J. Math. Soc. Japan
Vol. 39, No. 2, 1987

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

By Fumiyuki MOMOSE

(Received Jan. 5, 1984)
(Revised Sept. 18, 1985)

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 modular curve $X_0(N)$ is the coarse moduli space $/\boldsymbol{Q}$ of the isomorphism classes of the generalized elliptic curves E with a cyclic subgroup A of order N [**3**]. The fundamental involution w_N of $X_0(N)$ is defined by

$$(E, A) \longmapsto (E/A, E_N/A),$$

where $E_N = \ker(N : E \to E)$. Let $X_0^+(N)$ be the quotient $X_0(N)/\langle w_N \rangle$. The rational points on $X_0(N)$ are determined for all integers $N \geqq 1$ [**10**] [**5, 6, 7, 8**] [**12**]. We here discuss the rational points on $X_0^+(N)$. The author [**13, 14**] discussed the case when N are powers of a prime number. The similar method as in [**13, 14**] can be applied to the case for composite numbers N. There are $\boldsymbol{Q}$-rational points on $X_0^+(N)$ which are represented by elliptic curves with complex multiplication. We call these points *C.M. points*. Let $n(N)$ denote the number of the $\boldsymbol{Q}$-rational points on $X_0^+(N)$ which are neither cusps nor C.M. points. Then our result is as follows.

THEOREM (0.1). *Let N be a composite number. If N has a prime divisor p which satisfies the following conditions* (i) *and* (ii), *then* $n(N)=0$:
(i) $p \geqq 17$ *or* $p=11$.
(ii) $p \neq 37$ *and* $\#J_0^-(p)(\boldsymbol{Q}) < \infty$.
Here $J_0^-(p)$ is the quotient $J_0(p)/(1+w_p)J_0(p)$ of the jacobian variety $J_0(p)$ of $X_0(p)$ and w_p is the automorphism of $J_0(p)$ induced by the fundamental involution w_p of $X_0(p)$.

For the prime numbers p, $17 \leqq p < 300$, the condition (ii) above is satisfied, except for $p=37$, 151, 199, 227 and 277 [**9**] [**22**] table 5 pp. 135-141. We here describe a sketch of the proof of theorem (0.1). Let $f = f_{N,p}$ be the morphism of $X_0(N)$ to $J_0(p)$ defined by

$$f : (E, A) \longmapsto \mathrm{cl}((E/A_p, E_p/A_p) - (E/A, (E_p+A)/A)),$$

where A_p is the subgroup of A of order p. Then f defines a morphism

$f^+=f^+_{N,p}$ of $X_0^+(N)$ to $J_0^-(p)$. Firstly, using a result on the structure of $J_0(p)_{/\boldsymbol{Z}}\otimes\boldsymbol{F}_p$ etc. [9] Appendix 1, we show that $f^+(x)\otimes\boldsymbol{F}_p$ is the unit section for any non cuspidal $\boldsymbol{Q}$-rational point x on $X_0^+(N)$. Secondly, under the conditions (i) and (ii) as above, we show that $f^+(x)$ is the unit section. Finally, we show that the condition that $f^+(x)$ is the unit section leads to that x is a C.M. point.

In § 1, we prepare some results on modular curves $X_0(N)$ and some lemmas on elliptic curves. We will prove theorem (0.1) in § 2.

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 $\mathcal{O}_K$ denotes the ring of integers of K and $A_{/\mathcal{O}_K}$ denotes the Néron model of A over the base $\mathcal{O}_K$. Further $(A_{/\mathcal{O}_K}\otimes\bar{\boldsymbol{F}}_q)^0$ is the connected component of the unit section of the special fibre $A_{/\mathcal{O}_K}\otimes\bar{\boldsymbol{F}}_q$. For a quasi-finite flat group scheme G over $\mathcal{O}_K$, 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 $X_0(N)$.

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 $\Gamma_0(N)$. For a finite subgroup G of an elliptic curve and for an integer $d\geqq 1$, put $G_d=\ker(d:G\to G)$. Let $N=N'\cdot N''$ be a decomposition with coprime integers N' and N''. Let $w_{N'}$ be the canonical involution of $X_0(N)$ defined by

$$(E,\ A)\longmapsto(E/A_{N'},\ (E_{N'}+A)/A_{N'}).$$

The involutions $w_{N'}$ commute with each other. Let $X_0^+(N)$ be the quotient $X_0(N)/\langle w_N\rangle$ by the fundamental involution w_N. Let $g_0(N)$ (resp. $g_+(N)$) denote the genus of $X_0(N)$ (resp. $X_0^+(N)$). In § 2, we will discuss the $\boldsymbol{Q}$-rational points on $X_0^+(N)$ for composite integers N with $g_+(N)>0$. For any integer N with $g_+(N)>0$, we know that the set of the $\boldsymbol{Q}$-rational points $X_0(N)(\boldsymbol{Q})$ consists of cusps [10] [5, 6, 7, 8] [12].

Let N' be a positive divisor of N such that N/N' is a square of an integer $d>1$. Define a morphism of $X_0(N)$ to $X_0(N')$ by

$$(E,\ A)\longmapsto(E/A_d,\ A_{N'd}/A_d).$$

Then the morphism above induces a covering of $X_0^+(N)$ to $X_0^+(N')$. Let $J_0(N)$ and $J_0^+(N)$ denote the jacobian varieties of $X_0(N)$ and $X_0^+(N)$, respectively.

Further let J_d and J_d^+ denote the "new part" of $J_0(d)$ and $J_0^+(d)$ for each positive divisor d of N: Under the canonical identification of the space of the holomorphic cusp forms of weight 2 on $\Gamma_0(d)$ (resp. $\left\langle \Gamma_0(d), \begin{pmatrix} 0 & -1 \\ d & 0 \end{pmatrix} \right\rangle$) with the cotangent space of $J_0(d)$ (resp. $J_0^+(d)$), the cotangent space of J_d (resp. J_d^+) corresponds to the subspace spanned by the new forms of level d [1]. For each positive divisor d of N, $m(d)$ denotes the number of the positive divisors of N/d. Then the jacobian variety $J_0^+(N)$ is isogenous over $\boldsymbol{Q}$ to the following abelian variety:

$$\prod_{\substack{d \mid N \\ N/d \text{ is not square}}} J_d{}^{m(d)/2} \times \prod_{\substack{d \mid N \\ N/d \text{ is square}}} (J_d{}^{(m(d)-1)/2} \times J_d^+).$$

If $g_0(d)>0$ and d is not a power of 5, then $J_0(d)$ has a factor $/\boldsymbol{Q}$ with finite Mordell-Weil group [2] [9]. By the above formula, we see that $J_0^+(N)$ has a factor $/\boldsymbol{Q}$ with finite Mordell-Weil group, except for $N=65$, 91 and 5^r ($r \geqq 3$) loc. cit., [22] table 1 pp. 81-113, table 5 pp. 135-141.

(1.1) We will make use of the following morphisms. Let N' be a positive divisor of N and $N'=N_1' \cdot N_2'$ be a decomposition with coprime integers N_1' and N_2'. Let $\pi=\pi_{N,N'}$ be the natural morphism of $X_0(N)$ to $X_0(N')$:

$$(E, A) \longmapsto (E, A_{N'}).$$

Let $f=f_{N,N',N_1'}$ be the morphism of $X_0(N)$ to $J_0(N')$ defined by $f(z)=\mathrm{cl}((w_{N_1'}\pi(z))-(\pi w_N(z)))$, i. e.,

$$f : (E, A) \longmapsto \mathrm{cl}((E/A_{N_1'}, (E_{N_1'}+A_{N'})/A_{N_1'})-(E/A, (E_{N'}+A)/A)).$$

Then f induces a morphism $f^+=f^+_{N,N',N_1'}$ of $X_0^+(N)$ to the quotient $J_0^-(N', N_1')$ $=J_0(N')/(1+w_{N_1'})J_0(N')$:

$$\begin{array}{ccc} X_0(N) & \longrightarrow & X_0^+(N) \\ f \downarrow & \circlearrowright & \downarrow f^+ \\ J_0(N') & \longrightarrow & J_0^-(N', N_1'). \end{array}$$

If $N_1' \neq N$ and $g_0(N')>0$, then f is not a trivial morphism. Denote by $\mathfrak{X}_0(N)$ the normalization of the projective j-line $\mathfrak{X}_0(1) \simeq \boldsymbol{P}^1_{\boldsymbol{Z}}$ in the function field of $X_0(N)$. Let $\mathfrak{X}_0^+(N)$ denote the quotient $\mathfrak{X}_0(N)/\langle w_N \rangle$. Then $\mathfrak{X}_0^+(N) \otimes \boldsymbol{Z}[1/N]$ is smooth over $\boldsymbol{Z}[1/N]$, since $\mathfrak{X}_0(N) \otimes \boldsymbol{Z}[1/N]$ is smooth [3] and $w_N \otimes \boldsymbol{F}_2$ has fixed points of finite number. We denote also by $\pi=\pi_{N,N'}$ (resp. $f=f_{N,N',N_1'}$, resp. $f^+=f^+_{N,N',N_1'}$) the morphism of $\mathfrak{X}_0(N)$ to $\mathfrak{X}_0(N')$ (resp. the smooth part $/\boldsymbol{Z}$ $\mathfrak{X}_0(N)^{\mathrm{smooth}}$ to the Néron model $J_0(N')_{/\boldsymbol{Z}}$, resp. $\mathfrak{X}_0^+(N)^{\mathrm{smooth}}$ to $J_0^-(N', N_1')_{/\boldsymbol{Z}}$).

(1.2) ([3] V, VI.) Let p be a prime divisor of N with $r=\mathrm{ord}_p N$. Then the

special fibre $\mathfrak{X}_0(N)\otimes \boldsymbol{F}_p$ has $r+1$ irreducible components E_i for $0\leqq i\leqq r$. These irreducible components E_i are defined over $\boldsymbol{F}_p$ and intersect at the supersingular points on $\mathfrak{X}_0(N)\otimes \boldsymbol{F}_p$. Let $\zeta=\zeta_N$ be a primitive N-th root of unity. For each positive divisor d of N and an integer i, $0\leqq i<d$, prime to d, let $A_{d,i}$ be the subgroup of $\boldsymbol{G}_m\times \boldsymbol{Z}/(N/d)\boldsymbol{Z}$ generated by the section $(\zeta^i, 1 \bmod N/d)$. Let $\binom{i}{d}$ denote the cuspidal section of $\mathfrak{X}_0(N)$ which is represented by the pair $(\boldsymbol{G}_m\times \boldsymbol{Z}/(N/d)\boldsymbol{Z}, A_{d,i})$ for the integers d and i as above. For $d=1$ and N, we denote $\mathbf{0}=\binom{0}{1}$ and $\infty=\binom{1}{N}$. We choose the irreducible components E_j so that $\binom{i}{d}\otimes \boldsymbol{F}_p$ are the sections of E_j for the positive divisor d of N with $j=\mathrm{ord}_p d$. For a subscheme Y of a modular curve $X/\boldsymbol{Z}$, Y^h denotes the open subscheme of Y obtained by excluding the supersingular points on $Y\otimes \boldsymbol{F}_p$. Then E_0^h and E_r^h are smooth over $\boldsymbol{F}_p$. For an integer i, $1\leqq i\leqq r/2$, E_i^h has the multiplicity $p^{i-1}(p-1)$. The irreducible component 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 subgroup scheme A such that $A\simeq \boldsymbol{Z}/N\boldsymbol{Z}$ (resp. $A\simeq \mu_{p^r}\times \boldsymbol{Z}/(N/p^r)\boldsymbol{Z}$), locally for the étale topology. Let $N=N'\cdot N''$ be a decomposition with coprime integers N' and N''. If $p\nmid N'$, then $w_{N'}$ fixes E_i for all i. If $p\mid N'$, then $w_{N'}$ exchanges E_i by E_{r-i}. Now assume $p\| N$, i.e., $\mathrm{ord}_p N=1$. Let $\pi=\pi_{N,N/p}$ be the natural morphism of $\mathfrak{X}_0(N)$ to $\mathfrak{X}_0(N/p)$: $(E, A)\mapsto (E, A_{(N/p)})$. Let x be a supersingular point on $\mathfrak{X}_0(N)\otimes \boldsymbol{F}_p$ and $(E, A)_{/\bar{\boldsymbol{F}}_p}$ be a pair which represents $\pi(x)$. Then the completion of the local ring at x $(\otimes W(\bar{\boldsymbol{F}}_p))$ is isomorphic to

$$W(\bar{\boldsymbol{F}}_p)[[x, y]]/(xy-p^k)$$

for $k=(1/2)|\mathrm{Aut}(E, A)|$. When $p\geqq 5$, we know that if $k=2$, then the modular invariant $j(x)\equiv 1728 \bmod p$, and that if $k=3$, then $j(x)\equiv 0 \bmod p$.

(1.3) ([**3**] V lemme (2.8).) Let p be a prime number and K be a finite extension of $\boldsymbol{Q}_p{}^{ur}$ of degree e. Denote by R the ring of integers $\mathcal{O}_K$ of K with a prime element π. Let E be an elliptic curve over $\mathrm{Spec}\, R$ and A be a finite flat subgroup scheme of rank $(/R)$ p. Then

$$A\simeq \mathrm{Spec}\, R[x]/(x^p-\pi^a x)$$

for an integer a, $0\leqq a\leqq e$ [**17**] [**19**]. Let λ be the representation of $\mathrm{Gal}(\bar{K}/K)$ induced by the Galois action on $A(\bar{K})$. Then $\lambda=\theta_p{}^a$, where θ_p is the fundamental character loc. cit. Let z be the R-section of the fine moduli stack $\mathcal{M}_{\Gamma_0(N)}$ whose object is a pair $(E, A)_{/R}$. Assume that $z\otimes \bar{\boldsymbol{F}}_p$ is a supersingular point. Let $W(\bar{\boldsymbol{F}}_p)[[x, y]]/(xy-p)$ be the completion of the local ring at $z\otimes \bar{\boldsymbol{F}}_p$ such that the ideal (y, p) defines the locus of the irreducible component E_0 (1.2). Then $a\neq 0$ nor e, and $(z^*x, z^*y)=(\pi^a u, \pi^{e-a}u^{-1})$ for a unit u of R. On the

level of the coarse moduli space $\mathfrak{X}_0(p)$, the completion of the local ring along the section defined by $z\otimes\bar{\boldsymbol{F}}_p$ is isomorphic to

$$W(\bar{\boldsymbol{F}}_p)[[x', y']]/(x'y'-p^k)$$

for $k=(1/2)|\mathrm{Aut}(E\otimes\bar{\boldsymbol{F}}_p)|$ and $x'=x^k\times$(a unit), $y'=y^k\times$(a unit). Then the section z of $\mathfrak{X}_0(N)$ is defined by $(z^*x', z^*y')=(\pi^{ka}v, \pi^{k(e-a)}v^{-1})$ for a unit v of R.

We now prepare some lemmas on elliptic curves. Let K be a finite extension of $\boldsymbol{Q}_p{}^{ur}$ of degree e with $R=\mathcal{O}_K$. Let E be an elliptic curve defined over K with a cyclic subgroup A/K of order N. Let $A_{/R}$ denote the schematic closure of A in the Néron model $E_{/R}$. Then $A_{/R}$ is a quasi-finite flat subgroup scheme of $E_{/R}$ [**19**] § 2. Let x be an R-section of $\mathfrak{X}_0(N)$ such that $x\otimes K$ is represented by the pair (E, A).

LEMMA (1.4) ([**14**] lemma (2.2)). *Under the notation as above, assume that $E_{/R}$ is semi-stable and that $r=\mathrm{ord}_pN\geqq 2$. 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 of unity for $m(i)=\min\{i, r-i\}$.*

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

Let $n\geqq 3$ be an integer and

$$\rho_n : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}\, E_n(\bar{K}) \simeq \mathrm{GL}_2(\boldsymbol{Z}/n\boldsymbol{Z})$$

be the representation of the Galois action on the n-torsion points on an elliptic curve E over K. If $p\nmid n$, then the kernel of ρ_n is independent of n ($\geqq 3$, $p\nmid n$), and the image of ρ_n is contained in $\mathrm{SL}_2(\boldsymbol{Z}/n\boldsymbol{Z})$ [**21**]. Now assume $p\geqq 5$ and let L be the extension of K of degree $d=\#$(image of ρ_n) for $n\geqq 3$, $p\nmid n$. Then $E\otimes L$ has semi-stable reduction and $d=1$, 2, 3, 4 or 6 loc. cit. Put $e'=d$ if d is odd, and $e'=d/2$ if d is even.

LEMMA (1.5) ([**14**] corollary (2.3)). *Under the notation as above, assume that $r=\mathrm{ord}_pN\geqq 2$. Then*

(i) *If $x\otimes\bar{\boldsymbol{F}}_p$ is a section of E_i^h for an integer i, $1\leqq i\leqq r-1$, then $ee'\geqq p^{m(i)-1}(p-1)$ for $m(i)=\min\{i, r-i\}$.*

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

§ 2. Rational points on $X_0^+(N)$.

Let $N\geqq 1$ be a composite integer with the genus $g_+(N)>0$ of $X_0^+(N)$. Let N' be a positive divisor of N and $N'=N_1'\cdot N_2'$ be a decomposition with coprime integers N_1' and N_2'. Let $J_0^-(N', N_1')$ be the quotient $J_0(N')/(1+w_{N_1'})J_0(N')$ and $J_0^+(N', N_1')$ be the jacobian variety of $X_0(N')/\langle w_{N_1'}\rangle$. Further let $\pi=\pi_{N,N'}$,

$f=f_{N,N',N_1'}$ and $f^+=f^+_{N,N',N_1'}$ be the morphisms defined in (1.1). In this section, we always assume that

(2.1) $g_0(N')>0$, $N_1'\neq 1$ nor N, and $w_{N_1'}$ has fixed points if $g_0(N')=1$.

Under the assumption (2.1), the quotient $J_0^-(N', N_1')\neq\{0\}$. If $g_0(N')=1$, then $N'=11, 14, 15, 17, 19, 20, 21, 24, 27, 32$ or 36. For $(N', N_1')=(14, 2), (15, 3), (20, 5), (21, 7), (24, 3)$ and $(36, 9)$, $w_{N_1'}$ have no fixed point. Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(N)$. Let x and $x'=w_N(x)$ be the sections of the fibre $X_0(N)_y$ at y. Under the assumption $g_+(N)>0$, we know that $X_0(N)(\boldsymbol{Q})$ consists of cusps [**10**] [**5, 6, 7, 8**] [**12**]. Then x and x' are defined over a quadratic field k and $x'=x^\sigma$ for $1\neq\sigma\in\mathrm{Gal}(k/\boldsymbol{Q})$. These points x and x' are represented respectively by pairs (E, A) and $(E/A, E_N/A)$ for an elliptic curve E over k with a cyclic subgroup A /k of degree N [**3**] VI (3.2). The pair $(E/A, E_N/A)$ is isomorphic over $\boldsymbol{C}$ to (E^σ, A^σ).

There are rational points on $X_0^+(N)$ which are represented by elliptic curves with complex multiplication. We call them *C.M. points*. Let y be a $\boldsymbol{Q}$-rational C.M. point on $X_0^+(N)$ for an integer N with $g_+(N)>0$. Let x and $x'=w_N(x)$ be the sections of the fibre $X_0(N)_y$. These points x and x' are defined over a quadratic field and x is represented by an elliptic curve E over k with a cyclic subgroup A /k such that $E\otimes\boldsymbol{C}\simeq\boldsymbol{C}/\mathcal{O}$ for an order $\mathcal{O}$ of an imaginary quadratic field, changing x by x' if necessary. Then the class number $h(\mathcal{O})$ of $\mathcal{O}$ is one or two. Put $\mathfrak{a}=\{a\in\mathcal{O}\mid aA=\{0\}\}$. Then $(E/A)\otimes\boldsymbol{C}\simeq\boldsymbol{C}/\mathfrak{a}^{-1}$ and $E/A\simeq E^\sigma$ for $1\neq\sigma\in\mathrm{Gal}(k/\boldsymbol{Q})$. If $h(\mathcal{O})=2$, then E^σ is not isomorphic to E and $\mathfrak{a}$ is not a principal ideal of $\mathcal{O}$. We consider the case when N is not a prime number. There is an endomorphism $\alpha\in\mathcal{O}$ such that the principal ideal $\alpha\mathcal{O}$ divides $\mathfrak{a}$ and $\alpha\bar{\alpha}\neq N$, since $\mathfrak{a}$ is not principal if $h(\mathcal{O})=2$, where $\bar{\alpha}$ is the complex conjugate of α. Let $\mathfrak{b}$ be the ideal $\mathfrak{a}(\alpha)^{-1}$ and $\mathfrak{c}$ be an ideal such that $\mathfrak{b}\supset\mathfrak{c}\supset\mathfrak{a}$ and that the ideal $\mathfrak{c}\mathfrak{b}^{-1}$ is prime to $\mathfrak{b}$. Put $N'=\mathfrak{c}\bar{\mathfrak{c}}$ and $N_1'=\mathfrak{b}\bar{\mathfrak{b}}$. Then the pairs $(E/A, (E_{N'}+A)/A)\simeq\left(\boldsymbol{C}/\mathfrak{a}^{-1}, \left(\frac{1}{N'}\mathcal{O}+\mathfrak{a}^{-1}\right)\Big/\mathfrak{a}^{-1}\right)$ and $(E/A_{N_1'}, (E_{N_1'}+A_{N'})/A_{N_1'})\simeq\left(\boldsymbol{C}/\mathfrak{b}^{-1}, \left(\frac{1}{N_1'}\mathcal{O}+\mathfrak{c}^{-1}\right)\Big/\mathfrak{b}^{-1}\right)$. The endomorphism $\alpha:\boldsymbol{C}/\mathfrak{b}^{-1}\to\boldsymbol{C}/\mathfrak{b}^{-1}$ induces an isomorphism of the pair $\left(\boldsymbol{C}/\mathfrak{a}^{-1}, \left(\frac{1}{N'}\mathcal{O}+\mathfrak{a}^{-1}\right)\Big/\mathfrak{a}^{-1}\right)$ to $\left(\boldsymbol{C}/\mathfrak{b}^{-1}, \left(\frac{1}{N_1'}\mathcal{O}+\mathfrak{c}^{-1}\right)\Big/\mathfrak{b}^{-1}\right)$. Therefore $\pi_{N,N'}w_N(x)=w_{N_1'}\pi_{N,N'}(x)$. Then the morphism $f=f_{N,N',N_1'}$ sends the point x to the unit section of the jacobian variety $J_0(N')$. Then the $\boldsymbol{Q}$-rational point $f^+(y)$ is the unit section of $J_0^-(N', N_1')$.

We want to discuss the $\boldsymbol{Q}$-rational points on $X_0^+(N)$ for the integers N with the genus $g_+(N)>0$. The proposition below gives a criterion on the determination of the $\boldsymbol{Q}$-rational points.

PROPOSITION (2.2). *Under the notation as above and the assumption* (2.1), *let*

y be a non cuspidal $\boldsymbol{Q}$*-rational point on* $X_0^+(N)$ *for an integer* N *with* $g_+(N)>0$. *If the following condition is satisfied, then* y *is a C. M. point:*

$$N'\neq 37 \text{ and } f^+(y) \text{ is the unit section of } J_0^-(N', N_1').$$

PROOF. Let x and $x'=w_N(x)$ be the sections of the fibre $X_0(N)_y$ at y. Then x is represented by an elliptic curve E with a cyclic subgroup A of order N. The morphism f sends the point x to the divisor class

$$f(x) = \mathrm{cl}((w_{N_1'}\pi(x))-(\pi w_N(x))).$$

The points $w_{N_1'}\pi(x)$ and $\pi w_N(x)$ are represented by the pairs $(E/A_{N_1'}, (E_{N_1'}+A_{N'})/A_{N_1'})$ and $(E/A, (E_{N'}+A)/A)$, respectively. Firstly consider the case when $X_0(N')/\langle w_{N_1'}\rangle \simeq \boldsymbol{P}^1$. In this case, $J_0(N')=J_0^-(N', N_1')$ and $f(x)=f^+(y)$. By the assumption of this proposition, $w_{N_1'}\pi(x)=\pi w_N(x)$, so that $E/A_{N_1'}$ is isomorphic over $\boldsymbol{C}$ to E/A. Then there is an endomorphism α of E/A_{N_1} such that

$$\ker(\alpha : E/A_{N_1'} \to E/A_{N_1'}) \simeq \boldsymbol{Z}/(N/N_1')\boldsymbol{Z} \neq \{0\}.$$

Therefore $E/A_{N_1'}$ and E have complex multiplication. Now consider the case when $X_0(N')/\langle w_{N_1'}\rangle$ is not $\boldsymbol{P}^1$. In this case $g_0(N')\geqq 2$, since $w_{N_1'}$ has fixed points if $g_0(N')=1$ (2.1). By the assumption of this proposition, $f(x)$ is a section of the jacobian variety $J_0^+(N', N_1')$ of $X_0(N')/\langle w_{N_1'}\rangle$. Then $w_{N_1'}f(x)=f(x)$, and we get the following linearly equivalent relation of divisors of degree 2:

$$(w_{N_1'}\pi(x))+(w_{N_1'}\pi w_N(x)) \sim (\pi(x))+(\pi w_N(x)).$$

Since $g_0(N')\geqq 2$, by the relation above, we get

$$w_{N_1'}\pi(x) = \pi(x) \quad \text{or} \quad \pi w_N(x), \qquad \text{or} \quad \pi w_N(x) = \gamma\pi(x)$$

for the hyperelliptic involution γ of $X_0(N')$ if $X_0(N')$ is hyperelliptic. If $w_{N_1'}\pi(x) = \pi(x)$, then the elliptic curves $E/A_{N_1'}$ and E are isomorphic over $\boldsymbol{C}$. Since $N_1'\neq 1$ (2.1), E has complex multiplication. If $w_{N_1'}\pi(x)=\pi w_N(x)$, then $E/A_{N_1'}$ and E/A are isomorphic over $\boldsymbol{C}$. Since $N_1'\neq N$, E has complex multiplication. There are exactly 19 values of integers N' for which $X_0(N')$ are hyperelliptic with $g_0(N')\geqq 2$. These integers are $N'=22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59$ and 71 [**16**]. Except for $N'=37, 40$ and 48, the hyperelliptic involutions are the canonical involutions w_M for some positive divisors of N' prime to N'/M. Firstly consider the cases for $N'\neq 37, 40$ nor 48. The point $\gamma\pi(x)$ is represented by the pair $(E/A_M, (E_{N'}+A_M)/A_M)$. Then E/A and E/A_M are isomorphic over $\boldsymbol{C}$. If $M=N$, then $N'=N$ and $g_+(N)=0$. Thus by the assumption $g_+(N)\neq 0$, $M\neq N$, so that E has complex multiplication. For $N'=40$ and 48, the hyperelliptic involutions γ are represented by the matrices g below

loc. cit. :

$$g=\begin{cases}\begin{pmatrix}-10 & 1\\ -120 & 10\end{pmatrix} & \text{if } N'=40, \text{ and}\\ \begin{pmatrix}-6 & 1\\ -48 & 6\end{pmatrix} & \text{if } N'=48.\end{cases}$$

The point x is represented by an elliptic curve $\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}\tau$ for $\tau\in\boldsymbol{C}$ with $\mathrm{Im}(\tau)>0$. Then $\pi w_N(x)$ is represented by $\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}(-1/N\tau)\simeq\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}N\tau$. Then by the relation $\pi w_N(x)=\gamma\pi(x)$, for some integers a, b, c, d with $ad-bc=1$,

$$\frac{aN\tau+b}{cN\tau+d}=\begin{cases}\dfrac{-10\tau+1}{-120\tau+10} & \text{if } N'=40,\\ \dfrac{-6\tau+1}{-48\tau+6} & \text{if } N'=48.\end{cases}$$

Then τ is a root of a quadratic equation with rational coefficients. Thus x is a C.M. point. □

REMARK (2.3). The group $\mathrm{Aut}\,X_0(37)$ is isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2\boldsymbol{Z}$ [**11**] §5 [**16**]. The hyperelliptic involution of $X_0(37)$ is not represented by any matrix loc. cit.

For an application of proposition (2.2) to a non cuspidal $\boldsymbol{Q}$-rational point y on $X_0^+(N)$, we discuss the special fibre $y\otimes\boldsymbol{F}_p$ and $f^+(y)\otimes\boldsymbol{F}_p$ for a prime divisor p of N'.

LEMMA (2.4). *Under the assumption* (2.1), *let p be a prime divisor of N'. If the following conditions* $(\mathrm{i})_1$ *and* $(\mathrm{i})_2$ *are satisfied, then $f^+(y)\otimes\boldsymbol{F}_p$ is the unit section of $J_0^-(N', N_1')_{/\boldsymbol{Z}}\otimes\boldsymbol{F}_p$:*

$(\mathrm{i})_1$ *$f^+(y)\otimes\boldsymbol{F}_p$ is a section of the connected component $(J_0^-(N', N_1')_{/\boldsymbol{Z}}\otimes\boldsymbol{F}_p)^0$ of the unit section.*

$(\mathrm{i})_2$ $J_0^-(N', N_1')_{/\boldsymbol{Z}}(\boldsymbol{Z})\cap(J_0^-(N', N_1')_{/\boldsymbol{Z}}\otimes\boldsymbol{F}_p)^0=\{0\}$.

If the following conditions $(\mathrm{ii})_1$ *and* $(\mathrm{ii})_2$ *are satisfied, then $f^+(y)$ is the unit section:*

$(\mathrm{ii})_1$ *$f^+(y)\otimes\boldsymbol{F}_p$ is the unit section.*

$(\mathrm{ii})_2$ *$J_0^-(N', N_1')(\boldsymbol{Q})$ generates a finite étale subgroup scheme of the Néron model $J_0^-(N', N_1')_{/\boldsymbol{Z}_p}$.*

Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(N)$ for an integer N with $g_+(N)>0$. Let $x, x'=w_N(x)$ be the sections of the fibre $X_0(N)_y$ at y, which are defined over a quadratic field k and $x'=x^\sigma$ for $1\neq\sigma\in\mathrm{Gal}(k/\boldsymbol{Q})$. The point x is represented by an elliptic curve E with a cyclic subgroup A defined over k [**3**] VI (3.2). Let N' be a positive divisor of N satisfying the condition (2.1), p be a prime divisor of N', p be a prime of k lying over the rational prime p and e_k be the ramification index of p in k. If the modular invariant $j(x)=0$ or

1728, then we can easily check the rational points with these modular invariants. So we assume $j(x)\neq 0$ nor 1728. Then the pairs (E^σ, A^σ) and $(E/A, E_N/A)$ are isomorphic over a quadratic extension k' of k. Let λ, $\hat{\lambda}$ and λ^σ be the characters of the idèle group $k_A^\times$ of k induced by the Galois action of $\mathrm{Gal}(\bar{k}/k)$ on $A_p(\bar{k})$, $((E_p+A)/A)(\bar{k})\simeq(E_p/A_p)(\bar{k})$ and $A_p{}^\sigma(\bar{k})$, respectively. Then

$$\text{(2.5)}\qquad \begin{cases} \lambda\cdot\hat{\lambda}=\chi_p, \\ \lambda^\sigma=\lambda\cdot\mu \quad \text{for a character } \mu \text{ of degree 1 or 2,} \end{cases}$$

where χ_p is the cyclotomic character. The restriction of χ_p to the decomposition group of a prime p of k lying over the rational prime p is ${\theta_p}^{e_k}$ for the fundamental character θ_p [**17**] [**19**]. Let $\tilde{\mathcal{X}}_0(N)\to\mathrm{Spec}\boldsymbol{Z}$ be the minimal model of $X_0(N)$ and $\tilde{\mathcal{Y}}_0(N)\to\mathrm{Spec}\mathcal{O}_K$ be the minimal model of $X_0(N)\otimes k$. Further, let λ_p, $\hat{\lambda}_p$ be the restrictions of λ and $\hat{\lambda}$ to the subgroup $\mathcal{O}_p^\times$ of $k_A^\times$. The following lemma (2.6) gives a sufficient condition for $(\mathrm{i})_1$ in lemma (2.4).

LEMMA (2.6). *Under the notation as above and the assumption* (2.1), *assume that N has a prime divisor p, $p=11$ or $p\geqq 17$. Let $f=f_{N,p}$ be the morphism of $X_0(N)$ to $J_0(p)$ defined in* § 1. *Then $f(x)\otimes\kappa(p)$ is a section of the connected component $(J_0(p)_{/\mathcal{O}_k}\otimes\kappa(p))^0$ of the unit section.*

REMARK (2.7). For the prime numbers p, $p\leqq 7$ or $p=13$, $X_0(p)$ are of genus zero. If the square of $p=13$ divides N, we can show that $f_{N,169}(x)\otimes\kappa(p)$ is a section of the connected component $(J_0(169)_{/\mathcal{O}_k}\otimes\kappa(p))^0$ of the unit section.

PROOF OF LEMMA (2.6). Let E_i be the irreducible components $\mathcal{X}_0(N)\otimes\boldsymbol{F}_p$ for $i=0, 1, \cdots, r=\mathrm{ord}_pN$ (1.2). Let $\pi=\pi_{N,p}$ be the natural morphism of $\mathcal{X}_0(N)$ to $\mathcal{X}_0(p)$: $(E, A)\mapsto(E, A_p)$. It suffices to show that $w_p\pi(x)$ and $\pi w_N(x)$ define the sections of the same irreducible component of the smooth part $\tilde{\mathcal{Y}}_0(p)^{\mathrm{smooth}}\otimes\kappa(p)$, where $\tilde{\mathcal{Y}}_0(p)\to\mathrm{Spec}\mathcal{O}_k$ is the minimal model of $X_0(p)\otimes k$. If $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$, then the result follows, since w_N exchanges E_0^h by E_r^h and w_p exchanges the two irreducible components of $\mathcal{X}_0(p)\otimes\boldsymbol{F}_p$ (1.2). If p^2 divides N, then by (1.5), $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$, since $3e_k\leqq 6<p-1$. If p^2 does not divide N and $x\otimes\kappa(p)$ is not a supersingular point, then $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$ for $r=1$. Now consider the case when p^2 does not divide N and $x\otimes\kappa(p)$ is a supersingular point. The elliptic curve E/k associated with the point x has good reduction over an extension K of $k_p\otimes{\boldsymbol{Q}_p}^{ur}$, of degree $e\leqq 6$ [**22**] p. 46. The k-rational points $w_p\pi(x)$ and $\pi w_N(x)$ are represented by the pairs $(E/A_p, E_p/A_p)$ and $(E/A, (E_p+A)/A)$, respectively. Let ν be the character of $\mathrm{Gal}(\bar{K}/K)$ which is induced by the Galois action on $(E_p/A_p)(\bar{K})\simeq((E_p+A)/A)(\bar{K})$. The completion of the local ring at $x\otimes\kappa(p)$ $(\otimes W(\bar{\boldsymbol{F}}_p))$ is isomorphic to

$$W(\bar{\boldsymbol{F}}_p)[[x, y]]/(xy-p^k),$$

for $k=1, 2$ or 3 (1.2). We choose the coordinate y so that the ideal (y, p) defines the locus of E_0. Firstly consider the case $e_k=1$. Then $k=2$ ($j(x)\equiv 1728 \bmod p$) or $k=3$ ($j(x)\equiv 0 \bmod p$), and $w_p\pi(x)$, $\pi w_N(x)$ define the sections of the smooth part $\tilde{\mathcal{J}}_0(p)^{\mathrm{smooth}}$. The modular invariants $j(w_p\pi(x))\equiv j(\pi(x))\equiv j(\pi w_N(x)) \bmod p$, hence $w_p\pi(x)\otimes\kappa(p)=\pi w_N(x)\otimes\kappa(p)$. Further there is a unique integer a with $1\leqq a\leqq e-1$ such that $\nu=\theta_p{}^a$, since $e<p-1$ [17] [18]. Then

$$(w_p\pi(x)^*x,\ w_p\pi(x)^*y) = (\alpha^{ka}u,\ \alpha^{k(e-a)}u^{-1}) \quad \text{and}$$
$$(\pi w_N(x)^*x,\ \pi w_N(x)^*y) = (\alpha^{ka}v,\ \alpha^{k(e-a)}v^{-1})$$

for some units u, v of $\mathcal{O}_K$ and a prime element α of $\mathcal{O}_K$ (1.2). Therefore $w_p\pi(x)$ and $\pi w_N(x)$ define the sections of the same irreducible component of $\tilde{\mathcal{J}}_0(p)^{\mathrm{smooth}}\otimes\kappa(p)$. Secondly consider the case $e_k=2$. In this case, $\kappa(p)=\boldsymbol{F}_p$ and $x\otimes\kappa(p)=x^\sigma\otimes\kappa(p)=\pi w_N(x)\otimes\kappa(p)$ for $1\neq\sigma\in\mathrm{Gal}(k/\boldsymbol{Q})$. Further $w_p\pi(x)\otimes\kappa(p)=\pi(x)\otimes\kappa(p)=\pi w_N(x)\otimes\kappa(p)$, since w_p fixes all the $\boldsymbol{F}_p$-rational supersingular points on $\mathcal{X}_0(p)\otimes\boldsymbol{F}_p$. Since $\mathrm{ord}_p\pi(x)^*x=\mathrm{ord}_p(\pi(x)^*x)^\sigma=\mathrm{ord}_p\pi w_N(x)^*x$, the restrictions of the characters λ_p, $\lambda_p{}^\sigma$ and $\hat{\lambda}_p$ to $\mathrm{Gal}(\bar{K}/K)$ are all equivalent to ν (1.2). Then by (2.5), $\nu^2=\theta_p{}^{2e}$. Then $\nu=\theta_p{}^e$, or $\nu=\theta_p{}^{e+(p-1)/2}$ if $p=11$ and $e=6$. If $\nu=\theta_p{}^e$, then by the same argument as above gives the result. In the remaining case, the modular invariant $j(x)\equiv 0 \bmod p$ and $\mathrm{ord}_\alpha\pi(x)^*x=3$ or 33 (1.2), where α is a prime element of $\mathcal{O}_K$. But then $\mathrm{ord}_p\pi(x)^*x=1/2$ or $11/2$. It is a contradiction. □

Now consider the condition $(\mathrm{i})_2$ in lemma (2.4). For $p=11$ or $p\geqq 17$, $g_0(p)>0$ and the torsion part of the Mordell-Weil group of $J_0(p)$ is a cyclic group of order $n=\mathrm{num}\left(\frac{p-1}{12}\right)$, which is the cuspidal group $C=\langle \mathrm{cl}((\boldsymbol{0})-(\infty))\rangle$ [9]. The natural morphism of $J_0(p)$ to $J_0^-(p)=J_0(p)/(1+w_p)J_0(p)$ sends C isomorphically onto $J_0^-(p)(\boldsymbol{Q})_{\mathrm{tor}}$ loc. cit. In the rest of this section, J, J^+ and J^- denote respectively $J_0(p)$, $J_0^+(p)$ and $J_0^-(p)$. Let g be the natural morphism of $X_0(p)$ to $X_0^+(p)=X_0(p)/\langle w_p\rangle$. Then g has ramification points, so that the natural morphism $i=g^*$ of J^+ to J as Picard varieties is injective. Then we have the following exact sequence of the abelian varieties:

$$0 \longrightarrow J^+ \xrightarrow{i=g^*} J \xrightarrow{u} J^- \longrightarrow 0.$$

Denote also by C the image $u(C)$ of the cuspidal subgroup C. The schematic closure $\mathcal{C}=C_{/\mathcal{O}_K}$ of C in the Néron model $J^-{}_{/\mathcal{O}_K}$ is a finite étale subgroup scheme for any finite extension K of $\boldsymbol{Q}_p{}^{ur}$.

PROPOSITION (2.8). *Under the notation as above, let K be an extension of*

$\boldsymbol{Q}_p{}^{ur}$ *of degree* $\leqq 2$. *Then*

$$C\otimes\bar{\boldsymbol{F}}_p\cap(J^-{}_{/\mathcal{O}_K}\otimes\bar{\boldsymbol{F}}_p)^0=\{0\}.$$

PROOF. Since $C\simeq(\boldsymbol{Z}/n\boldsymbol{Z})_{/R}$ for $n=\mathrm{num}\left(\frac{p-1}{12}\right)$ and $R=\mathcal{O}_K$, it suffices to show that

$$C\otimes\bar{\boldsymbol{F}}_p\cap(J^-{}_{/R}\otimes\bar{\boldsymbol{F}}_p)^0_n=\{0\}.$$

For a semistable abelian variety A defined over K, let $A(K)[n^\infty]^d$ denote the divisible part of torsion group $A(K)[n^\infty]=\bigcup_{l=1}^\infty A(K)_{n^l}$, and put $A_n(K)^d=A(K)[n^\infty]^d\cap A_n(K)$. Then $A_n(K)^d$ generates a finite étale subgroup scheme $\mathcal{A}_n$ such that $\mathcal{A}_n\otimes\bar{\boldsymbol{F}}_p=(A_{/R}\otimes\bar{\boldsymbol{F}}_p)^0_n$. Put $D_n^+=J_n^+(K)/J_n^+(K)^d$, $D_n=J_n(K)/J_n(K)^d$, $D_n^-=J_n^-(K)/J_n^-(K)^d$. In the following diagram, the vertical sequences and the second horizontal sequence are exact, and the map i^d is injective:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J_n^+(K)^d & \xrightarrow{i^d} & J_n(K)^d & \xrightarrow{u^d} & J_n^-(K)^d & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J_n^+(K) & \xrightarrow{i} & J_n(K) & \xrightarrow{u} & J_n^-(K) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & D_n^+ & \xrightarrow{\bar{i}} & D_n & \xrightarrow{\bar{u}} & D_n^- & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

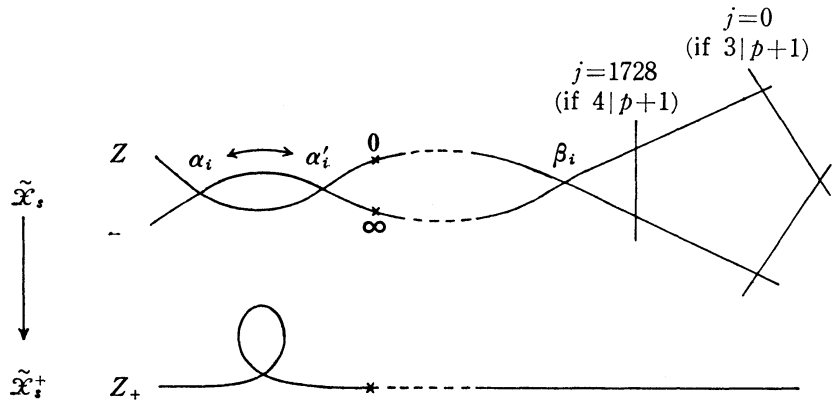
If $\bar{i}$ is injective, then the horizontal sequences are exact, since degree of $J_n(K)^d$ = degree of $J_n^+(K)^d$+degree of $J_n^-(K)^d$ and the second horizontal sequence is exact. Then it suffices to show that $\bar{i}$ is injective and

$$C\cap J_n(K)^d=\{0\},\qquad \bar{i}(D_n^+)\cap(C \bmod J_n(K)^d)=\{0\}.$$

Let $\mathcal{J}^+$, $\mathcal{J}$ and $\mathcal{J}^-$ denote the Néron models $J^+{}_{/R}$, $J_{/R}$ and $J^-{}_{/R}$, respectively. Let $\mathcal{J}_s^+$, $\mathcal{J}_s$ and $\mathcal{J}_s^-$ denote the special fibres $\mathcal{J}^+\otimes\bar{\boldsymbol{F}}_p$, $\mathcal{J}\otimes\bar{\boldsymbol{F}}_p$ and $\mathcal{J}^-\otimes\bar{\boldsymbol{F}}_p$, and $(\mathcal{J}_s^+)^0$, $\mathcal{J}_s^0$ and $(\mathcal{J}_s^-)^0$ denote the connected components of the special fibres of the unit sections. Then D_n^+, D_n and D_n^- can be regarded as subgroups of $\mathcal{J}_s^+/(\mathcal{J}_s^+)^0$, $\mathcal{J}_s/\mathcal{J}_s^0$ and $\mathcal{J}_s^-/(\mathcal{J}_s^-)^0$, respectively. Let $g=g_0(p)$ and $g_+=g_+(p)$ be the genus of $X_0(p)$ and $X_0^+(p)$, respectively. Let $\alpha_i=x_{2i-1}$, $\alpha_i'=\alpha_i^{(p)}=x_{2i}$ be the non $\boldsymbol{F}_p$-rational supersingular points on $\mathcal{X}_0(p)\otimes\boldsymbol{F}_p$ for $1\leqq i\leqq g_+$, and let $\beta_i=x_{2g_++i}$ be $\boldsymbol{F}_p$-rational supersingular points on $\mathcal{X}_0(p)\otimes\boldsymbol{F}_p$ for $1\leqq i\leqq g-2g_++1$. The fundamental involution w_p exchanges α_i by α_i' and fixes β_i. Let $\tilde{\mathcal{X}}\to\mathrm{Spec}\,W(\bar{\boldsymbol{F}}_p)$ be the minimal model of $X_0(p)\otimes\boldsymbol{Q}_p{}^{ur}$, which is obtained by blowing up along

the supersingular points x with modular invariants $j(x)=1728$ if $p\equiv -1 \bmod 4$, and $j(x)=0$ if $p\equiv -1 \bmod 3$. The quotient $\tilde{\mathcal{X}}^+=\mathcal{X}_0(p)/\langle w_p\rangle$ is the minimal model of $X_0^+(p)$.

$e=1$

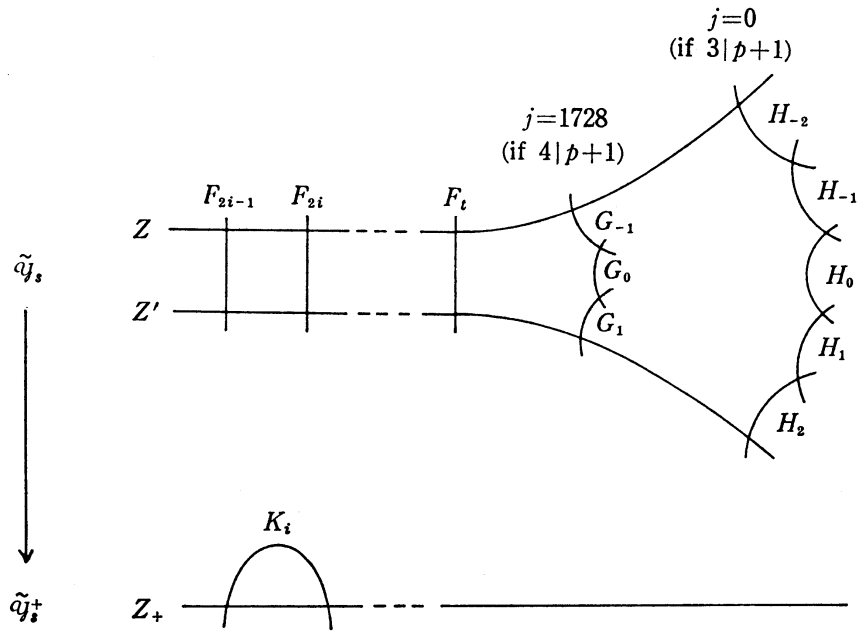


The minimal model $\tilde{\mathcal{Y}}\to \mathrm{Spec}R$ (resp. $\tilde{\mathcal{Y}}^+\to \mathrm{Spec}R$) of $X_0(p)\otimes K$ (resp. $X_0^+(p)\otimes K$) is obtained by blowing up along the non regular ordinary double points on $\tilde{\mathcal{X}}\otimes R$ (resp. $\tilde{\mathcal{X}}^+\otimes R$) (if $e=2$). Denote also by g the morphism of $\tilde{\mathcal{Y}}$ to $\tilde{\mathcal{Y}}^+$ induced by g of $\mathcal{X}_0(p)$ to $\mathcal{X}_0(p)/\langle w_p\rangle$. Let $\mathcal{P}^0$ and $\mathcal{P}_+^0$ be the connected components of the Picard groups $\mathcal{P}=\mathrm{Pic}\,\tilde{\mathcal{Y}}_{/R}$ and $\mathcal{P}_+=\mathrm{Pic}\,\tilde{\mathcal{Y}}^+_{/R}$ of the unit sections. Let $\mathcal{P}^\tau$ and $\mathcal{P}_+^\tau$ be the kernels of the degree maps $\mathcal{P}\to \boldsymbol{Z}$ and $\mathcal{P}_+\to \boldsymbol{Z}$, and E, E_+ be the Zariski closures of the unit sections of $\mathcal{P}\otimes K$ and $\mathcal{P}_+\otimes K$ in $\mathcal{P}$ and $\mathcal{P}_+$, respectively. Then $\mathcal{J}=\mathcal{P}^\tau/E$ and $\mathcal{J}_+=\mathcal{P}_+^\tau/E_+$ [**18**] § 8. Let $\{C_i\}$, $\{C'_j\}$ be the sets of the irreducible components of the special fibres $\tilde{\mathcal{Y}}_s=\tilde{\mathcal{Y}}\otimes\bar{\boldsymbol{F}}_p$ and $\tilde{\mathcal{Y}}_s^+=\tilde{\mathcal{Y}}^+\otimes\bar{\boldsymbol{F}}_p$. Let $\mathcal{D}$, $\mathcal{D}_+$ be the free groups generated by the divisors C_i and C'_j, and $\mathcal{D}^0$, $\mathcal{D}_+^0$ be the subgroups of divisors of degree zero. Let $\alpha:\mathcal{D}\to\mathcal{D}$ (resp. $\alpha_+:\mathcal{D}_+\to\mathcal{D}_+$) be the maps defined by

$$\alpha(C)=\sum_i (C, C_i)C_i \qquad (\text{resp. } \alpha_+(C')=\sum_j (C', C'_j)C'_j),$$

where (C, C_i) and (C', C'_j) are the intersection numbers (Note. $\tilde{\mathcal{Y}}_s$ and $\tilde{\mathcal{Y}}_s^+$ are reduced loc. cit.). Then $\mathcal{J}_s/\mathcal{J}_s^0\simeq\mathcal{D}^0/\alpha(\mathcal{D})$ and $\mathcal{J}_s^+/(\mathcal{J}_s^+)^0\simeq\mathcal{D}_+^0/\alpha_+(\mathcal{D}_+)$ loc. cit. The morphism g^* defines a map of $\mathcal{D}_+^0/\alpha_+(\mathcal{D}_+)$ to $\mathcal{D}^0/\alpha(\mathcal{D})$. If $e=1$, then $\tilde{\mathcal{Y}}_s^+$ is irreducible and $\mathcal{J}_s^+$ is connected. Then $D_n^+=\{0\}$ and $\mathcal{J}_s=\mathcal{J}_s^0\times C\otimes\bar{\boldsymbol{F}}_p$ [**9**] Appendix 1. Now consider the case $e=2$. The pictures of the special fibres $\tilde{\mathcal{Y}}_s$ and $\tilde{\mathcal{Y}}_s^+$ are as follows:

$e=2$



Put $t=g+1$ if $p\equiv 1 \bmod 12$, $t=g-1$ if $p\equiv -1 \bmod 12$ and $t=g$ otherwise. Let $\bar{Z}=Z-Z'$, $\bar{F}_i=F_i-Z'$, $\bar{G}_i=G_i-Z'$ and $\bar{H}_i=H_i-Z'$ be the basis of $\mathcal{D}^0$, and $\bar{K}_i=K_i-Z_+$ be the basis of $\mathcal{D}^0_+$ (see above pictures). By a calculation, we see that

$$\mathcal{D}^0_+/\alpha_+(\mathcal{D}_+)=\langle \bar{K}_i\rangle/\langle 2\bar{K}_i\rangle_{1\le i\le g_+} \quad \text{and}$$

$$\mathcal{D}^0/\alpha(\mathcal{D})=\begin{cases} \langle \bar{F}_i\rangle/\langle 2\bar{F}_i-2\bar{F}_1,\ 2n\bar{F}_1\rangle_{1\le i\le t} \text{ and } \bar{Z}\equiv 2\bar{F}_1 \bmod \alpha(\mathcal{D}) \\ \qquad\qquad \text{if } p\not\equiv -1 \bmod 12 \\ \langle \bar{F}_i,\ \bar{H}_0\rangle/\langle 2\bar{F}_i-2\bar{H}_0,\ 2n\bar{H}_0\rangle_{1\le i\le t} \text{ and } \bar{Z}\equiv 2\bar{H}_0 \bmod \alpha(\mathcal{D}) \\ \qquad\qquad \text{if } p\equiv -1 \bmod 12 \end{cases}$$

for $n=\mathrm{num}\left(\frac{p-1}{12}\right)$. Further $g^*(Z_+)=Z+Z'$ and $g^*(K_i)=F_{2i-1}+F_{2i}$ for $1\le i\le g_+$. Then

$$g^*(\bar{K}_i)\equiv \bar{F}_{2i-1}+\bar{F}_{2i}-\bar{Z}\equiv \bar{F}_{2i-1}-\bar{F}_{2i} \bmod \alpha(\mathcal{D}).$$

Thus we see that $\bar{i}$ is injective and that $C\otimes \bar{\boldsymbol{F}}_p\cap J_n(K)^d=\{0\}$. Since $\mathcal{D}^0_+/\alpha_+(\mathcal{D}_+)\simeq(\boldsymbol{Z}/2\boldsymbol{Z})^{g_+}$, $\langle\bar{Z}\rangle\cap\bar{i}(D_n^+)$ is a subgroup of $\left\langle\frac{n}{2}\bar{Z}\right\rangle \bmod \alpha(\mathcal{D})$. If $p\not\equiv 1 \bmod 8$, then n is odd and $\langle\bar{Z}\rangle\cap\bar{i}(D_n^+)=\{0\}$ in $\mathcal{D}^0/\alpha(\mathcal{D})$. Suppose that $p\equiv 1 \bmod 8$ and $\frac{n}{2}\bar{Z} \bmod \alpha(\mathcal{D})$ belongs to $\bar{i}(\mathcal{D}_n^+)$. Then $\frac{n}{2}\bar{Z}\equiv n\bar{F}_1\equiv\sum_{i=1}^{g_+}\varepsilon_i(\bar{F}_{2i-1}-\bar{F}_{2i}) \bmod \alpha(\mathcal{D})$ for $\varepsilon_i=0$ or 1. But we see that $n\bar{F}_1-\sum_{i=1}^{g_+}\varepsilon_i(\bar{F}_{2i-1}-\bar{F}_{2i})$ does not belong to $\alpha(\mathcal{D})$ for any $\varepsilon_i=0$ or 1. Thus $\bar{i}(D_n^+)\cap(\mathcal{D} \bmod J_n(K))=\{0\}$. □

COROLLARY (2.9). *Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(N)$ for an integer N divisible by a prime number $p=11$ or $p\geqq 17$. If the Mordell-Weil group $J_0^-(p)(\boldsymbol{Q})$ is of finite order, then $f_{N,p}^+(y)$ is the unit section of $J_0^-(p)$.*

PROOF. Let x, $x'=w_N(x)$ be the sections of the fibre $X_0(N)_y$ at y. Under the notation as in lemma (2.6), $f_{N,p}(x)\otimes\kappa(p)$ is a section of the connected component $(J_0(p)_{/\mathcal{O}_k}\otimes\kappa(p))^0$ of the unit section. Under the assumption that $\#J_0^-(p)(\boldsymbol{Q})<\infty$, $f_{N,p}^+(y)$ is a section of the cuspidal subgroup $C=\langle \mathrm{cl}((\mathbf{0})-(\infty))\rangle$ in $J_0^-(p)$ [**9**]. Then by proposition (2.8), $f_{N,p}^+(y)\otimes\kappa(p)$ is the unit section of $J_0^-(p)_{/\mathcal{O}_k}\otimes\kappa(p)$. Then $f_{N,p}^+(y)$ is the unit section of $J_0^-(p)$, since C generates a finite étale subgroup scheme $\simeq (\boldsymbol{Z}/n\boldsymbol{Z})_{/\mathcal{O}_k}$ for $n=\mathrm{num}\left(\frac{p-1}{12}\right)$ loc. cit. □

Now we can show the following theorem.

THEOREM (2.10). *Let N be a composite number divisible by a prime number $p=11$ or $p\geqq 17$. If $p\neq 37$ and $\#J_0^-(p)(\boldsymbol{Q})<\infty$, then $n(N)=0$.*

PROOF. Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(N)$. Then by corollary (2.9), $f_{N,p}^+(y)$ is the unit section of $J_0^-(p)$ under the assumption $\#J_0^-(p)(\boldsymbol{Q})<\infty$. If moreover $p\neq 37$, by proposition (2.2), y is a C.M. point. □

The same method can be applied to some other cases. For an example, we get the following result.

PROPOSITION (2.11). *Let N be a composite number with the genus $g_+(N)>0$. If one of the following conditions* (a) *and* (b) *is satisfied, then $n(N)=0$:*

(a) *$M=27$, 35 or 26 divides N.*

(b) *$M=49$ divides N and $m=N/49$ satisfies one of the following conditions:*
(1) *7 or 9 divides m,* (2) *a prime number q with $q\equiv -1 \bmod 3$ divides m, and*
(3) *m is prime to 7 and the quadratic residue $\left(\frac{-7}{m}\right)=-1$.*

PROOF. In the case $M=27$ (resp. 49, resp. 35, resp. 26), put $N'=N_1'=27$ (resp. $N'=N_1'=49$, resp. $N'=35$ and $N_1'=7$, resp. $N'=26$ and $N_1'=13$). In the cases $M=27$ and 49, we know that

$$X_0(N')/\langle w_{N_1'}\rangle \simeq \boldsymbol{P}^1 \quad \text{and}$$
$$J_0^-(N', N_1')_{/\boldsymbol{Z}}(\boldsymbol{Z})\cap(J_0^-(N', N_1')_{/\boldsymbol{Z}}\otimes\boldsymbol{F}_p)^0 = \{0\}$$

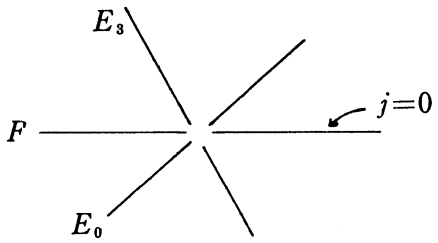
for $p=3$ if $M=27$, and $p=7$ if $M=49$ [**22**] table 1 pp. 81-113. Let y be a non cuspidal $\boldsymbol{Q}$-rational point on $X_0^+(N)$ and x, $x'=w_N(x)$ be the sections of the fibre $X_0(N)_y$ at y. Further let k, p, and e_k be the quadratic field over which x and x' are defined cf. § 2, a prime ideal of k lying over the rational prime p ($|N_1'$) as above, and the ramification index of p in k.

Case $M=27$: If $x\otimes\kappa(p)$ is not a supersingular point, then $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$ for $r=\mathrm{ord}_3 N$ [**14**] theorem (3.2). If $x\otimes\kappa(p)$ is a supersingular point, then $w_{27}\pi(x)$ and $\pi w_N(x)$ define sections of the Néron model $\mathcal{E}=\tilde{q}_0(27)^{\mathrm{smooth}}$ over the base $\mathcal{O}_k$ whose special fibres at p are contained in the same irreducible component F of $\mathcal{E}\otimes\kappa(p)$ loc. cit. (see below). Further we know that the Mordell-Weil group $C=X_0(27)(\boldsymbol{Q})$ is of order 3 and

$$C_{/\mathcal{O}_k}\otimes\kappa(p)\cap(\mathcal{E}\otimes\kappa(p))^0=\{0\},$$

where $C_{/\mathcal{O}_k}$ is the schematic closure of C in $\mathcal{E}$ loc. cit. Therefore $f^+_{N,27}(y)$ is the unit section of $X_0(27)$. Then proposition (2.2) gives the result.

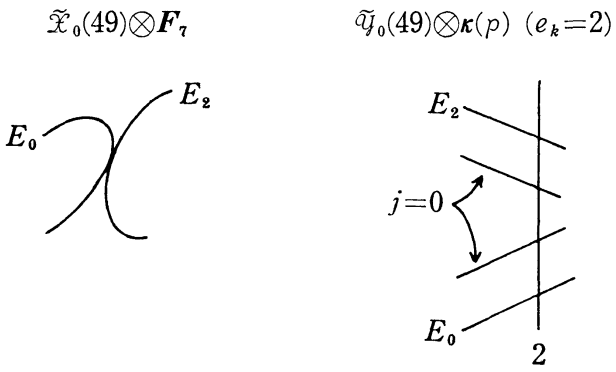
$\mathcal{E}\otimes\kappa(p)$:



Case $M=49$: If the modular invariant $j(x)\not\equiv 0 \bmod p$, then $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$ for $r=\mathrm{ord}_7 N$ (1.4) (1.5). Suppose $j(x)\equiv 0 \bmod p$. If $e_k=1$, then $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$ loc. cit. If $e_k=2$, then $x\otimes\kappa(p)=x^\sigma\otimes\kappa(p)=x'\otimes\kappa(p)$ for $1\neq\sigma\in\mathrm{Gal}(k/\boldsymbol{Q})$, so that $r=\mathrm{ord}_7 N$ is even and $x\otimes\kappa(p)$ is a section of $E^h_{(r/2)}$. By (1.5), there remains the case $r=2$. If the quadratic residue $\left(\frac{-7}{m}\right)=-1$, then $x\otimes\kappa(p)$ is not a fixed point of w_N, so that $e_k=1$ and $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$. For the remaining cases, put $q=9$ or a prime number with $q\equiv -1 \bmod 3$. Let E be an elliptic curve with a cyclic subgroup A of order N defined over k which represents the point x [**3**] VI (3.3). Then E has good reduction over the quadratic extension of $k_p\otimes\boldsymbol{Q}_7{}^{ur}$ and $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$ (1.5). Let $\mathcal{E}=\tilde{q}_0(49)^{\mathrm{smooth}}$ be the Néron model over the base $\mathcal{O}_k$ and $C=X_0(49)(\boldsymbol{Q})$ be the Mordell-Weil group. Then C is of order 2 and

$$C_{/\mathcal{O}_k}\otimes\kappa(p)\cap(\mathcal{E}\otimes\kappa(p))^0=\{0\}$$

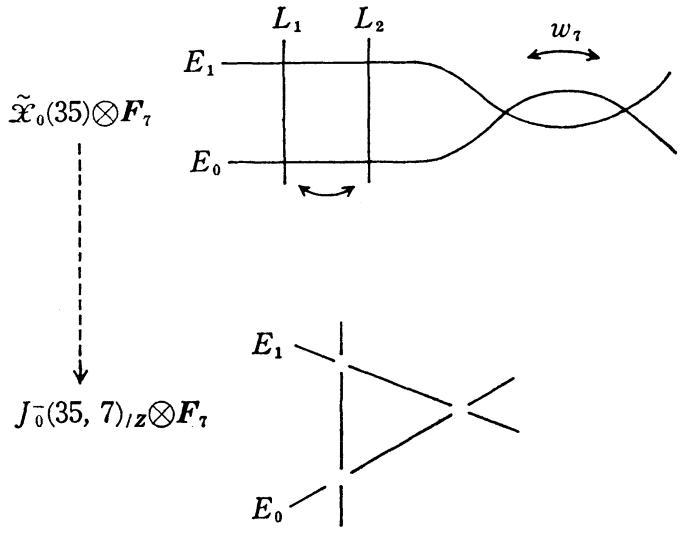
[**22**] table 1 pp. 81-113 (see below). Then proposition (2.2) and lemma (2.4) give the result.



Case $M=35$ *and* $49 \nmid N$: The supersingular point on $\mathcal{X}_0(35)\otimes \boldsymbol{F}_7$ are not $\boldsymbol{F}_7$-rational. If $x\otimes\kappa(p)$ is not a supersingular point, then $x\otimes\kappa(p)$ is a section of $E_0^h \cup E_1^h$. If $x\otimes\kappa(p)$ is a supersingular point, then $e_k=1$ and $w_7\pi(x)$, $\pi w_N(x)$ define the sections of the minimal model $\tilde{\mathcal{X}}_0(35)$ whose special fibres at p are contained in $L_1\cup L_2$ see below. Let u be the natural morphism of $J_0(35)$ to $J_0^-(35,7)$. Since $w_N(x)\otimes\kappa(p)=(x\otimes\kappa(p))^{(7)}$ and $w_7\pi(x)\otimes\kappa(p)=(\pi(x)\otimes\kappa(p))^{(7)}$, $uf_{N,35}(x)\otimes\kappa(p)$ becomes a section of the connected component of $J_0^-(35,7)_{/Z}\otimes \boldsymbol{F}_7$ of the unit section. Further

$$J_0^-(35,7)_{/Z}(\boldsymbol{Z})\cap(J_0^-(35,7)_{/Z}\otimes \boldsymbol{F}_7)^0 = \{0\}$$

[**22**] table 1 pp. 81-113. Then proposition (2.2) and lemma (2.4) give the result.



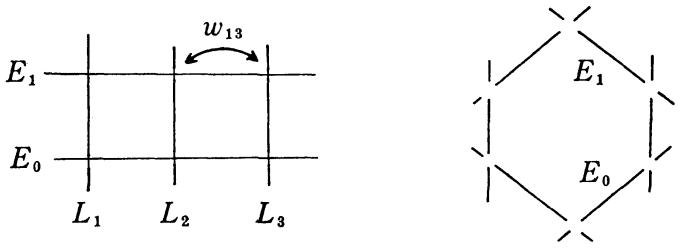
Case $M=26$: If 13^2 divides N, then $x\otimes\kappa(p)$ is a section of $E_0^h\cup E_r^h$ for $r=\mathrm{ord}_{13}N$ (1.5). Now we discuss the case $\mathrm{ord}_{13}N=1$. If $e_k=1$, then $x\otimes\kappa(p)$ is not a supersingular point (1.2), since the modular invariants of the supersingular points on $\mathcal{X}_0(N)\otimes \boldsymbol{F}_{13}$ $=5$. If $e_k=2$ and $x\otimes\kappa(p)$ is a supersingular point, then

$w_{13}\pi(x)$ and $\pi w_N(x)$ define sections of the smooth part $\tilde{\mathcal{J}}_0(26)^{\text{smooth}}$ of the minimal model of $X_0(26)\otimes k$ whose special fibres at p are contained in the same irreducible component L_1 see below. Let u be the natural morphism of $J_0(26)$ to $J_0^-(26, 13)$. Then $uf(x)\otimes \boldsymbol{F}_{13}$ becomes a section of the connected component $(J_0^-(26, 13)_{/\boldsymbol{Z}}\otimes \boldsymbol{F}_{13})^0$ of the unit section. Further

$$J_0^-(26, 13)_{/\boldsymbol{Z}}(\boldsymbol{Z})\cap(J_0^-(26, 13)_{/\boldsymbol{Z}}\otimes \boldsymbol{F}_{13})^0 = \{0\}$$

[**22**] table 1 pp. 81-113. Then proposition (2.2) and lemma (2.4) give the result.

$$\tilde{\mathcal{J}}_0(26)\otimes\kappa(p) \dashrightarrow J_0^-(26, 13)_{/\boldsymbol{Z}}\otimes\kappa(p)$$



□

References

[1] A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann., **185** (1970), 134-160.

[2] V. G. Berkovic, The rational points on the jacobians of modular curves, Math. USSR Sbornik, **30**-4 (1976), 485-500.

[3] P. Deligne and M. Rapoport, Schémas de modules des courbes elliptiques, Proc. International Summer School on Modular Functions, Antwerp 1972, Vol. II, Lecture Notes in Math., **349**, Springer, 1973.

[4] N. Ishii and F. Momose, Hyperelliptic modular curves, to appear.

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

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

[7] M. A. Kenku, The modular curve $X_0(169)$ and rational isogeny, J. London Math. Soc. (2), **22** (1980), 239-244.

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

[9] B. Mazur, Modular curves and the Eisenstein ideals, Publ. Math. I. H. E. S., **47**, 1977.

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

[11] B. Mazur and H. P. F. Swinnerton-Deyer, Arithmetic of Weil curves, Invent. Math., **25** (1974), 1-61.

[12] J. F. Mestre, Points rationnels de la courbe modulaire $X_0(169)$, Ann. Inst. Fourier (Grenoble), **30**-2 (1980), 17-27.

[13] F. Momose, Rational points on the modular curves $X_{\text{split}}(p)$, Compositio Math., **52** (1984), 115-137.

[14] F. Momose, Rational points on the modular curves $X_0^+(p^r)$, to appear.
[15] A. Ogg, Über die Automorphismengruppe von $X_0(N)$, Math. Ann., **228** (1977), 279-292.
[16] A. Ogg, Hyperelliptic modular curves, Bull. Soc. Math. France, **102** (1974), 449-462.
[17] F. Oort and J. Tate, Group schemes of prime order, Ann. Sci. École Norm. Sup. (4), **3** (1970), 1-21.
[18] M. Raynaud, Spécialisation du foncteur de Picard, Publ. Math. I. H. E. S., **38**, 1970, pp. 27-76.
[19] M. Raynaud, Schémas en groupes de type $(p, \cdots, p)$, Bull. Soc. Math. France, **102** (1974), 241-280.
[20] K. A. Ribet, Endomorphisms of semi-stable abelian varieties over number fields, Ann. of Math., **101** (1975), 555-562.
[21] J. P. Serre, Propriétés galoissiennes des points d'ordre fini des courbes elliptiques, Invent. Math., **15** (1972), 259-331.
[22] B. J. Birch and W. Kuyk ed., Modular functions of one variable IV, Lecture Notes in Math., **476**, Springer, 1975.

Fumiyuki MOMOSE
Department of Mathematics
Faculty of Science and Engineering
Chuo University
Kasuga, Bunkyo-ku
Tokyo 112
Japan