j -invariant 0, it is an elliptic curve of j -invariant 0. Moreover the map $J'(2) \rightarrow J_\Gamma$ has finite kernel. The result follows. □

It is well known that the modular curve $X_0(27)$ has j -invariant 0, and that the Fermat curve is a model for $X_0(27)$. We might expect a connection between $X_0(27)$ and X'_3 . Let $\Gamma = \bar{\Gamma}(2) \cap \Gamma_0(27)$. It is a congruence subgroup. But it is not contained in $\Gamma'(2)$. Thus, if we apply theorem 3 to the group Γ , we obtain, counterintuitively, the 0-morphism $J'_3 \rightarrow J_\Gamma$. *A fortiori*, if we push forward $J_\Gamma \rightarrow J_0(27)$ we obtain 0.

3.5. Mixed homology groups. In [5], the homology group of X_N relative to the whole set of cusps is thoroughly studied, by the method of Manin [9]. We found fruitful in [2] to consider the following slightly different point of view: for Γ a subgroup of finite index of $\bar{\Gamma}(2)$, the corresponding modular curve X_Γ covers $X(2)$, which admits three cusps: $\Gamma(2)0$, $\Gamma(2)1$ and $\Gamma(2)\infty$. Let ∂_Γ^+ (resp. ∂_Γ^-) be the set of cusps above $\Gamma(2)0 \cup \Gamma(2)\infty$ (resp. $\Gamma(2)1$). It is thus possible to consider the mixed homology group $H_1(X_\Gamma - \partial_\Gamma^-, \partial_\Gamma^+; \mathbb{Z})$ (and its dual $H_1(X_\Gamma - \partial_\Gamma^+, \partial_\Gamma^-; \mathbb{Z})$). One gets a group isomorphism

$$\xi_\Gamma^+ : \mathbb{Z}[\Gamma \backslash \bar{\Gamma}(2)] \rightarrow H_1(X_\Gamma - \partial_\Gamma^-, \partial_\Gamma^+; \mathbb{Z})$$

which, for $g \in \bar{\Gamma}(2)$, associates to Γg the class $\xi_\Gamma(g)$ in $H_1(X_\Gamma - \partial_\Gamma^-, \partial_\Gamma^+; \mathbb{Z})$ of a path from $g0$ to $g\infty$ in the upper half-plane.

Consider now the case where $\Gamma = \Phi'_N$. To simplify notations, set $\partial^+ = \partial_\Gamma^+$ and $\partial^- = \partial_\Gamma^-$. Recall that we have a group isomorphism $\Phi'_N \backslash \Gamma(2) \rightarrow H_{N,N,N'}$ which, for $(a, b, c) \in (\mathbb{Z})^3$, to

$\Phi'_N A^a C^c B^b$ associates $x^a z^c y^b$. We get thus a group isomorphism

$$\mathbb{Z}[H_{N,N,N'}] \simeq H_1(X'_N - \partial^-, \partial^+; \mathbb{Z}).$$

For $(a, b, c) \in (\mathbb{Z}/N\mathbb{Z})^2 \times (\mathbb{Z}/N'\mathbb{Z})$, set $i(a, b, c) = \xi_{\Phi'_N}^+(\Phi'_N A^a C^c B^b)$.

Thus, $H_{N,N,N'}$ acts on the curve X'_N , and transitively on the sets of cusps of X'_N above 0, 1 and ∞ respectively. Thus the stabilizer of a cusp is cyclic of order N .

The long exact sequence of relative homology yields:

$$0 \rightarrow H_1(X'_N - \partial^-; \mathbb{Z}) \rightarrow H_1(X'_N - \partial^-, \partial^+; \mathbb{Z}) \xrightarrow{\delta_N} \mathbb{Z}[\partial^+]^0 \rightarrow 0$$

where δ_N is the boundary map. Similarly we have a dual exact sequence:

$$0 \rightarrow \mathbb{Z}[\partial^-]^0 \xrightarrow{\delta_N^*} H_1(X'_N - \partial^-, \partial^+; \mathbb{Z}) \rightarrow H_1(X'_N, \partial^+; \mathbb{Z}) \rightarrow 0$$

where δ_N^* is the dual boundary map. It induces

$$0 \rightarrow \mathbb{Z}[\partial^-]^0 \xrightarrow{\delta_N^*} H_1(X'_N - \partial^-; \mathbb{Z}) \rightarrow H_1(X'_N; \mathbb{Z}) \rightarrow 0.$$

Hence $H_1(X'_N; \mathbb{Z})$ can be described as a subquotient of the group $H_1(X'_N - \partial^-, \partial^+; \mathbb{Z})$. We will make this explicit by spelling out the maps δ_N and δ_N^* .

The sets of cusps of X'_N lying above $\infty, 0$ and 1 are respectively $\Phi'_N \backslash \Gamma(2)/A^{\mathbb{Z}}, \Phi'_N \backslash \Gamma(2)/B^{\mathbb{Z}}$ and $\Phi'_N \backslash \Gamma(2)/(AB^{-1})^{\mathbb{Z}}$. All three sets can be understood as follows.

Proposition 24. *We have three bijective maps as follows:*

$$\Phi'_N \backslash \Gamma(2)/A^{\mathbb{Z}} \rightarrow (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N'\mathbb{Z})$$

given by $x^a z^c y^b \mapsto (b, c + ab)$,

$$\Phi'_N \backslash \Gamma(2)/B^{\mathbb{Z}} \rightarrow (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N'\mathbb{Z})$$

given by $x^a z^c y^b \mapsto (a, c)$, and

$$\Phi'_N \backslash \Gamma(2)/(AB^{-1})^{\mathbb{Z}} \rightarrow (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N'\mathbb{Z})$$

given by $x^a z^c y^b \mapsto (a + b, c - b(b + 1)/2)$.

Proof. The first two identifications are straightforward. We establish the third one. Let k be an integer. One finds by induction on k , $x^a z^c y^b (xy^{-1})^k = x^{a+k} z^{c-kb+k(k-1)/2} y^{b-k}$. Since $(a + k) + (b - k) = a + b$ and

$$c - kb + k(k - 1)/2 - (b - k)(b - k + 1)/2 = c - b(b + 1)/2,$$

the map passes indeed to the quotient $\Phi'_N \backslash \Gamma(2)/(AB^{-1})^{\mathbb{Z}}$. It is surjective (take $b = 0$). Since there are NN' cusps above 1, it is bijective. □

Denote by $j_\infty(b, c)$ the cusp $\Phi'_N A^a C^{c-ab} B^b A^{N\mathbb{Z}}$, for any $a \in \mathbb{Z}$, by $j_0(a, c)$ the cusp $\Phi'_N A^a C^c B^b B^{N\mathbb{Z}}$, for any $b \in \mathbb{Z}$, and $j_1(d, c)$ the cusp $\Phi'_N A^a C^{c-b(b+1)/2} B^b (AB^{-1})^{N\mathbb{Z}}$, for any $a, b \in \mathbb{Z}$ such that $a + b = d$. With these conventions we can express δ_N .

Proposition 25. *Let $a, b, c \in \mathbb{Z}$. One has $\delta_N(i(a, b, c)) = j_\infty(b, c - ab) - j_0(a, c)$.*

Proof. The boundary of the modular symbol $\{A^a C^c B^b 0, A^a C^c B^b \infty\}$ is

$$[\Phi'_N A^a C^c B^b A^{\mathbb{Z}}] - [\Phi'_N A^a C^c B^b B^{\mathbb{Z}}],$$

which translates immediately into the claimed formula. □

We use [2, Proposition 5] to determine δ_N^* .

Proposition 26. *One has, for $d \in \mathbb{Z}/N\mathbb{Z}$ and $c \in \mathbb{Z}/N'\mathbb{Z}$,*

$$\delta_N^*(j_1(d, c)) = \sum_{\substack{a, b \in \mathbb{Z}/N\mathbb{Z}, \\ a+b=d}} i(a, b+1, c - b(b+1)/2) - i(a, b, c - b(b+1)/2).$$

Proof. We just need to translate the third statement [2, Proposition 5]. With the notations of that proposition, we have $w_1 = N$. It remains to use the third bijection of proposition 24 and the definition of i . □

Let S_N be the subgroup of $\mathbb{Z}[(\mathbb{Z}/N\mathbb{Z})^2 \times \mathbb{Z}/N'\mathbb{Z}]$ formed by the elements of the form $\sum_{a,b,c} \lambda_{a,b,c} [a, b, c]$, satisfying, for every $(a, c) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N'\mathbb{Z})$, the relation $\sum_{b \in \mathbb{Z}/N\mathbb{Z}} \lambda_{a,b,c} = 0$ and, for every $(b, c) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N'\mathbb{Z})$, the relation $\sum_{a \in \mathbb{Z}/N\mathbb{Z}} \lambda_{a,b,c+ab} = 0$. By Proposition 25, its image by i has boundary 0.

Let R_N be the subgroup of $\mathbb{Z}[(\mathbb{Z}/N\mathbb{Z})^2 \times \mathbb{Z}/N'\mathbb{Z}]$ spanned by elements of the form

$$e_{c,d} = \sum_{\substack{a, b \in \mathbb{Z}/N\mathbb{Z}, \\ a+b=d}} [a, b+1, c - b(b+1)/2] - [a, b, c - b(b+1)/2],$$

for $(d, c) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N'\mathbb{Z})$. By Proposition 26, it is a subgroup of S_N . Thus we get a presentation by generators and relations of the homology of X'_N .

Corollary 27. *The map i produces an exact sequence*

$$0 \rightarrow R_N \rightarrow S_N \rightarrow H_1(X'_N; \mathbb{Z}) \rightarrow 0.$$

Remark 28. By exchanging the roles of ∂^+ and ∂^- , it is possible to give a dual presentation of $H_1(X'_N; \mathbb{Z})$. We leave this to the reader.

4. THE HEISENBERG COVERING AND ITS MODELS

In this section, we assume N to be odd. Therefore $N' = N$.

4.1. Modular functions. Let $z \in \mathbb{H}$. For $q_2 = \exp(\pi iz)$, consider the classical λ -function [13]:

$$\lambda(z) = 16q_2 \prod_{n \geq 1} \left(\frac{1 + q_2^{2n}}{1 + q_2^{2n-1}} \right)^8, \quad 1 - \lambda(z) = \prod_{n \geq 1} \left(\frac{1 - q_2^{2n-1}}{1 + q_2^{2n-1}} \right)^8.$$

From the above expression, it is clear that $\lambda(1) = 1$ and $(1 - \lambda(1)) = 0$. The N -th roots

$$x := \sqrt[N]{\lambda}, y := \sqrt[N]{1 - \lambda}$$

define modular units for Φ_N . We recover thus the familiar model of the Fermat curve.

Since the λ function identifies $\mathbb{P}^1 - \{0, 1, \infty\}$ to $Y(2)$, a covering of $\mathbb{P}^1 - \{0, 1, \infty\}$ can be understood as a covering of $Y(2)$, *i.e.* a modular curve.

4.2. Reminder on Fermat curves. The N -th Fermat curve F_N is given by the projective model:

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

Fermat curves and their points at infinity (cusps) are studied extensively by Rohrlich [16], [17], V'elu [18] and Posingies [15]. In particular, these authors consider the map

$$\beta_N : F_N \rightarrow \mathbb{P}^1$$

given by $(X : Y : Z) \rightarrow (X^N : Z^N)$. The map β_N is of degree N^2 . It is ramified only above the points $0, 1, \infty$. The corresponding ramification points are given by $a_j = (0 : \zeta^j : 1)$, $b_j = (\zeta^j : 0 : 1)$, $c_j = (\epsilon \zeta^j : 1 : 0)$, for $j \in \mathbb{Z}/N\mathbb{Z}$.

Recall that ζ is a primitive N -th root of unity and ϵ is a square root of ζ . Each of the above points has ramification index N over \mathbb{P}^1 . For all $j \in \mathbb{Z}/N\mathbb{Z}$, the cusps a_j, b_j, c_j are all defined over the cyclotomic field $\mathbb{Q}(\mu_N)$. Among them, only a_0, b_0 and c_0 are defined over \mathbb{Q} .

4.3. The cuspidal subgroup of the Fermat curve. The divisors of following modular functions are given by:

$$\operatorname{div}(x - \zeta^j) = Nb_j - \sum_j c_j, \operatorname{div}(y - \zeta^j) = Na_j - \sum_j c_j, \operatorname{div}(x - \epsilon \zeta^j y) = Nc_j - \sum_j c_j.$$

Rohrlich [17] has determined the structure of the cuspidal group of the Jacobian of F_N (see also V'elu's alternative proof and description [18]). Since every cuspidal divisor on F_N is annihilated by N in the Jacobian, the cuspidal group is a quotient of $\mathbb{Z}/N\mathbb{Z}[\partial_{\Phi_N}]^0$. The additional relations are given as follows. Recall that N is odd.

Theorem 29 (Rohrlich [17]). *The group \mathcal{P} of principal divisors is spanned by the following set*

$$\left\{ \sum_{i=0}^{N-1} [a_i] - [P], \sum_{i=0}^{N-1} [b_i] - [P], \sum_{i=0}^{N-1} [c_i] - [P], \right. \\ \left. \sum_{i=0}^{N-1} i([a_i] - [b_i]), \sum_{i=0}^{N-1} i([a_i] - [c_i]), \sum_{i=0}^{N-1} i^2([a_i] + [b_i] + [c_i] - 3[P]) \right\},$$

where P is any cusp of F_N . Thus the cuspidal subgroup of the Jacobian of F_N is a free $\mathbb{Z}/N\mathbb{Z}$ -module of rank $3N - 7$.

We set

$$D_A = \sum_{i \in \mathbb{Z}/N\mathbb{Z}} \{i\}[a_i],$$

(resp. $D_B = \sum_{i \in \mathbb{Z}/N\mathbb{Z}} \{i\}[b_i]$, resp. $D_C = \sum_{i \in \mathbb{Z}/N\mathbb{Z}} \{i\}[c_i]$) and

$$f_A = \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^{\{i\}}.$$

Corollary 30. *The class of D_A is of order N in the cuspidal subgroup of the Jacobian of F_N . Moreover it is congruent to D_B and D_C modulo \mathcal{P} .*

Proof. Indeed the divisor of f_A is ND_A . By Rohrlich’s theorem, D_A is of order N . The congruence of D_A, D_B and D_C modulo \mathcal{P} follows from Rohrlich’s relations. □

4.4. The covering as a function field extension. By Rohrlich’s theorem, the order of D_A in the cuspidal group is N , therefore an N -th root of f_A defines a cyclic covering $G \rightarrow F_N$ (a provisional notation, since G will be shown to be equal to F'_N) of degree N . Such a morphism is indeed unramified, since the divisor of f_A belongs to $N\mathbb{Z}[\partial_{\Phi_N}]^0$. Since $D_A - D_B$ is a principal divisor, exchanging the roles of X and Y would give the same covering. A similar reasoning with respect to D_C holds. The cyclic covering $G \rightarrow F_N$ translates into a covering of Riemann surfaces $W \rightarrow X_N$.

Consider now the third term $[\Gamma(2), [\Gamma(2), \Gamma(2)]]$ in the lower central series of $\Gamma(2)$. It is not a subgroup of finite index of $\Gamma(2)$, but one can still consider the Riemann surface $X_{[\Gamma(2), [\Gamma(2), \Gamma(2)]]}$.

Proposition 31. *The covering $W \rightarrow X_N$ factorizes through $X_{[\Gamma(2), [\Gamma(2), \Gamma(2)]]}$.*

Proof. Let $U \in \Gamma(2)$ and $V \in [\Gamma(2), \Gamma(2)]$. Let g be an N -th root of f_A . One has to prove that g is invariant under $[U, V]$, that is $g_{|UV} = g_{|VU}$. Note first that $y|_U = \zeta^r y$, with $r \in \mathbb{Z}$. One has

$$g_{|U}^N = \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-\zeta^r y + \zeta^i)^{\{i\}} = \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^{i-r})^{\{i\}} = \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^{\{i+r\}}.$$

Write $\{i + r\} = \{i\} + r + t$, with $t \in N\mathbb{Z}$. Thus we get

$$g_{|U}^N = g^N \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^r \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^t.$$

The last factor is obviously an N -th power. By the description of Rohrllich of the cuspidal subgroup of F_N , the factor $\prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^r$ is an N -th power in the function field of F_N . So there exists a function h on F_N , and an integer s such that $g_{|U} = g\zeta^s h$. Note that $h_{|V} = h$ and $g_{|V} = \zeta^q g$, with $q \in \mathbb{Z}$. Therefore, one has:

$$g_{|UV} = g_{|V}\zeta^s h_{|V} = \zeta^{s+q} g h = \zeta^q g_{|U} = g_{|UV}.$$

□

Proposition 32. *Any covering of degree N of the Fermat modular curve X_N that factors through $X_{[\Gamma(2), [\Gamma(2), \Gamma(2)]]}$, factors through the Heisenberg covering.*

Proof. Such a covering corresponds to a cyclic quotient of order N of Φ_N . Denote by Γ the corresponding cocyclic subgroup of Φ_N . Since the covering is unramified at the cusps, Γ contains the matrices A^N and B^N . Recall that Φ_N is generated by A^N , B^N and the commutator subgroup of $\Gamma(2)$. Since the covering factors through $X_{[\Gamma(2), [\Gamma(2), \Gamma(2)]]}$, the group Γ contains $[\Gamma(2), [\Gamma(2), \Gamma(2)]]$. In particular, Γ contains $[A, C]$ and $[B, C]$. Thus the image of C in Φ_N/Γ is of order N . Consequently, Γ is the group generated by $[\Gamma(2), [\Gamma(2), \Gamma(2)]]$, A^N , B^N , C^N . □

Corollary 33. *Let ζ be a primitive N -th root of unity in $\mathbb{Q}(\mu_N)$. The function*

$$f'_A = \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^{\{i\}}$$

admits an N -th root in the function field of F'_N .

Proof. Indeed, the covering of F_N defined by an N -th root of f'_A is cyclic of order N and factorizes through $X_{[\Gamma(2), [\Gamma(2), \Gamma(2)]]}$. Consequently, it is F'_N . □

Let K be the field of fractions of the curve given in the introduction over the complex numbers. In inhomogeneous form, it is generated by the variable X, Y, T_ζ for every primitive N -th root of unity ζ , with the relations

$$X^N + Y^N = 1$$

and, for every primitive N -th root of unity ζ (in $\mathbb{Q}(\mu_N)$)

$$\prod_{j=1}^{(N-1)/2} (Y - \zeta^{-j})^j T_\zeta^N = \prod_{j=1}^{(N-1)/2} (Y - \zeta^j)^j.$$

Corollary 34. *The function field of F'_N over \mathbb{C} is isomorphic to K .*

Proof. Indeed, the function field of F'_N is the subfield of K generated by an N -th root of f_A over the function field of F_N . Let ζ' be a primitive N -th root of unity. By the preceding corollary, $T_{\zeta'}$ belongs to K . Thus all of K is contained in the function field of F'_N . \square

Thus we have shown that the curve F'_N extends the Riemann surface X'_N .

Corollary 35. *The Riemann surfaces X'_N and $F'_N(\mathbb{C})$ are isomorphic.*

4.5. The Heisenberg covering. Denote by G the Galois group of the field extension $K|\mathbb{Q}(X^N)$. It sits in an exact sequence

$$1 \rightarrow H_N \rightarrow G \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow 1$$

by the transitive action of G on N -th roots of unity, and the fact that the Heisenberg covering is defined over $\mathbb{Q}(\zeta)$. Recall that for $i \in (\mathbb{Z}/N\mathbb{Z})$, $\{i\}$ denotes the representative of i in $\{-(N-1)/2, \dots, (N-1)/2\}$.

Proposition 36. *For $\sigma \in G$, there exists $u, v, s \in (\mathbb{Z}/N\mathbb{Z})$ and $r \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $\sigma(X) = \zeta^u X$, $\sigma(Y) = \zeta^v(Y)$, $\sigma(\zeta) = \zeta^r$. For ρ a representative of r in \mathbb{Z} ,*

$$\sigma(T^\rho) = \zeta^s T X^v \prod_{i \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^i)^{\rho\{i/\rho\} - \{i\}}/N.$$

Furthermore, $(u, v, s, r) \in (\mathbb{Z}/N\mathbb{Z})^3 \times (\mathbb{Z}/N\mathbb{Z})^\times$ characterizes σ .

Proof. The first three identities are evident. A simple calculation establishes the last one. Indeed

$$\sigma(T^\rho)^N = \sigma(T^N)^\rho = \sigma\left(\prod_{i \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^i)^{\{i\}}\right)^\rho = \prod_{i \in (\mathbb{Z}/N\mathbb{Z})} (-\zeta^v Y + \zeta^{\rho i})^{\{i\}\rho}.$$

By factoring T^N and $\prod_i \zeta^{v\{i\}}$, and replacing the variable i by $j = \rho i - v$, one gets

$$\sigma(T^\rho)^N = T^N \prod_i \zeta^{v\{i\}} \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)^{\rho\{(j+v)/\rho\}} \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)^{-\{j\}}.$$

We use $\prod_i \zeta^{v\{i\}} = 1$ and we get

$$\sigma(T^\rho)^N = T^N \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)^{\rho\{(j+v)/\rho\} - \{j\} - v} \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)^v.$$

Using the identity $X^N = (1 - Y^N) = \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)$, we get

$$\sigma(T^\rho)^N = T^N X^{Nv} \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)^{\rho\{(j+v)/\rho\} - \{j\} - v}.$$

The desired formula follows by taking N -th roots. \square

With the notations of the proposition, we note $\sigma = \sigma_{u,v,r,s}$. Murty and Ramakrishnan note that Deligne showed that F'_N can be defined over \mathbb{Q} , without giving a reference. We spell out this assertion.

Proposition 37. *The curve F'_N can be defined over \mathbb{Q} . More precisely, the surjective map $G \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ admits the map $r \mapsto \sigma_{0,0,r,0}$ as a section. Denote by S the corresponding subgroup of G . It acts trivially on N -th roots of unity. Consequently, the field of invariants by S in K is the function field of a curve over \mathbb{Q} , and defines F'_N over \mathbb{Q} . The Heisenberg covering $F'_N \rightarrow F_N$ extends also over \mathbb{Q} .*

Proof. Group theoretic arguments about the structure of G as an extension imply easily the existence of the section. We will show that our explicit map is indeed a section. Let $r, r' \in (\mathbb{Z}/N\mathbb{Z})^\times$ and ρ and ρ' be representatives of r and r' respectively in \mathbb{Z} . We need to check that $\sigma_{0,0,r',0}\sigma_{0,0,r,0} = \sigma_{0,0,rr',0}$, which need to be verified only by application on T , or equivalently on $T^{\rho\rho'}$, and on ζ . This is trivial for ζ . Here is the computation on $T^{\rho\rho'}$. We first simplify the formula of the previous proposition

$$\sigma_{0,0,r,0}(T^{\rho\rho'}) = T^{\rho'} \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)^{(\rho\{j/\rho\} - \{j\})\rho'/N}.$$

Thus one has

$$\sigma_{0,0,r',0}\sigma_{0,0,r,0}(T^{\rho\rho'}) = T \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)^{(\rho'\{j/\rho'\} - \{j\})/N} \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^{\rho'j})^{(\rho\{j/\rho\} - \{j\})\rho'/N}.$$

A change of variable in the second product of the right-hand side gives

$$\sigma_{0,0,r',0}\sigma_{0,0,r,0}(T^{\rho\rho'}) = T \prod_{j \in (\mathbb{Z}/N\mathbb{Z})} (-Y + \zeta^j)^{(\rho\rho'\{j/\rho\rho'\} - \{j\})/N} = \sigma_{0,0,rr',0}(T^{\rho\rho'}).$$

□

4.6. Automorphisms. The group $(\mathbb{Z}/N\mathbb{Z})^2 \simeq \Gamma(2)/\Phi_N$ acts on $F_N : (i, j) \in (\mathbb{Z}/N\mathbb{Z})^2$ acts by the rule $(x, y) \mapsto (\zeta^i x, \zeta^j y)$. Such an action is defined on $\mathbb{Q}(\mu_N)$. It lifts to an action of $H_{\mathbb{Z}/N\mathbb{Z}} \simeq \Gamma(2)/\Phi'_N$ on F'_N .

Lemma 38. *The action of $H_{\mathbb{Z}/N\mathbb{Z}}$ on F'_N is defined over $\mathbb{Q}(\mu_N)$.*

Proof. For $U \in H_{\mathbb{Z}/N\mathbb{Z}}$, one needs to check that the action of U on a $\mathbb{Q}(\zeta)$ -rational function is still $\mathbb{Q}(\zeta)$ -rational. It suffices to verify this for g , an N -th root of f_A . We repeat a previous calculation and get

$$g|_U^N = g^N \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^r \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^t,$$

with $t \in N\mathbb{Z}$. Both factors $\prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^r$ and $\prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-y + \zeta^i)^t$ are N -th power, (of, say, g_1 and g_2) in the function field of F_N over $\mathbb{Q}(\zeta)$. We thus find that $g|_U$ is equal to $\zeta^p g g_1 g_2$, which belongs to the function field of X_N over $\mathbb{Q}(\zeta)$. \square

Remark 39. We do not give an explicit algebraic model of the curve X''_N . But it can be obtained by taking N'' -th roots of the functions whose divisors are $\sum_{i=0}^{N-1} i^2([a_i] - [P])$, $\sum_{i=0}^{N-1} i^2([b_i] - [P])$ and $\sum_{i=0}^{N-1} i^2([c_i] - [P])$.

4.7. Regular integral models of Heisenberg curves. We relate the Heisenberg covering to the model given in the introduction. Note that the inhomogeneous version of the projective model is given by:

$$X^N + Y^N = 1$$

and, for every primitive N -th root of unity ζ (in a fixed cyclotomic extension of \mathbb{Q})

$$\prod_{j=1}^{(N-1)/2} (Y - \zeta^{-j})^j T_\zeta^N = \prod_{j=1}^{(N-1)/2} (Y - \zeta^j)^j.$$

We now prove Theorem 1 (in the spirit of e.g. [3, Proposition 1.1.13]).

Proof. We have indeed a scheme of relative dimension 1 over $\text{Spec}(\mathbb{Z}[\mu_N, 1/N])$. We just have to establish the smoothness. We use the Jacobian criterion (e.g. [8, p. 130, Theorem 2.19]).

Since the Heisenberg covering is obtained by taking the N -th root of a function which does not vanish outside the zero locus of XY , all points away from $X = 0$ and $Y = 0$ are regular in all characteristics prime to N . It remains to establish the regularity of a point P_ζ of the form $(X, Y) = (0, \zeta)$ or $(X, Y) = (\zeta, 0)$ with ζ a primitive N -th root of unity. Suppose $(X, Y) = (0, \zeta)$. For points of this form, one has $T_\zeta = 0$. We set

$$F_\zeta = \prod_{j=1}^{(N-1)/2} (Y - \zeta^{-j})^j T_\zeta^N - \prod_{j=1}^{(N-1)/2} (Y - \zeta^j)^j$$

and compute the partial derivative at P_ζ . One obtains

$$\frac{\partial F_\zeta}{\partial Y}(P_\zeta) = - \prod_{j=2}^{(N-1)/2} (\zeta - \zeta^j)^j,$$

which is a cyclotomic unit that belongs to $\mathbf{Z}[\mu_N, 1/N]^\times$. Thus the jacobian matrix is non-zero over any fiber in characteristic prime to N . This is sufficient to establish the regularity of P_ζ over $\text{Spec}(\mathbf{Z}[\mu_N, 1/N])$ since the structural morphism is of relative dimension 1. This reasoning applies to the zero locus of Y , by exchanging the roles of X and Y . \square

4.8. Cusps. The term cusp refers to the cusps of the modular curve X_Γ attached to a subgroup Γ of $\Gamma(2)$. These points are not intrinsic to the corresponding algebraic curves. In the cases of interest to us, we have a morphism $X_N \rightarrow X(2)$, given by the function x^N . Thus the cusps of F_N are the $3N$ points above the points $0, 1$, and ∞ described above.

Since the morphism $F'_N \rightarrow F_N$ is unramified, the modular curve F'_N possesses $3N^2$ cusps.

Proposition 40. *If N is prime to 3, the cusps of F'_N are defined over $\mathbb{Q}(\zeta)$. If 3 divides N , the cusps of F'_N are defined over the cyclotomic field generated by the $3N$ -th roots of unity.*

Proof. Let a be a cusp of F'_N above a_0 . It is defined over the field generated by $g(a)$ and $\mathbb{Q}(\zeta)$, where g is an N -th root of f_A . One has

$$f_A(a_0) = \prod_{i \in \mathbb{Z}/N\mathbb{Z}} (-1 + \zeta^i)^{\{i\}} = \prod_{i=1}^{(N-1)/2} \frac{(-1 + \zeta^i)^i}{(-1 + \zeta^{-i})^i} = \prod_{i=1}^{(N-1)/2} (-\zeta^i)^i.$$

Thus we get

$$f_A(a_0) = (-1)^{\sum_{i=1}^{(N-1)/2} i} \zeta^{\sum_{i=1}^{(N-1)/2} i^2} = (-1)^{(N^2-1)/8} \zeta^{(N-1)(N+1)N/24},$$

which is a 6-th root of unity.

Suppose N is prime to 3. Then $g(a)$ is an N -th root of unity, up to sign. Since the group H_N acts transitively on the cups above ∞ , and its action is $\mathbb{Q}(\zeta)$ -rational, we deduce that all the cusps above ∞ are defined over $\mathbb{Q}(\zeta)$. A similar reasoning apply to the cusps above 0, and above 1.

A similar reasoning applies when 3 divides N . Indeed $g(a)$ is a $3N$ -th root of unity, up to sign. □

The cusps of F'_N above the cusp ∞ (resp. 0, resp. 1) of $X(2)$ coincide with the classes $\Gamma \backslash \Gamma(2) \infty$ (resp. $\Gamma \backslash \Gamma(2)0$, resp. $\Gamma \backslash \Gamma(2)1$), which in turn can be identified with the double classes $\Gamma \backslash \Gamma(2) / A^{\mathbb{Z}}$ (resp. $\Gamma \backslash \Gamma(2) / B^{\mathbb{Z}}$, resp. $\Gamma \backslash \Gamma(2) / (AB^{-1})^{\mathbb{Z}}$).

4.9. About the Manin-Drinfeld principle for F'_3 . Recall that $g_3 = 1$ and observe that F'_3 has 27 cusps. Fix one cusp P_0 of F'_3 , which becomes thus an elliptic curve (F'_3, P_0) . Since a cyclic group of order 3 acts on F'_3 and stabilizes P_0 , the elliptic curve (F'_3, P_0) admits an automorphism of order 3. Thus the j -invariant of (F'_3, P_0) is 0.

Proposition 41. *Divisors supported on the cusps of F'_3 above ∞ (resp. 0, resp. 1) are of order dividing 3 in the Jacobian of F'_3 . Furthermore, cuspidal divisors of degree 0 are torsion in the Jacobian of F'_3 , and of order dividing 9.*

Proof. Let X be a compact connected Riemann surface of genus 1. Let J be the Jacobian of X . Recall the exact sequence

$$0 \rightarrow J(\mathbf{C}) \rightarrow \text{Aut}(X) \rightarrow \text{Aut}(J) \rightarrow 0,$$

where Aut denotes the automorphisms over \mathbf{C} . The first map associates to the class of a divisor D the translation by D in X .

For $X = F'_3$, the group $\text{Aut}(J)$ is cyclic of order 6. One gets a group homomorphism $H_{\mathbf{Z}/3\mathbf{Z}} \rightarrow \text{Aut}(J)$, whose kernel is of order 9, and therefore isomorphic to $(\mathbf{Z}/3\mathbf{Z})^2$. Since this kernel identifies to a subgroup of the one dimensional complex torus $J(\mathbf{C})$, the latter subgroup is $J(\mathbf{C})[3]$. We have proved that the orbit of any cusps Q by $H_{\mathbf{Z}/3\mathbf{Z}}$ contains $Q + J(\mathbf{C})[3]$. But these sets are both of cardinality 9, and are therefore equal. Since $H_{\mathbf{Z}/3\mathbf{Z}}$ acts transitively on the cusps above ∞ (resp. 0, resp. 1), the first statement of the proposition is proved.

About the second statement, it is sufficient to prove this for a divisor of the form $(\alpha) - (\beta)$ where α and β are cusps of F'_3 not above the same point of $\{0, 1, \infty\}$. Without loss of generality, say they are above 0 and ∞ respectively. Let a and b be the cusps of F_3 below α and β respectively. We have

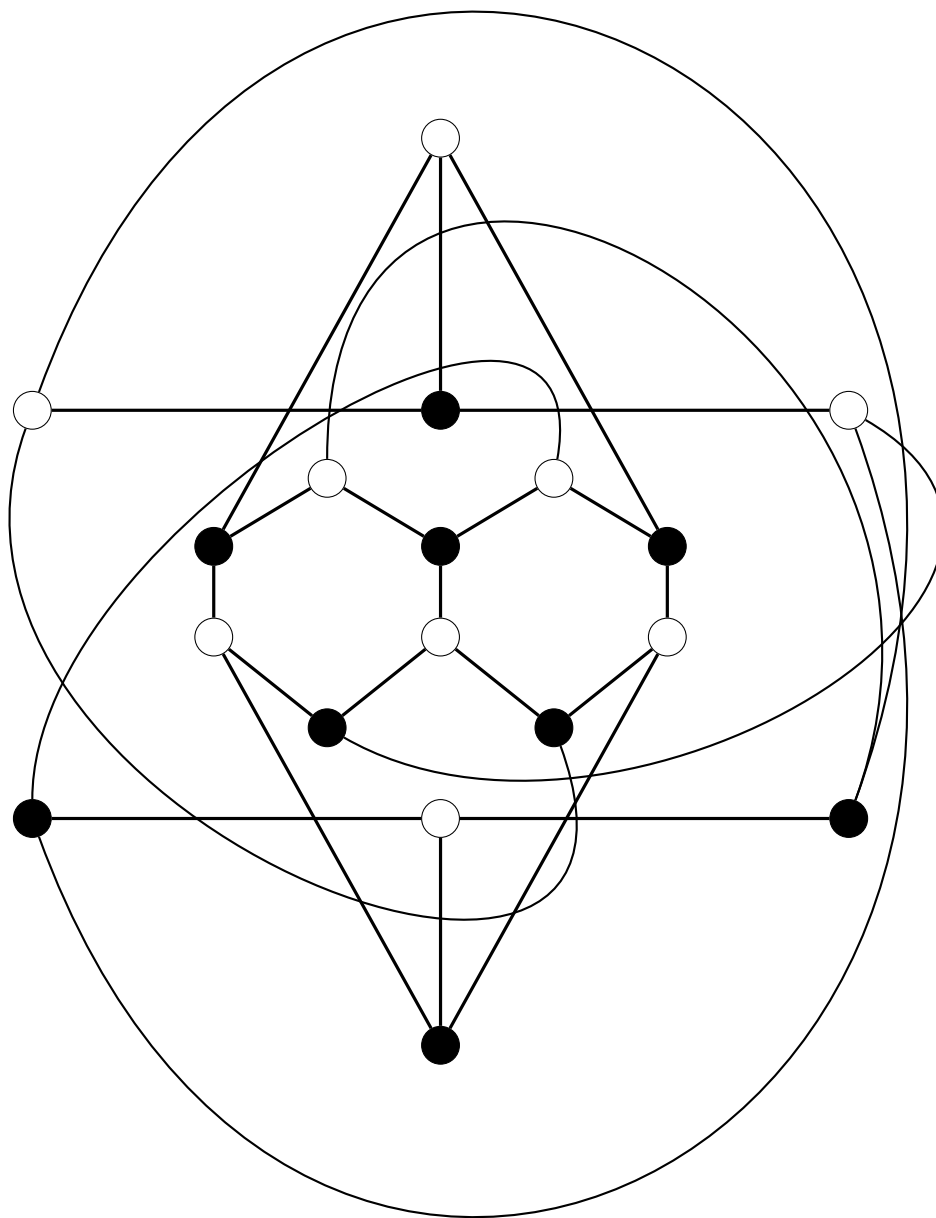
$$3((\alpha) - (\beta)) = (3(\alpha) - \sum_{\alpha'}(\alpha')) + (\sum_{\alpha'}(\alpha') - \sum_{\beta'}(\beta')) + (\sum_{\beta'}(\beta') - 3(\beta)),$$

where α' (resp. β') runs through the cusps of F'_3 above a (resp. b). By the first statement of the proposition and the torsion properties of the cuspidal subgroup of the F_3 , each of the three terms of the right-hand side is of order dividing 3. □

Recall that the dessin for X'_N is a graph with the following additional structure: the vertices are bicolored (white and black) and the of set edges attached to any given vertex are endowed with a cyclic ordering (a transitive action of \mathbb{Z}). The vertices are the cusps of X'_N above 0 and ∞ . The edges form the coset $\Phi'_N \backslash \Gamma(2) \simeq H_{\mathbb{Z}/N\mathbb{Z}}$, which is in bijection with $(\mathbb{Z}/N\mathbb{Z})^3$. the edge associated with $\Phi'_N g$ has extremities $\Phi'_N g 0$ and $\Phi'_N g \infty$. The cyclic ordering of the edges attached to the vertices $\Phi'_N g 0$ (resp. $\Phi'_N g \infty$) is given by the action of B (resp. A^{-1}). To sum up the dessin can be drawn on X'_N .

To be more concrete, each edge is in bijection with $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, via the map $\Phi'_N A^a C^c B^b \mapsto (a, c, b)$. The edge thus labeled (a, c, b) is connected to the edge labeled $(a, c, b + 1)$ via a black vertex (cusp above 0) and the edge labeled (a, c, b) is connected to the edge labeled $(a - 1, c - ab, b)$ via a white vertex (cusp above ∞). The line segments represent the arcs on X'_3 above the geodesic arc from 0 to ∞ in the upper half-plane.

We illustrate all this for $N = 3$. In that case, the genus of X'_3 is equal to 1. According to these rules, the drawing (dessin) for X'_3 is given as follows.



As the group Φ_3 is not a congruence subgroup [14], Φ'_3 is *a fortiori* not a congruence subgroup. The latter fact can be derived alternately from Wolfart’s criterion and an examination of the dessin. Indeed, the width of the each cusps is equal to 6 and $[\Gamma(2) : \Phi'_3] = 27$. Wolfart’s criterion, to check that Φ'_3 is a congruence subgroup or not it is enough to check $\Gamma(6) \subset \Phi'_3 \subset \Gamma(2)$. However, $[\Gamma(2) : \Gamma(6)] = 144$ is not divisible by the index 27.

4.10. About the failure of the Manin-Drinfeld principle for F'_5 . Suppose $N = 5$. We show that the Manin-Drinfeld theorem fails for the Heisenberg covering \mathcal{F}'_5 of \mathcal{F}_5 . Consider the scheme \mathcal{C}_5 over $\text{Spec}(\mathbf{Z}[\mu_5, 1/5])$ given by the system of equations

$$T^5_\zeta = \frac{(-Y + \zeta)(-Y + \zeta^2)^2}{(-Y + \zeta^{-1})(-Y + \zeta^{-2})^2},$$

where ζ runs through the primitive 5-th roots of unity in $\mathbb{Q}(\mu_5)$. It is smooth, as can be shown by applying the Jacobian criterion. One has an obvious morphism of schemes $\mathcal{F}'_5 \rightarrow \mathcal{C}_5$.

Denote by C_5 the generic fiber of \mathcal{C}_5 . Over \mathbb{C} , C_5 identifies to a modular curve as follows. Consider the morphism $\bar{\Gamma}(2) \rightarrow H_{5,5,5}$ and the inverse image Γ' of the subgroup of $H_{5,5,5}$ generated by B . Then Γ' defines a corresponding modular curve isomorphic to the Riemann surface $C_5(\mathbb{C})$.

The curve C_5 possesses 19 cusps, given by the following planar coordinates $(Y, T_\zeta) : (0, \epsilon), (\infty, \epsilon), (1, -\delta), (\zeta, 0), (\zeta^2, 0), (\zeta^{-1}, \infty), (\zeta^{-2}, \infty)$, where ϵ and δ run through the 5-th roots of unity. Set $T = T_\zeta$. The function fields of F'_5 and C_5 are $\mathbf{Q}(\zeta, X, Y, T)$ and $\mathbf{Q}(\zeta, Y, T)$ respectively.

The obvious morphism $\pi : F'_5 \rightarrow C_5$ sends the cusps of F'_5 to the cusps of C_5 . We show that C_5 does not satisfy the Manin-Drinfeld principle. Since \mathcal{C}_5 is smooth, the Jacobian of \mathcal{C}_5 extends to an abelian scheme \mathcal{J}_5 over $\text{Spec}(\mathbf{Z}[\mu_5, 1/5])$.

Proposition 42. *There exists a divisor of infinite order supported on the cusps of C_5 .*

Proof. We suppose that all cuspidal divisors are torsion in C_5 . Our proof is organized around the following calculation. One has

$$(4.1) \quad T^5 + 1 = \frac{(1 - Y)(2Y^2 + (2 - 2(\zeta^2 + \zeta^{-2}) - \zeta - \zeta^{-1})Y + 2)}{(-Y + \zeta^{-1})(-Y + \zeta^{-2})^2}.$$

Let y_1 and y_2 be the roots of the polynomial $2Y^2 + (2 - 2(\zeta^2 + \zeta^{-2}) - \zeta - \zeta^{-1})Y + 2$. Let ζ_1 be a 5-th root of unity in $\mathbf{Z}[\mu_5]$. Consider the function $T + \zeta_1$, which divides $T^5 + 1$. The divisor of the function $T + \zeta_1$ is (in terms of planar coordinates for (Y, T)): $(1, -\zeta_1) + (y_1, -\zeta_1) + (y_2, -\zeta_1) - D$, where $D = (\zeta^{-1}, \infty) + 2(\zeta^{-2}, \infty)$. Apparently fortuitously, this divisor is cuspidal in the fibers at 11 and at 2 of C_5 .

Lemma 43. *Let ζ_1 and ζ_2 be distinct primitive 5-th roots of unity in $\mathbf{Z}[\mu_5]$. The divisors $3(1, \zeta_1) - 3(1, \zeta_2)$ and $3(1, \zeta_1) - D$ are principal in any fiber above 11 of C_5 .*

Proof. In characteristic 11, the polynomial $2Y^2 + (2 - 2(\zeta^2 + \zeta^{-2}) - \zeta - \zeta^{-1})Y + 2$ has the providential property of having a double root equal to 1. Therefore the divisor of the function $T + \zeta_1$ over \mathbb{F}_{11} is cuspidal and equal to $3(1, \zeta_1) - D$. It follows that the function $(T + \zeta_1)/(T + \zeta_2)$ has divisor $3(1, \zeta_1) - 3(1, \zeta_2)$. \square

We return to the proof of the proposition. By our Manin-Drinfeld assumption in C_5 , the divisor $3(1, \zeta_1) - D$ is torsion in the Jacobian of C_5 . It extends to a torsion point of \mathcal{J}_5 , whose order is determined in any special fiber at a prime π of residual characteristic p , provided $p - 1 > e$, where e is the ramification index at π of the extension $\mathbb{Q}(\mu_5)|\mathbb{Q}$ [11]. This applies for any prime except perhaps $p = 2$ and $p = 5$. The calculation for $p = 11$ ensures that the divisors $3(1, \zeta_1) - 3(1, \zeta_2)$ and $3(1, \zeta_1) - D$ are principal in C_5 .

Therefore those divisors are principal in any special fiber of \mathcal{C}_5 . Consider any fiber \bar{C} above 2 of C_5 . In that fiber, the function $T - \zeta = T + \zeta$ has divisor, in view of Equation 4.1, $(0, \zeta) + (1, \zeta) + (\infty, \zeta) - D_\zeta$, which is principal. Thus, by taking $\zeta_1 = \zeta$, the divisor

$$(3(1, \zeta) - D_\zeta) - ((0, \zeta) + (1, \zeta) + (\infty, \zeta) - D_\zeta) = 2(1, \zeta) - (0, \zeta) - (1, \zeta)$$

is principal in \bar{C} . Thus there exists $f : \bar{C} \rightarrow \mathbb{P}^1$ of degree 2. So \bar{C} is hyperelliptic. The principality of the divisor $3(1, \zeta_1) - 3(1, \zeta_2)$ ensures that there is a degree 3 morphism $\bar{C} \rightarrow \mathbb{P}^1$. By Castelnuovo-Severi type inequalities, this imposes that the genus of \bar{C} is ≤ 2 . But the genus of \bar{C} equals the genus of C_5 ; it is equal to 6 and we have reached a contradiction. \square

REFERENCES

- [1] G. Anderson and Y. Ihara, *Pro- l branched coverings of \mathbb{P}^1 and higher circular l -units*, Ann. of Math. (2) **128** (1988), no. 2, 271–293.
- [2] D. Banerjee and L. Merel, *The Eisenstein cycles and Manin–Drinfeld properties*, in Forum Mathematicum, Vol. 36, 305–325, De Gruyter (2024).
- [3] C. Curilla, *Regular models of Fermat’s curves and applications to Arakelov theory*, ProQuest LLC, Ann Arbor, MI (2010). Thesis (Ph.D.)–Yale University.
- [4] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, in Galois groups over \mathbb{Q} (Berkeley, CA, 1987), Vol. 16 of *Math. Sci. Res. Inst. Publ.*, 79–297, Springer, New York (1989).
- [5] O. Ejder, *Modular symbols for Fermat curves*, Proc. Amer. Math. Soc. **147** (2019), no. 6, 2305–2319.
- [6] M. Hall, Jr., *The theory of groups*, The Macmillan Company, New York, N.Y. (1959).
- [7] S. Lang, *Introduction to algebraic and abelian functions*, Vol. 89 of *Graduate Texts in Mathematics*, Springer-Verlag, New York-Berlin, second edition (1982), ISBN 0-387-90710-6.
- [8] Q. Liu, *Algebraic geometry and arithmetic curves*, Vol. 6 of *Oxford Graduate Texts in Mathematics*, Oxford University Press, Oxford (2002), ISBN 0-19-850284-2. Translated from the French by Reinie Ern e, Oxford Science Publications.
- [9] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972) 19–66.
- [10] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes  tudes Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

- [11] ———, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, *Invent. Math.* **44** (1978), no. 2, 129–162.
- [12] L. Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$* , *J. Reine Angew. Math.* **477** (1996) 71–115.
- [13] V. K. Murty and D. Ramakrishnan, *The Manin-Drinfeld theorem and Ramanujan sums*, *Proc. Indian Acad. Sci. Math. Sci.* **97** (1987), no. 1-3, 251–262 (1988).
- [14] R. Phillips and P. Sarnak, *The spectrum of Fermat curves*, *Geom. Funct. Anal.* **1** (1991), no. 1, 80–146.
- [15] A. E. Posingies, *Belyi pairs and scattering constants*, Ph.D. thesis, Humboldt-University Berlin, Berlin (2010).
- [16] D. E. Rohrlich, *Modular functions and the Fermat's curves*, ProQuest LLC, Ann Arbor, MI (1976). Thesis (Ph.D.)–Yale University.
- [17] ———, *Points at infinity on the Fermat curves*, *Invent. Math.* **39** (1977), no. 2, 95–127.
- [18] J. Vélou, *Le groupe cuspidal des courbes de Fermat*, in *Séminaire Delange-Pisot-Poitou*, 20e année: 1978/1979. *Théorie des nombres*, Fasc. 2 (French), Exp. No. 28, 11, Secrétariat Math., Paris (1980).

INDIAN INSTITUTE OF SCIENCE, EDUCATION AND RESEARCH, PUNE, INDIA

UNIVERSITÉ PARIS CITÉ AND SORBONNE UNIVERSITÉ, CNRS, IMJ-PRG, F-75013 PARIS, FRANCE.