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

$$E_p^n(k) = \bigcup_{m \geq 0} \ker (p^m): E \to E(k) \subseteq E_p^n$$

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 $p \geq 17$ as above (see loc. cit.). It seems that $n(k, p) = 0$ for all prime numbers $p \geq 17$ 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 $N \geq 1$ be an integer and $m$ a positive divisor of $N$. Let $X_i(m, N)$ be the modular curve which corresponds to the finite adèlic modular group

$$\Gamma_i(m, N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \GL_2(\hat{\mathbb{Z}}) | a - 1 \equiv c \equiv 0 \mod N, \ b \equiv d - 1 \equiv 0 \mod m \right\},$$

where $\hat{\mathbb{Z}} = \lim_{n} \mathbb{Z}/n\mathbb{Z}$. Then $X_i(m, N)$ is defined over $\mathbb{Q}(\zeta_m)$, where $\zeta_m$ is a primitive $m$-th root of $1$. Put $Y_i(m, N) = X_i(m, N) \setminus \{\text{cusps}\}$, which is the coarse moduli space ($\mathbb{Q}(\zeta_m)$) 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 $\simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, up to the isomorphism $(-1)_E: E \cong E$. For $m = 1$, let $X_i(N) = X_i(1, N)$, $\Gamma_i(N) = \Gamma_i(1, N)$ and $Y_i(N) = Y_i(1, N)$. For the integers $N = 2^4, 11$ and $13$, $X_i(N)$ 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 $2, 3, 5,$
7, 11 and 13, let m be a positive divisor of \( N \). If \( X_i(m, N) \) is not hyperelliptic (i.e. the genus \( g,(m, N) \neq 0 \) and \((m, N) \neq (1,11), (1,13), (1,14), (1,15), (1,16), (1,18), (2,10) \) nor \((2,12)\)), then \( Y,(m, N)(k) = \phi \) for all quadratic fields \( k \).

For prime numbers \( p \geq 17 \), it seems that \( Y,(p)(k) = \phi \) 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:

\[
\begin{align*}
Z/NZ & \quad \text{for } 1 \leq N \leq 10 \text{ or } N = 12 \\
Z/2Z \times Z/2nZ & \quad \text{for } 1 \leq n \leq 4 \\
Z/3n \times Z/3nZ & \quad \text{for } n = 1 \text{ or } 2 \text{ with } k = Q(\sqrt{-3}) \\
Z/4Z \times Z/4Z & \quad \text{with } k = Q(\sqrt{-1}) \\
or \\
Z/NZ & \quad \text{for } N = 11, 14 \text{ or } 16 \\
Z/NZ & \quad \text{for } N = 18, 16 \text{ or } 18 \\
Z/2Z \times Z/2nZ & \quad \text{for } n = 5 \text{ or } 6 
\end{align*}
\]

For \((m, N) = (1,14), (1,15), (1,18), (2,10) \) and \((2,12)\), we give examples of quadratic fields \( k \) such that \( Y,(m, N)(k) = \phi \) (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 \( Y,(m, N) \) for a pair \((m, N)\) as in (0.1). Then \( x \) defines a rational function \( g \) \((/Q)\) on a subcovering \( X: X,(m, N) \rightarrow X \rightarrow X,(N) \), 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 \( m \geq 2 \).

Notation. For a rational prime \( p \), \( Q_p^{nr} \) denotes the maximal unramified extension of \( Q_p \). Let \( K \) be a finite extension of \( Q, Q_p \) or \( Q_p^{nr} \), and \( A \) an abelian variety defined over \( K \). Then \( \vartheta_K \) denotes the ring of integers of \( K \), and \( A,_{/K} \) denotes the Néron model of \( A \) over the base \( \vartheta_K \). For a finite subgroup \( G \) of \( A \) defined over \( K, \vartheta_K \) denotes the schematic closure of \( G \) in the Néron model \( A,_{/K} \) (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 \( p \), \( Y^{,y} \) denotes the open subscheme \( Y \setminus \{\text{supersingular points on} \}

\[https://doi.org/10.1017/S0027763000002816\text{ Published online by Cambridge University Press} \]
ELLIPTIC CURVES

Y ⊗ F_p. For a finite extension K of Q and for a prime p of K, (O_K)_{(p)} denotes the local ring at 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 ≥ 1 be an integer and m a positive divisor of N. Let X_0(m, N) (resp. X_0(m, N)) be the modular curve (Q(ζ_m)) (resp. Q) which corresponds to the finite adèlic modular group

\[ \Gamma_0(m, N) = \{ (a, b, c, d) \in \text{GL}_2(\hat{\mathbb{Z}}) \mid a - 1 \equiv c \equiv 0 \mod N, \ b \equiv d - 1 \equiv 0 \mod m \}. \]

The modular curve X_0(m, N) is the coarse moduli space Q(ζ_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 \( \sim \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \), up to the isomorphism \((-1)_E: E \approx E \) [4]. Let \( Y_0(m, N), Y_0(m, N) \) denote the open affine subschemes X_0(m, N) \{cusps\} and X_0(m, N) \{cusps\}. For m = 1, let X_0(N) = X_0(1, N), X_0(N) = X_0(1, N), \( \Gamma_0(N) = \Gamma_0(1, N), \Gamma_0(N) = \Gamma_0(1, N), Y_0(N) = Y_0(1, N) \) and \( Y_0(N) = Y_0(1, N) \). Let \( K \) be a subfield of \( C \). For a \( K \)-rational point x on \( Y_0(m, N) \) (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 \( Q \) to X_0(m, N) by

\[ (E, A) \mapsto (E/A_N, A_N/A_N, E/A_N), \]

where \( E_N = \ker(N: E \to E) \) and \( A_N \) is the cyclic subgroup of order \( N \) of \( A \). Let \( \pi = \pi_{m,N} \) be the natural morphism of \( X_0(m, N) \) 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 \( \langle P_N \rangle \) are the cyclic subgroups generated by \( P_m \) and \( P_N \), respectively. Then \( \pi \) is a Galois covering with the Galois group \( \Gamma_0(m, N) = \Gamma_0(1, N) / \pm \Gamma_0(1, N) \approx ((\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/N\mathbb{Z})^\times) / \pm 1 \). For integers \( \alpha, \beta \) prime to \( N \), \( [\alpha, \beta] \) denotes the automorphism of \( X_0(m, N) \) 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

https://doi.org/10.1017/S00277630000002816 Published online by Cambridge University Press
When $\alpha \equiv \beta \mod N$ or $m = 1$, let $[\alpha]$ denote $[\alpha, \beta]$. When $m = 1$, let $\pi_N = \pi_{1, N}$ and $\Gamma_1(N) = \Gamma_0(1, N)$. For a positive divisor $d$ of $N$ prime to $N/d$, let $w_d$ denote the automorphism of $X_0(N)$ defined by

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

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 $\zeta_d$ of 1. ($e_d: E_d \times E_d \to \mu_d$ is the $e_d$-pairing).

For a subcovering $X : X_0(m, N) \to X \to X_0(N)$, 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 $X_0(N) \to X_0(N)$ is unramified at the cusps. Let $X$ denote the normalization of the projective $j$-line $\mathbb{P}^1$ in $X$. For $X = X_0(m, N), X = X_0(m, N), X = X_0(N)$ and $X = X_0(N)$, let $X = X_0(m, N), X = X_0(m, N), X = X_0(N)$ and $X = X_0(N)$. Then $X \otimes Z[1/N] \to \text{Spec } Z[1/N]$ is smooth [4] VI (6.7).

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

(1.2) Let $A \subset (Z/NZ)^\times$ be a subgroup containing $\pm 1$ and $X = X_A$ be the modular curve ($/Q$) corresponding to the modular group

$$\Gamma_A = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma_0(N) | (a \text{ mod } N) \in A \right\}.$$ 

Then $X_A$ is the subcovering of $X_0(N) \to X_0(N)$ associated with the subgroup $A$. For a prime divisor $p$ of $N$, let $Z'$ (resp. $Z$) be the irreducible component of the special fibre $X_0(N) \otimes F_p$ such that $Z'^h = Z' \setminus \{\text{supersingular points on } X_0(N) \otimes F_p\}$ (resp. $Z^h$) is the coarse moduli space ($/F_p$) of the
isomorphism classes of the generalized elliptic curves $E$ with a cyclic subgroup $A$, $A \simeq \mathbb{Z}/N\mathbb{Z}$ (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 $p \mid d$, then $w_d$ exchanges $Z'$ with $Z$. If $p \nmid d$, then $w_d$ fixes $Z'$ and $Z$. Let $Z'_X$ be the fibre $X \times_{\mathbb{Z}/(N)} Z'$. Then $Z'_X$ is smooth over $F_p$ and the 0-cusps $(\otimes F_p)$ are the sections of $Z'_X$. If $p \mid |N$ and $\Delta$ contains the subgroup

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

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

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

<table>
<thead>
<tr>
<th>$m$</th>
<th>$N$</th>
<th>$X$</th>
<th>$\Delta$</th>
<th>genus of $X$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14</td>
<td>$X = X_i(14) \xrightarrow{3} X_i(14)$</td>
<td>${\pm 1}$</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>15</td>
<td>$X = X_i(15) \xrightarrow{4} X_i(15)$</td>
<td>${\pm 1}$</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>18</td>
<td>$X = X_i(18) \xrightarrow{3} X_i(18)$</td>
<td>${\pm 1}$</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>20</td>
<td>$X = X_i(20) \xrightarrow{4} X_i(20)$</td>
<td>${\pm 1}$</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>21</td>
<td>$X_i(21) \xrightarrow{2} X \xrightarrow{3} X_i(21)$</td>
<td>$(\mathbb{Z}/3\mathbb{Z})^\times \times {\pm 1}$</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>24</td>
<td>$X_i(24) \xrightarrow{2} X \xrightarrow{2} X_i(24)$</td>
<td>$(\mathbb{Z}/3\mathbb{Z})^\times \times {\pm 1}$</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>35</td>
<td>$X_i(35) \xrightarrow{4} X \xrightarrow{3} X_i(35)$</td>
<td>$(\mathbb{Z}/5\mathbb{Z})^\times \times {\pm 1}$</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>55</td>
<td>$X_i(55) \xrightarrow{10} X \xrightarrow{2} X_i(55)$</td>
<td>${\pm 1} \times (\mathbb{Z}/11\mathbb{Z})^\times$</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>$X_i(32) \xrightarrow{2} X = X_i(2, 16) \xrightarrow{8} X_i(32)$</td>
<td>${\pm (1 + 16)}$</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>$X_i(20) \xrightarrow{2} X = X_i(2, 10) \xrightarrow{2} X_i(20)$</td>
<td>${\pm 1} \times {\pm 1}$</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>$X_i(24) \xrightarrow{2} X = X_i(2, 12) \xrightarrow{2} X_i(24)$</td>
<td>${\pm 1} \times {\pm 1}$</td>
<td>1</td>
</tr>
</tbody>
</table>

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

Let $J_i(m, N)$ and $J_0(m, N)$ be the jacobian varieties of $X_i(m, N)$ and $X_0(m, N)$, respectively. For $m = 1$, $J_i(1, N) = J_i(N)$ 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 $J_i(N)$ 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/10.1017/50027763000002816 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 \( J_i(2,10) \) and \( J_i(2,12) \) are elliptic curves with finite Mordell-Weil groups ([36] table 1). Let \( \text{Coker} \ (J_\ell(N) \to J(X)) \) be the cokernels of the morphisms as the Picard varieties. In the following table, the factors \( A (/\mathbb{Q}) \) of \( J(X) \) have finite Mordell-Weil groups ([36] table 1, 5, [8] [14] [19], (1.5) below).

<table>
<thead>
<tr>
<th>( N )</th>
<th>factor ( A ) of ( J(X) ) or ( A = J_\ell(N) )</th>
<th>( \text{dim} \ A )</th>
<th>genus of ( X_\ell(N) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>( J_\ell(22) )</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>33</td>
<td>( J_\ell(33) )</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>55</td>
<td>( \text{Coker} \ (J_\ell(55) \to J(X)) )</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>77</td>
<td>( J_\ell(77)/(1 + w_1)J_\ell(77) )</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>14</td>
<td>( J_\ell(14) )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>( \text{Coker} \ (J_\ell(21) \to J(X)) )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>28</td>
<td>( J_\ell(28) )</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>35</td>
<td>( \text{Coker} \ (J_\ell(35) \to J(X)) )</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>20</td>
<td>( J_\ell(20) )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>( J_\ell(30) )</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>45</td>
<td>( J_\ell(45) )</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>24</td>
<td>( \text{Coker} \ (J_\ell(24) \to J(X)) )</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>( J_\ell(15) )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>( J_\ell(18) )</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>36</td>
<td>( J_\ell(36) )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>72</td>
<td>( J_\ell(72) )</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td>( J_\ell(32) )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>( J_\ell(27) )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>( J_\ell(2,10) )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>( J_\ell(2,12) )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>( J_\ell(2,16) )</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

**Proposition (1.5).** For the integers \( N = 20, 21, 24, 35 \) and 55, let \( X = X_\ell \) be the subcoverings in (1.3) and put \( C_X = \text{Coker} \ (J_\ell(N) \to J(X)) \). Then \( \# C_X(\mathbb{Q}) < \infty \).

**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 \( \chi \)
be the multiplicative character of \((\mathbb{Z}[\sqrt{-1}]/(2 + \sqrt{-1}))^*\) with \(\chi(\sqrt{-1}) = -\sqrt{-1}\), and put
\[
\varepsilon = \left(\frac{-1}{\mathbb{Z}/(2 + \sqrt{-1})}\right) \quad \text{and} \quad \bar{\varepsilon} = \left(\frac{-1}{\mathbb{Z}/(2 + \sqrt{-1})}\right),
\]
where \(\left(\frac{-1}{\cdot}\right)\) is the quadratic residue symbol. Let \(f_\varepsilon, f_{\bar{\varepsilon}}\) be the new forms ([2]) belonging to \(S_2(\Gamma_1(20))\) (= the \(C\)-vector space of holomorphic cusp forms of weight 2 belonging to \(\Gamma_1(20)\)) which are associated with the nebentypen characters \(\varepsilon\) and \(\bar{\varepsilon}\), respectively; Let \(\psi\) be the primitive Grössen character of \(Q(\sqrt{-1})\) with conductor \((2 + \sqrt{-1})\) such that \(\psi((\alpha)) = \chi(\alpha)\alpha\) for \(\alpha \in Q(\sqrt{-1})^*\) prime to the conductor \((2 + \sqrt{-1})\). Then
\[
f_{\varepsilon}(z) = \sum_{\mathfrak{a}} \psi(\mathfrak{a}) \exp(2\pi i N(\mathfrak{a}) z),
\]
where \(N(\mathfrak{a}) = N_{Q(\sqrt{-1})/Q}(\mathfrak{a})\) is the norm of the ideal \(\mathfrak{a} \neq \{0\}\) and \(\mathfrak{a}\) runs over the set of integral ideals of \(Q(\sqrt{-1})\) ([33]). The modular curve \(X_0(20)\) is of genus 3 and \(H^0(X_0(20) \otimes C, \Omega^i) = H^0(X_0(20) \otimes C, \Omega^i) \oplus C \psi, dz \oplus C\psi, dz\).

For a cusp form \(f \in S_2(\Gamma_1(20))\) and \(g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(Q)\), put
\[
f[[g]](z) = (ad - bc)(cz + d)^i f \left(\frac{az + b}{cz + d}\right) \quad \text{and} \quad f | K(z) = (f(-z))^\dagger,
\]
where \(-\) is the complex conjugation. Then for \(H = \begin{pmatrix} 0 & -1 \\ 20 & 0 \end{pmatrix}\), \(f_\varepsilon|H = \lambda f_\varepsilon\) with the absolute value \(|\lambda| = 1\) ([2]). Put \(g = f_\varepsilon - f_{\bar{\varepsilon}}|H\) and \(h = f_\varepsilon + f_{\bar{\varepsilon}}|H\). Then \(g = f_\varepsilon + e^{-i\theta} f_{\bar{\varepsilon}}|K = e^{-i\theta} (e^{-i\theta} f_\varepsilon + e^{-i\theta} f_{\bar{\varepsilon}}|K)\) for a real number \(\theta\), and \(e^{-i\theta} g\) is real on the pure imaginary axis ([24] §2). \(C_X = \text{Coker}(J(\Gamma_0(20)) \to J(X))\) is isogenous over \(Q(\sqrt{-1})\) to the product of two elliptic curves \(E_\varepsilon\) and \(E_{\bar{\varepsilon}}\) with \(H^0(E_\varepsilon \otimes C, \Omega^i) = C \psi, dz\) and \(H^0(E_{\bar{\varepsilon}} \otimes C, \Omega^i) = C \psi, dz\). Further \(C_X\) is isogenous over \(Q\) to the restriction of scalars \(\text{Re}_{Q(\sqrt{-1})/Q}(E_{\varepsilon/Q(\sqrt{-1})})\) ([5] [34]). For a cusp form \(f \in S_2(\Gamma_1(20))\), put
\[
(2\pi/\sqrt{20})^{-1} \Gamma(s)L_f(s) = \int_0^\infty tf(\sqrt{-1}t/\sqrt{20}) dt
\]
and
\[
I(f) = \int_0^\infty f(\sqrt{-1}t/\sqrt{20}) dt.
\]

The (1-dimensional) \(L\)-function of \(C_X/Q\) and that of \(E_{\varepsilon/Q(\sqrt{-1})}\) are \(L_f(s)L_{f_{\varepsilon}}(s)\) and \(L_f(1)L_{f_{\varepsilon}}(1) = |L_{f_{\varepsilon}}(1)|^2\) (since \(f_\varepsilon = f_{\varepsilon}|K\) ([21]). The rank of \(C_X(Q)\) is zero if and only if \(E_{\varepsilon/Q(\sqrt{-1})} < \infty\). Then by the result on the Birch-Swinnerton Dyer conjecture for elliptic curves with complex multi-
application ([1] [3] [29]), it suffices to show that \( I(f, \epsilon) = 0 \). One sees that \( I(h) = 0 \) and \( I(f, \epsilon) = \frac{1}{2} (I(g) + I(h)) \). Since \( \epsilon \sqrt{-1} g \) 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 \( \tau = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma_0(20) \) with \( \epsilon(a) = -1 \). The \( g|\tau| = -g = g|H \), hence for \( \delta = \tau^{-1} \left( \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right) \), \( g|\delta| = g \). The quotient \( \Gamma_0(20)/\langle \delta \rangle \) is an elliptic curve, so the zero points of \( gdz \) are the fixed points of \( \delta \). The automorphism \( \delta \) has four fixed points, which correspond to \( -20\alpha + \sqrt{-20}/20 \alpha \) for integers \( \alpha \) and \( \beta \) such that \( \epsilon(\alpha) = -1 \) and \( \left( \begin{array}{cc} \alpha & \beta \\ \alpha & \beta \end{array} \right) \in \Gamma_0(20) \). Then \( \beta \neq 0 \), so \( \delta \) 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 \( \mathbb{Q} \)-simple and that \( C_X(\mathbb{Q}) \) has a subgroup \( \neq \{0\} \) of order prime to the class numbers of \( \mathbb{Q}(\zeta_N) \), where \( \zeta_N \) 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 \( \mathbb{Q} \)-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 \( S_2(\Gamma_0) \) (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 \( \mathbb{Q} \)-simple. There is a cuspidal subgroup of order 13 (see loc. cit.).

**Case** \( N = 55 \): The characteristic polynomial of \( T_2 \) on \( S_2(\Gamma_0) \) is

\[
(X + 2)^2(X - 1)(X^3 - 2X - 1) \times (X^4 - 9X^2 + 12).
\]

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

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

<table>
<thead>
<tr>
<th>curve</th>
<th>hyperelliptic involution</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_0(18) )</td>
<td>( w_5 ) [5]</td>
</tr>
<tr>
<td>( X_0(22) )</td>
<td>( w_{22} )</td>
</tr>
<tr>
<td>( X_0(33) )</td>
<td>( w_{11} )</td>
</tr>
<tr>
<td>( X_0(28) )</td>
<td>( w_7 )</td>
</tr>
<tr>
<td>( X_0(30) )</td>
<td>( w_{15} )</td>
</tr>
<tr>
<td>( X_0(13) )</td>
<td>[5]</td>
</tr>
</tbody>
</table>
**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. $X = X_{\nu}(77)$). For an automorphism $\iota$ of $X$, let $S_{\iota}$ denote the number of the fixed points of $\iota$. Then we see the following.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$\iota$</th>
<th>$S_{\iota}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>$(E, A_{n}, \pm P_{n}) \mapsto (E/A_{n}, E/A_{n}, \pm 3P_{n} \mod A_{n})$</td>
<td>12</td>
</tr>
<tr>
<td>55</td>
<td>$(E, A_{n}, \pm P_{n}, A_{n}) \mapsto (E/A_{n}, \pm 2P_{n} \mod A_{n}, E/A_{n})$</td>
<td>16</td>
</tr>
<tr>
<td>77</td>
<td>$\iota = \nu_{77}: (E, A) \mapsto (E/A, E/A_{77})$</td>
<td>8</td>
</tr>
</tbody>
</table>

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 $(1 \neq) \iota$ an automorphism of $X$ with the fixed points $x_{i}, 1 \leq i \leq s$. Let $f$ be a rational function on $X$ such that the divisors $(\iota^{*}f) \neq (f)$. Then the degree of $f \leq s/2$ and

\[
(\iota^{*}f - 1)_{0} > \sum' (x_{i}),
\]

where $\sum'$ is the sum of the divisors $(x_{i})$ such that $f(x_{i}) \neq 0, \infty$.

**Proof.** Let $S_{0}$ (resp. $S_{\infty}$, resp. $T$) be the set of the fixed points of $\iota$ consisting of $x_{i}$ with $f(x_{i}) = 0$ (resp. $f(x_{i}) = \infty$, resp. $x_{i} \not\in S_{0} \cup S_{\infty}$). 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

\[
(\iota^{*}f) = \iota^{*}E + F - E - \iota^{*}F.
\]

By the assumption $(\iota^{*}f) \neq (f)$, $g = \iota^{*}f - f$ is not a constant function, so

\[
\deg (g) \leq 2 \cdot \deg (f) - \sum_{x_{i} \in S_{0} \cup S_{\infty}} n_{i}.
\]

For $x_{i} \in T$, $g(x_{i}) = 1$. Therefore

\[
(g - 1)_{0} > \sum_{x_{i} \in T} (x_{i}).
\]

Then $\deg (g) \geq \# T$. Further $2 \cdot \deg (f) \geq \deg (g) + \sum_{x_{i} \in S_{0} \cup S_{\infty}} n_{i} \geq s$. 

**PROPOSITION (1.10)** ([28] (3.3.2) [27]). Let $K$ be a finite extension of $\mathbb{Q}_{p}$ of degree $e \leq p - 1$ 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 $f: G_{1} \rightarrow G_{2}$ be a homomorphism such that $f \otimes K: G_{i} \otimes K \rightarrow G_{i} \otimes K$ is an isomorphism. If $e < \text{deg}(f)$,

https://doi.org/10.1017/S00277630000002816 Published online by Cambridge University Press
$p - 1$, then $f$ is an isomorphism. If $e = p - 1$ and $f$ is not an isomorphism, then $G_1 \simeq (\mathbb{Z}/p\mathbb{Z})/R$ and $G_2 \simeq \mu_{p\mathbb{Z}}/R$.

**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 $x \otimes \bar{F}_p = 0$ (= the unit section), then $x = 0$.

(1.12) Let $K$ be a finite extension of $\mathbb{Q}_p$ with the ring of integers $R = O_K$ and its residue field $\simeq F_q$. Put $N = N'.p'$ 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 $K$) $\geq p - 1$. 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 $G_{\mathbb{Z}/R}$ 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 $F = F_q : E_{/R} \otimes F_q \to E_{/R} \otimes F_q$ acts trivially on $G_{/R} \otimes F_q$. In particular, $N \leq (1 + \sqrt{q})^2$ (by the Riemann-Weil condition). When $E$ has multiplicative reduction, the connected component $T$ of $E_{/R}(g) F_q$ of the unit section is a torus such that $T(F_q) \simeq Z/(q - \epsilon)Z$ for $\epsilon = \pm 1$. For a prime divisor $l$ of $N$, the $l$-primary part of $G(F_q) \simeq Z/l'^{s}Z \times Z/l'^{t}Z$ for integers $s, t$ with $0 \leq s \leq t$. Then $l'$ divides $q - \epsilon$ and $E_{/R} \otimes F_q$ contains $T \times Z/l'Z$. If $l' \mid q - \epsilon$, then $E_{/R} \otimes F_q$ contains $T \times Z/l'Z$.

(1.13) Let $X(\to X_0(1))$ be a modular curve defined over $\mathbb{Q}$ with its jacobian variety $J = J(X)$. Let $k$ be a quadratic field and $p$ a prime of $k$ lying over a rational prime $p$. Let $R = O_k(p), Z(p)$ denote the localizations at $p$ and $p$, respectively. Let $x$ be a $k$-rational point on $X$ such that $x \otimes \kappa(p)$ is a section of the smooth part $\mathbb{Z}^{\text{smooth}} \otimes Z(p)$ and that $x \otimes \kappa(p) = C \otimes \kappa(p), x^* \otimes \kappa(p) = C_e \otimes \kappa(p)$ for $Q$-rational cusps $C, C_e$ and $1 \neq \sigma \in \text{Gal}(k/Q)$, where $\mathbb{A}$ is the normalization of the projective $j$-line $\mathbb{A}_1$ isomorphic to $P^1_\mathbb{Q}$ in $X$. Consider the $Q$-rational section $i(x) = cl((x) + (x^*) - (C) - (C_0))$ of the Néron model $J_{/Z}$:

\[
\begin{array}{ccc}
\text{Spec } R \times \text{Spec } R & \xrightarrow{x \otimes x^*} & (\mathbb{A} \times \mathbb{A})^{\text{smooth}} \\
\downarrow J: \text{diagonal} & & \downarrow + \ \\
\text{Spec } Z(p) & \xrightarrow{i(x)} & J_{/Z}.
\end{array}
\]

Then $(x \otimes x^*) \cdot i(+) \otimes \kappa(p) = 0$ (= the unit section), hence $i(x) \otimes F_p = 0$. 

https://doi.org/10.1017/500277630000002816 Published online by Cambridge University Press
Let $A/Q$ be a quotient of $J$; $J \rightarrow A$ 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 $C_\sigma$ are not $Q$-rational. Assume that the set $\{C, C_\sigma\}$ is $Q$-rational and that $C \otimes Z_{(p)}$ and $C_\sigma \otimes Z_{(p)}$ are the sections of $Z' \otimes Z_{(p)}$.

Let $K$ be the quadratic field over which $C$ and $C_\sigma$ are defined. Let $\rho'$ 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 $i(x) \otimes \kappa(p') = 0$ in $J/K$. If $e' < p - 1$ or $p$ does not divide $\#A(Q)$, then $j \cdot i(x) = 0$.

For a finite extension $K$ of $Q$ 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 $Q$ and $L$ be a quadratic extension of $K$, with the relative discriminant $D = D(L/K)$. Then the restriction of scalars $Re_{L/K}(E/L)$ ([5] [34]) is isogenous over $K$ to a product of $E$ and an elliptic curve $F(K)$ with $f(E/K)f(F/K) = N_{L/K}(f(E/L))^2D$.

§ 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 $1 \neq \sigma \in \text{Gal}(k/Q)$, $x^\sigma$ is represented by the pair $(E^\sigma, \pm P^\sigma)$. For the integers $N$, $1 \leq N \leq 10$ or $N = 12$, $X_1(N) \simeq P^1$. 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 $\geq 2$ and is not hyperelliptic, then $Y_1(N)(k) = \emptyset$ 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 $1 \neq \sigma \in \text{Gal}(k/Q)$.
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 \( \mathbb{Q} \)-rational point on \( X_1(13)/\langle [5]\rangle \simeq P^1 \), where \( [5] \) is the automorphism of \( X_1(13) \) represented by \( g \in \Gamma_1(13) \) such that \( g \equiv \begin{pmatrix} 5 & * \\ 0 & * \end{pmatrix} \mod 13 \).

Let \( \pi: X_1(13q) \to X_1(13) \) be the natural morphism and \( y \) be the \( \mathbb{Q} \)-rational point \( \{\pi(x), [5]\pi(x)\} \) on \( Y_1(13)/\langle [5]\rangle \). Let \( p \) be a prime of \( k \) lying over the rational prime \( p = 3 \) if \( q = 2 \), and \( p = 5 \) if \( q \geq 3 \). Then the condition \( \mathbb{Z}/N\mathbb{Z} \subset E(k) \) leads that \( (\mathbb{Z}/N\mathbb{Z})_R \subset E_R \), where \( R \) is the localization \( (\mathcal{O}_k)_{(p)} \) of \( \mathcal{O}_k \) at \( p \) (1.12). Then \( E_R \) has multiplicative reduction cf. (1.12). Let \( F \) be an elliptic curve defined over \( \mathbb{Q} \) with a \( \mathbb{Q} \)-rational set \( \{\pm Q, \pm 5Q\} \) for a point \( Q \) of order 13 such that the pair \( (F, \{\pm Q, \pm 5Q\}) \) represents \( 3^6 \) on \( Y_1(13)/\langle [5]\rangle \). Let \( \rho = \rho_q \) be the representation of the Galois action of \( G = Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \) on the \( q \)-torsion points \( F_q(\overline{\mathbb{Q}}) \). Then \( F \simeq E \) over a quadratic extension \( K \) of \( k \), since \( E \) has multiplicative reduction at \( p \).

Then for \( G_k = Gal(\overline{\mathbb{Q}}/K) \),

\[
\rho(G_k) \longrightarrow \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset GL_2(F_q) \simeq Aut F_q(\overline{\mathbb{Q}}).
\]

When \( q = 2 \), \( GL_2(F_q) \simeq S_3 \) (the symmetric group of three letters) and \([\rho(G): \rho(G_k)] \) divides 4, so that \( \rho(G) \hookrightarrow \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \). Then \( E \) has a \( \mathbb{Q} \)-rational point \( Q \), of order 2 and the pair \( (F, \{\pm Q, \pm 5Q\}) \) represents \( 3^6 \) on \( Y_1(26) \). But we know that \( Y_1(26)(\mathbb{Q}) = \phi \) ([18] [24] [36] table 1, 5). Now consider the cases for \( q \geq 3 \). Let \( \theta_q \) be the cyclotomic character

\[
\theta_q: G = Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mu_q(\overline{\mathbb{Q}}).
\]

Then \( \det \rho = \theta_q \). Let \( P_q \) be a \( K \)-rational point on \( F \) of order \( q \) and \( g \in G_k \setminus G_\kappa \) for \( G_\kappa = Gal(\overline{\mathbb{Q}}/k) \). If \( P_q \neq \pm P_q \), then \( \langle P_q \rangle \neq \langle P_q \rangle \) and \( \rho(G_k) = 1 \). Then \( \theta_q(G_\kappa) = 1 \), hence \( q = 3 \), or \( q = 5 \) and \( K = \mathbb{Q}(\zeta_5) \). For \( q = 3 \), if \( k \neq \mathbb{Q}(\zeta_5) \), then \( K \) is an abelian extension of \( \mathbb{Q} \) with the Galois group \( \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) and \( \rho(G) \hookrightarrow \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix} \). If \( k = \mathbb{Q}(\zeta_5) \), then \( \rho(G_\kappa) = \{\pm 1\} \), since \( \det \rho(G_k) = \theta_3(G_\kappa) = 1 \). Then \( \rho(G) \hookrightarrow \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \), since \( \theta_3(G) = \{\pm 1\} \). For \( q = 5 \), \( K = \mathbb{Q}(\zeta_5) \) and \( \rho(G) \hookrightarrow \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \). Thus there exists a subgroup
$A_q/Q$ of $F$ of order $q$. Then the pair $(F, A_q + \langle Q \rangle)$ represents a $Q$-rational point on $Y_0(13q)$. But we know that $Y_0(13q)(Q) = \phi$ for $q \geq 2$ ([9, 10, 11] [18] [20]). Now suppose that $P_q^e = \pm P_q$. Then $\rho(G_q) \rightarrow \begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix}$. Take $h \in G \setminus G_k$ 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 $Q$-rational point on $Y_0(13q)$. Therefore, $A_q^h \neq A_q$ and $\rho(G_q) \rightarrow \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$, then $q = 3$, $k = Q(\zeta_3)$ and $\rho(G)$ \rightarrow \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ and the same argument as above gives a contradiction. If $\rho(G_q) \simeq \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$, then $q = 3$ and $\rho(G)$ is contained in the normalizer of a split Cartan subgroup (since $\det = \theta_q$). Let $Y$ be the modular curve $\Gamma_0$ which corresponds to the modular group $\Gamma^0(13)$ such that $g \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ mod $3$. Then the isomorphism of $X_0(9 \cdot 13)$ to $Y$:

$$(C, A_q + A_{11}) \rightarrow (C/A_3, \{A_3/A_2, C_1/A_2\}, (A_{13} + A_3)/A_2)$$

induces an isomorphism of $X_0(9 \cdot 13)/\langle \omega \rangle$ to $Z = Y/\langle \omega \rangle$, where $A_m$ are cyclic subgroups of order $m$ with $A_3 \subset A_m$. The jacobian variety $J = J(Z)$ of $Z$ has an optimal quotient $A/Q(J \rightarrow A)$ with finite Mordell-Weil group ([36] table 1.5). As was seen as above, $F$ has potentially multiplicative reduction at $5$. Let $z$ be the $Q$-rational point on $Y$ represented by $(F, \langle Q \rangle)$ with a level structure mod $3$; then $z \otimes F_5 = C \otimes F$, for a $Q$-rational cusp $C$ on $Z$. Let $f: Z \rightarrow J \rightarrow A$ be the morphism defined by $f(y) = cl((y) - (C))$. Then we see that $f(z) = 0$ (see (1.11)). Let $X$ denote the normalization of $X_0(1)$ in $Z$. Then we see that $f \otimes Z: X \otimes Z_5 \rightarrow A_{/Z_5}$ 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 $\rho$ be a prime of $k$ lying over the rational prime $3$ and put $R = (O_k)_{13}$. The condition $Z[N]Z \subset E(k)$ shows that $(Z[N]Z)_R \subset E_{/R}$ if $q = 2$ or $q = 3$ is unramified (1.11). If $q = 3$ ramifies in $k$, then $(Z/11Z)_R \subset E_{/R}$ and $k(\rho) = F_3$. Hence $x \otimes k(\rho)$ is also a cusp (see (1.12)). Denote also by $x, x'$ the images of $x$ and $x'$ under the natural morphism $\pi: X_0(N) \rightarrow X_0(N)$. Then $x \otimes k(\rho) =$
Let \( i(x) = \text{cl}((x) + (x^*) - (C) - (C_s)) \) be the \( Q \)-rational section of \( J_0(11q) \).

Since \( \gamma(C) \oplus F_5 \neq C \oplus F_5, \gamma(x) \neq x \). If \( f \) is a constant function, then \( \gamma(x) = x^* \) and the set \( \{ x, \gamma(x) = x^* \} \) defines a \( Q \)-rational point on \( Y_0(55) \). But \( Y_0(55)(Q) = \phi \) [18], so that \( f \) is not a constant function. If \( (\delta^*f) = (f) \), then \( \delta(C) = C \) or \( C_s \). But \( C, C_s \) are \( 0 \)-cusps and \( \delta(C) \) is not a \( 0 \)-cusps, so that \( (\delta^*f) \neq (f) \). Applying (1.9) to \( f \) and \( \delta \), we get a contradiction.

Remark (2.3). For any cubic field \( k' \), \( Y_0(55)(k') = \phi \). It is shown by the same way as above, taking a prime \( \nu' \) of the smallest Galois extension of \( Q \) containing \( k' \).
\( q = 7 \): Let \( \pi\colon \mathbb{X}_0(77) \to \mathbb{X}_0(77)/\langle w_1 \rangle \) be the natural morphism and \( J' \) be the jacobian variety of \( \mathbb{X}_0(77)/\langle w_1 \rangle \). Then \( A = \text{Coker} (\pi_i^*\colon J' \to J_i(77)) \) 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 \( \mathbb{Z}/77\mathbb{Z} \subset E(k) \) shows that \( x \otimes \kappa(p) \) is a 0-cusp \((\otimes \kappa(p)) \) (1.12). Denote also by \( x, x' \) the images of \( x \) and \( x' \) under the natural morphism \( \mathbb{X}_0(77) \to \mathbb{X}_0(77) \). Then \( x \otimes \kappa(p) = 0 \otimes \kappa(p) \). Let \( i(x) = cl((x) + (x') - 2(0)) \) be the \( \mathbb{Q} \)-rational section of \( J_{\mathbb{Q}}(77)_7 \) (see (1.11), (1.13)). Then we get a rational function \( f/\mathbb{Q} \) on \( \mathbb{X}_0(77) \) such that

\[
(f) = (x) + (x') + 2(w_1(0)) - (w_1(x)) - (w_1(x')) - 2(0).
\]

Then \((w_{11}^*f) = -(f) \neq 0\), since \( w_{11}(0) \neq 0\). Hence \( w_{11}^*f = \alpha/f \) for \( \alpha \in \mathbb{Q}^\times \). The fundamental involution \( w = w_7 \) of \( \mathbb{X}_0(77) \) has 8 fixed points \( x_i (1 \leq i \leq 8) \). The cusps \( w_1(0) \otimes F_i \) and \( 0 \otimes F_i \) are not the fixed point of \( w \). Therefore by (1.9),

\[
(w^*f/f - 1)_i = \sum_{i=1}^{8} (x_i) (\equiv D).
\]

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

\[
(g) = (x) + (x') + 2(w_1(0)) + (w_1(x)) + (w_1(x')) + 2(\infty) - D
\]

and

\[
w^*g = w_{11}^*g = -1 - g.
\]

Then \( g \) defines a rational function \( h \) on \( Y = \mathbb{X}_0(77)/\langle w_1 \rangle \) with \( \pi_i^*(h) = g \), where \( \pi_i\colon \mathbb{X}_0(77) \to Y \) is the natural morphism. Set \( \{y_i\}_{i \leq 1 \leq 8} = \{\pi_i(x_i)\} \), and put \( E = \sum_{i=1}^{8} (y_i) \) and \( C = \pi_i(\infty) \) \( (= \pi_i(w_1(0))) \). 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 \( w_1 \)). Then

\[
w^*h = -1 - h \quad \text{and} \quad (h)_* = E.
\]

Let \( \pi_Y\colon Y \to Z = \mathbb{X}_0(77)/\langle w_1, w_{11} \rangle \) 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 \( \omega \) be the base of \( H^0(Z, \Omega^1) \) and \( \omega_1 = \pi_i^*(\omega) \), \( \omega_2 \) and \( \omega_3 \) be the basis of \( H^0(Y, \Omega^1) \) such that \( \omega_i(C) = 1 \) and that \( \omega_i \) are eigenforms of the Hecke ring \( \mathbb{Q}[T_{w_1}, w_{11}(m, n)] \) with \( T_{w_1}^*\omega_2 = 0 \) and \( T_{w_1}^*\omega_3 = \omega_3 \) (see \([36]\) table 1, 3, 5). Then \( \{1, f_1 = \omega_2/\omega_1, f_3 = \omega_3/\omega_1\} \) is the set of basis of \( H^0(Y, \mathcal{O}_Y(E)) \) such that \( f_1 = 1 + q + \cdots \) 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 \( a_i \in \mathbb{Q} \). The
conditions \(w^*h = -1 - h\) and \(w^*f_i = -f_i\) show that \(a_i = -\frac{1}{2}\). Further by the condition \((h)_s \geq 2(C)\), \(a_2 = \frac{1}{2}\) and \(a_3 = \frac{1}{2}\). Let \(\mathcal{O}_i\) be the quotient \(\mathcal{O}_i(77)/\langle w_i \rangle \otimes \mathbb{Z}_s\) and \(\hat{\mathcal{O}}_{w_i,C}\) be the completion of the local ring \(\mathcal{O}_{w_i,C}\) along the cuspidal section \(C\). Then \(f_i \in \hat{\mathcal{O}}_{w_i,C}\), so that \(h \in \hat{\mathcal{O}}_{w_i,C}\). Put \(C' = \pi_i(0) (= \pi_i(w_i(0)))\). Then \(w^*h \in \hat{\mathcal{O}}_{w_i,C}\) and \(w^*h(\pi_i(x)) = (-1 - h)(\pi_i(x)) = -1, w^*h(C') = (-1 - g)(0) = 0\). But the conditions that \(x \otimes \kappa(p) = 0 \otimes \kappa(p)\) for \(p\) (5) and \(w^*h \in \hat{\mathcal{O}}_{w_i,C}\) give the congruence \(w^*h(\pi_i(x)) \equiv w^*h(C') \mod p\). Thus we get a contradiction.

**Case \(N = 7n\) for \(n = 3, 4\) and 7:**

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

\[
X(21) \xrightarrow{2} X(3) \xrightarrow{3} X(21),
\]

which corresponds to the subgroup \(\Delta = (\mathbb{Z}/3\mathbb{Z})^* \times \{\pm 1\}\). Let \(\mathcal{X}\) denote the normalization of \(\mathcal{X}(1)\) in \(X\). The special fibre \(\mathcal{X} \otimes \mathbb{F}_p\) is reduced (1.2).

Let \(p\) be a prime of \(k\) lying over the rational prime 3 and put \(R = (\mathcal{O}_1)_p\). The condition \(\mathbb{Z}/21\mathbb{Z} \subset \mathbb{E}(k)\) shows that \((\mathbb{Z}/21\mathbb{Z})_R \subset E_R\) if the rational prime 3 is unramified in \(k\) (1.11), (1.12). If 3 ramifies in \(k\), then \(\kappa(p) = F_s\), so that in both cases \(E_R\) has multiplicative reduction see (1.12). Therefore, \(x \otimes \kappa(p) = C \otimes \kappa(p), x^* \otimes \kappa(p) = C_e \otimes \kappa(p)\) for \(Q\)-rational cusps \(C\) and \(C_e\) (see loc. cit.). Let \(i(x) = cl((x) + (x^*) - (C) - (C_e))\) be the \(Q\)-rational section of \(J(X)_F\). Since the Mordell-Weil group of \(J(X)\) is finite (1.4), (1.5), \((x) + (x^*) \sim (C) + (C_e)\). But \(X\) is not hyperelliptic (1.7).

\(n = 4\): Let \(p\) be a prime of \(k\) lying over the rational prime 3 and put \(R = (\mathcal{O}_1)_p\). The condition \(\mathbb{Z}/28\mathbb{Z} \subset \mathbb{E}(k)\) shows that \((\mathbb{Z}/28\mathbb{Z})_R \subset E_R\). Denote also by \(x, x^*\) the images of \(x\) and \(x^*\) under the natural morphism \(X(28) \to X(28)\). Then \(x \otimes \kappa(p) = C \otimes \kappa(p), x^* \otimes \kappa(p) = C_e \otimes \kappa(p)\) for \(Q\)-rational cusps \(C\) and \(C_e\). These cusps \(C, C_e\) are represented by \((G_m \times \mathbb{Z}/7m\mathbb{Z}, H)\) and \((G_m \times \mathbb{Z}/7m_e\mathbb{Z}, H_e)\) for integers \(m\) and \(m_e\) and cyclic subgroups \(H, H_e\) containing \(\{1\} \times \mathbb{Z}/7m\mathbb{Z}\) and \(\{1\} \times \mathbb{Z}/7m_e\mathbb{Z}\), respectively. Let \(i(x) = cl((x) + (x^*) - (C) - (C_e))\) be the \(Q\)-rational section of \(J(28)_F\). Since the Mordell-Weil group of \(J(28)\) is finite (1.4), \(i(x) = 0\) (1.13) and \((x) + (x^*) \sim (C) + (C_e)\). \(X(28)\) has the hyperelliptic involution \(w_n\), so \(C_e = w_n(C)\). But as noted as above, \(C_e \neq w_n(C)\).

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

\[
X(35) \xrightarrow{\pi_1} X \xrightarrow{\pi_X} X(35),
\]
which corresponds to the subgroup $J = (\mathbb{Z}/5\mathbb{Z})^\times \times \{\pm 1\}$. The automorphism $\tau$ of $X$ represented by

$$(F, B_5, \pm Q) \mapsto (F/B_5, F_5/B_5, \pm 3Q, \text{mod } B_0)$$

has 12 fixed points (1.8). Let $p$ be a prime of $k$ lying over the rational prime 3 and put $R = (\mathcal{O}_k)_{(p)}$. The condition $\mathbb{Z}/35\mathbb{Z} \subseteq E(k)$ shows that $(\mathbb{Z}/35\mathbb{Z})_R \subset E_R$. Denote also by $x, x'$ the images of $x$ and $x'$ by the natural morphism $\pi: X(35) \to X$. Then $x \otimes \kappa(p) = C \otimes \kappa(p), x' \otimes \kappa(p) = C' \otimes \kappa(p)$ for $\mathbb{Q}$-rational cusps $C$ and $C'$ (1.12). Let $i(x) = cl((x) + (x') - (C) - (C'))$ be the $\mathbb{Q}$-rational section of $J(X)/J$. The Mordell-Weil group of $C_x = \text{Coker}(\tau_x: J_x(35) \to J(X))$ is finite (1.5). Let $\delta$ be a generator of $\text{Gal}(X/X_0(35))$. Then we get a rational function $f$ on $X$ such that

$$(f) = (x) + (x') + (\delta(C)) + (\delta(C')) - (\delta(x)) - (\delta(x')) - (C) - (C')$$

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

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

$n = 4$: Let $p$ be a prime of $k$ lying over the rational prime 3 and put $R = (\mathcal{O}_k)_{(p)}$. The condition $\mathbb{Z}/20\mathbb{Z} \subseteq E(k)$ shows that $(\mathbb{Z}/20\mathbb{Z})_R \subset E_R$ and that $E_R$ has multiplicative reduction (1.12). Let $T$ be the connected component of the special fibre $E_R \otimes \kappa(p)$ of the unit section. If $p$ is of degree one, then $\mathbb{Z}/5\mathbb{Z} \nsubseteq T(F_5)$. Then $x \otimes \kappa(p) = C \otimes \kappa(p), x' \otimes \kappa(p) = C_\tau \otimes \kappa(p)$ for $\mathbb{Q}$-rational cusps $C$ and $C_\tau$, since $\left(\frac{-1}{3}\right) = -1$, where $\left(\frac{-1}{3}\right)$ is the quadratic residue symbol. If $p$ is of degree two, then $x \otimes \kappa(p) = C \otimes \kappa(p)$ for a $Q(\sqrt{-1})$-rational cusp $C$, and $x' \otimes \kappa(p) = C_\tau \otimes \kappa(p)$ with $C_\tau = C_\tau^\tau$ for $1 \neq \tau \in \text{Gal}(Q(\sqrt{-1})/Q)$. Let $i(x) = cl((x) + (x') - (C) - (C'))$ be the $\mathbb{Q}$-rational section of $J(20)/J$. Since $\#J(20)(\mathbb{Q}) < \infty$ (1.4) (1.5), $i(x) = 0$ (1.14) and $(x) + (x') \sim (C) + (C')$. But $X_{(20)}$ 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 $p$ be a prime of $k$ lying over the rational prime 3 and put $R = (\mathcal{O}_k)_{(p)}$. Then $(\mathbb{Z}/10\mathbb{Z})_R \subset E_R$ and $E_R$ is semistable (1.12). If 3 is unramified in $k$, then $(\mathbb{Z}/30\mathbb{Z})_R \subset E_R$. Then $E_R$ has multiplicative reduction and $(\mathbb{Z}/3\mathbb{Z})_R \otimes \kappa(p)$ 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 multiplicative reduction and $(\mathbb{Z}/5\mathbb{Z})_{/R} \otimes \kappa(p)$ is not contained in the connected component of $E_{/R} \otimes \kappa(p)$ of the unit section (see loc. cit.). Denote also by $x, x'$ the images of $x$ and $x'$ under the natural morphism $X,(30) \to X,(30)$. Then $x \otimes \kappa(p) = C \otimes \kappa(p), x' \otimes \kappa(p) = C_s \otimes \kappa(p)$ for $Q$-fibre rational cusps $C$ and $C_s$. These cusps $C, C_s$ are represented by $(G_m \times \mathbb{Z}/q_m\mathbb{Z}, H_s)$ and $(G_m \times \mathbb{Z}/q_m\mathbb{Z}, H_s)$ for integers $m, m_s \geq 1$ and cyclic subgroups $H, H_s$ containing $\{1\} \times m\mathbb{Z}/q_m\mathbb{Z}$ and $\{1\} \times m_s\mathbb{Z}/q_m\mathbb{Z}$ for $q = 3$ or 5, respectively. Let $i(x) = cl((x) + (x') - (C) - (C_s))$ be the $Q$-rational section of $J,(30)\mathbb{Z}$. Since $\#J,(30)(Q) < \infty$ (1.4), $i(x) = 0$ (1.13) and $(x) + (x') \sim (C) + (C_s)$.

Let $\pi : X,(24) \to X,(30)$, which corresponds to the subgroup $\mathfrak{A} = \{\pm 1\} \times (\mathbb{Z}/3\mathbb{Z})^\times$. Let $p$ be a prime of $k$ lying over the rational prime 5 and put $R = (\mathbb{C}_k)_{(p)}$. Then $(\mathbb{Z}/45\mathbb{Z})_{/R} \subset E_{/R}$ and $x \otimes \kappa(p) = C \otimes \kappa(p), x' \otimes \kappa(p) = C_s \otimes \kappa(p)$ for 0-cusps $C$ and $C_s$ (1.11), (1.12). Denote also by $x, x', C$ and $C_s$ the images of $x, x'$, $C$ and $C_s$ under the natural morphism $X,(45) \to X,(30)$. Let $i(x) = cl((x) + (x') - (C) - (C_s))$ be the $Q$-rational section of $J,(45)\mathbb{Z}$. Since $\#J,(45)(Q) < \infty$ (1.4), $i(x) = 0$ (1.13). But $X,(45)$ is not hyperelliptic [25].

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

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

$$X,(24) \xrightarrow{\pi_1} X \xrightarrow{\pi_x} X,(24),$$

which corresponds to the subgroups $\mathfrak{A} = \{\pm 1\} \times (\mathbb{Z}/3\mathbb{Z})^\times$. Let $p$ be a prime of $k$ lying over the rational prime 3 and put $R = (\mathbb{C}_k)_{(p)}$. Then $(\mathbb{Z}/8\mathbb{Z})_{/R} \subset E_{/R}$ and $E_{/R}$ is semistable (1.12). If 3 is unramified in $k$, then $(\mathbb{Z}/24\mathbb{Z})_{/R} \subset E_{/R}$ (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 $x, x'$ the images of $x$ and $x'$ by the natural morphism $\pi : X,(24) \to X$. If $p$ is of degree one, then $x \otimes \kappa(p) = C \otimes \kappa(p), x' \otimes \kappa(p) = C_s \otimes \kappa(p)$ for $Q$-rational cusps $C$ and $C_s$. Any cusp on $X$ is defined over $Q$ or $Q(\sqrt{2})$. If $p$ is of degree two, then $x \otimes \kappa(p) = C \otimes \kappa(p)$ for a $Q(\sqrt{2})$-rational cusp $C$. Then $x' \otimes \kappa(p) = C_s \otimes \kappa(p)$ for $C_s = C$ and $1 \neq \tau \in \text{Gal}(Q(\sqrt{2})/Q)$, since $\left(-\frac{2}{3}\right) = -1$. Let $i(x) = cl((x) + (x') - (C) - (C_s))$ be the $Q$-rational section of $J(X)\mathbb{Z}$. Since $\#J(X)(Q) < \infty$ (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
Then \((Z/36Z)_{\Lambda}\) and \(E_1/R\) is semistable (1.12). If \(E_1/R\) has good reduction, then \(\#E_1(R(F_{25})) = 1 + 25 - (-10)\) (since \(Z/36Z \subset E_1(R(F_{25}))\) and \(\#E_1(R(F_{25})) \leq 36\)). But then the Frobenius map \(F = F_{25} : E_1/R \otimes F_{25} \rightarrow E_1/R \otimes F_{25}\) does not act trivially on \(E_1(R(F_{25})) \rightarrow Z/36Z\). Hence \(E_1/R\) has multiplicative reduction. Let \(T\) be the connected component of \(E_1/R \otimes \kappa(p)\) of the unit section. Then \(Z/9Z \subset T(R(F))\). Denote also by \(x, x'\) the images of \(x\) and \(x'\) under the natural morphism \(X_0(36) \rightarrow X_1(18)\). Then \(x \otimes \kappa(p) = C \otimes \kappa(p), x' \otimes \kappa(p) = C_2 \otimes \kappa(p)\) for \(q\)-rational cusps \(C\) and \(C_2\) on \(X_1(18)\) (see above). The modular curve \(X_1(18)\) has the hyperelliptic involution \(w_5[5]\) (1.6):

\[(F, B_2, \pm Q_9) \mapsto (F/B_2, F_{25}/B_2, \pm 5Q_9 \text{ mod } B_2),\]

where \(B_2\) is a subgroup of order 2 and \(Q_9\) is a point of order 9. Let \(i(x) = cl((x) + (x') - (C) - (C'))\) be the \(q\)-rational section of \(J_1(18)\). Since \(\#J_1(18)(Q) < \infty\) (1.4), \(i(x) = 0\) (1.13) and \(x' = w_5[5](x)\). For a \(q\)-rational point \(Q\) of order 18, the pairs \((E_1, \pm Q), (E_1', \pm Q')\) represent \(x\) and \(x'\) on \(X_1(18)\). Put \(A_2 = \langle 9Q \rangle\). Then there is a quadratic extension \(K\) of \(q\) over which

\[\lambda : (E_1', \pm Q') \rightarrow (E/A_2, \pm (Q'_2 + 5Q) \text{ mod } A_2),\]

where \(Q'_2\) is a point of order 2 not contained in \(A_2\). For \(1 \neq \tau \in \Gal(K/q)\), \(\lambda' = \pm \lambda\), since \(x \otimes \kappa(p)\) is a cusp. Then \(\lambda(Q') = \varepsilon(Q'_2 + 5Q) \text{ mod } A_2\) for \(\varepsilon = \pm 1\). The points \(Q'_2\) and \(\lambda(Q'_2)\) are \(q\)-rational, so \(\lambda'(Q'_2) = (\lambda(Q'_2))' = \lambda(Q'_2)\). Therefore \(\lambda' = \lambda\) and \(\lambda\) is defined over \(q\). Since \(E/A_2\) contains \(E_2/A_2 \oplus \langle 9P \rangle/A_2 (\simeq Z/2Z \times Z/2Z), E_1''(q) \supset Z/2Z \times Z/36Z\). Let \(X_0(2, 36)\) be the modular curve \((q)\) corresponding to \(\Gamma(2, 36)\). Then \(E_1''\) and \(E_1'\) (with level structures) define \(q\)-rational points \(y, y''\) on \(X_0(2, 36)\) such that \(y \otimes \kappa(p) = D \otimes \kappa(p), y'' \otimes \kappa(p) = D_2 \otimes \kappa(p)\) for \(q\)-rational cusps \(D, D_2\). Let \(i(y) = cl((y) + (y') - (D) - (D_2))\) be the \(q\)-rational section of \(J_0(2, 36)\). Then \(i(y) = 0\), since \(\#J_0(2, 36)(q) < \infty\) (1.4) (1.13). But \(X_0(2, 36)\) is not hyperelliptic [25].

Now we discuss the \(q\)-rational points on \(X_0(N)\) for \(N = 14, 15\) and 18. The modular curves \(X_0(14)\) and \(X_0(15)\) are elliptic curves, and \(X_0(18)\) is hyperelliptic of genus 2. We here give examples of quadratic fields \(q\) such that \(Y_0(N)(q) = \phi\) for each integer \(N\) as above.

**Proposition (2.4).** Let \(q\) be a quadratic field. If one of the following conditions (i), (ii) and (iii) is satisfied, then \(Y_0(18)(q) = \phi\):

\[R = (\mathcal{O}_k)_p.\]
(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 \( \mathcal{O} = (\mathcal{O}_x)_p \) for a prime \( p \) of \( k \) lying over \( p \). Then \( (\mathbb{Z}/18\mathbb{Z})_R \subset E_R \) if \( p = 5 \) or 7, \( (\mathbb{Z}/9\mathbb{Z})_R \subset E_R \) if \( p = 2 \) and \( (\mathbb{Z}/18\mathbb{Z})_R \subset E_R \) 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 \( x \otimes \kappa(p) = C \otimes \kappa(p) \), \( x' \otimes \kappa(p) = C' \otimes \kappa(p) \), for \( \mathbb{Q} \)-rational cusps \( C \) and \( C' \) and for a prime \( p \) of \( k \) lying over \( p = 3 \). Using the \( \mathbb{Q} \)-rational section \( i(x) = cl((x) + (x') - (C) - (C')) \) of \( J_1(18)_{/\mathbb{Z}} \), we see that \( w_i[5](C) = C' \). If 3 remains prime in \( k \), then \( C' \otimes F_9 = x' \otimes F_9 = (x \otimes F_9)^{(3)} = C \otimes F_9 \). But \( C \otimes F_i \) is not a fixed point of the hyperelliptic involution \( w_i[5] \). In the case (ii), the same argument as above shows that \( C \otimes F_i = C_\ast \otimes F_i \). But \( C \otimes F_i \) is not a fixed point of \( w_i[5] \).

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 \( k = \mathbb{Q}(\sqrt{-3}) \) and \( \mathbb{Q}(\sqrt{-7}) \).
(2) \( Y_1(15)(\mathbb{Q}(\sqrt{5})) = \phi \).

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] \( \text{Re}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(X_0(14)/\mathbb{Q}(\sqrt{-3})) \), \( \text{Re}_{\mathbb{Q}(\sqrt{-7})/\mathbb{Q}}(X_0(14)/\mathbb{Q}(\sqrt{-7})) \) and \( \text{Re}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(X_0(15)/\mathbb{Q}(\sqrt{5})) \) are isogenous over \( \mathbb{Q} \) (respectively) to products \( X_0(14) \times E_{15}, X_0(14) \times E_{15} \) and \( X_0(15) \times E_{15} \) 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 \( \#X_0(N)(k) < \infty \) for \( (N, k) \) as above. Let \( x \) be a \( k \)-rational point on \( X_0(N) \) and denote also by \( x \) the image of \( x \) under natural morphism \( X_0(N) \to X_0(N) \) for \( (N, k) \) as above. Then \( x \otimes \kappa(p) = C \otimes \kappa(p) \) for a \( \mathbb{Q} \)-rational cusp \( C \) on \( X_0(N) \) and for a prime \( p \) 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 \( X_0(m, N) \)

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 $X_i(m, N)$. For $(m, N) = (2, 2), (2, 4), (2, 6), (2, 8); (3, 3), (3, 6); (4, 4), X_i(m, N) \simeq P/$. For $(m, N) = (2, 10)$ and $(2, 12), X_i(m, N)$ are elliptic curves. For the other pairs $(m, N)$ as above, $X_i(m, N)$ are not hyperelliptic [7]. We first discuss the $k$-rational points on $Y_i(m, N)$ for the pairs $(m, N)$ such that $X_i(m, N)$ are not hyperelliptic. It suffices to treat the cases for the pairs $(m, N): m = 2, N = 10, 12, 14, 16, 18; m = 3 (k = Q(V^1)), N = 9, 12, 15; m = 4 (k = Q(\sqrt{-1})), N = 8, 12; m = 6 (k = Q(\sqrt{-3})), N = 6$. Let $x$ be a $k$-rational point on $Y_i(m, N)$. Then there exists an elliptic curve $E$ defined over $k$ with $k$-rational points $P_m$ and $P_N$ such that the pair $(E, \pm (P_m, P_N))$ represents $x$ [4] VI (3.2). For $1 \neq \sigma \in \text{Gal}(k/Q)$, $x^\sigma$ 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 $X_i(m, N)$ is not hyperelliptic (i.e., $X_i(m, N) \not\simeq P^1$ nor $(m, N) \neq (2, 10), (2, 12))$, then $Y_i(m, N)(k) = \phi$.

**Proof.** Let $J_i(m, N)$ and $J_i(m, N)$ be the jacobian varieties of the modular curves $X_i(m, N)$ and $X_i(m, N) \simeq X_i(mN)$, respectively, and $\pi: X_i(m, N) \rightarrow X_i(m, N)$ be the natural morphism. Suppose that there is a $k$-rational point $x$ on $Y_i(m, N)$. 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 $p$ be a prime of $k = Q(\sqrt{-3})$ lying over the rational prime 7 and put $R = (O_q)_{(p)}$. Then $(Z/6Z)_{(p)}, (Z/6Z)_{(p)} \subset E_{/R}$ (1.12), so that $\pi(x) \otimes k(p) = C \otimes k(p)$ for a $Q(\sqrt{-3})$-rational cusp $C$. The modular curve $X_i(6, 6)$ is an elliptic curve and the restriction of scalars $\text{Re}_{Q(\sqrt{-3})/Q}(X_i(6, 6), Q(\sqrt{-3}))$ is isogenous over $Q$ to the product $X_i(6, 6) \times X_i(6, 6)$. Since $\#X_i(6, 6)(Q) < \infty$ [36] table 1, we see that $\#X_i(6, 6)(Q(\sqrt{-3}) < \infty$. Then $\pi(x) = C (1,11)$, which is a contradiction.

**Case m = 4 (N = 8, 12):** In both cases for $N = 8$ and 12, $\pi(x) \otimes k(p) = C \otimes k(p)$ for a prime $p$ of $k = Q(\sqrt{-1})$ lying over the rational prime 5 and for $k$-rational cusps $C (1.12)$. Let $\pi: X_i(4, 12) \rightarrow X_i(2, 12)$ be the natural morphism. The modular curves $X_i(4, 8)$ and $X_i(2, 12)$ are elliptic curves and $\#X_i(4, 8)(Q(\sqrt{-1})), \#X_i(2, 12)(Q(\sqrt{-1}))$ are finite (1.15) [36] table 1. Then the same argument as in the proof for $m = 6$ gives a contradiction.
Case \( m = 3 \) (\( N = 9, 12, 15 \)): In all the cases for \( N = 9, 12 \) and 15,
\[ \pi(x) \otimes \kappa(p) = C \otimes \kappa(p) \] for a prime \( p \) of \( k = \mathbb{Q}(\sqrt{-3}) \) lying over the rational prime 7 and for \( k \)-rational cusps \( C(1.12) \). The modular curves \( X_6(3, 9) \) and \( X_6(3, 12) \) are elliptic curves over \( \mathbb{Q} \) with complex multiplication \( \mathbb{Q}(\sqrt{-3}) \), the restriction of scalars \( \text{Re}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(X_6(3, N)) \) \( (N = 9, 12) \) are isogenous over \( \mathbb{Q} \) to the products \( X_6(3, N) \times X_6(3, N) \). Further \( \text{Re}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(X_6(3, N)) \) is isogenous over \( \mathbb{Q} \) to an elliptic curve with conductor 15 \( (1.15) \) \( (1.13) \). Then \( \#J_6(3N)(\mathbb{Q}(\sqrt{-3})) < \infty \) for \( N = 9, 12 \) and 15 \( (1.13) \). The same argument as above gives contradictions.

Case \( m = 2 \) (\( N = 14, 16, 18 \)):
\( N = 14 \): The modular curve \( X_6(2, 14) \sim X_6(28) \) has the hyperelliptic involution \( \nu \) (see \( [36] \) table 5). Let \( p \) be a prime of \( k \) lying over the rational prime 3. Then \( \pi(x) \otimes \kappa(p) = C \otimes \kappa(p) \), \( \pi(x^*) \otimes \kappa(p) = C_\sigma \otimes \kappa(p) \) for \( \mathbb{Q} \)-rational cusps \( C \) and \( C_\sigma \). These cusps \( C \) and \( C_\sigma \) are represented by \( (G_m \times \mathbb{Z}/14\mathbb{Z}, A_2, B_{14}) \) and \( (G_m \times \mathbb{Z}/14\mathbb{Z}, A_2, B_{14}) \) such that \( A_2 \supset \{1\} \times 2\mathbb{Z}/14\mathbb{Z} \) and \( B_{14} \supset \{1\} \times 2\mathbb{Z}/14\mathbb{Z} \) \( (1.12) \). Let \( i(x) = \text{cl}(x + (x^*) - (C) - (C_\sigma)) \) be the \( \mathbb{Q} \)-rational section of \( J_6(2, 14) \). Then \( i(x) = 0 \) and \( i(x) + (x^*) \sim (C) + (C_\sigma) \), since \( \#J_6(2, 14)(\mathbb{Q}) < \infty \) \( (1.4) \). But as noted as above, \( \nu(C) \neq C_\sigma \).

\( N = 16 \): Let \( \iota \) be a generator of the covering group of \( X_6(32) \rightarrow X_6(2, 16) \) and \( \#J_{16}(\mathbb{Q}) < \infty \) \( (1.4) \). Let \( p \) be a prime of \( k \) lying over the rational prime 3. Then \( x \otimes \kappa(p) = C \otimes \kappa(p) \), \( x^* \otimes \kappa(p) = C_\sigma \otimes \kappa(p) \) for \( \mathbb{Q} \)-rational cusps \( C \) and \( C_\sigma \). These cusps \( C \) and \( C_\sigma \) are represented respectively by \( (G_m \times \mathbb{Z}/16\mathbb{Z}, A_2, B_{16}) \), \( (G_m \times \mathbb{Z}/16\mathbb{Z}, A_2, B_{16}) \), where \( A_2 \) and \( B_{16} \) are points of order \( n \) such that \( A_2, B_{16} \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \) (see loc. cit.). Denote also by \( x, x^*, C \) and \( C_\sigma \) the images of \( x, x^*, C \) and \( C_\sigma \) under the natural morphism of \( X_6(2, 16) \) to \( X_6(16) \).

\( N = 18 \): Let \( p \) be a prime of \( k \) lying over the rational prime 5 and put \( R = (\mathbb{S}^2)_{p, n} \). By the condition \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \subset E(k), E_{18} \otimes \kappa(p) = G_m \times \mathbb{Z}/18n\mathbb{Z} \) for an integer \( n \geq 1 \) \( (1.12) \). Then \( x \otimes \kappa(p) = C \otimes \kappa(p) \), \( x^* \otimes \kappa(p) = C_\sigma \otimes \kappa(p) \) for \( \mathbb{Q} \)-rational cusps \( C \) and \( C_\sigma \). These cusps \( C \) and \( C_\sigma \) are represented respectively by \( (G_m \times \mathbb{Z}/18\mathbb{Z}, Q_5, \pm P_{18}) \), \( (G_m \times \mathbb{Z}/18\mathbb{Z}, Q_5, \pm Q_{18}) \), where \( P_{18}, Q_{18} \) are points of order \( n \) such that \( P_{18}, Q_{18} \in \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \) (see loc. cit.). Denote also by \( x, x^*, C \) and \( C_\sigma \) the images of \( x, x^*, C \) and \( C_\sigma \) under the natural morphism of \( X_6(2, 18) \) to \( X_6(18) \):

\[ \begin{pmatrix} F, B_{18} \pm B_{18} \end{pmatrix} \mapsto \begin{pmatrix} F, \pm B_{18} \end{pmatrix}. \]

Let \( i(x) = \text{cl}(x + (x^*) - (C) - (C_\sigma)) \) be the \( \mathbb{Q} \)-rational section of \( J_6(18) \).
Since \( \#J(18)(\mathbb{Q}) < \infty \) (1.4), \( i(x) = 0 \) and \((x') \sim (C) + (C')\). The modular curve \( X(18) \) has the hyperelliptic involution \( \tau = w_3[5] \):

\[
(F, \pm Q_0) \mapsto (F/\langle Q_0 \rangle, \pm (Q'_0 + 5Q_0) \mod \langle Q_0 \rangle),
\]

where \( Q_0, Q'_0 \) are points of order 2 with \( Q_0 \in \langle Q_0 \rangle \) and \( Q'_0 \in \langle Q_0 \rangle \). Then \( x' = \lambda(x) \), so there exists an isomorphism \( \lambda \):

\[
\lambda: (E', \pm P_{18}) \longrightarrow (E/\langle 9P_{18} \rangle, \pm (P' + 5P_{18}) \mod \langle 9P_{18} \rangle),
\]

where \( P' \) is a point of order 2 not contained in \( \langle P_{18} \rangle \). Since \( x \otimes \kappa(\rho) \) is a cusp, \( \lambda \) is defined over a quadratic extension \( K \) of \( k \) and \( \lambda' = \pm \lambda \) for \( 1 \neq \tau \in \text{Gal}(K/k) \). Then \( \lambda(P_{18}) = \varepsilon(P' + 5P_{18}) \mod \langle 9P_{18} \rangle \) 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 \( \lambda'(P_{18}) = (\lambda(P_{18}))' = (\lambda(P_{18}))' = \lambda(P_{18}) \). Thus \( \lambda' = \lambda \) and \( \lambda \) is defined over \( k \). Then \( \lambda \) induces the isomorphism

\[
\lambda: (E', P'_{18}, P'_0) \longrightarrow (E/\langle 9P_{18} \rangle, \lambda(P'_0), \varepsilon(P' + 5P_{18}) \mod \langle 9P_{18} \rangle).
\]

Let \( \mu: E \to E/\langle 9P_{18} \rangle \) be the natural morphism and put \( B = \lambda^{-1}[0, \lambda(P'_0)] \). 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 \( \gamma, \gamma' \) be the \( k \)-rational points on \( X_0(72) \) represented by the triples \((E, B, A')\) and \((E', B', A'')\), respectively. Noting that \( B \not\subseteq P' \) and \( B \in 9P_{18} \), we see that \( \gamma \otimes \kappa(\rho) = C' \otimes \kappa(\rho) \) and \( \gamma' \otimes \kappa(\rho) = C'' \otimes \kappa(\rho) \) for \( Q \)-rational cusps \( C \) and \( C' \) (1.12). The remaining part of the proof is the same as that for the case \( X_0(36) \).

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

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


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


https://doi.org/10.1017/S0027763000000281 Published online by Cambridge University Press
[29] K. Rubin, Congruences for special values of \(L\)-functions of elliptic curves with
[30] J. P. Serre, Propriétés galoisienne des points d’ordre fini des courbes elliptiques,
[31] ——, \(p\)-torsion des courbes elliptiques (d’après Y. Manin), Sèm. Boubaki 1969/70,
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
[34] A. Weil, Adèles and algebraic groups, Lecture Notes, Inst. for Advanced Study,
Princeton, N.J.
[36] Modular functions of one variable IV (ed. by B. J. Birch and W. Kuyk), Lecture

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