Points on $X_0^+(N)$ over quadratic fields

by

Keisuke Arai and Fumiyuki Momose (Tokyo)

1. Introduction. In this article, we study points on the modular curve $X_0^+(N)$ over quadratic fields, and show that such points consist of cusps and CM points under certain conditions.

Let $N \geq 1$ be an integer. Let $X_0(N)$ be the modular curve over $\mathbb{Q}$ associated to the subgroup $\{ (\ast \ast) \} \subseteq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (cf. [5]). A non-cuspidal point on $X_0(N)$ corresponds to a pair $(E, A)$ where $E$ is an elliptic curve and $A$ is a cyclic subgroup of $E$ of order $N$. For rational points on $X_0(N)$, we know the following.

Theorem 1.1 ([8, p. 129, Theorem 1]). If $N > 163$, then $X_0(N)(\mathbb{Q}) = \{ \text{cusps} \}$.

The second author studied points on $X_0(N)$ over quadratic fields when $N$ is a prime number.

Theorem 1.2 ([12, p. 330, Theorem B]). Let $K$ be a quadratic field which is not an imaginary quadratic field of class number one. Then for every sufficiently large prime number $p$, we have $X_0(p)(K) = \{ \text{cusps} \}$.

For any number field $K$, it seems likely that

$$X_0(N)(K) = \{ \text{cusps, CM points} \}$$

for every sufficiently large integer $N$ (cf. [16, p. 187]). But this still remains unsolved. Here a point $x$ on a modular curve (e.g. $X_0(N)$, $X_0^+(N)$ defined below) is called a CM point if $x$ is represented by an elliptic curve with complex multiplication.

Define an involution $w_N$ on $X_0(N)$ by

$$(E, A) \mapsto (E/A, E[N]/A),$$
where $E[N]$ is the kernel of multiplication by $N$ in $E$. Put

$$X_0^+(N) := X_0(N)/w_N.$$

We have the following open question: For a number field $K$, does

$$X_0^+(N)(K) = \{\text{cusps, CM points}\}$$

hold for every sufficiently large integer $N$? Notice that there are arbitrarily large $N$ such that $X_0^+(N)(\mathbb{Q}) = \{\text{cusps}\}$ does not hold. We know the following partial answers (Theorem 1.3, Theorem 1.5) to the above question.

**Theorem 1.3** ([2]). For every sufficiently large prime number $p$, we have $X_0^+(p^2)(\mathbb{Q}) = \{\text{cusps, CM points}\}$.

**Remark 1.4.** We have a natural isomorphism $X_0^+(p^2) \cong X_{\text{split}}(p)$, where $X_{\text{split}}(p)$ is the modular curve (over $\mathbb{Q}$) associated to the subgroup $\{(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}) , (\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}) \} \subseteq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $p$ be a prime number. We have an involution $w_p$ on $X_0(p)$ as above. By abuse of notation, we also write $w_p$ for the induced map $J_0(p) \to J_0(p)$.

Put

$$J_0^-(p) := J_0(p)/(1 + w_p)J_0(p).$$

Let

$$C := \langle cl((0) - (\infty)) \rangle \subseteq J_0(p)(\mathbb{Q})$$

be the subgroup generated by the divisor class $cl((0) - (\infty))$ (for the precise definition of the cusps $0$ and $\infty$, see the next section). Then $C = J_0(p)(\mathbb{Q})_{\text{tor}}$ (the torsion subgroup of $J_0(p)(\mathbb{Q})$) and $C$ maps isomorphically to $J_0^-(p)(\mathbb{Q})_{\text{tor}}$ by the natural map ([6] p. 143, Corollary (1.4), cf. [14] p. 229]). By abuse of notation we identify $C = J_0^-(p)(\mathbb{Q})_{\text{tor}}$. The order of $C$ is equal to the numerator of $\frac{p-1}{12}$ ([14] p. 228, Theorem) or [6] p. 98, Proposition (11.1)).

**Theorem 1.5** ([11] p. 269, Theorem (0.1), cf. [9], [10]). Let $N$ be a composite number. If $N$ has a prime divisor $p$ which satisfies the following conditions (1) and (2), then $X_0^+(N)(\mathbb{Q}) = \{\text{cusps, CM points}\}$.

1. $p \geq 17$ or $p = 11$.
2. $p \neq 37$ and $\sharp J_0^-(p)(\mathbb{Q}) < \infty$.

We generalize Theorem 1.5 to quadratic fields. The following is the main theorem of this article.

**Theorem 1.6.** Let $N$ be a composite number. Let $p$ be a prime divisor of $N$ such that $(p = 11$ or $p \geq 17$) and $p \neq 37$. Suppose $\text{ord}_p N = 1$ if $p = 11$. Let $K$ be a quadratic field where $p$ is unramified. Assume $X_0(N)(K) = \{\text{cusps}\}$ and $J_0^-(p)(K) = C$. Then $X_0^+(N)(K) = \{\text{cusps, CM points}\}$. 
Remark 1.7. Since the modular curve $X_0(37)$ is peculiar ([15]), we exclude $p = 37$ in the above theorems. But we have recently shown that Theorem 1.5 holds even if $p = 37$, and have generalized the result to certain imaginary quadratic fields ([1]).

Remark 1.8. (1) For $N$ as in Theorem 1.5, we have $X_0(N)(\mathbb{Q}) = \{\text{cusps}\}$ ([8, pp. 129–131]).

(2) The assumption $X_0(N)(K) = \{\text{cusps}\}$ in Theorem 1.6 is usually satisfied by Theorem 1.2.

We have the following examples of the condition $J_0^-(p)(K) = C$ in Theorem 1.6. For a number field $K$, let $h_K$ be the class number of $K$.

Proposition 1.9. Let $K$ be an imaginary quadratic field.

(1) Suppose 11 does not split in $K$ and 5 does not divide $h_K$. Then $J_0^-(11)(K) = C$.

(2) Suppose 17 does not split in $K$ and 2 does not divide $h_K$. Then $J_0^-(17)(K) = C$.

(3) Suppose 19 does not split in $K$ and 3 does not divide $h_K$. Then $J_0^-(19)(K) = C$.

In Section 2, we prepare the necessary material on modular curves. In Section 3, we introduce a key proposition (Proposition 3.1) and from it we deduce Theorem 1.6. In Section 4, we prove Proposition 3.1. In Section 5, we prove Proposition 1.9.

2. Modular curves. For a prime number $p$, let $g : X_0(p) \to X_0^+(p)$ be the quotient map. We know that the Jacobian variety $J_0^+(p)$ of $X_0^+(p)$ is isomorphic to $(1 + w_p)J_0(p)$ and there is an exact sequence of abelian varieties

$$0 \to J_0^+(p) \xrightarrow{g^*} J_0(p) \xrightarrow{u} J_0^-(p) \to 0,$$

where $g^*$ is the pull back and $u$ is the quotient map ([11, p. 278]).

For an integer $N \geq 1$, let $\mathcal{X}_0(N)$ be the normalization of the composite

$$X_0(N) \xrightarrow{j} X_0(1) = \mathbb{P}_\mathbb{Q}^1 \subseteq \mathbb{P}_\mathbb{Z}^1,$$

where $j : (E, A) \mapsto E$. If $p$ is a prime divisor of $N$ with $r = \text{ord}_p N$, then the special fiber $\mathcal{X}_0(N) \otimes \mathbb{F}_p$ has $r + 1$ irreducible components $E_0, E_1, \ldots, E_r$. They are defined over $\mathbb{F}_p$ and intersect at the supersingular points. Let $\zeta = \zeta_N$ be a primitive $N$th root of unity. For each positive divisor $d$ of $N$ and an integer $i$, $0 \leq i < d$, prime to $d$, let $A_{d,i}$ be the subgroup of $\mathbb{G}_m \times \mathbb{Z} / (N/d)\mathbb{Z}$ generated by $(\zeta^i, 1 \text{ mod } N/d)$. Let $(\binom{i}{d})$ be the cuspidal section of $\mathcal{X}_0(N)$ which is represented by the pair $(\mathbb{G}_m \times \mathbb{Z} / (N/d)\mathbb{Z}, A_{d,i})$ for the integers $d, i$ as above. For $d = 1, N$, we write $0 = \binom{0}{1}$ and $\infty = \binom{1}{N}$. We choose the irreducible
components $E_t$ so that $(\frac{t}{d}) \otimes \mathbb{F}_p$ are sections of $E_t$ for a positive divisor $d$ of $N$ with $t = \text{ord}_p \, d$. For $0 \leq t \leq r$, let $E_t^h$ be the open subscheme of $E_t$ obtained by excluding the supersingular points.

The special fiber $X_0^+(p) \otimes \mathbb{Z}_p \mathbb{F}_p$ has $g_0(p) + 1$ supersingular points. They can be described as follows. Let $\alpha_i, \alpha_i' := w_p(\alpha_i)$ be the non-$\mathbb{F}_p$-rational supersingular points on $X_0^+(p) \otimes \mathbb{Z}_p \mathbb{F}_p$ for $1 \leq i \leq g_0^+ (p)$, and let $\beta_i$ be the $\mathbb{F}_p$-rational supersingular points on $X_0^+(p) \otimes \mathbb{Z}_p \mathbb{F}_p$ for $1 \leq i \leq g_0(p) - 2g_0^+(p) + 1$. The involution $w_p$ exchanges $\alpha_i$ and $\alpha'_i$ and fixes $\beta_i$ (\cite{11} p. 279).

For a finite abelian group $G$ and an integer $n \geq 1$, let $G^{(n)}$ be the prime-to-$n$ subgroup of $G$. For an abelian group (or a commutative group scheme) $G$ and an integer $n$, let $G[n]$ be the kernel of multiplication by $n$ in $G$. For a group scheme $G$, let $G^0$ be the connected component of the identity in $G$. For a morphism of schemes $X \to S$, let $X^{\text{sm}}$ be the smooth locus of $X$. For a prime number $p$, let $\mathbb{Q}_p^{\text{unr}}$ be the maximal unramified extension of $\mathbb{Q}_p$, and let $\mathbb{Z}_p^{\text{unr}}$ be the ring of integers of $\mathbb{Q}_p^{\text{unr}}$. For a number field or a discrete valuation field $L$, let $\mathcal{O}_L$ be the ring of integers. For an abelian variety $J$ over a number field or a discrete valuation field $L$, let $J/\mathcal{O}_L$ be the Néron model of $J$ over $\mathcal{O}_L$ (later we take $J_0(p)$ or $J_0^- (p)$ as $J$).

Let $p$ be a prime number and $M \geq 1$ be an integer. Let

$$\pi : X_0(pM) \to X_0(p), \quad (E, A) \mapsto (E, A[p]).$$

Define

$$h : X_0(pM) \to J_0(p), \quad h(x) := cl((w_p \pi(x)) - (\pi w_{pM}(x))).$$

Put

$$\tilde{h}^- : X_0(pM) \xrightarrow{h} J_0(p) \to J_0^- (p),$$

where $J_0(p) \to J_0^- (p)$ is the quotient map. The map $\tilde{h}^-$ factors as $X_0(pM) \to X_0^+(pM) \to J_0^- (p)$, where $X_0(pM) \to X_0^+(pM)$ is the quotient map. We call the induced map $h^- : X_0^+(pM) \to J_0^- (p)$. Thus we have the following commutative diagram:

$$\begin{array}{ccc}
X_0(pM) & \xrightarrow{h} & J_0(p) \\
\downarrow & & \downarrow \\
X_0^+(pM) & \xrightarrow{h^-} & J_0^- (p)
\end{array}$$

See \cite{11} p. 2276.

3. Key proposition

**Proposition 3.1.** Let $K$ be a quadratic field. Let $p$ be a prime number such that $p = 11$ or $p \geq 17$. Let $M \geq 2$ be an integer and suppose $X_0(pM)(K) = \{\text{cusps}\}$. Let $y \in X_0^+(pM)(K)$ be a non-cuspidal point, and $x,$
\(w_{p,M}(x)\) be sections of the fiber \(X_0(pM)_y\). Let \(L\) be the quadratic extension of \(K\) over which \(x\) and \(w_{p,M}(x)\) are defined. Take a prime \(p\) of \(L\) above \(p\), and let \(\kappa(p)\) be the residue field of \(p\). Assume \(p \nmid M\) if \(p = 11\).

1. If \(p \mid M\) or \(x \otimes \kappa(p)\) is not a supersingular point, then \(h(x) \otimes \kappa(p)\) is a section of the connected component \((J_0(p)/\mathcal{O}_L \otimes \kappa(p))^0\) of the identity.

2. Suppose otherwise (i.e. \(p \nmid M\) and \(x \otimes \kappa(p)\) is a supersingular point).

   2-a. If one of the following three conditions is satisfied, then \(h(x) \otimes \kappa(p)\) is a section of \((J_0(p)/\mathcal{O}_L \otimes \kappa(p))^0\).
   
   - \(p\) is unramified in \(L/\mathbb{Q}\).
   - \(p\) is ramified in \(L/K\) and \(p\) is split in \(K\).
   - \(p\) is inert in \(L/K\) and \(p\) is ramified in \(K\).

   2-b. If \(p\) is ramified in \(L/K\) and \(p\) is inert in \(K\), then \(h^-(y) \otimes \kappa(p)\) is a section of \((J_0^-(p)/\mathcal{O}_L \otimes \kappa(p))^0\).

   Remark 3.2. (1) In Proposition 3.1, \(h^-(y) \otimes \kappa(p)\) is a section of \((J_0^-(p)/\mathcal{O}_L \otimes \kappa(p))^0\) in any case.

   (2) We do not treat the case where \(p\) is split in \(L/K\) and \(p\) is ramified in \(K\) in Proposition 3.1. In that case the proof does not work.

   (3) We do not use the last two cases of (2-a) in Proposition 3.1 for proving Theorem 1.6.

Lemma 3.3 ([11, p. 278 Proposition (2.8)]). Let \(L'\) be an extension of \(\mathbb{Q}_p^{unr}\) of degree \(\leq 2\). Let \(C \subseteq J_0^-(p)/\mathcal{O}_{L'}\) be the finite flat subgroup scheme generated by \(C\). Then \((C \otimes \mathbb{F}_p) \cap (J_0^-(p)/\mathcal{O}_{L'} \otimes \mathbb{F}_p)^0 = \{0\}\).

Proposition 3.4. Under the hypothesis in Proposition 3.1, further assume that \(p\) is unramified in \(K\) and \(J_0^-(p)(K) = C\). Then \(h^-(y) = 0\).

Proof. By assumption we have \(h^-(y) \in J_0^-(p)(K) = C\). Let \(L'\) be the maximal unramified extension of the completion \(L_p\). Then \([L' : \mathbb{Q}_p^{unr}] \leq 2\) because \(p\) is unramified in \(K\). Since \(h^-(y) \in C \subseteq J_0^-(p)(L')\), we have \(h^-(y) \in C(\mathcal{O}_{L'}) \subseteq J_0^-(p)/\mathcal{O}_{L'}(\mathcal{O}_{L'})\). Hence \(h^-(y) \otimes \mathbb{F}_p \in C(\mathbb{F}_p) \subseteq J_0^-(p)/\mathcal{O}_{L'}(\mathbb{F}_p)\). On the other hand \(h^-(y) \otimes \mathbb{F}_p \in (J_0^-(p)/\mathcal{O}_L \otimes \kappa(p))^0(\mathbb{F}_p) = (J_0^-(p)/\mathcal{O}_{L'} \otimes \mathbb{F}_p)^0(\mathbb{F}_p)\) by Proposition 3.1. Notice that taking the connected component is compatible with base change since \(J_0^-(p)\) is semi-stable ([11, p. 183, Corollary 4]). Then \(h^-(y) \otimes \mathbb{F}_p = 0\) by Lemma 3.3. Since the order of \(C\) is prime to \(p\), the group scheme \(C\) over \(\mathcal{O}_{L'}\) is étale. Therefore \(h^-(y) = 0\).

The condition \(h^-(y) = 0\) implies that \(y\) is a CM point since \(p \neq 37\) ([11, p. 274, Proposition (2.2)]).. Thus Theorem 1.6 follows from Proposition 3.1.

For simplicity write $N = pM$. Let $\tilde{X}_0(p) \rightarrow \text{Spec } O_L$ be the minimal proper regular model of $X_0(p) \otimes \mathbb{Q} L$. We may canonically identify $X_0(N)(O_L) = X_0(N)(L)$ and $X_0(p)(O_L) = X_0(p)(L) = \tilde{X}_0(p)(O_L)$. If $w_p\pi(x)$ and $\pi w_N(x)$ define sections of the same irreducible component of $\tilde{X}_0(p)_{\text{sm}} \otimes \kappa(p)$, then $h(x) \otimes \kappa(p)$ is a section of $(J_0(p)/O_L \otimes \kappa(p))^0$ ([6, p. 179, Proposition (1.4)]). Put $r = \text{ord}_p N$. If $x \otimes \kappa(p)$ is a section of $E_0^h \cup E_r^h$, then $w_p\pi(x)$ and $\pi w_N(x)$ define sections of the same irreducible component of $\tilde{X}_0(p)_{\text{sm}} \otimes \kappa(p)$. To see this, we use the following: $\pi$ maps $E_0$ to $E_0$ and $E_r$ to $E_1$; $w_N$ exchanges $E_0$ and $E_r$; $w_p$ exchanges $E_0$ and $E_1$ ([10, p. 446]). Notice that here we use the symbol $E_i$ in two ways.

If $p \mid M$, then $x \otimes \kappa(p)$ is a section of $E_0^h \cup E_r^h$ since $e_{L/\mathbb{Q}}(p) \leq 4$ and $3e_{L/\mathbb{Q}}(p) < p - 1$ ([10, p. 452, Corollary (2.3)], cf. [13, p. 159, Main Theorem]). Here we used $p \geq 17$. If $p \nmid M$ and $x \otimes \kappa(p)$ is not a supersingular point, then $x \otimes \kappa(p)$ is a section of $E_0^h \cup E_r^h$ for $r = 1$.

From now on we consider the case when $p \nmid M$ and $x \otimes \kappa(p)$ is a supersingular point.

**CASE (i): $p$ is unramified in $L/\mathbb{Q}$.** In this case $j(x \otimes \kappa(p)) = 0$ or 1728, and

$$\hat{O}_{X_0(N) \otimes \mathbb{Z}_p^{\text{unr}}, x} \cong \mathbb{Z}_p^{\text{unr}}[[u, v]]/(uv - p^i)$$

where $i = 3$ (resp. 2) if $j(x \otimes \kappa(p)) = 0$ (resp. 1728) ([6, p. 63]). Here $\hat{O}_{X_0(N) \otimes \mathbb{Z}_p^{\text{unr}}, x}$ is the completion of the local ring $O_{X_0(N) \otimes \mathbb{Z}_p^{\text{unr}}, x}$ at the maximal ideal. Since $w_N$ is an automorphism, we have

$$\hat{O}_{X_0(N) \otimes \mathbb{Z}_p^{\text{unr}}, w_N(x)} \cong \mathbb{Z}_p^{\text{unr}}[[u, v]]/(uv - p^i).$$
Then \( j(w_N(x) \otimes \kappa(\mathfrak{p})) = j(x \otimes \kappa(\mathfrak{p})) = 0 \) (resp. 1728). Hence \( j(\pi w_N(x) \otimes \kappa(\mathfrak{p})) = j(\pi(x) \otimes \kappa(\mathfrak{p})) \). Since \( w_p \) fixes all the \( \mathbb{F}_p \)-rational supersingular points on \( X_0(p) \otimes \mathbb{F}_p \), we have \( \pi w_N(x) \otimes \kappa(\mathfrak{p}) = \pi(x) \otimes \kappa(\mathfrak{p}) = w_p \pi(x) \otimes \kappa(\mathfrak{p}) \).

If \( j(x \otimes \kappa(\mathfrak{p})) = 1728 \), then \( w_p \pi(x) \otimes \kappa(\mathfrak{p}) \) and \( \pi w_N(x) \otimes \kappa(\mathfrak{p}) \) define sections of the unique exceptional irreducible component \( B \) of \( \tilde{Y}_0(p)^{sm} \otimes \mathcal{O}_L \kappa(\mathfrak{p}) \). Therefore \( h(x) \otimes \kappa(\mathfrak{p}) \) is a section of \( (J_0(p)/\mathcal{O}_L \otimes \kappa(\mathfrak{p}))^0 \).

Assume \( j(x \otimes \kappa(\mathfrak{p})) = 0 \). Then \( \tilde{Y}_0(p)^{sm} \otimes \mathcal{O}_L \kappa(\mathfrak{p}) \) has two exceptional irreducible components, say \( B_1, B_2 \). Also \( \tilde{Y}_0(N)^{sm} \otimes \mathcal{O}_L \kappa(\mathfrak{p}) \) has two exceptional irreducible components over \( x \otimes \kappa(\mathfrak{p}) \) (resp. \( w_N(x) \otimes \kappa(\mathfrak{p}) \)), say \( A_1, A_2 \) (resp. \( A_3, A_4 \)). See the figure below. We may assume \( x \otimes \kappa(\mathfrak{p}) \) is a section of \( A_1^{sm} \). Then \( w_N(x) \otimes \kappa(\mathfrak{p}) \) is a section of \( A_4^{sm} \). Hence \( \pi(x) \otimes \kappa(\mathfrak{p}) \) (resp. \( \pi w_N(x) \otimes \kappa(\mathfrak{p}) \)) is a section of \( B_1^{sm} \) (resp. \( B_2^{sm} \)). Therefore \( w_p \pi(x) \otimes \kappa(\mathfrak{p}) \) and \( \pi w_N(x) \otimes \kappa(\mathfrak{p}) \) are sections of the same irreducible component \( B_2^{sm} \), and so \( h(x) \otimes \kappa(\mathfrak{p}) \) is a section of \( (J_0(p)/\mathcal{O}_L \otimes \kappa(\mathfrak{p}))^0 \). Note that \( x \otimes \kappa(\mathfrak{p}) \) and \( w_N(x) \otimes \kappa(\mathfrak{p}) \) may be equal in \( X_0(N) \otimes \mathbb{Z} \kappa(\mathfrak{p}) \). Then \( A_1 = A_3, A_2 = A_4 \).
CASE (ii): \( p \) is ramified in \( L/K \) and \( p \) is split in \( K \). Let \( \sigma \in \Gal(L/K) \) be the non-trivial element. Since \( p \) is ramified in \( L/K \), we have \( x^\sigma \otimes \kappa(p) = x \otimes \kappa(p) \). Since \( \kappa(p) = \mathbb{F}_p \), the sections \( x \otimes \kappa(p) \) and \( w_N(x) \otimes \kappa(p) = x^\sigma \otimes \kappa(p) \) are \( \mathbb{F}_p \)-rational. Thus \( \pi(x) \otimes \kappa(p) \) and \( \pi w_N(x) \otimes \kappa(p) \) are also \( \mathbb{F}_p \)-rational. Since \( \pi w_N(x) \otimes \kappa(p) = \pi(x) \otimes \kappa(p) = \pi x = \pi \in \mathfrak{X}_0(p)(\kappa(p)) \). If \( j(x \otimes \kappa(p)) \neq 0, 1728 \), then \( \pi_x \otimes \kappa(p) \) and \( \pi w_N(x) \otimes \kappa(p) \) correspond to sections in the unique exceptional irreducible component of \( \mathfrak{Y}_0(p)^{\text{sm}} \otimes \mathcal{O}_L \kappa(p) \).

Suppose \( j(x \otimes \kappa(p)) = 0, 1728 \). Let \( \mathfrak{X}_0(N) \) (resp. \( \mathfrak{X}_0(p) \)) be the minimal regular model of \( X_0(N) \) (resp. \( X_0(p) \)) over \( \mathbb{Z}_p \). Then \( \mathfrak{Y}_0(p) \otimes \mathcal{O}_L \) is obtained from \( \mathfrak{X}_0(p) \otimes \mathcal{O}_L(p) \) by blowing-up at the singular points of the special fiber. Assume \( j(x \otimes \kappa(p)) = 1728 \). If \( x \otimes \kappa(p) \) define a section of \( \mathfrak{X}_0(N)^{\text{sm}} \otimes \kappa(p) \), then \( \pi(x) \otimes \kappa(p), \pi w_N(x) \otimes \kappa(p) \) and \( w_p \pi(x) \otimes \kappa(p) \) define sections of the unique irreducible component of \( \mathfrak{X}_0(p)^{\text{sm}} \otimes \kappa(p) \). Hence \( \pi(x) \otimes \kappa(p), \pi w_N(x) \otimes \kappa(p) \) and \( w_p \pi(x) \otimes \kappa(p) \) define sections of the same irreducible component of \( \mathfrak{Y}_0(p)^{\text{sm}} \otimes \kappa(p) \).

\[
\mathfrak{X}_0(N) \otimes \kappa(p) \quad \xrightarrow{\text{blow-up}} \quad \mathfrak{X}_0(N) \otimes \kappa(p) \quad \xrightarrow{\text{blow-up}} \quad \mathfrak{X}_0(p) \otimes \kappa(p)
\]

\[
\pi(x) \quad \xrightarrow{\text{blow-up}} \quad \pi w_N(x) \quad \xrightarrow{\text{blow-up}} \quad \mathfrak{Y}_0(p) \otimes \kappa(p)
\]

If \( x \otimes \kappa(p) \) corresponds to a singular point of \( \mathfrak{X}_0(N) \otimes \kappa(p) \), then by an easy calculation, \( w_p \pi(x) \otimes \kappa(p) \) and \( \pi w_N(x) \otimes \kappa(p) \) define sections of the same irreducible component of \( \mathfrak{Y}_0(p)^{\text{sm}} \otimes \kappa(p) \) (see the figure below).
Points on $X_0^+(N)$ over quadratic fields

Assume $j(x \otimes \kappa(p)) = 0$. Looking at a similar figure, we can show $w_p \pi(x) \otimes \kappa(p)$ and $\pi w_N(x) \otimes \kappa(p)$ define sections of the same irreducible component of $\tilde{Y}_0(p)^{\text{sm}} \otimes \kappa(p)$.

**Case (iii):** $p$ is inert in $L/K$ and $p$ is ramified in $K$. We have $\kappa(p) = \mathbb{F}_{p^2}$. The sections $x$ and $w_N(x) = x^\sigma$ correspond to Gal($L/K$)-conjugate $L$-rational points. Hence $\pi(x) \otimes \kappa(p)$ and $\pi w_N(x) \otimes \kappa(p)$ correspond to Gal($\mathbb{F}_{p^2}/\mathbb{F}_p$)-conjugate $\mathbb{F}_{p^2}$-rational supersingular points. If one of them is $\mathbb{F}_p$-rational, they coincide. Then $w_p \pi(x) \otimes \kappa(p) = \pi(x) \otimes \kappa(p) = \pi w_N(x) \otimes \kappa(p) \in X_0(p)(\mathbb{F}_p)$. (When $j(x \otimes \kappa(p)) = 0, 1728$, look at some figures.) Otherwise they correspond to distinct but Gal($\mathbb{F}_{p^2}/\mathbb{F}_p$)-conjugate $\mathbb{F}_{p^2}$-rational supersingular points. Then $w_p \pi(x) \otimes \kappa(p) = \pi w_N(x) \otimes \kappa(p) \in X_0(p)(\kappa(p))$. In any case $w_p \pi(x) \otimes \kappa(p)$ and $\pi w_N(x) \otimes \kappa(p)$ define sections of the same irreducible component of $\tilde{Y}_0(p)^{\text{sm}} \otimes \kappa(p)$.

**Case (iv):** $p$ is ramified in $L/K$ and $p$ is ramified in $K$. We have $\kappa(p) = \mathbb{F}_p$ and $x \otimes \kappa(p) = x^\sigma \otimes \kappa(p) = w_N(x) \otimes \kappa(p) \in X_0(N)(\mathbb{F}_p)$. Then $\pi(x) \otimes \kappa(p) = \pi w_N(x) \otimes \kappa(p)$, which is $\mathbb{F}_p$-rational. Hence $w_p \pi(x) \otimes \kappa(p) = \pi(x) \otimes \kappa(p) = \pi w_N(x) \otimes \kappa(p) \in X_0(p)(\mathbb{F}_p)$. For $j(x \otimes \kappa(p)) \neq 0, 1728$, see the figures below (there are two cases).
For \( j(x \otimes \kappa(p)) = 0, 1728 \) we need more complicated figures, but we omit them.

**Case (v): p is ramified in \( L/K \) and \( p \) is inert in \( K \).** We have \( \kappa(p) = \mathbb{F}_p^2 \). Since \( L/K \) is ramified at \( p \), we have \( x \otimes \kappa(p) = x^\sigma \otimes \kappa(p) = w_N(x) \otimes \kappa(p) \). Hence \( \pi(x) \otimes \kappa(p) = \pi w_N(x) \otimes \kappa(p) \).

If \( \pi(x) \otimes \kappa(p) = \mathbb{F}_{p^2} \)-rational, we have \( w_p \pi(x) \otimes \kappa(p) = \pi(x) \otimes \kappa(p) = \pi w_N(x) \otimes \kappa(p) \in \mathcal{X}_0(p)(\mathbb{F}_p) \). (When \( j(x \otimes \kappa(p)) = 0, 1728 \), look at some figures.) Then \( w_p \pi(x) \otimes \kappa(p) \) and \( \pi w_N(x) \otimes \kappa(p) \) define sections of the same irreducible component of \( \tilde{\mathcal{Y}}_0(p)^{sm} \otimes_{\mathcal{O}_L} \kappa(p) \).

Suppose \( \pi(x) \otimes \kappa(p) \) is not \( \mathbb{F}_{p^2} \)-rational. Note that \( j(\pi(x) \otimes \kappa(p)) \neq 0, 1728 \) in this case. Then \( \pi w_N(x) \otimes \kappa(p) \) and \( \pi w_N(x) \otimes \kappa(p) \) correspond to distinct \( \mathbb{F}_{p^2} \)-rational supersingular points. Hence \( w_p \pi(x) \otimes \kappa(p) \) and \( \pi w_N(x) \otimes \kappa(p) \) define sections of two distinct exceptional irreducible components of \( \tilde{\mathcal{Y}}_0(p)^{sm} \otimes_{\mathcal{O}_L} \kappa(p) \). Let \( \mathcal{J} \) (resp. \( \mathcal{J}^+, \mathcal{J}^- \)) be the Néron model of \( J_0(p) \otimes \mathcal{L} \) (resp. \( J_0^+(p) \otimes \mathcal{L}_p, J_0^-(p) \otimes \mathcal{L}_p \)) over \( \mathcal{O}_{\mathcal{L}_p} \). Considering the ramification index \( e(L_p/\mathbb{Q}_p) = 2 < p - 1 \), we have an induced exact sequence

\[
0 \rightarrow \mathcal{J}^+ \rightarrow \mathcal{J} \rightarrow \mathcal{J}^-
\]

([4] p. 187, Theorem 4)). To simplify the notation let \( \mathcal{J}_s \) (resp. \( \mathcal{J}_s^+, \mathcal{J}_s^- \)) be the geometric special fiber \( \mathcal{J} \otimes_{\mathcal{O}_{\mathcal{L}_p}} \mathbb{F}_p \) (resp. \( \mathcal{J}^+ \otimes_{\mathcal{O}_{\mathcal{L}_p}} \mathbb{F}_p, \mathcal{J}^- \otimes_{\mathcal{O}_{\mathcal{L}_p}} \mathbb{F}_p \)). Then the natural composite map

\[
\mathcal{J}_s^+/(\mathcal{J}_s^+)^0 \rightarrow \mathcal{J}_s/(\mathcal{J}_s)^0 \rightarrow \mathcal{J}_s^-/(\mathcal{J}_s^-)^0
\]

is the zero map. Let \( \tilde{\mathcal{Y}}_0^+ \rightarrow \text{Spec} \mathcal{O}_{\mathcal{L}_p} \) be the minimal proper regular model of \( X_0^+(p) \otimes \mathbb{Q} \mathcal{L}_p \). Let \( \{C_i\} \) (resp. \( \{C'_j\} \)) be the set of irreducible components of \( \tilde{\mathcal{Y}}_0(p) \otimes \overline{\mathbb{F}}_p \) (resp. \( \tilde{\mathcal{Y}}_0^+ \otimes \overline{\mathbb{F}}_p \)). Let \( \mathcal{D} \) (resp. \( \mathcal{D}_+ \)) be the free abelian group generated by the divisors \( C_i \) (resp. \( C'_j \)). Let \( \mathcal{D}^0 \subseteq \mathcal{D} \) (resp. \( \mathcal{D}_+^0 \subseteq \mathcal{D}_+ \)) be the subgroup of divisors of degree 0. Let \( \alpha : \mathcal{D} \rightarrow \mathcal{D} \) (resp. \( \alpha_+ : \mathcal{D}_+ \rightarrow \mathcal{D}_+ \)) be the \( \mathbb{Z} \)-linear map defined by

\[
\alpha(B) = \sum_i (B, C_i) C_i \quad (\text{resp. } \alpha_+(B') = \sum_j (B', C'_j) C'_j)
\]

where \( (B, C_i) \) (resp. \( (B', C'_j) \)) is the intersection number. Then we have the following commutative diagram:

\[
\begin{array}{ccc}
\mathcal{J}_s^+/(\mathcal{J}_s^+)^0 & \longrightarrow & \mathcal{J}_s/(\mathcal{J}_s)^0 \\
\approx & \downarrow & \approx \\
\mathcal{D}_+^0/\alpha_+(\mathcal{D}_+) & \longrightarrow & \mathcal{D}^0/\alpha(\mathcal{D})
\end{array}
\]

where \( g^* \) is the natural map induced by the quotient map \( g : X_0(p) \rightarrow X_0^+(p) \) and the vertical maps are the natural isomorphisms ([6], p. 179, Proposition (1.4))). Let \( Z \) (resp. \( Z' \)) be the irreducible component of \( \tilde{\mathcal{Y}}_0(p) \otimes \overline{\mathbb{F}}_p \) over \( E_0 \).
We may assume \( w_p \pi(x) \otimes F_p = \alpha_1 \), \( \pi w_N(x) \otimes F_p = \alpha'_1 \) in \( \mathcal{X}_0(p) \otimes F_p \). Then \( w_p \pi(x) \otimes F_p \) (resp. \( \pi w_N(x) \otimes F_p \)) defines a section of \( F_1^{sm} \) (resp. \( F_2^{sm} \)) in \( \tilde{\mathcal{Y}}_0(p) \otimes F_p \). In the isomorphism \( J_s/(J_s)^0 \cong \mathcal{D}^0/\alpha(D) \), the section \( h(x) \otimes F_p \) corresponds to \( F_1 - F_2 \). We have \( F_1 - F_2 = \tilde{F}_1 - \tilde{F}_2 \in g^*(\mathcal{D}^0/\alpha_+ (D_+)) \subseteq \mathcal{D}^0/\alpha(D) \) by the discussion in [11] pp. 279–281 (especially by the line “\( g^*(\tilde{K}_i) = \tilde{F}_2i - \tilde{Z} = \tilde{F}_2i - \tilde{F}_2i \mod \alpha(D) \)” on p. 281). Therefore we get \( h^-(y) \otimes F_p = 0 \) in \( J_s^-/(J_s^-)^0 \).

Now we have completed the proof of Proposition 3.1 and hence that of Theorem 1.6.

5. Mordell–Weil groups over quadratic fields. In this section we prove Proposition 1.9. Notice that \( g_0(p) = 1 \) if and only if \( p \in \{11, 17, 19\} \). In this case we have \( J_0^- \approx X_0(p) \) and \( J_0(p)(\mathbb{Q}) = C \) ([6] p. 151, Theorem (4.1))). Let \( F \) (resp. \( G, H \)) be the Néron models of \( J_0(11) \) (resp. \( J_0(17), J_0(19) \)) over \( \mathbb{Z} \).

Proposition 5.1.

1. We have \( F(\mathbb{F}_2) = F(\mathbb{F}_4) \cong \mathbb{Z}/5\mathbb{Z} \). For any quadratic field \( K \), we have \( F(K)_{tor} = C \).

2. We have \( G(\mathbb{Q}(\sqrt{-1}))_{tor} \cong G(\mathbb{F}_5) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). For any quadratic field \( K \) other than \( \mathbb{Q}(\sqrt{-1}) \), we have \( G(K)_{tor} = C \).

3. We have \( H(\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z} \) and \( H(\mathbb{Q}(\sqrt{-3}))_{tor} \cong H(\mathbb{F}_4) \cong (\mathbb{Z}/3\mathbb{Z})^2 \). For any quadratic field \( K \) other than \( \mathbb{Q}(\sqrt{-3}) \), we have \( H(K)_{tor} = C \).

Proof. (1) Let \( f_{11} \) be the cusp form of weight 2 and level 11 corresponding to \( J_0(11) \). Then \( a_2(f_{11}) = -2 \) and \( a_3(f_{11}) = -1 \), where \( a_i(f_{11}) \) is the \( i \)th Fourier coefficient of \( f_{11} \) for \( i = 2, 3 \) ([3] p. 117]). We then have \( \# F(\mathbb{F}_2) = \# F(\mathbb{F}_3) = \# F(\mathbb{F}_4) = 5 \), \( \# F(\mathbb{F}_9) = 15 \). Now \( F(\mathbb{F}_2) = F(\mathbb{F}_4) \cong \mathbb{Z}/5\mathbb{Z} \) has been shown.

For any quadratic field \( K \), we have inclusions \( C = F(\mathbb{Q})[5] \subseteq F(K)[5] \subseteq F(K)_{tor}^{(2)} \subseteq F(\mathbb{F}_4) \cong \mathbb{Z}/5\mathbb{Z} \), where \( F(K)_{tor}^{(2)} \) is the prime-to-2 subgroup of
$F(K)_{tor}$ (the notation introduced in Section 2). Since $\#C = 5$, the above inclusions are all isomorphisms. Finally we show $F(K)_{tor}^{(2)} = F(K)_{tor}$. Since $F(K)[2] \hookrightarrow F(F_9)$ and $\#F(F_9) = 15$, we have $F(K)[2] = \{0\}$. Thus indeed $F(K)_{tor}^{(2)} = F(K)_{tor}$.

(2) Let $f_{17}$ be the cusp form of weight 2 and level 17 corresponding to $J_0(17)$. Then we know the Fourier coefficients $a_2(f_{17}) = -1$, $a_3(f_{17}) = 0$ and $a_5(f_{17}) = -2$ (loc. cit.). We then have $\#G(F_4) = 8$, $\#G(F_3) = 4$, $\#G(F_9) = 16$, $\#G(F_5) = 8$.

For any quadratic field $K$, we have an inclusion $\mathbb{Z}/4\mathbb{Z} \cong C = G(\mathbb{Q}) \subseteq G(K)_{tor}$. Since $G(K)_{tor}^{(2)} \hookrightarrow G(F_4)$ and $\#G(F_4) = 8$, we have $G(K)_{tor}^{(2)} = \{0\}$.

We know that $G(Q(\sqrt{-1}))$ has a subgroup which is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (see p. 103). Since $G(Q(\sqrt{-1}))[5] = \{0\}$, we have $G(Q(\sqrt{-1}))_{tor} = G(Q(\sqrt{-1}))_{tor}^{(5)} \hookrightarrow G(F_5)$. By using $\#G(F_5) = 8$, we conclude $G(Q(\sqrt{-1}))_{tor} \cong G(F_5) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Let $G_\mathbb{Q} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$. Let $\rho : G_\mathbb{Q} \to \text{GL}_2(\mathbb{F}_2)$ be the Galois representation determined by the $G_\mathbb{Q}$-action on $G(\overline{\mathbb{Q}})[2]$. Since $G(\mathbb{Q}) = C \cong \mathbb{Z}/4\mathbb{Z}$, we have $G(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. Then the image $r(G_\mathbb{Q})$ is conjugate to the subgroup $\{(0 1), (1 1)\}$. Since $G(Q(\sqrt{-1}))[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the restriction $r|_{G_{Q(\sqrt{-1})}}$ is trivial, where $G_{Q(\sqrt{-1})} = \text{Gal}(\overline{\mathbb{Q}}/Q(\sqrt{-1}))$ is the absolute Galois group of $Q(\sqrt{-1})$ considered as a subgroup of $G_\mathbb{Q}$. Then Ker $\rho$ corresponds to the quadratic field $Q(\sqrt{-1})$. So, for any quadratic field $K$ other than $Q(\sqrt{-1})$, the restriction $r|_{G_K}$ is not trivial. Then $G(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$. Since $G(K)_{tor}^{(2)} = \{0\}$ and $G(\mathbb{Q}) = C \cong \mathbb{Z}/4\mathbb{Z}$, we have $G(K)_{tor} \cong \mathbb{Z}/2^n\mathbb{Z}$ for $n \geq 2$.

Since $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong G(Q(\sqrt{-1}))_{tor} = G(Q(\sqrt{-1}))_{tor}^{(3)} \hookrightarrow G(F_9)$ and $\#G(F_9) = 16$, we have $G(F_9) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Let $G_{\mathbb{F}_3} = \text{Gal}(\overline{\mathbb{F}_3}/\mathbb{F}_3)$ be the absolute Galois group of $\mathbb{F}_3$. Let $\rho : G_{\mathbb{F}_3} \to \text{GL}_2(\mathbb{Z}/4\mathbb{Z})$ be the Galois representation determined by the $G_{\mathbb{F}_3}$-action on $G(\overline{\mathbb{F}_3})[4]$. Since $\mathbb{Z}/4\mathbb{Z} \cong C = G(\mathbb{Q}) = G(\mathbb{Q})_{tor} \hookrightarrow G(F_3)$ and $\#G(F_3) = 4$, we have $G(F_3) \cong \mathbb{Z}/4\mathbb{Z}$, and so we may assume that $\rho$ is of the form $\left( \begin{array}{cc} \chi & \ast \\ 0 & 1 \end{array} \right)$, where $\chi$ is the mod 4 cyclotomic character. Let $\overline{\rho} : G_{\mathbb{F}_3} \to \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$ be the restriction of $\rho$ modulo 2. Since $G(F_3)[2] \cong \mathbb{Z}/2\mathbb{Z}$, we have $\overline{\rho}(G_{\mathbb{F}_3}) = \{(0 1), (1 1)\}$. Since $\chi(G_{\mathbb{F}_3}) = \{1, -1\}$ and the Galois group $G_{\mathbb{F}_3}$ is topologically generated by one element, we have $\rho(G_{\mathbb{F}_3}) = \{(0 1), (1 1)\}$. 

Let $G_{\mathbb{F}_9} = \text{Gal}(\overline{\mathbb{F}_9}/\mathbb{F}_9)$ be the absolute Galois group of $\mathbb{F}_9$ considered as a subgroup of $G_{\mathbb{F}_3}$. Since $G(F_9)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the restriction $\overline{\rho}|_{G_{\mathbb{F}_9}}$ is trivial. Then $\rho(G_{\mathbb{F}_9}) \subseteq \{(0 1), (0 2)\}$, because $\chi|_{G_{\mathbb{F}_9}}$ is trivial. This combined with the above consideration of $\rho(G_{\mathbb{F}_3})$ implies that the restriction $\rho|_{G_{\mathbb{F}_9}}$ is trivial. Therefore $G(F_9) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. 

Points on $X_0^+(N)$ over quadratic fields
Hence, for any quadratic field $K$ other than $\mathbb{Q}(\sqrt{-1})$, we have $\mathbb{Z}/2^n\mathbb{Z} \cong G(K)_{\text{tor}} = G(K)^{(3)}_{\text{tor}} \hookrightarrow G(\mathbb{F}_9) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Since $n \geq 2$, we have $n = 2$. Therefore we conclude $G(K)_{\text{tor}} = C$.

(3) Let $f_{19}$ be the cusp form of weight 2 and level 19 corresponding to $J_0(19)$. Then $a_2(f_{19}) = 2$ and $a_5(f_{19}) = 3$ (loc. cit.). We then have $\sharp H(\mathbb{F}_2) = \sharp H(\mathbb{F}_5) = 3$, $\sharp H(\mathbb{F}_4) = 9$ and $\sharp H(\mathbb{F}_{25}) = 27$. Thus $H(\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z}$.

By [6, p. 125, Corollary (16.3)], we have $H[3] \cong \mathbb{Z}/3\mathbb{Z}$ as group schemes over $\mathbb{Z}$, where $\mu_3 = \text{Spec}(\mathbb{Z}[X]/(X^3 - 1))$. Then we have $H[3](\mathbb{Q}(\sqrt{-3})) \cong (\mathbb{Z}/3\mathbb{Z})^2$ and $H[3](K) \cong \mathbb{Z}/3\mathbb{Z}$ for any quadratic field $K$ other than $\mathbb{Q}(\sqrt{-3})$. Since $H(\mathbb{F}_{25})$ has an odd order, so do $H(\mathbb{Q}(\sqrt{-3}))_{\text{tor}}$ and $H(K)_{\text{tor}}$. Then we have inclusions $H[3](\mathbb{Q}(\sqrt{-3})) \subseteq H(\mathbb{Q}(\sqrt{-3}))_{\text{tor}} \hookrightarrow H(\mathbb{F}_4)$. Comparing the orders, we get $H(\mathbb{Q}(\sqrt{-3}))_{\text{tor}} \cong H(\mathbb{F}_4) \cong (\mathbb{Z}/3\mathbb{Z})^2$. So, for any quadratic field $K$ other than $\mathbb{Q}(\sqrt{-3})$, we have $C = H[3](K) \subseteq H(K)_{\text{tor}} \hookrightarrow H(\mathbb{F}_4) \cong (\mathbb{Z}/3\mathbb{Z})^2$. Therefore $H(K)_{\text{tor}} = H[3](K) = C$.

Proof of Proposition 1.9. It suffices to show $\sharp J_0(p)(K) < \infty$ for $p = 11, 17, 19$. But this is done in [7, p. 143, Corollary 1]. For $p = 11, 19$, the same method as in [1] p. 2278, Proposition 4.3] also works.

Acknowledgements. This work was supported in part by Japan Society for the Promotion of Science Core-to-Core Program [18005]; and Japan Society for the Promotion of Science Grant-In-Aid [19204002]. We would like to thank the anonymous referee for useful comments, which have helped us to improve Proposition 1.9(2) and Proposition 5.1(2).

References

Points on $X_0^+(N)$ over quadratic fields


Keisuke Arai
Department of Mathematics
School of Engineering
Tokyo Denki University
2-2 Kanda-Nishiki-cho, Chiyoda-ku
Tokyo, Japan 101-8457
E-mail: araik@mail.dendai.ac.jp

Fumiyuki Momose
Department of Mathematics
Faculty of Science and Engineering
Chuo University
1-13-27 Kasuga, Bunkyo-ku
Tokyo, Japan 112-8551
E-mail: momose@math.chuo-u.ac.jp

Received on 19.11.2010
and in revised form on 19.4.2011 (6555)