Journal of Number Theory 188 (2018) 71–87

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Congruence formulas for Legendre modular polynomials

Adel Betina [a], Emmanuel Lecouturier [b,*]

[a] *The University of Sheffield, Hicks building, Western Bank, Sheffield S10 2TN, United Kingdom*
[b] *Université Paris-Diderot, 5 Rue Thomas Mann, 75013 Paris, France*

A R T I C L E   I N F O

Article history:
Received 30 October 2017
Received in revised form 24 January 2018
Accepted 24 January 2018
Available online 20 February 2018
Communicated by F. Pellarin

MSC:
14K22
14K10
11S80

Keywords:
Rigid analytic geometry
Mumford uniformization
Semi-stable curves
Modular curves
Modular polynomials
Supersingular elliptic curves

A B S T R A C T

Let $p \geq 5$ be a prime number. We generalize the results of E. de Shalit [4] about supersingular j-invariants in characteristic p. We consider supersingular elliptic curves with a basis of 2-torsion over $\overline{\mathbf{F}}_p$, or equivalently supersingular Legendre λ-invariants. Let $F_p(X,Y) \in \mathbf{Z}[X,Y]$ be the p-th modular polynomial for λ-invariants. A simple generalization of Kronecker's classical congruence shows that $R(X) := \frac{F_p(X,X^p)}{p}$ is in $\mathbf{Z}[X]$. We give a formula for $R(\lambda)$ if λ is supersingular. This formula is related to the Manin–Drinfeld pairing used in the p-adic uniformization of the modular curve $X(\Gamma_0(p) \cap \Gamma(2))$. This pairing was computed explicitly modulo principal units in a previous work of both authors. Furthermore, if λ is supersingular and is in $\mathbf{F}_p$, then we also express $R(\lambda)$ in terms of a CM lift (which is shown to exist) of the Legendre elliptic curve associated to λ.

* Corresponding author.
E-mail addresses: a.betina@sheffield.ac.uk (A. Betina), emmanuel.lecouturier@imj-prg.fr (E. Lecouturier).

https://doi.org/10.1016/j.jnt.2018.01.006

1. Introduction

Let $p \geq 5$ be a prime number. We are interested in this article in the modular curve $X(\Gamma(2) \cap \Gamma_0(p))$. A plane equation of this curve is given by the classical p-th *modular polynomial à la Legendre*, which we denote by $F_p(X, Y)$. It is shown that it satisfies the same properties as the classical modular polynomials for the j-invariants, namely it is symmetric, has integer coefficients and we have the Kronecker congruence $F_p(X, Y) \equiv (X^p - Y)(X - Y^p)$ modulo p.

This last congruence can be roughly interpreted by saying that the reduction modulo p of $X(\Gamma(2) \cap \Gamma_0(2))$ is a union of two irreducible components isomorphic to $\mathbf{P}^1$. In this work, we show a congruence formula for $F_p(X, X^p)$ modulo p^2, which intuitively gives us information about the reduction of our curve modulo p^2. The tools that we use to study this reduction is the p-adic uniformization (due to Mumford and Manin–Drinfeld). We do a detailed study of some annuli in the supersingular residue disks of the rigid modular curve. This was already used by E. de Shalit in [4] (in the absence of level 2 structure), and we follow his method in our case.

By combining our previous work (*cf.* [1]) on the p-adic uniformization of our modular curve and the present results, we obtain an elementary formula for values taken by $F_p(X, X)$ modulo p^2 (which does not however give us a formula for the polynomial itself). We now give more details about ours results.

Let $\mathfrak{M}_{\Gamma_0(p)\cap\Gamma(2)}$ be the stack over $\mathbf{Z}[1/2]$ whose S-points are the isomorphism classes of generalized elliptic curves E/S, endowed with a locally free subgroup A of rank p such that $A + E[2]$ meets each irreducible component of any geometric fiber of E ($E[2]$ is the subgroup of 2-torsion points of E) and a basis of the 2-torsion (*i.e.* an isomorphism $\alpha_2 : E[2] \simeq (\mathbf{Z}/2\mathbf{Z})^2$). Deligne and Rapoport proved in [3] that $\mathfrak{M}_{\Gamma_0(p)\cap\Gamma(2)}$ is a regular algebraic stack, proper, of pure dimension 2 and flat over $\mathbf{Z}[1/2]$.

Let $M_{\Gamma_0(p)\cap\Gamma(2)}$ be the coarse space of the algebraic stack $\mathfrak{M}_{\Gamma_0(p)\cap\Gamma(2)}$ over $\mathbf{Z}[1/2]$. Deligne–Rapoport proved that $M_{\Gamma_0(p)\cap\Gamma(2)}$ is a normal scheme and proper flat of relative dimension one over $\mathbf{Z}[1/2]$. Moreover, Deligne–Rapoport proved that $M_{\Gamma_0(p)\cap\Gamma(2)}$ is smooth over $\mathbf{Z}[1/2]$ outside the points associated to supersingular elliptic curves in characteristic p and that $M_{\Gamma_0(p)\cap\Gamma(2)}$ is a regular scheme with semi-stable reduction (*cf.* [3, VI.6.9] and [1, Proposition 2.1] for more details).

Let K be the unique quadratic unramified extension of $\mathbf{Q}_p$, $\mathcal{O}_K$ be the ring of integers of K and k be the residual field. Let $\mathfrak{X}$ be the base change $M_{\Gamma_0(p)\cap\Gamma(2)} \otimes \mathcal{O}_K$; it is the coarse moduli space of the base change $\mathfrak{M}_{\Gamma_0(p)\cap\Gamma(2)} \otimes \mathcal{O}_K$ (because the formation of coarse moduli space commutes with flat base change).

Let $M_{\Gamma(2)}$ be the model over $\mathbf{Z}[1/2]$ of the modular curve $X(2)$ introduced by Igusa [10]. The special fiber of the scheme $\mathfrak{X}$ is the union of two copies of $M_{\Gamma(2)} \otimes k$ meeting transversally at the supersingular points, and such that a supersingular point x of the first copy is identified with the point $x^p = \mathrm{Frob}_p(x)$ of the second copy (the supersingular points of the special fiber of $\mathfrak{X}$ are k-rational). Moreover, we have $M_{\Gamma(2)} \otimes k \simeq \mathbf{P}^1_k$ (*cf.* [1, Proposition 2.1]).

The cusps of $M_{\Gamma_0(p)\cap\Gamma(2)}$ correspond to Néron 2-gons or $2p$-gons and are given by sections $\operatorname{Spec}\mathbf{Z}[1/2] \to \mathfrak{M}_{\Gamma_0(p)\cap\Gamma(2)}$ composed with the coarse moduli map $\mathfrak{M}_{\Gamma_0(p)\cap\Gamma(2)} \to M_{\Gamma_0(p)\cap\Gamma(2)}$.

Mumford's theorem [14] implies that the rigid space $\mathfrak{X}^{rig}$ attached to $\mathfrak{X}$ is the quotient of a p-adic half plane $\mathfrak{H}_\Gamma = \mathbf{P}^1_K - \mathcal{L}$ by a Schottky group Γ, where $\mathcal{L}$ is the set of the limits points of Γ. Manin and Drinfeld constructed a pairing $\Phi : \Gamma^{ab} \times \Gamma^{ab} \to K^\times$ in [13] and explained how this pairing gives a p-adic uniformization of the Jacobian of $\mathfrak{X}_K$.

Let Δ be the dual graph of the special fiber of $\mathfrak{X}$. Mumford's construction shows that Γ is isomorphic to the fundamental group $\pi_1(\Delta)$. The abelianization of Γ is isomorphic to the augmentation subgroup of the free $\mathbf{Z}$-module with basis the isomorphism classes of supersingular elliptic curves over $\overline{\mathbf{F}}_p$. Let $S := \{e_i\}$ be the set of supersingular points of $\mathfrak{X}_k$. We proved in [1], using the ideas of [5], that the pairing Φ can be expressed, modulo the principal units, in terms of the modular invariant λ as follow.

i. The Manin–Drinfeld pairing $\Phi : \Gamma^{ab} \times \Gamma^{ab} \to K^\times$ takes values in $\mathbf{Q}_p^\times$.
ii. Let $\bar{\Phi}$ be the residual pairing modulo the principal units $U_1(\mathbf{Q}_p)$ of $\mathbf{Q}_p$. Then, after the identification $\Gamma^{ab} \simeq H_1(\Delta, \mathbf{Z}) \simeq \mathbf{Z}[S]^0$, $\bar{\Phi}$ extends to a pairing $\mathbf{Z}[S] \times \mathbf{Z}[S] \to K^\times/U_1(K)$ such that:

$$\bar{\Phi}(e_i, e_j) = \begin{cases} (\lambda(e_i) - \lambda(e_j))^{p+1} & \text{if } i \neq j; \\ \pm p \cdot \prod_{k\neq i}(\lambda(e_i) - \lambda(e_k))^{-(p+1)} & \text{if } i = j, \end{cases}$$

where the sign $\pm$ is $+$ except possibly if $p \equiv 3$ (modulo 4) and $\lambda(e_i) \notin \mathbf{F}_p$.

Remark 1. i) We have also proved an analogue of the above result for the congruence subgroup $\Gamma(3) \cap \Gamma_0(p)$ when $p \equiv 1 \pmod 3$, for a suitable model $\mathfrak{X}$ of the modular curve of level $\Gamma_0(p) \cap \Gamma(3)$ over $\mathbf{Z}_p$.

ii) The above formula was first conjectured by Oesterlé using the modular invariant j instead of the modular invariant λ for the modular curve $X_0(p)$ instead of $\mathfrak{X}$, and E. de Shalit proved this conjecture in [5] (up to a sign if $p \equiv 3 \pmod 4$).

We recall that the Lambda modular invariant $\lambda : M_{\Gamma(2)} \otimes \mathbf{Q} \to \mathbf{P}^1_{\mathbf{Q}}$ is an isomorphism of curves. Let $F_p(X, Y) \in \mathbf{C}[X, Y]$ be the unique polynomial such that for all τ in the complex upper-half plane, we have:

$$F_p(\lambda, X) = (X - \lambda(p\tau)) \cdot \prod_{0\leq a\leq p-1} (X - \lambda((\tau + a)/p)).$$

Note that this polynomial has much smaller coefficients than the corresponding polynomial for the j-invariants. For example, we have:

$$\begin{aligned} F_3(X, Y) = {} & X^4 + X^3(-256Y^3 + 384Y^2 - 132Y) + X^2(384Y^3 - 762Y^2 + 384Y) \\ & + X(-132Y^3 + 384Y^2 - 256Y) + Y^4 \end{aligned}$$

and

$$\begin{aligned}F_5(X,Y) = {} & X^6+Y^6-65536\cdot X^5Y^5+163840\cdot X^5Y^4+163840\cdot X^4Y^5\\ & -138240\cdot X^5Y^3-133120\cdot X^4Y^4-138240\cdot X^3Y^5+43520\cdot X^5\cdot Y^2\\ & -207360\cdot X^4Y^3-207360\cdot X^3Y^4+43520\cdot X^2Y^5-3590\cdot X^5Y\\ & +133135\cdot X^4Y^2+691180\cdot X^3Y^3+133135\cdot X^2Y^4-3590\cdot XY^5\\ & +43520\cdot X^4Y-207360\cdot X^3Y^2-207360\cdot X^2Y^3+43520\cdot XY^4\\ & -138240\cdot X^3Y-133120\cdot X^2Y^2-138240\cdot X\cdot Y^3\\ & +163840\cdot X^2Y+163840\cdot XY^2-65536\cdot XY\end{aligned}$$

while the corresponding polynomials for j-invariant involve much larger coefficients (compare with [16, p. 193]).

This agrees with the principle that adding a $\Gamma(2)$ structure simplifies a lot the computations. Another instance of this principle was applied in a paper of the second author about the Eisenstein ideal and the supersingular module (*cf.* [12]). Also, in the case of λ-invariants, there are no complications due to the elliptic points, so the formula are smoother. This principle is one of the motivations we had for generalizing E. de Shalit's results to our case.

In this article, we prove that the affine scheme $\mathrm{Spec}\,\mathbf{Q}[X,Y]/(F_p(X,Y))$ is a plane model of $M_{\Gamma_0(p)\cap\Gamma(2)}$ over $\mathbf{Q}$ (*i.e.* both curves are birational), and that the polynomial $F_p(X,Y)$ satisfies the same basic properties as Kronecker's p-th modular polynomial for the modular curve $X_0(p)$. We derive another formula for the diagonal values of $\bar{\Phi}$, related to the polynomial F_p as follows.

Theorem 1.1.

i. *We have* $F_p(\lambda,X)\in\mathbf{Z}[\lambda,X]$ *and* F_p *gives a planar model the modular curve* $M_{\Gamma_0(p)\cap\Gamma(2)}\otimes\mathbf{Q}$.
ii. *For any lift* β_i *of* $\lambda(e_i)$ *in* K*, we have*

$$\bar{\Phi}(e_i,e_i)\equiv F_p(\beta_i,\beta_i^p)\ (\textit{modulo}\ U_1(K)).$$

iii. *Assume that* $\lambda(e_i)\in\mathbf{F}_p$*. Then* $p\equiv 3$ *(modulo 4). Let* E_i *be a lift of* e_i *to a Legendre elliptic curve over* $\mathbf{Q}_p(\sqrt{-p})$ *with complex multiplication by the maximal order of* $\mathbf{Q}_p(\sqrt{-p})$*. Then*

$$\bar{\Phi}(e_i,e_i)\equiv(\lambda(E_i)-\lambda(E_i)^p)^2\ (\textit{modulo}\ U_1(\overline{\mathbf{Q}}_p)).$$

Our approach is based on the techniques of p-adic uniformization of [5] and [4], on a detailed analysis of the supersingular annuli in $\mathfrak{X}^{an}$ and on the action of the Atkin–Lehner involution $w_p : \mathfrak{X} \simeq \mathfrak{X}$. The key point is to relate the diagonal elements of the extended period matrix $\bar{\Phi}$ to the polynomial $F_p(X,Y)$.

Corollary 1.2. *Let $R(X) = F_p(X, X^p)/p \in \mathbf{Z}[X]$, and $\bar{R}(X) \in \mathbf{F}_p$ be the reduction of $R(X)$ mod p. Let $\lambda(e_i) \in \mathbf{F}_{p^2}$ be the λ-invariant of a supersingular elliptic curve e_i. Then, we have:*

$$\bar{R}(\lambda(e_i)) = \pm(-1)^{\frac{p-1}{2}} \prod_{k \neq i} (\lambda(e_i) - \lambda(e_k))^{-(p+1)}$$

where the $\pm$ sign is $+$ except possibly if $p \equiv 3$ (modulo 4) and $\lambda(e_i) \notin \mathbf{F}_p$. On the other hand, if $\lambda \in \mathbf{F}_{p^2}$ is not a supersingular invariant, then $\bar{R}(\lambda) = 0$.

Proof. The first assertion follows by comparing [1, Theorem 1] and Theorem 1.1.

Let $\lambda \in \mathbf{F}_{p^2}$ such that λ is not supersingular. Let $\tilde{X}$ be the scheme over $\mathcal{O}_K$ defined by $F_p(X,Y) = 0$. Let $\beta \in \mathcal{O}_K$ be a lift of λ (this lift exists since $M_{\Gamma(2)}$ is proper over $\mathbf{Z}[1/2]$). The closed point x of $\tilde{X}$ corresponding to the maximal ideal $\mathcal{M} = (p, X-\beta, Y-\beta^p) \subset \mathcal{O}_K[X,Y]$ is regular on $\tilde{X}$ if and only if $F_p(X,Y)$ does not belong to $\mathcal{M}^2$. Using Taylor expansion of F_p at (β, β^p), we get that $F_p(X,Y) = p.R(\beta) + F_X(\beta,\beta^p)(X-\beta) + F_Y(\beta,\beta^p)(Y-\beta^p)$ mod $\mathcal{M}^2$. But it is clear from Kronecker's congruence that $F_X(\beta,\beta^p)$ and $F_Y(\beta,\beta^p)$ are divisible by p. Thus, our regularity conditions is equivalent to the fact that $\bar{R}(\lambda) \neq 0$.

Corollary 2.3 shows that (λ, λ^p) is a singular point of the special fiber of $\tilde{X}$. But the elliptic curve E corresponding to x has ordinary reduction, so the corresponding point on the special fiber of $\mathfrak{X}$ is non-singular. Since the minimal regular model of the normalization of $\tilde{X}$ is unique, it is $\mathfrak{X}$. Since any local regular ring is normal (since it is factorial), the point x is not regular in $\tilde{X}$ and $\bar{R}(\lambda(E)) = 0$. □

Notation.

i. For any algebraic extension k of the field $\mathbf{Z}/p\mathbf{Z}$, we denote by $\bar{k}$ the separable closure of k.

ii. For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbf{Z})$, we denote by $\mathfrak{M}_\Gamma$ the stack over $\mathbf{Z}$ whose S-points classify generalized elliptic curves over S with a Γ-level structure.

iii. For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbf{Z})$ and any $c \in \mathbf{P}^1(\mathbf{Q})$, we denote by $[c]_\Gamma$ the cusp of $\Gamma\backslash(\mathfrak{H} \cup \mathbf{P}^1(\mathbf{Q}))$ corresponding to the class of c, where $\mathfrak{H}$ is the (complex) upper-half plane.

iv. For two congruence subgroups Γ and L, we denote by $\mathfrak{m}_{\Gamma\cap L}$ the fiber product of algebraic stacks $\mathfrak{M}_\Gamma \times_{\mathfrak{M}} \mathfrak{M}_L$, where $\mathfrak{M}$ is the stack over $\mathbf{Z}$ whose S-points classify generalized elliptic curves over the scheme S.

v. For any algebraic stack $\mathfrak{M}_\Gamma$ over a noetherian scheme S, we denote by M_Γ the coarse moduli space attached to $\mathfrak{M}_\Gamma$ (M_Γ is an algebraic space).

vi. For any proper and flat scheme $\mathfrak{X}$ over $\mathcal{O}_K$, we denote by $\mathfrak{X}_K^{an}$ the rigid analytic space given by the generic fiber of the completion of $\mathfrak{X}$ along its special fiber (in particular, we have $\mathfrak{X}_K(\bar{K}) \simeq \mathfrak{X}_K^{an}(\bar{K})$).
vii. Let $| \,.\, |_p$ be the normalized p-adic valuation on $\bar{\mathbf{Q}}_p$, then for non-zero x, y we write $x \sim y$ if and only if $|xy^{-1} - 1|_p < 1$.

Acknowledgments. The first named author's research is supported by a EPSRC Grant EP/R006563/1 and the first author has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 682152). Both authors would like to thank the Université Paris 7, where most of our discussions took place, for its hospitality. The second named author (E.L.) has received funding from Université Paris 7 for his PhD thesis and would like to thank this institution.

2. Basic properties of coarse moduli spaces of moduli stacks of generalized elliptic curves with $\Gamma(2)$-level structure

Let $\mathfrak{M}_{\Gamma(2)}$ be the stack over $\mathbf{Z}[1/2]$ parametrizing generalized elliptic curves with $\Gamma(2)$-level structure (see [3, IV. Definition 2.4]). Deligne–Rapoport proved in [3, Théorème 2.7] that $\mathfrak{M}_{\Gamma(2)}$ is an algebraic stack proper smooth of relative dimension one over $\mathbf{Z}[1/2]$. Let $M_{\Gamma(2)}$ be the coarse algebraic space associated to $\mathfrak{M}_{\Gamma(2)}$. Proposition [3, VI.6.7] implies that $M_{\Gamma(2)}$ is smooth over $\mathbf{Z}[1/2]$; and hence $M_{\Gamma(2)} \otimes \mathcal{O}_K$ is a scheme since it is a regular algebraic space of relative dimension one over $\mathcal{O}_K$.

By the universal property of the coarse moduli space attached to an algebraic stack over a noetherian scheme, we have a coarse moduli map

$$g : \mathfrak{M}_{\Gamma(2)} \to M_{\Gamma(2)}$$

such that for any field L of characteristic different from two, g induces a bijection

$$\mathfrak{M}_{\Gamma(2)}(L) \simeq M_{\Gamma(2)}(L).$$

For any elliptic curve E with a basis of its 2-torsion over a field L of characteristic different from 2, E is isomorphic to a unique Legendre curve E_λ: $Y^2 = X(X-1)(X-\lambda)$ with basis of 2-torsion the points $(0,0)$ and $(0,1)$. Hence, we have a bijection

$$M_{\Gamma(2)}(L) \to \mathbf{P}^1_{\mathbf{Z}[1/2]}(L),$$

associating to an elliptic curve E its lambda invariant λ.

Proposition 2.1. *There exists an isomorphism $\lambda : M_{\Gamma(2)} \to \mathbf{P}^1_{\mathbf{Z}[1/2]}$ inducing the previous map on L-points for every field L of characteristic different from* 2.

Proof. We use similar arguments to those given in the proof of [3, VI. Théorème 1.1]. Let $c = [1]_{\Gamma(2)}$ be the cusp at which the complex modular invariant λ has a pole. Since a cusp of $\mathfrak{M}_{\Gamma(2)}$ is given by a section $\operatorname{Spec}\mathbf{Z}[1/2] \to \mathfrak{M}_{\Gamma(2)}$, then by composing with the coarse moduli map g, a cusp of $M_{\Gamma(2)}$ is also given by a section $\operatorname{Spec}\mathbf{Z}[1/2] \to M_{\Gamma(2)}$. Since $\mathfrak{M}_{\Gamma(2)}$ is proper, there exists a section $c : \operatorname{Spec}\mathbf{Z}[1/2] \to M_{\Gamma(2)}$ corresponding to $[1]_{\Gamma(2)}$ after base change to $\mathbf{C}$.

Now, we obtain a section $c : \operatorname{Spec}\mathbf{Z}[1/2] \to M_{\Gamma(2)}$ giving rise to a Cartier divisor D of $\mathfrak{M}_{\Gamma(2)}$. By [3, V. Proposition 5.5], the geometric fibers of $M_{\Gamma(2)}$ are absolutely irreducible. The genus is constant on the geometric fibers of $M_{\Gamma(2)}$ and equals the genus of the complex modular curves $M_{\Gamma(2)}(\mathbf{C})$, which is zero (see [7, Proposition 7.9]). Hence, by applying Riemann–Roch to each geometric fiber of $M_{\Gamma(2)}$ (see [9, III. Corollary 9.4]) we obtain:

$$\mathrm{H}^1(M_{\Gamma(2)}, \mathcal{O}_{M_{\Gamma(2)}}(D)) = 0.$$

Thus, $\mathrm{H}^0(M_{\Gamma(2)}, \mathcal{O}_{M_{\Gamma(2)}}(D))$ has rank two over $\mathbf{Z}[1/2]$ and is generated by $\{1, \lambda\}$, so we have a morphism $\lambda : M_{\Gamma(2)} \to \mathbf{P}^1_{\mathbf{Z}[1/2]}$ (which we normalize so that it coincides with the Legendre lambda-invariant on L-points as above). On each geometric fiber $\mathfrak{M}_{\Gamma(2)} \otimes \bar{k}$ away from characteristic 2, we see that the degree of the divisor $D_{\bar{k}}$ corresponding to D on $\mathfrak{M}_{\Gamma(2)} \otimes \bar{k}$ is 1, hence $D_{\bar{k}}$ is very ample (see [9, IV. corollary 3.2]). Thus, D is relatively very ample over $\mathbf{Z}[1/2]$ (see [8, 9.6.5]) and λ is an isomorphism. $\square$

Let $M'_{\Gamma(2)}$ be the affine open of $M_{\Gamma(2)}$ corresponding to $\mathbf{A}^1_{\mathbf{Z}[1/2]} \subset \mathbf{P}^1_{\mathbf{Z}[1/2]}$, $\varphi : M_{\Gamma_0(p)\cap\Gamma(2)} \to M_{\Gamma(2)}$ be the map forgetting the $\Gamma_0(p)$-level structure (*cf.* [3, IV Proposition 3.19]), and $M'_{\Gamma_0(p)\cap\Gamma(2)}$ be the inverse image of $M'_{\Gamma(2)}$ by φ, which is an affine scheme since φ is a finite morphism. Denote by w_p the Atkin–Lehner involution on $M_{\Gamma_0(p)\cap\Gamma(2)}$; it preserves $M'_{\Gamma_0(p)\cap\Gamma(2)}$ by [1, Lemma 7.4]. Thus, we obtain finite maps

$$(\varphi, \varphi \circ w_p) : M_{\Gamma_0(p)\cap\Gamma(2)} \to M_{\Gamma(2)} \times M_{\Gamma(2)}$$

and

$$(\varphi, \varphi \circ w_p) : M'_{\Gamma_0(p)\cap\Gamma(2)} \to M'_{\Gamma(2)} \times M'_{\Gamma(2)}.$$

Let R such that $M'_{\Gamma_0(p)\cap\Gamma(2)} = \operatorname{Spec} R$ and $\operatorname{Spec}\mathbf{Z}[1/2][\lambda, \lambda'] = M_{\Gamma(2)} \times M_{\Gamma(2)}$. The image of the finite (hence proper) morphism $(\varphi, \varphi \circ w_p) : M'_{\Gamma_0(p)\cap\Gamma(2)} \to M'_{\Gamma(2)} \times M'_{\Gamma(2)}$ is a reduced closed subset $V(I)$, where I is an ideal of $\operatorname{Spec}\mathbf{Z}[1/2][\lambda, \lambda']$ and this ideal equals the kernel of the map $\mathbf{Z}[1/2][\lambda, \lambda'] \to R$. Thus, we have a finite injective morphism $\mathbf{Z}[1/2][\lambda, \lambda']/I \hookrightarrow R$. Using the going up theorem, we get a surjection $\operatorname{Spec} R \to \operatorname{Spec}\mathbf{Z}[1/2][\lambda, \lambda']/I$ and the fact that the ring $\mathbf{Z}[1/2][\lambda, \lambda']/I$ is equidimensional of dimension two. Hence, the ideal I has codimension one.

Moreover, the affine scheme $M'_{\Gamma(2)} \times M'_{\Gamma(2)}$ is isomorphic to $\mathbf{A}^2_{\mathbf{Z}[1/2]}$, hence it is a factorial scheme. The ideal I is generated by an element $F(X, Y) \in \mathbf{Z}[1/2][X, Y]$ since the Picard group of a factorial ring is trivial. Thus, $V(I)$ is a principal Weil divisor.

Since the degree of the two projections $\varphi, \varphi \circ w_p : M_{\Gamma_0(p)\cap\Gamma(2)} \to M_{\Gamma(2)}$ is equal to $p+1 = \#\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ and $M_{\Gamma_0(p)\cap\Gamma(2)} \to M_{\Gamma(2)} \times M_{\Gamma(2)}$ is injective outside CM-points and the special fiber at p, the degree of F as a polynomial in X equals to the degree of F as a polynomial in Y, equals to $p+1$. Thus, we have $F(X,Y) = uX^{p+1} + vY^{p+1} + \sum_{i+j\leq p+1\ ,i<p+1,j<p+1} a_{i,j}X^iY^j$, where u, v are invertible in $\mathbf{Z}[1/2]$. Moreover, since w_p is an involution, we have $F(X,Y) = \alpha \cdot F(Y,X)$ where α is invertible in $\mathbf{Z}[1/2]$. We must have $\alpha = 1$ since else, we have $F(X,X) = 0$. This is impossible since this implies that every elliptic curve over $\mathbf{C}$ has CM by some quadratic order. Thus we can assume that $F \in \mathbf{Z}[1/2][X,Y]$ is monic in X and Y. It is then clear that $F = F_p$ (the p-th modular polynomial). Moreover, the coefficients of F_p are in some cyclotomic ring and thus are in $\mathbf{Z}$. More precisely, the Fourier coefficients of $\lambda(p\tau)$ and $\lambda((\tau+a)/p)$ are in $\mathbf{Z}[\zeta_p]$. Consequently, any coefficient of $F_p(X,\lambda)$ (as a polynomial in X) is a polynomial in λ with coefficients in $\mathbf{Z}[\zeta_p]$ (*cf.* [11, Chapter 5, Theorem 2]).

We have thus proved the first part of the following result.

Proposition 2.2. *We have $F_p \in \mathbf{Z}[X,Y]$ and $F_p(X,Y) = F_p(Y,X)$. The curve $M_{\Gamma_0(p)\cap\Gamma(2)} \otimes \mathbf{Q}$ is birational to* $\operatorname{Spec}\mathbf{Q}[X,Y]/(F_p(X,Y))$.

Proof. Since $M'_{\Gamma_0(p)\cap\Gamma(2)}$ is irreducible, $\operatorname{Spec}\mathbf{Z}[1/2][X,Y]/(F_p(X,Y))$ is irreducible (we have $\mathbf{Z}[1/2][X,Y]/(F_p(X,Y)) \subset R$ where $\operatorname{Spec}(R) = M'_{\Gamma_0(p)\cap\Gamma(2)}$ and R is an integral domain). Let $K(M_{\Gamma_0(p)\cap\Gamma(2)})$ be the field of rational functions of $M_{\Gamma_0(p)\cap\Gamma(2)}$ and $\mathbf{Q}(X)[Y]/(F_p(X,Y))$ be the function field of $\operatorname{Spec}\mathbf{Z}[1/2][X,Y]/(F_p(X,Y))$.

We have inclusions

$$\mathbf{Q}(\lambda) \subset \mathbf{Q}(X)[Y]/(F_p(X,Y)) \subset K(M_{\Gamma_0(p)\cap\Gamma(2)})$$

and by comparing degrees, we have $\mathbf{Q}(X)[Y]/(F_p(X,Y)) = K(M_{\Gamma_0(p)\cap\Gamma(2)})$. Thus, the curve $M_{\Gamma_0(p)\cap\Gamma(2)} \otimes \mathbf{Q}$ is birational to $\operatorname{Spec}\mathbf{Q}[X,Y]/(F_p(X,Y))$, since they have the same field of rational functions and $\mathbf{Q}(X)[Y]/(F_p(X,Y)) \cap \bar{\mathbf{Q}} = \mathbf{Q}$ (the cusps of $M_{\Gamma_0(p)\cap\Gamma(2)} \otimes \mathbf{Q}$ are $\mathbf{Q}$-rational). □

If E is an elliptic curve over $\overline{\mathbf{F}}_p$ and $E \to E^{(p)}$ is the relative Frobenius, then E is ordinary if and only if the kernel of Frobenius is isomorphic to the finite flat group scheme μ_p. The Atkin–Lehner involution w_p sends the multiplicative component of the special fiber of $M_{\Gamma_0(p)\cap\Gamma(2)}$ to the étale component via $\lambda \mapsto \lambda^p$.

Corollary 2.3. *The reduction of $F_p(X,Y)$ modulo p is $(X^p - Y)(X - Y^p)$.*

Proof. Let x be an element of $\mathfrak{X}(\bar{k})$ corresponding to (E, α_2, H) such that E is not supersingular. We have two cases:

If H is a multiplicative subgroup of order p, then from the discussion above, it is clear that $\lambda(x)^p = \lambda(w_p(x))$.

Otherwise, H is étale and $\lambda(x) = \lambda(w_p(w_p(x))) = \lambda(w_p(x))^p$.

Moreover, since the open set given by the complementary of supersingular elliptic curves is dense in the special fiber of $\mathfrak{X}$, the zeros of the polynomial $(X^p - Y)(Y^p - X) \in \overline{\mathbf{F}}_p[X,Y]$ are zeros of F_p modulo p. Furthermore, $\mathbf{Z}[1/2][X,Y]/(F_p(X,Y))$ is reduced ($\operatorname{Spec} \mathbf{Z}[1/2][X,Y]/(F_p(X,Y))$ is the scheme theoretic image of $(c, c \circ w_p)$). Thus, in the ring $\mathbf{Z}[1/2][X,Y]/(F_p(X,Y))$, we have $(X^p - Y)(Y^p - X) = 0$ and by comparing the degree we have the equality. □

Remark 2. This corollary could be proved in a more down-to-earth way, like in [11].

3. *p*-adic uniformization and the reduction map

Let $\mathfrak{X}$ be the modular curve $M_{\Gamma_0(p)\cap\Gamma(2)} \otimes \mathcal{O}_K$. Since the singularities of the special fiber of $\mathfrak{X}$ are k-points where $k = \mathbf{F}_{p^2}$, Mumford's Theorem [14] shows the existence of a free discrete subgroup $\Gamma \subset \mathrm{PGL}_2(K)$ (*i.e.* a Schottky group) and of a $\mathrm{Gal}(\bar{K}/K)$-equivariant morphism of rigid spaces:

$$\tau : \mathfrak{H}_\Gamma \to \mathfrak{X}_K^{an}$$

inducing an isomorphism $\mathfrak{X}_K^{an} \simeq \mathfrak{H}_\Gamma/\Gamma$, where $\mathfrak{H}_\Gamma = \mathbf{P}_K^1 - \mathcal{L}$ and $\mathcal{L}$ is the set of limit points of Γ. Note that $\mathfrak{H}_\Gamma$ is an admissible open of the rigid projective line $\mathbf{P}_K^1$.

Let $\mathcal{T}_\Gamma$ be the subtree of the Bruhat–Tits tree for $\mathrm{PGL}_2(K)$ generated by the axes whose ends correspond to the limit points of Γ. Mumford constructed in [14] a continuous map $\rho : \mathfrak{H}_\Gamma \to \mathcal{T}_\Gamma$ called the reduction map.

The special fiber of $\mathfrak{X}$ has two components, and each component has 3 cusps. One of these components, which we call the *étale* component, classifies elliptic curves or $2p$-sided Néron polygons over $\bar{k}$ with an étale subgroup of order p and a basis of the 2-torsion. The other component, which we call the *multiplicative* component, classifies elliptic curves or 2-sided Néron polygons over $\bar{k}$ with a multiplicative subgroup of order p and a basis of the 2-torsion. The involution w_p sends a $2p$-gon to a 2-gon. Let c and $c' = w_p(c)$ be two cusps of $M_{\Gamma_0(p)\cap\Gamma(2)}(\mathbf{C})$ such that c is above $c_{\Gamma(2)}$. By [1, Proposition 7.4], c' is also above $c_{\Gamma(2)}$ (ξ_c corresponds to a $2p$-gon and $\xi_{c'} = w_p(\xi_c)$ corresponds to a 2-gon).

The dual graph Δ of the special fiber of $\mathfrak{X}$ has two vertices $v_{c'}$ and v_c indexed respectively by the cusps $\xi_{c'}$ and ξ_c. There are $g+1$ edges e_i ($i \in \{0, ..., g\}$) corresponding to supersingular elliptic curves with a $\Gamma(2)$-structure, where g is the genus of $M_{\Gamma_0(p)\cap\Gamma(2)}(\mathbf{C})$. We orient these edges so that they point out of $v_{c'}$.

The Atkin–Lehner involution w_p exchanges the two vertices $v_{c'}$ and v_c and also acts on edges (reversing the orientation). More precisely, if E_i is a supersingular elliptic curve with $\Gamma(2)$-structure corresponding to e_i, then $w_p(e_i) = e_j$ where e_j is the isomorphism class of the elliptic curve (with $\Gamma(2)$-structure) associated to $E_i^{(p)} = w_p(E_i)$ (here w_p is the Frobenius). Thanks to Lemma 3.1 below, one can identify the generators $\{\gamma_i\}_{1\leq i\leq g}$ of Γ with $(e_i - e_0)_{1\leq i\leq g}$.

Let $\tilde{v}_c$ and $\tilde{v}_{c'}$ be two neighbor vertices of $\mathcal{T}_\Gamma$ reducing to $v_{c'}$ and v_c respectively, such that the edge linking $\tilde{v}_c$ to $\tilde{v}_{c'}$ reduces to e_0 modulo Γ. For $0 \leq i \leq g$, let $\tilde{e}_i'$ be an edge pointing out of $\tilde{v}_{c'}$ and reducing to e_i modulo Γ. Let $\tilde{e}_i$ be oriented edges of $\mathcal{T}_\Gamma$ lifting e_i and pointing to $\tilde{v}_c$. Note that $\tilde{e}_0 = \tilde{e}'_0$.

Let $A = \rho^{-1}(\tilde{v}_c)$ and $A' = \rho^{-1}(\tilde{v}_{c'})$. Then A (resp. A') is the complement of $g+1$ open disks in $\mathbf{P}^1_K$, hence $\mathbf{P}^1_K - A = \coprod_{0\le i\le g} B_i$ and $\mathbf{P}^1_K - A' = \coprod_{0\le i\le g} C'_i$. We index C'_i and B_i such that $A \subset C'_0$, $A' \subset B_0$, C'_i and B_i are associated to $\tilde{e}'_i$ and $\tilde{e}_i$ respectively.

For all $0 \le i \le g$, $\rho^{-1}(\tilde{e}'_i) = c_i$ is an annulus of C'_i and $C_i = C'_i - \rho^{-1}(\tilde{e}'_i)$ is a closed disk; we also have $\mathbf{P}^1_K - C_0 = B_0$. We have

$$\mathbf{P}^1_K - \rho^{-1}(\bigcup_{0\le i\le g} \tilde{e}_i{}' \cup \tilde{v}_{c'}) = \coprod_{0\le i\le g} C_i \ .$$

Note that $\tilde{v}_c \cup \tilde{v}_{c'} \cup_i \{\tilde{e}'_i\}$ is a fundamental domain of $\mathcal{T}_\Gamma$, so

$$D = \mathbf{P}^1_K - \coprod_{1\le i\le g} B_i \cup \coprod_{1\le i\le g} C_i$$

is a fundamental domain of $\mathfrak{H}_\Gamma$.

Lemma 3.1. *[1, Lemma 3.3] We can choose* Γ *such that there is a Schottky basis* $\alpha_1, ..., \alpha_g$ *of* Γ*, and a fundamental domain* D *satisfying:*

i. *B_i is the open residue disk in the closed unit disk of $\mathbf{P}^1_K$ which reduces to $\lambda(e_i)^p$, $\forall 0 \le i \le g$.*
ii. *For $1 \le i \le g$, α_i corresponds, under the identification $\Gamma^{ab} = \mathbf{Z}[S]^0$, to $e_i - e_0$.*
iii. *α_i sends $\mathbf{P}^1_K - B_i$ bijectively to C_i and α_i^{-1} sends $\mathbf{P}^1_K - C_i$ bijectively to B_i.*
iv. *The annulus c_i is isomorphic, as a rigid analytic space, to $\{z, |p| < |z| < 1\}$.*

For $a, b \in \mathfrak{H}_\Gamma$, define the meromorphic function $\theta(a, b; z) = \theta((a) - (b); z)$ $(z \in \mathfrak{H}_\Gamma)$ by the convergent product

$$\theta(a, b; z) = \prod_{\gamma\in\Gamma} \frac{z - \gamma a}{z - \gamma b} \ .$$

See [13] for the basic properties of these theta functions.

For all $a, b \in \mathfrak{H}_\Gamma$, the theta series $\theta(a, b; .)$ converges and defines a rigid meromorphic function on $\mathfrak{H}_\Gamma$ (which is modified by a constant if we conjugate Γ). We extend θ to degree zero divisors D of $\mathfrak{H}_\Gamma$. The series $\theta(D; .)$ is entire if and only if $\tau_*(D) = 0$, where we recall that $\tau : \mathfrak{H}_\Gamma \to \mathfrak{X}^{an}_K$ is the uniformization.

The proposition below follows from [13] (see also [5]).

Proposition 3.2. *[13]*

i. *$\theta(a, b; z) = c(a, b, \alpha)\theta(a, b; \alpha z)$, where $\alpha \in \Gamma$ and $c(a, b, \alpha\beta) = c(a, b, \alpha)c(a, b, \beta)$.*
ii. *The function $u_\alpha(z) = \theta(a, \alpha a; z)$ does not depend on a, and $u_{\alpha\beta} = u_\alpha u_\beta$.*

iii. $c(a,b,\alpha) = u_\alpha(a)/u_\alpha(b)$.
iv. $\theta(a,b;z)/\theta(a,b;z') = \theta(z,z';a)/\theta(z,z';b)$.

We recall that $\Phi : \mathbf{Z}[S]^0 \times \mathbf{Z}[S]^0 \to K^\times$ is defined by:

$$\Phi(\alpha,\beta) = \theta(a,\alpha a;z)/\theta(a,\alpha a;\beta z) = u_\alpha(z)/u_\alpha(\beta z).$$

The results of Mumford [14] imply that we can identify Γ^{ab} with $\mathbf{Z}[S]^0$ and that $\mathcal{T}_\Gamma$ is the universal covering of the graph Δ. Moreover, Manin and Drinfeld proved that $v_K \circ \Phi$ is positive definite (v_K is the p-adic valuation of K). According to [1, Lemma 4.2], the pairing Φ takes values in $\mathbf{Q}_p^\times$.

We recall that we defined in [1] an extension $\Phi : \mathbf{Z}[S] \times \mathbf{Z}[S] \to K^\times$ as follow:

For all $0 \leq i \leq g$, we chose $\xi_c^{(i)}$ (resp. $\xi_{c'}^{(i)}$) in $\mathfrak{H}_\Gamma$ which reduces modulo Γ to the cusp $\xi_c \otimes \mathbf{Q}_p$ (resp. $\xi_{c'} \otimes \mathbf{Q}_p$), and such that $\xi_c^{(i)}$ and $\xi_{c'}^{(i)}$ are separated by an annulus reducing to e_i. Let $\tilde{v}_c^{(i)}$ and $\tilde{v}_{c'}^{(i)}$ be two neighbor vertices of $\mathcal{T}_\Gamma$ above v_c and $v_{c'}$ respectively, separated by an edge reducing to e_i. We fix $\tilde{v}_c^{(0)} = \tilde{v}_c$ and $\tilde{v}_{c'}^{(0)} = \tilde{v}_{c'}$. Thus, we chose $\xi_c^{(i)}$ (resp. $\xi_{c'}^{(i)}$) in $\rho^{-1}(\tilde{v}_c^{(i)})$ (resp. $\rho^{-1}(\tilde{v}_{c'}^{(i)})$). Let for all $0 \leq i \leq g$, $\xi_c^{(i)} = z_0 \in A$. Then $\xi_{c'}^{(i)}$ satisfy

$$\xi_{c'}^{(i)} = \alpha_i^{-1}(\xi_{c'}^{(0)}) \in B_i \ .$$

Therefore, we have $\xi_{c'}^{(0)} \in \rho^{-1}(\tilde{v}_{c'}) = A'$ and $\alpha_i^{-1}(A') \subset \alpha_i^{-1}(\mathbf{P}^1 - C_i') \subset B_i$. We can assume also without losing in generality that $z_0 \neq \infty$.

We defined an extension of Φ to a pairing on $\mathbf{Z}[S]^0 \times \mathbf{Z}[S]$ (and taking values in K) as follows:

Fix $a \in \mathfrak{H}_\Gamma$ (the definition is independent of this choice). For all $\alpha \in \Gamma$, we let:

$$\Phi(\alpha, e_i) = \frac{\theta(a,\alpha(a);\xi_{c'}^{(i)})}{\theta(a,\alpha(a);\xi_c^{(i)})} = \frac{u_\alpha(\xi_{c'}^{(i)})}{u_\alpha(\xi_c^{(i)})} = \frac{u_\alpha(\xi_{c'}^{(i)})}{u_\alpha(z_0)} \tag{1}$$

Let $\lambda' : \mathfrak{X}_K \to \mathbf{P}^1_K$ be $\lambda' = \lambda \circ w_p$. The Atkin–Lehner involution acts on $\Gamma\backslash\mathcal{T}_\Gamma$ and lifts to an orientation reversing involution w_p of $\mathcal{T}_\Gamma$ (by the universal covering property). By [6] ch. VII Sect. 1, there is a unique class in $N(\Gamma)/\Gamma$ (where $N(\Gamma)$ is the normalizer of Γ in $\mathrm{PGL}_2(K)$) inducing w_p on $\mathcal{T}_\Gamma$. We denote by w_p the induced map of $\mathfrak{H}_\Gamma$ (it is only unique modulo Γ).

Let $z \in \mathfrak{H}_\Gamma$ near $\xi_c^{(i)}$ and z' near $\xi_{c'}^{(i)}$ such that $\tau(z) = w_p(\tau(z'))$. Recall that by hypothesis, $\xi_c^{(i)} = z_0$ is independent of i.

For $0 \leq i,j \leq g$, We bilinearly extend Φ to $\mathbf{Z}[S] \times \mathbf{Z}[S]$ in [1] as follow:

$$\Phi(e_i, e_j) = \lim \lambda'(\tau(z))^2 \cdot \frac{\theta(z',z;\xi_{c'}^{(j)})}{\theta(z',z;\xi_c^{(j)})} \tag{2}$$

where z and z' approach $\xi_c^{(i)}$ et $\xi_{c'}^{(i)}$ respectively. Since at $z = z_0$, $\lambda' \circ \tau$ has a simple pole and the numerator and denominator have a simple zero and simple pole respectively, $\Phi(e_i, e_j)$ is finite, and is in $K^\times$ since K is complete (we may choose z and z' in K to compute the limit).

4. Proof of the main theorem

4.1. *Case where $\lambda(e_0) \in \mathbf{F}_p$*

Assume that $\lambda(e_0) \in \mathbf{F}_p$. We can choose a lift of the involution w_p to $\tilde{w}_p$ of $N(\Gamma) \subset \mathrm{PGL}_2(K)$ preserving the edge e_0 and reversing the orientation of this edge. Thus, w_p preserves the annulus $\tilde{e_0}'$, so sends A to A'. Hence, $\tilde{w}_p$ is an involution (we have $\tilde{w}_p^2 \in \Gamma$ and the stabilizer of an edge in Γ is trivial, so $\tilde{w}_p^2 = 1$).

Let $\zeta = w_p(\infty)$ (*i.e.* $w_p(\zeta) = \infty$). Then our choice of the fundamental domain of $\mathfrak{H}_\Gamma$ implies that $B_0 = \{z \in \mathbf{P}^1_K, |z - \zeta|_p < 1\}$, $\mathbf{P}^1_K \backslash C'_0 = B_0 \backslash c_0 = \{z \in \mathbf{P}^1_K, |z - \zeta|_p < |p|_p\}$, and $B_0 \bmod p = \lambda(e_0)$.

Any involution of $\mathbf{P}^1_K$ exchanging 0 and ∞ has the form

$$z \to \frac{\pi}{z},$$

where π is an uniformizer of $\mathcal{O}_K$. Thus, we have:

$$w_p(z) - \zeta = \frac{\pi}{z - \zeta} \tag{3}$$

Lemma 4.1. *We have $\Phi(e_0, e_0) \sim \pi$.*

Proof. Recall the definition:

$$\Phi(e_0, e_0) = \lim \lambda'(\tau(z))^2 \cdot \frac{\theta(z', z; \xi_{c'}^{(0)})}{\theta(z', z; \xi_c^{(0)})}$$

where z approaches $z_0 \in A$ and $z' = w_p(z)$. We now do a similar analysis as in [1, Section 6.1]. By [1, Proposition 6.3],

$$\lim \frac{\lambda'(\tau(z)) \cdot (z_0 - z)}{z_0^2} = 1 \ .$$

Recall also that

$$\frac{\theta(z', z; \xi_{c'}^{(0)})}{\theta(z', z; \xi_c^{(0)})} = \prod_{\gamma \in \Gamma} \frac{(z' - \gamma(\xi_{c'}^{(0)})) \cdot (z - \gamma(z_0))}{(z - \gamma(\xi_{c'}^{(0)})) \cdot (z' - \gamma(z_0))} \ .$$

The only term in this infinite product which is not *a priori* a principal unit is the one corresponding to $\gamma = 1$, which is equivalent modulo principal units to

$$\frac{(z' - \xi_{c'}^{(0)}) \cdot (z - z_0)}{-z_0^2} .$$

Indeed, if $\gamma \neq 1$, γ sends the fundamental domain to some B_i or to some C_i. If it is some B_i, the term is seen to be a principal unit. Else, if it is some C_i, we apply the Atkin–Lehner involution and use the invariance of the cross ratio by the Atkin–Lehner involution. Thus, we have:

$$\Phi(e_0, e_0) \sim \frac{z_0^2}{z_0 - z} \cdot (z' - \xi_{c'}^{(0)}) .$$

To conclude the proof of the Lemma, note that

$$z' - \xi_{c'}^{(0)} = (z' - \zeta) - (\xi_{c'}^{(0)} - \zeta) = \frac{\pi}{z - \zeta} - \frac{\pi}{z_0 - \zeta} \sim \frac{\pi \cdot (z_0 - z)}{z_0^2} . \qquad \square$$

4.1.1. Conclusion of the proof of point (ii) of Theorem 1.1 in the case where $\lambda(e_0) \in \mathbf{F}_p$

To conclude the proof of point (ii) of Theorem 1.1, it remains to show that

$$\pi \sim F_p(\beta_0, \beta_0^p)$$

for any lift β_0 of $\lambda(e_i)$ in K.

The proof is really the same as [4, 3.1–3.3], using our analogous fundamental domain for Γ, and replacing j by λ'. Thus, we shall be really sketchy and refer the reader to de Shalit's paper for details.

We recall that $\mathrm{ord}_p(\pi) = 1$. By slight abuse of notation we shall write λ for $\lambda \circ \varphi$ and λ' for $\lambda \circ \varphi \circ w_p$.

Let $y = z - \zeta$; it identifies the annulus $a = \rho^{-1}(\tilde{e_0})$ with

$$A(p, 1) := \{x \in \mathbf{P}_K^1, |p|_p < |x|_p < 1\} .$$

Consider the map $\Psi : a \to B_0$ defined by

$$\Psi(z) = \lambda' \circ \tau(z) \tag{4}$$

This is a covering of B_0 by a since a is the intersection of our fundamental domain D with B_0 (although it might seem surprising compared to the classical complex situation, such a covering indeed exists).

There exists $\beta_0 \in B_0$, such that

$$\Psi(z) = \beta_0 + \sum_{n \geq 1} a_n y^n + \sum_{n \geq 1} b_n (\pi / y)^n \tag{5}$$

where all the coefficients a_n, b_n are in K (since Ψ is K-rational by Proposition 2.1). Using [1, Lemma 6.2] and similar computations as in [4, p. 143-144], we get:

Lemma 4.2. *We have $a_1 \sim 1$, $b_p \sim 1$ and for $n < p$, $|b_n|_p < |p|_p$.*

For $t \in \mathbf{C}_p^\times$ such that

$$|p|_p < |t|_p < 1,$$

let $a(t, 1)$ be the open annulus where $|t|_p < |y|_p < 1$.

For t close enough to 1 and $y \in a(t, 1)$, we set

$$u = \lambda' - \lambda^p = \Psi(\pi/y) - \Psi(y)^p \ .$$

We have, by definition:

$$F_p(\lambda, \lambda^p + u) = 0 \ .$$

This gives us, using partial derivatives and Corollary 2.3:

$$u \cdot (\lambda^{p^2} - \lambda + u^p) = -pR(\lambda) - p \cdot h(u, \lambda)$$

where $R(X) = \frac{F_p(X, X^p)}{p} \in \mathbf{Z}[X]$ and $h(X, Y) \in \mathbf{Z}[X, Y]$ is some integer coefficients polynomial.

We work modulo the ideal $I(t)$ generated by rigid analytic functions on $a(t, 1)$ which are strictly smaller than $|p|_p$ in absolute value. The term $-pR(\lambda) - p \cdot h(u, \lambda)$ is congruent to $-pR(\lambda)$ modulo $I(t)$. A simple computation using Lemma 4.2 shows that we must have $u \equiv \pi/y$ modulo $I(t)$ and

$$\lambda^{p^2} - \lambda = \Psi(y)^{p^2} - \Psi(y) \equiv -y + O(y^2) \text{ (modulo } p).$$

This shows what we needed to conclude the proof of point (ii) of Theorem 1.1:

$$(\pi/y) \cdot y \sim pR(\lambda) \ .$$

4.1.2. Existence of CM lifts

In this section, we prove part (iii) of Theorem 1.1 in the case $\lambda(e_0) \in \mathbf{F}_p$.

Proposition 4.3. *Let $\lambda \in \mathbf{F}_p$ be a supersingular λ-invariant. Then $p \equiv 3$ (modulo 4) and there exists precisely two λ-invariants in $\mathbf{Q}_p(\sqrt{-p})$ lifting λ, such that the associated Legendre elliptic curve has complex multiplication by $\mathbf{Z}[\frac{1+\sqrt{-p}}{2}]$.*

Furthermore, when $p \equiv 3$ (modulo 4) (and $p \geq 5$ as usual), the number of supersingular λ-invariants in $\mathbf{F}_p$ is $3 \cdot h(-p)$ where $h(-p)$ is the class number of $\mathbf{Q}(\sqrt{-p})$.

Proof. The fact that $p \equiv 3$ (modulo 4) follows from [2, Theorem 1 a]. Let $\mathcal{O} = \mathbf{Z}[\frac{1+\sqrt{-p}}{2}]$ and let F be the fraction field of $\mathcal{O}$. Let $\mathfrak{a}$ an element of the ideal class group of $\mathcal{O}$. We denote by $j(\mathfrak{a})$ the j-invariant of the isomorphism class of the elliptic curve $\mathbf{C}/\mathfrak{a}$. It is classical (*cf.* for instance [15, Theorem 5.6]) that if λ is any λ-invariant above $j(\mathfrak{a})$, then $F(\lambda)$ is an extension of $F(j)$ contained in the ray class field of F of conductor $2 \cdot \mathcal{O}$.

Lemma 4.4. *The ideal above p in $\mathcal{O}$ is totally split in $F(\lambda)$.*

Proof. If $p \equiv -1$ (modulo 8), then 2 splits in F, so $\sqrt{-p} - 1 \in \mathfrak{p}_2$ if $\mathfrak{p}_2$ is any prime ideal of $\mathcal{O}$ above (2). Thus, by class field theory, since $(\sqrt{-p})$ is principal, it splits in the ray class field of conductor $2 \cdot \mathcal{O}$ and we are done.

If $p \equiv 3$ (modulo 8), then 2 is inert in F. The prime ideal above 2 in $\mathcal{O}$ is $\mathfrak{P}_2 = (2, \alpha^2 + \alpha + 1)$ where $\alpha = \frac{1+\sqrt{-p}}{2}$. Since $\alpha^2 = \alpha - \frac{p+1}{4}$, we have $\mathfrak{P}_2 = (2, \frac{3-p}{4} + \sqrt{-p} + 1)$. Thus we have $\sqrt{-p} - 1 \in \mathfrak{P}_2$. As above, class field theory shows that $(\sqrt{-p})$ splits in the ray class field of F of conductor $\mathfrak{P}_2$, which concludes the proof of the lemma. □

Lemma 4.5. *Let $\lambda \in \overline{\mathbf{Z}}_p$ such that the Legendre curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$ has supersingular reduction. Then λ is a root of $F_p(X, X)$ if and only if E_λ has CM by $\mathbf{Z}[\frac{1+\sqrt{-p}}{2}]$. Furthermore in this case λ is a simple root of $F_p(X, X)$.*

Proof. It is clear that if $F_p(\lambda, \lambda) = 0$, the elliptic curve E_λ has CM by a quadratic order $\mathcal{O}$ such that p either splits or ramifies in the fraction field. But p has to ramify since the reduction of E_λ is supersingular (this comes from the standard description of the local Galois representation attached to a supersingular elliptic curve). Furthermore, there is an endomorphism of E whose square is $-p$. Thus, $\sqrt{-p} \in \mathcal{O}$. But in fact we have $\sqrt{-p} \in 1 + 2\mathcal{O}$ since the endomorphism $\sqrt{-p}$ has to preserve the $\Gamma(2)$-structure. Thus we have $\mathcal{O} = \mathbf{Z}[\frac{1+\sqrt{-p}}{2}]$. □

Corollary 2.3 shows that

$$F_p(X, X) \equiv -(X^p - X)^2 \text{ (modulo } p).$$

Thus, any supersingular λ-invariant in $\mathbf{F}_p$ is a double root of $F_p(X, X)$. Using the previous lemma, we get:

$$\prod_{\lambda \text{ supersingular in } \mathbf{F}_p} (X - \lambda)^2 \equiv \prod_{[\mathfrak{a}] \in Cl(\mathbf{Z}[\frac{1+\sqrt{-p}}{2}]),\ \lambda \text{ such that } j(\lambda) = j(\mathfrak{a})} (X - \lambda)\ .$$

This shows that for any supersingular λ-invariant in $\mathbf{F}_p$, λ has two CM lifts in characteristic 0 which have CM by $\mathbf{Z}[\frac{1+\sqrt{-p}}{2}]$, and by Lemma 4.4, these lifts can be seen as living in $\mathbf{Q}_p(\sqrt{-p})$. This formula also shows the last assertion of the Proposition on the number of supersingular λ-invariants in $\mathbf{F}_p$ (there are 6 λ-invariants above each j-invariant since $j(\mathfrak{a}) \neq 0, 1728$ because $p \geq 5$). □

We now finish the proof of point (*iii*) of Theorem 1.1. This is done in a similar way as [4, p. 146]. Let λ_1 and λ_2 be the two CM values of lambda invariants in $\mathbf{Q}_p(\sqrt{-p})$ which lift $\lambda(e_i)$ (which exist by Proposition 4.3). It is clear that λ_1 and λ_2 are not in $\mathbf{Q}_p$, so they must be conjugate. Write $\lambda_1 = a + b\sqrt{-p}$ and $\lambda_2 = a - b\sqrt{-p}$ for some $a, b \in \mathbf{Z}_p$. By point (ii) of 1.1, it suffices to prove:

$$F_p(\lambda_1, \lambda_1^p) \equiv (\lambda_1 - \lambda_1^p)^2 \text{ (modulo } p\sqrt{-p}).$$

We know that $F_p(\lambda_1, \lambda_1) = 0$. Therefore, we have:

$$0 = F_p(\lambda_1, \lambda_1) = F_p(\lambda_1, \lambda_1^p + (\lambda_1 - \lambda_1^p)) \equiv F_p(\lambda_1, \lambda_1^p) + (\lambda_1 - \lambda_1^p) \cdot (\lambda_1^{p^2} - \lambda_1) \text{ (modulo } p\sqrt{-p})$$

where the last congruence follows from Corollary 2.3 (which gives $\partial_Y F_p(X, Y) \equiv -(X - Y^p)$ (modulo p)). Since $\lambda_1^{p^2} \equiv \lambda_1^p \equiv a$ (modulo p) and $\lambda_1 \equiv \lambda_1^p$ (modulo $\sqrt{-p}$), we get:

$$F_p(\lambda_1, \lambda_1^p) \equiv (b \cdot \sqrt{-p})^2 \text{ (modulo } p\sqrt{-p})$$

which concludes the proof of Theorem 1.1 if $\lambda(e_0) \in \mathbf{F}_p$.

4.2. Case $\lambda(e_0) \in \mathbf{F}_{p^2} \backslash \mathbf{F}_p$

Assume now that $\lambda(e_0) \in \mathbf{F}_{p^2} \backslash \mathbf{F}_p$, and without loss of generality that $\lambda(e_0)^p = \lambda(e_g)$. In this case, we choose w_p such that $w_p(\tilde{e}'_0) = \tilde{e}'_g$. Since $w_p^2 \in \Gamma$, we have $w_p^2 = \alpha_g$ (see [1, p. 14] for more details).

Let $z_g^+ \in C_g$ (resp. $z_g^- \in B_g$) be the attractive (resp. repulsive) fixed point of α_g. As in the case $\lambda(e_0) \in \mathbf{F}_p$, the idea is to compute w_p. Let

$$\sigma(z) = \frac{z - z_g^+}{z - z_g^-} .$$

Then $\sigma \circ \alpha_g \circ \sigma^{-1}$ fixes 0 and ∞, and we get

$$\sigma \circ w_p \circ \sigma^{-1} = \kappa \cdot z$$

for some $\kappa \in \mathbf{C}_p$ of absolute value $|p|_p$. We let

$$\pi := -\kappa \cdot (z_g^+ - z_g).$$

Similar arguments as in the case $\lambda(e_0) \in \mathbf{F}_p$ give:

Lemma 4.6. *We have*

$$\Phi(e_0, e_0) \sim \pi$$

and

$$\pi \sim F_p(\beta_0, \beta_0^p)$$

for any lift β_0 *of* $\lambda(e_0)$ *in* K*.*

We refer as before to [4, Sections 4.1–4.2] for details in the j-invariant case.

References

[1] A. Betina, E. Lecouturier, On the p-adic periods of the modular curve $X(\Gamma_0(p) \cap \Gamma(2))$, Trans. Amer. Math. Soc. (2018), https://doi.org/10.1090/tran/7236, in press.

[2] J. Brillhart, P. Morton, Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial, J. Number Theory 106 (1) (2004) 79–111, https://doi.org/10.1016/j.jnt.2004.01.006.

[3] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, Lecture Notes in Math. 349 (1973) 143–316.

[4] E. de Shalit, Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves, in: p-Adic Monodromy and the Birch and Swinnerton–Dyer Conjecture, Boston, MA, 1991, in: Contemp. Math., vol. 165, Amer. Math. Soc., Providence, RI, 1994, pp. 135–148.

[5] E. de Shalit, On the p-adic periods of $X_0(p)$, Math. Ann. 303 (3) (1995) 457–472, https://doi.org/10.1007/BF01461000.

[6] L. Gerritzen, M. van der Put, Schottky Groups and Mumford Curves, Lecture Notes in Mathematics, vol. 817, Springer, Berlin, 1980.

[7] A. Grothendieck, Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. II, Publ. Math. Inst. Hautes Études Sci. 17 (1963) 91, http://www.numdam.org/item?id=PMIHES_1963__17__91_0.

[8] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III, Publ. Math. Inst. Hautes Études Sci. 28 (1966) 255, http://www.numdam.org/item?id=PMIHES_1966__28__255_0.

[9] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York-Heidelberg, 1977.

[10] J.-i. Igusa, On the algebraic theory of elliptic modular functions, J. Math. Soc. Japan 20 (1968) 96–106, https://doi.org/10.2969/jmsj/02010096.

[11] S. Lang, Elliptic Functions, 2nd edition, Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, with an appendix by J. Tate.

[12] E. Lecouturier, Higher Eisenstein elements, higher Eichler formulas and ranks of Hecke algebras, Preprint.

[13] Y. Manin, V. Drinfeld, Periods of p-adic Schottky groups, J. Reine Angew. Math. 262/263 (1973) 239–247, https://doi.org/10.1142/9789812830517__0012, collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday.

[14] D. Mumford, An analytic construction of degenerating curves over complete local rings, Compos. Math. 24 (1972) 129–174.

[15] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[16] N. Yui, Explicit form of the modular equation, J. Reine Angew. Math. 299/300 (1978) 185–200, https://doi.org/10.1515/crll.1978.299-300.185.