M. A. Kenku and F. Momose
Nagoya Math. J.
Vol. 109 (1988), 125–149

TORSION POINTS ON ELLIPTIC CURVES DEFINED OVER QUADRATIC FIELDS

M. A. KENKU AND F. MOMOSE

Let k be a quadratic field and E an elliptic curve defined over k. The authors [8, 12, 13] [23] discussed the k-rational points on E of prime power order. For a prime number p, let $n = n(k, p)$ be the least non negative integer such that

$$E_{p^\infty}(k) = \bigcup_{m \geqq 0} \ker(p^m\colon E \longrightarrow E)(k) \subset E_{p^n}$$

for all elliptic curves E defined over a quadratic field k ([15]). For prime numbers $p < 300$, $p \neq 151$, 199, 227 nor 277, we know that $n(k, 2) = 3$ or 4, $n(k, 3) = 2$, $n(k, 5) = n(k, 7) = 1$, $n(k, 11) = 0$ or 1, $n(k, 13) = 0$ or 1, and $n(k, p) = 0$ for all the prime numbers $p \geqq 17$ as above (see loc. cit.). It seems that $n(k, p) = 0$ for all prime numbers $p \geqq 17$ and for all quadratic fields k. In this paper, we discuss the N-torsion points on E for integers N of products of powers of 2, 3, 5, 7, 11 and 13. Let $N \geqq 1$ be an integer and m a positive divisor of N. Let $X_1(m, N)$ be the modular curve which corresponds to the finite adèlic modular group

$$\Gamma_1(m, N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\hat{\boldsymbol{Z}}) | a - 1 \equiv c \equiv 0 \bmod N,\ b \equiv d - 1 \equiv 0 \bmod m\right\},$$

where $\hat{\boldsymbol{Z}} = \varprojlim_n \boldsymbol{Z}/n\boldsymbol{Z}$. Then $X_1(m, N)$ is defined over $\boldsymbol{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of 1. Put $Y_1(m, N) = X_1(m, N) \setminus \{\text{cusps}\}$, which is the coarse moduli space $(/\boldsymbol{Q}(\zeta_m))$ of the isomorphism classes of elliptic curves E with a pair (P_m, P_N) of points P_m and P_N which generate a subgroup $\simeq \boldsymbol{Z}/m\boldsymbol{Z} \times \boldsymbol{Z}/N\boldsymbol{Z}$, up to the isomorphism $(-1)_E\colon E \simeq E$. For $m = 1$, let $X_1(N) = X_1(1, N)$, $\Gamma_1(N) = \Gamma_1(1, N)$ and $Y_1(N) = Y_1(1, N)$. For the integers $N = 2^4$, 11 and 13, $X_1(N)$ are hyperelliptic and $n(k, 2)$, $n(k, 11)$ and $n(k, 13)$ depend on k [23] (3.3). Our result is the following.

THEOREM (0.1). *Let N be an integer of a product of powers of* 2, 3, 5,

Received September 29, 1986.

7, 11 *and* 13, *let* m *be a positive divisor of* N. *If* $X_1(m, N)$ *is not hyperelliptic* (*i.e. the genus* $g_1(m, N) \neq 0$ *and* $(m, N) \neq (1,11), (1,13), (1,14), (1.15), (1,16), (1,18), (2,10)$ *nor* $(2,12)$), *then* $Y_1(m, N)(k) = \phi$ *for all quadratic fields* k.

For prime numbers $p \geqq 17$, it seems that $Y_1(p)(k) = \phi$ for all quadratic fields k [23]. With Theorem (0.1), we may conjecture that the torsion subgroup of $E(k)$ (k = a quadratic field) is isomorphic to one of the following groups:

		$g_1(m, N)$
Z/NZ	for $1 \leqq N \leqq 10$ or $N = 12$	0
$Z/2Z \times Z/2nZ$	for $1 \leqq n \leqq 4$	0
$Z/3n \times Z/3nZ$	for $n = 1$ or 2 with $k = \boldsymbol{Q}(\sqrt{-3})$	0
$Z/4Z \times Z/4Z$	with $k = \boldsymbol{Q}(\sqrt{-1})$	0

or

Z/NZ	for $N = 11$, 14 or 16	1
Z/NZ	for $N = 13$, 16 or 18	2
$Z/2Z \times Z/2nZ$	for $n = 5$ or 6	1.

For $(m, N) = (1,14), (1,15), (1,18), (2,10)$ and $(2,12)$, we give examples of quadratic fields k such that $Y_1(m, N)(k) = \phi$ (2.4), (2.5) (see also [23] (3.3)).

The proof of Theorem (0.1) consists of two parts. One is a study on the Mordell-Weil groups of jacobian varieties of some modular curves (1.4), (1.5). The other is a similar discussion as in [8, 12, 13] [23]. Suppose that there is a k-rational point x on $Y_1(m, N)$ for a pair (m, N) as in (0.1). Then x defines a rational function g ($/\boldsymbol{Q}$) on a subcovering X: $X_1(m, N) \rightarrow X \rightarrow X_0(N)$, whose divisor (g) is determined by x. Using the methods as in [8, 12, 13] [23], we show that such a function does not exist and get the result. It will be proved in Section 2 for $m = 1$ and in Section 3 for $m \geqq 2$.

Notation. For a rational prime p, $\boldsymbol{Q}_p^{ur}$ denotes the maximal unramified extension of $\boldsymbol{Q}_p$. Let K be a finite extension of $\boldsymbol{Q}$, $\boldsymbol{Q}_p$ or $\boldsymbol{Q}_p^{ur}$, and A 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 $\mathcal{O}_K$. For a finite subgroup G of A defined over K, $G_{/\mathcal{O}_K}$ denotes the schematic closure of G in the Néron model $A_{/\mathcal{O}_K}$ (, which is a quasi finite flat group scheme [28] § 2). For a subscheme Y of a modular curve X/Z and for a fixed rational prime p, Y^h denotes the open subscheme $Y \setminus$\{supersingular points on

$Y \otimes F_p\}$. For a finite extension K of $\boldsymbol{Q}$ and for a prime $\mathfrak{p}$ of K, $(\mathcal{O}_K)_{(\mathfrak{p})}$ denotes the local ring at $\mathfrak{p}$.

§ 1. Preliminaries

In this section, we give a review on modular curves and discuss the Mordell-Weil groups of jacobian varieties of some modular curves. Let $N \geqq 1$ be an integer and m a positive divisor of N. Let $X_1(m, N)$ (resp. $X_0(m, N)$) be the modular curve $(/\boldsymbol{Q}(\zeta_m))$ (resp. $/\boldsymbol{Q}$) which corresponds to the finite adèlic modular group

$$\Gamma_1(m, N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\hat{\boldsymbol{Z}}) | a - 1 \equiv c \equiv 0 \bmod N,\ b \equiv d - 1 \equiv 0 \bmod m\right\}.$$

$$\left(\text{resp. } \Gamma_0(m, N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\hat{\boldsymbol{Z}}) | c \equiv 0 \bmod N,\ b \equiv 0 \bmod m\right\}\right).$$

The modular curve $X_1(m, N)$ is the coarse moduli space $(/\boldsymbol{Q}(\zeta_m))$ of the isomorphism classes of the generalized elliptic curves E with a pair (P_m, P_N) of points P_m and P_N which generate a subgroup $\simeq \boldsymbol{Z}/m\boldsymbol{Z} \times \boldsymbol{Z}/N\boldsymbol{Z}$, up to the isomorphism $(-1)_E \colon E \rightleftarrows E$ [4]. Let $Y_1(m, N)$, $Y_0(m, N)$ denote the open affine subschemes $X_1(m, N)\backslash\{\text{cusps}\}$ and $X_0(m, N)\backslash\{\text{cusps}\}$. For $m = 1$, let $X_1(N) = X_1(1, N)$, $X_0(N) = X_0(1, N)$, $\Gamma_1(N) = \Gamma_1(1, N)$, $\Gamma_0(N) = \Gamma(1, N)$, $Y_1(N) = Y_1(1, N)$ and $Y_0(N) = Y_0(1, N)$. Let K be a subfield of $\boldsymbol{C}$. For a K-rational point x on $Y_1(m, N)$ (resp. $Y_0(m, N)$), there exists an elliptic curve E defined over K with a pair (P_m, P_N) of K-rational points P_m and P_N (resp. (A_m, A_N) of cyclic subgroups A_m and A_N defined over K) such that (the isomorphism class containing) the pair $(E, \pm(P_m, P_N))$ (resp. the triple (E, A_m, A_N)) represents x [4] VI (3.2). The modular curve $X_0(mN)$ is isomorphic over $\boldsymbol{Q}$ to $X_0(m, N)$ by

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

where $E_N = \ker(N\colon E \to E)$ and A_N is the cyclic subgroup of order N of A. Let $\pi = \pi_{m,N}$ be the natural morphism of $X_1(m, N)$ to $X_0(m, N)$: $(E, \pm(P_m, P_N)) \mapsto (E, \langle P_m\rangle, \langle P_N\rangle)$, where $\langle P_m\rangle$ and $\langle P_m\rangle$ are the cyclic subgroups generated by P_m and P_N, respectively. Then π is a Galois covering with the Galois group $\bar{\Gamma}_0(m, N) = \Gamma_0(m, N)/\pm\Gamma_1(m, N) \simeq ((\boldsymbol{Z}/m\boldsymbol{Z})^\times \times (\boldsymbol{Z}/N\boldsymbol{Z})^\times)/\pm 1$. For integers α, β prime to N, $[\alpha, \beta]$ denotes the automorphism of $X_1(m, N)$ which is represented by $g \in \Gamma_0(m, N)$ such that $g \equiv \begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix}$ mod N. Then $[\alpha, \beta]$ acts as

$$(E, \pm(P_m, P_N)) \longmapsto (E, \pm(\alpha P_m, \beta P_N)).$$

When $\alpha \equiv \beta \bmod N$ or $m = 1$, let $[\alpha]$ denote $[\alpha, \beta]$. When $m = 1$, let $\pi_N = \pi_{1,N}$ and $\bar{\Gamma}_0(N) = \bar{\Gamma}_0(1, N)$. For a positive divisor d of N prime to N/d, let w_d denote the automorphism of $X_1(N)$ defined by

$$(E, \pm P) \longmapsto (E/\langle P_d \rangle, \pm(P + Q) \bmod \langle P_d \rangle),$$

where $P_d = (N/d)P$ and Q is a point of order d such that $e_d(P_d, Q) = \zeta_d$ for a fixed primitive d-th root ζ_d of 1. (e_d: $E_d \times E_d \to \mu_d$ is the e_d-pairing). For a subcovering $X : X_1(m, N) \to X \to X_0(N)$ (resp. $X_1(N) \to X \to X_0(N)$), we denote also by $[\alpha, \beta]$ (resp. w_d) the automorphism of X induced by $[\alpha, \beta]$ (resp. w_d). For a square free integer N, the covering $X_1(N) \to X_0(N)$ is unramified at the cusps. Let $\mathscr{X}$ denote the normalization of the projective j-line $\mathscr{X}_0(1) \simeq \boldsymbol{P}^1_{\boldsymbol{Z}}$ in X. For $X = X_1(m, N)$, $X = X_0(m, N)$, $X = X_1(N)$ and $X = X_0(N)$, let $\mathscr{X} = \mathscr{X}_1(m, N)$, $\mathscr{X} = \mathscr{X}_0(m, N)$, $\mathscr{X} = \mathscr{X}_1(N)$ and $\mathscr{X} = \mathscr{X}_0(N)$. Then $\mathscr{X} \otimes \boldsymbol{Z}[1/N] \to \operatorname{Spec} \boldsymbol{Z}[1/N]$ is smooth [4] VI (6.7).

(1.1) Let $\mathbf{0} = \binom{0}{1}$, $\boldsymbol{\infty} = \binom{1}{0}$ be the $\boldsymbol{Q}$-rational cusps on $X_0(N)$ which are represented by $(\boldsymbol{G}_m \times \boldsymbol{Z}/N\boldsymbol{Z}, \boldsymbol{Z}/N\boldsymbol{Z})$ and $(\boldsymbol{G}_m, \mu_N)$. Then $w_N(\mathbf{0}) = \boldsymbol{\infty}$. The cuspidal sections of the fibre $X_1(N) \times_{X_0(N)} \mathbf{0}$ are represented by the pairs $(\boldsymbol{G}_m \times \boldsymbol{Z}/N\boldsymbol{Z}, \pm P)$ for the points $P \in \{1\} \times \boldsymbol{Z}/N\boldsymbol{Z}$ of order N, which are all $\boldsymbol{Q}$-rational. We call them the $\mathbf{0}$-cusps. For a positive divisor d of N with $1 < d < N$ and for an integer i prime to N, let $\binom{i}{d}$ denote the cusps on $X_0(N)$ which is represented by $(\boldsymbol{G}_m \times \boldsymbol{Z}/(N/d)\boldsymbol{Z}, \boldsymbol{Z}/N\boldsymbol{Z}(\zeta_N, i))$, where $\boldsymbol{Z}/N\boldsymbol{Z}(\zeta_N, i)$ is the cyclic subgroup of order N generated by the section (ζ_N, i). Then $\binom{i}{d}$ is defined over $\boldsymbol{Q}(\zeta_n)$, where $n =$ G.C.M. of d and N/d. When N is a product of 2^m for $0 \leqq m \leqq 2$ and a square free odd integer, all the cusps on $X_0(N)$ are $\boldsymbol{Q}$-rational.

(1.2) Let $\Delta \subset (\boldsymbol{Z}/N\boldsymbol{Z})^\times$ be a subgroup containing ± 1 and $X = X_\Delta$ be the modular curve ($/\boldsymbol{Q}$) corresponding to the modular group

$$\Gamma_\Delta = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \middle| (\text{a} \bmod N) \in \Delta \right\}.$$

Then X_Δ is the subcovering of $X_1(N) \to X_0(N)$ associated with the subgroup Δ. For a prime divisor p of N, let Z' (resp. Z) be the irreducible component of the special fibre $\mathscr{X}_0(N) \otimes \boldsymbol{F}_p$ such that Z'^h ($= Z' \setminus \{$supersingular points on $\mathscr{X}_0(N) \otimes \boldsymbol{F}_p\}$) (resp. Z^h) is the coarse moduli space ($/\boldsymbol{F}_p$) of the isomorphism classes of the generalized elliptic curves E with a cyclic subgroup A, $A \simeq Z/NZ$ (resp. $A \simeq \mu_N$), locally for the étale topology ([4] V, VI). Let d be a positive divisor of N coprime to N/d. If $p|d$, then w_d exchanges Z' with Z. If $p \nmid d$, then w_d fixes Z' and Z. Let Z'_X be the fibre $\mathscr{X} \times_{\mathscr{X}_0(N)} Z'$. Then Z'^h_X is smooth over F_p and the 0-cusps $(\otimes F_p)$ are the sections of Z'^h_X. If $p||N$ and Δ contains the subgroup

$$\{a \in (Z/NZ)^\times | (a \bmod N/p) = \pm 1\},$$

then $\mathscr{X} \otimes F_p$ is reduced and $\mathscr{X}^h \otimes Z_{(p)} \to \operatorname{Spec} Z_{(p)}$ is smooth, where $Z_{(p)}$ is the localization of Z at (p) ([4] VI).

(1.3) We will make use of the following subcoverings $X = X_\Delta$: $X_1(mN) \to X \to X_0(mN)$.

m	N	X	Δ	genus of X
1	14	$X = X_1(14) \xrightarrow{3} X_0(14)$	$\{\pm 1\}$	1
1	15	$X = X_1(15) \xrightarrow{4} X_0(15)$	$\{\pm 1\}$	1
1	18	$X = X_1(18) \xrightarrow{3} X_0(18)$	$\{\pm 1\}$	2
1	20	$X = X_1(20) \xrightarrow{4} X_0(20)$	$\{\pm 1\}$	3
1	21	$X_1(21) \xrightarrow{2} X \xrightarrow{3} X_0(21)$	$(Z/3Z)^\times \times \{\pm 1\}$	3
1	24	$X_1(24) \xrightarrow{2} X \xrightarrow{2} X_0(24)$	$(Z/3Z)^\times \times \{\pm 1\}$	3
1	35	$X_1(35) \xrightarrow{4} X \xrightarrow{3} X_0(35)$	$(Z/5Z)^\times \times \{\pm 1\}$	7
1	55	$X_1(55) \xrightarrow{10} X \xrightarrow{2} X_0(55)$	$\{\pm 1\} \times (Z/11Z)^\times$	9
2	16	$X_1(32) \xrightarrow{2} X = X_1(2, 16) \xrightarrow{8} X_0(32)$	$\{\pm (1+16)\}$	5
2	10	$X_1(20) \xrightarrow{2} X = X_1(2, 10) \xrightarrow{2} X_0(20)$	$\{\pm 1\} \times \{\pm 1\}$	1
2	12	$X_1(24) \xrightarrow{2} X = X_1(2, 12) \xrightarrow{2} X_0(24)$	$\{\pm 1\} \times \{\pm 1\}$	1

(1.4) Mordell-Weil group of $J(X)$.

Let $J_1(m, N)$ and $J_0(m, N)$ be the jacobian varieties of $X_1(m, N)$ and $X_0(m, N)$, respectively. For $m = 1$, $J_1(1, N) = J_1(N)$ and $J_0(1, N) = J_0(N)$. For the integers $N = 13q$, $q = 2, 3, 5$ and 11, there exist (optimal) quotients $(/Q)$ of $J_0(N)$ whose Mordell-Weil groups are of finite order ([36] table 1,5). For $m = 1$ and $N = 14, 15, 18, 20, 21, 24, 35$ and 55, and $(m, N) =$

https://doi.org/10.1017/S0027763000002816 Published online by Cambridge University Press

(2,10), (2,12), let $X = X_\Delta$ be the subcoverings in (1.3) and $J(X)$ be their jacobian varieties. Then $J_1(2,10)$ and $J_1(2,12)$ are elliptic curves with finite Mordell-Weil groups ([36] table 1). Let $\mathrm{Coker}\,(J_0(N) \to J(X))$ be the cokernels of the morphisms as the Picard varieties. In the following table, the factors A $(/\mathbf{Q})$ of $J(X)$ have finite Mordell-Weil groups ([36] table 1, 5, [8] [14] [19], (1.5) below).

N	factor A of $J(X)$ or $A = J_0(N)$	dim A	genus of $X_0(N)$
22	$J_0(22)$	2	2
33	$J_0(33)$	3	3
55	$\mathrm{Coker}\,(J_0(55) \longrightarrow J(X))$	4	5
77	$J_0(77)/(1 + w_{11})J_0(77)$	3	7
14	$J_1(14)$	1	1
21	$\mathrm{Coker}\,(J_0(21) \longrightarrow J(X))$	3	1
28	$J_0(28)$	2	2
35	$\mathrm{Coker}\,(J_0(35) \longrightarrow J(X))$	4	3
20	$J_1(20)$	3	1
30	$J_0(30)$	3	3
45	$J_0(45)$	3	3
24	$\mathrm{Coker}\,(J_0(24) \longrightarrow J(X))$	3	1
15	$J_1(15)$	1	1
18	$J_1(18)$	2	0
36	$J_0(36)$	1	1
72	$J_0(72)$	5	5
32	$J_0(32)$	1	1
27	$J_0(27)$	1	1
10	$J_1(2, 10)$	1	1
12	$J_1(2, 12)$	1	1
16	$J_1(2, 16)$	5	1

PROPOSITION (1.5). *For the integers* $N = 20, 21, 24, 35$ *and* 55, *let* $X = X_\Delta$ *be the subcoverings in* (1.3) *and put* $C_X = \mathrm{Coker}\,(J_0(N) \to J(X))$. *Then* $\# C_X(\mathbf{Q}) < \infty$.

Proof.

Case $N = 20$: We use a result of Coates-Wiles on the Mordell-Weil groups of elliptic curves with complex multiplication ([1] [3] [29]). Let χ

https://doi.org/10.1017/S0027763000002816 Published online by Cambridge University Press

be the multiplicative character of $(\boldsymbol{Z}[\sqrt{-1}]/(2+\sqrt{-1}))^{\times}$ with $\chi(\sqrt{-1}) = -\sqrt{-1}$, and put

$$\varepsilon = \left(\frac{-1}{\ }\right)\cdot \chi_{|(\boldsymbol{Z}/5\boldsymbol{Z})^{\times}} \quad \text{and} \quad \bar{\varepsilon} = \left(\frac{-1}{\ }\right)\cdot \chi^{-1}_{|(\boldsymbol{Z}/5\boldsymbol{Z})^{\times}},$$

where $\left(\frac{-1}{\ }\right)$ is the quadratic residue symbol. Let $f_{\varepsilon}, f_{\bar{\varepsilon}}$ be the new forms ([2]) belonging to $S_2(\Gamma_1(20))$ (= the $\boldsymbol{C}$-vector space of holomorphic cusp forms of weight 2 belonging to $\Gamma_1(20)$) which are associated with the neben types characters ε and $\bar{\varepsilon}$, respectively; Let ψ be the primitive Grössen character of $\boldsymbol{Q}(\sqrt{-1})$ with conductor $(2+\sqrt{-1})$ such that $\psi((\alpha)) = \chi(\alpha)\alpha$ for $\alpha \in \boldsymbol{Q}(\sqrt{-1})^{\times}$ prime to the conductor $(2+\sqrt{-1})$. Then

$$f_{\varepsilon}(z) = \sum \psi(\mathfrak{A}) \exp(2\pi\sqrt{-1}N(\mathfrak{A})z),$$

where $N(\mathfrak{A}) = N_{\boldsymbol{Q}(\sqrt{-1})/\boldsymbol{Q}}(\mathfrak{A})$ is the norm of the ideal $\mathfrak{A} \neq \{0\}$ and $\mathfrak{A}$ runs over the set of integral ideals of $\boldsymbol{Q}(\sqrt{-1})$ ([33]). The modular curve $X_1(20)$ is of genus 3 and $H^0(X_1(20)\otimes \boldsymbol{C}, \Omega^1) = H^0(X_0(20)\otimes\boldsymbol{C}, \Omega^1) \oplus \boldsymbol{C}f_{\varepsilon}\,dz \oplus \boldsymbol{C}f_{\bar{\varepsilon}}\,dz$. For a cusp form $f \in S_2(\Gamma_1(20))$ and $g = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{GL}_2^+(\boldsymbol{Q})$, put

$$f|[g]_2(z) = (ad-bc)(cz+d)^{-2} f\left(\frac{az+b}{cz+d}\right) \quad \text{and} \quad f|K(z) = (f(-\bar{z}))^{-},$$

where $^{-}$ is the complex conjugation. Then for $H = \left[\begin{pmatrix} 0 & -1 \\ 20 & 0\end{pmatrix}\right]_2$, $f_{\varepsilon}|H = \lambda f_{\bar{\varepsilon}}$ with the absolute value $|\lambda| = 1$ ([2]). Put $g = f_{\varepsilon} - f_{\varepsilon}|H$ and $h = f_{\varepsilon} + f_{\varepsilon}|H$. Then $g = f_{\varepsilon} + e^{-2\sqrt{-1}\theta} f_{\varepsilon}|K = e^{-\sqrt{-1}\theta}(e^{\sqrt{-1}\theta} f_{\varepsilon} + e^{\sqrt{-1}\theta} f_{\varepsilon}|K)$ for a real number θ, and $e^{\sqrt{-1}\theta} g$ is real on the pure imaginary axis ([24] § 2). $C_X = \mathrm{Coker}(J_0(20) \to J(X))$ is isogenous over $\boldsymbol{Q}(\sqrt{-1})$ to the product of two elliptic curves E_{ε} and $E_{\bar{\varepsilon}}$ with $H^0(E_{\varepsilon}\otimes\boldsymbol{C}, \Omega^1) = \boldsymbol{C}f_{\varepsilon}dz$ and $H^0(E_{\bar{\varepsilon}}\otimes\boldsymbol{C}, \Omega^1) = \boldsymbol{C}f_{\bar{\varepsilon}}dz$. Further C_X is isogenous over $\boldsymbol{Q}$ to the restriction of scalars $\mathrm{Re}_{\boldsymbol{Q}(\sqrt{-1})/\boldsymbol{Q}}(E_{\varepsilon/\boldsymbol{Q}(\sqrt{-1})})$ ([5] [34]). For a cusp form $f \in S_2(\Gamma_1(20))$, put

$$(2\pi/\sqrt{20})^{-s}\Gamma(s)L_f(s) = \int_0^{\infty} t^s f(\sqrt{-1}t/\sqrt{20})\frac{dt}{t}$$

and

$$I(f) = \int_0^{\infty} f(\sqrt{-1}\,t/\sqrt{20})dt.$$

The (1-dimensional) L-function of $C_X/\boldsymbol{Q}$ and that of $E_{\varepsilon}/\boldsymbol{Q}(\sqrt{-1})$ are $L_{f_{\varepsilon}}(s)L_{f_{\bar{\varepsilon}}}(s)$ and $L_{f_{\varepsilon}}(1)L_{f_{\bar{\varepsilon}}}(1) = |L_{f_{\varepsilon}}(1)|^2$ (, since $f_{\bar{\varepsilon}} = f_{\varepsilon}|K$) ([21]). The rank of $C_X(\boldsymbol{Q})$ is zero if and only if $E_{\varepsilon}(\boldsymbol{Q}\sqrt{-1}) < \infty$. Then by the result on the Birch-Swinnerton Dyer conjecture for elliptic curves with complex multiplication ([1] [3] [29]), it suffices to show that $I(f_\varepsilon) \neq 0$. One sees that $I(h) = 0$ and $I(f_\varepsilon) = \frac{1}{2}(I(g) + I(h))$. Since $e^{\sqrt{-1}\theta}g$ is real on the pure imaginary axis, it suffices to show that $g(\sqrt{-1}t/\sqrt{20}) \neq 0$ for all $t > 0$. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(20)$ with $\varepsilon(a) = -1$. The $g|[\gamma]_2 = -g = g|H$, hence for $\delta = \gamma^{-1}\begin{pmatrix} 0 & -1 \\ 20 & 0 \end{pmatrix}$, $g|[\delta]_2 = g$. The quotient $X_1(20)/\langle\delta\rangle$ is an elliptic curve, so the zero points of gdz are the fixed points of δ. The automorphism δ has four fixed points, which correspond to $(-20\beta + \sqrt{-20})/20\alpha$ for integers α and β such that $\varepsilon(\alpha) = -1$ and $\begin{pmatrix} \alpha & \beta \\ * & * \end{pmatrix} \in \Gamma_0(20)$. Then $\beta \neq 0$, so δ does not have the fixed points on the pure imaginary axis.

For the remaining cases for $N = 21, 24, 35$ and 55, we apply a Mazur's method in [14] [19]. It suffices to show that C_X is $\boldsymbol{Q}$-simple and that $C_X(\boldsymbol{Q})$ has a subgroup $\neq \{0\}$ of order prime to the class numbers of $\boldsymbol{Q}(\zeta_N)$, where ζ_N is a primitive N-th root of 1 (see loc. cit.). For the class numbers, see e.g. [6] table.

Case $N = 21$ *and* 24: C_X are $\boldsymbol{Q}$-simple. By [35], one finds cuspidal subgroups of order 13 ($N = 21$) and 5 ($N = 24$).

Case $N = 35$: The characteristic polynomial of the Hecke operator T_2 on $S_2(\Gamma_\Delta)$ (associated with the prime number 2) is

$$(X^3 + X^2 - 4X) \times (X^4 + 2X^3 - 7X^2 - 14X + 1).$$

The first factor of the above polynomial corresponds to $X_0(35)$, so C_X is $\boldsymbol{Q}$-simple. There is a cuspidal subgroup of order 13 (see loc. cit.).

Case $N = 55$: The characteristic polynomial of T_2 on $S_2(\Gamma_\Delta)$ is

$$(X + 2)^2(X - 1)(X^2 - 2X - 1) \times (X^4 - 9X^2 + 12).$$

C_X corresponds to $X^4 - 9X^2 + 12$ ([36] table 5), so C_X is $\boldsymbol{Q}$-simple. There is a cuspidal subgroup of order 3. ■

(1.6) The following curves are hyperelliptic (of genus $\geqq 2$).

curve	hyperelliptic involution
$X_1(18)$	$w_2[5]$
$X_0(22)$	w_{22}
$X_0(33)$	w_{11}
$X_0(28)$	w_7
$X_0(30)$	w_{15}
$X_1(13)$	$[5]$

PROPOSITION (1.7) ([7], [8]). *Let X be the subcoverings in* (1.3) *for* $(m, N) = (2,16)$, $(1,20)$, $(1,21)$, $(1,24)$ *and* $(1,35)$. *Then X are not hyperelliptic.*

(1.8) For $N = 35, 55$ (resp. 77), let X be the subcoverings in (1.3) (resp. $X = X_0(77)$). For an automorphism γ of X, let S_γ denote the number of the fixed points of γ. Then we see the following.

N	γ	S_γ
35	$(E, A_5, \pm P_7) \longmapsto (E/A_5, E_5/A_5, \pm 3P_7 \bmod A_5)$	12
55	$(E, \pm P_5, A_{11}) \longmapsto (E/A_{11}, \pm 2P_5 \bmod A_{11}, E_{11}/A_{11})$	16
77	$\gamma = w_{77}\colon (E, A) \longmapsto (E/A, E_{77}/A)$	8

Here P_m is a point of order m and A_m is a subgroup of order m.

For the integers N in (1.8), we will apply the following lemma.

LEMMA (1.9). *Let K be a field, X a proper smooth curve defined over K and $(1 \neq)$ γ an automorphism of X with the fixed points x_i, $1 \leqq i \leqq s$. Let f be a rational function on X such that the divisors $(\gamma^* f) \neq (f)$. Then the degree of $f \leqq s/2$ and*

$$(\gamma^* f/f - 1)_0 > \textstyle\sum' (x_i)\,,$$

where $\sum'$ is the sum of the divisors (x_i) such that $f(x_i) \neq 0, \infty$.

Proof. Let S_0 (resp. S_∞, resp. T) be the set of the fixed points of γ consisting of x_i with $f(x_i) = 0$ (resp. $f(x_i) = \infty$, resp. $x_i \notin S_0 \cup S_\infty$). Then the divisor

$$(f) = E + \sum_{x_i \in S_0} n_i(x_i) - F - \sum_{x_i \in S_\infty} n_i(x_i)\,,$$

for effective divisors E and F, and positive integers n_i. Then

$$(\gamma^* f/f) = \gamma^* E + F - E - \gamma^* F\,.$$

By the assumption $(\gamma^* f) \neq (f)$, $g = \gamma^* f/f$ is not a constant function, so $\deg(g) \leqq 2 \cdot \deg(f) - \sum_{x_i \in S_0 \cup S_\infty} n_i$. For $x_i \in T$, $g(x_i) = 1$. Therefore

$$(g - 1)_0 > \sum_{w_i \in T} (x_i)\,.$$

Then $\deg(g) \geqq \sharp T$. Further $2 \cdot \deg(f) \geqq \deg(g) + \sum_{x_i \in S_0 \cup S_\infty} n_i \geqq s$. ∎

PROPOSITION (1.10) ([28] (3.3.2) [27]). *Let K be a finite extension of $\boldsymbol{Q}_p^{ur}$ of degree $e \leqq p - 1$ with the ring of integers $R = \mathcal{O}_K$. Let G_i $(i = 1, 2)$ be finite flat group schemes over R of rank p and $f\colon G_1 \to G_2$ be a homomorphism such that $f \otimes K\colon G_1 \otimes K \to G_2 \otimes K$ is an isomorphism. If $e <$*

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

COROLLARY (1.11). *Under the notation as in* (1.10), *assume that $e < p-1$. Let G be a finite flat group scheme over R of rank p and x an R-section of G. If $x \otimes \bar{\boldsymbol{F}}_p = 0$ (= the unit section), then $x = 0$.*

(1.12) Let K be a finite extension of $\boldsymbol{Q}_p$ with the ring of integers $R = \mathcal{O}_K$ and its residue field $\simeq \boldsymbol{F}_q$. Put $N = N' \cdot p^r$ for the integer N' prime to p. We here set an assumption on N that $r = 0$ if the absolute ramification index e of p (in K) $\geqq p-1$. Let E be an elliptic curve defined over K with a finite subgroup $G \subset E(K)$ of order N. Then by the universal property of the Néron model, the schematic closure $G_{/R}$ of G in $E_{/R}$ is a finite étale subgroup scheme (, since $e < p-1$ if $r > 0$ (1.11)). If $N \neq 2, 3$ nor 4, then $E_{/R}$ is semistable (see e.g. [36] p. 46). When E has good reduction, the Frobenius map $F = F_q \colon E_{/R} \otimes \boldsymbol{F}_q \to E_{/R} \otimes \boldsymbol{F}_q$ acts trivially on $G_{/R} \otimes \boldsymbol{F}_q$. In particular, $N \leqq (1 + \sqrt{q})^2$ (by the Riemann-Weil condition). When E has multiplicative reduction, the connected component T of $E_{/R} \otimes \boldsymbol{F}_q$ of the unit section is a torus such that $T(\boldsymbol{F}_q) \simeq \boldsymbol{Z}/(q-\varepsilon)\boldsymbol{Z}$ for $\varepsilon = \pm 1$. For a prime divisor l of N, the l-primary part of $G(\boldsymbol{F}_q) \simeq \boldsymbol{Z}/l^s\boldsymbol{Z} \times \boldsymbol{Z}/l^t\boldsymbol{Z}$ for integers s, t with $0 \leqq s \leqq t$. Then l^s divides $q - \varepsilon$ and $E_{/R} \otimes \boldsymbol{F}_q$ contains $T \times \boldsymbol{Z}/l^s\boldsymbol{Z}$. If $l^t \nmid q - \varepsilon$, then $E_{/R} \otimes \boldsymbol{F}_q$ contains $T \times \boldsymbol{Z}/l^t\boldsymbol{Z}$.

(1.13) Let X $(\to X_0(1))$ be a modular curve defined over $\boldsymbol{Q}$ with its jacobian variety $J = J(X)$. Let k be a quadratic field and $\mathfrak{p}$ be a prime of k lying over a rational prime p. Let $R = (\mathcal{O}_k)_{(\mathfrak{p})}$, $\boldsymbol{Z}_{(p)}$ denote the localizations at $\mathfrak{p}$ and p, respectively. Let x be a k-rational point on X such that $x \otimes \kappa(\mathfrak{p})$ is a section of the smooth part $\mathscr{X}^{\text{smooth}} \otimes \boldsymbol{Z}_{(p)}$ and that $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$, $x^\sigma \otimes \kappa(\mathfrak{p}) = C_\sigma \otimes \kappa(\mathfrak{p})$ for $\boldsymbol{Q}$-rational cusps C, C_σ and $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$, where $\mathscr{X}$ is the normalization of the projective j-line $\mathscr{X}_0(1) \simeq \boldsymbol{P}^1_{\boldsymbol{Z}}$ in X. Consider the $\boldsymbol{Q}$-rational section $i(x) = cl((x) + (x^\sigma) - (C) - (C_\sigma))$ of the Néron model $J_{/\boldsymbol{Z}}$:

$$
\begin{array}{ccc}
\mathrm{Spec}\, R \times \mathrm{Spec}\, R \xrightarrow{x \times x^\sigma} (\mathscr{X} \times \mathscr{X})^{\text{smooth}} & \xrightarrow{\ i\ } & J_{/\boldsymbol{Z}} \times J_{/\boldsymbol{Z}} \\
 & (z, z') \longmapsto & (cl((z) - (C)),\ cl((z') - (C_\sigma)) \\
\Big\downarrow {\scriptstyle \Delta:\ \text{diagonal}} & & \Big\downarrow {\scriptstyle +} \\
\mathrm{Spec}\, \boldsymbol{Z}_{(p)} & \xrightarrow{\qquad i(x) \qquad} & J_{/\boldsymbol{Z}}\,.
\end{array}
$$

Then $((x \times x^\sigma) \cdot i \cdot +) \otimes \kappa(\mathfrak{p}) = 0$ (= the unit section), hence $i(x) \otimes \boldsymbol{F}_p = 0$.

Let $A/\boldsymbol{Q}$ be a quotient of J; $J \xrightarrow{j} A$ which has the Mordell-Weil group of finite order. If $p \neq 2$, then the specialization Lemma (1.11) shows that $j \cdot i(x) = 0$.

Remark (1.14). Under the notation as in (1.13), we here consider the case when C and C_σ are not $\boldsymbol{Q}$-rational. Assume that the set $\{C, C_\sigma\}$ is $\boldsymbol{Q}$-rational and that $C \otimes \boldsymbol{Z}_{(p)}$ and $C_\sigma \otimes \boldsymbol{Z}_{(p)}$ are the sections of $\mathscr{X}^{\text{smooth}} \otimes \boldsymbol{Z}_{(p)}$. Let K be the quadratic field over which C and C_σ are defined. Let $\mathfrak{p}'$ be a prime of K lying over p and e' be the ramification index p in K. Then by the same way as in (1.3), we get $i(x) \otimes \kappa(\mathfrak{p}') = 0$ in $J_{/\mathcal{O}_K}$. If $e' < p - 1$ or p does not divide $\sharp A(\boldsymbol{Q})$, then $j \cdot i(x) = 0$.

For a finite extension K of $\boldsymbol{Q}$ and for an abelian variety A defined over K, let $f(A/K)$ denote the conductor of A over K.

LEMMA (1.15) ([21] Proposition 1). *Let E be an elliptic curve defined over a finite extension K of $\boldsymbol{Q}$ and L be a quadratic extension of K, with the relative discriminant $D = D(L/K)$. Then the restriction of scalars* $\mathrm{Re}_{L/K}(E_{/L})$ ([5] [34]) *is isogenous over K to a product of E and an elliptic curve $F(/K)$ with $f(E/K)f(F/K) = N_{L/K}(f(E/L))^2 D$.*

§ 2. Rational points on $X_1(N)$

Let k be a quadratic field and N an integer of a product of 2, 3, 5, 7, 11 and 13. Let x be a k-rational point on $X_1(N)$. Then there exists an elliptic curve E/k with a k-rational point P of order N such that (the isomorphism class containing) the pair $(E, \pm P)$ represents x ([4] VI (3.2)). For $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$, x^σ is represented by the pair $(E^\sigma, \pm P^\sigma)$. For the integers N, $1 \leqq N \leqq 10$ or $N = 12$, $X_1(N) \simeq \boldsymbol{P}^1$. For $N = 11, 14$ and 15, $X_1(N)$ are elliptic curves. For $N = 13, 16$ and 18, $X_1(N)$ are hyperelliptic curves of genus 2. In this section, we prove the following theorem.

THEOREM (2.1). *Let N be an integer of a product of* 2, 3, 5, 7, 11 *and* 13. *If $X_1(N)$ is of genus $\geqq 2$ and is not hyperelliptic, then $Y_1(N)(k) = \phi$ for any quadratic field k.*

Proof. It suffices to discuss the cases for the following integers $N = 2 \cdot 13, 3 \cdot 13, 5 \cdot 13, 7 \cdot 13, 11 \cdot 13; 2 \cdot 11, 3 \cdot 11, 5 \cdot 11, 7 \cdot 11; 3 \cdot 7, 4 \cdot 7, 5 \cdot 7; 4 \cdot 5, 6 \cdot 5, 9 \cdot 5; 8 \cdot 3, 4 \cdot 9$ (see [8, 12] [23]). Suppose that there exists a k-rational point x on $Y_1(N)$. Let $(E, \pm P)/k$ be a pair which represents x with a k-rational point P of order N and let $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$.

Case $N = 13q$ for $q = 2, 3, 5, 7$ and 11: We make use of the following lemma.

LEMMA (2.2) ([23] (3.2)). *Let y be a k-rational point on $Y_1(13)$. Then the set $\{y, [5](y)\}$ represents a $\boldsymbol{Q}$-rational point on $X_1(13)/\langle[5]\rangle \simeq \boldsymbol{P}^1_{\boldsymbol{Q}}$, where $[5]$ is the automorphism of $X_1(13)$ represented by $g \in \Gamma_0(13)$ such that* $g \equiv \begin{pmatrix} 5 & * \\ 0 & * \end{pmatrix} \bmod 13$.

Let $\pi\colon X_1(13q) \to X_1(13)$ be the natural morphism and y be the $\boldsymbol{Q}$-rational point $\{\pi(x), [5]\pi(x)\}$ on $Y_1(13)/\langle[5]\rangle$. Let $\mathfrak{p}$ be a prime of k lying over the rational prime $p = 3$ if $q = 2$, and $p = 5$ if $q \geqq 3$. Then the condition $\boldsymbol{Z}/N\boldsymbol{Z} \subset E(k)$ leads that $(\boldsymbol{Z}/N\boldsymbol{Z})_{/R} \subset E_{/R}$, where R is the localization $(\mathcal{O}_k)_{(\mathfrak{p})}$ of $\mathcal{O}_k$ at $\mathfrak{p}$ (1.12). Then $E_{/R}$ has multiplicative reduction cf. (1.12). Let F be an elliptic curve defined over $\boldsymbol{Q}$ with a $\boldsymbol{Q}$-rational set $\{\pm Q, \pm 5Q\}$ for a point Q of order 13 such that the pair $(F, \{\pm Q, \pm 5Q\})$ represents y on $Y_1(13)/\langle[5]\rangle$. Let $\rho = \rho_q$ be the representation of the Galois action of $G = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on the q-torsion points $F_q(\bar{\boldsymbol{Q}})$. Then $F \simeq E$ over a quadratic extension K of k, since E has multiplicative reduction at $\mathfrak{p}$. Then for $G_K = \mathrm{Gal}(\bar{\boldsymbol{Q}}/K)$,

$$\rho(G_K) \hookrightarrow \left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}\right\} \subset \mathrm{GL}_2(\boldsymbol{F}_q) \simeq \mathrm{Aut}\, F_q(\bar{\boldsymbol{Q}}).$$

When $q = 2$, $\mathrm{GL}_2(\boldsymbol{F}_q) \simeq \mathcal{S}_3$ (= the symmetric group of three letters) and $[\rho(G)\colon \rho(G_K)]$ divides 4, so that $\rho(G) \hookrightarrow \left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}\right\}$. Then F has a $\boldsymbol{Q}$-rational point Q_2 of order 2 and the pair $(F, \langle Q_2, Q\rangle)$ represents a $\boldsymbol{Q}$-rational point on $Y_0(26)$. But we know that $Y_0(26)(\boldsymbol{Q}) = \phi$ ([18] [24] [36] table 1, 5). Now consider the cases for $q \geqq 3$. Let θ_q be the cyclotomic character

$$\theta_q\colon G = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) \longrightarrow \mathrm{Aut}\, \mu_q(\bar{\boldsymbol{Q}}).$$

Then $\det \cdot \rho = \theta_q$. Let P_q be a K-rational point on F of order q and $g \in G_k \backslash G_K$ for $G_k = \mathrm{Gal}(\bar{\boldsymbol{Q}}/k)$. If $P_q^g \neq \pm P_q$, then $\langle P_q^g\rangle \neq \langle P_q\rangle$ and $\rho(G_K) = \{1\}$. Then $\theta_q(G_K) = \{1\}$, hence $q = 3$, or $q = 5$ and $K = \boldsymbol{Q}(\zeta_5)$. For $q = 3$, if $k \neq \boldsymbol{Q}(\zeta_3)$, then K is an abelian extension of $\boldsymbol{Q}$ with the Galois group $\simeq \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$ and $\rho(G) \hookrightarrow \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}$. If $k = \boldsymbol{Q}(\zeta_3)$, then $\rho(G_k) = \{\pm 1\}$, since $\det \rho(G_k) = \theta_3(G_k) = \{1\}$. Then $\rho(G) \hookrightarrow \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}$, since $\theta_3(G) = \{\pm 1\}$. For $q = 5$, $K = \boldsymbol{Q}(\zeta_5)$ and $\rho(G) \hookrightarrow \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}$. Thus there exists a subgroup

$A_q/\boldsymbol{Q}$ of F of order q. Then the pair $(F, A_q + \langle Q\rangle)$ represents a $\boldsymbol{Q}$-rational point on $Y_0(13q)$. But we know that $Y_0(13q)(\boldsymbol{Q}) = \phi$ for $q \geqq 2$ ([9, 10, 11] [18] [20]). Now suppose that $P_q^g = \pm P_q$. Then $\rho(G_k) \hookrightarrow \left\{\begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix}\right\}$. Take $h \in G \backslash G_k$ and put $A_q = \langle P_q\rangle$. If $A_q^h = A_q$, then the pair $(F, A_q + \langle Q\rangle)$ represents a $\boldsymbol{Q}$-rational point on $Y_0(13q)$. Therefore, $A_q^h \neq A_q$ and $\rho(G_k) \hookrightarrow \left\{\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}\right\}$. If $\rho(G_k) \hookrightarrow \left\{\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$, then $q = 3$, $k = \boldsymbol{Q}(\zeta_3)$ and $\rho(G) \hookrightarrow \left\{\pm\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}$ and the same argument as above gives a contradiction. If $\rho(G_k) \simeq \left\{\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}\right\}$, then $q = 3$ and $\rho(G)$ is contained in the normalizer of a split Cartan subgroup (, since $\det \rho = \theta_q$). Let Y be the modular curve $/\boldsymbol{Q}$ which corresponds to the modular group

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(13) \,|\, b \equiv c \equiv 0 \text{ or } a \equiv d \equiv 0 \bmod 3\right\}.$$

Let w be the involution of Y represented by a matrix $g \in \Gamma_0(13)$ such that $g \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \bmod 3$. Then the isomorphism of $X_0(9 \cdot 13)$ to Y:

$$(C, A_9 + A_{13}) \longmapsto (C/A_3, \{A_9/A_3, C_3/A_3\}, (A_{13} + A_3)/A_3)$$

induces an isomorphism of $X_0(9 \cdot 13)/\langle w_9\rangle$ to $Z = Y/\langle w\rangle$, where A_m are cyclic subgroups of order m with $A_3 \subset A_9$. The jacobian variety $J = J(Z)$ of Z has an optimal quotient $A/\boldsymbol{Q}\,(J \twoheadrightarrow A)$ with finite Mordell-Weil group ([36] table 1,5). As was seen as above, F has potentially mutiplicative reduction at 5. Let z be the $\boldsymbol{Q}$-rational point on Y represented by $(F, \langle Q\rangle)$ with a level structure mod 3, then $z \otimes \boldsymbol{F}_5 = C \otimes \boldsymbol{F}_5$ for a $\boldsymbol{Q}$-rational cusp C on Z. Let $f\colon Z \to J \to A$ be the morphism defined by $f(y) = cl((y) - (C))$. Then we see that $f(z) = 0$ (see (1.11)). Let $\mathscr{Z}$ denote the normalization of $\mathscr{X}_0(1)$ in Z. Then we see that $f \otimes \boldsymbol{Z}_5\colon \mathscr{Z} \otimes \boldsymbol{Z}_5 \to A_{/\boldsymbol{Z}_5}$ is a formal immersion along the cusp C (see the proof in [22] (2.5)). Therefore, Mazur's method in [18] Section 4 can be applied to yield $z = C$. Thus we get a contradiction.

Case $N = 11q$ *for* $q = 2, 3, 5$ *and* 7: $q = 2$ and 3: Let $\mathfrak{p}$ be a prime of k lying over the rational prime 3 and put $R = (\mathcal{O}_k)_{(\mathfrak{p})}$. The condition $\boldsymbol{Z}/N\boldsymbol{Z} \subset E(k)$ shows that $(\boldsymbol{Z}/N\boldsymbol{Z})_{/R} \subset E_{/R}$ if $q = 2$ or $q = 3$ is unramified (1.11). If $q = 3$ ramifies in k, then $(\boldsymbol{Z}/11\boldsymbol{Z})_{/R} \subset E_{/R}$ and $\kappa(\mathfrak{p}) = \boldsymbol{F}_3$. Hence $x \otimes \kappa(\mathfrak{p})$ is also a cusp (see (1.12)). Denote also by x, x^σ the images of x and x^σ under the natural morphism $\pi\colon X_1(N) \to X_0(N)$. Then $x \otimes \kappa(\mathfrak{p}) =$

https://doi.org/10.1017/S0027763000002816 Published online by Cambridge University Press

$C \otimes \kappa(p)$, $x^\sigma \otimes \kappa(p) = C_\sigma \otimes \kappa(p)$ for $\boldsymbol{Q}$-rational cusps C and C_σ on $X_0(N)$. Let $i(x) = cl((x) + (x^\sigma) - (C) - (C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J_0(N)_{/\boldsymbol{Z}}$. The Mordell-Weil groups of $J_0(11q)$ for $q = 2$ and 3 are finite and their orders are prime to 3 [36] table 1, 3, 5. Therefore $i(x) = 0$, see (1.13). Since $Y_0(11q)(\boldsymbol{Q}) = \phi$ [18], $C_\sigma = w_{22}(C)$ if $q = 2$ and $C_\sigma = w_{11}(C)$ if $q = 3$ (see (1.6)). As was seen as above, C and C_σ are represented by $(\boldsymbol{G}_m \times \boldsymbol{Z}/11m\boldsymbol{Z}, H)$ and $(\boldsymbol{G}_m \times \boldsymbol{Z}/11m_\sigma\boldsymbol{Z}, H_\sigma)$ for integers $m, m_\sigma \geqq 1$ and cyclic subgroup H, H_σ containing the subgroup $\simeq \boldsymbol{Z}/11\boldsymbol{Z}$. Thus we get a contradiction, since $w_{22}(C)$, $w_{11}(C)$ are represented by $(\boldsymbol{G}_m \times \boldsymbol{Z}/m'\boldsymbol{Z}, H')$ for integers m' prime to 11 [4] VII.

$q = 5$: Let X be the subcovering as in (1.3):

$$X_1(55) \xrightarrow{\pi_1} X \xrightarrow{\pi_X} X_0(55)\,.$$

Let $1 \neq \gamma \in \mathrm{Gal}\,(X/X_0(55))$ and δ be the automorphism of X defined by

$$(F, \pm P_5, B_{11}) \longmapsto (F/B_{11}, \pm 2P_5 \bmod B_{11}, E_{11}/B_{11})\,,$$

where P_5 is a point of order 5 and B_{11} is a subgroup of order 11. Then δ has 16 fixed points (1.8). Let p be a prime of k lying over the rational prime 5 and put $R = (\mathcal{O}_k)_{(p)}$. The condition $\boldsymbol{Z}/55\boldsymbol{Z} \subset E(k)$ shows that $x \otimes \kappa(p) = C \otimes \kappa(p)$, $x^\sigma \otimes \kappa(p) = C_\sigma \otimes \kappa(p)$ for $\boldsymbol{0}$-cusps C and C_σ (see (1.11), (1.12)). Denote also by x, x^σ, C and C_σ the images of x, x^σ, C and C_σ under the natural morphism π_1: $X_1(55) \to X$. Put $C_X = \mathrm{Coker}\,(\pi_X^*\colon J_0(55) \to J(X))$, which has the Mordell-Weil group of finite order (1.5). Let $i(x) = cl((x) + (x^\sigma) - (C) - (C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J(X)_{/\boldsymbol{Z}}$. Then $i(x) \otimes \boldsymbol{F}_5 = 0$ (1.13), so by (1.11), $i(x) \in \pi_X^*(J_0(55))$. Then we get a rational function f on X such that

$$(f) = (x) + (x^\sigma) + (\gamma(C)) + (\gamma(C_\sigma)) - (\gamma(x)) - (\gamma(x^\sigma)) - (C) - (C_\sigma)\,.$$

Since $\gamma(C) \otimes \boldsymbol{F}_5 \neq C \otimes \boldsymbol{F}_5$, $\gamma(x) \neq x$. If f is a constant function, then $\gamma(x) = x^\sigma$ and the set $\{x, \gamma(x) = x^\sigma\}$ defines a $\boldsymbol{Q}$-rational point on $Y_0(55)$. But $Y_0(55)(\boldsymbol{Q}) = \phi$ [18], so that f is not a constant function. If $(\delta^* f) = (f)$, then $\delta(C) = C$ or C_σ. But C, C_σ are $\boldsymbol{0}$-cusps and $\delta(C)$ is not a $\boldsymbol{0}$-cusps, so that $(\delta^* f) \neq (f)$. Applying (1.9) to f and δ, we get a contradiction.

Remark (2.3). For any cubic field k', $Y_1(55)(k') = \phi$. It is shown by the same way as above, taking a prime $p'|5$ of the smallest Galois extension of $\boldsymbol{Q}$ containing k'.

$q = 7$: Let π_{11}: $X_0(77) \to X_0(77)/\langle w_{11} \rangle$ be the natural morphism and J' be the jacobian variety of $X_0(77)/\langle w_{11} \rangle$. Then $A = \operatorname{Coker}(\pi_{11}^*: J' \to J_0(77))$ has the Mordell-Weil group of finite order [36] table 1,5. Let p be a prime of k lying over the rational prime 5. The condition $\boldsymbol{Z}/77\boldsymbol{Z} \subset E(k)$ shows that $x \otimes \kappa(p)$ is a $\mathbf{0}$-cusp $(\otimes \kappa(p))$ (1.12). Denote also by x, x^σ the images of x and x^σ under the natural morphism $X_1(77) \to X_0(77)$. Then $x \otimes \kappa(p) = \mathbf{0} \otimes \kappa(p)$. Let $i(x) = cl((x) + (x^\sigma) - 2(\mathbf{0}))$ be the $\boldsymbol{Q}$-rational section of $J_0(77)_{/\boldsymbol{Z}}$. Then $i(x) \otimes \boldsymbol{F}_5 = 0$ and $i(x) \in \pi_{11}^*(J')$ (see (1.11), (1.13)). Then we get a rational function $f/\boldsymbol{Q}$ on $X_0(77)$ such that

$$(f) = (x) + (x^\sigma) + 2(w_{11}(\mathbf{0})) - (w_{11}(x)) - (w_{11}(x^\sigma)) - 2(\mathbf{0})\,.$$

Then $(w_{11}^* f) = -(f) \neq 0$, since $w_{11}(\mathbf{0}) \neq \mathbf{0}$. Hence $w_{11}^* f = \alpha/f$ for $\alpha \in \boldsymbol{Q}^\times$. The fundamental involution $w = w_{77}$ of $X_0(77)$ has 8 fixed points $x_i\,(1 \leqq i \leqq 8)$. The cusps $w_{11}(\mathbf{0}) \otimes \boldsymbol{F}_5$ and $\mathbf{0} \otimes \boldsymbol{F}_5$ are not the fixed point of w. Therefore by (1.9),

$$(w^* f/f - 1)_0 = \sum_{i=1}^{8} (x_i) \;(\underset{\text{put}}{=} D)\,.$$

Put $g = (w^* f/f - 1)^{-1}$. Then

$$(g) = (x) + (x^\sigma) + 2(w_{11}(\mathbf{0})) + (w_7(x)) + (w_7(x^\sigma)) + 2(\infty) - D$$

and

$$w^* g = w_{11}^* g = -1 - g\,.$$

Then g defines a rational function h on $Y = X_0(77)/\langle w_7 \rangle$ with $\pi_7^*(h) = g$, where π_7: $X_0(77) \to Y$ is the natural morphism. Set $\{y_i\}_{1 \leqq i \leqq 4} = \{\pi_7(x_j)\}$, and put $E = \sum_{i=1}^{4} (y_i)$ and $C = \pi_7(\infty)$ $(= \pi_7(w_7(\mathbf{0})))$. Then h is of degree 4 and $h \in H^0(Y, \mathcal{O}_Y(E - 2(C)))$. Denote also by w the involution of Y induced by w (and w_{11}). Then

$$w^* h = -1 - h \quad \text{and} \quad (h)_\infty = E\,.$$

Let π_Y: $Y \to Z = X_0(77)/\langle w_7, w_{11} \rangle$ be the natural morphism. Z is an elliptic curve [36] table 5. The canonical divisor $K_Y \sim E$ (linearly equivalent) and $\dim H^0(Y, \mathcal{O}_Y(E)) = 3$. Let ω be the base of $H^0(Z, \Omega^1)$ and $\omega_1 = \pi_Y^*(\omega)$, ω_2 and ω_3 be the basis of $H^0(Y, \Omega^1)$ such that $\omega_i(C) = 1$ and that ω_i are eigen forms of the Hecke ring $\boldsymbol{Q}[T_m, w]_{(m,77)=1}$ with $T_2^* \omega_2 = 0$ and $T_2^* \omega_3 = \omega_3$ (see [36] table 1, 3, 5). Then $\{1, f_2 = \omega_2/\omega_1, f_3 = \omega_3/\omega_1\}$ is the set of basis of $H^0(Y, \mathcal{O}_Y(E))$ such that $f_2 = 1 + q + \cdots$ and $f_3 = 1 - 3q + \cdots$ for $q = \exp(2\pi\sqrt{-1}z)$ (see loc. cit.). Then $h = a_1 + a_2 f_2 + a_3 f_3$ for $a_i \in \boldsymbol{Q}$. The conditions $w^*h = -1 - h$ and $w^*f_i = -f_i$ show that $a_1 = -\frac{1}{2}$. Further by the condition $(h)_0 \succ 2(C)$, $a_2 = \frac{1}{3}$ and $a_3 = \frac{1}{6}$. Let $\mathscr{Y}$ be the quotient $\mathscr{X}_0(77)/\langle w_7\rangle \otimes \boldsymbol{Z}_5$ and $\widehat{\mathscr{O}_{\mathscr{Y},C}}$ be the completion of the local ring $\mathscr{O}_{\mathscr{Y},C}$ along the cuspidal section C. Then $f_i \in \widehat{\mathscr{O}_{\mathscr{Y},C}}$, so that $h \in \widehat{\mathscr{O}_{\mathscr{Y},C}}$. Put $C' = \pi_7(\mathbf{0})$ $(= \pi_7(w_7(\mathbf{0})))$. Then $w^*h \in \widehat{\mathscr{O}_{\mathscr{Y},C'}}$ and $w^*h(\pi_Y(x)) = (-1 - h)(\pi_Y(x)) = -1$, $w^*h(C') = (-1 - g)(\mathbf{0}) = 0$. But the conditions that $x \otimes \kappa(\mathfrak{p}) = \mathbf{0} \otimes \kappa(\mathfrak{p})$ for $\mathfrak{p}(|5)$ and $w^*h \in \widehat{\mathscr{O}_{\mathscr{Y},C'}}$ give the congruence $w^*h(\pi_Y(x)) \equiv w^*h(C') \bmod \mathfrak{p}$. Thus we get a contradiction.

Case $N = 7n$ for $n = 3, 4$ and 7:

$n = 3$: Let X be the subcovering as n (1.3):

$$X_1(21) \xrightarrow{2} X \xrightarrow{3} X_0(21)\,,$$

which corresponds to the subgroup $\varDelta = (\boldsymbol{Z}/3\boldsymbol{Z})^\times \times \{\pm 1\}$. Let $\mathscr{X}$ denote the normalization of $\mathscr{X}_0(1)$ in X. The special fibre $\mathscr{X} \otimes \boldsymbol{F}_3$ is reduced (1.2). Let $\mathfrak{p}$ be a prime of k lying over the rational prime 3 and put $R = (\mathscr{O}_k)_{(\mathfrak{p})}$. The condition $\boldsymbol{Z}/21\boldsymbol{Z} \subset E(k)$ shows that $(\boldsymbol{Z}/21\boldsymbol{Z})_{/R} \subset E_{/R}$ if the rational prime 3 is unramified in k (1.11), (1.12). If 3 ramifies in k, then $\kappa(\mathfrak{p}) = \boldsymbol{F}_3$, so that in both cases $E_{/R}$ has multiplicative reduction see (1.12). Therefore, $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$, $x^\sigma \otimes \kappa(\mathfrak{p}) = C_\sigma \otimes \kappa(\mathfrak{p})$ for $\boldsymbol{Q}$-rational cusps C and C_σ (see loc. cit.). Let $i(x) = cl((x) + (x^\sigma) - (C) - (C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J(X)_{/\boldsymbol{Z}}$. Since the Mordell-Weil group of $J(X)$ is finite (1.4), (1.5), $(x) + (x^\sigma) \sim (C) + (C_\sigma)$. But X is not hyperelliptic (1.7).

$n = 4$: Let $\mathfrak{p}$ be a prime of k lying over the rational prime 3 and put $R = (\mathscr{O}_k)_{(\mathfrak{p})}$. The condition $\boldsymbol{Z}/28\boldsymbol{Z} \subset E(k)$ shows that $(\boldsymbol{Z}/28\boldsymbol{Z})_{/R} \subset E_{/R}$. Denote also by x, x^σ the images of x and x^σ under the natural morphism $X_1(28) \to X_0(28)$. Then $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$, $x^\sigma \otimes \kappa(\mathfrak{p}) = C_\sigma \otimes \kappa(\mathfrak{p})$ for $\boldsymbol{Q}$-rational cusps C and C_σ. These cusps C, C_σ are represented by $(\boldsymbol{G}_m \times \boldsymbol{Z}/7m\boldsymbol{Z}, H)$ and $(\boldsymbol{G}_m \times \boldsymbol{Z}/7m_\sigma\boldsymbol{Z}, H_\sigma)$ for integers m and m_σ and cyclic subgroups H, H_σ containing $\{1\} \times m\boldsymbol{Z}/7m\boldsymbol{Z}$ and $\{1\} \times m_\sigma\boldsymbol{Z}/7m_\sigma\boldsymbol{Z}$, respectively. Let $i(x) = cl((x) + (x^\sigma) - (C) - (C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J_0(28)_{/\boldsymbol{Z}}$. Since the Mordell-Weil group of $J_0(28)$ is finite (1.4), $i(x) = 0$ (1.13) and $(x) + (x^\sigma) \sim (C) + (C_\sigma)$. $X_0(28)$ has the hyperelliptic involution w_7, so $C_\sigma = w_7(C)$. But as noted as above, $C_\sigma \neq w_7(C)$.

$n = 5$: Let X be the subcovering as in (1.3):

$$X_1(35) \xrightarrow{\pi_1} X \xrightarrow{\pi_X} X_0(35)\,,$$

which corresponds to the subgroup $\varDelta = (\boldsymbol{Z}/5\boldsymbol{Z})^{\times} \times \{\pm 1\}$. The automorphism γ of X represented by

$$(F, B_5, \pm Q_7) \longmapsto (F/B_5, F_5/B_5, \pm 3Q_7 \bmod B_5)$$

has 12 fixed points (1.8). Let $\mathfrak{p}$ be a prime of k lying over the rational prime 3 and put $R = (\mathcal{O}_k)_{(\mathfrak{p})}$. The condition $\boldsymbol{Z}/35\boldsymbol{Z} \subset E(k)$ shows that $(\boldsymbol{Z}/35\boldsymbol{Z})_{/R} \subset E_{/R}$. Denote also by x, x^{σ} the images of x and x^{σ} by the natural morphism $\pi_1 \colon X_1(35) \to X$. Then $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$, $x^{\sigma} \otimes \kappa(\mathfrak{p}) = C_{\sigma} \otimes \kappa(\mathfrak{p})$ for $\boldsymbol{Q}$-rational cusps C and C_{σ} (1.12). Let $i(x) = cl((x) + (x^{\sigma}) - (C) - (C_{\sigma}))$ be the $\boldsymbol{Q}$-rational section of $J(X)_{/\boldsymbol{Z}}$. The Mordell-Weil group of $C_X =$ Coker $(\pi_X^{*} \colon J_0(35) \to J(X))$ is finite (1.5). Let δ be a generator of Gal $(X/X_0(35))$. Then we get a rational function f on X such that

$$(f) = (x) + (x^{\sigma}) + (\delta(C)) + (\delta(C_{\sigma})) - (\delta(x)) - (\delta(x^{\sigma})) - (C) - (C_{\sigma})$$

(see (1.13)). If f is a constant function, then $\{x, x^{\sigma}\} = \{\delta(x), \delta(x^{\sigma})\}$. Then $x = \delta(x) = \delta^2(x)$, hence $C \otimes \kappa(\mathfrak{p}) = \delta(C \otimes \kappa(\mathfrak{p}))$. But $C \otimes \kappa(\mathfrak{p})$ is not a fixed point of δ. The similar argument as above shows that $(\gamma^{*}f) \neq (f)$. Applying (1.9) to f and γ, we get a contradiction.

Case $N = 5n$ *for* $n = 4, 6$ *and* 9:

$n = 4$: Let $\mathfrak{p}$ be a prime of k lying over the rational prime 3 and put $R = (\mathcal{O}_k)_{(\mathfrak{p})}$. The condition $\boldsymbol{Z}/20\boldsymbol{Z} \subset E(k)$ shows that $(\boldsymbol{Z}/20\boldsymbol{Z})_{/R} \subset E_{/R}$ and that $E_{/R}$ has multiplicative reduction (1.12). Let T be the connected component of the special fibre $E_{/R} \otimes \kappa(\mathfrak{p})$ of the unit section. If $\mathfrak{p}$ is of degree one, then $\boldsymbol{Z}/5\boldsymbol{Z} \not\subset T(\boldsymbol{F}_3)$. Then $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$, $x^{\sigma} \otimes \kappa(\mathfrak{p}) = C_{\sigma} \otimes \kappa(\mathfrak{p})$ for $\boldsymbol{Q}$-rational cusps C and C_{σ}, since $\left(\frac{-1}{3}\right) = -1$, where $\left(\frac{-1}{}\right)$ is the quadratic residue symbol. If $\mathfrak{p}$ is of degree two, then $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$ for a $\boldsymbol{Q}(\sqrt{-1})$-rational cusp C, and $x^{\sigma} \otimes \kappa(\mathfrak{p}) = C_{\sigma} \otimes \kappa(\mathfrak{p})$ with $C_{\sigma} = C^{\tau}$ for $1 \neq \tau \in \mathrm{Gal}\,(\boldsymbol{Q}(\sqrt{-1})/\boldsymbol{Q})$. Let $i(x) = cl((x) + (x^{\sigma}) - (C) - (C_{\sigma}))$ be the $\boldsymbol{Q}$-rational section of $J_1(20)_{/\boldsymbol{Z}}$. Since $\sharp J_1(20)(\boldsymbol{Q}) < \infty$ (1.4) (1.5), $i(x) = 0$ (1.14) and $(x) + (x^{\sigma}) \sim (C) + (C_{\sigma})$. But $X_1(20)$ is not hyperelliptic (1.7).

$n = 6$: The modular curve $X_0(30)$ has the hyperelliptic involution w_{15}: $(F, B) \mapsto (F/B_{15}, (B + F_{15})/B_{15})$, where B_{15} is the subgroup of B of order 15. Let $\mathfrak{p}$ be a prime of k lying over the rational prime 3 and put $R = (\mathcal{O}_k)_{(\mathfrak{p})}$. Then $(\boldsymbol{Z}/10\boldsymbol{Z})_{/R} \subset E_{/R}$ and $E_{/R}$ is semistable (1.12). If 3 is unramified in k, then $(\boldsymbol{Z}/30\boldsymbol{Z})_{/R} \subset E_{/R}$. Then $E_{/R}$ has multiplicative reduction and $(\boldsymbol{Z}/3\boldsymbol{Z})_{/R} \otimes \kappa(\mathfrak{p})$ is not contained in the connected component of the special

$E_{/R}\otimes\kappa(p)$ of the unit section (see (1.11), (1.12)). If 3 ramifies in k, then $E_{/R}$ has also mutliplicative reduction and $(\boldsymbol{Z}/5\boldsymbol{Z})_{/R}\otimes\kappa(p)$ is not containted in the connected component of $E_{/R}\otimes\kappa(p)$ of the unit section (see loc. cit.). Denote also by x, x^σ the images of x and x^σ under the natural morphism $X_1(30)\to X_0(30)$. Then $x\otimes\kappa(p) = C\otimes\kappa(p)$, $x^\sigma\otimes\kappa(p) = C_\sigma\otimes\kappa(p)$ for $\boldsymbol{Q}$-fibre rational cusps C and C_σ. These cusps C, C_σ are represented by $(\boldsymbol{G}_m\times\boldsymbol{Z}/qm_\sigma\boldsymbol{Z}, H_\sigma)$ and $(\boldsymbol{G}_m\times\boldsymbol{Z}/qm_\sigma\boldsymbol{Z}, H_\sigma)$ for integers $m, m_\sigma\geqq 1$ and cyclic subgroups H, H_σ containing $\{1\}\times m\boldsymbol{Z}/qm\boldsymbol{Z}$ and $\{1\}\times m_\sigma\boldsymbol{Z}/qm_\sigma\boldsymbol{Z}$ for $q=3$ or 5, respectively. Let $i(x) = cl((x)+(x^\sigma)-(C)-(C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J_0(30)_{/\boldsymbol{Z}}$. Since $\sharp J_0(30)(\boldsymbol{Q})<\infty$ (1.4), $i(x)=0$ (1.13) and $(x)+(x^\sigma)\sim(C)+(C_\sigma)$. It yields $w_{15}(C)=C_\sigma$. But as noted as above, $w_{15}(C)\neq C_\sigma$.

$n=9$: Let p be a prime of k lying over the rational prime 5 and put $R=(\mathcal{O}_k)_{(p)}$. Then $(\boldsymbol{Z}/45\boldsymbol{Z})_{/R}\subset E_{/R}$ and $x\otimes\kappa(p) = C\otimes\kappa(p)$, $x^\sigma\otimes\kappa(p) = C_\sigma\otimes\kappa(p)$ for 0-cusps C and C_σ (1.11), (1.12). Denote also by x, x^σ, C and C_σ the images of x, x^σ, C and C_σ under the natural morphism $X_1(45)\to X_0(45)$. Let $i(x) = cl((x)+(x^\sigma)-(C)-(C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J_0(45)_{/\boldsymbol{Z}}$. Since $\sharp J_0(45)_{/\boldsymbol{Z}})(\boldsymbol{Q})<\infty$ (1.4), $i(x)=0$ (1.13). But $X_0(45)$ is not hyperelliptic [25].

Case $N=3n$ *for* $n=8$ *and* 12:

$n=8$: Let X be the subcovering as in (1.3):

$$X_1(24)\xrightarrow{\pi_1} X\xrightarrow{\pi_X} X_0(24),$$

which corresponds to the subgroup $\Delta=\{\pm1\}\times(\boldsymbol{Z}/3\boldsymbol{Z})^\times$. Let p be a prime of k lying over the rational prime 3 and put $R=(\mathcal{O}_k)_{(p)}$. Then $(\boldsymbol{Z}/8\boldsymbol{Z})_{/R}\subset E_{/R}$ and $E_{/R}$ is semistable (1.12). If 3 is unramified in k, then $(\boldsymbol{Z}/24\boldsymbol{Z})_{/R}\subset E_{/R}$ (1.11) and $E_{/R}$ has multiplicative reduction (1.12). If 3 ramifies in k, then p is of degree one, so $E_{/R}$ has also multiplicative reduction (see loc. cit.). Denote also by x, x^σ the images of x and x^σ by the natural morphism $\pi\colon X_1(24)\to X$. If p is of degree one, then $x\otimes\kappa(p) = C\otimes\kappa(p)$, $x^\sigma\otimes\kappa(p) = C_\sigma\otimes\kappa(p)$ for $\boldsymbol{Q}$-rational cusps C and C_σ. Any cusp on X is defined over $\boldsymbol{Q}$ or $\boldsymbol{Q}(\sqrt{2})$. If p is of degree two, then $x\otimes\kappa(p) = C\otimes\kappa(p)$ for a $\boldsymbol{Q}(\sqrt{2})$-rational cusp C. Then $x^\sigma\otimes\kappa(p) = C_\sigma\otimes\kappa(p)$ for $C_\sigma = C^\tau$ and $1\neq\tau\in\mathrm{Gal}(\boldsymbol{Q}\sqrt{2})/\boldsymbol{Q})$, since $\left(\frac{2}{3}\right)=-1$. Let $i(x)=cl((x)+(x^\sigma)-(C)-(C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J(X)_{/\boldsymbol{Z}}$. Since $\sharp J(X)(\boldsymbol{Q})<\infty$ (1.4) (1.5), $i(x)=0$ (1.13). But X is not hyperelliptic (1.7).

$n=12$: Let p be a prime of k lying over the rational prime 5 and put

$R = (\mathcal{O}_k)_{(p)}$. Then $(\boldsymbol{Z}/36\boldsymbol{Z})_{/R} \subset E_{/R}$ and $E_{/R}$ is semistable (1.12). If $E_{/R}$ has good reduction, then $\sharp E_{/R}(\boldsymbol{F}_{25}) = 1 + 25 - (-10)$ (, since $\boldsymbol{Z}/36\boldsymbol{Z} \subset E_{/R}(\boldsymbol{F}_{25})$ and $\sharp E_{/R}(\boldsymbol{F}_{25}) \leqq 36$). But then the Frobenius map $F = F_{25}$: $E_{/R} \otimes \boldsymbol{F}_{25} \to E_{/R} \otimes \boldsymbol{F}_{25}$ does not act trivially on $E_{/R}(\boldsymbol{F}_{25}) \hookleftarrow \boldsymbol{Z}/36\boldsymbol{Z}$. Hence $E_{/R}$ has multiplicative reduction. Let T be the connected component of $E_{/R} \otimes \kappa(p)$ of the unit section. Then $\boldsymbol{Z}/9\boldsymbol{Z} \not\subset T(\boldsymbol{F}_{25})$. Denote also by x, x^σ the images of x and x^σ under the natural morphism $X_1(36) \to X_1(18)$. Then $x \otimes \kappa(p) = C \otimes \kappa(p)$, $x^\sigma \otimes \kappa(p) = C_\sigma \otimes \kappa(p)$ for $\boldsymbol{Q}$-rational cusps C and C_σ on $X_1(18)$ (see above). The modular curve $X_1(18)$ has the hyperelliptic involution $w_2[5]$ (1.6):

$$(F, B_2, \pm Q_9) \longmapsto (F/B_2, F_2/B_2, \pm 5Q_9 \bmod B_2),$$

where B_2 is a subgroup of order 2 and Q_9 is a point of order 9. Let $i(x) = cl((x) + (x^\sigma) - (C) - (C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J_1(18)_{/\boldsymbol{Z}}$. Since $\sharp J_1(18)(\boldsymbol{Q}) < \infty$ (1.4), $i(x) = 0$ (1.13) and $x^\sigma = w_2[5](x)$. For a k-rational point $Q \in \langle P\rangle$ of order 18, the pairs $(E, \pm Q)$, $(E^\sigma, \pm Q^\sigma)$ represent x and x^σ on $X_1(18)$. Put $A_2 = \langle 9Q\rangle$. Then there is a quadratic extension K of k over which

$$\lambda\colon (E^\sigma, \pm Q^\sigma) \xrightarrow{\sim} (E/A_2, \pm(Q_2' + 5Q) \bmod A_2),$$

where Q_2' is a point of order 2 not contained in A_2. For $1 \neq \tau \in \mathrm{Gal}(K/k)$, $\lambda^\tau = \pm\lambda$, since $x \otimes \kappa(p)$ is a cusp. Then $\lambda(Q^\sigma) = \varepsilon(Q_2' + 5Q) \bmod \mathrm{A}_2$ for $\varepsilon = \pm 1$. The points Q^σ and $\lambda(Q^\sigma)$ are k-rational, so $\lambda^\tau(Q^\sigma) = (\lambda(Q^{\sigma\tau}))^\tau = \lambda(Q^\sigma)$. Therefore $\lambda^\tau = \lambda$ and λ is defined over k. Since E/A_2 contains $E_2/A_2 \oplus \langle 9P\rangle/A_2 (\simeq \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z})$, $E^\sigma(k) \supset \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/36\boldsymbol{Z}$. Let $X_0(2, 36)$ be the modular curve $/\boldsymbol{Q}$ corresponding to $\Gamma_0(2, 36)$. Then E and E^σ (with level structures) define k-rational points y and y^σ on $X_0(2, 36)$ such that $y \otimes \kappa(p) = D \otimes \kappa(p)$, $y^\sigma \otimes \kappa(p) = D_\sigma \otimes \kappa(p)$ for $\boldsymbol{Q}$-rational cusps D and D_σ. Let $i(y) = cl((y) + (y^\sigma) - (D) - (D_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J_0(2, 36)_{/\boldsymbol{Z}}$. Then $i(y) = 0$, since $\sharp J_0(2, 36)(\boldsymbol{Q}) < \infty$ (1.4) (1.13). But $X_0(2, 36)$ is not hyperelliptic [25]. ■

Now we discuss the k-rational points on $X_1(N)$ for $N = 14, 15$ and 18. The modular curves $X_1(14)$ and $X_1(15)$ are elliptic curves, and $X_1(18)$ is hyperelliptic of genus 2. We here give examples of quadratic fields k such that $Y_1(N)(k) = \phi$ for each integer N as above.

PROPOSITION (2.4). *Let k be a quadratic field. If one of the following conditions* (i), (ii) *and* (iii) *is satisfied, then* $Y_1(18)(k) = \phi$:

https://doi.org/10.1017/S0027763000002816 Published online by Cambridge University Press

(i) *The rational prime* 3 *remains prime in* k.
(ii) 3 *splits in* k *and* 2 *does not split in* k.
(iii) 5 *or* 7 *ramifies in* k.

Proof. Let x be a k-rational point on $Y_1(18)$. Then x is represented by an elliptic curve E defined over k with a k-rational point P of order 18 [4] VI (32.). Let $p = 2, 3, 5$ or 7, and put $R = (\mathcal{O}_k)_{(\mathfrak{p})}$ for a prime $\mathfrak{p}$ of k lying over p. Then $(\boldsymbol{Z}/18\boldsymbol{Z})_{/R} \subset E_{/R}$ if $p = 5$ or 7, $(\boldsymbol{Z}/9\boldsymbol{Z})_{/R} \subset E_{/R}$ if $p = 2$ and $(\boldsymbol{Z}/18\boldsymbol{Z})_{/R} \subset E_{/R}$ if $p = 3$ is unramified in k (1.11).

Case (*i*) *and* (ii): The same argument as in the proof for $N = 36$ shows that $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$, $x^\sigma \otimes \kappa(\mathfrak{p}) = C_\sigma \otimes \kappa(\mathfrak{p})$ for $\boldsymbol{Q}$-rational cusps C and C_σ and for a prime $\mathfrak{p}$ of k lying over $p = 3$. Using the $\boldsymbol{Q}$-rational section $i(x) = cl((x) + (x^\sigma) - (C) - (C_\sigma))$ of $J_1(18)_{/\boldsymbol{Z}}$, we see that $w_2[5](C) = C_\sigma$. If 3 remains prime in k, then $C_\sigma \otimes \boldsymbol{F}_9 = x^\sigma \otimes \boldsymbol{F}_9 = (x \otimes \boldsymbol{F}_9)^{(3)} = C \otimes \boldsymbol{F}_9$. But $C \otimes \boldsymbol{F}_9$ is not a fixed point of the hyperelliptic involution $w_2[5]$. In the case (ii), the same argument as above shows that $C \otimes \boldsymbol{F}_4 = C_\sigma \otimes \boldsymbol{F}_4$. But $C \otimes \boldsymbol{F}_4$ is not a fixed point of $w_2[5]$.

Case (iii): Under the assumption that $p = 5$ or 7 ramifies in k, the same argument as above gives the result. ∎

Example (2.5). (1) $Y_1(14)(k) = \phi$ for $k = \boldsymbol{Q}(\sqrt{-3})$ and $\boldsymbol{Q}(\sqrt{-7})$.
(2) $Y_1(15)(\boldsymbol{Q}(\sqrt{5})) = \phi$.

Proof. For $N = 14$ and 15, $X_0(N)$ are elliptic curves with finite Mordell-Weil groups [36] table 1. The restriction of scalars [5] [34] $\mathrm{Re}_{\boldsymbol{Q}(\sqrt{-3})/\boldsymbol{Q}}(X^0(14)_{/\boldsymbol{Q}(\sqrt{-3})})$, $\mathrm{Re}_{/\boldsymbol{Q}(\sqrt{-7})/\boldsymbol{Q}}(X_0(14)_{/\boldsymbol{Q}(\sqrt{-7})})$ and $\mathrm{Re}_{\boldsymbol{Q}(\sqrt{5})/\boldsymbol{Q}}(X_0(15)_{/\boldsymbol{Q}(\sqrt{5})})$ are isogenous over $\boldsymbol{Q}$ (respectively) to products $X_0(14) \times E_{126}$, $X_0(14) \times E_{98}$ and $X_0(15) \times E_{75}$ for elliptic curves E_n with conductor n (1.15). These E_n have the Mordell-Weil groups of finite order [36] table 1. Therefore $\sharp X_0(N)(k) < \infty$ for (N, k) as above. Let x be a k-rational point on $X_1(N)$ and denote also by x the image of x under natural morphism $X_1(N) \to X_0(N)$ for (N, k) as above. Then $x \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$ for a $\boldsymbol{Q}$-rational cusp C on $X_0(N)$ and for a prime $\mathfrak{p}$ of k lying over $p = 7$ if $N = 14$, and $p = 5$ if $N = 15$ (1.11) (1.12). Then the specialization Lemma (1.11) yields that $x = C$. ∎

§ 3. Rational points on $X_1(m, N)$

Let N be an integer of a product of powers of 2, 3, 5, 7, 11 and 13, and $m \neq 1$ be a positive divisor of N. Let k be a quadratic field. In this section, we discuss the k-rational points on $X_1(m, N)$. For $(m, N) = (2, 2)$, $(2, 4)$, $(2, 6)$, $(2, 8)$; $(3, 3)$, $(3, 6)$; $(4, 4)$, $X_1(m, N) \simeq \boldsymbol{P}^1$. For $(m, N) = (2, 10)$ and $(2, 12)$, $X_1(m, N)$ are elliptic curves. For the other pairs (m, N) as above, $X_1(m, N)$ are not hyperelliptic [7]. We first discuss the k-rational points on $Y_1(m, N)$ for the pairs (m, N) such that $X_1(m, N)$ are not hyperelliptic. It suffices to treat the cases for the pairs (m, N): $m = 2$, $N = 10$, 12, 14, 16, 18; $m = 3$ ($k = \boldsymbol{Q}(\sqrt{-3})$), $N = 9$, 12, 15; $m = 4$ ($k = \boldsymbol{Q}(\sqrt{-1})$), $N = 8, 12$; $m = 6$ ($k = \boldsymbol{Q}(\sqrt{-3})$), $N = 6$. Let x be a k-rational point on $Y_1(m, N)$. Then there exists an elliptic curve E defined over k with a pair (P_m, P_N) or k-rational points P_m and P_N such that $\langle P_m \rangle + \langle P_N \rangle \simeq \boldsymbol{Z}/m\boldsymbol{Z} \times \boldsymbol{Z}/N\boldsymbol{Z}$ and that the isomorphism class containing the pair $(E, \pm(P_m, P_N))$ represents x [4] VI (3.2). For $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$, x^σ is represented by the pair $(E^\sigma, \pm(P_m^\sigma, P_N^\sigma))$.

THEOREM (3.1). *Let (m, N) be a pair as above and k be any quadratic field. If $X_1(m, N)$ is not hyperelliptic (i.e., $X_1(m, N) \not\simeq \boldsymbol{P}^1$ nor $(m, N) \neq (2, 10)$, $(2, 12)$), then $Y_1(m, N)(k) = \phi$.*

Proof. Let $J_1(m, N)$ and $J_0(m, N)$ be the jacobian varieties of the modular curves $X_1(m, N)$ and $X_0(m, N) \simeq X_0(mN)$, respectively, and π: $X_1(m, N) \to X_0(m, N)$ be the natural morphism. Suppose that there is a k-rational point x on $Y_1(m, N)$. Let E be an elliptic curve defined over k with k-rational points P_m and P_N such that the pair $(E, \pm(P_m, P_N))$ represents x.

Case $m = 6$ ($N = 6$): Let $\mathfrak{p}$ be a prime of $k = \boldsymbol{Q}(\sqrt{-3})$ lying over the rational prime 7 and put $R = (\mathcal{O}_k)_{(\mathfrak{p})}$. Then $(\boldsymbol{Z}/6\boldsymbol{Z})_{/R} \times (\boldsymbol{Z}/6\boldsymbol{Z})_{/R} \subset E_{/R}$ (1.12), so that $\pi(x) \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$ for a $\boldsymbol{Q}(\sqrt{-3})$-rational cusp C. The modular curve $X_0(6, 6)$ is an elliptic curve and the restriction of scalars $\mathrm{Re}_{\boldsymbol{Q}(\sqrt{-3})/\boldsymbol{Q}}(X_0(6, 6)_{/\boldsymbol{Q}(\sqrt{-3})})$ [5] [34] is isogenous over $\boldsymbol{Q}$ to the product $X_0(6, 6) \times X_0(6, 6)$. Since $\sharp X_0(6, 6)(\boldsymbol{Q}) < \infty$ [36] table 1, we see that $\sharp X_0(6, 6)(\boldsymbol{Q}(\sqrt{-3})) < \infty$. Then $\pi(x) = C$ (1,11), which is a contradiction.

Case $m = 4$ ($N = 8, 12$): In both cases for $N = 8$ and 12, $\pi(x) \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$ for a prime $\mathfrak{p}$ of $k = \boldsymbol{Q}(\sqrt{-1})$ lying over the rational prime 5 and for k-rational cusps C (1.12). Let π': $X_0(4, 12) \to X_0(2, 12)$ be the natural morphism. The modular curves $X_0(4, 8)$ and $X_0(2, 12)$ are elliptic curves and $\sharp X_0(4, 8)(\boldsymbol{Q}(\sqrt{-1}))$, $\sharp X_0(2, 12)(\boldsymbol{Q}(\sqrt{-1}))$ are finite (1.15) [36] table 1. Then the same argument as in the proof for $m = 6$ gives a contradiction.

Case $m=3$ ($N=9, 12, 5$): In all the cases for $N=9, 12$ and 15, $\pi(x)\otimes\kappa(p)=C\otimes\kappa(p)$ for a prime p of $k=\boldsymbol{Q}(\sqrt{-3})$ lying over the rational prime 7 and for k-rational cusps C (1.12). The modular curves $X_0(3, 9)$ and $X_0(3, 12)$ are elliptic curves $/\boldsymbol{Q}$ with complex multiplication $/\boldsymbol{Q}(\sqrt{-3})$, so the restriction of scalars $\mathrm{Re}_{\boldsymbol{Q}(\sqrt{-3})/\boldsymbol{Q}}(X_0(3, N)_{/\boldsymbol{Q}(\sqrt{-3})})$ ($N=9, 12$) are isogenous over $\boldsymbol{Q}$ to the products $X_0(3, N)\times X_0(3, N)$. Further $\mathrm{Re}_{\boldsymbol{Q}(\sqrt{-3})/\boldsymbol{Q}}(X_0(45)_{/\boldsymbol{Q}(\sqrt{-3})})$ is isogenous over $\boldsymbol{Q}$ to a product $X_0(45)$ and an elliptic curve with conductor 15 (1.15) [36] table 1. Then $\sharp X_0(3N)(\boldsymbol{Q}(\sqrt{-3}))<\infty$ for $N=9, 12$ and 15 [36] table 1. The same argument as above gives contradictions.

Case $m=2$ ($N=14, 16, 18$):

$N=14$: The modular curve $X_0(2, 14)\simeq X_0(28)$ has the hyperelliptic involution w_7 (see [36] table 5). Let p be a prime of k lying over the rational prime 3. Then $\pi(x)\otimes\kappa(p)=C\otimes\kappa(p)$, $\pi(x^\sigma)\otimes\kappa(p)=C_\sigma\otimes\kappa(p)$ for $\boldsymbol{Q}$-rational cusps C and C_σ. These cusps C, C_σ are represented by $(\boldsymbol{G}_m\times \boldsymbol{Z}/14\boldsymbol{Z}, A_2, A_{14})$ and $(\boldsymbol{G}_m\times\boldsymbol{Z}/14\boldsymbol{Z}, B_2, B_{14})$ such that $A_{14}\supset\{1\}\times 2\boldsymbol{Z}/14\boldsymbol{Z}$ and $B_{14}\supset\{1\}\times 2\boldsymbol{Z}/14\boldsymbol{Z}$ (1.12). Let $i(x)=cl((x)+(x^\sigma)-(C)-(C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J_0(2, 14)_{/\boldsymbol{Z}}$. Then $i(x)=0$ and $^?(x)+(x^\sigma)\sim(C)+(C_\sigma)$, since $\sharp J_0(2, 14)(\boldsymbol{Q})<\infty$ (1.4) (1.13). But as noted as above, $w_7(C)\neq C_\sigma$.

$N=16$: Let γ be a generator of the covering group of $X_1(32)\to X_0(32)$. Then $Y=X_1(32)/\langle\gamma^4\rangle\simeq X_1(2, 16)$ and $\sharp J(Y)(\boldsymbol{Q})<\infty$ (1.4). Let p be a prime of k lying over the rational prime 3. Then $x\otimes\kappa(p)=C\otimes\kappa(p)$, $x^\sigma\otimes\kappa(p)=C_\sigma\otimes\kappa(p)$ for $\boldsymbol{Q}$-rational cusps C and C_σ (1.12). Considering the $\boldsymbol{Q}$-rational section $i(x)=cl((x)+(x^\sigma)-(C)-(C_\sigma))$ of $J_1(2, 16)_{/\boldsymbol{Z}}$, we get the relation $(x)+(x^\sigma)\sim(C)+(C_\sigma)$. But $X_1(2, 16)$ is not hyperelliptic 1(1.7).

$N=18$: Let p be a prime of k lying over the rational prime 5 and put $R=(\mathcal{O}_k)_{(p)}$. By the condition $\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/18\boldsymbol{Z}\subset E(k)$, $E_{/R}\otimes\kappa(p)=\boldsymbol{G}_m\times\boldsymbol{Z}/18n\boldsymbol{Z}$ for an integer $n\geqq 1$ (1.12). Then $x\otimes\kappa(p)=C\otimes\kappa(p)$, $x^\sigma\otimes\kappa(p)=C_\sigma\otimes\kappa(p)$ for $\boldsymbol{Q}$-rational cusps C and C_σ. These cusps C and C_σ are represented respectively by $(\boldsymbol{G}_m\times\boldsymbol{Z}/18\boldsymbol{Z}, P_2, \pm P_{18})$, $(\boldsymbol{G}_m\times\boldsymbol{Z}/18\boldsymbol{Z}, Q_2, \pm Q_{18})$, where P_n, Q_n are points of order n such that $P_{18}, Q_{18}\in\mu_2\times\boldsymbol{Z}/18\boldsymbol{Z}$ (see loc. cit.). Denote also by x, x^σ, C and C_σ the images of x, x^σ, C and C_σ under the natural morphism of $X_1(2, 18)$ to $X_1(18)$:

$$(F, B_2, \pm B_{18})\longmapsto(F, \pm B_{18})\,.$$

Let $i(x)=cl((x)+(x^\sigma)-(C)-(C_\sigma))$ be the $\boldsymbol{Q}$-rational section of $J_1(18)_{/\boldsymbol{Z}}$.

Since $\sharp J_1(18)(\boldsymbol{Q}) < \infty$ (1.4), $i(x) = 0$ and $(x) + (x^\sigma) \sim (C) + (C_\sigma)$. The modular curve $X_1(18)$ has the hyperelliptic involution $\gamma = w_2[5]$:

$$(F, \pm Q_{18}) \longmapsto (F/\langle Q_2 \rangle, \pm(Q_2' + 5Q_{18}) \bmod \langle Q_2 \rangle),$$

where Q_2, Q_2' are points of order 2 with $Q_2 \in \langle Q_{18} \rangle$ and $Q_2' \notin \langle Q_{18} \rangle$. Then $x^\sigma = \lambda(x)$, so there exists an isomorphism $\lambda\,(/C)$

$$\lambda\colon (E^\sigma, \pm P_{18}^\sigma) \xrightarrow{\sim} (E/\langle 9P_{18} \rangle, \pm(P' + 5P_{18}) \bmod \langle 9P_{18} \rangle),$$

where P' is a point of order 2 not contained in $\langle P_{18} \rangle$. Since $x \otimes \kappa(\mathfrak{p})$ is a cusp, λ is defined over a quadratic extension K of k and $\lambda^\tau = \pm\lambda$ for $1 \neq \tau \in \mathrm{Gal}(K/k)$. Then $\lambda(P_{18}^\sigma) = \varepsilon(P' + 5P_{18}) \bmod \langle 9P_{18} \rangle$ for $\varepsilon = \pm 1$, and it is k-rational. Noting that all the 2-torsion points on E are defined over k, we see that $\lambda^\tau(P_{18}^\sigma) = (\lambda(P_{18}^{\sigma\tau}))^\tau = (\lambda(P_{18}^\sigma))^\tau = \lambda(P_{18}^\tau)$, Thus $\lambda^\tau = \lambda$ and λ is defined over k. Then λ induces the isomorphism

$$\lambda\colon (E^\sigma, P_2^\sigma, P_{18}^\sigma) \xrightarrow{\sim} (E/\langle 9P_{18} \rangle, \lambda(P_2^\sigma), \varepsilon(P' + 5P_{18}^\sigma) \bmod \langle 9P_{18} \rangle).$$

Let $\mu\colon E \to E/\langle 9P_{18} \rangle$ be the natural morphism and put $B = \lambda^{-1}\{0, \lambda(P_2^\sigma)\}$. Then $B \neq E_2$, so that B is a cyclic subgroup of order 4 defined over k. Put $A' = \langle P' + 2P_{18} \rangle$ and let y, y^σ be the k-rational points on $X_0(4, 18) \simeq X_0(72)$ represented by the triples (E, B, A') and $(E^\sigma, B^\sigma, A'^\sigma)$, respectively. Noting that $B \not\ni P'$ and $B \in 9P_{18}$, we see that $y \otimes \kappa(\mathfrak{p}) = C' \otimes \kappa(\mathfrak{p})$ and $y^\sigma \otimes \kappa(\mathfrak{p}) = C_\sigma' \otimes \kappa(\mathfrak{p})$ for $\boldsymbol{Q}$-rational cusps C and C_σ (1.12). The remaining part of the proof is the same as that for the case $X_1(36)$. ■

In the rest of this section, we give examples of quadratic fields k such that $Y_1(2, N)(k) = \phi$ for $N = 10$ and 12.

EXAMPLE (3.2). For $N = 10$ and 12, $X_1(2, N)$ are elliptic curves. Let $\mathfrak{p}$ be a prime of k lying over the rational prime 3. Then for a k-rational point x on $X_1(2, N)$ $(N = 10, 12)$, $\pi(x) \otimes \kappa(\mathfrak{p}) = C \otimes \kappa(\mathfrak{p})$ for a $\boldsymbol{Q}$-rational cusp C (1.12), where $\pi\colon X_1(2, N) \to X_0(2, N)$ is the natural morphism. Set an assumption: $\sharp J_0(2, N)(k) < \infty$, and the rational prime 3 is unramified in k or $3 \nmid \sharp J_0(2, N)(k)$. Under this assumption, the same argument as in the proof for $m = 6,4$ and 3 (in (3.1)) shows that $Y_1(2, N)(k) = \phi$. For example, $\sharp J_0(2, 10)(\boldsymbol{Q}(\sqrt{-1})) < \infty$, $\sharp J_0(2, 12)(\boldsymbol{Q}(\sqrt{-3})) < \infty$ and $3 \nmid \sharp J_0(2, 12)(\boldsymbol{Q}(\sqrt{-3}))$ (1.15) [36] table 1, 3, 5.

References

[1] N. Authaud, On Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication, Compositio Math., **37**, 2 (1978), 209–232.

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

[3] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton Dyer, Invent. Math., **39** (1977), 223–251.

[4] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptique, Proceedings of the International Summer School on Modular functions of one variable, vol. II, Lecture Notes in Math., **349**, Springer-Verlag, Berlin-Heidelberg-New York (1973).

[5] A. Grothendieck, Fondements de la géométrie algébrique, Sèm. Bourbaki, 1957–1962.

[6] H. Hasse, Über die Klassenzahl Abelscher ZahlKörper (1952), Akademie-Verlag GmbH., Berlin.

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

[8] M. A. Kenku, Certain torsion points on elliptic curves defined over quadratic fields, J. London Math. Soc. (2) **19** (1979), 233–240.

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

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

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

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

[13] ——, Rational torsion points on elliptic curves defined over quadratic fields, to appear.

[14] D. Kubert, Universal bounds on the torsion points of elliptic curves, Proc. London Math. Soc. (3), **33** (1976), 193–237.

[15] Yu. I. Manin, The p-torsion of elliptic curves is uniformally bounded, Math. USSR-Izvestija, **3** (1969), 433–438.

[16] ——, Parabolic points and zeta-functions of modular curves, Math. USSR-Izvestija, **6** (1972), 19–64.

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

[18] ——, Rational isogenies of prime degree, Invent. Math., **44** (1978), 129–162.

[19] B. Mazur and J. Tate, Points of order 13 on elliptic curves, Invent. Math., **22** (1973), 41–49.

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

[21] J. S. Milne, On the arithmetic of abelian varieties, Invent. Math., **17** (1972), 177–190.

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

[23] ——, p-torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J., **96** (1984), 139–165.

[24] A. Ogg, Rational points on certain elliptic modular curves, Proc. Symposia in Pure Math. XXIX, AMS, (1973) 221–231.

[25] ——, Hyperelliptic modular curves, Bull. Soc. Math. France, **102** (1974), 449–462.
[26] ——, Diophantine equations and modular forms, Bull. AMS, **81** (1975), 14–27.
[27] F. Oort and J. Tate, Group schemes of prime order, Ann. Scient. Ec. Norm. Sup. serie 4, **3** (1970), 1–21.
[28] M. Raynaud, Schémas en groupes de type $(p, \cdots, p)$, Bull. Soc. Math. France, **102** (1974), 241–280.
[29] K. Rubin, Congruences for special values of L-functions of elliptic curves with complex multiplication, Invent. Math., **71** (1983), 339–364.
[30] J. P. Serre, Propriétés galoissiennes des points d'ordre fini des courbes elliptiques, Invent. Math., **15** (1972), 259–331.
[31] ——, p-torsion des courbes elliptiques (d'après Y. Manin), Sèm. Boubaki 1969/70, 281–294, Lecture Notes in Math. 180, Springer-Verlag, Berlin-Heidelberg-New York (1971).
[32] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan 11, Iwanami Shoten, Tokyo-Princeton Univ. Press, Princeton, N.J.
[33] ——, On elliptic curves with complex multiplication as factors of the jacobians of modular function fields, Nagoya Math. J., **43** (1971), 199–208.
[34] A. Weil, Adèles and algebraic groups, Lecture Notes, Inst. for Advanced Study, Princeton, N.J.
[35] J. Yu, A cuspidal class number formula for the modular curves $X_1(N)$, Math. Ann., **252** (1980), 197–216.
[36] Modular functions of one variable IV (ed. by B. J. Birch and W. Kuyk), Lecture Notes in Math., **476**, Springer-Verlag, Berlin-Heidelberg-New York (1975).

M. A. Kenku
Department of Mathematics
Faculty of Science
University of Lagos
Lagos, Nigeria

F. Momose
Department of Mathematics
Chuo University
1-13-27 Kasuga, Bunkyo-ku
Tokyo 112, Japan

https://doi.org/10.1017/S0027763000002816 Published online by Cambridge University Press