DINO J. LORENZINI

Torsion points on the modular jacobian $J_0(N)$

Compositio Mathematica, tome 96, nº 2 (1995), p. 149-172

<http://www.numdam.org/item?id=CM_1995__96_2_149_0>

Compositio Mathematica **96**: 149–172, 1995.
© 1995 *Kluwer Academic Publishers. Printed in the Netherlands.*

Torsion points on the modular Jacobian $J_0(N)$

DINO J. LORENZINI
Department of Mathematics, University of Georgia, Athens, GA 30602

(Received 10 May 1993; accepted in final form 12 April 1994)

Introduction

Fix an integer N and let $X_0(N)/\mathbf{Q}$ denote the Shimura model over $\mathbf{Q}$ of the classical modular curve associated to the subgroup $\Gamma_0(N)$ of SL(2, $\mathbf{Z}$). Let $J_0(N)/\mathbf{Q}$ denote the Jacobian of $X_0(N)/\mathbf{Q}$. Let C_N denote the $\mathbf{Q}$-rational cuspidal subgroup of $J_0(N)$. The group C_N consists of the $\mathbf{Q}$-rational points of the subgroup of $J_0(N)(\overline{\mathbf{Q}})$ generated by the cusps of $X_0(N)$. Let J_N denote the torsion subgroup of $J_0(N)(\mathbf{Q})$. Manin [Man] has shown that $C_N \subseteq J_N$. Let p be a prime. Let $\Phi_N(p)$ denote the group of components of the Néron model of $J_0(N)_{\mathbf{Q}_p}/\mathbf{Q}_p$. Let $\pi_{N,p}\colon J_N \to \Phi_N(p)$ be the canonical reduction map.

Mazur [Maz] has shown, when $N = p$, that the three abelian groups C_N, J_N, and $\Phi_N(p)$ are isomorphic (Conjecture of Ogg). In this paper, we study the reduction map $\pi_{N,p}$, and obtain bounds for the orders of the groups J_N, C_N, and $\Phi_N(p)$. When $N = p^r$ and $p \not\equiv 11 \pmod{12}$, we show that the prime-to-$2p$ parts of the groups C_{p^r} and J_{p^r} are equal, and we explicitly compute them.

1. The results

Let G be any abelian group and let n be any integer. We denote by $G^{(n)}$ the prime-to-n part of the group G. When p is a prime, we let G_p denote the p-part of G.

THEOREM 2.3. *Let $p \geqslant 5$ be a prime. The exponent of the group $\Phi_N(p)/\pi_{N,p}(C_N)$ divides* 12. *In particular, the map $\pi^{(6)}_{N,p}\colon C^{(6)}_N \to \Phi^{(6)}_N(p)$ is surjective.*

We shall show in Remark 4.12 and in Remark 2.8 that the reduction map $\pi_{N,p}$ is, generally, neither injective nor surjective. However, we believe that it is surjective in the special case where $N = p^r$ and $p \geqslant 5$. Fix a prime $p \geqslant 5$ and define two integers a and b as the only positive integers having the following properties: (i) $(p^2 - 1)/24 = ab$, (ii) a divides $(p-1)/2$, and (iii) b divides $(p+1)/2$. Clearly, $\gcd(a, b) = 1$. The integer a is equal to the numerator n (in the notation of [Maz]) of the reduced fraction $(p-1)/12$.

To simplify our notations when $N = p^r$, we denote the group $\Phi_N(p)$ simply by Φ_{p^r}. Note that, if $q \neq p$ is any prime, then the group $\Phi_{p^r}(q)$ is trivial because the Jacobian $J_0(p^r)/\mathbf{Q}$ has good reduction at q. It is shown in [Ma-Ra] that $\Phi_p \cong \mathbf{Z}/a\mathbf{Z}$, and it is shown in [Edi2] that $\Phi_{p^2} \cong \mathbf{Z}/ab\mathbf{Z}$.

THEOREM 1.1. *(See Theorems 3.2, 4.3, and Corollay 4.5). Let $p \geqslant 5$ be a prime. Then*

(i) *The group Φ_{p^r} contains a subgroup isomorphic to $\mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$.*

(ii) *Assume* that $p \not\equiv 11 \pmod{12}$. *Then $\Phi_{p^r}^{(p)}$ is isomorphic to $\mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$. Moreover, the map $\pi_{p^r}\colon C_{p^r} \to \Phi_{p^r}$ is surjective.*

We believe that the above assumption on the congruence class of p modulo 12 is superfluous and that the statement of Theorem 1.1 should be true for all primes $p \geqslant 5$. The surjectivity of the map $\pi_{N,p}\colon C_N \to \Phi_N(p)$ has several interesting consequences, including the corollary discussed below. This corollary was pointed out to us by Mazur. It provides a new proof, for the group $\Phi_N^{(6)}(p)$, of a result that Edixhoven [Edi2] proved for $\Phi_N(p)$.

COROLLARY 1.2. *Let ℓ be a prime, with* $\gcd(\ell, N) = 1$. *Denote by T_ℓ the Hecke operator acting on $\Phi_N(p)$. Then T_ℓ acts on the group $\Phi_N^{(6)}(p)$ by multiplication by $\ell + 1$.*

Proof. The Hecke operator T_ℓ acts on the group C_N by multiplication by $\ell + 1$, as one can easily check explicitly. Theorem 2.3 shows that the map $\pi_{N,p}^{(6)}\colon (C_N)^{(6)} \to \Phi_N(p)^{(6)}$ is surjective. Therefore, our corollary follows. □

THEOREM 4.6. *Let $p \geqslant 5$ be a prime, $p \not\equiv 11 \pmod{12}$. Then*

$$C_{p^r}^{(2p)} = J_{p^r}^{(2p)} \cong \textit{prime-to-2 part of } (\mathbf{Z}/a\mathbf{Z})^r \times (\mathbf{Z}/b\mathbf{Z})^{r-1}.$$

An explicit description of the p-parts of the groups C_{p^r}, J_{p^r}, and Φ_{p^r} is very hard to obtain in general. As the following theorems show, the p-parts of these groups are much larger and much more complicated than their prime-to-p parts. Note that in the case where $r = 1$, it is easy to show that $(C_p)_p = (J_p)_p = (0)$. Indeed, the group of components $(\Phi_p)_p$ can be computed, and is found to be trivial. Let $K = \mathbf{Q}_p^{\mathrm{unr}}$ denote the maximal unramified extension of $\mathbf{Q}_p$. Since the valuation of p in K is equal to 1, the torsion subgroup of $J_0(p^r)(K)$ injects into the special fiber of the Néron model $\mathcal{J}_0(p^r)/\mathcal{O}_K$ of $J_0(p^r)/K$ (see for instance [Kat], Appendix). The special fiber $\mathcal{J}_0(p)_{\overline{\mathbf{F}}_p}/\overline{\mathbf{F}}_p$ is an extension of Φ_p by a torus $\mathcal{T}(p)/\overline{\mathbf{F}}_p$. Since a torus over $\overline{\mathbf{F}}_p$ does not contain any non-trivial point of order p, we conclude that the reduction map $\pi_p\colon (J_p)_p \to (\Phi_p)_p$ is injective. Therefore, $(J_p)_p = (0)$.

When $r \geqslant 2$, the special fiber of the Néron model $\mathcal{J}_0(p^r)/\mathcal{O}_K$ of $J_0(p^r)/K$ always contains a non-trivial unipotent group scheme, which may contain non-trivial points of order p. It is thus not possible anymore to use the above argument to show that the reduction map $\pi_{p^r}\colon (J_{p^r})_p \to (\Phi_{p^r})_p$ is injective.

THEOREM 1.3. *(See Theorems 3.2 and 3.12). Let $p \geqslant 5$ be a prime. Assume that* $p \not\equiv 11 \pmod{12}$. *Then*

$$|(\Phi_{p^r})_p| = \begin{cases} p^{2s^2} & \textit{if } r = 2s+1, \\ p^{2s(s-1)} & \textit{if } r = 2s. \end{cases}$$

Let w denote the involution of Φ_{p^r} induced by the Atkin–Lehner involution of $X_0(p^r)/\mathbf{Q}$. Let $\Phi_{p^r}^+$ and $\Phi_{p^r}^-$ denote the images in Φ_{p^r} of $(w + \mathrm{id})$ and $(w - \mathrm{id})$, respectively.

THEOREM 1.4. *Let* $p \equiv 1 \pmod{12}$. *Then* $(\Phi_{p^2})_p = \{0\}$, *and* $(\Phi_{p^3})_p = (\Phi_{p^3})_p^- = \mathbf{Z}/p^2\mathbf{Z}$. *Moreover, if* $r = 2s$, *then*

$$(\Phi_{p^r})_p^+ = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p^3\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{2s-3}\mathbf{Z},$$

$$(\Phi_{p^r})_p^- = \mathbf{Z}/p^3\mathbf{Z} \times \mathbf{Z}/p^5\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{2s-1}\mathbf{Z}.$$

If $r = 2s + 1$, *then*

$$(\Phi_{p^r})_p^+ = \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p^4\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{2s-2}\mathbf{Z},$$

$$(\Phi_{p^r})_p^- = \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p^4\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{2s}\mathbf{Z}.$$

In particular, the exponent of $(\Phi_{p^r})_p$ *is equal to* p^{r-1}, *and the group* $(\Phi_{p^r})_p$ *has a minimal system of generators consisting of* $r - 2$ *distinct elements.*

We believe that the assumptions on the congruence class of p modulo 12 are superfluous and that the statements of Theorem 1.3 and of Theorem 1.4 should be true for all primes $p \geqslant 5$. Theorem 1.4 will not be proved in this paper. The proof of this theorem consists in a rather complicated row and column reduction of the intersection matrix associated to a regular model $\mathcal{X}/\mathbf{Z}_p$ of $X_0(p^r)/\mathbf{Q}_p$.

Poulakis [Pou], 3.2, has computed the groups C_{5^3} and J_{5^3} and found both groups to be cyclic of order 25. The group Φ_{5^3} can be computed easily using the results recalled in section 3, and is also found to be cyclic of order 25. Hence, since the map $\pi_{p^r}\colon (C_{p^r})_p \to (\Phi_{p^r})_p$ is surjective if $p \geqslant 5$, we find that $C_{5^3} = J_{5^3} \xrightarrow{\sim} \Phi_{5^3}$.

This article will proceed as follows. In section two, we study the reduction map $\pi_{N,p}\colon C_N \to \Phi_N(p)$. In the third section, we explicitly compute the order of the group of components Φ_{p^r}. In the last section, we describe the prime-to-$2p$ part of the group J_{p^r} of $\mathbf{Q}$-rational torsion points on $J_0(p^r)$.

2. The reduction map $\pi_{N,p}\colon C_N \to \Phi_N(p)$

Let K be a complete field with respect to a discrete valuation. Let $\mathcal{O}_K$ denote the ring of integers of K. Assume that the residue field k is algebraically closed. Let X/K denote any smooth, proper, geometrically irreducible curve having a K-rational point. Let A/K denote the Jacobian of X/K. Let Φ be the group of components of the Néron model of A/K. Let $\pi\colon A(K) \to \Phi$ be the natural reduction map. We recall below Raynaud's description of the group Φ and of the map π in terms of a regular model $\mathcal{X}/\mathcal{O}_K$ of X/K.

The special fiber $\mathcal{X}_k$ of a regular model $\mathcal{X}/\mathcal{O}_K$ is a Cartier divisor, and, as such, we write it $\mathcal{X}_k = \Sigma_{i=1}^n r_i C_i$, where C_i is an irreducible component of multiplicity r_i. Let $L := \oplus_{i=1}^n \mathbf{Z}C_i$ denote the free abelian group generated by the components C_i, $i = 1, \dots, n$. Let $L^* := \mathrm{Hom}_{\mathbf{Z}}(L, \mathbf{Z})$, and let $\{x_1, \dots, x_n\}$ denote the dual basis of L, so that $x_i(C_j) = \delta_{ij}$. Let ${}^tR$: $L^* \to \mathbf{Z}$ be the map $\Sigma_{i=1}^n a_i x_i \mapsto \Sigma_{i=1}^n a_i r_i$.

2.1. Consider the following commutative diagram:

$$\begin{tikzcd}
L \arrow[r, "i"] \arrow[d, equal] & \mathrm{Pic}(\mathcal{X}) \arrow[r, "\mathrm{res}"] \arrow[d, "\phi"] & \mathrm{Pic}(X) \arrow[r, "\deg"] \arrow[d, "\psi"] & \mathbf{Z} \arrow[d, equal] \\
L \arrow[r, "\mu"] & L^* \arrow[r] & L^*/\mu(L) \arrow[r, "{}^tR"] & \mathbf{Z}
\end{tikzcd}$$

The map i is defined as follows: $i(C_j) :=$ curve C_j in $\mathcal{X}$, where the curve C_j is viewed as an element of $\mathrm{Pic}(\mathcal{X})$. The map res restricts a divisor of $\mathcal{X}$ to the open set X of $\mathcal{X}$. The map res is surjective because the scheme $\mathcal{X}$ is regular. The map deg is defined as follows: $\deg(\Sigma_{i=1}^s a_i P_i) := \Sigma_{i=1}^s a_i [K(P_i){:}K]$, where $K(P_i)$ is the residue field of P_i in X. We denote by $\mathrm{Pic}^0(X)$ the kernel of the map deg. Let $M = ((C_i \cdot C_j))_{1 \leqslant i,j \leqslant n}$ denote the symmetric intersection matrix associated to $\mathcal{X}_k$. This matrix can be thought of as a bilinear map on $L \times L$ and, therefore, induces a map μ: $L \to L^*$ defined by $\mu(C_i) := \Sigma_{j=1}^n (C_i \cdot C_j) x_j$. It is a well-known fact that ${}^tR \circ \mu = 0$. Let D be an irreducible divisor on $\mathcal{X}$, and define $\phi(D) := \Sigma_{j=1}^n (C_j \cdot D) x_j$. The map ψ is the natural map induced by ϕ.

2.2. One easily checks that $\mathrm{Ker}({}^tR)/\mu(L)$ is the torsion subgroup of $L^*/\mu(L)$. Raynaud [BLR], 9.6, showed that the group of components Φ of the Jacobian A/K of the curve X/K is isomorphic to the group $\mathrm{Ker}({}^tR)/\mu(L)$. It follows from this description that the group Φ can be explicitly computed using a row and column reduction of the matrix $M := ((C_i \cdot C_j))$ (see [Lor1], 1.4). Raynaud ([BLR], 9.5/9 and 9.6/1) has shown that the reduction map π: $A(K) \to \Phi$ corresponds to the restricted map ψ: $\mathrm{Pic}^0(X) \to \mathrm{Ker}({}^tR)/\mu(L)$.

Let $p \geqslant 5$ be a prime and let D be any integer prime to p. Set $N := Dp^r$. Let K denote the maximal unramified extension of $\mathbf{Q}_p$. Let $k = \overline{\mathbf{F}}_p$ denote the residue field of $\mathcal{O}_K$. Our aim in this section is to apply Raynaud's general results recalled above to the particular case of modular curves $X_0(N)/K$.

THEOREM 2.3. *Let $p \geqslant 5$ be a prime. The exponent of the group $\Phi_N(p)/\pi_{N,p}(C_N)$ divides* 12. *In particular, the map $\pi_{N,p}^{(6)}$: $C_N^{(6)} \to \Phi_N^{(6)}(p)$ is surjective.*

Proof. Edixhoven describes a regular model $\mathcal{X}/\mathcal{O}_K$ of $X_0(N)/K$ in [Edi1], 1.4. We recall here the main properties of this model. Let $\mathcal{Y}/\mathcal{O}_K$ denote the compactified coarse moduli scheme $\overline{M}([\Gamma_0(Dp^r)])$, constructed by Katz and Mazur in [K-M], Chapter 8. The regular model $\mathcal{X}$ is obtained by contracting the exceptional rational curves having self-intersection (-1) in the desingularization p: $\mathcal{Z} \to \mathcal{Y}$ of the scheme $\mathcal{Y}$. This model $\mathcal{X}$ is the minimal model of $X_0(N)$, except for some low values of N ($N = p = 11$ is an example where $\mathcal{X}$ is not minimal). Before describing the resolution of the singularities of $\mathcal{Y}$, let us recall the description of the special fiber $\mathcal{Y}_k/k$ of $\mathcal{Y}$. Let C denote the compactified modular curve $X_0(D)/k$. Index $r+1$ copies of C by $C_{(a,b)}$, with $a+b=r$, $a, b \geqslant 0$. Let

$$f\colon \bigsqcup_{a+b=r} C_{(a,b)} \to C$$

denote the following map:

$$f_{|C_{(a,b)}} := \begin{cases} \text{identity} & \text{if } a \geqslant b, \\ (\text{absolute Frobenius})^{b-a} & \text{if } a \leqslant b. \end{cases}$$

The curve $C = X_0(D)$ is equipped with finitely many marked points, namely, the supersingular points. Indeed, recall that a supersingular point x on C corresponds to a pair (E, G) where E is a supersingular elliptic curve and G is a cyclic group of order D in $E(k)$. The reduced curve $(\mathcal{Y}_k)_{\text{red}}$ is obtained from $\sqcup_{a+b=r} C_{(a,b)}$ by contracting the fiber $f^{-1}(x)$ to a single point whenever x is a supersingular point of C. The multiplicity of the component $C_{(a,b)}$ in $\mathcal{Y}_k$ is equal to

$$\begin{cases} 1 & \text{if } ab = 0, \\ (p-1)p^{\min(a,b)-1} & \text{if } a, b \geqslant 1. \end{cases}$$

The scheme $\mathcal{Y}$ is singular at certain closed points y of $\mathcal{Y}_k$ corresponding to pairs (E, G) with E an elliptic curve of j-invariant 0 or 1728. The strict transform in $\mathcal{Z}$ of a component $C_{(a,b)} \subset \mathcal{Y}$ is not contracted in $\mathcal{X}$. Therefore, we may consider the components $C_{(a,b)}$, $a+b=r$, as irreducible divisors in the group $\operatorname{Pic}(\mathcal{X})$.

Let L denote the free abelian group generated by the irreducible components of $\mathcal{X}_k$. We will, from now on, identify $\Phi_N(p)$ with the torsion subgroup of $L^*/\mu(L)$. Let $c(a, b)$ denote the dual element in L^* of the irreducible curve $C_{(a,b)}$. Since $C_{(a,b)}$ and $C_{(b,a)}$ have the same multiplicity in $\mathcal{X}_k$, it is clear that the elements

$$u(a, b) := c(a, b) - c(b, a), \quad a+b=r,$$

and the elements

$$v(a, b) := c(a, b) + c(b, a) - (\text{multiplicity of } C_{(a,b)})(c(0, r) + c(r, 0)),$$
$$a+b=r,$$

are in the kernel of ${}^tR$: $L^* \to \mathbf{Z}$ and, hence, define elements in the torsion group $\Phi_N(p)$. Let H denote the subgroup of $\Phi_N(p)$ generated by the images of the elements $u(a, b)$ and $v(a, b)$ with $a + b = r$.

LEMMA 2.4. *The subgroup H is contained in the image $\pi_{N,p}(C_N)$.*

Proof. Ogg shows in [Ogg1], Proposition 2, that every cusp of $X_0(N)(\overline{\mathbf{Q}})$ can be represented by a pair $[x, d]$, with $\gcd(d, x) = 1$ and $d|N$ and, letting $t := \gcd(d, N/d)$, with $\gcd(t, x) = 1$ and $0 \leqslant x \leqslant t$. The pairs $[0, 1]$ and $[1, 1]$ represent the same cusp in $X_0(N)$. Let $\varphi(t)$ denote the Euler function. The set of $\varphi(t)$ cusps $\{[x, d], d \text{ fixed}, 0 \leqslant x \leqslant t, \gcd(t, x) = 1\}$ is an orbit under $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Each cusp $[x, d]$ is defined over $\mathbf{Q}(\xi_t)$, where ξ_t denotes a primitive t^{th} root of unity.

For each pair (a, b) with $a + b = r$, denote by $P(a, b)$ the closed point of the scheme $X_0(Dp^r)/\mathbf{Q}$ corresponding to the orbit $\{[x, p^a], 0 \leqslant x \leqslant p^{\min(a,b)}, \gcd(p, x) = 1\}$. Let $\overline{P(a, b)}$ denote the closure of the point $P(a, b)$ in $\mathcal{X}$. Since each point $P(a, b)$ reduces to a nonsingular point in the special fiber of the normal model $\mathcal{Y}$ ([Edi1], 1.2.3.1), we find that $\overline{P(a, b)} \cap \mathcal{X}_k$ belongs to a single component $C_{(u,v)}$. Since

$$\varphi(p^{\min(a,b)}) = \overline{P(a, b)} \cdot \mathcal{X}_k = \varphi(p^{\min(u,v)})\overline{P(a, b)} \cdot C_{(u,v)} = \varphi(p^{\min(u,v)}),$$

we find that exactly one of the sets $\overline{P(a, b)} \cap C_{(a,b)}$ and $\overline{P(a, b)} \cap C_{(b,a)}$ is nonempty. Since $P(b, a)$ and $C_{(b,a)}$ are, respectively, the images of $P(a, b)$ and $C_{(a,b)}$ under the Atkin–Lehner involution (see 2.5 below), we find that $\overline{P(a, b)} \cap C_{(u,v)} \neq \emptyset$ if and only if $\overline{P(b, a)} \cap C_{(v,u)} \neq \emptyset$. Consider the following divisors of $X_0(Dp^r)/\mathbf{Q}$: $U(a, b) := P(a, b) - P(b, a)$, with $a + b = r$, and

$$V(a, b) := P(a, b) + P(b, a) - \varphi(p^{\min(a,b)})(P(r, 0) + P(0, r)).$$

One easily check that these divisors correspond to elements in $C_N \subseteq \mathrm{Pic}^0(X_0(Dp^r) \times_{\mathbf{Q}} \overline{\mathbf{Q}})$. Let ϕ: $\mathrm{Pic}(\mathcal{X}) \to L^*$ be the map described in 2.1. It follows from the facts recalled above that $\phi(\overline{U(a, b)}) = \pm u(a, b)$, and $\phi(\overline{V(a, b)}) = v(a, b)$. This proves our lemma. □

2.5. To show that $\Phi_N(p)/\pi_{N,p}(C_N)$ is killed by 12, it is sufficient to show that $\Phi_N(p)/H$ is killed by 12. To prove that $\Phi_N(p)/H$ is killed by 12, we use an involution of $\Phi_N(p)$ to show the existence of two subgroups Φ^+ and Φ^- of $\Phi_N(p)$ such that (1) the group $\Phi_N(p)/(\Phi^+ + \Phi^-)$ is killed by 2, and (2) $H \subseteq (\Phi^+ + \Phi^-)$ and $(\Phi^+ + \Phi^-)/H$ is killed by 6. Consider the involution

$$w\colon \bigoplus_{a+b=r} \mathbf{Z}C_{(a,b)} \to \bigoplus_{a+b=r} \mathbf{Z}C_{(a,b)},$$

$$C_{(a,b)} \mapsto C_{(b,a)}.$$

It is easy to check, using the symmetry of the special fiber of $\mathcal{X}_k$, that the involution w can be extended to an involution $w: L \to L$. We let $w': L^* \to L^*$ denote the dual involution. One also easily checks that $w' \circ \mu = \mu \circ w$. It follows that w' induces an involution $w: \Phi_N(p) \to \Phi_N(p)$.

2.6. We sketch below how one may also describe w as the map induced on $\Phi_N(p)$ by an Atkin–Lehner involution of $X_0(N)/\mathbf{Q}$. Recall that, since $N = Dp^r$ and $\gcd(p^r, D) = 1$, there exists an Atkin–Lehner involution $w_{p^r}: X_0(N) \to X_0(N)$, defined over $\mathbf{Q}$, and acting on the cusp $[x, p^a]$ as follows:

$$w_{p^r}([x, p^a]) = [-x, p^b], \quad \text{where} \quad a + b = r.$$

(See for instance [Ogg2], Proposition 2.) By functoriality, w_{p^r} induces an involution on the Néron model of $J_0(N)/\mathbf{Q}_p$ and, hence, also induces an involution $w_{p^r}: \Phi_N(p) \to \Phi_N(p)$. To identify this involution w_{p^r} of $\Phi_N(p)$ to the involution w defined in 2.5, it is sufficient, first, to check that the map $w_{p^r}: X_0(N) \to X_0(N)$ extends to a map $\overline{w_{p^r}}: \mathcal{X} \to \mathcal{X}$, and then, to check that the map $\overline{w_{p^r}}$ induces the map w on L. The key is to note that the map w_{p^r}, being defined as a map of moduli problems over $\mathbf{Z}$, can be extended to an involution $\overline{w_{p^r}}$ of the normal model $\mathcal{Y}/\mathbf{Z}_p$ of $X_0(N)/\mathbf{Q}_p$, such that $\overline{w_{p^r}}(C_{(a,b)}) = C_{(b,a)}$.

Let $\mathcal{Z}$ be any scheme. Let $\sigma: \mathcal{Z} \to \mathcal{Z}$ be an automorphism of $\mathcal{Z}$. Let $P \in \mathcal{Z}$ be any closed point. Let $\mathcal{Z}_P$ denote the blow-up of $\mathcal{Z}$ at P. It follows from the universal property of blow-ups that the automorphism σ induces an automorphism $\sigma_P: \mathcal{Z}_P \to \mathcal{Z}_{\sigma(P)}$. Let E_P denote the exceptional divisor in the blow-up $\mathcal{Z}_P$. Let $\tau: \mathcal{Z}_P \to \mathcal{Z}_Q$ be an isomorphism such that $\tau(E_P) = E_Q$. Assume that $\mathcal{Z}$ is normal. It follows from the fact that the maps $\mathcal{Z}_P \to \mathcal{Z}$ and $\mathcal{Z}_Q \to \mathcal{Z}$ are proper and birational that τ induces an automorphism $\sigma: \mathcal{Z} \to \mathcal{Z}$ such that $\sigma(P) = Q$. These remarks show that the map $\overline{w_{p^r}}: \mathcal{Y} \to \mathcal{Y}$ induces an involution $\overline{w_{p^r}}: \mathcal{X} \to \mathcal{X}$ and, hence, induces an involution $w_{p^r}: L \to L$. Since $w_{p^r}(C_{(a,b)}) = C_{(b,a)}$ for all (a, b) with $a + b = r$, it is easy to check that the involutions w_{p^r} and w are equal as involutions of L.

2.7. Let $w: \Phi_N(p) \to \Phi_N(p)$ be the involution defined in 2.5. Let Φ^+ and Φ^- denote the images in $\Phi_N(p)$ of $w + \mathrm{id}$ and $w - \mathrm{id}$, respectively. Let $x \in \Phi_N(p)$. Since $2x = (x + w(x)) + (x - w(x)) \in \Phi^+ + \Phi^-$, Property (1) in 2.5 is true. It is clear that Φ^- is generated by the elements of L^* of the form $u(c) := c - w'(c)$, with $c \in L^*$. It is also clear that Φ^+ is generated by the elements of L^* of the form $v(c) := c + w'(c) - (\text{multiplicity of } C)(c(0, r) + c(r, 0))$, with $c \in L^*$, where C denotes the component of $\mathcal{X}_k$ whose dual in L^* is c.

Clearly, $H \subseteq \Phi^+ + \Phi^-$. Let us now show that $(\Phi^+ + \Phi^-)/H$ is killed by 6. Let $p: \mathcal{Z} \to \mathcal{Y}$ denote a resolution of the singularities of $\mathcal{Y}$, and let $c: \mathcal{Z} \to \mathcal{X}$ denote the contraction map. Recall that the strict transform of $C_{(a,b)} \subset \mathcal{Y}$ is not contracted by c, even in the few cases where the strict transform of $C_{(a,b)}$ is a rational curve with self-intersection equal to (-1). Let $E \subseteq \mathcal{X}_k$ be an irreducible component such that $p(c^{-1}(E))$ is a closed point of $\mathcal{Y}$. Let e denote the dual element of E in L^*.

The fact that the orders of the images of $u(e)$ and $v(e)$ in $(\Phi^+ + \Phi^-)/H$ divide 6 is a consequence, as we shall see below, of the fact that the self-intersection $(E \cdot E)$ of E in $\mathcal{X}$ is equal to -2 or -3. There are several cases to be treated separately, namely:

(i) the image $p(c^{-1}(E))$ is a nonsingular point of $(\mathcal{Y}_k)_{\text{red}}$.
(ii) The image $p(c^{-1}(E))$ is a singular point of $(\mathcal{Y}_k)_{\text{red}}$ which corresponds to a supersingular curve with $j = 1728$.
(iii) r is even, and the image $p(c^{-1}(E))$ is a singular point of $(\mathcal{Y}_k)_{\text{red}}$ which corresponds to a supersingular curve with $j = 0$.
(iv) r is odd, and the image $p(c^{-1}(E))$ is a singular point of $(\mathcal{Y}_k)_{\text{red}}$ which corresponds to a supersingular curve with $j = 0$.

We shall treat only the first case. The other cases are similar. We leave the verification that our claim is true in cases (ii), (iii), and (iv) to the reader.

Assume that $p(c^{-1}(E))$ is a nonsingular point of $\mathcal{Y}_k$. The description of the singularities of the normal model $\mathcal{Y}$ implies that $p(c^{-1}(E))$, which belongs to one of the modular curves $C_{(a,b)}$, corresponds to an ordinary elliptic curve of invariant $j = 0$ or $j = 1728$. It follows from the work of Edixhoven [Edi1], 1.3.3 and 1.3.6, that

$$c(p^{-1}(p(c^{-1}(E)))) = E,$$

and that $(E \cdot E)_{\mathcal{X}}$ equals -3 or -2, depending on whether $j = 0$ or 1728. Since $p(c^{-1}(E))$ belongs to exactly one component of $\mathcal{Y}_k$, say $C_{(a,b)}$, we find that

$$(E \cdot E)e + c(a, b) = \mu(E) \in \mu(L),$$

and

$$(E \cdot E)w'(e) + c(b, a) = \mu(w(E)) \in \mu(L).$$

Therefore

$$(E \cdot E)u(e) + u(a, b) = 0 \text{ in } \Phi_N(p),$$

and

$$(E \cdot E)v(e) + v(a, b) = 0 \text{ in } \Phi_N(p).$$

This concludes the proof of Theorem 2.3. □

REMARK 2.8. The map $\pi_{N,p}\colon C_N \to \Phi_N(p)$ is not surjective, in general, when $N = Dp^r$ and $D \neq 1$. This can be seen, for instance, when $N = q_1q_2p$, with $q_1 = 13$, $q_2 = 37$, and $p = 11$. The tables in [Edi2], 4.4.1, show that, for this particular choice of N, the group $\Phi_N(p)$ is the product of five cyclic groups. To show that the map $\pi_{N,p}$ cannot be surjective, we simply note that the group $\pi_{N,p}(C_N)$ must be cyclic. Indeed, each one of the eight cusps on the curve $X_0(q_1q_2p)$ is rational. Each cusp reduces to a non-singular point in the special fiber of the normal model $\mathcal{Y}$. This shows that the image $\pi_{N,p}(C_N)$ of C_N is contained in the subgroup of $\Phi_N(p)$ generated by the image of $c(1, 0) - c(0, 1)$ under the natural map $L^* \to L^*/\mu(L)$.

3. Computation of Φ_{p^r}

Let X/K be a smooth, proper, geometrically connected curve having a K-rational point. Let $\mathcal{X}/\mathcal{O}_K$ be a regular model of X/K. Let $\mathcal{X}_k = \Sigma_{i=1}^n r_i C_i$ denote the special fiber of $\mathcal{X}$ and let $M = ((C_i \cdot C_j))_{1\leqslant i,j\leqslant n}$ be the associated intersection matrix. The dual graph $G = G(\mathcal{X})$, associated to the special fiber $\mathcal{X}_k$, is defined as follows. The vertices of G are the curves C_i and, when $j \neq h$, the vertex C_j is linked in G to the vertex C_h by exactly $(C_j \cdot C_h)$ edges. The *degree* of the vertex C_i in G is the integer $d_i := \Sigma_{i\neq j}(C_i \cdot C_j)$.

Let ${}^tR := (r_1, \ldots, r_n)$, so that $MR = 0$. The triple (G, M, R) is an example of what we called an *arithmetical graph* in [Lor1]. We call the group $\Phi(G) := \mathrm{Ker}({}^tR)/\mathrm{Im}(M)$ the *group of components* of the arithmetical graph (G, M, R). When no confusion may result, we denote this group simply by Φ. When we need to emphasize the dependence of G, M, and R on $\mathcal{X}$, we write $G(\mathcal{X})$, $M(\mathcal{X})$, and $R(\mathcal{X})$. When M is not the intersection matrix attached to a given special fiber $\mathcal{X}_k$, we may denote the coefficients of M by c_{ij}, $1 \leqslant i, j \leqslant n$, rather than by $(C_i \cdot C_j)$.

3.1. Let (G, M, R) be an arithmetical graph. In [Lor1], 2.3, we showed that, when G is a tree, $|\Phi(G)| = \Pi_{i=1}^n r_i^{d_i-2}$. Let ℓ be any prime and assume again that G is a tree. In [Lor2], 2.1, we explicitly describe the group structure of the ℓ-part of Φ when the tree G satisfies an additional explicit "Condition C_ℓ" ([Lor2], 1.5). Our aim in this section is to apply these two results describing the group Φ to the case of $X_0(p^r)$.

THEOREM 3.2. *Let $p \geqslant 5$ be a prime and let $N = p^r$. Assume that either (1) $p \equiv 1 \pmod{12}$, or (2) $p \equiv 7 \pmod{12}$, or (3) $p \equiv 5 \pmod{12}$ and r is even, or (4) $p = 5$. Then $\Phi_{p^r}^{(p)}$ is isomorphic to $\mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$, and*

$$|p\text{-}part\ of\ \Phi_{p^r}| = \begin{cases} p^{2s^2} & if\ r = 2s+1, \\ p^{2s(s-1)} & if\ r = 2s. \end{cases}$$

REMARK 3.3. Let X/K be any curve and let $\mathcal{X}/\mathcal{O}_K$ be a regular model of X/K such that the components of the curve $(\mathcal{X}_k)_{\mathrm{red}}$ are smooth and intersect normally. We call such a model a good model. Raynaud has shown that the graph $G(\mathcal{X}_k)$ is a tree if and only if the toric rank of the Jacobian of X/K is equal to zero ([BLR], Proposition 10, page 249). In the case of the modular curve $X_0(p^r)/K$, the toric rank of $J_0(p^r)/K$ is equal to $r \cdot \mathrm{genus}(X_0(p))$. Therefore, the toric rank of $J_0(p^r)/K$ equals zero only when $p = 5$, 7, or 13. In these three cases, the graph associated to a good model of $X_0(p^r)$ is a tree and the group Φ_{p^r} can be computed using the results recalled in 3.1. In all other cases, the graph $G(\mathcal{X}_k)$ associated to a good model $\mathcal{X}/\mathcal{O}_K$ of $X_0(N)/K$ is not a tree and, therefore, the results of 3.1 cannot be applied to $G(\mathcal{X}_k)$ to compute Φ_{p^r}.

Proof of Theorem 3.2. Let $\mathcal{X}/\mathcal{O}_K$ denote the regular model of $X_0(p^r)/K$ described by Edixhoven in [Edi1], 1.4. In general, the graph associated to $\mathcal{X}_k$ is not a tree simply because two components $C_{(a,b)}$ and $C_{(\alpha,\beta)}$ do not intersect transversally. Indeed, let P denote a point on $C_{(a,b)} \cap C_{(\alpha,\beta)}$ in the normal model $\mathcal{Y}$. The local equation at the point P in $\mathcal{Y}_k$ is given by

$$(x^{p^r} - y)(x - y^{p^r}) \prod_{a+b=r,\, a,b>0} (x^{p^{a-1}} - y^{p^{b-1}})^{p-1}.$$

The component $C_{(a,b)}$ has local equation $x^{p^{a-\min(a,b)}} - y^{p^{b-\min(a,b)}}$. When P is a nonsingular point of $\mathcal{Y}$, the intersection number of $C_{(a,b)}$ and $C_{(\alpha,\beta)}$ in $\mathcal{X}$ at P is obtained by computing the length over k of the quotient $k[[x, y]]/I$, where

$$I = (x^{p^{a-\min(a,b)}} - y^{p^{b-\min(a,b)}},\ x^{p^{\alpha-\min(\alpha,\beta)}} - y^{p^{\beta-\min(\alpha,\beta)}}).$$

One shows easily that

$$(C_{(a,b)} \cdot C_{(\alpha,\beta)})_P = \begin{cases} 1 & \text{if } (a-b)(\alpha-\beta) \leqslant 0, \\ p^{\min(|a-b|,|\alpha-\beta|)} & \text{if } (a-b)(\alpha-\beta) > 0. \end{cases}$$

This computation of $(C_{(a,b)} \cdot C_{(\alpha,\beta)})$ clearly shows that, in general, the graph $G(\mathcal{X})$ is not a tree. As we point out in Remark 3.3, no good regular model of $X_0(p^r)/K$ has, in general, an associated graph which is a tree. To be able nevertheless to apply the results recalled in 3.1 to compute Φ_{p^r}, we will associate to the arithmetical graph $(G(\mathcal{X}), M(\mathcal{X}), R(\mathcal{X}))$ a new arithmetical graph $(\overline{G}, \overline{M}, \overline{R})$ in such a way that $\Phi(G(\mathcal{X})) = \Phi(\overline{G})$ and $\overline{G}$ is a tree. To describe the construction of the arithmetical graph $(\overline{G}, \overline{M}, \overline{R})$, we need to recall the definition of the blow-up of an arithmetical graph.

3.4. Let $\mathcal{X}/\mathcal{O}_K$ be a regular model of a curve X/K. Let $(G(\mathcal{X}), M(\mathcal{X}), R(\mathcal{X}))$ denote the associated arithmetical graph. Let $P \in \mathcal{X}_k$. Let $\mathcal{X}_P$ denote the blow-up of $\mathcal{X}$ at P. Then $\Phi(G(\mathcal{X}_P)) = \Phi(G(\mathcal{X}))$. Indeed, the generic fibers of $\mathcal{X}$ and $\mathcal{X}_P$ are equal. Hence, both group $\Phi(G(\mathcal{X}_P))$ and $\Phi(G(\mathcal{X}))$ are isomorphic to $\Phi(\mathrm{Jac}(X))$.

Let $J \subseteq \{1, \ldots, n\}$ be any subset. Let $Q = Q(J)$ denote the transpose of the matrix

$${}^tQ = (q_1, \ldots, q_n),$$

where $q_i = 1$ if $i \in J$, and $q_i = 0$ otherwise. Let (G, M, R) be any arithmetical graph, with $M = (c_{ij})_{1 \leqslant i,j \leqslant n}$. If $c_{ij} > 0$ for all $(i, j) \in J \times J$, $i \neq j$, then we let

$$M_Q := \begin{pmatrix} M - Q({}^tQ) & Q \\ {}^tQ & -1 \end{pmatrix},$$

and

$${}^tR_Q = \left(r_1, \ldots, r_n, \sum_{i=1}^{n} q_i r_i \right).$$

Let G_Q denote the graph associated to M_Q. The triple (G_Q, M_Q, R_Q) is a new arithmetical graph. It is easy to check (see for instance [Lor1], 1.8) that $\Phi(G_Q) = \Phi(G)$. By analogy to the geometric case, we call (G_Q, M_Q, R_Q) the *blow-up* of (G, M, R) at Q. In fact, when $P \in \mathcal{X}_k$ (and $\mathcal{X}$ is a good model) and $J := \{j | P \in C_j\}$, then $G_{Q(J)} = G(\mathcal{X}_P)$.

CLAIM 3.5. *Let (G_0, M_0, R_0) denote the arithmetical graph associated to the model $\mathcal{X}/\mathcal{O}_K$ of $X_0(p^r)/K$ described in [Edi1]. If $p \equiv 1 \pmod{12}$, or if $p \equiv 7 \pmod{12}$, or if $p \equiv 5 \pmod{12}$ and r is even, or if $p = 5$, then there exists a sequence of arithmetical graphs (G_i, M_i, R_i), $i = 1, \ldots, m$, such that $(G_{i+1}, M_{i+1}, R_{i+1})$ is a blow-up of (G_i, M_i, R_i) for all $i = 0, \ldots, m-1$, and G_m is a tree. In particular, $\Phi(G_m) = \Phi(G_0)$, and $\Phi(G_m)$ can be computed using the results quoted in 3.1.*

3.6. To describe the sequence of blowups whose existence is stated in the above claim, we found it convenient to introduce the following terminology. Let $\mathcal{Z}_k = \Sigma_{i=1}^n r_i C_i$ denote the special fiber of a regular model $\mathcal{Z}/\mathcal{O}_K$. The diagram of $\mathcal{Z}_k$, denoted by $\mathcal{D}(\mathcal{Z}_k)$, is a topological space defined as follows. For each $i = 1, \ldots, n$, let D_i denote a copy of the interval $(0, 1) \subset \mathbf{R}$, and let

$$\{P_{i,1}, \ldots, P_{i,s_i}\} := C_i \cap \left(\bigcup_{j \neq i} C_j \right).$$

Mark s_i distinct points $P'_{i,j}$ on the interval D_i. Let

$$\mathcal{D}(\mathcal{Z}_k) := \left(\bigcup_{i=1}^{n} D_i \right) \Big/ \sim,$$

where $\sim$ denote the following equivalence: $P'_{i,\ell}$ is glued to $P'_{j,m}$ in $\mathcal{D}(\mathcal{Z}_k)$ if and only if $P_{i,\ell} = P_{j,m}$.

Let (G, M, R) be an arithmetical graph, with $M = (c_{ij})_{1 \leqslant i,j \leqslant n}$. We associate to M a topological space as follows. Let $I = \{1, \ldots, n\}$. Choose a subset I_1 of maximal cardinality in I with the property that $c_{ij} > 0$, $\forall\, i, j \in I_1$, $i \neq j$. Assume that subsets $I_1, I_2, \ldots, I_{\ell-1}$ have been chosen. Then choose a subset I_ℓ of maximal cardinality in $I \backslash \sqcup_{j=1}^{\ell-1} I_j$ with the property that $c_{ab} > 0$, $\forall\, a, b \in I_\ell$, $a \neq b$. Let us assume that $|I_r| \geqslant 2$, and that $|I_s| \leqslant 1$ if $s > r$. Set $J := I \backslash \sqcup_{i=1}^{r} I_i$, so that $I = I_1 \sqcup \cdots \sqcup I_r \sqcup J$. Let D_i, $i = 1, \ldots, n$, be n copies of the interval $(0, 1) \subseteq \mathbf{R}$. Let $\mathcal{D}(M) = \mathcal{D}(M, I_1, \ldots, I_r)$ denote the union $\sqcup_{i=1}^{n} D_i$, with the following glueing data:

- For each $i \in I \backslash J$, mark a point $P_{i,0}$ on D_i. Then glue $P_{i,0}$ to $P_{j,0}$ if and only if there exists $s \in \{1, \ldots, r\}$ such that $i, j \in I_s$.
- When $i \in I_\ell$ and $\ell \leqslant r$, let $S_i := \{j \in I \backslash I_\ell \,|\, c_{ij} > 0\}$. Let $s_i := |S_i|$. Mark s_i distinct points $P_{i,j}$, $j \in S_i$, on $D_i \backslash \{P_{i,0}\}$. When $i \in J$, let $S_i := \{j \in I | c_{ij} > 0\}$. Let $s_i := |S_i|$. Mark s_i distinct points $P_{i,j}$, $j \in S_i$, on D_i. Then glue $P_{i,a}$ to $P_{j,b}$ if and only if $a = j$ and $b = i$.

The space $\mathcal{D}(M)$ depends on the choice of a partition of I. Each such space $\mathcal{D}(M)$ is called a *diagram* associated to (G, M, R).

REMARK 3.7. Let $\mathcal{X}/\mathcal{O}_K$ denote the regular model of $X_0(p^r)/K$ described in [Edi1]. In general, the topological space $\mathcal{D}(\mathcal{X}_k)$ is not simply connected. On the other hand, when $p \equiv 1 \pmod{12}$, or $p \equiv 7 \pmod{12}$, or $p \equiv 5 \pmod{12}$ and r is even, then every diagram associated to $M(\mathcal{X}_k)$ is simply connected.

Let (G, M, R) be an arithmetical graph, and let $\mathcal{D}(M) = \sqcup_{i=1}^{n} D_i$ be a diagram associated to M. Let $P \in \mathcal{D}(M)$. Let ${}^tQ := (q_1, \ldots, q_n)$, where $q_i = 1$ if $P \in D_i$, and $q_i = 0$ otherwise. By analogy to the geometric case, we will call the arithmetical graph (G_Q, M_Q, R_Q) the *blow-up* of (G, M, R) with respect to $P \in \mathcal{D}(M)$.

3.8. Let (G, M, R) be the arithmetical graph associated to the model $\mathcal{X}/\mathcal{O}_K$ of $X_0(p^r)/K$ described in [Edi1]. We construct a sequence of blow-ups (G_i, M_i, R_i) as follows. Let $(G_0, M_0, R_0) = (G, M, R)$.

- Let $\mathcal{D}(M_i) = \sqcup_{j=1}^{n} D_j$ denote a diagram associated to (G_i, M_i, R_i). Let $P \in \mathcal{D}(M_i)$ be such that either
  (1) $P \in D_h \cap D_j$ for some $h \neq j$ and $c_{hj} > 1$, or
  (2) $P \in D_h \cap D_j \cap D_\ell$ for some distinct integers h, j, ℓ.
  Let $(G_{i+1}, M_{i+1}, R_{i+1})$ denote the arithmetical graph obtained as the blow-up of (G_i, M_i, R_i) at $P \in \mathcal{D}(M_i)$. If $\mathcal{D}(M_i)$ does not contain such a point P, then let $(G_{i+1}, M_{i+1}, R_{i+1}) = (G_i, M_i, R_i)$.

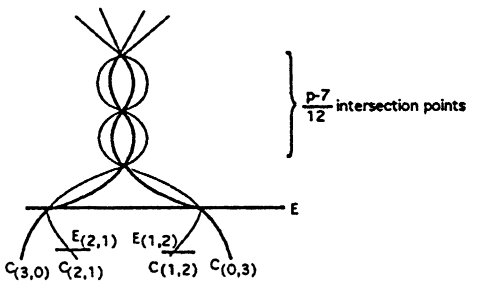
It is clear that there exists an integer i_0 such that $(G_j, M_j, R_j) = (G_{i_0}, M_{i_0}, R_{i_0})$ if $j \geqslant i_0$. We denote the arithmetical graph $(G_{i_0}, M_{i_0}, R_{i_0})$ by $(\overline{G}, \overline{M}, \overline{R})$. Since the arithmetical graph $(\overline{G}, \overline{M}, \overline{R})$ is obtained from (G, M, R) by a sequence of blow-ups, we find that $\Phi(G) = \Phi(\overline{G})$. We may now state a precise version of Claim 3.5.

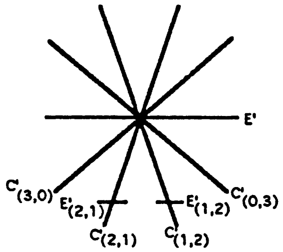
CLAIM 3.9. *Let $(\overline{G}, \overline{M}, \overline{R})$ be an arithmetical graph associated to $X_0(p^r)/K$ as* *in 3.8. If $p \equiv 1 \pmod{12}$, or if $p \equiv 7 \pmod{12}$, or if $p \equiv 5 \pmod{12}$ and r is even, or if $p = 5$, then the graph $\overline{G}$ is a tree. Moreover, the arithmetical graph $(\overline{G}, \overline{M}, \overline{R})$ satisfies Condition C_ℓ stated in [Lor2], 1.5, for all primes ℓ, $\ell \neq p$.*

Proof. The proof of this claim consists simply in exhibiting the graph $\overline{G}$ in each of the cases listed in the claim. We leave the verification that the graph $\overline{G}$ is a tree to the reader. An example of such a graph $\overline{G}$ is given below in Example 3.10. □

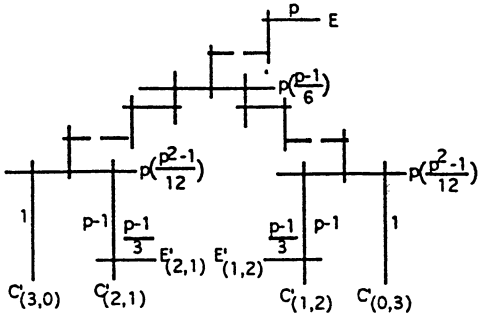
We may now conclude the proof of Theorem 3.2. It suffices to apply the results quoted in 3.1 to the arithmetical graph $(\overline{G}, \overline{M}, \overline{R})$ in all cases where $\overline{G}$ is a tree. We leave the details of the computations to the reader. □

EXAMPLE 3.10. Let us explicitly perform the computation of $(\overline{G}, \overline{M}, \overline{R})$ in the case where $p \equiv 7 \pmod{12}$ and $r = 3$, $p \neq 7$. The diagram $\mathcal{D}(\mathcal{X}_k)$ associated to the special fiber of the regular model $\mathcal{X}$ described by Edixhoven is pictured below on the left. The dual graph of the special fiber of $\mathcal{X}$ is not a tree, and the diagram $\mathcal{D}(\mathcal{X}_k)$ is not simply connected. The unique diagram associated to $M(\mathcal{X})$ is represented below on the right. (We denote by C' the "component" of $\mathcal{D}(M(\mathcal{X}))$ that corresponds to a component C in $\mathcal{X}_k$.)





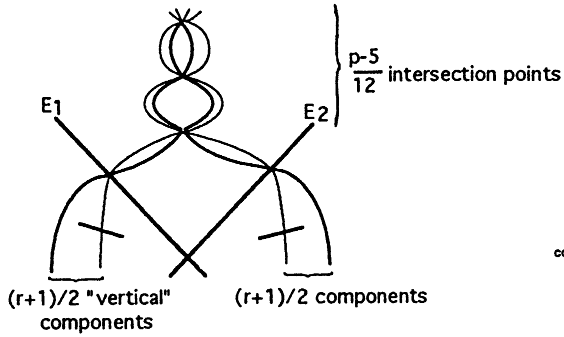
The procedure described in 3.8 calls for performing a sequence of blow-ups on this diagram to obtain the graph $(\overline{G}, \overline{M}, \overline{R})$ associated to $\mathcal{X}_k$. The new graph $\overline{G}$ is a tree. We represent below the unique diagram associated to $\overline{M}$, which is "tree-like." The multiplicities of the components indicated in the next diagram are the ones needed to compute the group Φ_{p^3} using the results recalled in 3.1.

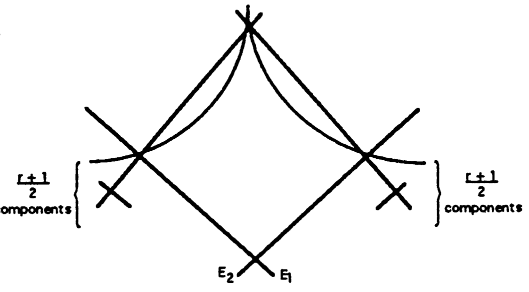


REMARK 3.11. The methods developed in this section to compute the groups Φ_{p^r} cannot be applied in the case $p \equiv 11 \pmod{12}$. The case where $p \equiv 5 \pmod{12}$, $p \neq 5$ and r odd, is already more difficult than the cases treated in Theorem 3.2, and will be treated below in Proposition 3.12 by an *ad hoc* method. However, the procedure used in Theorem 3.2 to compute $\Phi_N(p)$ when $N = p^r$ can also be successfully performed in many cases where $N = Dp^r$, and $D \neq 1$. Let x be a point of $Y_0(D)/\overline{\mathbf{F}_p}$. Such a point is represented by a pair $(E, \mathcal{C}_D)$, where E is an elliptic curve and $\mathcal{C}_D$ is a cyclic subgroup of order D. The automorphism group $\mathrm{Aut}_{\overline{\mathbf{F}}_p}(x)$ is the set of automorphisms $\sigma\colon E \to E$ such that $\sigma(\mathcal{C}_D) = \mathcal{C}_D$. Let s_4 and s_6 denote the number of supersingular points of $Y_0(D)/\overline{\mathbf{F}_p}$ whose automorphism groups have order 4 and 6, respectively. Both integers s_4 and s_6 depend on D (see the tables in [Edi2], 4.4.1). When $(s_4, s_6) = (1, 0)$ and r is even, or $(0, 0)$, or $(0, 1)$, the procedure 3.8 applied to the regular model of $X_0(Dp^r)/\mathbf{Q}_p$ successfully terminates in a tree $(\overline{G}, \overline{M}, \overline{R})$.

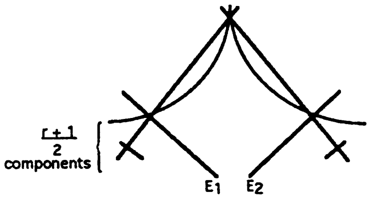
PROPOSITION 3.12. *Let $p \equiv 5 \pmod{12}$, $p \neq 5$, and let $r \geqslant 1$ be odd. Then* $|\Phi_{p^r}| = ab^{r-1}p^{2s^2}$.

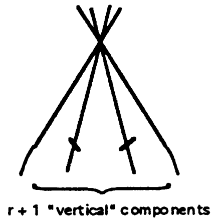
Proof. Let $\mathcal{X}/\mathcal{O}_K$ denote the model of $X_0(p^r)/K$ described in [Edi1]. The diagram $\mathcal{D}(\mathcal{X}_k)$ is represented below on the left. The diagram $\mathcal{D}(M(\mathcal{X}_k))$ associated to $M(\mathcal{X}_k)$ is represented below on the right. It is not simply connected.


E1
E2
$\frac{p-5}{12}$ intersection points
(r+1)/2 "vertical" components
(r+1)/2 components



Let (G, M, R) denote the arithmetical graph associated to $\mathcal{X}/\mathcal{O}_K$. We leave it to the reader to check that the procedure described in 3.8 does not terminate in a tree $(\overline{G}, \overline{M}, \overline{R})$ when applied to (G, M, R). We compute nevertheless $|\Phi_{p^r}|$ as follows. Since E_1 and E_2 have the same multiplicity in G (namely, $p^{(r-1)/2}$), we may use the construction described in [Lor1], 5.1, to compute $|\Phi(G)|$. Let (G_1, M_1, R_1) and (G_2, M_2, R_2) denote the two arithmetical graphs associated to (G, M, R) and to the pair of vertices (E_1, E_2) of G having same multiplicity. The graph G_1 is the graph obtained from G by removing the edge linking the vertices E_1 and E_2 in G. The graph G_2 is the graph obtained from G_1 by identifying the vertices E_1 and E_2. We proved in [Lor1], 5.1, that $|\Phi(G)| = |\Phi(G_1)| + |\Phi(G_2)|$. The drawing below on the left represents the diagram associated to M_1. In the new arithmetical graph G_1, the curves/vertices E_1 and E_2 have self-intersection (-1). We may therefore blow them down to get a new arithmetical graph (G'_1, M'_1, R'_1). The drawing below on the right represents the diagram associated to M'_1. Note that this diagram is simply connected.





CLAIM 3.13. *The procedure described in 3.8 applied to (G'_1, M'_1, R'_1) terminates in a tree $(\overline{G}'_1, \overline{M}'_1, \overline{R}'_1)$. Using the tree $\overline{G}'_1$ and the results quoted in 3.1, we find that*

$$|\Phi(G_1)| = |\Phi(G'_1)| = |\Phi(\overline{G}'_1)| = (2m+1)b^{r-1}p^{2s^2},$$

where $m = (p-5)/12$, and $r = 2s+1$. The proof of this claim is left to the reader.

CLAIM 3.14. *The diagram associated to M_2 is simply connected. The procedure described in 3.8 applied to (G_2, M_2, R_2) terminates in a tree $(\overline{G}_2, \overline{M}_2, \overline{R}_2)$. Using the tree $\overline{G}_2$ and the results quoted in 3.1, we find that $|\Phi(G_2)| = |\Phi(\overline{G}_2)| = mb^{r-1}p^{2s^2}$, where $m = (p-5)/12$ and $r = 2s+1$. The proof of this claim is left to the reader.*

To conclude the proof of Proposition 3.12, we note that $m + (2m+1) = (p-1)/4 = a$. Therefore, $|\Phi(G)| = |\Phi(G_1)| + |\Phi(G_2)| = ab^{r-1}p^{2s^2}$.

REMARK 3.15. Let $p \geqslant 5$ be a prime. Let $p^* := (-1)^{(p-1)/2}p$. Let $K = \mathbf{Q}_p^{\mathrm{unr}}$, and let K_2 denote the unique quadratic extension of K. Let

J'_{p^r} := torsion subgroup of $J_0(p^r)(\mathbf{Q}(\sqrt{p^*}))$.

C'_{p^r} := cuspidal subgroup of J'_{p^r}.

Φ'_{p^r} := group of components of the Néron model of $J_0(p^r)_{K_2}/K_2$.

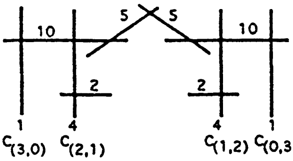
We believe that it is possible to determine a lower bound for the order of the p-part $(J'_{p^r})_p$ of the group J'_{p^r} using the 3-step method discussed in this article. For the convenience of the reader, we shall now briefly recall these three steps.

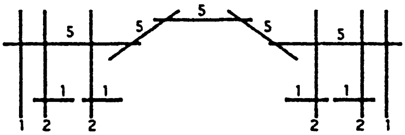
Step I: Describe a regular model over $\mathcal{O}_{K_2}$ of $X_0(p^r)_{K_2}/K_2$. Since $p \neq 2$, such a model can be obtained from an appropriate model of $X_0(p^r)/K$ by a process of "base change followed by normalization" (see for instance [Lor3], section 3). Step I presents no difficulty.

Step II: Compute Φ'_{p^r}. This step is more difficult than in the case of Φ_{p^r}.

Step III: Determine whether the reduction map $\pi'_{p^r|(C'_{p^r})_p}: (C'_{p^r})_p \to (\Phi'_{p^r})_p$ is surjective. As in Lemma 2.4, the reduction map $\pi'_{p^r|(C'_{p^r})_p}$ is surjective if the "vertical components" of the regular model of $X_0(p^r)/K_2$ generate $(\Phi'_{p^r})_p$.

EXAMPLE 3.16. The diagram below on the left represents the special fiber of a model of $X_0(5^3)/K$ over $\mathcal{O}_K$. All components are rational. The diagram below on the right represents the special fiber of the minimal model of $X_0(5^3)/K_2$ over $\mathcal{O}_{K_2}$. All components are again rational.





One easily computes that $\Phi_{5^3} \cong \mathbf{Z}/25\mathbf{Z}$ and $\Phi'_{5^3} \cong \mathbf{Z}/25\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$. It is likely that $(\Phi_{p^3})_p \cong \mathbf{Z}/p^2\mathbf{Z}$ and that $(\Phi'_{p^3})_p \cong \mathbf{Z}/p^2\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^2$ for all possible values of $p \geqslant 5$.

If $p = 5, 7$, or 13, then one finds that $|(\Phi'_{p^r})_p| = |(\Phi_{p^r})_p|^2$. Again, this equality is likely to hold for all values of $p \geqslant 5$.

4. Degeneracy maps and old subvarieties

Let $p \geqslant 5$ be a prime, and fix an integer $r \geqslant 1$. There exist two degeneracy maps

$$u_i(p^r) \colon X_0(p^r) \to X_0(p^{r-1}), \quad i = 0, 1.$$

Let $\mathcal{H}$ denote the upper halfplane. Let $\mathcal{H}^* = \mathcal{H} \sqcup \mathbf{P}^1(\mathbf{Q})$. When $X_0(p^r)$ is identified to the quotient $\mathcal{H}^*/\Gamma_0(p^r)$, the maps $u_0(p^r)$ and $u_1(p^r)$ are defined as follows:

$$u_i(p^r) \colon \mathcal{H}^*/\Gamma_0(p^r) \to \mathcal{H}^*/\Gamma_0(p^{r-1}),$$
$$z \mapsto p^i z.$$

These maps are defined over $\mathbf{Q}$ and can also be given the following modular interpretation. Let $E/\mathbf{C}$ be an elliptic curve and let G_{p^r} be a cyclic subgroup of $E(\mathbf{C})$ of order p^r. Let G_p and $G_{p^{r-1}}$ denote the unique subgroups of G_{p^r} of order p and p^{r-1}, respectively. The pair (E, G_{p^r}) represents a point of $Y_0(p^r)(\mathbf{C})$, and

$$u_0(p^r)(E, G_{p^r}) := (E, G_{p^{r-1}}),$$
$$u_1(p^r)(E, G_{p^r}) := (E/G_p, G_{p^r}/G_p).$$

Let $1 \leqslant h \leqslant r-1$. Define

$$v_{h,i}\colon X_0(p^r) \to X_0(p^h), \quad i = 0, \dots, r-h,$$

as follows:

$$\begin{aligned} v_{h,0} &:= u_0(p^{h+1}) \circ \cdots \circ u_0(p^r), \\ v_{h,i} &:= u_0(p^{h+1}) \circ \cdots \circ u_0(p^{r-i}) \circ u_1(p^{r-i+1}) \circ \cdots \circ u_1(p^r), \\ &\qquad i = 1, \dots, r-h-1, \\ v_{h,r-h} &:= u_1(p^{h+1}) \circ \cdots \circ u_1(p^r). \end{aligned}$$

Let $v_{h,i}^*\colon J_0(p^h) \to J_0(p^r)$ and $(v_{h,i})_*\colon J_0(p^r) \to J_0(p^h)$ denote the maps induced by functoriality on the Jacobians. The maps $v_{h,i}^*$ and $(v_{h,i})_*$ induce by functoriality natural maps on C_{p^h}, J_{p^h}, and Φ_{p^h}. In order to simplify our notations, we shall also denote the induced maps on C_{p^h}, J_{p^h}, and Φ_{p^h} by $v_{h,i}^*$ and $(v_{h,i})_*$. Let

$$\sigma_h\colon [J_0(p^h)]^{r-h+1} \to J_0(p^r),$$

$$(x_0, \dots, x_{r-h}) \mapsto \sum_{i=0}^{r-h} v_{h,i}^*(x_i).$$

We let $B_h/\mathbf{Q}$ denote the image of the map σ_h in $J_0(p^r)/\mathbf{Q}$. The map σ_h induces natural maps on $[J_{p^h}]^{r-h+1}$, $[C_{p^h}]^{r-h+1}$ and $[\Phi_{p^h}]^{r-h+1}$. We shall also denote the induced maps on $[J_{p^h}]^{r-h+1}$, $[C_{p^h}]^{r-h+1}$ and $[\Phi_{p^h}]^{r-h+1}$ by σ_h. Let us record here for future use that $B_1 \subset B_2$. Indeed, the map

$$\varphi\colon J_0(p)^r \to J_0(p^2)^{r-1},$$

$$\begin{aligned} (x_1, \dots, x_r) \mapsto\ & (u_0(p^2)^*(x_1) + \\ & + u_1(p^2)^*(x_2),\ u_1(p^2)^*(x_3), \dots, u_1(p^2)^*(x_n)) \end{aligned}$$

is such that $\sigma_1 = \sigma_2 \circ \varphi$.

LEMMA 4.1. *The map $v_{1,i}^*\colon \Phi_p \to \Phi_{p^r}$, $i = 0, 1$, is injective and, therefore, the group Φ_{p^r} contains a subgroup isomorphic to $\mathbf{Z}/a\mathbf{Z}$.*

Proof. The map $v_{1,i}\colon X_0(p^r) \to X_0(p)$ has degree p^{r-1}. Hence, the composition $(v_{1,i})_* \circ v_{1,i}^*$ on Φ_p is the multiplication by p^{r-1}. Since $\Phi_p \cong \mathbf{Z}/a\mathbf{Z}$ and since $\gcd(p, a) = 1$, our lemma follows. □

LEMMA 4.2. *The group Φ_{p^2} is cyclic of order ab. The cusp* $[0, 1] - [1, p^2]$ *in C_{p^2} reduces to a generator y of Φ_{p^2}.*

Proof. Directly compute Φ_{p^2} using Edixhoven's description of the special fiber of a regular model of $X_0(p^2)$ ([Edi1], 1.5). The reduction of $[0, 1] - [1, p^2]$ in Φ_{p^2}

is easy to compute using Lemma 2.4. □

THEOREM 4.3. *The map* σ_2: $[\Phi_{p^2}]^{r-1} \to \Phi_{p^r}$ *is injective when restricted to the b-part of* $[\Phi_{p^2}]^{r-1}$. *In particular, the group* Φ_{p^r} *contains a subgroup isomorphic to* $\mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$.

Proof. Let x denote the image in Φ_p, under the map π_p, of the element $[0, 1] - [1, p]$ of C_p. The element x is a generator of Φ_p. Let y be the reduction in Φ_{p^2} of the element $[0, 1] - [1, p^2]$ in C_{p^2}. The element y is a generator of Φ_{p^2}.

LEMMA 4.4. *Let* $0 \leqslant i, j \leqslant r-2$ *be two integers. Then, in the group* Φ_{p^2},

$$((v_{2,j})_* \circ v_{2,i}^*)(y) = \begin{cases} p^{r-2-(j-i)} u_1(p^2)^*(x) & \textit{if } j > i. \\ p^{r-2} y & \textit{if } j = i. \\ p^{r-2-(i-j)} u_0(p^2)^*(x) & \textit{if } j < i. \end{cases}$$

Proof. The explicit computation of $((v_{2,j})_* \circ v_{2,i}^*)(y)$ presents no difficulty and follows immediately from the definitions and the ramification properties of the maps $v_{2,i}$, $i = 0, \dots, r-2$. Unfortunately, this computation is rather tedious. We recall below only the ramification properties of the maps $u_i(p^r)$: $X_0(p^r) \to X_0(p^{r-1})$, $r \geqslant 2$, and we leave the proof of Lemma 4.4 to the reader. Let $[x, p^a]$ denote a cusp of $X_0(p^r)(\overline{\mathbf{Q}})$, with $a \leqslant r$, $\gcd(x, p^{\min(a,r-a)}) = 1$, and $0 \leqslant x < p^{\min(a,r-a)}$. Then

$$u_0(p^r)([x, p^a]) = \begin{cases} [x, p^a] & \text{if } 0 \leqslant a \leqslant (r-1)/2. \\ & \quad \text{This point is ramified,} \\ [x \,(\operatorname{mod} p^{r-a-1}),\, p^a] & \text{if } (r-1)/2 \leqslant a \leqslant r-1, \\ [1, p^{r-1}] & \text{if } a = r. \end{cases}$$

$$u_1(p^r)([x, p^a]) = \begin{cases} [0, 1] & \text{if } a = 0, \\ [x \,(\operatorname{mod} p^{a-1}),\, p^{a-1}] & \text{if } 1 \leqslant a < (r+1)/2, \\ [x, p^{a-1}] & \text{if } (r+1)/2 \leqslant a \leqslant r. \\ & \quad \text{This point is ramified.} \end{cases}$$ □

Let us now complete the proof of Theorem 4.3. Since $\gcd(a, b) = 1$, we find that an element of $[\Phi_{p^2}]^{r-1}$ of order dividing b is of the form $(ay_1, \dots, ay_{r-1})$ for some element $(y_1, \dots, y_{r-1}) \in [\Phi_{p^2}]^{r-1}$. Let τ denote the composition

$$[\Phi_{p^2}]^{r-1} \xrightarrow{\sigma_2 = \sum_{i=0}^{r-2} v_{2,i}^*} \Phi_{p^r} \xrightarrow{((v_{2,0})_*, \dots, (v_{2,r-2})_*)} [\Phi_{p^2}]^{r-1}.$$

Since both $u_0(p^2)^*(x)$ and $u_1(p^2)^*(x)$ have order equal to a in Φ_{p^2}, Lemma 4.4 shows that $\tau(ay_1, \dots, ay_{r-1}) = p^{r-2}(ay_1, \dots, ay_{r-1})$. Therefore, τ is equal to the multiplication by p^{r-2} when restricted to the b-part of $[\Phi_{p^2}]^{r-1}$. Since $\gcd(b, p) = 1$, the map τ is then an isomorphism when restricted to the b-part of $[\Phi_{p^2}]^{r-1}$. Therefore, Φ_{p^r} contains a subgroup isomorphic to $(\mathbf{Z}/b\mathbf{Z})^{r-1}$. Lemma 4.1 shows that Φ_{p^r} contains a subgroup isomorphic to $\mathbf{Z}/a\mathbf{Z}$. Hence, since $\gcd(a, b) = 1$, our theorem follows. □

COROLLARY 4.5. *Let $p \geqslant 5$ be a prime and let $N = p^r$. Assume that $|\Phi_{p^r}^{(p)}| = ab^{r-1}$. Then $\Phi_{p^r}^{(p)} \cong \mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$, and the reduction map π: $C_{p^r}^{(p)} \to \Phi_{p^r}^{(p)} \cong \mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$ is surjective. In particular, π is surjective when $p \not\equiv 11 \pmod{12}$.*

Proof. Since $\Phi_{p^r}^{(p)}$ has order ab^{r-1} and contains a subgroup isomorphic to $\mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$, we find that $\Phi_{p^r}^{(p)} \cong \mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$. It follows from Lemma 4.1 and from the commutativity of the diagram

$$\begin{tikzcd}
C_p \arrow[r, "v_{1,0}^*"] \arrow[d] & C_{p^r} \arrow[d] \\
\Phi_p \arrow[r, "v_{1,0}^*"] & \Phi_{p^r}
\end{tikzcd}$$

that the a-part of Φ_{p^r} is in the image of C_{p^r}. It follows from Lemma 4.2, Theorem 4.3, and from the commutativity of the diagram

$$\begin{tikzcd}
{[C_{p^2}]^{r-1}} \arrow[r, "\sigma_2"] \arrow[d] & C_{p^r} \arrow[d] \\
{[\Phi_{p^2}]^{r-1}} \arrow[r, "\sigma_2"] & \Phi_{p^r}
\end{tikzcd}$$

that the b-part of Φ_{p^r} is in the image of C_{p^r}.

Theorem 3.2 and Proposition 3.12 imply, when $p \not\equiv 11 \pmod{12}$, that $|\Phi_{p^r}^{(p)}| = ab^{r-1}$. This concludes the proof of Corollary 4.5. □

THEOREM 4.6. *Let $p \geqslant 5$ be a prime. Assume that $p \not\equiv 11 \pmod{12}$. Then*

$$C_{p^r}^{(2p)} = J_{p^r}^{(2p)} \cong \textit{prime-to-2 part of } (\mathbf{Z}/a\mathbf{Z})^r \times (\mathbf{Z}/b\mathbf{Z})^{r-1}.$$

Proof. Let $\mathcal{J}_0(p^h)/\mathbf{Z}_p$ denote the Néron model of $J_0(p^h)/\mathbf{Q}_p$. The map

$$\sigma_h\colon [J_0(p^h)]^{r-h+1} \to J_0(p^r)$$

extends to a map of the respective Néron models, again denoted by σ_h. The connected component of zero of the special fiber of $\mathcal{J}_0(p^h)$ contains a maximal torus $\mathcal{T}(p^h)/\mathbf{F}_p$. We let

$$\overline{\sigma}_h\colon [\mathcal{T}(p^h)]^{r-h+1} \dot{\to} \mathcal{T}(p^r)$$

denote the map induced by σ_h. The dimension of the torus $\mathcal{T}(p^h)$ can be computed explicitly (e.g., [Lor4], proof of Theorem 1). One finds that $\dim(\mathcal{T}(p^r)) = r\dim(\mathcal{T}(p))$. Since the map σ_1 has finite kernel (e.g., [Lor4], Proposition 4), we find that $\overline{\sigma}_1\colon [\mathcal{T}(p)]^r \to \mathcal{T}(p^r)$ has finite kernel and, hence, is surjective.

4.7. Let $x \in J_0(p^r)(\mathbf{Q}_p)$ be a torsion point of order prime to p such that its image under the canonical reduction map

$$\pi_{p^r}\colon J_0(p^r)(\mathbf{Q}_p) \to \mathcal{J}_0(p^r)_{\mathbf{F}_p}(\mathbf{F}_p)$$

is in $\mathcal{T}(p^r)(\mathbf{F}_p)$. Let $y \in [\mathcal{T}(p)]^r(\overline{\mathbf{F}_p})$ be such that $\overline{\sigma}_1(y) = \pi_{p^r}(x)$. Then there exist a finite unramified extension $M/\mathbf{Q}_p$ and a torsion point $z \in [J_0(p)]^r(M)$, of order prime to p, such that $(\pi_p)^r(z) = y$. Since the map π_{p^r} is injective when restricted to the prime-to-p torsion of $J_0(p^r)(\mathbf{Q}_p)$, we find that $\sigma_1(z) = x$, and, therefore, $x \in \sigma_1([J_0(p)]^r) = B_1$.

4.8. Let $u \in J_{p^r}^{(p)}$. When the map $\pi_{p^r}\colon C_{p^r}^{(p)} \to \Phi_{p^r}^{(p)}$ is surjective, we can find $c \in C_{p^r}^{(p)}$ such that $\pi_{p^r}(u-c) \in \mathcal{T}(p^r)(\mathbf{F}_p)$. Let $x := u - c$. Note that, since u and c belong to $J_0(p^r)(\mathbf{Q})$, so does x. It follows from our previous discussion that $x \in B_1(\mathbf{Q})$ and, therefore

$$u = x + c \in B_1(\mathbf{Q})_{\text{tors}}^{(p)} + C_{p^r}.$$

(If A/K is any abelian variety, then we denote by $A(K)_{\text{tors}}$ the torsion subgroup of $A(K)$.) Since Mazur [Maz], Theorem 1, has shown that $J_p^{(p)} = C_p$, we find that, when the map $\sigma_1\colon [J_p^{(p)}]^r \to B_1(\mathbf{Q})_{\text{tors}}^{(p)}$ is surjective, then $B_1(\mathbf{Q})_{\text{tors}}^{(p)} \subseteq C_{p^r}$. Hence, $u \in C_{p^r}$, and $C_{p^r}^{(p)} = J_{p^r}^{(p)}$. Similarly, if the map $\sigma_1\colon [J_p^{(2p)}]^r \to B_1(\mathbf{Q})_{\text{tors}}^{(2p)}$ is surjective, then $C_{p^r}^{(2p)} = J_{p^r}^{(2p)}$. Under the hypothesis that $p \not\equiv 11 \pmod{12}$, Corollary 4.5 implies that the map $\pi_{p^r}\colon C_{p^r}^{(p)} \to \Phi_{p^r}^{(p)}$ is surjective. Let us now show that the map $\sigma_1\colon [J_p^{(2p)}]^r \to B_1(\mathbf{Q})_{\text{tors}}^{(2p)}$ is an isomorphism.

4.9. Let Σ denote the Shimura subgroup of $J_0(p)$. Ling [Lin], Theorem 2, has shown that

$$\operatorname{Ker}(\sigma_1)(\overline{\mathbf{Q}}) = \left\{(x_1,\dots,x_r) | x_i \in \Sigma(\overline{\mathbf{Q}}),\ \forall i = 1,\dots,r, \text{ and } \sum_{i=1}^{r} x_i = 0\right\}.$$

Let $\mathcal{K}$ denote the prime-to-2 part of $\mathrm{Ker}(\sigma_1)(\overline{\mathbf{Q}})$. Let $\mathcal{Q}$ denote the prime-to-2 part of the subgroup $\sigma_1^{-1}(B_1(\mathbf{Q})^{(2p)}_{\mathrm{tors}})$ of $J_0(p)^r(\overline{\mathbf{Q}})$. The following sequence of finite $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules is exact:

$$(0) \to \mathcal{K} \to \mathcal{Q} \xrightarrow{\sigma_1} B_1(\mathbf{Q})^{(2p)}_{\mathrm{tors}} \to (0).$$

We claim that the group $\mathcal{Q}$ is contained in the group $(\Sigma(\overline{\mathbf{Q}})^{(2)} \oplus C_p^{(2)})^r$. Let $\mathbf{T}$ denote the subring of $\mathrm{End}_{\mathbf{Q}}(J_0(p))$ generated by the Hecke operators T_ℓ of $J_0(p)$, ℓ prime, $\ell \neq p$, and by the involution $w = w_p$. Let $\mathcal{I}$ denote the ideal of $\mathbf{T}$ generated by the elements $w+1$ and $T_\ell - (\ell+1)$, $\ell \neq p$. The algebra $\mathbf{T}$ is called the Hecke algebra, and the ideal $\mathcal{I}$ is called the Eisenstein ideal. The algebra $\mathbf{T}$ acts in a natural way on $J_0(p)^r$. Let us show that, for all $\eta \in \mathcal{I}$, $\eta(\mathcal{Q}) = 0$ (i.e. that the finite group $\mathcal{Q}$ is in the kernel of the Eisenstein ideal). It is well-known that the Shimura subgroup is contained in the kernel of $\mathcal{I}$ (see for instance [Maz], II, 11.7). Let $\ell \neq p$ be any prime. Since $T_\ell(\mathcal{K}) \subseteq \mathcal{K}$, we find that the endomorphism T_ℓ of $\mathcal{Q}$ induces a map φ_ℓ on $B_1(\mathbf{Q})^{(2p)}_{\mathrm{tors}}$. It is easy to show that the map φ_ℓ is equal to the restriction to $B_1(\mathbf{Q})^{(2p)}_{\mathrm{tors}}$ of the Hecke operator T_ℓ of $J_0(p^r)$. The Jacobian $J_0(p^r)/\mathbf{Q}_\ell$ has good reduction modulo ℓ. Let $J_0(p^r)/\mathbf{F}_\ell$ denote the special fiber of the Néron model of $J_0(p^r)/\mathbf{Q}_\ell$ over $\mathbf{Z}_\ell$. Let Frob_ℓ and $\mathrm{Frob}_\ell^\#$ denote the Frobenius endomorphism of $J_0(p^r)/\mathbf{F}_\ell$ and its dual. The Eichler–Shimura relation states that the reduction of $(\ell+1-T_\ell)$ modulo ℓ is equal to the endomorphism $(1-\mathrm{Frob}_\ell^\#)(1-\mathrm{Frob}_\ell)$ of $J_0(p^r)/\mathbf{F}_\ell$. In particular, this relation shows that $\forall\, x \in J_0(p^r)(\mathbf{Q})^{(p)}_{\mathrm{tors}}$, $(\ell+1-T_\ell)(x) = 0$. Hence, $(\ell+1-T_\ell)(B_1(\mathbf{Q})^{(2p)}_{\mathrm{tors}}) = \{0\}$. Since $T_\ell - (\ell+1)$ kills both $\mathcal{K}$ and $B_1(\mathbf{Q})^{(2p)}_{\mathrm{tors}}$, and since the action of $T_\ell - (\ell+1)$ commutes with the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, we conclude that $T_\ell - (\ell+1)$ induces a map t_ℓ from $B_1(\mathbf{Q})^{(2p)}_{\mathrm{tors}}$ to $\mathcal{K}^{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}$. The map $T_\ell - (\ell+1)$ kills $\mathcal{Q}$ if and only if t_ℓ is the zero map. The group $\Sigma(\overline{\mathbf{Q}})$ has been computed in general in [L-O]. It follows from Corollary 1 to Theorem 2 in [L-O] that $\Sigma(\mathbf{Q})$ is trivial if a is odd, and equal to $\mathbf{Z}/2\mathbf{Z}$ if a is even. Therefore, since $\mathcal{K} \subseteq (\Sigma(\overline{\mathbf{Q}})^{(2)})^r$, we conclude that $\mathcal{K}^{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}$ is trivial, and that $T_\ell - (\ell+1)$ kills $\mathcal{Q}$ for all $\ell \neq p$.

Since the order of $\mathcal{Q}$ is odd, we find that $\mathcal{Q} = \mathrm{Ker}(w+1) \oplus \mathrm{Ker}(w-1)$. Mazur has shown in [Maz], II, proof of 14.1, that the ideal generated in $\mathbf{T}$ by the elements $w-1$, $T_\ell - (\ell+1)$, $\ell \neq p$, and a prime $q \neq 2$, is the unit ideal in $\mathbf{T}$. It follows then that $\mathrm{Ker}(w-1) = \{0\}$. Hence, the group $\mathcal{Q}$ is killed by the Eisenstein ideal. Therefore, it follows from Mazur's Theorem ([Maz], II, 16.4) that $\mathcal{Q} \subseteq (\Sigma(\overline{\mathbf{Q}})^{(2)} \oplus C_p^{(2)})^r$.

Let us now show that $\mathcal{Q}$ is isomorphic to $\mathcal{K} \oplus (C_p^{(2)})^r$. We have shown already that $\mathcal{Q} \subseteq (\Sigma(\overline{\mathbf{Q}})^{(2)} \oplus C_p^{(2)})^r$. Let $\tau \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and denote by x^τ the action of τ on a point $x \in J_0(p^i)$. Let $(x_1, \dots, x_r) \in (\Sigma(\overline{\mathbf{Q}})^{(2)})^r$ be such that $\sigma_1(x_1, \dots, x_r) \in B_1(\mathbf{Q})^{(2p)}_{\mathrm{tors}}$. Then

$$\forall\, \tau \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \quad (x_1^\tau - x_1, \dots, x_r^\tau - x_r) \in \mathrm{Ker}(\sigma_1)(\overline{\mathbf{Q}}).$$

Hence,

$$\sum_{i=1}^{r}(x_i^r - x_i) = 0 = \left(\sum_{i=1}^{r} x_i\right)^r - \left(\sum_{i=1}^{r} x_i\right).$$

It follows that $\Sigma_{i=1}^{r} x_i \in \Sigma(\mathbf{Q})$. Therefore, since $|\Sigma(\mathbf{Q})| \leqslant 2$, we find that the order of $\sigma_1(x_1, \dots, x_r) \in B_1^{(2)}(\mathbf{Q})$ must divide 2. Hence, $\sigma_1(x_1, \dots, x_r) = 0$, and $(x_1, \dots, x_r) \in \mathcal{K}$. In particular, $\mathcal{Q} = \mathcal{K} \oplus (C_p^{(2)})^r$, and the map $\sigma_1\colon (C_p^{(2)})^r \to B_1(\mathbf{Q})_{\text{tors}}^{(2p)}$ is bijective.

To prove that when $p \not\equiv 11 \pmod{12}$, the group $J_{p^r}^{(2p)}$ is isomorphic to the prime-to-2 part of $(\mathbf{Z}/a\mathbf{Z})^r \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$, we proceed as follows. It follows from our hypothesis on p that the group $\Phi_{p^r}^{(p)}$ is isomorphic to $\mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$, and that the reduction map $\pi_{p^r}\colon C_{p^r}^{(p)} \to \Phi_{p^r}^{(p)}$ is surjective. Let $x_1, \dots, x_{r-1}$ be elements in C_{p^r} such that the $b^{(2)}$-part of $\Phi_{p^r}^{(2p)}$ is generated by $\pi_{p^r}(x_1), \dots, \pi_{p^r}(x_{r-1})$. Write the order of x_i as $d_i b^{(2)}$. Without loss of generality, we may assume that d_i is divisible only by primes that divide $b^{(2)}$. Since $x_i^{b^{(2)}}$ belongs to the kernel of π_{p^r} and since $\gcd(d_i, 2p) = 1$, 4.7 shows that $x_i^{b^{(2)}} \in B_1(\mathbf{Q})_{\text{tors}}^{(2p)}$. We showed in 4.9 that the order of $B_1(\mathbf{Q})_{\text{tors}}^{(2p)}$ is prime to $b^{(2)}$. Hence, $d_i = 1$. We may therefore assume that $x_1, \dots, x_{r-1}$ have exact order $b^{(2)}$. Let $y \in B_1(\mathbf{Q})_{\text{tors}}^{(2p)}$ be an element of exact order $a^{(2)}$ such that the $a^{(2)}$-part of $\Phi_{p^r}^{(2p)}$ is generated by $\pi_{p^r}(y)$. Lemma 4.1 shows that such an element y exists. Every element of $J_{p^r}^{(2p)}$ can be written as the sum of an element u belonging to the subgroup generated by $x_1, \dots, x_{r-1}$, y, and of an element z such that $\pi_{p^r}(z) \in \mathcal{T}(p^r)(\mathbf{F}_p)$. Such an element z belongs to $B_1(\mathbf{Q})$ (see 4.7). Hence, $J_{p^r}^{(2p)}$ is generated by $B_1(\mathbf{Q})_{\text{tors}}^{(2p)}$ and the elements $x_1, \dots, x_{r-1}$. Since $\gcd(a, b) = 1$, our claim follows. This concludes the proof of Theorem 4.6. □

COROLLARY 4.10. *Let $p \geqslant 5$ be a prime. Assume that $p \not\equiv 11 \pmod{12}$. Then $J_{p^r}^{(p)} = B_2(\mathbf{Q})_{\text{tors}}^{(p)}$. Moreover, $J_{p^r}^{(p)}$ is killed by $24ab = p^2 - 1$.*

Proof. Let $u \in J_{p^r}^{(p)}$. Since the map $\pi_{p^r}\colon C_{p^r}^{(p)} \to \Phi_{p^r}^{(p)}$ is surjective, we can find $c \in C_{p^r}^{(p)}$ such that $\pi_{p^r}(u - c) \in \mathcal{T}(p^r)(\mathbf{F}_p)$. Let $x := u - c$. We can find $c_a \in \sigma_1([C_p]^r)$, or order a, and $c_b \in \sigma_2([C_{p^2}]^{r-1})$, of order b, such that $\pi_{p^r}(c - c_a - c_b) \in \mathcal{T}(p^r)(\mathbf{F}_p)$. Write $c' := c - c_a - c_b$. The discussion in 4.7 shows that c' and $x := u - c$ belong to $B_1(\mathbf{Q})$. Hence, since $B_1 \subset B_2$, $u = x + c_a + c_b + c'$ belongs to $B_2(\mathbf{Q})$. We have thus shown that $J_{p^r}^{(p)} \subset B_2(\mathbf{Q})$. To conclude the proof of Corollary 4.10, note first that, by construction, $c_a + c_b$ is killed by $ab = (p^2 - 1)/24$. We are going to show below that $x + c'$ is killed by $p^2 - 1$. It will follow then that $J_{p^r}^{(p)}$ is killed by $p^2 - 1$.

We can obtain a bound for the order of an element z of $J_{p^r}^{(p)}$ such that $\pi_{p^r}(z) \in \mathcal{T}(p^r)(\mathbf{F}_p)$ by using a theorem of Ling ([Lin], Theorem 1), which states that the map $\overline{\sigma}_1\colon [\mathcal{T}(p)]^r \to \mathcal{T}(p^r)$ is injective. It follows then that $\overline{\sigma}_1$ is an isomorphism of schemes and, therefore, the order of z divides the order of $\mathcal{T}(p)(\mathbf{F}_p)$.

The group $\mathcal{T}(p)$ is described as follows in [Ray], page 14. Let $\mathcal{X}/\mathbf{Z}_p$ denote the stable normal model of $X_0(pD)/\mathbf{Q}_p$. The special fiber $\mathcal{X}_{\mathbf{F}_p}/\mathbf{F}_p$ is the union of two copies of the modular curve $X_0(D)/\mathbf{F}_p$. Let x_j, $j \in J$, denote the singular points of $\mathcal{X}_{\mathbf{F}_p}/\mathbf{F}_p$ (which correspond to supersingular points on the two copies of $X_0(D)$). Let $k_j/\mathbf{F}_p$ denote the residue field of x_j. Then the group $\mathcal{T}(p)/\mathbf{F}_p$ is described by an exact sequence

$$(1) \to \mathbf{G}_m \to \prod_{j\in J} R_{k_j/\mathbf{F}_p}\mathbf{G}_m \to \mathcal{T}(p) \to (1),$$

where $R_{k_j/\mathbf{F}_p}\mathbf{G}_m$ denotes the Weil restriction of the multiplicative group $\mathbf{G}_m$ from k_j to $\mathbf{F}_p$. In particular, $R_{k_j/\mathbf{F}_p}\mathbf{G}_m(\mathbf{F}_p) = \mathbf{G}_m(k_j)$. Since $H^1(\mathrm{Gal}(\overline{\mathbf{F}_p}/\mathbf{F}_p), \mathbf{G}_m) = (0)$, we conclude that the sequence of $\mathbf{F}_p$-rational points of the above group schemes

$$(1) \to \mathbf{F}_p^* \to \prod_{j\in J} k_j^* \to \mathcal{T}(p)(\mathbf{F}_p) \to (1)$$

is exact. Since the j-invariant of a supersingular elliptic curve belongs to $\mathbf{F}_{p^2}$, we find that $k_j = \mathbf{F}_p$ or $\mathbf{F}_{p^2}$ and, hence, the exponent of $\mathcal{T}(p)(\mathbf{F}_p)$ divides $p^2 - 1$. We conclude then that the order of $z \in J_0(p^r)(\mathbf{Q}_p)$ divides $p^2 - 1$. □

COROLLARY 4.11. *Assume that* $p = 5$, 7, *or* 13, *so that* $X_0(p)$ *has genus zero. Then* $C_{p^r}^{(p)} = J_{p^r}^{(p)} \cong (\mathbf{Z}/b\mathbf{Z})^{r-1}$, *and the natural reduction map* $\pi_{p^r}^{(p)}\colon J_{p^r}^{(p)} \to \Phi_{p^r}^{(p)}$ *is an isomorphism, for all* $r \geqslant 1$.

Proof. Corollary 4.5 shows, when $p = 5$, 7 or 13, that the map π_{p^r} is surjective, and that $\Phi_{p^r}^{(p)}$ is isomorphic to $\mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$. Note that for these three values of p, the associated integer a is equal to 1. Since $J_0(p)$ is trivial when $p = 5, 7$, or 13, we conclude that $B_1(\mathbf{Q})_{\text{tors}}^{(p)} = \{0\}$. We may therefore apply 4.8 to find that $C_{p^r}^{(p)} = J_{p^r}^{(p)}$. Since the reduction map π_{p^r} is injective when restricted to $J_{p^r}^{(p)}$, we conclude that $J_{p^r}^{(p)} \cong \Phi_{p^r}^{(p)}$. □

REMARK 4.12. The map $\pi_{p^r}\colon J_{p^r} \to \Phi_{p^r}$ is not injective in general. For instance, when $p \equiv 7 \pmod{12}$, the group $\mathrm{Ker}(\pi_{p^r})$ contains a subgroup isomorphic to $(\mathbf{Z}/a\mathbf{Z})^{r-1}$.

References

[BLR] S. Bosch, W. Lütkebohmert, and M. Raynaud, Néron Models, Springer Verlag, 1990.

[Edi1] B. Edixhoven, Minimal resolution and stable reduction of $X_0(N)$, *Ann. Inst. Fourier* 40, 1 (1990), 31–67.

[Edi2] B. Edixhoven, L'action de l'algèbre de Hecke sur le groupe des composantes des Jacobiennes des courbes modulaires est "Eisenstein", in *Astérisque* 196–197 (1991), 159–170.

[Kat] N. Katz, Galois properties of torsion points on abelian varieties, *Inv. Math.* 62 (1981), 481-502.

[K-M] N. Katz and B. Mazur, Arithmetic moduli of elliptic curves, Princeton University Press, 1985.

[Lin] S. Ling , Congruences between cusps forms and the geometry of Jacobians of modular curves, *Math. Ann.* 295 (1993), 111–133.

[L-O] S. Ling and J. Oesterlé, The Shimura subgroup of $J_0(N)$, in *Astérisque* 196–197 (1991), 171–203.

[Lor1] D. Lorenzini, Arithmetical graphs, *Math. Ann.* 285 (1989), 481–501.

[Lor2] D. Lorenzini, Jacobians with potentially good ℓ-reduction, *J. Reine Angew. Math.* 430 (1992), 151–177.

[Lor3] D. Lorenzini, The characteristic polynomial of a monodromy transformation attached to a family of curves, *Comment. Math. Helvetici* 68 (1993), 111–137.

[Lor4] D. Lorenzini, On the Jacobian of the modular curve $X_0(N)$, Preprint (1993).

[Man] Y. Manin, Parabolic points and zeta functions of modular curves, *Math. USSR Izvestija* 6 (1972), n° 1.

[Maz] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. I.H.E.S.* 47 (1977), 33–172.

[Ma-Ra] R. Mazur and M. Rapoport, Behavior of the Néron model of the Jacobian of $X_0(N)$ at bad primes, *Publ. I.H.E.S.* 47 (1977), 173–185.

[Ogg1] A. Ogg, Rational points on certain elliptic modular curves, Proceedings of Symposia in Pure Mathematics 24, *American Mathematical Society*, 1973.

[Ogg2] A. Ogg, Hyperelliptic modular curves, *Bull. Soc. Math. France* 102 (1974), 449–462.

[Pou] D. Poulakis, La courbe modulaire $X_0(125)$ et sa jacobienne, *J. Number Theory* 25 (1987), 112–131.

[Ray] M. Raynaud, Jacobienne des courbes modulaires et opérateurs de Hecke, in *Astérisque* 196–197 (1991), 9–25.