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

Keisuke Arai (Tokyo Denki University)

(joint work with Fumiyuki Momose)

Abstract: Momose proved that the $\mathbb{Q}$-rational points on the modular curve $X_0^+(N)$ consist of cusps and CM points under certain conditions. Here we generalize the previous result for quadratic fields.

Let $N \geq 1$ be an integer. Let $X_0(N)$ be the modular curve over $\mathbb{Q}$ associated to the subgroup $\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. 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 0.1. *(Mazur, 1978) If $N > 163$, then $X_0(N)(\mathbb{Q}) = \{cusps\}$.* □

Define an involution w_N on $X_0(N)$ by $(E, A) \longmapsto (E/A, E[N]/A)$, 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:

"Does $X_0^+(N)(\mathbb{Q}) = \{\text{cusps, CM points}\}$ hold for every sufficiently large N ?"

Here a CM point corresponds to an elliptic curve with complex multiplication. Notice that there is an arbitrarily large N such that $X_0^+(N)(\mathbb{Q}) = \{\text{cusps}\}$ does not hold. We know the following partial answers (Theorem 0.2, Theorem 0.4) to the question.

Theorem 0.2. *(Bilu-Parent, 2009) For every sufficiently large prime number p, we have $X_0^+(p^2)(\mathbb{Q}) = \{cusps, CM points\}$.* □

Remark 0.3. We have a natural isomorphism $X_0^+(p^2) \cong X_{split}(p)$, where $X_{split}(p)$ is the modular curve (over $\mathbb{Q}$) associated to the subgroup $\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

For a prime number p, let $J_0(p)$ be the Jacobian variety of $X_0(p)$ and put $J_0^-(p) := J_0(p)/(1 + w_p)J_0(p)$. Let $C := \langle cl((\mathbf{0}) - (\boldsymbol{\infty})) \rangle \subseteq J_0(p)(\mathbb{Q})$ be the cuspidal subgroup (where $\mathbf{0}$, $\boldsymbol{\infty}$ are the cusps of $X_0(p)$). Then $C = J_0(p)(\mathbb{Q})_{tor}$ (the torsion subgroup of $J_0(p)(\mathbb{Q})$) and C maps isomorphically to $J_0^-(p)(\mathbb{Q})_{tor}$ by the natural map. By abuse of notation we identify $C = J_0^-(p)(\mathbb{Q})_{tor}$. The order of C is equal to the numerator of $\frac{p-1}{12}$.

Theorem 0.4. *(Momose, 1987) Let N be a composite number. Let p be a prime divisor of N such that ($p = 11$ or $p \geq 17$) and $p \neq 37$. Assume $J_0^-(p)(\mathbb{Q}) = C$. Then $X_0^+(N)(\mathbb{Q}) = \{cusps, CM points\}$.* □

We generalize Theorem 0.4 for quadratic fields. The following (Theorem 0.5) is the main theorem of this work.

Theorem 0.5. *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 $\mathrm{ord}_p N = 1$ if $p = 11$. Let K be a quadratic field where p is unramified. Assume $X_0(N)(K) = \{cusps\}$ and $J_0^-(p)(K) = C$. Then $X_0^+(N)(K) = \{cusps, CM points\}$.*

Remark 0.6. Since the modular curve $X_0(37)$ is peculiar ($\mathrm{Aut}X_0(37) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), $p = 37$ is excluded in Theorem 0.4 and Theorem 0.5. But we have recently shown that Theorem 0.4 holds even if $p = 37$, and have generalized the result for certain imaginary quadratic fields.

Remark 0.7. (1) For N as in Theorem 0.4, we have $X_0(N)(\mathbb{Q}) = \{\text{cusps}\}$ (Mazur, 1978).
(2) If K is a quadratic field which is not an imaginary quadratic field with class number one, then we have $X_0(p)(K) = \{\text{cusps}\}$ for every sufficiently large prime number p (Momose, 1995). So the assumption $X_0(N)(K) = \{\text{cusps}\}$ in Theorem 0.5 is usually satisfied.

For the latter assumption of Theorem 0.5, we have the following examples.

Proposition 0.8. *Let K be an imaginary quadratic field.*
(1) If 11 does not split in K and 5 does not divide the class number h_K, then $J_0^-(11)(K) = C$.
(2) If 19 does not split in K and 3 does not divide h_K, then $J_0^-(19)(K) = C$. □

Sketch of proof of Theorem 0.5

Let $\pi : X_0(pM) \longrightarrow X_0(p)$ be the natural map defined by $(E, A) \longmapsto (E, A[p])$. Define a map $h : X_0(pM) \longrightarrow J_0(p)$ by $h(x) := cl((w_p\pi(x)) - (\pi w_{pM}(x)))$. If $x = (E, A)$, then $h(x) = cl((E/A[p], E[p]/A[p]) - (E/A, (E[p] + A)/A))$. Put

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

where $J_0(p) \longrightarrow J_0^-(p)$ is the quotient map. The map $\widetilde{h}^-$ factors through $X_0(pM) \longrightarrow X_0^+(pM) \longrightarrow J_0^-(p)$, where $X_0(pM) \longrightarrow X_0^+(pM)$ is the quotient map. Let $h^- : X_0^+(pM) \longrightarrow J_0^-(p)$ be the induced map. Thus we have the following commutative diagram:

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

Proposition 0.9. *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 $X_0(pM)(K) = \{cusps\}$. Let $y \in X_0^+(pM)(K)$ be a non-cuspidal point, and x, $w_{pM}(x)$ be the sections of the fiber $X_0(pM)_y$. Let L be the quadratic extension of K over which x, $w_{pM}(x)$ are defined. Take a prime $\mathfrak{p}$ of L above p, and let $\kappa(\mathfrak{p})$ be the quotient field of $\mathfrak{p}$. Assume $p \nmid M$ if $p = 11$. Then $h^-(y) \otimes \kappa(\mathfrak{p})$ is a section of $(J_0^-(p)_{/\mathcal{O}_L} \otimes \kappa(\mathfrak{p}))^0$ (the unit component of the special fiber of the Néron model).* □

Proposition 0.10. *Under the hypothesis in Proposition 0.9, suppose $J_0^-(p)(K) = C$. Then we have $h^-(y) = 0$.* □

The condition $h^-(y) = 0$ implies that y is a CM point since $p \neq 37$. Thus we have the conclusion of Theorem 0.5.

Remark 0.11. Strategy to get CM:
E : elliptic curve
$E \supsetneq A$: cyclic subgroup of order $d \geq 2$
If $E \cong E/A$
$\Longrightarrow E \longrightarrow E/A \cong E$ (first map: quotient map)
$\Longrightarrow \mathrm{End}(E) \supsetneq \mathbb{Z}$
$\Longrightarrow E$ has CM.