F. Momose and M. Shimura
Nagoya Math. J.
Vol. 165 (2002), 159–178

# LIFTING OF SUPERSINGULAR POINTS ON $X_0(p^r)$ AND LOWER BOUND OF RAMIFICATION INDEX

FUMIYUKI MOMOSE AND MAHORO SHIMURA

**Abstract.** Let $K$ be a finite extension of $\mathbf{Q}_p^{ur}$ (= the maximal unramified extension of $\mathbf{Q}_p$) of degree $e_K$, $\mathcal{O}$ its integer ring, $p$ a rational prime and $r$ a positive integer. If there exists a one parameter formal group defined over $\mathcal{O}$ whose reduction is of height 2 with a cyclic subgroup $V$ of order $p^r$ defined over $\mathcal{O}$, then $e_K \geq 2p^l$ (resp. $p^l + p^{l-1}$) if $r = 2l+1$ (resp. $r = 2l$).

We apply this result to a criterion for non-existence of $\mathbf{Q}$-rational point of $X_0^+(p^r)$. (This criterion is Momose's theorem in [14] except for the cases $p = 5$ and $p = 13$, but our new proof does not require defining equations of modular curves except for the case $p = 2$.)

## §0. Introduction

Let $p$ be a rational prime and let $r$ be a positive integer. We denote $\mathbf{Q}_p$ and $\mathbf{Q}_p^{ur}$ the $p$-adic number field and the maximal unramified extension of $\mathbf{Q}_p$. Let $K$ be a finite extension of $\mathbf{Q}_p^{ur}$, $\mathcal{O}$ the ring of integers of $K$, $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$ and $e_K$ the degree of $K$ over $\mathbf{Q}_p^{ur}$. Let $E$ be an elliptic curve with cyclic subgroup $A$ of order $p^r$ defined over $\mathcal{O}$ whose reduction mod $\mathfrak{m}$ is a supersingular elliptic curve. In this paper, we will show that the existence of such a pair $(E, A)$ gives a lower bound for $e_K$ with respect to $p$ and $r$. If $r$ is greater than one, the known lower bound of $e_K$ is $p+1$ ([14]). We note that it depends only on $p$. Our main result is as follows.

MAIN THEOREM. *Notation is as above. If such a pair $(E, A)$ exists, then*

$$e_K \geq \begin{cases} 2p^l & \text{if } r = 2l+1 \\ p^l + p^{l-1} & \text{if } r = 2l. \end{cases}$$

We have two proofs of this theorem, one is obtained by using the formal groups associated to elliptic curves, the other is due to the crossing theorem of modular curves ([9, Chap. 13, Theorem 13.4.7]). As an application of

Received July 30, 1999.
Revised January 12, 2001.

this theorem, we discuss the rational points of the modular curve $X_0^+(p^r) = X_0(p^r)/\langle w_{p^r}\rangle$. A point of $X_0^+(p^r)$ is called a CM point, if the corresponding elliptic curve has a complex multiplication. Let $g_0^+(p^r)$ denote the genus of $X_0^+(p^r)$. Let $n(p,r)$ be the number of the $\mathbf{Q}$-rational points on $X_0^+(p^r)$ which are neither cusps nor CM points. Then the following theorem holds. (See Section 3.1 about the definition of $J_0^-(p)$. Table (2) in Section 3.1 gives pairs $(p,r)$ which satisfy $g_0^+(p^r) > 0$.)

THEOREM 0.1. *Let $p$ be a prime number and $r \geq 2$ be an integer with $g_0^+(p^r) > 0$. Then $n(p,r) = 0$ for $p = 2,3,7,11$, $p = 5$ with $r \geq 4$, $p = 13$ with $r \geq 3$ and $p \geq 17$ with $\sharp J_0^-(p)(\mathbf{Q}) < \infty$.*

This result is already proved by the first author, except for the cases $p = 5$ and $p = 13$. The result for $p = 5$ is based on the finiteness of the $\mathbf{Q}$-rational points of $J_0^-(125)$ ([16]).

To prove this theorem, the first author used the defining equations of $X_0(p^r)$ in [14] for the cases $p = 2,3,5$. But our new proof requires the discussions of the defining equations only for the cases $p = 2$ with $r = 6$.

**Acknowledgement.** We would like to thank the referee for one's many helpful remarks concerning our paper. In particular, Theorem 3.3 and its related lemmas are owed to the referee.

**Notation**

- $N$, $n$ : positive integers, $p$ : a prime.
- $W(F)$ : the Witt algebra over $F$ ($F$ : a field).
- $\mathbf{Q}_p^{ur}$ : the maximal unramified extension of $\mathbf{Q}_p$.
- $\mathbf{Z}_p^{ur}$ : the ring of integers of $\mathbf{Q}_p^{ur}$.
- $\widehat{\mathbf{Q}}_p^{ur}$ : the completion of $\mathbf{Q}_p^{ur}$. (We note that $\widehat{\mathbf{Q}}_p^{ur}$ is isomorphic to the field of fractions of $W(\overline{\mathbf{F}}_p)$.)
- $K$ : a finite extension of $\mathbf{Q}_p^{ur}$ of degree $e_K$.
- $\widehat{K}$ : the completion of $K$.
- $\mathcal{O} = \mathcal{O}_K$ : the ring of integers of $K$.
- $\widehat{\mathcal{O}}$ : the completion of $\mathcal{O}$.
- $\mathfrak{m}$ : the maximal ideal of $\mathcal{O}$.
- $k := \mathcal{O}/\mathfrak{m}$ : the residue field with $\mathrm{char}(k) = p$ ($k \cong \overline{\mathbf{F}}_p$).
- $\pi$ : a prime element of $\mathcal{O}$.

- $v$ : the normalized valuation of $\mathcal{O}$, i.e. $v(\pi) = 1$.
- $v_p := \frac{1}{v(p)} v$.
- $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; c \equiv 0 \ (N) \right\}$.
- $\mathfrak{H} := \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$.
- $\mathfrak{H}^* := \mathfrak{H} \cup \mathbf{Q} \cup \{i\infty\} = \mathfrak{H} \cup \mathbf{P}^1(\mathbf{Q})$.
- $X_0(N)$ : the modular curve corresponding to $\Gamma_0(N)$. Its $\mathbf{C}$-valued points are

$$X_0(N)(\mathbf{C}) = \Gamma_0(N) \backslash \mathfrak{H}^*.$$

## §1. Main Theorem

We here discuss an elliptic curve $E$ defined over $K$ with a cyclic subgroup $V$ of order $p^r$ defined over $K$ which has supersingular good reduction. Let $\mathcal{F}$ be the associated formal group of $E$, then $\mathcal{F}$ mod $\mathfrak{m}$ is of height 2.

PROPOSITION 1.1. *Let $\mathcal{F}$ be a one parameter formal group over $\mathcal{O}$ whose reduction mod $\mathfrak{m}$ is of height 2 with a cyclic subgroup $V$ of order $p^r$ defined over $\mathcal{O}$, and $x$ a generator of $V$. Then the ramification index $v(p)$ and $v(x)$ satisfy the following inequality.*

$$\frac{v(p) - p^{r-t-1}}{p^t} \geq \varphi(p^r) v(x) \geq 1, \quad 0 \leq \exists t \leq \left[\frac{r}{2}\right],$$

*where $\varphi(\,\cdot\,)$ is the Euler function, $[x]$ is the greatest integer not exceeding $x$.*

*Proof.* First of all, we will show the right side inequality. Since the addition map of $\mathcal{F}$ is defined over $\mathcal{O}$, any pair $x$, $x'$ of generators of $V$ satisfies $K(x) = K(x')$. Hence irreducible polynomials over $K$ of $x$ and $x'$ have same degree. It implies that the degree (= the number of conjugates of $x$) divides the number of the generators of $V$ $(= \varphi(p^r))$. Since the conjugates of $x$ have same valuations and $V$ is defined over $\mathcal{O}$, $\varphi(p^r)v(x)$ is a positive integer. Hence, $\varphi(p^r)v(x) \geq 1$. We will show the left side inequality. The $p$-times map of $\mathcal{F}$ mod $\mathfrak{m}$ can be written $[p](x) = h(x^{p^2})$, $h'(0) \neq 0$, $h(x) \in k[x]$, since $\mathcal{F}$ mod $\mathfrak{m}$ is of height 2. So the $p$-times map of $\mathcal{F}$ must be the following form (cf. [17]):

$$(1) \qquad \begin{aligned} &[p](T) = pf(T) + \pi g(T^p) + h(T^{p^2}), \quad f(T), g(T), h(T) \in \mathcal{O}[[T]], \\ &f(0) = g(0) = h(0) = 0, \quad f'(0) = 1. \end{aligned}$$

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

**Step 1** : $r = 1$;

Suppose $x \neq 0$ and $[p](x) = 0$;

$$0 = [p](x) = pf(x) + \pi g(x^p) + h(x^{p^2}).$$

Comparing each leading terms of $pf(x)$, $\pi g(x^p)$ and $h(x^{p^2})$, we have

$$v(px) \geq v(\pi x^p).$$

(Since $p > 1$ and $(p-1)v(x) \geq 1$, $v(\pi x^p) < v(x^{p^2})$. So we can omit $v(x^{p^2})$.)

Hence

$$v(p) - 1 \geq (p-1)v(x) = \varphi(p)v(x),$$

which proves the theorem for $r = 1$.

**Step 2** : $r = s \geq 1$;

Suppose the following inequality holds for $x$ of order $p^s$.

$$\frac{v(p) - p^{s-t-1}}{p^t} \geq \varphi(p^s)v(x), \quad 0 \leq \exists t \leq \left[\frac{s}{2}\right].$$

**Step 3** : $r = s + 1$;

By the hypothesis of Step 2, if $x$ is of order $p^{s+1}$, then

$$\frac{v(p) - p^{s-t-1}}{p^t} \geq \varphi(p^s)v([p]x), \quad 0 \leq \exists t \leq \left[\frac{s}{2}\right].$$

By (1),

$$\frac{v(p) - p^{s-t-1}}{p^t} \geq \varphi(p^s)\min\{v(p) + v(x), 1 + pv(x), p^2v(x)\}.$$

Since $v(p) + v(x) \geq 1 + pv(x)$ (by Step 1),

$$\min\{v(p) + v(x), 1 + pv(x), p^2v(x)\} = \min\{1 + pv(x), p^2v(x)\}.$$

**Case 1**

If $1 + pv(x) \leq p^2v(x)$, then

$$\frac{v(p) - p^{s-t-1}}{p^t} \geq \varphi(p^s)(1 + pv(x)) = \varphi(p^s) + \varphi(p^{s+1})v(x).$$

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

Therefore,

$$\frac{v(p)-p^{(s+1)-t-1}}{p^t} \geq \frac{v(p)-p^{s-t-1}}{p^t} - \varphi(p^s) \geq \varphi(p^{s+1})v(x), \qquad 0 \leq t \leq \left[\frac{s+1}{2}\right],$$

which proves the theorem in this case.

**Case 2**

If $1 + pv(x) \geq p^2 v(x)$, then

$$\frac{v(p)-p^{s-t-1}}{p^t} \geq \varphi(p^s)(p^2 v(x)) = p\varphi(p^{s+1})v(x).$$

$$\frac{v(p)-p^{(s+1)-(t+1)-1}}{p^{t+1}} \geq \varphi(p^{s+1})v(x).$$

If $s$ is odd or $s = 2l$ and $t < l$, then $0 \leq t+1 \leq \left[\frac{s+1}{2}\right]$. Hence the theorem holds in this case. If $s = 2l$ and $t = l$, then by the hypothesis of Step 2 and $\varphi(p^s)v([p]x) \geq 1$, we have

$$v(p) \geq \left(p^l + p^{l-1}\right).$$

Then

$$\frac{v(p)-p^{(s+1)-t-1}}{p^t} - \frac{v(p)-p^{(s+1)-(t+1)-1}}{p^{t+1}}$$

$$= \frac{(p-1)(v(p)-(p^l+p^{l-1}))}{p^{l+1}} \geq 0.$$

Hence

$$\frac{v(p)-p^{(s+1)-t-1}}{p^t} \geq \frac{v(p)-p^{(s+1)-(t+1)-1}}{p^{t+1}} \geq \varphi(p^{s+1})v(x), \qquad 0 \leq t = l \leq \left[\frac{s+1}{2}\right]$$

So we have the desired result. □

Finally, we prove the Main Theorem.

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

*Proof of the Main Theorem.* By Proposition 1.1, we have

$$\frac{v(p)-p^{r-t-1}}{p^t} \geq 1, \quad 0 \leq \exists t \leq \left[\frac{r}{2}\right].$$

$$e_K = v(p) \geq p^{r-t-1}+p^t, \quad 0 \leq \exists t \leq \left[\frac{r}{2}\right].$$

It is easy to show the right hand side is minimum, if $t=[r/2]$. □

## §2. Another proof of the Main Theorem

(Ell) is the category whose objects are elliptic curves $E \xrightarrow{\pi} S$ over variable base schemes, and whose morphisms are cartesian squares of elliptic curves

$$\begin{array}{ccc} E_1 & \xrightarrow{a} & E \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi} \\ S_1 & \xrightarrow{f} & S \end{array}$$

i.e. commutative squares such that the induced morphism of $S_1$-schemes $E_1 \xrightarrow{(a,\pi_1)} E \times_S S_1$ is an isomorphism of elliptic curves over $S_1$ ([9]). This category (Ell) is the "modular stack" of Deligne-Rapoport ([5]). Let $R$ be a ring. The category (Ell/$R$) is a subcategory of (Ell) whose objects are elliptic curves over variable $R$-schemes, and whose morphisms are the cartesian squares whose bottom arrow is $R$-linear.

Let $\mathfrak{T}$ be a representable moduli problem of elliptic curves whose tensored by $\mathbf{Z}_{(p)}$, $\mathfrak{T}\otimes\mathbf{Z}_{(p)}$ is finite etale over (Ell/$\mathbf{Z}_{(p)}$). Then $\mathfrak{T}\times[\Gamma_0(p^r)]$ is also representable and represented by $M=\mathfrak{M}(\mathfrak{T},[\Gamma_0(p^r)])$ ([9, Chap. 4]) and the fine moduli stack $M\otimes\mathbf{Z}_{(p)}$ is regular ([9, Chap. 5]).

Let $(E,A)$ be the pair in the Main Theorem. We consider the point in $\mathfrak{M}([\Gamma_0(p^r)])$ corresponding to $(E,A)$. Since $\mathfrak{T}\otimes\mathbf{Z}_{(p)}$ is etale over (Ell/$\mathbf{Z}_{(p)}$) and $\mathcal{O}$ is strictly henselian, we can lift the point of $\mathfrak{M}([\Gamma_0(p^r)])$ to a point $P$ of $\mathfrak{M}(\mathfrak{T},[\Gamma_0(p^r)])$. We give $P$ by the following $\mathcal{O}$-valued point of $\mathfrak{M}(\mathfrak{T},[\Gamma_0(p^r)])$.

$$f : \mathrm{Spec}(\mathcal{O}) \longrightarrow M$$

Since $\widehat{\mathcal{O}}$ includes $W(k)$, the morphism $f$ lifts uniquely to a $W(k)$-morphism $F : \mathrm{Spec}(\widehat{\mathcal{O}}) \to M_{W(k)} := M\otimes_{\mathbf{Z}} W(k)$.

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

**Notation**

- $A$ : the complete local ring of $M_{W(k)}$ at the image by $F$ of the closed point of $\mathrm{Spec}(\widehat{\mathcal{O}})$.
- $\mathfrak{m}_R$ : the maximal ideal of a local ring $R$.

To prove the theorem, we need the following two facts.

(I) $A$ becomes a 2-dimensional regular local ring.
(II) $A/(p)(= A \otimes_{W(k)} k) \cong k[[s,t]]/(h(s,t))$,
$h(s,t) := (s^{p^r} - t)(s - t^{p^r}) \prod_{\substack{a,b\geq 1 \\ a+b=r}} (s^{p^{a-1}} - t^{p^{b-1}})^{p-1}$. ([9, Chap. 13]).

(I) and (II) deduce the surjection $k[[s,t]] \twoheadrightarrow A/(p)$ lifts to a surjection $W(k)[[s,t]] \twoheadrightarrow A$.

We claim that the following formula holds in $A$.

$$p = h(s,t)g(s,t), \quad g(s,t) \in W(k)[[s,t]].$$

In fact, we can show the claim as follows.

(I) implies that $\dim_k(\mathfrak{m}_A/\mathfrak{m}_A^2) = 2$. (II) implies that $A/(p)$ becomes a 2-dimensional regular local ring. Hence, $\dim_k(\mathfrak{m}_{A/(p)}/\mathfrak{m}_{A/(p)}^2) = 2$. Therefore, the natural surjection $\mathfrak{m}_A/\mathfrak{m}_A^2 \twoheadrightarrow \mathfrak{m}_{A/(p)}/\mathfrak{m}_{A/(p)}^2$ is bijective. Thus, since $p$ vanishes in the target, $p$ also vanish in the source, or, equivalently, $p \in \mathfrak{m}_A^2$. Since $\mathfrak{m}_{W(k)[[s,t]]}^2 \to \mathfrak{m}_A^2$ is surjective, we can take $f \in \mathfrak{m}_{W(k)[[s,t]]}^2$ such that $p = f(s,t)$ holds in $A$. Now, since $f \pmod{(p)}$ is divisible by $h \pmod{(p)}$, we can write $f = ah + bp$ for some $a, b \in W(k)[[s,t]]$, or $f - ah = bp$. Since both $f$ and $h$ belong to $\mathfrak{m}_{W(k)[[s,t]]}^2$, so does $bp$. Now since $p$ is a non-trivial element of $\mathfrak{m}_{W(k)[[s,t]]}/\mathfrak{m}_{W(k)[[s,t]]}^2$, $b$ cannot be a unit, or, equivalently, $b \in \mathfrak{m}_{W(k)[[s,t]]}$. In particular, $(1-b)$ is a unit. Now put $g = (1-b)^{-1}a \in W(k)[[s,t]]$. Then we have $gh = (1-b)^{-1}ah = (1-b)^{-1}(f-bp)$ in $W(k)[[s,t]]$, which maps to $(1-b)^{-1}(p-bp) = p$ in $A$.

Moreover, we can show the following facts.

(i) $W(k)[[s,t]]/(h(s,t)g(s,t) - p) \cong A$.
(ii) $g(s,t) \in W(k)[[s,t]]^\times$.

In fact, the surjection $W(k)[[s,t]]/(h(s,t)g(s,t) - p) \twoheadrightarrow A$ is between two 2-dimensional regular local rings, it must be an isomorphisms. Hence (i)

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

holds. By (i), we have $A/(p) = k[[s,t]]/(h(s,t)g(s,t) \bmod (p))$. On the other hand we know that $A/(p) = k[[s,t]]/(h(s,t) \bmod (p))$. Hence $g(s,t) \bmod (p)$ must be a unit and so is $g(s,t)$.

Since

$$f^* : A \longrightarrow \widehat{\mathcal{O}},\ s \longmapsto \pi\alpha,\ t \longmapsto \pi\beta,\ (\exists \alpha,\ \beta \in \widehat{\mathcal{O}})$$

and $p = g(s,t)h(s,t)$, $g(s,t) \in W(k)[[s,t]]^\times$,

$$\begin{aligned} e_K &= v(p) \\ &= v\big((\pi\alpha)^{p^r} - \pi\beta\big) + v\big(\pi\alpha - (\pi\beta)^{p^r}\big) + (p-1)\sum v\big((\pi\alpha)^{p^{a-1}} - (\pi\beta)^{p^{b-1}}\big) \\ &\geq 1 + 1 + (p-1)\sum \min\big\{p^{a-1}, p^{b-1}\big\} \\ &= \begin{cases} 2p^l & \text{if } r = 2l+1 \\ p^l + p^{l-1} & \text{if } r = 2l. \end{cases} \end{aligned}$$

## §3. Application to rational points of $X_0^+(p^r)$

### 3.1. Notation and Facts

Let $p$ be a prime number, $r \geq 1$ an integer. The fundamental involution $w_{p^r}$ of $X_0(p^r)$ is defined by the functor; $(E,A) \mapsto (E/A, E[p^r]/A)$, where $E[p^r] := \ker([p^r] : E \to E)$. Let $X_0^+(p^r)$ denote the quotient $X_0(p^r)/\langle w_{p^r}\rangle$. There exists a covering over $\mathbf{Q}$ of $X_0^+(p^{r+2})$ to $X_0^+(p^r)$, which is induced by the morphism over $\mathbf{Q}$ of $X_0(p^{r+2})$ to $X_0(p^r)$ defined by

$$(E,A) \longmapsto (E/A[p],\ A[p^{r+1}]/A[p]),$$

where $A[p^i]$ is the unique cyclic subgroup of $A$ of order $p^i$. Let $X_s(p^t) = X_{sp.Car.}(p^t)$ be the modular curve over $\mathbf{Q}$ which corresponds to the modular group

$$\Gamma_s(p^t) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; b \equiv c \equiv 0 \pmod{p^t} \right\}.$$

Then $X_s(p^t)$ is the coarse moduli space of the generalized elliptic curves $E$ with independent cyclic subgroups $C_1$ and $C_2$ of order $p^t$, which is defined over $\mathbf{Q}$. The fundamental involution $w(p^t)$ of $X_s(p^t)$ is defined by

$$(E, C_1, C_2) \longmapsto (E, C_2, C_1).$$

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

Let $X_s^n(p^t) = X_{split}(p^t)$ be the quotient $X_s(p^t)/\langle w(p^t)\rangle$, which corresponds to the modular group $\left\langle \Gamma_s(p^t), \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$. There exists a canonical isomorphism defined over $\mathbf{Q}$ of $X_0(p^{2t})$ (resp. $X_0^+(p^{2t})$) to $X_s(p^t)$ (resp. $X_s^n(p^t)$) which is defined by

$$(E, A) \longmapsto (E/A[p^t],\ A/A[p^t],\ E[p^t]/A[p^t]).$$

The inverse map is given by

$$(E, C_1, C_2) \longmapsto (E/C_2,\ (C_1 + (E/C_1)[p^t])/C_2).$$

Let $J_0(p^r)$, $J_0^+(p^r)$ be the Jacobian varieties of $X_0(p^r)$ and $X_0^+(p^r)$, respectively. Let $J_0^-(p^s)$ be the quotient $J_0(p^s)/(1 + w_{p^s})J_0(p^s)$, where $w_{p^s}$ is the automorphism of $J_0(p^s)$ induced by the involution $w_{p^s}$ of $X_0(p^s)$ ([10]). Let $\pi = \pi_{r,s}$ be the natural morphism of $X_0(p^r)$ to $X_0(p^s)$ defined by $(E, A) \mapsto (E, A[p^s])$ for an integer $s$, $1 \leq s \leq r-1$. Let $f = f_{r,s}$ be the morphism of $X_0(p^r)$ to $J_0(p^s)$ defined by $f(x) = \mathrm{cl}((w_{p^s}\pi(x)) - (\pi w_{p^r}(x)))$, i.e. $f : (E, A) \mapsto \mathrm{cl}((E/A[p^s], E[p^s]/A[p^s]) - (E/A, (E[p^s] + A)/A))$. Then $f$ induces a morphism $f^+ = f_{r,s}^+$ of $X_0^+(p^r)$ to $J_0^-(p^s)$, which is defined by the following commutative diagram:

$$\begin{array}{ccc} X_0(p^r) & \xrightarrow{can.} & X_0^+(p^r) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f^+} \\ J_0(p^s) & \xrightarrow{can.} & J_0^-(p^s). \end{array}$$

We will make use of $f$ and $f^+$ in the following cases:

(2)

| $p$ | $r$ | $s$ |
|---|---|---|
| 2 | $\geq 6$ | 5 |
| 3 | $\geq 4$ | 3 |
| 5 | $\geq 4$ | 3 |
| 7 | $\geq 3$ | 2 |
| 11 | $\geq 2$ | 1 |
| 3 | $\geq 3$ | 2 |
| $p \geq 17$ | $\geq 2$ | 1 |

*Remark.* In this table, $s$ is the minimal value satisfying $g_0(p^s) > 0$, and $r \geq s+1$. Then $g_0^+(p^r) > 0$ holds automatically. And the Mordell-Weil group of $J_0^-(p^s)$ is finite for such $(p, s)$ with $p = 2, 3, 5, 7, 13$ ([10], [2], [16], [7]).

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

*Remark.* We note that the known results about the finiteness of $J_0^-(p)(\mathbf{Q})$. By Mazur's result, the $\mathbf{Q}$-rank of any Eisenstein quotient is zero ([10]). It is true that $J_0^-(p)$ contains at least one Eisenstein quotient. Hence, if $J_0^-(p)$ is simple, then the rank of $J_0^-(p)(\mathbf{Q})$ is zero, or, equivalently the Mordell-Weil group of $J_0^-(p)$ is finite. For example, $J_0^-(11)(\mathbf{Q})$ is finite, because $J_0^-(11)$ is an elliptic curve. For $p < 2000$, the table of splittings of $J_0^-(p)$ is given by Mazur and Brumer ([10], [3]). If $J_0^-(p)$ contains non-Eisenstein quotient, we don't know its rank is zero or not. However, if the quotient is elliptic curve and its conductor less than 1000, we know the rank by Cremona's table ([4]).

Let $\mathfrak{X}_0(p^r)$ be the normalization of the projective $j$-line $\mathfrak{X}_0(1) \cong \mathbf{P}^1_{\mathbf{Z}}$ in the function field of $X_0(p^r)$ and $\mathfrak{X}_0^+(p^r) = \mathfrak{X}_0(p^r)/\langle w_{p^r} \rangle$. Denote also by $\pi = \pi_{r,s}$ the natural morphisms of $\mathfrak{X}_0(p^r)$ to $\mathfrak{X}_0(p^s)$, and by $f$, (resp. $f^+$) the morphisms of the smooth part $\mathfrak{X}_0(p^r)^{smooth}$ (resp. $\mathfrak{X}_0^+(p^r)^{smooth}$) to the Neron models $J_0(p^s)_{/\mathbf{Z}}$ (resp. $J_0^-(p^s)_{/\mathbf{Z}}$).

Let $E_i$ $(0 \leq i \leq r)$ be the irreducible components of $\mathfrak{X}_0(p^r) \otimes \mathbf{F}_p$. $E_i$ contains the following cuspidal section. i.e. $\binom{0}{1} \otimes \mathbf{F}_p \in E_0$, $\binom{1}{0} \otimes \mathbf{F}_p \in E_r$ and $\binom{i}{p^i} \otimes \mathbf{F}_p \in E_i$ $(1 \leq i \leq r-1)$ ([14]).

Let $E_i^h$ be $E_i \backslash \{\text{supersingular points on } E_i\}$.

### 3.2. Elliptic curves

LEMMA 3.1. *Let $E$ be a semistable elliptic curve with a cyclic subgroup $A$ of order $p^r$ defined over $K$. Let $x$ be an $\mathcal{O}$-section of $\mathfrak{X}_0(p^r)$ such that $x \otimes K$ is represented by the pair $(E, A)$. Then*

(i) *If $x \otimes k$ is a section of $E_i^h$, then $K$ contains a primitive $p^{m(i)}$-th root $\zeta_{p^{m(i)}}$ of unity for $m(i) = \min\{i, r-i\}$.*

(ii) *If $x \otimes k$ is a supersingular point, then*

$$e_K \geq \begin{cases} 2p^l, & \text{if } r = 2l+1, \\ p^l + p^{l-1}, & \text{if } r = 2l. \end{cases}$$

*Proof.* (i) [14, Lemma 2.2 (i)]. (ii) It is obvious by the Main Theorem. □

Let $E$ be an elliptic curve with a cyclic subgroup $A$ defined over $K$ and $x$ be an $\mathcal{O}$-section of $\mathfrak{X}_0(p^r)$ such that $x \otimes K$ is represented by the pair

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

$(E, A)$. We put

$$e' = \begin{cases} 1, & \text{if } j(x) \not\equiv 0,\ 1728 \pmod{\mathfrak{m}}, \\ 2, & \text{if } j(x) \equiv 1728 \pmod{\mathfrak{m}},\ p \geq 5, \\ 3, & \text{if } j(x) \equiv 0 \pmod{\mathfrak{m}},\ p \geq 5, \\ 6, & \text{if } j(x) \equiv 0 \pmod{\mathfrak{m}},\ p = 3, \\ 12, & \text{if } j(x) \equiv 0 \pmod{\mathfrak{m}},\ p = 2. \end{cases}$$

Then $E$ (or its quadratic twist) has semistable reduction over a finite extension of $K$ with degree $e'$ ([20, pp. 33–52]).

COROLLARY 3.2. *Let $E$ be a elliptic curve with a cyclic subgroup $A$ of order $p^r$ defined over $K$. Let $x$ be an $\mathcal{O}$-section of $\mathfrak{X}_0(p^r)$ such that $x \otimes K$ is represented by the pair $(E, A)$. Then*

(i) *If $x \otimes k$ is a section of $E_i^h$, then $e_K e' \geq p^{m(i)-1}(p-1)$ if $1 \leq i \leq r-1$.*

(ii) *If $x \otimes k$ is a supersingular point, then*

$$e_K e' \geq \begin{cases} 2p^l, & \text{if } r = 2l+1, \\ p^l + p^{l-1}, & \text{if } r = 2l. \end{cases}$$

### 3.3. Local moduli and $X_0^+(p^r)$

In this section, we treat purely local situation, where the base field is $\mathbf{Q}_p^{ur}$ or $\widehat{\mathbf{Q}}_p^{ur}$.

Let $(p, r)$ be a pair in Table (2). Let $y$ be a non-cuspidal $\mathbf{Q}_p^{ur}$-rational point on $X_0^+(p^r)$, and $x$, $x' = w_{p^r}(x)$ the sections of the fiber $X_0(p^r)_y$ at $y$. They are defined over a field $M$ with degree $e_M$. $M$ is $\mathbf{Q}_p^{ur}$ or a quadratic field of $\mathbf{Q}_p^{ur}$. Denote also by $x$ and $x'$ (resp. $y$) the $\mathcal{O}_M$ (resp. $\mathcal{O}$)-sections of $\mathfrak{X}_0(p^r)$ (resp. $\mathfrak{X}_0^+(p^r)$) with generic fibers $x$ and $x'$ (resp. $y$).

We shall start with the special case $p = 2$.

THEOREM 3.3. *Let $y$ be a $\mathbf{Q}_2^{ur}$-rational point of $X_0^+(2^r)$ for $r \geq 6$, and $x$ a point of the fiber in $X_0(2^r)$ at $y$. Then $j(x) \not\equiv 0 \pmod 2$.*

Let $E$ be an elliptic curve over $\mathcal{O}$. Then the universal formal deformation ring $R = R_{E_k}$ of the elliptic curve $E_k = E \otimes_{\mathcal{O}} k$ over $k$ is known to be isomorphic to the formal power series ring $W(k)[[T]]$. By universality, we have a canonical homomorphism $\varphi_E : R \to \widehat{\mathcal{O}}$. Then we define $v(E)$ (resp. $v_p(E)$) to be the minimum of $v(\varphi_E(x))$ (resp. $v_p(\varphi_E(x))$) for $x \in \mathfrak{m}_R$, the maximal

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

ideal of $R$. More concretely, if we fix an isomorphism $R \cong W(k)[[T]]$, then we have $v(E) = \min(v(\varphi_E(T)), v(p))$ (resp. $v_p(E) = \min(v_p(\varphi_E(T)), 1)$). Note that $v_p(E)$ is preserved under change of the base $\mathcal{O}$. (Thus we can define $v_p(E)$ for an arbitrary elliptic curve over $K$).

LEMMA 3.4. *Assume $p = 2$ and $j(E) \equiv 0 \pmod{\mathfrak{m}}$. Then we have $v_2(E) < 1/4 \iff v_2(j(E)) < 3$, and if one of these conditions holds, we have $v_2(E) = \frac{1}{12} v_2(j(E))$.*

*Proof.* $R_{E_k} = W(k)[[T]]$ admits a natural faithful action of $\mathrm{Aut}(E_k)/\{\pm 1\}$ and the quotient by this action coincides with $W(k)[[j]]$ (See [9, Proposition 8.2.3]). In our case, it is known that $(\mathrm{Aut}(E_k) : \{\pm 1\}) = 12$ and that the degree 12 extension $R_{E_k}/W(k)[[j]]$ contains the degree 3 subextension $W(k)[[j^{1/3}]]/W(k)[[j]]$. Write $j^{1/3} = \sum_{i=0}^{\infty} a_i T^i$ with $a_i \in W(k)$. Then, considering the degrees, we must have $a_i \equiv 0 \pmod{(p)}$ for $0 \leq i \leq 3$ and $a_4 \not\equiv 0 \pmod{(p)}$. Now, comparing the valuations of the images by $\varphi_E$ of both sides of the equality, we can deduce $v_2(j(E)^{1/3}) = v_2(\varphi_E(T)^4)$, if we use one of the conditions $v_2(E) < 1/4$ and $v_2(j(E)) < 3$. Or, equivalently, $v_2(\varphi_E(T)) = \frac{1}{12} v_2(j(E))$. Since this is $< 1/4 < 1$, we have $v_2(E) = v_2(\varphi_E(T))$. Finally, the condition that we did not use follows from this identity and the other condition that we used. □

*Remark.* Assume $p = 2$ and $j(E) \equiv 0 \pmod{\mathfrak{m}}$. Then in general, we can prove:

$$v_2(E) = \min\Big(\frac{1}{12} v_2(j(E)), 1\Big).$$

(We will not use this fact, though.)

Let $E_1$ be an elliptic curve over $\mathcal{O}$ with $E_{1,k}$ supersingular, and $C$ a cyclic subgroup of $E_1$ of order $p^r$. Put $E_2 = E_1/C$. Since $E_{1,k} \to E_{2,k}$ can be identified with the composition of the $r$ Frobenii, $E_{2,k}$ can be canonically identified with $E_{1,k} \otimes_{k,\sigma^r} k$ and $R_{E_{2,k}}$ can be canonically identified with $R_{E_{1,k}} \otimes_{W(k),\sigma^r} W(k)$, where $\sigma$ denotes the Frobenius automorphism on $k$ or $W(k)$. Accordingly, if we fix an identification $R_{E_{1,k}} = W(k)[[T]]$, then we also have $R_{E_{2,k}} = W(k)[[T]]$. Now, we can take $f^*(s) = \varphi_{E_1}(T)$, $f^*(t) = \varphi_{E_2}(T)$. (See the definitions of $s$, $t$ and $f^*$ in Section 2.)

Put $\mathbf{v}_i = v(E_i)$ $(i = 1, 2)$. We prove the following lemma for later use. (In fact, only the case $p = 2$, $r = 1$ will be used later.)

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

LEMMA 3.5. *At least one of the following holds.*
(i) $p^a\mathbf{v}_1 = p^b\mathbf{v}_2$ *for some* $a, b \geq 0$, $a + b = r$.
(ii) $\mathbf{v}_1$, $\mathbf{v}_2 \geq v(p)/(p^r + p^{r-1})$.

*Proof.* Suppose that (ii) does not hold. For example, suppose $\mathbf{v}_1 < v(p)/(p^r + p^{r-1})$. (The other case is similar.) Then, since, in particular, $\mathbf{v}_1 < v(p)$, we have $\mathbf{v}_1 = v(\varphi_{E_1}(T)) = v(f^*(s))$. Suppose further that $p^a v(f^*(s)) \neq p^b v(f^*(t))$ for any $a, b \geq 0$, $a + b = r$. Then by comparing the valuations of both sides of $p = h(f^*(s), f^*(t))g(f^*(s), f^*(t))$, we obtain

$$v(p) = \sum_{a,b\geq 0,\, a+b=r} \delta(a,b) \min\bigl(p^a v(f^*(s)), p^b v(f^*(t))\bigr),$$

where $\delta(a, b)$ is 1 (resp. $(p-1)/p$) for $a = 0$ or $b = 0$ (resp. $a, b \geq 1$). From this,

$$v(p) \leq \sum_{a,b\geq 0,\, a+b=r} \delta(a,b) p^a v(f^*(s)) \leq (p^r + p^{r-1}) v(f^*(s)) < v(p),$$

which is absurd. Thus $v(f^*(t)) = p^{a-b}v(f^*(s))$ for some $a, b \geq 0$, $a + b = r$. In particular, $v(f^*(t)) \leq p^r v(f^*(s)) \leq p^r v(p)/(p^r + p^{r-1}) < v(p)$, hence $\mathbf{v}_2 = v(f^*(t))$. Now (i) follows. □

Next, consider the situation of Section 2 for $p = 2$ and $\mathcal{T} = \Gamma(3)$. Let $X$ be the (compactified) modular curve over $\mathbf{Z}$ corresponding to the moduli problem $[\Gamma_0(2^r), \Gamma(3)]$. Since $2^r \equiv \pm 1 \pmod 3$, $X$ admits a natural action of $W \times G$, where $W = \langle w \rangle$ ($w = w_{2^r}$) and $G = \mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})/\{\pm 1\}$. (The involution $w$ acts as $(E, C, (\alpha, \beta)) \mapsto (E/C, E[p^r]/C, (\alpha \bmod C,\ \beta \bmod C))$.) $X$ is a fine moduli scheme and $X_0^+(2^r)$ is the quotient of $X$ by $W \times G$. Note that the integral closure of $\mathbf{Z}$ in $X$ is $\mathbf{Z}[\zeta_3]$ and that the action of $W \times G$ on $\mathbf{Z}[\zeta_3]$ is via $\chi_r : W \times G \to (\mathbf{Z}/3\mathbf{Z})^\times$,

$$\chi_r(w^i, g) = (2^r)^i \det(g) = \begin{cases} \det(g), & r : \text{even}, \\ (-1)^i \det(g), & r : \text{odd}, \end{cases}$$

Let $H_r$ denote the kernel of $\chi_r$, which depends only on $r \pmod 2$. More explicitly, we have $H_r = W \times S$, where $S = \mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})/\{\pm 1\}$, for $r$ even, and $H_r \xrightarrow{\sim} G$ by the projection, for $r$ odd.

Let $y$ be a $\mathbf{Q}_2^{ur}$-rational point of $X_0^+(2^r)$, and $\xi$ a point of the fiber in $X$ at $y$. We may assume that the residue field of $\xi$ is $K$. Then we obtain

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

the following subgroups: $I \subset D \subset H_r \subset W \times G$, where $D$ (resp. $I$) is the decomposition (resp. inertia) subgroup at $\xi$. (Thus $D/I \cong \mathrm{Gal}(K/\mathbf{Q}_2^{ur})$.) Observe that $j(x) = 0, 1728 \Longrightarrow I \neq \{\pm 1\} \Longrightarrow x$ : a CM point or a cusp. We would like to estimate the degree $\mathbf{e} = (D : I)$ of the field of definition of $\xi$ over $\mathbf{Q}_2^{ur}$. (Note that $\mathbf{e}$ corresponds to $e_K e'$.)

Now, assume that $\xi$ has supersingular reduction, or, equivalently, that $j(x) \equiv 0 \pmod{\mathfrak{m}}$. Then $\xi$ induces a homomorphism $f^* : W(k)[[s,t]] \to \widehat{\mathcal{O}}$, as in Section 2.

LEMMA 3.6. *We have* $\mathbf{e} \leq 24$. *Moreover, one of the following holds*:
(i) $\mathbf{e} \leq 12$;
(ii) $\mathbf{e} = 24$, $r = 2l$ : *even, and* $\mathbf{e} > (2^l + 2^{l-1})\mathbf{v}$, *where* $\mathbf{v} := v(f^*(s)) = v(f^*(t))$.

*Proof.* Since $H_r \supset D \twoheadrightarrow D/I$ and $\sharp(H_r) = 24$, we have $\mathbf{e}|24$, hence, in particular, $\mathbf{e} \leq 24$. Suppose that (i) does not hold, i.e. $\mathbf{e} > 12$. Then we must have $\mathbf{e} = 24$, $D = H_r$ and $I = \{1\}$. Since $D$ is a Galois group over $\mathbf{Q}_2^{ur}$, the Sylow 2-subgroup of $D$ has to be a normal subgroup of $D$. However, if $r$ is odd, then we can easily check that the Sylow 2-subgroup of $H_r$ ($\cong G$) is not a normal subgroup of $H_r$. Therefore, $r$ is even.

Define $\sigma \in \mathrm{Gal}(K/\mathbf{Q}_2^{ur})$ to correspond to $w \in W \subset W \times S = H_r$. Then, $f^*$ is compatible with the involution $(s,t) \mapsto (t,s)$ on $W(k)[[s,t]]$ and $\sigma$ on $\widehat{\mathcal{O}}$. From this we obtain $f^*(t) = \sigma(f^*(s))$ and $v(f^*(t)) = v(f^*(s))$.

Finally, we have to prove the strict inequality $\mathbf{e} = v(2) > (2^l + 2^{l-1})\mathbf{v}$, in the context of Section 2. This comes from the middle term $v\big(f^*(s)^{2^{l-1}} - f^*(t)^{2^{l-1}}\big)$ which was estimated as $\geq 2^{l-1}\mathbf{v}$ in Section 2. However, we have

$$f^*(s)^{2^{l-1}} - f^*(t)^{2^{l-1}} = f^*(s)^{2^{l-1}} - \sigma\big(f^*(t)^{2^{l-1}}\big),$$

and $\sigma$ acts trivially on $\mathfrak{m}^{2^{l-1}\mathbf{v}}/\mathfrak{m}^{2^{l-1}\mathbf{v}+1}$ since $p = 2$ and $\sigma$ is of order 2. Accordingly, we have $v\big(f^*(s)^{2^{l-1}} - f^*(t)^{2^{l-1}}\big) > 2^{l-1}\mathbf{v}$. This completes the proof. □

End of the proof of Theorem 3.3. Suppose the existence of such a rational point. In the notation above, put $\mathbf{v}_1 = v(f^*(s))$, $\mathbf{v}_2 = v(f^*(t))$. ($r \geq 9$) We have a contradiction as follows.

$$24 \geq \mathbf{e} \geq 2^{[r/2]} + 2^{[(r-1)/2]} \geq 32.$$

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

($r = 8$) First we obtain $24 \geq \mathbf{e} \geq 2^4 + 2^3 = 24$. Then, by Lemma 3.6, conclude: $24 = \mathbf{e} > 2^4 + 2^3 = 24$.
($r = 7$) by Lemma 3.6, conclude: $12 \geq \mathbf{e} \geq 2 \cdot 2^3 = 16$.
($r = 6$) First we obtain $\mathbf{e} \geq 2^3 + 2^2 = 12$. Since $\mathbf{e}|24$, we have two possibilities: (1) $\mathbf{e} = 12$; (2) $\mathbf{e} = 24$. In the case (1), since $\mathbf{e} = 2^3 + 2^2$, we must have $\mathbf{v}_1 = \mathbf{v}_2 = 1$. In the case (2), by Lemma 3.6, conclude $\mathbf{v}_1 = \mathbf{v}_2 = \mathbf{v}$ and $24 = \mathbf{e} > 12\mathbf{v}$. Hence $\mathbf{v} = 1$. Now, for the point $x = (E, C, (\alpha, \beta))$ of $X$ above $y$, put $E_i = E/C[2^i]$ for $i = 0, \ldots, 6$. Then our conclusion above means $v(E_0) = v(E_6) = 1$. Applying Lemma 3.5 to the pairs $(E_0, E_1)$ and $(E_5, E_6)$ ($r = 1$), we obtain $v(E_1) = v(E_5) = 2$, or, equivalently, we have (1) $\mathbf{e} = 12$, $v_2(E_1) = v_2(E_5) = 1/6$; or (2) $\mathbf{e} = 24$, $v_2(E_1) = v_2(E_5) = 1/12$.

Note that $\{E_1, E_5\}$ defines a $\mathbf{Q}_2^{ur}$-rational point of $X_0^+(2^4)$. Now we resort to the defining equation to prove the following:

LEMMA 3.7. *Let $y$ be a $\mathbf{Q}_2^{ur}$-rational point of $X_0^+(2^4)$, $\{x, x'\}$ the (geometric) fiber in $X_0^+(2^4)$ at $y$, and $j(x) \equiv 0 \pmod{\mathfrak{m}}$. (If $y$ is a ramified point, we put $x' = x$.) Then the unordered pair $\{j(x), j(x')\}$ satisfies the following*:

$$\{v_2(j(x)), v_2(j(x'))\} = \begin{cases} \{1, 4\}, & x,\ x' \text{ are } \mathbf{Q}_2^{ur}\text{-rational}, \\ \{1/2, 1/2\}, \{3/2, 3/2\}, & \text{otherwise}. \end{cases}$$

*Proof.* The modular curve $X_0(2^4)$ is defined by the equation

$$j(X) = g(X)/X(X+4)(X^2+4X+8)(X+2)^4$$

with $w_{16}^*(X) = 8/X$, where $g(X) = (X^8 + 2^4X^7 + 7 \cdot 2^4X^6 + 7 \cdot 2^6X^5 + 69 \cdot 2^4X^4 + 13 \cdot 2^7X^3 + 11 \cdot 2^7X^2 + 2^9X + 2^4)^3$ ([6]). If $v_2(x) \leq 0$, then $v_2(j(x)) \leq 0$. If $v_2(x) \geq 3$, then $v_2(j(x')) \leq 0$. Hence, $0 < v_2(x) < 3$.

If $x$ and $x'$ are $\mathbf{Q}_2^{ur}$-rational points, then $\{v_2(x), v_2(x')\} = \{1, 2\}$. If $v_2(x) = 1$,

$$\begin{aligned} v_2(j(x)) &= v_2(g(x)) - v_2(x(x+4)(x^2+4x+8)(x+2)^4) \\ &\geq 8 - 4v_2(x+2). \end{aligned}$$

$v_2(x+2) \geq 2$ implies $v_2(j(x)) \leq 0$. Hence, $v_2(x+2) = 1$ and $v_2(j(x)) = 4$. By the same argument, we have $v_2(j(x)) = 1$, if $v_2(x) = 2$.

If $x$ and $x'$ are not $\mathbf{Q}_2^{ur}$-rational points, then $x$ and $x'$ become the solutions of $X^2 - aX + 8 = 0$ for $a \in \mathbf{Z}_2^{ur}$, $a = x + x' = x + 8/x$, $v_2(a) \geq 2$

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

and both $v_2(x)$ and $v_2(x')$ are half integers. Since $v_2(a) = v_2(x + 8/x)$ is integer, $v_2(x) = v_2(8/x) = 3/2$.

$$v_2(j(x)) \geq 5 - v_2((a+4)x)) = 7/2 - v_2(a+4).$$

Since $a \neq -4$ (if so, the denominator of $j(X)$ vanishes), $v_2(a+4) \geq 2$ and $v_2(a+4)$ is integer. Hence, $\{v_2(j(x)), v_2(j(x'))\} = \{1/2, 1/2\}, \{3/2, 3/2\}$. □

From this and Lemma 3.4, we must have

$$\{v_2(E_1), v_2(E_5)\} = \{1/12, \geq 1/4\}, \{1/24, 1/24\}, \{1/8, 1/8\},$$

(In fact, the first one must be $\{1/12, 1/3\}$ by Remark to Lemma 3.4.) This contradicts our former conclusion

$$\{v_2(E_1), v_2(E_5)\} = \{1/6, 1/6\}, \{1/12, 1/12\}.$$

LEMMA 3.8. *Let $(p, r)$ be a pair in Table (2), and $x$, $x'$, $y$ and $e_M$ be as above. If $e_M = 2$, then $x$ is a section of $E_t$ if $r = 2t$ is even, and it is a supersingular point if $r$ is odd.*

*Proof.* [14, Lemma 3.1]. We note that the proof in [14] can be applied to our purely local situation. □

We recall that each non-cuspidal $F$-rational point ($F$ : a field) of $X_0(p^r)$ is represented by an object $(E, C)$ defined over $F$.

LEMMA 3.9. *If $r = 2t$ is even and $p \neq 2$. Then Corollary 3.2 holds if we replace $e_K e'$ by $e'$.*

*Proof.* If $r = 2t$ is even, then there exists the following diagram

$$\begin{array}{ccc} X_0(p^{2t}) & \xrightarrow{\sim} & X_s(p^t) \\ \downarrow & & \downarrow \\ X_0^+(p^{2t}) & \xrightarrow{\sim} & X_s^n(p^t). \end{array}$$

Let $\eta$ be the image of $y \in X_0^+(p^{2t})(\mathbf{Q})$ by the lower isomorphism and $\eta$ is represented by $(E', \{A, B\})$ for an elliptic curve $E'$ over $\mathbf{Q}$, where $A$ and

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

$B$ are independent cyclic subgroups of $E'$ and $\{A, B\}$ is an unordered pair. The sections of the fiber $X_s(p^t)_\eta$ at $\eta$ are represented by $(E', (A, B))$ and $(E', (B, A))$ where $(A, B)$ and $(B, A)$ are ordered pairs.

$E'$ is defined over $\mathbf{Q}_p^{ur}$. $A$ and $B$ are defined over the quadratic field $L_0$ over $\mathbf{Q}_p^{ur}$. $E'$ has multiplicative reduction over a field $L$ of degree $e'$ over $\mathbf{Q}_p^{ur}$. Since $e'$ is even and $L_0$ is the unique tamely quadratic extension over $\mathbf{Q}_p^{ur}$, $L$ contains $L_0$. It implies that $(E', (A, B))$ defined over $L$ and $E'$ has multiplicative reduction over $L$. Hence, we may replace $e_K e'$ by $e'$. □

The following theorem is the same as Theorem (3.2) in [14].

THEOREM 3.10. *Let $(p, r)$ be a pair in Table (2), and $x$, $x'$, $y$ and $e_M$ be as above. Further $x$ and $x'$ are sections of $E_0^h \cup E_r^h$ if $p \neq 2$ and they are sections of $E_0^h \cup E_1^h \cup E_{r-1}^h \cup E_r^h$ if $p = 2$.*

*Proof.* Case for $p \geq 11$. Corollary 3.2, applied to the inequality $e_M e' \leq 6 < p - 1$, shows that $x$ and $x'$ are sections of $E_0^h \cup E_r^h$.

Case for $p = 7$. If $j(x) \not\equiv 0, 1728 \bmod \mathfrak{m}$, then $e_M e' = e_M \leq 2 < p - 1$. If $x$ is a supersingular point, then $e_M e' \geq 7^1 + 7^0 = 8$. But $e_M e' \leq 6$, so it is not supersingular. If $j(x) \equiv 0 \bmod \mathfrak{m}$ and $e_M e' \geq p - 1$, then $e_M = 2$ and $r$ is even. Then $e_M e' \leq 6 < p(p - 1)$. Therefore Corollary 3.2 and Lemma 3.1 give the result.

Case for $p = 5$ $(r \geq 3)$. We can show that $x$ is not a section of $E_i^h$ $(1 \leq i \leq r - 1)$ by the same argument as for $p = 7$. If $x$ is a supersingular point, then $e_M e' \geq 2 \cdot 5^1 = 10$. But $e_M e' \leq 6$, so it is not supersingular.

Case for $p = 3$ $(r \geq 4)$. The same argument as for $p = 7$ gives the result, except for the case when $j(x) \equiv 0 \bmod \mathfrak{m}$. If $r = 2t$ is even, then we can take $e_M = 1$ by Lemma 3.9. If $j(x) \equiv 0 \bmod \mathfrak{m}$, $r = 2t$ $(t \geq 2)$ and $x$ is supersingular, then $e_M e' \geq 3^2 + 3^{2-1} = 12$. But $e_M e' \leq 6$, so it is not supersingular. It remains the case for odd integer $r \geq 5$. It suffices to discuss the case for $r = 5$ and $j(x) \equiv 0 \bmod \mathfrak{m}$. If $x$ is supersingular, then $e_M e' \geq 2 \cdot 3^2 = 18$ but $e_M e' \leq 12$, so it is not supersingular.

Case for $p = 2$ $(r \geq 6)$. If $j(x) \not\equiv 0 \bmod \mathfrak{m}$, then $e' = 1$. If $x$ is a section of $E_i^h$ for $2 \leq i \leq r - 2$, then $e_M e' \geq 2^{m(i)-1} \geq 2$ by Corollary 3.2. By Lemma 3.8, if $x \notin E_{r/2}$, then $e_M = 1$ and if $x \in E_{r/2}$, then $e_M \leq 2$ and $2^{m(i)-1} \geq 4$. Summing up these facts, we have $x$ and $x'$ are sections of $E_0^h \cup E_1^h \cup E_{r-1}^h \cup E_r^h$. If $x$ is supersingular, then $j(x) \equiv 0 \bmod \mathfrak{m}$. But by the Theorem 3.3, it does not happen. So it is not supersingular. □

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

PROPOSITION 3.11. *Let $(p, r)$ be a pair as in Table (2), $x$ and $\mathfrak{m}$ be as at the beginning of this section. Let $f = f_{r,s}$ be the morphism of $\mathfrak{X}_0(p^r)^{smooth}$ to the Neron model $J_0(p^s)_{/\mathbf{Z}}$. If $x$ is a section of $E_0^h \cup E_r^h$, then $f(x) = 0$ (the unit section of $J_0(p^s)_{/\mathbf{Z}} \otimes \mathbf{F}_p$).*

*Proof.* [14, Proposition 3.3]. □

### 3.4. Rational points on $X_0^+(p^r)$

In this section, we resort to the global techniques in [14].

Let $(p, r)$ be a pair in Table (2). Let $y$ be a non-cuspidal $\mathbf{Q}$-rational point on $X_0^+(p^r)$, and $x$, $x' = w_{p^r}(x)$ the sections of the fiber $X_0(p^r)_y$ at $y$. Then $x$ and $x'$ are not defined over $\mathbf{Q}$ ([14, (1.1)]). They are defined over a quadratic field $M$. Denote also by $x$ and $x'$ (resp. $y$) the $\mathcal{O}_M$ (resp. $\mathbf{Z}$)-sections of $\mathfrak{X}_0(p^r)$ (resp. $\mathfrak{X}_0^+(p^r)$) with generic fibers $x$ and $x'$ (resp. $y$). Let $\mathfrak{p}$ be a prime of $M$ lying over the rational prime $p$ and $\kappa(\mathfrak{p})$ the residue filed $\mathcal{O}_M/\mathfrak{p}$.

PROPOSITION 3.12. *Let $x$ and $f$ be as in Proposition 3.11 above, and let $f^+$ be the morphisms defined in Section 3.1 for a triple $(p, r, s)$ in Table (2). If $f(x) \otimes \kappa(\mathfrak{p}) = 0$ and the Mordell-Weil group of $J_0^-(p^s)$ is of finite order, then $f^+(y) = 0$.*

*Proof.* [14, Proposition 3.4]. □

PROPOSITION 3.13. *Let $x$, $y$ and $f^+$ be as in Proposition 3.12 above. If $p \neq 37$ and $f^+(y) = 0$, then $y$ is a CM point.*

*Proof.* [14, Proposition 3.5]. □

THEOREM 3.14. *For the following pairs $(p, r)$, $n(p, r) = 0$:*

| $p$ | $r$ | |
|---|---|---|
| 2 | $\geq 6$ | |
| 3 | $\geq 4$ | |
| 5 | $\geq 4$ | |
| 7 | $\geq 3$ | |
| 11 | $\geq 2$ | |
| 13 | $\geq 3$ | |
| $p \geq 17$ | $\geq 2$ | *if* $\sharp J_0^-(p)(\mathbf{Q}) < \infty$. |

https://doi.org/10.1017/S0027763000008199 Published online by Cambridge University Press

*Proof.* [14, Theorem 3.6], which can be applied to $p = 5$ and to $p = 13$. We also use the results in [16], [8] and [7]. □

*Remark.* This theorem contains other new results owing to Y. Hasegawa, T. Hibino, N. Murabayashi and the second author for $p = 13$ and $p = 37$. In case of $p = 13$, Y. Hasegawa has shown the finiteness of $J_0^-(13^2)(\mathbf{Q})$ by calculating the special value of the $L$-function of a two dimensional factor of $J_0^-(13^2)$ ([7]). And in case of $p = 37$, Momose determined the rational points on $X_0(37N)/\langle w_{37N}\rangle$ ([15]), using the defining equation of $X_0(37)$ in [11] and the minimal model of $X_0(37)$ over $\mathbf{Z}[1/37]$. T. Hibino has given the relation of certain defining equation of $X_0(37)$ and invariant $j$-function. By using this result, T. Hibino and N. Murabayashi have decided the $\mathbf{Q}$-rational points of $X_{split}(37) \cong X_0^+(37^2)$ ([8]).

## References


[1] V. G. Bercovic, *The rational points on the jacobians of modular curves*, Math. USSR-sb., **30** (1976), 485–500.

[2] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J., **44** (1977), no. 4, 715–743.

[3] A. Brumer, *The rank of $J_0(N)$*, Columbia University Number Theory Seminar (New York, 1992). Astérisque no. 228 (1995), no. 3, 41–68.

[4] J. E. Cremona, Algorithms for modular elliptic curves, Cambridge University Press, Cambridge, 1992.

[5] P. Deigne and M. Rapoport, *Les schémas de modules des courbes elliptiques*, vol. II of the Proceedings of the International Summer School on Modular Functions, Antwerp, 1972, Lecture Notes in Math. vol. 349, Springer (1973).

[6] R. Fricke, Die Elliptischen Funktionen und ihre Anwendungen, Teubner, Leipzig-Berlin, 1922.

[7] Y. Hasegawa and F. Momose, *Rational points on $X_0^+(13^r)$*, preprint.

[8] T. Hibino and N. Murabayashi, *Modular equations of hyperelliptic $X_0(N)$ and an application*, Acta Arith., **82** (1997), no. 3, 279–291.

[9] N. Katz and R. Mazur, Arithmetic moduli of elliptic curves, Annals of Math. Studies 108, Princeton Univ. Press, 1985.

[10] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S., **47** (1977), 33–186.

[11] ———, *Rational points on modular curves*, Proceedings of conference on Modular functions held in Bonn, Lecture Notes in Math. vol. 601.

[12] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math., **25** (1974), 1–61.

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

[14] ———, *Rational points on the modular curves* $X_0^+(p^r)$, J. Fac. Sci. Univ. Tokyo Sect. IA, Math. **33** (1986), 441–466.
[15] ———, *Rational points on* $X_0(37N)/\langle w_{37N}\rangle$, preprint.
[16] D. Poulakis, *La courbe modulaire* $X_0(125)$ *et sa jacobienne*, J. of Number Theory, **25** (1987), 112–131.
[17] J. Silverman, The Arithmetic of Elliptic Curves, SLN **106**, Springer, 1986.
[18] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan 11, Iwanami Shoten, Tokyo-Princeton Univ. Press, Princeton N. J., 1971.
[19] J. Tate, *p-divisible groupes*, Proceedings of a Conference on Local Fields, Driebergen, 1966, Springer, 1967, 158–183.
[20] B. J. Birch and W. Kuyk, eds., Modular functions of one variable IV, Lecture Note in Math. vol. 476, Springer, 1975.

Fumiyuki Momose
*Department of Mathematics*
*Chuo University*
*1-13-27, Kasuga Bunkyou-ku*
*Tokyo, 112*
*Japan*
momose@math.chuo-u.ac.jp

Mahoro Shimura
*Department of Mathematics*
*Waseda University*
*3-4-1, Okubo Shinjuku-ku*
*Tokyo, 169-8555*
*Japan*
shimura@gm.math.waseda.ac.jp