J. Fac. Sci. Univ. Tokyo
Sect. IA, Math.
33 (1986), 441-466.

Rational points on the modular curves $X_0^+(p^r)$

By Fumiyuki MOMOSE

(Communicated by Y. Ihara)

Let $N \geqq 1$ be an integer and $X_0(N)$ be the modular curve defined over $\boldsymbol{Q}$ which corresponds to the modular group $\Gamma_0(N)$. The fundamental involution w_N of $X_0(N)$ is represented by the matrix $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Let $X_0^+(N)$ denote the quotient $X_0(N)/\{1, w_N\}$. All the $\boldsymbol{Q}$-rational points on $X_0(N)$ were determined [14] [5, 6, 7, 8] [15]. In this paper, we discuss the $\boldsymbol{Q}$-rational points on $X_0^+(p^r)$ for prime numbers p and integers $r \geqq 2$. When $r=2$, $X_0^+(p^2)$ is isomorphic to the modular curve $X_{\mathrm{split}}(p)$ cf. §1, [13] [16]. The author [16] discussed the $\boldsymbol{Q}$-rational points on $X_{\mathrm{split}}(p)$. The same idea as in [16] can be applied to the modular curves $X_0^+(p^r)$ for $r \geqq 2$ with genus $g_0^+(p^r) > 0$. For such a modular curve $X_0(p^r)$, the set of the $\boldsymbol{Q}$-rational points consists of only cusps [14] [7, 8] [15]. On the other hand, there are $\boldsymbol{Q}$-rational points of $X_0^+(p^r)$ which are represented by elliptic curves with complex multiplication. We call them the C. M. points. Let $n(p, r)$ denote the number of the $\boldsymbol{Q}$-rational points on $X_0^+(p^r)$ which are neither the cusps nor the C. M. points. We make use of quotients ($\neq\{0\}$) of the jacobian varieties $J_0^+(p^r)$ of $X_0^+(p^r)$ whose Mordell-Weil groups are of finite order. Let $J_0(p^r)$ be the jacobian variety of the modular curve $X_0(p^r)$. Then the quotient $J_0^-(p^r) = J_0(p^r)/(1+w_{p^r})J_0(p^r)$ becomes naturally a quotient of $J_0^+(p^{r+1})$ cf. §1 (1.2). Then our main result is as follows.

THEOREM (0.1). *Let p be a prime number and $r \geqq 2$ be an integer with $g_0^+(p^r) > 0$. Then $n(p, r) = 0$ for $p = 2$, 3, 7, 11, and $p \geqq 17$ with $\sharp J_0^-(p)(\boldsymbol{Q}) < \infty$.*

For the prime numbers p, $17 \leqq p < 300$, except for $p = 151$, 199, 227 and 277, it is known that $\sharp J_0^-(p)(\boldsymbol{Q}) < \infty$ [12] p. 40, [24] Table 5 pp. 135–141. For $p = 5$ and 13, we do not know whether the Mordell-Weil groups of $J_0^-(125)$ and $J_0^-(169)$ are finite or not (cf. [2]). The proof of main theorem above is essentially same as in [16]. One of the key steps is as follows. Let $\mathscr{X}_0(p^r)$ be the normalization of the projective j-line $\mathscr{X}_0(1) \simeq \boldsymbol{P}^1_{\boldsymbol{Z}}$ in

the function field of $X_0(p^r)$. Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(p^r)$ with $g_0^+(p^r)>0$, and $x, x'=w_{p^r}(x)$ be the sections of the fibre of $X_0(p^r)$ at y. Then x, x' are not defined over $\boldsymbol{Q}$ [14] [7, 8] [15], so they are defined over a quadratic field k. Let $\mathfrak{p}$ be a prime of k lying over the rational prime p.

THEOREM (0.2). *Under the notation as above, $x\otimes\kappa(\mathfrak{p})$ and $x'\otimes\kappa(\mathfrak{p})$ are the sections of the smooth part $\mathscr{X}_0(p^r)^{\mathrm{smooth}}$ of $\mathscr{X}_0(p^r)$.*

The first two sections are preparations of the last section. In the first section, we give a review of the results on the modular curves $\mathscr{X}_0(p^r)$. In the second section, we prepare lemmas on elliptic curves. In the last section, we prove main theorem etc., and also give some related results.

Notation. For a prime number q, $\boldsymbol{Z}_q$, $\boldsymbol{Q}_q$ and $\boldsymbol{Q}_q^{ur}$ denote respectively the ring of q-adic integers, the q-adic completion of $\boldsymbol{Q}$ and the maximal unramified extension of $\boldsymbol{Q}_q$. Let K be a finite extension of $\boldsymbol{Q}$, $\boldsymbol{Q}_q$ or $\boldsymbol{Q}_q^{ur}$, and A be an abelian variety defined over K. Then $\mathscr{O}_K$ denotes the ring of integers of K, and $A_{/\mathscr{O}_K}$ denotes the Néron model of A over the base $\mathscr{O}_K$. Further $(A_{/\mathscr{O}_K}\otimes\bar{\boldsymbol{F}}_q)^0$ is the connected component of the unit section of the special fibre $A_{/\mathscr{O}_K}\otimes\bar{\boldsymbol{F}}_q$. For a quasi-finite flat group scheme $G/\mathscr{O}_K$, G^0 denotes the connected component of the unit section. For a subscheme Y of a modular curve $/\boldsymbol{Z}$, Y^h denotes the open subscheme of Y obtained by excluding the supersingular points on $Y\otimes\boldsymbol{F}_p$ for a fixed prime number p.

§1. Modular curves $X_0(p^r)$.

Let p be a prime number, $r\geqq 1$ be an integer and $X_0(p^r)$ be the modular curve $/\boldsymbol{Q}$ corresponding to the modular group $\Gamma_0(p^r)$. Then $X_0(p^r)$ is the coarse moduli space $/\boldsymbol{Q}$ of the generalized elliptic curves E with a cyclic subgroup A of order p^r [3]. The fundamental involution w_{p^r} of $X_0(p^r)$ is defined by the functor

$$(E, A)\longmapsto(E/A, E_{p^r}/A),$$

where $E_{p^r}=\ker(p^r: E\to E)$. Let $X_0^+(p^r)$ denote the quotient $X_0(p^r)/\langle w_{p^r}\rangle$. For the following pairs (p, r) $(r\geqq 2)$, $X_0^+(p^r)$ are not projective line:

p	r
2	$\geqq 6$

(1.0)
$$\begin{array}{rr} p & r \\ 3 & \geqq 4 \\ 5 & \geqq 3 \\ 7 & \geqq 3 \\ p \geqq 11 & \geqq 2. \end{array}$$

We know the following result.

THEOREM (1.1) ([14] [7, 8] [15]). *The rational points on* $X_0(p^r)$ *must be the cusps for any pair* (p, r) *in* (1.0).

There exists a covering of $X_0^+(p^{r+2})$ to $X_0^+(p^r)$, which is induced by the morphism of $X_0(p^{r+2})$ to $X_0(p^r)$ defined by

$$(E, A) \longmapsto (E/A, A_{p^{r+1}}/A_p) ,$$

where A_{p^i} is the unique cyclic subgroup of A of order p^i. Let $X_s(p^t) = X_{\mathrm{sp,Car}}(p^t)$ be the modular curve $/\boldsymbol{Q}$ which corresponds to the modular group

$$\Gamma_s(p^t) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \boldsymbol{SL}_2(\boldsymbol{Z}) \mid b \equiv c \equiv 0 \bmod p^t \right\}.$$

Then $X_s(p^t)$ is the coarse moduli space $/\boldsymbol{Q}$ of the generalized elliptic curves E with independent cyclic subgroups C_1 and C_2 of order p^t. The fundamental involution $w = w(p^t)$ of $X_s(p^t)$ is defined by

$$(E, C_1, C_2) \longmapsto (E, C_2, C_1).$$

Let $X_s^n(p^t) = X_{\mathrm{split}}(p^t)$ be the quotient $X_s(p^t)/\langle w \rangle$, which corresponds to the modular group $\left\langle \Gamma_s(p^t), \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$. There exists a canonical isomorphism $(/\boldsymbol{Q})$ of $X_0(p^{2t})$ (resp. $X_0^+(p^{2t})$) to $X_s(p^t)$ (resp. $X_s^n(p^t)$) defined by

$$(E, A) \longmapsto (E/A_{p^t}, A/A_{p^t}, E_{p^t}/A_{p^t}).$$

For even integers $r \geqq 2$, we will make use of this isomorphism.

Let $J_0(p^r)$, $J_0^+(p^r)$ be the jacobian varieties of $X_0(p^r)$ and $X_0^+(p^r)$, respectively. Further, let $J_r = J_{p,r}$, $J_r^+ = J_{p,r}^+$ be respectively the "new part" of $J_0(p^r)$ and $J_0^+(p^r)$ (, i.e., under the canonical identification of the space of holomorphic cusp forms of weight 2 belonging to $\Gamma_0(p^r)$ $\left(\text{resp. } \left\langle \Gamma_0(p^r), \begin{pmatrix} 0 & -1 \\ p^r & 0 \end{pmatrix} \right\rangle\right)$ with the cotangent space of $J_0(p^r)$ (resp. $J_0^+(p^r)$), the cotangent space of J_r (resp. J_r^+) corresponds to the subspace spanned

by the new forms of level p^r ([1] [22] Chapter 7). Using the decomposition of the cotangent space of $J_0(p^r)$ by the action of w_{p^r}, we see that $J_0^+(p^r)$ is isogenous over $\boldsymbol{Q}$ to one of the following abelian varieties:

$$(1.2)\qquad \begin{cases} \prod_{\substack{1\leqq i<r \\ \text{odd}}} J_i^{(r+1-i)/2} \times \prod_{\substack{1<i<r \\ \text{even}}} J_i^{(r-i)/2} \times \prod_{\substack{1<i\leqq r \\ \text{even}}} J_i^+ & \text{if } r \text{ is even,} \\ \prod_{\substack{1<i<r \\ \text{even}}} J_i^{(r+1-i)/2} \times \prod_{\substack{1\leqq i<r \\ \text{odd}}} J_i^{(r-i)/2} \times \prod_{\substack{1\leqq i\leqq r \\ \text{odd}}} J_i^+ & \text{if } r \text{ is odd.} \end{cases}$$

Let $J_0^-(p^s)$ be the quotient $J_0(p^s)/(1+w_{p^s})J_0(p^s)$, where w_{p^s} is the automorphism of $J_0(p^s)$ induced by the involution w_{p^s} of $X_0(p^s)$. Let $\boldsymbol{T}$ be the subring of the ring of endomorphisms of $J_0(p^s)$ generated by Hecke operators T_m for $p\nmid m$ and w_{p^s}, and $\mathscr{I}$ be the ideal of $\boldsymbol{T}$ generated by $1+l-T_l$ and $1+w_{p^s}$ for prime numbers $l\neq p$. Put $\tilde{J}_0(p^s)=J_0(p^s)/(\cap_{n\geqq 1}\mathscr{I}^n)J_0(p^s)$ and $\tilde{J}_0(p^s)_{(m)}=J_0(p^s)/(\cap_{n\geqq 1}(m,\mathscr{I})^n)J_0(p^s)$ for integers $m\geqq 1$. For $p\leqq 7$ and $p=13$, $X_0(p)\simeq \boldsymbol{P}^1$ and for the other prime numbers p, $X_0(p)\neq \boldsymbol{P}^1$. Let 0 and ∞ be the $\boldsymbol{Q}$-rational cusps of $X_0(p^s)$ which are represented respectively by $(\boldsymbol{G}_m\times \boldsymbol{Z}/p^s\boldsymbol{Z}, \boldsymbol{Z}/p^s\boldsymbol{Z})$ and $(\boldsymbol{G}_m, \mu_{p^s})$, where $\mu_{p^s}=\mathrm{Spec}\, \boldsymbol{Z}[X]/(X^{p^s}-1)$. Then we know the following result.

THEOREM (1.3) (Mazur [12]). *For $p\geqq 17$ or $p=11$, the natural morphism $J_0(p)\to\tilde{J}_0(p)$ induces an isomorphism of the cuspidal subgroup $C=\langle \mathrm{cl}((0)-(\infty))\rangle$ of order $n=\mathrm{num}((p-1)/12)$ to the Mordell-Weil group of $J_0^-(p)$, and $\tilde{J}_0(p)$ is an optimal quotient of $J_0^-(p)$. Further the natural morphisms $J_0(p)(\boldsymbol{Q})_{\mathrm{tor}}\to J_0^-(p)(\boldsymbol{Q})_{\mathrm{tor}}\to\tilde{J}_0(p)(\boldsymbol{Q})$ are isomorphisms.*

(1.4) For the pairs $(p, s)=(2, 5)$, $(3, 3)$ and $(7, 2)$, $X_0(p^s)$ are elliptic curves with finite Mordell-Weil groups of order 4, 3 and 2 ([24] Table 1 pp. 81–113), respectively, and $J_0(p^s)=J_0^-(p^s)=\tilde{J}_0(p^s)$. For $(p, s)=(13, 2)$, $\tilde{J}_0(169)_{(7)}$ is an optimal quotient of $J_0^-(169)$ with finite Mordell-Weil group [2] §3. We do not know whether $J_0^-(125)$ has a quotient ($\neq\{0\}$) with finite Mordell-Weil group (see loc.cit.).

We will make use of the following morphisms for $r\geqq 2$. Let $\pi=\pi_{r,s}$ be the natural morphism of $X_0(p^r)$ to $X_0(p^s)$ defined by $(E, A)\mapsto(E, A_{p^s})$ for an integer s, $1\leqq s\leqq r-1$. Let $f=f_{r,s}$ be the morphism of $X_0(p^r)$ to $J_0(p^s)$ defined by $f(x)=\mathrm{cl}((w_{p^s}\pi(x))-(\pi w_{p^r}(x)))$, i.e.,

$$f\colon (E, A)\longmapsto \mathrm{cl}((E/A_{p^s}, E_{p^s}/A_{p^s})-(E/A, (E_{p^s}+A)/A)).$$

Then f induces a morphism $f^+=f^+_{r,s}$ of $X_0^+(p^r)$ to $J_0^-(p^s)$, which is defined by the following diagram:

$$\begin{array}{ccc} X_0(p^r) & \xrightarrow{\text{can.}} & X_0^+(p^r) \\ f\downarrow & \subset & \downarrow f^+ \\ J_0(p^s) & \xrightarrow{\text{can.}} & J_0^-(p^s). \end{array}$$

We will make use of f and f^+ in the following cases:

(1.5)

p	r	s
2	$\geqq 6$	5
3	$\geqq 4$	3
5	$\geqq 4$	3
7	$\geqq 3$	2
11	$\geqq 2$	1
13	$\geqq 3$	2
$p \geqq 17$	$\geqq 2$	1.

For a triple (p, r, s) as above, let $\tilde{f}=\tilde{f}_{r,s}$ be the morphism of $X_0(p^r)$ to $\tilde{J}_0(p^s)$ (for $p\neq 5, 13$), $\tilde{J}_0(125)_{(5)}$ and $\tilde{J}_0(169)_{(7)}$ induced by $f=f_{r,s}$. Let $\mathscr{X}_0(p^r)$, $\mathscr{X}_s(p^t)$ and $\mathscr{X}_s^n(p^t)$ be respectively the normalizations of the projective j-line $\mathscr{X}_0(1)\simeq \boldsymbol{P}_{\boldsymbol{Z}}^1$ in $X_0(p^r)$, $X_s(p^t)$ and $X_s^n(p^t)$. Further put $\mathscr{X}_0^+(p^r)=\mathscr{X}_0(p^r)/\langle w_{p^r}\rangle$. Then $\mathscr{X}_0^+(p^r)\otimes \boldsymbol{Z}[1/p]$ is smooth over $\boldsymbol{Z}[1/p]$, since $\mathscr{X}_0(p^r)\otimes \boldsymbol{Z}[1/p]$ is smooth [3] VI §6 and the fundamental involution $w_{p^r}\otimes \boldsymbol{F}_2$ (for $p\neq 2$) has at most finitely many fixed points. Denote also by $\pi=\pi_{r,s}$ the natural morphism of $\mathscr{X}_0(p^r)$ to $\mathscr{X}_0(p^s)$, and by f, $\tilde{f}$ (resp. f^+) the morphisms of the smooth part $\mathscr{X}_0(p^r)^{\text{smooth}}$ (resp. $\mathscr{X}_0^+(p^r)^{\text{smooth}}$) to the Néron models $J_0(p^s)_{/\boldsymbol{Z}}$ and $\tilde{J}_0(p^s)_{/\boldsymbol{Z}}$ (for $p\neq 5, 13$), $\tilde{J}_0(125)_{(5)/\boldsymbol{Z}}$ and $\tilde{J}_0(169)_{(7)/\boldsymbol{Z}}$ (resp. $J_0^-(p^s)_{/\boldsymbol{Z}}$).

(1.6) Let $0=\begin{pmatrix}0\\1\end{pmatrix}$, $\infty=\begin{pmatrix}1\\0\end{pmatrix}$ be the $\boldsymbol{Q}$-rational cuspidal sections of $\mathscr{X}_0(p^r)$ represented by the pairs $(\boldsymbol{G}_m\times \boldsymbol{Z}/p^r\boldsymbol{Z}, \boldsymbol{Z}/p^r\boldsymbol{Z})$ and $(\boldsymbol{G}_m, \mu_{p^r})$, respectively. Let (t, i) be a pair of integers t and i satisfying the following conditions: $1\leqq t\leqq r-1$, $(i, p)=1$ and $1\leqq i\leqq p^{m(t)}-1$ for $m(t)=\min\{t, r-t\}$. Let $\zeta=\zeta_{p^r}$ be a primitive p^r-th root of unity. For each pair (t, i) as above, let $\begin{pmatrix}i\\p^t\end{pmatrix}$ be the cuspidal section of $\mathscr{X}_0(p^r)$ represented by $(\boldsymbol{G}_m\times \boldsymbol{Z}/p^{r-t}\boldsymbol{Z}, \langle(\zeta^i, 1)\rangle)$ (over $\boldsymbol{Z}[1/p]$), where $\langle(\zeta^i, 1)\rangle$ is the subgroup of $\boldsymbol{G}_m\times \boldsymbol{Z}/p^{r-t}\boldsymbol{Z}$ generated by the section $(\zeta^i, 1)$. These cuspidal sections $\begin{pmatrix}i\\p^t\end{pmatrix}$ are $\boldsymbol{Q}(\zeta_{p^{m(t)}})$-rational and are conjugate over $\boldsymbol{Q}$ (for the fixed integer t). The fundamental

involution w_{p^r} exchanges 0 with ∞, and $\begin{pmatrix} i \\ p^t \end{pmatrix}$ with $\begin{pmatrix} j \\ p^{r-t} \end{pmatrix}$ for an integer j congruent to $-i^{-1} \bmod p^{m(t)}$. Let $\pi_{r+1}=\pi_{r+1,r}$ be the natural morphism of $\mathscr{X}_0(p^{r+1})$ to $\mathscr{X}_0(p^r)$: $(E, A)\mapsto(E, A_{p^r})$. Then π_{r+1} is isomorphic along ∞ and $\begin{pmatrix} i \\ p^r \end{pmatrix}\otimes \boldsymbol{Z}[1/p]$. The ramification indices of π_{r+1} at 0 and at $\begin{pmatrix} i \\ p^t \end{pmatrix}\otimes \boldsymbol{Z}[1/p]$ for $1\leqq t\leqq r-1$ are all p. Further π_{r+1} sends 0 to 0, $\begin{pmatrix} i \\ p^t \end{pmatrix}$ (for $1\leqq t\leqq r-1$) to $\begin{pmatrix} i \\ p^t \end{pmatrix}$, and ∞ and $\begin{pmatrix} i \\ p^r \end{pmatrix}$ to ∞.

(1.7) The irreducible components of $\mathscr{X}_0(p^r)\otimes \boldsymbol{F}_p$ are all defined over $\boldsymbol{F}_p$, and they intersect each other at the supersingular points on $\mathscr{X}_0(p^r)\otimes \boldsymbol{F}_p$ [3] VI §6. Let E_0 and E_r (resp. E_t for $1\leqq t\leqq r-1$) be the irreducible components of $\mathscr{X}_0(p^r)\otimes \boldsymbol{F}_p$ such that $0\otimes \boldsymbol{F}_p\in E_0$ and $\infty\otimes \boldsymbol{F}_p\in E_r$ $\left(\text{resp. } \begin{pmatrix} i \\ p^t \end{pmatrix}\otimes \boldsymbol{F}_p\in E_t\right)$. For a subscheme Y of a modular curve $X/\boldsymbol{Z}$, Y^h denotes the open subscheme $Y\backslash\{\text{supersingular points on } Y\otimes \boldsymbol{F}_p\}$ of Y. The following facts are induced by the construction of the fine moduli stack $\mathscr{M}^h_{\Gamma(p^r)}$ [3] V, and they will be explained below. The irreducible components E_0^h and E_r^h are smooth over $\boldsymbol{F}_p$. Further E_0^h (resp. E_r^h) is the coarse moduli space $/\boldsymbol{F}_p$ of the isomorphism classes of the generalized elliptic curves E with a cyclic subgroup scheme A which is isomorphic to $\boldsymbol{Z}/p^r\boldsymbol{Z}$ (resp. μ_{p^r}) for the étale topology. When $p=2$, E_1^h and E_{r-1}^h are also smooth over $\boldsymbol{F}_2$. For an integer i, $1\leqq i\leqq r/2$, the multiplicity of E_i^h is $p^{r-i}(p-1)$. The fundamental involution w_{p^r} exchanges E_i with E_{r-i}. When $r=2t$ is even, w_{p^r} fixes E_t. Let $\pi_r=\pi_{r,r-1}$ be the natural morphism of $\mathscr{X}_0(p^r)$ to $\mathscr{X}_0(p^{r-1})$: $(E, A)\mapsto(E, A_{p^{r-1}})$. Then $\pi_r(E_i)=E_i$ for the integers i, $0\leqq i\leqq r-1$, and $\pi_r(E_r)=E_{r-1}$. The restriction of π_r to E_r^h: $E_r^h\to E_{r-1}^h$ is an isomorphism and its restriction to E_0^h: $E_0^h\to E_0^h$ is radicial of degree p. When $p=2$, its restriction to E_{r-1}^h: $E_{r-1}^h\to E_{r-1}^h$ is also an isomorphism and its restriction to E_1^h: $E_1^h\to E_1^h$ (for $r\geqq 3$) is radicial of degree 2. Further we know the following facts. Let $\mathscr{M}_{\Gamma(p^r)}$ be the fine moduli stack which corresponds to the finite adèlic modular group

$$\Gamma_0(p^r)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{GL}_2(\hat{\boldsymbol{Z}})\mid c\equiv 0 \bmod p^r\right\},$$

where $\hat{\boldsymbol{Z}}=\varprojlim_n \boldsymbol{Z}/n\boldsymbol{Z}$ [3]. Let E be a semistable elliptic curve over a scheme S with a cyclic subgroup A of rank$(/S)$ p^r. Let x be an object of $\mathscr{M}_{\Gamma_0(p^r)}(S)$ represented by the pair (E, A). Then if $x\otimes \boldsymbol{F}_p$ define a

section of E_i^h for $1 \leqq i \leqq r-1$, then A admits the following exact sequence

$$0 \longrightarrow \mu_{p^i} \longrightarrow A \longrightarrow \boldsymbol{Z}/p^{r-i}\boldsymbol{Z} \longrightarrow 0.$$

Now we here explain the statements as above. For a primitive p^r-th root $\zeta = \zeta_{p^r}$ of unity and $\zeta: \boldsymbol{Z}/p^r\boldsymbol{Z} \to \mu_{p^r}$ be the homomorphism $/\boldsymbol{Z}[\zeta]$ which sends 1 to ζ over $\boldsymbol{Q}(\zeta)$. For a cyclic subgroup A of $\boldsymbol{Z}/p^r\boldsymbol{Z}$, define the finite flat group scheme $R(A)$ $(/\boldsymbol{Z}[\zeta])$ by "push out" in the following diagram [3] V:

$$\begin{array}{ccccc} A & \longrightarrow & (\boldsymbol{Z}/p^r\boldsymbol{Z})^2 & \longrightarrow & (\boldsymbol{Z}/p^r\boldsymbol{Z})/A \\ \downarrow \zeta & \subset & \downarrow g & \subset & \| \\ A \otimes \mu_{p^r} & \longrightarrow & R(A) & \longrightarrow & (\boldsymbol{Z}/p^r\boldsymbol{Z})/A. \end{array}$$

Let $\mathscr{C}_A$ be the finite moduli space which represents the following functor: for a scheme S $/\boldsymbol{Z}[\zeta]$, $\mathscr{C}_A(S)$ is the set of the isomorphism classes of the generalized elliptic curves E $/S$ with an isomorphism $\alpha: E_{p^r} \simeq R(A) \times S$. Then $\mathscr{C}_A$ is an open subspace of $\mathscr{M}^h_{\Gamma(p^r)} (= M^h_{\Gamma(p^r)})$, which is a scheme if $p^r \geqq 3$ [3] V, VII p. 300). Let G be the schematic closure of $g(\boldsymbol{Z}/p^r\boldsymbol{Z} \times \{0\})$ in $R(A)$. Consider the following canonical morphisms

$$M^h_{\Gamma(p^r)} \xrightarrow{\psi} M^h_{\Gamma_0(p^r)} \xrightarrow{\pi_r} M^h_{\Gamma_0(p^{r-1})}.$$

Then ψ sends (E, α) to $(E, \alpha^{-1}(G \times S))$. Set $A_0 = \{0\} \times \boldsymbol{Z}/p^r\boldsymbol{Z}$ and $A_i = \langle (1, p^i) \rangle$ for $1 \leqq i \leqq r$. Then for $(E, \alpha) \in \mathscr{M}^h_{A_i}(S)$, $(G \times S) \cap g(A_i) \simeq \mu_{p^i}$ and $\alpha^{-1}(G \times S)$ admits the following exact sequence

$$0 \longrightarrow \mu_{p^i} \longrightarrow \alpha^{-1}(G \times S) \longrightarrow \boldsymbol{Z}/p^{r-i}\boldsymbol{Z} \longrightarrow 0.$$

Now assume $r \geqq 2$. The subgroup of $\Gamma_0(p^{r-1})$ consisting of the automorphisms which fixes $\mathscr{C}_{A_r}$ is $\Gamma_0(p^r)$, so that π_r induces an isomorphism of E_r^h **onto** E_{r-1}^h. When $p=2$, by the same way as above, we see that π_r induces an isomorphism of E_{r-1}^h onto E_{r-1}^h.

REMARK (1.8). The non cuspidal $\boldsymbol{F}_p$-rational point on E_r^h (resp. E_0^h) is represented by an elliptic curve E $/\boldsymbol{F}_p$ with the subgroup $A = (E_{p^r})^0 = \ker(F^r: E \to E^{(p^r)} = E)$ (resp. $A = \ker(V^r: E^{(p^r)} = E \to E)$), where F is the Frobenius map and V is the Verschiebung.

Let $N \geqq 1$ be an integer and $J_0(N)$ be the jacobian variety of $X_0(N)$. Let B be an abelian subvariety of $J_0(N)$ defined over $\boldsymbol{Q}$, $A = J_0(N)/B$ be

the (optimal) quotient and $a: J_0(N) \to A$ be the natural morphism. Let N' (resp. N'') be the product of all the prime divisors q of N with $q^2 \nmid N$ (resp. $q^2 | N$). Let $g: X \to Y$ be a morphism of schemes and x be a section of X. Denote by $\mathrm{Cot}_x(g): \mathrm{Cot}_{g(x)} Y \to \mathrm{Cot}_x X$ the morphism of the cotangent spaces along x and $g(x)$. The morphism g is a formal immersion along x if $g^*(\widehat{\mathcal{O}_{Y,g(x)}}) = \widehat{\mathcal{O}_{X,x}}$, where $\widehat{\mathcal{O}_{X,x}}$ and $\widehat{\mathcal{O}_{Y,g(x)}}$ are the completions of the local rings by the maximal ideals $m_{X,x}$ and $m_{Y,g(x)}$. A criterion of the formal immersion is seen in E. G. A. IV 17.44. This tells us that g is a formal immersion along x if and only if the following conditions are satisfied: (i) $g^*(\mathcal{O}_{Y,g(x)}/m_{Y,g(x)}) = \mathcal{O}_{X,x}/m_{X,x}$ and (ii) $\mathrm{Cot}_x(g)$ is a surjective morphism.

PROPOSITION (1.9) (Mazur [14] §3). *Under the notation as above, let q be a prime number not dividing $2N''$. Then* $\mathrm{Cot}_0(a \otimes \boldsymbol{F}_q): \mathrm{Cot}_0(A_{/\boldsymbol{Z}} \otimes \boldsymbol{F}_q) \to \mathrm{Cot}_0(J_0(N)_{/\boldsymbol{Z}} \otimes \boldsymbol{F}_q)$ *is surjective, where* 0 *are the unit sections of group schemes* $A_{/\boldsymbol{Z}} \otimes \boldsymbol{F}_q$ *and* $J_0(N)_{/\boldsymbol{Z}} \otimes \boldsymbol{F}_q$.

Let $\tilde{\mathscr{X}}_0(N) \to \mathrm{Spec}\, \boldsymbol{Z}$ be the minimal model of $X_0(N)$, q be a prime number not dividing N'' and $R = W(\bar{\boldsymbol{F}}_q)$ be the ring of integers of $\boldsymbol{Q}_q^{ur}$. Denote by ι the duality of Grothendieck [14] §2:

$$\iota: \mathrm{Cot}_0 J_0(N)_{/\boldsymbol{Z}[1/N']} \xrightarrow{\sim} H^0(\tilde{\mathscr{X}}_0(N) \otimes \boldsymbol{Z}[1/N''], \Omega) ,$$

where Ω is the sheaf of regular differentials [3] p. 162. Let x be a section: $\mathrm{Spec}\, R \to \mathscr{X}_0(N)^{\mathrm{smooth}}$, and b be the morphism of $X_0(N)$ to $J_0(N)$ defined by $z \mapsto \mathrm{cl}((z) - (x))$. Denote also by b the morphism of $\mathscr{X}_0(N)^{\mathrm{smooth}} \otimes R$ to $J_0(N)_{/R}$, which is induced by the universal property of the Néron model.

PROPOSITION (1.10) (Mazur [14] §2 Lemma (2.1)). *Under the notation as above, the following diagram is commutative up to sign:*

$$\begin{array}{ccc} \mathrm{Cot}_x \mathscr{X}_0(N) \otimes R & \xleftarrow{\mathrm{Cot}_x(b)} & \mathrm{Cot}_0 J_0(N)_{/R} \\ {\scriptstyle a_1}\uparrow & \nwarrow \quad \swarrow{\scriptstyle \sim}\,\iota & \\ & H^0(\tilde{\mathscr{X}}_0(N) \otimes R, \Omega) & \\ \omega = \sum a_n q^n \frac{dq}{q} \mapsto & & \end{array}$$

where $q = q_x$ is the local parameter along x.

LEMMA (1.11) ([16] (3.6)). *Let p be a prime number congruent to $1 \bmod 8$, and c be the natural morphism of $J_0(p)_{/Z}$ to $\tilde{J}_0(p)_{/Z}$. Then there exists a form $\omega \in c^*(\mathrm{Cot}_0 \tilde{J}_0(p)_{/Z_2})$ $(\subset H^0(\tilde{\mathscr{X}}_0(p) \otimes \boldsymbol{Z}_2, \Omega^1))$ whose value at the cuspidal section $0=\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is a unit of $\boldsymbol{Z}_2$.*

PROPOSITION (1.12) ([16] (2.5)). *Let $p \geqq 17$ or $p=11$ be a prime number and $\tilde{f}=\tilde{f}_{2,1}: \tilde{\mathscr{X}}_0(p^2) \otimes \boldsymbol{Z}[1/p] \to \tilde{J}_0(p)_{/\boldsymbol{Z}[1/p]}$ be the morphism for a triple $(p, r, s)=(p, 2, 1)$ defined before. Then $\tilde{f} \otimes \boldsymbol{Z}_q$ is a formal immersion along any cuspidal section of $\tilde{\mathscr{X}}_0(p^2) \otimes \boldsymbol{Z}_q$ for $q \neq 2, p$.*

LEMMA (1.13). *Let $(p, s)=(2, 5)$, (3.3) or (7, 2) be a pair as in (1.4). The natural morphism of $\tilde{\mathscr{X}}_0(p^s)^{\mathrm{smooth}}$ to the Néron model $J_0(p^s)_{/Z}$ is an open immersion.*

PROOF. The modular curves $X_0(p^s)$ for (p, s) as above are elliptic curves. We can easily see this lemma, using the minimal models [24] Table 1 pp. 81–113. The details for $p=2$ and 3 will be explained in §3. □

PROPOSITION (1.14). *Under the notation as above, let (p, r, s) be a triple as in (1.5). Let q be a prime number and $\tilde{f}=\tilde{f}_{r,s}$ be the morphism of $\tilde{\mathscr{X}}_0(p^r)^{\mathrm{smooth}}$ to $\tilde{J}_0(p^s)_{/Z}$ (for $p \neq 5, 13$), $\tilde{J}_0(125)_{(5)/Z}$ or $\tilde{J}_0(169)_{(7)/Z}$ defined before. Then $\tilde{f} \otimes \boldsymbol{Z}_q$ is a formal immersion along the cuspidal sections for the following cuspidal sections:*

(i) *For $q \neq 2$, along $0=\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\infty=\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} i \\ p \end{pmatrix}$ and $\begin{pmatrix} i \\ p^{r-1} \end{pmatrix}$.*
(ii) *For $p \geqq 17$ or $p=11$, and $q=p$, along 0 and ∞.*
(iii) *For $p \geqq 17$, $p \equiv 1 \bmod 8$, and $q=2$, along 0 and ∞.*
(iv) *For $p=2, 3$ and 7, and $q=2$, along 0 and ∞.*
(v) *For $p=q=2$, along $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 2^{r-1} \end{pmatrix}$.*

PROOF. For the simplicity, we here denote by $\tilde{J}_0(125)$ and $\tilde{J}_0(169)$ the quotients $\tilde{J}_0(125)_{(5)}$ and $\tilde{J}_0(169)_{(7)}$. For a triple (p, r, s) and a rational prime q as in the statement of the above proposition, the cuspidal sections 0, ∞, $\begin{pmatrix} i \\ p \end{pmatrix}$ and $\begin{pmatrix} i \\ p^{r-1} \end{pmatrix}$ are contained in the smooth part $\tilde{\mathscr{X}}_0(p^r)^{\mathrm{smooth}}$ $(/\boldsymbol{Z}_q)$ (1.7). The fundamental involution w_{p^r} exchanges 0 with ∞, and $\begin{pmatrix} i \\ p \end{pmatrix}$ with $\begin{pmatrix} j \\ p^{r-1} \end{pmatrix}$ for an integer j congruent to $-i^{-1} \bmod p$. Therefore it suffices to consider the sections ∞ and $C_i=\begin{pmatrix} i \\ p^{r-1} \end{pmatrix}$. Denote

by q_∞, q_i the local parameters along the cuspidal sections ∞ and C_i of $\mathscr{X}_0(p^r)\otimes R$ for $R=W(\bar{F}_q)$, respectively. Further denote by q'_0, q'_∞ and q'_i the local parameters along the cuspidal sections 0, ∞ and $\binom{i}{p}$ of $\mathscr{X}_0(p^s)\otimes R$, respectively. Let $u=u_{r,s}$ be the morphism of $\mathscr{X}_0(p^s)^{\text{smooth}}$ to $\tilde{J}_0(p^s)_{/Z}$ defined by

$$\begin{aligned} u\colon \mathscr{X}_0(p^s)^{\text{smooth}} &\longrightarrow J_0(p^s)_{/Z} \xrightarrow{\text{can.}} \tilde{J}_0(p^s)_{/Z}. \\ z &\longmapsto \mathrm{cl}((z)-(0)) \end{aligned}$$

The morphism $\tilde{f}=\tilde{f}_{r,s}$ is defined by the following diagram:

$$\begin{array}{ccccccc} \mathscr{X}_0(p^r)^{\text{smooth}} & & & \overset{\tilde{f}}{\searrow} & & & \\ \downarrow{\scriptstyle w_{p^s}\pi\times\pi w_{p^r}} & & & \subset & & & \\ \mathscr{X}_0(p^s)^{\text{smooth}}\times\mathscr{X}_0(p^s)^{\text{smooth}} & \longrightarrow & J_0(p^s)_{/Z}\times J_0(p^s)_{/Z} & \longrightarrow & J_0(p^s)_{/Z} & \xrightarrow{\text{can.}} & \tilde{J}_0(p^s)_{/Z}. \end{array}$$

$$(z_1, z_2)\longmapsto(\mathrm{cl}((z_1)-(0)), \mathrm{cl}((z_2)-(0))) \quad (x, y)\longmapsto x+y$$

Then $\mathrm{Cot}_C(\tilde{f})=\mathrm{Cot}_C(uw_{p^s}\pi)-\mathrm{Cot}_C(u\pi w_{p^r})$ for any cuspidal section C: $\mathrm{Spec}\, R\to\mathscr{X}_0(p^r)^{\text{smooth}}$. For $q\neq p$, by (1.12), it suffices to consider for $r\geqq 3$. Then for $q\neq p$ and $r\geqq 3$,

$$\begin{aligned} &(w_{p^s}\pi)^*(q'_0)=q_\infty\times(\text{a unit}) \\ &(\pi w_{p^r})^*(q'_0)=(q)^{p^{r-s}}\times(\text{a unit}) \end{aligned} \qquad \text{along } \infty,$$

$$\begin{aligned} &(w_{p^s}\pi)^*(q'_0)=q_i\times(\text{a unit}) \\ &(\pi w_{p^r})^*(q'_\infty)=(q_i)^{p^{r-1}}\times(\text{a unit}) \end{aligned} \qquad \text{along } C_i \text{ if } s=1,$$

$$\begin{aligned} &(w_{p^s}\pi)^*(q'_0)=q_i\times(\text{a unit}) \\ &(\pi w_{p^r})^*(q'_j)=(q_i)^{p^{r-s}}\times(\text{a unit}) \end{aligned} \qquad \text{along } C_i \text{ if } s\geqq 2,$$

where j is an integer congruent to $-i^{-1} \bmod p$. Therefore $\mathrm{Cot}_\infty(\tilde{f})\otimes R$ and $\mathrm{Cot}_{C_i}(\tilde{f})\otimes R$ are surjective for $q\neq p$ (cf. (1.9), (1.10). (1.11), (1.12)). For $q=p$, (1.7) shows that $\mathrm{Cot}_\infty(u\pi w_{p^r})\otimes\bar{F}_p$ and $\mathrm{Cot}_{C_i}(u\pi w_{p^r})\otimes\bar{F}_p$ are 0-maps, and $\mathrm{Cot}_\infty(uw_{p^s}\pi)\otimes\bar{F}_p$ and $\mathrm{Cot}_{C_i}(uw_{p^s}\pi)\otimes\bar{F}_p$ are not 0-maps (see loc.cit.). Thus $\mathrm{Cot}_\infty(f)\otimes R$ and $\mathrm{Cot}_{C_i}(f)\otimes R$ are surjective for $q=p$. □

§2. Elliptic curves.

In this section, we prepare some lemmas on elliptic curves and finite flat group schemes. Throughout this section, K denotes a finite

extension of $\boldsymbol{Q}_p^{ur}$ of degree e_K, and $R=\mathcal{O}_K$ is the ring of integers of K. For an elliptic curve E with a finite subgroup A defined over K, $A_{/R}$ denotes the schematic closure of A in the Néron model $E_{/R}$. Then $A_{/R}$ is a quasi finite flat subgroup scheme [20] §2. The finite flat group schemes of type $(p, \cdots, p)$ over $\boldsymbol{Z}_p$ are classified in [19] [20]. Let v be the valuation of K such that $v(K^\times)=\boldsymbol{Z}$. Let G be a finite flat group scheme of rank p over $R=\mathcal{O}_K$, then $G\simeq \mathrm{Spec}\, R[X]/(X^p-\delta X)$ for $\delta\in R$ with $0\leqq v(\delta)\leqq e_K$. If $v(\delta)=0$ (resp. $v(\delta)=e_K$), then $G\simeq(\boldsymbol{Z}/p\boldsymbol{Z})_{/R}$ (resp. $G\simeq\mu_{p/R}$) (see loc.cit.).

THEOREM (2.1) ([20] §3 (3.3.2), [19]). *Let* $\mathrm{Spec}\, R[X]/(X^p-\delta_i X)$ *be finite flat group schemes of rank* p *over* R. *Let* g *be a homomorphism of* G_1 *to* G_2 *such that* $g\otimes K: G_1\otimes K\to G_2\otimes K$ *is an isomorphism. Then* $v(\delta_1)\equiv v(\delta_2) \bmod (p-1)$. *Further*

(i) *If* $e_K<p-1$, *then* g *is an isomorphism.*

(ii) *If* $e_K=p-1$ *and* g *is not an isomorphism, then* $G_1\simeq(\boldsymbol{Z}/p\boldsymbol{Z})_{/R}$ *and* $G_2\simeq\mu_{p/R}$.

LEMMA (2.2). *Let* E *be a semistable elliptic curve with a cyclic subgroup* A *of order* p^r *defined over* K *for* $r\geqq 2$. *Let* x *be the* R*-section of* $\mathscr{X}_0(p^r)$ *such that* $x\otimes K$ *is represented by the pair* (E, A). *Then*

(i) *If* $x\otimes\bar{\boldsymbol{F}}_p$ *is a section of* E_i^h, *then* K *contains a primitive* $p^{m(i)}$*-th root* $\zeta_{p^{m(i)}}$ *of unity for* $m(i)=\min\{i, r-i\}$.

(ii) *If* $x\otimes\boldsymbol{F}_p$ *is a supersingular point, then* $e_K\geqq p+1$.

PROOF. If $x\otimes\bar{\boldsymbol{F}}_p$ is a section of E_i^h, then A admits the following exact sequence (1.7):

$$0\longrightarrow\mu_{p^i\,/K}\longrightarrow A\longrightarrow(\boldsymbol{Z}/p^{r-i}\boldsymbol{Z})_{/K}\longrightarrow 0.$$

Since A is cyclic, K contains $\zeta_{p^{m(i)}}$. Now assume that $x\otimes\bar{\boldsymbol{F}}_p$ is a supersingular point. Let y be the R-section of $\mathscr{X}_s(p)\simeq\mathscr{X}_0(p^2)$ such that $y\otimes K$ is represented by the semistable elliptic curve $F=E/A_p$ with the independent cyclic subgroups $C_1=A_{p^2}/A_p$ and $C_2=E_p/A_p$ of order p. The schematic closure $C_{i/R}$ of C_i in the Néron model $F_{/R}$ are finite flat group schemes, and $C_{i/R}=\mathrm{Spec}\, R[X]/(X^p-\delta_i X)$ for $\delta_i\in R$ with $1\leqq v(\delta_i)\leqq e_K-1$. Consider the following morphisms of finite flat group schemes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_{1/R} & \longrightarrow & (E_{/R})_p & \longrightarrow & (E_{/R})_p/(C_{1/R}) & \longrightarrow & 0 \text{ (exact).} \\ & & & & \cup & \nearrow_{f} & \| & & \\ & & & & C_{2/R} & & C & & \end{array}$$

Then $f\otimes K: C_2 \to E_p/C_1 \simeq C\otimes K$ is an isomorphism. Then

$$C \simeq \operatorname{Spec} R[X]/(X^p - \delta X)$$

for $\delta \in R$ with $1 \leqq v(\delta) \leqq e_K - 1$ and $v(\delta) \equiv v(\delta_2) \bmod (p-1)$. If $v(\delta) = v(\delta_2)$, then f is an isomorphism and $C_{1/R} \cap C_{2/R} = \{0\}$. For any supersingular elliptic curve $H/\bar{\boldsymbol{F}}_p$, $H_p \simeq \operatorname{Spec} \bar{\boldsymbol{F}}_p[X]/(X^{p^2})$ as schemes, so that $(E_{/R})_p \neq C_{1/R} \oplus C_{2/R}$. Therefore $v(\delta) \neq v(\delta_2)$ and $e_K \geqq p+1$. □

Let m be the maximal ideal of R and E be an elliptic curve with a cyclic subgroup A defined over K. Then E has semistable reduction over a finite extension of K. If the modular invariant $j(E) \not\equiv 0$, $1728 \bmod m$, then there exists a semistable elliptic curve F with a cyclic subgroup B defined over K such that $(E, A) \simeq (F, B)$ over a quadratic extension of K. If $p \geqq 5$ and $j(E) \equiv 0 \bmod m$ (resp. $j(E) \equiv 1728 \bmod m$), then there exists a semistable elliptic curve F with a cyclic subgroup B defined over a finite extension K' of K of degree 1 or 3 (resp. of degree 1 or 2) such that $(E, A) \simeq (F, B)$ over the quadratic extension of K'.

COROLLARY (2.3). *Under the notation as Lemma* (2.2), *put* $e' = 1$ *if* $j(x) \not\equiv 0$, $1728 \bmod m$, $e' = 3$ *if* $j(x) \equiv 0 \bmod m$ *and* $e' = 2$ *if* $j(x) \equiv 1728 \bmod m$. *Then*

(i) *If* $x \otimes \bar{\boldsymbol{F}}_p$ *is a section of* E_i^k, *then* $e_K e' \geqq p^{m(i)-1}(p-1)$ *if* $1 \leqq i \leqq r-1$.

(ii) *If* $x \otimes \bar{\boldsymbol{F}}_p$ *is a supersingular point and* $p \geqq 5$, *then* $e_K e' \geqq p+1$.

§3. Rational points on $X_0^+(p^r)$.

In this section, we will prove Theorem (0.1) and give other results. Let (p, r) be a pair in (1.0). Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(p^r)$, and x, $x' = w_{p^r}(x)$ be the sections of the fibre $X_0(p^r)_y$ at y. Then x and x' are not defined over $\boldsymbol{Q}$ (1.1). They are defined over a quadratic field k, and $x' = x^\sigma$ for $1 \neq \sigma \in \operatorname{Gal}(k/\boldsymbol{Q})$. There is an elliptic curve E with a cyclic subgroup A of order p^r such that E and A are defined over k and that the pairs (E, A) and $(E/A, E_{p^r}/A)$ represent respectively x and x' [3] VI (3.2). Further the pair (E^σ, A^σ) is isomorphic /$\boldsymbol{C}$ to $(E/A, E_{p^r}/A)$. Denote also by x, x' (resp. y) the $\mathcal{O}_k$ (resp. $\boldsymbol{Z}$)-sections of $\mathscr{X}_0(p^r)$ (resp. $\mathscr{X}_0^+(p^r)$) with generic fibres x and x' (resp. y). Let $\mathfrak{p}$ be a prime of k lying over the rational prime p and e_k be the

ramification index of p in k. When $r=2t$ is even, the modular curves $\mathscr{X}_0(p^{2t})$ and $\mathscr{X}_0^+(p^{2t})$ are isomorphic respectively to $\mathscr{X}_s(p^t)$ and $\mathscr{X}_s^n(p^t)$. Let y' be the corresponding (to y) $\boldsymbol{Q}$-rational point on $X_s^n(p^t)$. Then there exists an elliptic curve E' defined over $\boldsymbol{Q}$ with independent cyclic subgroups C_1 and C_2 of order p^t such that the set $\{C_1, C_2\}$ is $\boldsymbol{Q}$-rational and that the pair $(E', \{C_1, C_2\})$ represents y' (see loc.cit.).

LEMMA (3.1). *Let (p, r) be a pair in* (1.0), *and x, x', y and e_k be as above. If $e_k=2$, then $x\otimes\kappa(\mathfrak{p})=x'\otimes\kappa(\mathfrak{p})$ is a section of E_t if $r=2t$ is even, and it is a supersingular point if r is odd* (1.7). *If $x\otimes\kappa(\mathfrak{p})$ is a section of E_i^h for an integer $i\neq r/2$, then the rational prime p splits in k.*

PROOF. First note that $x'=w_{p^r}(x)=x^\sigma$ for $1\neq\sigma\in\mathrm{Gal}(k/\boldsymbol{Q})$ and that the irreducible components E_i are all $\boldsymbol{F}_p$-rational (1.7). If $e_k=2$, then $x\otimes\kappa(\mathfrak{p})=x^\sigma\otimes\kappa(\mathfrak{p})=x'\otimes\kappa(\mathfrak{p})$, so that $x\otimes\kappa(\mathfrak{p})=x'\otimes\kappa(\mathfrak{p})$ is a section of E_t if $r=2t$ is even, and it is a supersingular point if r is odd. Now assume that $x\otimes\kappa(\mathfrak{p})$ is a section of E_i^h for an integer $i\neq r/2$. Then $x\otimes\kappa(\mathfrak{p})\neq x'\otimes\kappa(\mathfrak{p})=x^\sigma\otimes\kappa(\mathfrak{p})$. If the rational prime p remains prime in k, then $x^\sigma\otimes\kappa(\mathfrak{p})=(x\otimes\kappa(\mathfrak{p}))^{(p)}$ becomes a section of $(E_i^h)^{(p)}=E_i^h$. Here $(x\otimes\kappa(\mathfrak{p}))^{(p)}$ and $(E_i^h)^{(p)}$ are the images of $x\otimes\kappa(\mathfrak{p})$ and E_i^h under the Frobenius map $F\colon \mathscr{X}_0(p^r)\otimes\boldsymbol{F}_p\to\mathscr{X}_0(p^r)\otimes\boldsymbol{F}_p$. But $x'\otimes\kappa(\mathfrak{p})=x^\sigma\otimes\kappa(\mathfrak{p})$ is a section of $E_{r-i}^h\neq E_i^h$. Therefore p splits in k. □

Now we prove the following theorem.

THEOREM (3.2). *Let (p, r) be a pair in* (1.0), *and x, $x'=x^\sigma$, y and e_k be as above. Then the rational prime p splits in k. Further $x\otimes\kappa(\mathfrak{p})$ and $x'\otimes\kappa(\mathfrak{p})$ are the sections of $E_0^h\cup E_r^h$ if $p\neq2$, and they are the sections $E_0^h\cup E_1^h\cup E_{r-1}^h\cup E_r^h$ if $p=2$.*

PROOF. If the modular invariant $j(x)\equiv0$ (resp. 1728) mod $\mathfrak{p}$, then $j(x')\equiv0$ (resp. 1728) mod $\mathfrak{p}$. Put $e'=1$ if $j(x)\not\equiv0$, 1728 mod $\mathfrak{p}$, $e'=3$ if $j(x)\equiv0$ mod $\mathfrak{p}$ and $p\geqq5$, and $e'=2$ if $j(x)\equiv1728$ mod $\mathfrak{p}$ and $p\geqq5$ cf. (2.3).

Case for $p\geqq11$. Corollary (2.3), applied to the inequality $e_ke'\leqq6<p-1$, shows that $x\otimes\kappa(\mathfrak{p})$ and $x'\otimes\kappa(\mathfrak{p})$ are the sections of $E_0^h\cup E_r^h$. Then by Lemma (3.1), the rational prime p splits in k.

Case for $p=7$. If $j(x)\not\equiv0$, 1728 mod $\mathfrak{p}$, then $e_ke'=e_k<p-1$. If $x\otimes\kappa(\mathfrak{p})$ is a supersingular point, then $j(x)\equiv1728$ mod $\mathfrak{p}$. Then $e_ke'\leqq4<p+1$. If $j(x)\equiv0$ mod $\mathfrak{p}$ and $e_ke'\geqq p-1$, then $e_k=2$ and r is even

(3.1). Then $e_k e' \leqq 6 < p(p-1)$. Therefore Corollary (2.3) and Lemma (3.1) give the result.

Let v be the normalized valuation of $\bar{\boldsymbol{Q}}_p$ such that $v(p)=1$, and regard $k_{\mathfrak{p}}$ as a subfield of $\bar{\boldsymbol{Q}}_p$.

Case for $p=5$ ($r \geqq 3$). The supersingular modular invariant in characteristic 5 is 0. The same argument as for $p=7$ gives the result, except for the case when $j(x) \equiv j(x') \equiv 0 \bmod \mathfrak{p}$ and $e_k=2$. For the remaining cases, it suffices to discuss for $r=3$ and 4. We make use of the equations of $X_0(5)$ and $X_0(25)$ [4] IV. The modular curve $X_0(5)$ is defined by the equation

$$j=(X^2+10X+5)^3/X \tag{3.2.1}$$

with the fundamental involution $w_5^*(X)=125/X$ [4] IV §3. The modular curve $X_0(25)$ is defined by the equation

$$j=g(Y)/Y(Y^4+5Y^3+3\cdot 5Y^2+5^2Y+5^2) \tag{3.2.2}$$

with $w_{25}^*(Y)=5/Y$, where $g(Y)=(Y^{10}+2\cdot 5Y^9+11\cdot 5Y^8+8\cdot 5^2Y^7+21\cdot 5^2Y^6+202\cdot 5Y^5+57\cdot 5^2Y^4+56\cdot 5^2Y^3+7\cdot 5^3Y^2+2\cdot 5^3Y+5)^3$ see loc. cit.

Case for $r=3$. Consider the following coverings

$$\begin{array}{ccc} X_0(125) & & (E,\ A) \\ \swarrow \quad \searrow & & \swarrow \quad \searrow \\ X_0(5) \qquad X_0(25) & & (E/A_5,\ A_{25}/A_5) \qquad (E/A_5,\ A/A_5). \end{array}$$

Let z_1, z_2 be the images of x under the above morphisms of $X_0(125)$ to $X_0(5)$ and $X_0(25)$, respectively. Then $j(z_1)=j(z_2)$ and the set $\{z_1, w_5(z_2)\}$ defines a $\boldsymbol{Q}$-rational point on $X_0^+(5)$. The points z_1, $w_5(z_1)$ are defined by $X=a$ and $X=125/a=a^\sigma$ for $a \in k^\times$ and $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$ (3.2.1). Then the valuation $v(a)=3/2$ and $v(j(z_1))=3/2$ (see loc.cit.), since the rational prime $p=5$ ramifies in k. The point z_2 is defined by $Y=b$ for $b \in k^\times$ (3.2.2). Using the equation (3.2.2) and the condition $v(j(z_2))>0$, we see that $v(b)=1/2$ and $v(j(z_2))=1/2$. This contradicts that $j(z_1)=j(z_2)$.

Case for $r=4$. We make use of the modular curve $X_s(25)$. Let z, z' ($=z^\sigma$ for $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$) be the images of x and $x'=x^\sigma$ under the isomorphism of $X_0(5^4)$ to $X_s(25)$: $(E, A) \mapsto (E/A_{25}, A/A_{25}, E_{25}/A_{25})$. Let w, w' be the images of z and z' under the natural morphism of $X_s(25)$ to $X_0(25)$: $(E, C_1, C_2) \mapsto (E, C_1)$. Then $w'=w^\sigma$. Since $v(j(w))>0$, using the

equation (3.2.2), we see that w is defined by $Y=a\in k^\times$ with $v(a)=1/2$. Put $a=\sqrt{5}\,b$ for $b\in\bar{\boldsymbol{Q}}_5$ with $v(b)=0$. Then

$$j(w)=\sqrt{5}\,\frac{(1+\sqrt{5}\,c)^3}{b(b^4+3b^2+1+\sqrt{5}\,d)}$$

for $c, d\in\bar{\boldsymbol{Q}}_5$ with $v(c)\geqq 0$ and $v(d)\geqq 0$. Since $v(j(w))>0$, $b^4+3b^2+1\not\equiv 0 \bmod (\sqrt{5})$. Let C be the curve defined by the equation

(3.2.3)
$$0=\frac{Y(Y^4+5Y^3+15Y^2+25Y+25)g(Z)-Z(Z^4+5Z^3+15Z^2+25Z+25)g(Y)}{Y-Z}$$

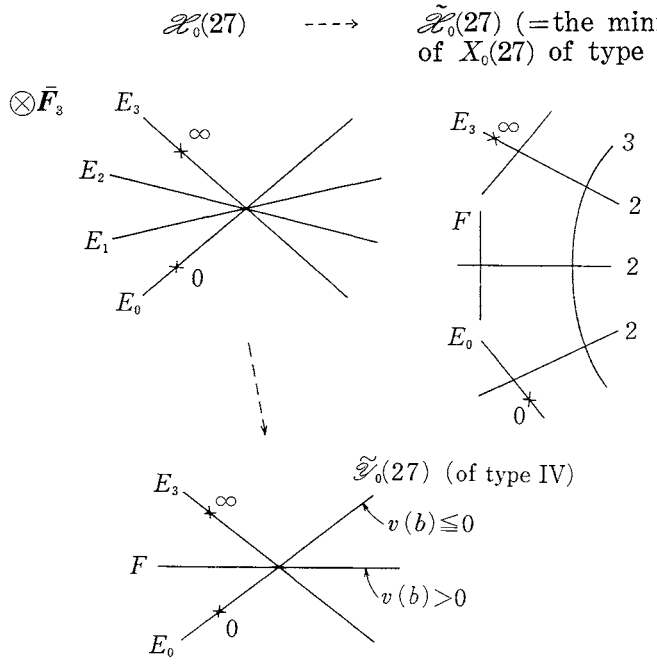
see loc.cit. The pair (w, w') of points defines a point on C defined by $(Y, Z)=(\sqrt{5}\,b, -\sqrt{5}\,b^\sigma)$. But the equation (3.2.3) gives the congruence $b^4+3b^2+1\equiv 0 \bmod (\sqrt{5})$. Thus we get a contradiction.

Proof for $p=3$ *and* $r\geqq 4$. The same argument as for $p=7$ gives the result, except for the case when $j(x)\equiv 0 \bmod \mathfrak{p}$. We first describe the $\boldsymbol{Q}$-rational points on $X_0^+(3^{2t})$ for $t\geqq 2$. The modular curve $X_0^+(81)$ is an elliptic curve and it is isogenous over $\boldsymbol{Q}$ to $X_0(27)$ [24] Table 5 pp. 135–141. Then $X_0^+(81)$ has three $\boldsymbol{Q}$-rational points [24] Table 1 pp. 81–113. Indeed, $X_0^+(3^{2t})$ $(t\geqq 2)$ has three $\boldsymbol{Q}$-rational points. One of them is a cusp and the others are C. M. points whose special fibres at the rational prime 3 are the sections of $(E_0\cup E_{2t})^h/\langle w_{3^{2t}}\rangle$. These C. M. points are represented by elliptic curves E and F $(/\boldsymbol{Q})$ which are isomorphic over $\boldsymbol{C}$ to $\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}\sqrt{-2}$ and $\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}(1+\sqrt{-11})/2$, respectively. Let c, $\bar{c}$ (resp. d, $\bar{d}$) be the endomorphisms of E (resp. F) corresponding to $1+\sqrt{-2}$ and $1-\sqrt{-2}$ (resp. $(1+\sqrt{-11})/2$ and $(1-\sqrt{-11})/2$) under the isomorphism $\mathrm{End}\,E\simeq\boldsymbol{Z}[\sqrt{-2}]$ (resp. $\mathrm{End}\,F\simeq\boldsymbol{Z}[(1+\sqrt{-11})/2]$). Put $A=\ker(c^t\colon E\to E)$, $\bar{A}=\ker(\bar{c}^t\colon E\to E)$, $B=\ker(d^t\colon F\to F)$ and $\bar{B}=\ker(\bar{d}^t\colon F\to F)$. Then the C. M. points are represented by the pairs $(E, \{A, \bar{A}\})$ and $(F, \{B, \bar{B}\})$.

Now consider the case for odd integers $r\geqq 5$. As was seen as above, it suffices to discuss the case for $r=5$ and $j(x)\equiv 0 \bmod \mathfrak{p}$. We make use of the minimal models of $X_0(27)$ over the basis $\boldsymbol{Z}_3$ and $\boldsymbol{Z}_3[\sqrt{-3}]$, and the equation of $X_0(9)$. The modular curve $X_0(9)$ is defined by the equation

(3.2.4)
$$j=g(X)/X(X^2+9X+27)$$

with $w_9^*(X)=27/X$, where $g(X)=(X^4+4\cdot 3X^3+2\cdot 27X^2+28\cdot 3X+3)^3$ [4] IV §2. Let z be the image of x under the morphism of $X_0(3^5)$ to $X_0(9)$ defined by $(E, A)\mapsto(E/A_3, A_{27}/A_3)$. Then z is defined by $X=a$ for $a\in k^\times$. Since $v(j(z))>0$, using the equation (3.2.4), we see that $v(a)=1/2$, 1, 3/2, 2 or 5/2. Let $\tilde{\mathscr{Y}}_0(27)\to\mathrm{Spec}\,\boldsymbol{Z}[(1+\sqrt{-3})/2]$ be the minimal model of $X_0(27)\otimes\boldsymbol{Q}(\sqrt{-3})$ ([24] Table 1 pp. 81-113).



LEMMA (3.2.5). *Let z be a $\boldsymbol{Q}_5^{ur}(\sqrt{-3})$-rational section of $\mathscr{X}_0(27)$ whose special fibre is the supersingular point. Denote also by z the $W(\bar{\boldsymbol{F}}_3)[\sqrt{-3}]$-section of the Néron model $\mathscr{E}=\tilde{\mathscr{Y}}_0(27)^{\mathrm{smooth}}$ defined by z. Then $z\otimes\bar{\boldsymbol{F}}_3$ is a section of the irreducible component F see above.*

PROOF. The modular curve $X_0(27)\otimes\boldsymbol{Q}(\sqrt{-3})$ is defined by the equation

$$\text{(3.2.6)}\qquad \begin{cases} Z^2=Y^4+4Y^3+6Y-3 \\ Y=(\sqrt[3]{3X^2+3X+1}-1)/(X+1) \end{cases}$$

with $w_{27}^*(Y)=Y$ and $w_{27}^*(Z)=-Z$ [4] IV §2. Here the function X in (3.2.6) is the same function in (3.2.4) see loc.cit. Blowing up along the super-

singular point $(Y, Z, \sqrt{-3})=(0, 0, 0)$, we get the minimal model $\tilde{\mathscr{Y}}_0(27)$. The section z of $X_0(27)$ is defined by $(X, Y, Z)=(a, b, c)$ for $a, b, c \in \boldsymbol{Q}_3^{ur}(\sqrt{-3})$. By the condition $v(j(z))>0$, we get $v(a)=1/2, 1, 3/2, 2$ or $5/2$ (3.2.4). Then by (3.2.6), $v(b)\geqq 1$. Further, if $z\otimes\bar{\boldsymbol{F}}_3$ is a section of $E_0\backslash\{\text{supersingular point}\}$, then $v(b)\leqq 0$. Therefore $z\otimes\bar{\boldsymbol{F}}_3$ is a section of $E_2\cup F$. But if $z\otimes\bar{\boldsymbol{F}}_3$ is a section of E_2 $(\subset\mathscr{E})$, then $w_3(z)\otimes\bar{\boldsymbol{F}}_3$ becomes a section of E_0. Thus $z\otimes\bar{\boldsymbol{F}}_3$ is a section of F. □

Let C be the schematic closure of the finite group $\langle \mathrm{cl}((0)-(\infty))\rangle$ in $\mathscr{E}$. Then by the construction of $\mathscr{E}$ (see above), we see that C is an étale subgroup of order 3 (cf. [24] Table 1 pp. 81–113). Let $f=f_{5,3}$ be the morphism of $\mathscr{X}_0(3^5)^{\mathrm{smooth}}$ to $J_0(27)_{/\boldsymbol{Z}}=J_0^-(27)_{/\boldsymbol{Z}}$ defined in §1. Then $f(x)\equiv m\,\mathrm{cl}((0)-(\infty))$, for an integer m, $0\leqq m\leqq 3$, since $J_0(27)(\boldsymbol{Q})=\langle \mathrm{cl}((0)-(\infty))\rangle$. Let $\mathscr{E}_0$ be the special fibre $\mathscr{E}\otimes\bar{\boldsymbol{F}}_3$ and $\mathscr{E}_0^0$ be the connected component of $\mathscr{E}_0$ of the unit section. Then $\mathscr{E}_0/\mathscr{E}_0^0\simeq \boldsymbol{Z}/3\boldsymbol{Z}$ and $\mathscr{E}_0/\mathscr{E}_0^0$ is generated by $\mathrm{cl}((0)-(\infty))\mathscr{E}_0^0$ (see the special fibre $\mathscr{E}_0$ as above). Then Lemma (3.2.5) shows that $f(x)\in\mathscr{E}_0^0$, so that $m=0$ and $f(x)=0$ (the unit section). Let E be an elliptic curve with a cyclic subgroup A of order 3^5 such that the pair (E, A) represents x. Then $(E/A_{27}, E_{27}/A_{27})\simeq (E/A, (E_{27}+A)/A)$ over $\boldsymbol{C}$. Therefore E is an elliptic curve with complex multiplication. Then for a $\boldsymbol{Q}$-rational point y on $X_0^+(3^5)$ and a section x of the fibre $X_0(3^5)_y$ at y, we see easily that $x\otimes\kappa(y)$ is a section of $E_0^h\cup E_5^h$.

Proof for $p=2$ *and* $r\geqq 6$. The same argument as for $p=7$ gives the result, except for the case when $j(x)\equiv 0 \bmod y$. We first describe the $\boldsymbol{Q}$-rational points on $X_0^+(2^t)$ for $t\geqq 3$. The modular curve $X_0^+(64)$ is an elliptic curve and it is isogenous over $\boldsymbol{Q}$ to $X_0(32)$ [24] Table 5 pp. 135–141. There are at most four $\boldsymbol{Q}$-rational points on $X_0^+(64)$ [24] Table 1 pp. 81–113. Indeed, $X_0^+(64)$ has four $\boldsymbol{Q}$-rational points. Two of them are cusps and the others are C. M. points. These special fibres at the rational prime 2 are sections of $(E_0\cup E_1\cup E_5\cup E_6)^h/\langle w_{64}\rangle$. We expain the corresponding C. M. points on $X_s^n(2^t)$ for $t\geqq 3$. Let E be an elliptic curve defined over $\boldsymbol{Q}$ which is isomorphic over $\boldsymbol{C}$ to $\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}(1+\sqrt{-7})/2$. Let c, $\bar{c}$ be the endomorphisms of E corresponding to $(1+\sqrt{-7})/2$ and $(1-\sqrt{-7})/2$ under the isomorphism $\mathrm{End}\,E\simeq\boldsymbol{Z}[(1+\sqrt{-7})/2]$. Let e, $\bar{e}$ be generators of the cyclic subgroups $A=\ker(c^t: E\to E)$ and $\bar{A}=\ker(\bar{c}^t: E\to E)$, respectively. Put $B=\langle e+2^{t-1}\bar{e}\rangle$ and $\bar{B}=\langle \bar{e}+2^{t-1}e\rangle$. Then the C. M. points on $X_s^n(2^t)$ $(t\geqq 3)$ are represented by the pairs

$(E, \{A, \bar{A}\})$ and $(E, \{B, \bar{B}\})$.

Now consider the case for odd integers $r \geqq 7$. As noted as above, it suffices to consider the case when $r=7$ and $j(x) \equiv 0 \bmod \mathfrak{p}$. We make use of the equation of $X_0(8)$, $X_0(16)$ [4] IV and the minimal model of $X_0(32)$ [24] Table 1 pp. 81-113. The modular curve $X_0(16)$ is defined by the equation

$$j = g(X)/X(X+4)(X^2+4X+8)(X+2)^4 \tag{3.2.7}$$

with $w_{16}^*(X) = 8/X$, where $g(X) = (X^8+2^4X^7+7\cdot 2^4X^6+7\cdot 2^6X^5+69\cdot 2^4X^4+13\cdot 2^7X^3+11\cdot 2^7X^2+2^9X+2^4)^3$ [4] IV §1. The modular curve $X_0(32)$ is defined by the equation

$$C\colon\ Y^2 = X^3+6X^2+16X+16 \tag{3.2.8}$$

with $w_{32}^*(X) = 8(2X+4-Y)/X^2$ [4] IV §1. Here the function X in (3.2.8) is the same function in (3.2.7). The lemma below shows that if $v(j(x))>0$, then the rational prime 2 ramifies in k.

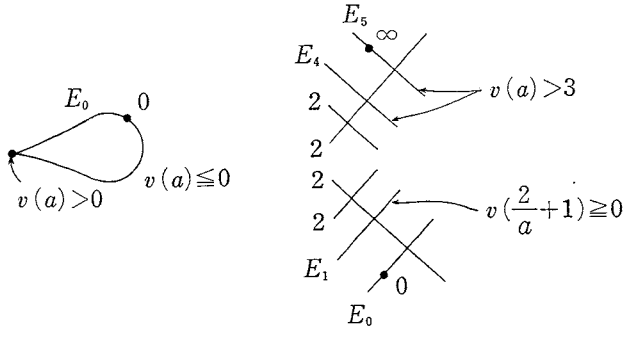
LEMMA (3.2.9). *Let z be a $\boldsymbol{Q}_2^{ur}$-rational point on $X_0(32)$. Then $v(j(z)) \leqq 0$.*

PROOF. The point z is defined by $(X, Y) = (a, b)$ for $0 \neq a, b \in \boldsymbol{Q}_2^{ur}$. Repeating the quadratic transformation, we get the minimal model $\tilde{\mathscr{X}}_0(32) \to \operatorname{Spec} \boldsymbol{Z}$ (3.2.7) (3.2.8) [24] Table 1 pp. 81-113:

$$C \quad \longleftarrow \quad \tilde{\mathscr{X}}_0(32) \qquad \text{(of type I*3)}$$

$\otimes \bar{\boldsymbol{F}}_2$

(3.2.10)



Using the equation (3.2.7), we see that if $v(j(z))>0$, then $v(a)=1$ or 2. Since x defines the $W(\bar{\boldsymbol{F}}_2)$-section of the Néron model $\tilde{\mathscr{X}}_0(32)^{\text{smooth}}$,

$v(a)\neq 2$ see (3.2.10). If $v(a)=1$, then by the equation (3.2.8), $v(b)\geqq 2$. The point $z'=w_{32}(z)$ is defined by $(X, Y)=(8(2a+4-b)/a^2, b')$ for $b'\in \boldsymbol{Q}_2^{ur}$ (3.2.8) and $v(j(z'))>0$. Then $v(8(2a+4-b)/a^2)\geqq 2$. Thus $v(j(z))\leqq 0$. □

The lemma below makes complete the proof of Theorem (3.2) for $p=2$.

LEMMA (3.2.11). *Let K be a quadratic extension of $\boldsymbol{Q}_2^{ur}$. Let z be a K-rational point on $X_0(32)$ such that $z'=w_{32}(z)=z^\sigma$ for $1\neq\sigma\in \mathrm{Gal}(K/\boldsymbol{Q}_2^{ur})$. Then $v(j(z))\leqq 0$.*

PROOF. Suppose $v(j(z))>0$. Then by Lemma (3.2.9), z is not defined over $\boldsymbol{Q}_2^{ur}$. Let z_1 (resp. z_2) be the image of z under the morphism of $X_0(32)$ to $X_0(8)$ (resp. $X_0(16)$) defined by $(E, A)\mapsto(E/A_2, A_{16}/A_2)$ (resp. $(E, A)\mapsto(E/A_2, A/A_2)$). Then $j(z_1)=j(z_2)$ and $w_8(z_1)=z_1^\sigma$. The point z_2 is defined by $X=c$ for $c\in K^\times$ (3.2.7). Let π be a prime element of $\mathcal{O}_K$. Using the equation (3.2.7), we see that $v(c)=1/2$, 1, 3/2, 2 or 5/2. Further we get

If $v(c)=1/2$, then $v(j(z_2))=8+3/2$ for $n=2\cdot v((c/\pi)^8+16/\pi^8)$.
If $v(c)=1$, then $2\nmid c/2+1$ and $v(j(z_2))=4-2n$ for

$$n=2\cdot v\left(\frac{c}{2}+1\right).$$

If $v(c)=3/2$, then $4\nmid c^2/8+c/2+1$ and $v(j(z_2))=2-n/2$ for

$$n=2\cdot v\left(\frac{c^2}{8}+\frac{c}{2}+1\right).$$

If $v(c)=2$, then $4\nmid c/4+1$ and $v(j(z_2))=2-n/2$ for

$$n=2\cdot v\left(\frac{c}{4}+1\right).$$

If $v(c)=5/2$, then $v(j(z_2))=1$.

In all cases above, $v(j(z_2))\neq 3$. The modular curue $X_0(8)$ is defined by the equation

$$j=2^8(Z^4+8Z^3+20Z^2+16Z+1)^3/Z(Z+4)(Z+2)^2 \tag{3.2.12}$$

with $w_8^*(Z)=8/Z$ [4] IV §1. Then z_1 is defined by $Z=d$ for $d\in K^\times$. Since $w_8(z_1)=z_1^\sigma$, $d=8/d$ and $v(d)=3/2$. Then by the equation (3.2.12), $v(j(z_1))=3$. This contradicts that $j(z_1)=j(z_2)$. □

PROPOSITION (3.3). *Let (p, r) be a pair as in* (1.0), *x and $\mathfrak{p}$ be as at the beginning of this section. Let $f=f_{r,s}$ be the morphism of $\mathscr{X}_0(p^r)^{\text{smooth}}$ to the Néron model $J_0(p^s)_{/Z}$ defined in* §1. *If $x\otimes\kappa(\mathfrak{p})$ is a section of $E_0^h\cup E_r^h$, then $f(x)\otimes\kappa(\mathfrak{p})=0$ ($=$the unit section of $J_0(p^s)_{/Z}\otimes\boldsymbol{F}_p$).*

PROOF. The rational prime p splits in k (3.1). If $x\otimes\kappa(\mathfrak{p})$ is a cusp, then $x\otimes\kappa(\mathfrak{p})=0\otimes\kappa(\mathfrak{p})$ or $\infty\otimes\kappa(\mathfrak{p})$, and $f(x)\otimes\kappa(\mathfrak{p})=0$. If $x\otimes\kappa(\mathfrak{p})$ is not a cusp, then $x\otimes\kappa(\mathfrak{p})$ is represented by an elliptic curve $C/\kappa(\mathfrak{p})=\boldsymbol{F}_p$ with the cyclic subgroup $B=\ker(F^r: C\to C=C^{(p^r)})$ or $B=\ker(V^r: C=C^{(p^r)}\to C)$ (1.8). Let $\pi=\pi_{r,s}$ be the natural morphism of $\mathscr{X}_0(p^r)$ to $\mathscr{X}_0(p^s)$: $(E, A)\mapsto(E, A_{p^s})$ for a triple (p, r, s) as in (1.5). Then $w_{p^s}\pi(x)\otimes\kappa(\mathfrak{p})$, $\pi w_{p^r}(x)\otimes\kappa(\mathfrak{p})$ are represented by the pairs $(C/B_{p^s}, C_{p^s}/B_{p^s})$ and $(C/B, (C_{p^s}+B)/B)$, respectively. Using the Frobenius map or the Verschiebung, we see that the pair $(C/B_{p^s}, C_{p^s}/B_{p^s})$ is isomorphic to $(C/B, (C_{p^s}+B)/B)$ see [16] (3.3). Then $w_{p^s}\pi(x)\otimes\kappa(\mathfrak{p})=\pi w_{p^r}(x)\otimes\kappa(\mathfrak{p})$ and $f(x)\otimes\kappa(\mathfrak{p})=0$. □

PROPOSITION (3.4). *Let x and f be as in* (3.3) *above, and let f^+, $\tilde{f}$ be the morphisms defined in* §1 *for a triple (p, r, s) in* (1.5). *For $p\neq5$, if $f(x)\otimes\kappa(\mathfrak{p})=0$, then $\tilde{f}(x)=0$. If moreover the Mordell-Weil group of $J_0^-(p^s)$ is of finite order, then $f^+(y)=0$ for $y=\{x, w_{p^r}(x)\}$.*

PROOF. The $\boldsymbol{Q}$-rational section $\tilde{f}(x)$ of $\tilde{J}_0(p^s)$ (for $p\neq5$, 7) or $\tilde{J}_0(169)_{(7)}$ is of finite order (1.3) (1.4). For the simplicity, we here denote $\tilde{J}_0(169)$ instead of $\tilde{J}_0(169)_{(7)}$. For $p\neq2$, 5, $\tilde{f}(x)$ generates a finite étale subgroup of the Néron model $J_0(p^s)_{/Z[1/2]}$. The group of $\boldsymbol{Q}$-rational points $J_0(32)(\boldsymbol{Q})$ is generated by the class $\mathrm{cl}((0)-(\infty))$ of order 4 [24] Table 1 pp. 81–113. Further we know that $\mathrm{cl}((0)-(\infty))\otimes\boldsymbol{F}_2$ is also of order 4 see loc.cit. (3.2.10). Therefore $\tilde{f}(x)$ generates a finite étale subgroup of $J_0(p^s)_{/Z_p}$ (for $p\neq5$). Then the assumption $\tilde{f}(x)\otimes\boldsymbol{F}_p=0$ leads $\tilde{f}(x)=0$. If moreover the Mordell-Weil group of $J_0^-(p^s)$ is of finite order, then $f^+(y)$ generates a finite étale subgroup of $J_0^-(p^s)_{/Z_p}$ and $f^+(y)=0$. □

PROPOSITION (3.5). *Let x, y and f^+ be as in* (3.4) *above. If $p\neq37$ and $f^+(y)=0$, then y is a C. M. point.*

PROOF. Let (E, A) be a pair which represents the point x. Then $w_{p^s}\pi(x)$ and $\pi w_{p^r}(x)$ are represented by $(E/A_{p^s}, E_{p^s}/A_{p^s})$ and $(E/a, (E_{p^s}+A)/A)$, respectively. If $X_0^+(p^s)\simeq\boldsymbol{P}^1$, then $J_0^-(p^s)=J_0(p^s)$ and the assumption $f^+(y)=0$ leads that $w_{p^s}\pi(x)=\pi w_{p^r}(x)$. Then $E/A_{p^s}\simeq E/A$ over $\boldsymbol{C}$ and A/A_{p^s} is a cyclic subgroup of order $p^{r-s}\neq1$, so that E is an elliptic curve with complex multiplication. Now consider the case

when $X_0^+(p^s)\neq \boldsymbol{P}^1$. The condition $f^+(y)=0$ gives the linearly equivalence relation below

$$(\pi w_{p^s}(x))+(\pi(x))\sim(w_{p^s}\pi(x))+(w_{p^s}\pi w_{p^r}(x)).$$

If $\pi(x)=w_{p^s}\pi(x)$ or $w_{p^s}\pi w_{p^r}(x)$, then the same argument as above shows that x is a C. M. point. In the other case, $X_0(p^s)$ must have the hyperelliptic involution γ such that $\gamma\pi(x)=\pi w_{p^r}(x)$. We know that if $X_0^+(p^s)\neq \boldsymbol{P}^1$, then $X_0(p^s)$ is not hyperelliptic, except for $(p, s)\neq(37, 1)$ [17] [18]. □

THEOREM (3.6). *For the following pairs (p, r), $n(p, r)=0$:*

p	r
2	$\geqq 6$
3	$\geqq 4$
7	$\geqq 3$
11	$\geqq 2$
$p\geqq 17$	$\geqq 2$ *if* $p\neq 37$ *and* $\sharp J_0^-(p)(\boldsymbol{Q})<\infty$.

PROOF. Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(p^r)$ and $x, x'=w_{p^r}(x)$ be the sections of the fibre $X_0(p^r)_y$ at y. For $p\geqq 3$, Theorem (3.2) and Proposition (3.3) show that $f(x)\otimes\kappa(\not{s})$ is the unit section of $J_0(p^s)_{/\boldsymbol{Z}}\otimes\boldsymbol{F}_p$. Then for any pair (p, r) $(p\geqq 3)$ as above, Proposition (3.4) and Proposition (3.5) show that y is a C. M. point. As was seen in the proof of Theorem (3.2), $X_0^+(2^{2t})(\boldsymbol{Q})$ $(t\geqq 3)$ consists of two cusps and two C. M. points. There remains the case for $X_0^+(2^r)$ for odd integers $r\geqq 7$.

LEMMA (3.6.1). *Let z_1, z_2 be $\boldsymbol{Q}$-rational points on $X_0^+(2^7)$. If $z_1\otimes\boldsymbol{F}_2=z_2\otimes\boldsymbol{F}_2$, then $z_1=z_2$. In particular, for a non cuspidal $\boldsymbol{Q}$-rational point z on $X_0^+(2^7)$, $z\otimes\boldsymbol{F}_2$ is not a cusp.*

PROOF. Let x_i and $x_i'=w_{2^7}(x_i)$ be the sections of the fibre $X_0(2^7)_{z_i}$ at z_i for $i=1, 2$. Then x_i and x_i' are defined over $\boldsymbol{Q}_2$ and they are the sections of $E_0^h\cup E_1^h\cup E_6^h\cup E_7^h$ (3.1) (3.2). If $z_1\otimes\boldsymbol{F}_2=z_2\otimes\boldsymbol{F}_2$, then changing x_2 by x_2', if necessary, we may assume that $x_1\otimes\boldsymbol{F}_2=x_2\otimes\boldsymbol{F}_2$. Let $f=f_{7,5}$ be the morphism of $\mathscr{X}_0(2^7)^{\text{smooth}}$ to $J_0(32)_{/\boldsymbol{Z}}$ defined in §1. Then $f(x_1)\otimes\boldsymbol{F}_2=f(x_2)\otimes\boldsymbol{F}_2$, and $f(x_1)$ and $f(x_2)$ are contained in the finite étale subgroup of order 4 generated by the class $\mathrm{cl}((0)-(\infty))$ [24] Table 1 pp. 81–113 (3.2.10). Therefore $f(x_1)=f(x_2)$. Then applying Proposition (1.14), we get $x_1=x_2$, hence $z_1=z_2$. □

Lemma (3.6.1) and Theorem (3.2) show that there are at most four $\boldsymbol{Q}$-rational points on $X_0^+(2^r)$ for any odd integer $r \geqq 7$. Two of them are the cusps $\{0, \infty\}$ and $\left\{\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}11\\2^{r-1}\end{pmatrix}\right\}$. There is a $\boldsymbol{Q}$-rational point on $X_0^+(2^r)$ which is represented by elliptic curves with complex multiplication. Let E be an elliptic curve defined over $\boldsymbol{Q}$ which is isomorphic over $\boldsymbol{C}$ to $\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}(1+\sqrt{-7})/2$. Let c, $\bar{c}$ be the endomorphisms of E which correspond to $(1+\sqrt{-7})/2$ and $(1-\sqrt{-7})/2$ under the isomorphism $\mathrm{End}\, E \simeq \boldsymbol{Z}[(1+\sqrt{-7})/2]$, respectively. Put $A=\ker(c^r: E \to E)$ and $\bar{A}=\ker(\bar{c}^r: E \to E)$. Then $(E/A, E_{2^r}/A) \simeq (E, \bar{A})$ over $\boldsymbol{C}$ and the set $\{(E, A), (E, \bar{A})\}$ represents the C. M. point on $X_0^+(2^r)$. The special fibre at the rational prime 2 of this C. M. point is a section of $(E_0 \cup E_r)^h/\langle w_{2^r}\rangle$. In the rest of the proof, we will show that $X_0^+(2^r)(\boldsymbol{Q})$ consists of these three points for any odd integer $r \geqq 7$. Suppose that there exists another $\boldsymbol{Q}$-rational point y on $X_0^+(2^r)$ and let $x, x'=w_{2^r}(x)$ be the sections of the fibre $X_0^+(2^r)_y$ at y. Then x and x' are defined over a quadratic field k in which the rational prime $p=2$ splits, and $x'=x^\sigma$ for $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$ (1.1) (3.1) (3.2). Let $\mathfrak{p}$ be a prime of k lying over the rational prime 2. Then by (3.2) and (3.6.1), $x \otimes \kappa(\mathfrak{p})$ and $x' \otimes \kappa(\mathfrak{p})$ are the sections of $E_1^h \cup E_6^h$. Let $z, z'=w_{32}(z)$ be the images of x and x' under the morphism of $X_0(2^r)$ to $X_0(32)$ defined by $(E, A) \mapsto (E/A_2, A_{64}/A_2)$. Then $z'=z^\sigma$ for $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$. These points z and z' are defined by $(X, Y)=(a, b)$ and $(X, Y)=(8(2a+4-b)/a^2, b')$ for $0 \neq a, b, b' \in k$ with $a^\sigma=8(2a+4-b)/a^2$ (3.2.7) (3.2.8). For a prime $\mathfrak{p}$ of k, $v_\mathfrak{p}$ denotes the normalized valuation of $k_\mathfrak{p}$.

CLAIM. For $\mathfrak{p} \nmid 2$, $v_\mathfrak{p}(a)=0$ and $(v_\mathfrak{p}(a), v_{\mathfrak{p}'}(a))=(3, 0)$ or $(0, 3)$, where $\mathfrak{p}\mathfrak{p}'=2\mathcal{O}_k$.

PROOF. Using the equation (3.2.7), we see that $v_\mathfrak{p}(a)$, $v_\mathfrak{p}(a^\sigma)=v_{\mathfrak{p}'}(a)$ are equal to 0, 1, 2 or 3. The sections $z \otimes \kappa(\mathfrak{p})$ and $z' \otimes \kappa(\mathfrak{p})$ are contained in $E_0^h \cup E_5^h$. Then by (3.2.10), we see that $(v_\mathfrak{p}(a), v_{\mathfrak{p}'}(a))=(3, 0)$ or $(0, 3)$. The class $\mathrm{cl}((0)-(\infty))$ generates a finite étale subgroup scheme in the Néron model $J_0(32)_{/\boldsymbol{Z}[1/2]}$ and $J_0(32)(\boldsymbol{Q})=\langle \mathrm{cl}((0)-(\infty))\rangle$ [24] Table 1 pp. 81–113, (3.2.10). Applying (1.14), we see that $z \otimes \kappa(\mathfrak{p})$ is not a cusp for any prime $\mathfrak{p} \nmid 2$. Then by (3.2.7), $v_\mathfrak{p}(a)=0$ for all $\mathfrak{p} \nmid 2$. □

Changing x by x', if necessary, we may assume that $x \otimes \kappa(\mathfrak{p})$ is a section of E_1^h. Then by the claim above, $a\mathcal{O}_k=\mathfrak{p}'^3$, $a^\sigma\mathcal{O}_k=\mathfrak{p}^3$ and $aa^\sigma=$

± 8. By the relations tnat $a^\sigma = 8(2a+4-b)/a^2$ and (3.2.8), there are two possibilities: (i) $a=(-5\pm\sqrt{-7})/2$ and (ii) $a=(3\pm\sqrt{41})/2$. The first case corresponds to the C. M. point. By our assumption, the rational point y corresponds to the second case. The section x is represented by a pair (E, A) for an elliptic curve E with a cyclic subgroup A of order 2^7 defined over $k=\boldsymbol{Q}(\sqrt{41})$. Put $(F, B)=(E/A_2, A/A_2)$, and let λ, $\hat{\lambda}$ be the characters of the idèle group $k_A^\times$ induced by the Galois action of $\mathrm{Gal}(\bar{k}/k)$ on $A(\bar{k})$ and $E_{2^7}/A(\bar{k})$, respectively. Then $\lambda\hat{\lambda}$ is the cyclotomic character $\theta=\theta_{2^7}$ induced by the Galois action on $\mu_{2^7}(\bar{k})$. For each prime $\mathfrak{p}$ of k, let $\lambda_\mathfrak{p}$, $\hat{\lambda}_\mathfrak{p}$ be the restrictions of λ and $\hat{\lambda}$ to $\mathcal{O}_\mathfrak{p}^\times$ $(\subset k_A^\times)$.

CLAIM. Under the notation as above, $\lambda_\mathfrak{p}=1$ on $(\mathcal{O}_\mathfrak{p}^\times)^4$ and $\lambda_\mathfrak{p}^2=1$ for all primes $\mathfrak{p}\nmid 2$.

PROOF. For each prime $\mathfrak{p}$, let $I_\mathfrak{p}$ be the inertia subgroup of $\mathfrak{p}$. Let ρ be the representation of the Galois action on $F_4(\bar{k})$. The subgroup of 2-torsion points F_2 is decomposed into the direct sum $A_4/A_2\oplus E_2/A_2$. Then $\rho(\tau)^2=1$ for $\mathfrak{p}\nmid 2$ and $\tau\in I_\mathfrak{p}$. The elliptic curve E is isogenous over k to F, so that $\lambda_\mathfrak{p}^2=1$ for $\mathfrak{p}\nmid 2$. Since the modular invariant $j(x)\not\equiv 0 \bmod \mathfrak{p}$ and $k\hookrightarrow\boldsymbol{Q}_2$, E and F have good reduction over a quadratic extension K of $\boldsymbol{Q}_2^{ur}$. Let x_1 be the image of x under the morphism of $X_0(2^7)$ to $X_0(2^6)$: $(E, A)\mapsto(E/A_2, A/A_2)$. By our choice of x, $x_1\otimes\kappa(\mathfrak{p})$ is a section of E_0^h. Then the schematic closure $B_{/\mathcal{O}_K}$ of B in the Néron model $F_{/\mathcal{O}_K}$ is a finite étale group scheme of rank 2^6 (1.7). Then for $\tau\in(I_\mathfrak{p})^2$, $\lambda_\mathfrak{p}(\tau)=1$ or $1+2^6 \pmod{2^7}$. Therefore for $\tau\in(I_\mathfrak{p})^4$, $\lambda_\mathfrak{p}(\tau)=1$. □

Now we make complete the proof for $(p, r)=(2, 7)$. Let $u=32-5\sqrt{41}$ and $u'=32+5\sqrt{41}$ be the units of $\mathcal{O}_k=\boldsymbol{Z}[(1+\sqrt{41})/2]$. Then $\mathfrak{p}^5\| u-1$ or $\mathfrak{p}^5\| u'-1$. Changing u by u', if necessary, we may assume that $\mathfrak{p}^5\| u-1$. For $1\neq\sigma\in\mathrm{Gal}(k/\boldsymbol{Q})$, $x^\sigma=w_{2^7}(x)$ and $(E^\sigma, A^\sigma)\simeq(E/A, E_{2^7}/A)$ over a quadratic extension of k (, since $j(x)\neq 0$, 1728). Let λ^σ be the character of $k_A^\times$ induced by the Galois action on $A^\sigma(\bar{k})$. Then $\lambda^\sigma=\lambda\mu$ for a character μ of order 1 or 2. The conductor of $\mu_\mathfrak{p}=\mu|\mathcal{O}_\mathfrak{p}^\times$ divides $\mathfrak{p}^3$ and $\mu_\mathfrak{p}(u)=1$. Then under the identification of $\mathcal{O}_\mathfrak{p}^\times$ with $\boldsymbol{Z}_2^\times$, we get $\lambda_{\mathfrak{p}'}(u)=\lambda_{\mathfrak{p}'}^\sigma(u)=(u \bmod \mathfrak{p}^7)$. Therefore $1=\lambda(u)=\lambda_\mathfrak{p}(u)\lambda_{\mathfrak{p}'}(u)=(u \bmod \mathfrak{p}^7)$. This contradicts that $\mathfrak{p}^5\| u-1$. Thus we completed the proof. □

Further we get the following results.

THEOREM (3.7). *For $p\geqq 17$ and $r\geqq 2$,*

$$n(p, r) \leqq \dim J_0(p) - \dim \tilde{J}_0(p).$$

PROOF. Its proof is the same as that of Theorem (4.1) [16] §4. □

Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(p^r)$ represented by an elliptic curve $E/\boldsymbol{Q}$ with a cyclic subgroup A of order p^r. For a rational prime q, if E has potentially good reduction at q, then we say that y has potentially good reduction at q. If y is a C. M. point, then y has potentially good reduction at any rational prime q.

THEOREM (3.8). *Let y be a non cuspidal $\boldsymbol{Q}$-rational point without C. M. on $X_0^+(p^r)$. Then y has potentially good reduction at q for any triple (p, r, q) below:*

All primes q for the pairs (p, r) in Theorem (0.1), *and*

p	r	q	
13	$\geqq 3$	$q \neq 2, 13$	
$p \geqq 17$	$\geqq 2$	all q	*if* $p \equiv 1 \bmod 8$
		$q \neq 2$	*otherwise.*

PROOF. By the existence of the canonical coverings of $X_0^+(p^{r+2})$ to $X_0^+(p^r)$ §1, it suffices to show the theorem (3.8) for the pairs $(p, r) = (13, 3)$, $(13, 4)$, and $(p, 2)$, $(p, 3)$ for $p \geqq 17$. Let y be a $\boldsymbol{Q}$-rational point on $X_0^+(p^r)$ for a pair (p, r) as above, and x be a section of the fibre $X_0^+(p^r)_y$ at y. Then x is defined over a number field of degree $\leqq 2$. Let $\tilde{f} = \tilde{f}_{r,k}$ be the morphism of $X_0(p^r)$ to $\tilde{J}_0(p)$ $(p \geqq 17)$ or to $\tilde{J}_0(169)_{(7)}$ $(p = 13)$ defined in §1. If x is a cusp, then $x = 0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ or $\infty = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (1.6). Then by (3.2), (3.3) and (3.4), we know that $\tilde{f}(x)$ is the unit section. Suppose that $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$ for a cusp C and a prime $\mathfrak{p}$ of k. Changing x by $w_{p^r}(x)$, if necessary, we may assume that $C = \begin{pmatrix} i \\ p^m \end{pmatrix}$ for integers i and m, $0 \leqq m \leqq r/2$ (1.6). Then C is defined over $\boldsymbol{Q}(\zeta_{p^m})$, where ζ_{p^m} is a primitive p^m-th root of unity see loc.cit.. The class $\mathrm{cl}((C) - (\infty))$ is of finite order [10] §3 (3.2), and it generates a finite étale subgroup scheme of the Néron model $J_0(p^r)_{/Z[1/2p]}$ (2.1). First consider the case when $\mathfrak{p} \nmid 2p$. The condition that $\tilde{f}(x)$ is the unit section and the assumption on $\mathfrak{p}$ show that $\tilde{f}(C)$ is also the unit section. For $p = 13$, $r = 4$ and $C' = \begin{pmatrix} i \\ 169 \end{pmatrix}$, $\tilde{f}(C') = \mathrm{cl}((0) - (\infty))$, which is of order 7. Thus $m = 0$ or 1. Then Proposition (1.14) applied to x, C and f leads that $x = C$. If $\mathfrak{p} \mid p$ $(p \geqq 17)$, then by (3.2), $m = 0$. The rational prime 2 is of

order $\leqq 2$ in $\boldsymbol{Q}(\zeta_p)$, so that if $\ell \mid 2$, then $m=0$. Then Proposition (1.14) leads $x=C$. □

References

[1] Atkin, A. O. L. and J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. **185** (1972), 134–160.

[2] Berkovic, V. G., The rational points on the jacobians of modular curves, Math. USSR-Sb. **30** (1976), 485–500.

[3] Deligne, P. and M. Rapoport, Schémas de modules des courbes elliptiques, vol. II of the Proceedings of the International Summer School on Modular Functions, Antwerp, 1972. Lecture Notes in Math. vol. 349, Springer, Berlin-Heidelberg-New York, 1973.

[4] Fricke, R., Die Elliptischen Funktionen und ihre Anwendungen, Teubner, Leipzig-Berlin, 1922.

[5] Kenku, M. A., The modular curve $X_0(39)$ and rational isogeny, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23.

[6] Kenku, M. A., The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20.

[7] Kenku, M. A., The modular curve $X_0(169)$ and rational isogeny, J. London Math. Soc. (2) **22** (1981), 239–244.

[8] Kenku, M. A., On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$, J. London Math. Soc. (2) **23** (1981), 415–427.

[9] Lang, S., Elliptic Functions, Addison-Wesley, Reading Mass, 1973.

[10] Manin, Y., Parabolic points and zeta functions of modular forms, Math. USSR-Izv. **6** (1972), 19–64.

[11] Manin, Y., The p-torsion of elliptic curves is uniformly bounded, Math. USSR-Izv. **3** (1969), 433–438.

[12] Mazur, B., Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S. **47** (1977), 33–186.

[13] Mazur, B., Rational points on modular curves, Proceedings of Conference on Modular Functions held in Bonn, Lecture Notes in Math. vol. 601, Springer-Verlag, Berlin-Heidelberg-New York, 1977.

[14] Mazur, B., Rational isogenies of prime degree, Invent. Math. **44** (1978), 129–162.

[15] Mestre, J. F., Points rationnels de la courbe modulaire $X_0(169)$, Ann. Inst. Fourier (Grenoble), **30** (1980), 17–27.

[16] Momose, F., Rational points on the modular curves $X_{\mathrm{split}}(p)$, Comositio Math. **52** (1984), 115–137.

[17] Ogg, A., Hyperelliptic modular curves, Bull. Soc. Math. France **102** (1975), 449–462.

[18] Ogg, A., Über die Automorphismengruppe von $X_0(N)$, Math. Ann. **228** (1977), 279–292.

[19] Oort, F. and J. Tate, Group schemes of prime order, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

[20] Raynaud, M., Schémas en groupes de type $(p, \cdots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

[21] Serre, J. P., Propriétés galoissiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331.

[22] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan 11, Iwanami Shoten, Tokyo-Princeton Univ. Press, Princeton N.J., 1971.

[23] Tate, J., p-divisible groups, Proceedings of a Conference on a Local Fields, Driebergen, 1966, Springer-Verlag, Berlin, 1967, 158–183.
[24] Modular functions of one variable IV (Ed. By B. J. Birch and W. Kuyk), Lecture Notea in Math. vol. 476, Springer-Verlag, Berlin-Heidelberg-New York, 1975.

(Received December 28, 1983)

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan