COMPOSITIO MATHEMATICA

FUMIYUKI MOMOSE

Rational points on the modular curves $X_{\text{split}}(p)$

Compositio Mathematica, tome 52, nº 1 (1984), p. 115-137

<http://www.numdam.org/item?id=CM_1984__52_1_115_0>

Compositio Mathematica 52 (1984) 115–137

RATIONAL POINTS ON THE MODULAR CURVES $X_{\text{split}}(p)$

Fumiyuki Momose

For a prime number p, let $X_{\text{split}}(p)$ be the modular curve defined over $\mathbb{Q}$ which corresponds to the modular curve

$$\Gamma_{\text{split}}(p)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | b \equiv c \equiv 0 \text{ or } a \equiv d \equiv 0 \bmod p\right\},$$

i.e., $X_{\text{split}}(p) \otimes \mathbb{C} \simeq \Gamma_{\text{split}}(p) \backslash H \cup \mathbb{P}^1(\mathbb{Q})$, where $H=\{z \in \mathbb{C} | \operatorname{Im}(z)>0\}$. We call the points $\in \Gamma_{\text{split}}(p) \backslash \mathbb{P}^1(\mathbb{Q})$ the cusps on $X_{\text{split}}(p)$. Then $X_{\text{split}}(p) \backslash \{\text{cusps}\}$ is the coarse moduli space $(/\mathbb{Q})$ of the isomorphism classes of elliptic curves with an unordered pair of independent subgroups of rank p (see [9]). We here discuss the $\mathbb{Q}$-rational points on $X_{\text{split}}(p)$. For the prime numbers $p \leqslant 7$, $X_{\text{split}}(p) \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{Q}}$. Mazur [10] III§6 showed that for each prime number $p=11$ or $p \geqslant 17$, there are finitely many $\mathbb{Q}$-rational points on $X_{\text{split}}(p)$. We have no results for $X_{\text{split}}(13)$. Let y be a non cuspidal $\mathbb{Q}$-rational point on $X_{\text{split}}(p)$ $(p \geqslant 5)$. Then there exists an elliptic curve E defined over $\mathbb{Q}$ with independent subgroups A, B of rank p such that the set $\{A, B\}$ is $\mathbb{Q}$-rational and the pair $(E, \{A, B\})$ represents y (see [3] VI Proposition (3.2)). Let $\rho=\rho_p$ be the representation of the Galois action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion points $E_p(\overline{\mathbb{Q}})$. Then $\rho(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is contained in the normalizer of the split Cartan subgroup $\operatorname{Aut} A(\overline{\mathbb{Q}}) \times \operatorname{Aut} B(\overline{\mathbb{Q}})$ $(\subset \operatorname{Aut} E_p(\overline{\mathbb{Q}}) \xrightarrow{\sim} GL_2(\mathbb{F}_p))$. The "expected" $\mathbb{Q}$-rational points on $X_{\text{split}}(p) \backslash \{\text{cusps}\}$ $(p \geqslant 11?)$ are those which are represented by the elliptic curves with complex multiplication. Let E be an elliptic curve defined over $\mathbb{Q}$ which has complex multiplication over an imaginary quadratic field k. Let $p \geqslant 5$ be a rational prime which splits in k. Then there are two independent subgroups A, B of rank p such that the pair $(E, \{A, B\})$ represents a non cuspidal $\mathbb{Q}$-rational point on $X_{\text{split}}(p)$. We call such a point a C.M.point.

Let $X_0(p)$ be the modular curve $(/\mathbb{Q})$ corresponding to the modular group $\Gamma_0(p)$ and $J_0(p)$ the jacobian variety of $X_0(p)$. Let w_p be the fundamental involution of $X_0(p):(E, A) \mapsto (E/A, E_p/A)$, where $E_p=\ker(p: E \rightarrow E)$. Denote also by w_p the automorphism of $J_0(p)$ which is induced by the involution w_p. Put $J_0^-(p)=J_0(p)/(1+w_p)J_0(p)$. Denote by $n(p)$ the number of the $\mathbb{Q}$-rational points on $X_{\text{split}}(p)$ which are neither cusps nor C.M.points. Our main result is the following.

THEOREM (0.1): *Let $p = 11$ or $p \geqslant 17$ be a prime number such that the Mordell-Weil group of $J_0^-(p)$ is of finite order. Then $n(p) = 0$, provided $p \neq 37$.*

For the primes p, $11 \leqslant p < 300$, except for $p = (13)$, 151(?), 199(?), 227(?) and 277(?), the assumption in (0.1) above is satisfied (see [10] p. 40, [21] Table 5 pp. 135–141). For $p = 37$, we know that $J_0^-(37)(\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z}$ (see loc.cit.), but we see only that $n(37) \leqslant 1$, see (5.A). We may conjecture that $n(p) = 0$ for $p \geqslant 11$, $p \neq 13(?)$, $\neq 37(?)$. The outline of the proof of (0.1) above is as follows. Let $X_{\mathrm{sp.Car}}(p)$ be the modular curve $(/\mathbb{Q})$ corresponding to the modular group

$$\Gamma_{\mathrm{sp.Car}}(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid b \equiv c \equiv 0 \bmod p \right\}.$$

Let w be the fundamental involution of $X_{\mathrm{sp.Car}}(p): (E, A, B) \mapsto (E, B, A)$, which is represented by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Then $X_{\mathrm{split}}(p) = X_{\mathrm{sp.Car}}(p)/\langle w \rangle$. Let y be a non cuspidal $\mathbb{Q}$-rational point on $X_{\mathrm{split}}(p)$ and x, $w(x)$ the sections of the fibre $(X_{\mathrm{sp.Car}}(p))_y$. Then x, $w(x)$ are defined over a quadratic field k. Denote by $\mathscr{X}_{\mathrm{sp.Car}}(p)$ and $\mathscr{X}_{\mathrm{split}}(p)$ the normalizations of the projective j-line $\mathscr{X}_0(1) \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{Z}}$ in $X_{\mathrm{sp.Car}}(p)$ and $X_{\mathrm{split}}(p)$, respectively. We denote also by y (resp. x and $w(x)$) the $\mathbb{Z}$-section (resp. the $\mathcal{O}_k$-sections) of $\mathscr{X}_{\mathrm{split}}(p)$ (resp. $\mathscr{X}_{\mathrm{sp.Car}}(p)$) with the generic fibre y (resp. x and $w(x)$) above. Firstly, we show that $y \otimes \mathbb{F}_p$ is not a supersingular point and x, $w(x)$ are the sections of the smooth part of $\mathscr{X}_{\mathrm{sp.Car}}(p)$ (see (1.4), $p \geqslant 11$). Secondly, we show that $y \otimes \mathbb{F}_p$ is not a cusp and that the rational prime p splits in k, see (3.1), (3.2). Then there exists an elliptic curve E defined over $\mathbb{F}_p$ such that the pair $(E, \{\ker(\mathrm{Frob}), \ker(\mathrm{Ver})\})$ represents $y \otimes \mathbb{F}_p$, where Frob is the Frobenius map: $E \to E^{(p)} = E$ and Ver is the Verschiebung: $E = E^{(p)} \to E$. Define the morphism g of $X_{\mathrm{sp.Car}}(p)$ to $J_0(p)$ by

$$g: (E, A, B) \mapsto cl\big((E, A) - (E/B, E_p/B)\big).$$

Then g induces the morphism g^- of $X_{\mathrm{split}}(p)$ to $J_0^-(p)$, i.e., $g(x) \bmod (1 + w_p)J_0(p) = g^-(y)$. Denote also by g (resp. g^-) the morphism of $\mathscr{X}_{\mathrm{sp.Car}}(p)^{\mathrm{smooth}}$ to the Néron model $J_0(p)_{/\mathbb{Z}}$ over the base $\mathbb{Z}$ (resp. of $\mathscr{X}_{\mathrm{split}}(p)^{\mathrm{smooth}}$ to $J_0^-(p)_{/\mathbb{Z}}$). Then for the k-rational point x as above, $g(x) \otimes \mathbb{F}_p = 0$, see (3.3). Then the assumption $\# J_0^-(p)(\mathbb{Q}) < \infty$ implies that $g^-(y) = 0$. Let $(E, \{A, B\})$ $(/\mathbb{Q})$ be a pair which represents y. Then by the condition $g^-(y) = 0$, using the result of Ogg [14] Satz 1, we get $E \xrightarrow{\sim} E/B$, provided $p \neq 37$.

Further, we get the following estimate of $n(p)$. Let $\tilde{J}_0(p)$ be the "Eisenstein quotient" of $J_0(p)$, see [10].

THEOREM (0.2): $n(p) \leqslant \dim J_0(p) - \dim \tilde{J}_0(p)$ *for* $p \geqslant 17$.

In §5, we discuss the cases for $p = 13$ and 37.

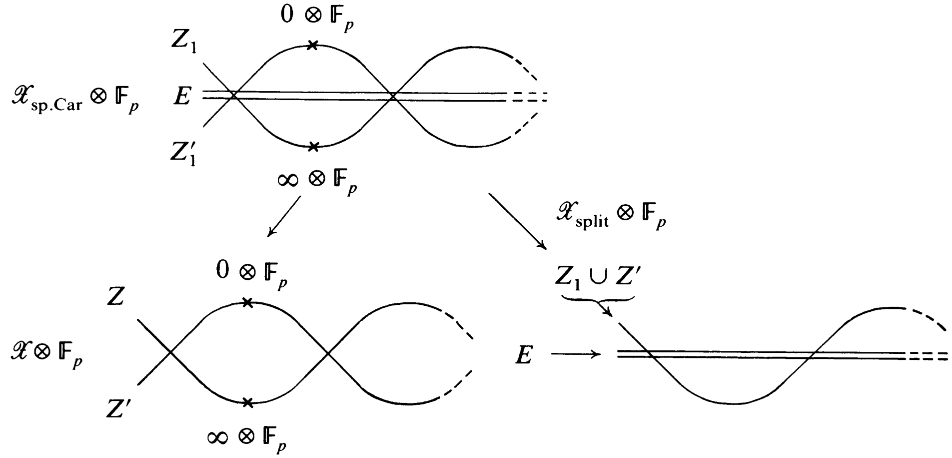
Notation: For a rational prime q, $\mathbb{Q}_q^{ur}$ denotes the maximal unramified extension of $\mathbb{Q}_q$ and $W(\overline{\mathbb{F}}_q)$ denotes the ring of integers of $\mathbb{Q}_q^{ur}$. For a finite extension K of $\mathbb{Q}$, $\mathbb{Q}_q$ or $\mathbb{Q}_q^{ur}$, $\mathcal{O}_K$ denotes the ring of integers of K. Let A be an abelian variety defined over K and G a finite subgroup of A defined over K. Then $A_{/\mathcal{O}_K}$ denotes the Néron model of A over the base $\mathcal{O}_K$ and $G_{/\mathcal{O}_K}$ denotes the flat closure of G in $A_{/\mathcal{O}_K}$ (which is a quasi finite flat subgroup scheme, see [17] §2). For a subscheme Y of a modular curve X $(/\mathbb{Z})$, Y^h denotes the open subscheme $Y \setminus \{$supersingular points on $Y \otimes \overline{\mathbb{F}}_p\}$ for the fixed rational prime p.

§1. Preliminaries

Let $p \geqslant 5$ be a prime number and $X_{\text{sp.Car}} = X_{\text{sp.Car}}(p)$ the modular curve $(/\mathbb{Q})$ corresponding to the modular group

$$\Gamma_{\text{sp.Car}}(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid b \equiv c \equiv 0 \bmod p \right\}.$$

$X_{\text{sp.Car}}$ is the coarse moduli space $(/\mathbb{Q})$ of the isomorphism classes of the generalized elliptic curves with an ordered pair of independent subgroups of rank p (see [3], [9]). Let w be the fundamental involution of $X_{\text{sp.Car}}: (E, A, B) \mapsto (E, B, A)$. Then $X_{\text{split}} = X_{\text{split}}(p) = X_{\text{sp.Car}}/\langle w \rangle$. Denote by $\mathscr{X}_{\text{sp.Car}} = \mathscr{X}_{\text{sp.Car}}(p)$, $\mathscr{X}_{\text{split}} = \mathscr{X}_{\text{split}}(p)$ and $\mathscr{X} = \mathscr{X}_0(p)$ the normalizations of the projective j-line $\mathscr{X}_0(p) \simeq \mathbb{P}^1_{\mathbb{Z}}$ in $X_{\text{Sp.Car}}$, X_{split} and $X = X_0(p)$, respectively. Let π be the canonical morphism of $\mathscr{X}_{\text{sp.Car}}$ to $\mathscr{X}$ which is generically defined by $(E, A, B) \mapsto (E, A)$. For a subscheme Y of a modular curve $/\mathbb{Z}$, Y^h denotes the open subscheme $Y \setminus \{$supersingular points on $Y \otimes \overline{\mathbb{F}}_p\}$ of Y. The special fibre $\mathscr{X} \otimes \mathbb{F}_p$ is reduced and has two irreducible components, say Z and Z', which intersect transversally at the supersingular points on $\mathscr{X} \otimes \mathbb{F}_p$ (see [3] VI§6). Z^h (resp. Z'^h) is the coarse moduli space $(/\mathbb{F}_p)$ of the isomorphism classes of the generalized elliptic curves with a subgroup A of rank p such that $A \xrightarrow{\sim} \mu_p$ (resp. $\xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$), isomorphic locally for the étale topology (see loc.cit.). The fibre $\pi^{-1}(Z)$ has one irreducible component Z_1, and $Z_1^h \to Z^h$ is radicial of degree p. The fibre $\pi^{-1}(Z')$ has two irreducible components Z_1' and E. The multiplicity of E is $p-1$ (see [15]) and $Z_1'^h \xrightarrow{\sim} Z'^h$ is an isomorphism (see loc.cit.). The fundamental involution w exchanges Z_1 by Z_1' and fixes E. These components Z_1, Z_1' and E_{red} intersect transversally at the supersingular points on $\mathscr{X}_{\text{sp.Car}} \otimes \mathbb{F}_p$.



Here, 0 and ∞ are the cuspidal sections which correspond to $(\mathbb{G}_m \times \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}, \mu_p)$ and $(\mathbb{G}_m \times \mathbb{Z}/p\mathbb{Z}, \mu_p, \mathbb{Z}/p\mathbb{Z})$ (resp. $(\mathbb{G}_m \times \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ and $(\mathbb{G}_m, \mu_p)$), see [3] II.

(1.1)N.B. (see [3] V, VII). Let $\mathcal{C}'$ be the algebraic stack which represents the following functor: for a scheme S $(/\mathbb{Z})$, $\mathcal{C}'(S)$ is the set of the isomorphism classes of the generalized elliptic curves C with an isomorphism α: $C_p \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \times \mu_p$. Then $\mathcal{C}'$ is an open subspace of $\mathcal{M}_p^h (= M_p^h$, which is a scheme for $p \geqslant 3$, see loc.cit. VII p. 300). Let $\Gamma_0(p)$, $\Gamma_{\mathrm{sp.Car}}(p)$ be the finite adèlic modular groups

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\hat{\mathbb{Z}}) \,|\, c \equiv 0 \bmod p \right\},$$

$$\Gamma_{\mathrm{sp.Car}}(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\hat{\mathbb{Z}}) \,|\, b \equiv c \equiv 0 \bmod p \right\}.$$

The natural morphisms of M_p^h to $M_{\mathrm{sp.Car}}(p)^h = M_p^h / \Gamma_{\mathrm{sp.Car}}(p)$ and to $M_0(p)^h = M_p^h / \Gamma_0(p)$ induce the surjective morphisms of $\mathcal{C}' \otimes \mathbb{F}_p$ onto $Z_1'^h$ and onto Z'^h. The subgroup of $\Gamma_0(p)$ consisting of the elements which fix $\mathcal{C}'$ is $\Gamma_{\mathrm{sp.Car}}(p)$. For a geometric point x on Z'^h, let (C, A) $(/\bar{\mathbb{F}}_p)$ be the pair which represents x. Then $\mathrm{Aut}(C, A) \subset \Gamma_{\mathrm{sp.Car}}(p)$ $(\bmod p)$. Therefore, π: $Z_1'^h \xrightarrow{\sim} Z'^h$ is an isomorphism and $Z_1'^h$ is the coarse moduli space $(/\mathbb{F}_p)$ of the isomorphism classes of the generalized elliptic curves with an ordered pair (A, B) of subgroups of rank p such that $(A, B) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z}, \mu_p)$, isomorphic locally for the étale topology. The morphism π induces $Z_1^h \to Z^h$: $(C, B, A) \longmapsto (C, B)$, so that $Z_1^h \longmapsto Z^h$ is radicial of degree p.

Let K be a finite extension of $\mathbb{Q}_p^{ur}$ of degree e with the ring $\mathcal{O} = \mathcal{O}_K$ of integers.

THEOREM (1.2) (*Raynaud* [17] §3 *Proposition* (3.3.2), *Oort-Tate* [16]): *Let* G_i $(i = 1, 2)$ *be finite flat group schemes of rank* p *over* Spec $\mathcal{O}$ *and* f: $G_1 \longrightarrow G_2$ *a homomorphism such that* $f \otimes K$: $G_1 \otimes K \xrightarrow{\sim} G_2 \otimes K$ *is an isomorphism. Then*,

(1) *If* $e < p - 1$, *then* f *is an isomorphism.*

(2) *If* $e = p - 1$ *and* f *is not an isomorphism, then* $G_1 \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})_{/\mathcal{O}}$ *and* $G_2 \xrightarrow{\sim} \mu_{p/\mathcal{O}}$.

LEMMA (1.3): *Let* E *be a semistable elliptic curve defined over* K *with independent subgroups* A, B *of rank* p *defined over* K. *If* $e < p - 1$, *then* $E_{/\mathcal{O}} \otimes \overline{\mathbb{F}}_p$ *is not supersingular and* $(E_{/\mathcal{O}})_p = A_{/\mathcal{O}} \oplus B_{/\mathcal{O}}$, *which is finite, where* $A_{/\mathcal{O}}$, $B_{/\mathcal{O}}$ *are the flat closures of* A *and* B *in the Néron model* $E_{/\mathcal{O}}$.

PROOF: (1.3.1). The case when $E_{/\mathcal{O}}$ is an elliptic curve (i.e., proper).

$A_{/\mathcal{O}}$ and $B_{/\mathcal{O}}$ are finite, hence they are finite flat group schemes. Consider the following morphisms f and f_A induced by the natural morphism of E onto E/B by the universal property of the Néron models:

$$\begin{array}{ccc} B_{/\mathcal{O}} \subset E_{/\mathcal{O}} & \xrightarrow{f} & (E/B)_{/\mathcal{O}} \\ \cup & \nearrow_{f_A} & \\ A_{/\mathcal{O}} & & \end{array}$$

Then $f_A \otimes K$: $A \xrightarrow{\sim} f(A)$ $(\subset E/B)$ is an isomorphism. By the condition $e < p - 1$, f_A is an isomorphism, see (1.2) above. Then $(E_{/\mathcal{O}})_p = A_{/\mathcal{O}} \oplus B_{/\mathcal{O}}$. If $(E_{/\mathcal{O}})_p(\overline{\mathbb{F}}_p) = \{0\}$, then $(E_{/\mathcal{O}})_p \otimes \overline{\mathbb{F}}_p \xrightarrow{\sim}$ Spec $\overline{\mathbb{F}}_p[X, Y]/(X^p, Y^p)$ as schemes. For a supersingular elliptic curve $F(/\overline{\mathbb{F}}_p)$, $F_p \xrightarrow{\sim}$ Spec $\overline{\mathbb{F}}_p[X]/(X^{p^2})$ as schemes. Therefore, $E_{/\mathcal{O}} \otimes \overline{\mathbb{F}}_p$ is not supersingular.

(1.3.2). The case when $E_{/\mathcal{O}}$ has multiplicative reduction.

We have the following exact sequence (see e.g., [8] Part 16):

$$0 \to \mu_p \to E_p \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Then A or $B \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$. By the condition $e < p - 1$, using the universal property of the Néron model $E_{/\mathcal{O}}$, we see that $(\mathbb{Z}/p\mathbb{Z})_{/\mathcal{O}} \subset E_{/\mathcal{O}}$. The connected component $(E_{/\mathcal{O}})_p^0$ of $(E_{/\mathcal{O}})_p$ of the unity is isomorphic to $\mu_{p/\mathcal{O}}$, see e.g., loc.cit., [3] VII. Then $(E_{/\mathcal{O}})_p \xrightarrow{\sim} \mu_{p/\mathcal{O}} \oplus (\mathbb{Z}/p\mathbb{Z})_{/\mathcal{O}}$ are finite schemes. Then, by the same way as in (1.3.1) above, we get $(E_{/\mathcal{O}})_p = A_{/\mathcal{O}} \oplus B_{/\mathcal{O}}$. □

COROLLARY (1.4): *Let* E *be an elliptic curve defined over* $\mathbb{Q}_p^{ur}$ *with independent subgroups* A, B *of rank* p *such that the set* $\{A, B\}$ *is* $\mathbb{Q}_p^{ur}$*-rational. Let* y *be a* $W(\overline{\mathbb{F}}_p)$*-section of* $\mathcal{X}_{\text{split}}$ *whose generic fibre is represented* *by the pair* $(E, \{A, B\})$. *If* $p \geqslant 11$, *then* y *is a section of the smooth part of* $\mathscr{X}_{\text{split}}$.

Proof: Let x, $w(x)$ be the sections of the fibre $(\mathscr{X}_{\text{sp.Car}})_y$, which are defined over an extension K' of $\mathbb{Q}_p^{ur}$ of degree $\leqslant 2$. We may assume that the triple (E, A, B) represents $x \otimes K'$. There exists an extension K of $\mathbb{Q}_p^{ur}$ of degree e with $e|4$ or $e|6$ over which E has semistable reduction (see e.g., [19] §5 (5.6)). We may take K with $e = 4$ or $e = 6$. Then $K' \subset K$. Let $\mathcal{O}$ denote $\mathcal{O}_K$. Then the triple $(E_{/\mathcal{O}}, A_{/\mathcal{O}}, B_{/\mathcal{O}})$ represents the section $x \otimes \mathcal{O}$: Spec $\mathcal{O} \longrightarrow \mathscr{X}_{\text{sp.Car}}$. By the condition that $e < 11 - 1 \leqslant p - 1$, $x \otimes \bar{F}_p$ is a section of $Z_1^h \cup Z_1'^h$, see (1.1), (1.3) above. □

§2. Modular curves and Jacobian variety of $X_0(p)$

Let $J = J_0(p)$ be the jacobian variety of $X = X_0(p)$, C the cuspidal subgroup of J which is generated by the class $cl((0) - (\infty))$. Put $J^- = J_0^-(p) = J/(1 + w_p)J$. Mazur [10] defined the "Eisenstein quotient" of J. Put $\mathbb{T} = \operatorname{End} J$, which is generated by the Hecke operators T_l and w_p, for the rational primes $l \neq p$, see [10] II Proposition (9.5). Let $\mathscr{I}$ be the ideal of $\mathbb{T}$ generated by $\eta_l = 1 + l - T_l$ and $w_p + 1$, for the rational primes $l \neq p$, which is called the "Eisenstein ideal". The Eisenstein quotient $\tilde{J} = \tilde{J}_0(p)$ is the quotient of J by the ($\mathbb{Q}$-rational) abelian subvariety $(\bigcap_{n \geqslant 1} \mathscr{I}^n)J$.

Theorem (2.1) (Mazur loc.cit.): *The natural morphism* $J \longrightarrow \tilde{J}$ *induces an isomorphism of* C *of order* $n = \operatorname{num}((p-1)/12)$ *onto the Mordell-Weil group of* $\tilde{J}$ *and* $\tilde{J}$ *is an optimal quotient of* J^-. *Further, the natural morphisms* $J(\mathbb{Q})_{\text{tor}} \xrightarrow{\sim} J^-(\mathbb{Q})_{\text{tor}} \xrightarrow{\sim} \tilde{J}(\mathbb{Q})$ *are isomorphisms.*

Proposition (2.2) (Mazur loc.cit. II Lemma (12.5)): *If* $p \equiv 1 \bmod 8$, $C_{/\mathbb{Z}}$ (= *the flat closure of* C *in the Néron model* $J_{/\mathbb{Z}}$) *contains the multiplicative group* $\mu_{2/\mathbb{Z}}$.

Let C_1, C_p be the morphisms of $X_{\text{sp.Car}}$ to J defined by $(E, A, B) \longmapsto cl((E, A) - (0))$ and $\longmapsto cl((E/B, E_p/B) - (0))$, respectively. Put $g = C_1 - C_p$: $(E, A, B) \longmapsto cl((E, A) - (E/B, E_p/B))$,

$$g: X_{\text{sp.Car}} \xrightarrow{C_1 \times C_p} J \times J \to J.$$
$$(x, y) \longmapsto x - y$$

Then g induces the following commutative diagram:

$$\begin{array}{ccccc}
X_{\text{sp.Car}} & \xrightarrow{\text{can.}} & X_{\text{split}} & & \\
g \downarrow & \circlearrowleft \; g^- & \downarrow \; \circlearrowleft & \searrow \tilde{g} & \\
J & \xrightarrow{\text{can.}} & J^- & \xrightarrow{\text{can.}} & \tilde{J}.
\end{array}$$

We denote also by g, g^- and $\tilde{g}$ the morphisms $\mathscr{X}_{\text{sp.Car}}^{\text{smooth}} \longrightarrow J_{/\mathbb{Z}}$, $\mathscr{X}_{\text{split}}^{\text{smooth}} \longrightarrow J_{/\mathbb{Z}}^-$ and $\mathscr{X}_{\text{split}}^{\text{smooth}} \longrightarrow \tilde{J}_{/\mathbb{Z}}$ which are induced by g, g^- and $\tilde{g}$ (by the universal property of the Néron models), respectively. Let $\tilde{\mathscr{X}} = \tilde{\mathscr{X}}_0(p) \longrightarrow \operatorname{Spec} \mathbb{Z}$ be the minimal model of $X = X_0(p)$ (see [3] VI§6). Let ι be the isomorphism induced by the duality of Grothendieck (see [11] §2):

$$\iota\colon \operatorname{Cot} J_{/\mathbb{Z}} \xrightarrow{\ \sim\ } H^0(\tilde{\mathscr{X}}, \Omega),$$

where $\operatorname{Cot} J_{/\mathbb{Z}}$ is the cotangent space of $J_{/\mathbb{Z}}$ at origin and Ω is the sheaf of regular differentials (see loc.cit., [3] p. 161). For a rational prime q, let $R = W(\overline{\mathbb{F}}_q)$ be the ring of integers of $\mathbb{Q}_q^{ur}$ and x: $\operatorname{Spec} R \to \mathscr{X}^{\text{smooth}}$ a section. Denote by $\operatorname{Spec} R[[q]]$ the completion of $\mathscr{X}$ along the section x.

Proposition (2.3) (Mazur [11] §2 Lemma (2.1)): *The following diagram is commutative up to sign*:

$$\begin{array}{ccc} \operatorname{Cot} J_{/R} & \xrightarrow[\ \sim\ ]{\iota} & H^0(\tilde{\mathscr{X}} \otimes R, \Omega) \\ & \operatorname{Cot}_x \searrow \qquad \swarrow & \omega = \sum a_m q^m \dfrac{dq}{q} \\ & \operatorname{Cot}_x \mathscr{X} = R \ni a_1 & \swarrow \end{array}$$

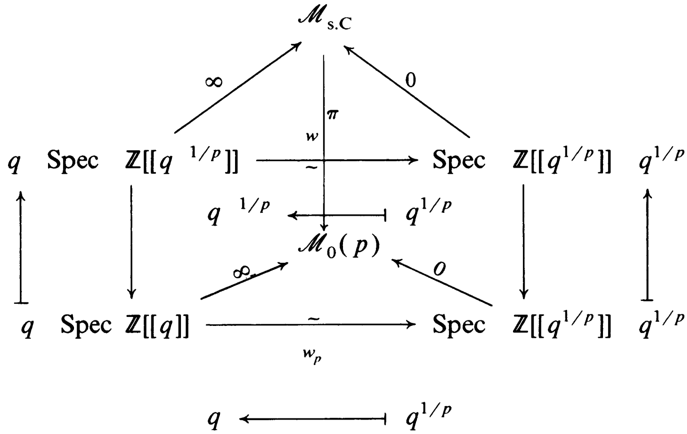
Denote by u the natural morphism of $J_{/\mathbb{Z}}$ onto $\tilde{J}_{/\mathbb{Z}}$. By [11] Corollary (1.1), $\operatorname{Cot} \tilde{J}_{/\mathbb{Z}} \otimes \mathbb{F}_q$ can be regarded as a subspace of $\operatorname{Cot} J_{/\mathbb{Z}} \otimes \mathbb{F}_q \xrightarrow{\sim} H^0(\tilde{\mathscr{X}} \otimes \mathbb{F}_q, \Omega)(= H^0(\mathscr{X} \otimes \mathbb{F}_q, \Omega)$, see [3] p. 162 (2.3)), for $q \neq 2$.

Lemma (2.4) (*Mazur* [11] §3): *Under the notation as above, let* $x = 0$ *or* ∞ (= *the cuspidal sections*). *If* $p = 11$ *or* $p \geqslant 17$, *for each rational prime* $q \neq 2$, *there exists a form* $\omega = \Sigma a_m q^m \mathrm{d}q/q \in \operatorname{Cot} \tilde{J}_{/\mathbb{Z}}$ *such that* $a_1 \in \mathbb{Z}_q^\times$.

Let m: $X \longrightarrow Y$ be a morphism of schemes. The morphism m is a formal immersion along a section x of X if $m^*(\widehat{\mathcal{O}_{Y,f(x)}}) = \widehat{\mathcal{O}_{X,x}}$, where $\widehat{\mathcal{O}_{Y,f(x)}}$ and $\widehat{\mathcal{O}_{X,x}}$ are the completions of the local rings along the sections $f(x)$ and x, respectively. If $m^*(\mathcal{O}_{Y,f(x)}/m_{f(x)}) = \mathcal{O}_{X,x}/m_x$ and $\operatorname{Cot}_x(m)$: $\operatorname{Cot}_{f(x)} Y \longrightarrow \operatorname{Cot}_x X$ is surjective, then m is a formal immersion along x (see E.G.A.IV, 17.44). Here, $m_{f(x)}$ and m_x are the maximal ideals of the local rings at $f(x)$ and x.

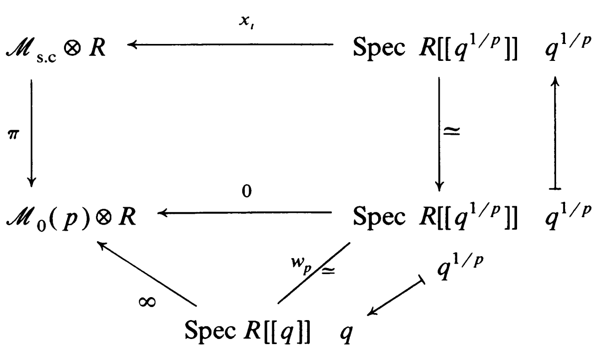
Proposition (2.5): *Let* $q \neq 2$ *be a rational prime. If* $p = 11$ *or* $p \geqslant 17$, $ug \otimes \mathbb{Z}_q\colon \mathscr{X}_{\text{sp.Car}} \otimes \mathbb{Z}_q^{\text{smooth}} \to \tilde{J}_{/\mathbb{Z}_q}$ *is a formal immersion along the cuspidal sections* 0 *and* ∞. *Further, if* $q \neq 2$ *nor* p, $ug \otimes \mathbb{Z}_q$ *is a formal immersion along any cuspidal section of* $\mathscr{X}_{\text{sp.Car}} \otimes \mathbb{Z}_q$.

Proof: There are $p+1$ cuspidal sections 0, ∞ and x_i of $\mathscr{X}_{\text{sp.Car}}$ which correspond to 0, ∞ and $1/i$ $(1 \leqslant i \leqslant p-1)$ by the canonical identification of $X_{\mathrm{sp.Car}} \otimes \mathbb{C}$ with $\Gamma_{\mathrm{sp.Car}}(p)\backslash H \cup \mathbb{P}^1(\mathbb{Q})$, where $H = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. The cuspidal sections 0 and ∞ are $\mathbb{Q}$-rational, and x_i are $\mathbb{Q}(\zeta_p)$-rational, where ζ_p is a primitive p-th root of 1. Let $\mathscr{M}_{\mathrm{s.C}} = \mathscr{M}_{\mathrm{sp.Car}}(p)$ and $\mathscr{M}_0(p)$ be the fine moduli stacks corresponding to finite adèlic modular groups $\Gamma_{\mathrm{sp.Car}}(p)$ and $\Gamma_0(p)$, respectively, see (1.1). The correspondence of the local coordinates along the cuspidal sections 0 and ∞ is as follows:



For each rational prime q, $\mathrm{Cot}(\pi)$ (resp. $\mathrm{Cot}(w_p \pi w)$): $\mathrm{Cot}_0 \mathscr{X} \otimes \mathbb{Z}_q \longmapsto \mathrm{Cot}_0 \mathscr{X}_{\mathrm{sp.Car}} \otimes \mathbb{Z}_q$ is an isomorphism (resp. a 0-map). Take a form $\omega \in \mathrm{Cot}\, \tilde{J}_{/\mathbb{Z}_q}$ as in Lemma (2.4) (for $q \neq 2$), then by Proposition (2.3), $\mathrm{Cot}(ug) = \mathrm{Cot}(uC_1) - \mathrm{Cot}(uC_p)$: $\mathrm{Cot}\, \tilde{J}_{/\mathbb{Z}_q} \longrightarrow \mathrm{Cot}_0 \mathscr{X}_{\mathrm{sp.Car}} \otimes \mathbb{Z}_q$ sends ω to $\pm a_1 \in \mathbb{Z}_q^{\times}$.

To investigate the cuspidal sections x_i, we consider all over $R = \mathbb{Z}[1/2p, \zeta_p]$. The group $\left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \middle| a \in (\mathbb{Z}/p\mathbb{Z})^{\times} \right\}$ acts trivially on $\mathscr{M}_{\mathrm{s.C}} \otimes R$. The correspondence of the local coordinates along the cuspidal sections x_i is as follows:



The Tate curves along these cuspidal sections are as follows (see [3] VII):

$$\begin{array}{ccc}
 & & (\overline{\mathscr{G}}_m^{q^{1/p}}\ q^{\mathbf{Z}}, \mathbf{Z}/p\mathbf{Z}(q^{1/p}), \mathbf{Z}/p\mathbf{Z}(\zeta_p q^{\prime/p})) \\
 & & \downarrow \\
(\overline{\mathscr{G}}_m^{q^{1/p}}/(q^{1/p})^{\mathbf{Z}}, \mu_p) & & (\overline{\mathscr{G}}_m^{q^{1/p}}/q^{\mathbf{Z}}, \mathbf{Z}/p\mathbf{Z}(q^{1/p})) \\
\updownarrow & \swarrow^{w_p} & \\
(\overline{\mathscr{G}}_m^{q}/q^{\mathbf{Z}}, \mu_p) & &
\end{array}$$

Here, $\mathbf{Z}/p\mathbf{Z}(q^{1/p})$ and $\mathbf{Z}/p\mathbf{Z}(\zeta_p q^{\prime/p})$ are the subgroup schemes of the Tate curve $\overline{\mathscr{G}}_m^{q^{1/p}}/q^{\mathbf{Z}}$ generated by the sections $q^{1/p}$ and $\zeta_p q^{\prime/p}$, respectively. Consider the morphism $w_p \pi w$: $(E, A, B) \longmapsto (E/B, E_p/B)(x_i \overset{w}{\longmapsto} x_{p-i} \overset{\pi}{\longmapsto} 0 \overset{w_p}{\longmapsto} \infty)$:

along x_i

$$\begin{array}{ll}
(\overline{\mathscr{G}}_m^{q^{1/p}}/q^{\mathbf{Z}}, \mathbf{Z}/p\mathbf{Z}(q^{1/p}), \mathbf{Z}/p\mathbf{Z}(\zeta_p q^{\prime/p})) & \\
\qquad\qquad \searrow^{w} & \\
\zeta_p^{a(i)} q^{1/p} \nwarrow & \text{along } x_{p-i} \\
\quad \zeta_p^{a(i)} q^{1/p} & (\overline{\mathscr{G}}_m^{q^{1/p}}/q^{\mathbf{Z}}, \mathbf{Z}/p\mathbf{Z}(\zeta_p q^{\prime/p}), \mathbf{Z}/p\mathbf{Z}(q^{1/p})) \\
\quad \| & \downarrow \quad \text{by } \begin{pmatrix} a(i) & 0 \\ 0 & i \end{pmatrix} \in SL_2(\mathbf{Z}/p\mathbf{Z}) \\
\quad \zeta_p^{a(i)} q^{1/p} & (\overline{\mathscr{G}}_m^{q^{1/p}}/q^{\mathbf{Z}}, \mathbf{Z}/p\mathbf{Z}(\zeta_p^{a(i)} q^{1/p}), \mathbf{Z}/p\mathbf{Z}(q^{\prime/p})) \\
\quad \updownarrow & \downarrow \\
\quad q^{1/p} & (\overline{\mathscr{G}}_m^{q^{1/p}}/q^{\mathbf{Z}}, \mathbf{Z}/p\mathbf{Z}(q^{1/p}), \mathbf{Z}/p\mathbf{Z}(\zeta_p^{-1} q^{\prime/p})) \\
\quad \| & \downarrow \\
\quad q^{1/p} & (\overline{\mathscr{G}}_m^{q^{1/p}}/q^{\mathbf{Z}}, \mathbf{Z}/p\mathbf{Z}(q^{1/p})) \\
q \nearrow & \text{along } 0 \\
(\overline{\mathscr{G}}_m^{q}/q^{\mathbf{Z}}, \mu_p) \overset{w_p}{\longleftarrow} & \\
\text{along } \infty &
\end{array}$$

Here, $a(i)$ is an integer congruent to $i^{-1} \bmod p$. Take the local coordinates along x_i, ∞ and 0 such that

$$\mathrm{Cot}(\pi)\colon \mathrm{Cot}_0 \mathscr{X} \otimes R \xrightarrow{\ \simeq\ } \mathrm{Cot}_{x_i} \mathscr{X}_{\mathrm{sp.Car}} \otimes R$$

$$\mathrm{Cot}(w_p)\colon \mathrm{Cot}_\infty \mathscr{X} \otimes R \xrightarrow{\ \simeq\ } \mathrm{Cot}_0 \mathscr{X} \otimes R$$

are the identity maps of R-modules R. Then

$$\mathrm{Cot}(w_p \pi w)\colon \mathrm{Cot}_\infty \mathscr{X} \otimes R \longrightarrow \mathrm{Cot}_{x_i} \mathscr{X}_{\mathrm{sp.Car}} \otimes R : 1 \longmapsto \zeta,$$

for a primitive p-th root ζ of 1. Take a form $\omega \in \mathrm{Cot}\, \tilde{J}/_{\mathbf{Z}_q}$ as in Lemma

(2.4), then by Proposition (2.3), $\mathrm{Cot}(ug)(\omega) = \pm a_1(1-\zeta) \in (R \otimes \mathbb{Z}_q)^{\times}$.
□

§3. Rational points on $X_{\mathrm{split}}(p)$

Let $p \geqslant 11$ be a prime number. Let y be a non cuspidal $\mathbb{Q}$-rational point on $X_{\mathrm{split}} = X_{\mathrm{split}}(p)$ and x, $w(x)$ the sections of the fibre $(X_{\mathrm{sp.Car}})_y$. Then there exists a number field k of degree $\leqslant 2$ over which x and $w(x)$ are defined. We denote also by y (resp. x and $w(x)$) the $\mathbb{Z}$-section (resp. $\mathcal{O}_k$-sections) of $\mathcal{X}_{\mathrm{split}}$ (resp. $\mathcal{X}_{\mathrm{sp.Car}}$) with the generic fibre y (resp. x and $w(x)$) above. There exists an elliptic curve E defined over $\mathbb{Q}$ with independent subgroups A, B of rank p such that the set $\{A, B\}$ is $\mathbb{Q}$-rational and the pair $(E, \{A, B\})$ represents $y = y \otimes \mathbb{Q}$ (see [3] VI Proposition (3.2)). Then A and B are defined over k. By Corollary (1.4), x and $w(x)$ are the sections of $\mathcal{X}_{\mathrm{sp.Car}}^{\mathrm{smooth}}$. We call that y (or x) has potentially good reduction at a prime q if E has potentially good reduction at q.

PROPOSITION (3.1): *Under the notation as above. If $p \neq 13$ ($\geqslant 11$), y has potentially good reduction at the rational prime $q \neq 2$.*

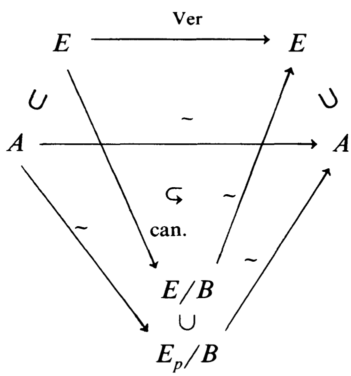
PROOF: Denote by 0, y_i $(1 \leqslant i \leqslant (p-1)/2)$ the cuspidal sections of $\mathcal{X}_{\mathrm{split}}$ which are the images of $\{0, \infty\}$ and $\{x_i, x_{p-1}\}$, respectively. If y does not have potentially good reduction at a rational prime q, then $y \otimes \mathbb{F}_q = 0 \otimes \mathbb{F}_q$ or $= y_i \otimes \mathbb{F}_q$ for an integer i. The latter case occurs only when $q \equiv \pm 1 \bmod p$. Denote also by C the cyclic subgroup of the image of the cuspidal subgroup $C = \langle cl((0)-(\infty))\rangle$ by the natural morphism of J onto $\tilde{J}$, see (2.1). Then $\tilde{g}(y) \otimes \mathbb{Z}[1/2] \in C_{/\mathbb{Z}[1/2]} \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})_{/\mathbb{Z}[1/2]}$, see loc. cit.. If $y \otimes \mathbb{F}_q = 0 \otimes \mathbb{F}_q$, Then $\tilde{g}(y) = 0$. If $y \otimes \mathbb{F}_q = y_i \otimes \mathbb{F}_q$, then $\tilde{g}(y) =$ the image of $cl((0)-(\infty))$. Then by Proposition (2.5), $y = 0$ or $= y_i$, which is a contradiction (see [11] Corollary (4.3)). □

LEMMA (3.2): *Under the notation as above. The sections x and $w(x)$ are not $\mathbb{Q}$-rational and the prime p splits in k.*

PROOF: The modular curve $X_0(p^2)$ is isomorphic over $\mathbb{Q}$ to $X_{\mathrm{sp.Car}} = X_{\mathrm{sp.Car}}(p)$: $(E, A) \longmapsto (E/A_p, A/A_p, E_p/A_p)$, where $A_p = \ker(p : A \to A)$. For the primes p ($\geqslant 7$), $X_0(p^2)(\mathbb{Q}) = \{0, \infty\}$, see [11], [6,7], [13]. Therefore, x and $w(x)$ are not $\mathbb{Q}$-rational and $w(x) = x^{\sigma}$ for $1 \neq \sigma \in \mathrm{Gal}(k/\mathbb{Q})$. If p ramifies in k, then $w(x) \otimes \mathbb{F}_p = x^{\sigma} \otimes \mathbb{F}_p = x \otimes \mathbb{F}_p$. If p remains prime in k, then $w(x) \otimes \mathbb{F}_{p^2} = x^{\sigma} \otimes \mathbb{F}_{p^2} = (x \otimes \mathbb{F}_{p^2})^{(p)}$, where $(x \otimes \mathbb{F}_{p^2})^{(p)}$ is the image of $x \otimes \mathbb{F}_{p^2}$ by the Frobenius map: $\mathcal{X}_{\mathrm{sp.Car}} \otimes \mathbb{F}_p \longrightarrow \mathcal{X}_{\mathrm{sp.Car}} \otimes \mathbb{F}_p$. The irreducible components Z_1, Z_1' and E_{red} are $\mathbb{F}_p$-rational, see §1 (1.1). In both cases above, $x \otimes \mathbb{F}_{p^2}$ is a section of E, see loc.cit. But, $x \otimes \mathbb{F}_{p^2}$ is a section of $Z_1^h \cup Z_1'^h$, see (1.4). □

PROPOSITION (3.3): *Let x and $w(x)$ be the sections as above for a rational prime $p \neq 13$ ($\geqslant 11$) and g the morphism of $\mathscr{X}^{\text{smooth}}_{\text{sp.Car}}$ to $J_{/\mathbb{Z}}$ defined in* §2: $(E, A, B) \longmapsto cl((E, A) - (E/B, E_p/B))$. *Then* $g(x) \otimes \mathbb{F}_p = g(w(x)) \otimes \mathbb{F}_p = 0$.

PROOF: By Corollary (1.4), $x \otimes \mathbb{F}_p$ and $w(x) \otimes \mathbb{F}_p$ are the sections of $Z_1^h \cup Z'^h_1$, see (3.2) above. We may assume that $x \otimes \mathbb{F}_p$ is a section of Z_1^h, changing x by $w(X)$ if necessary. Then there exists an elliptic curve E defined over $\mathbb{F}_p$ such that the triple (E, ker (Frob), ker(Ver)) represents $x \otimes \mathbb{F}_p$ and (E, ker(Ver), ker(Frob)) represents $w(x) \otimes \mathbb{F}_p$, where Frob is the Frobenius map: $E \longrightarrow E = E^{(p)}$ and Ver is the Verschiebung: $E = E^{(p)} \longrightarrow E$. Put A = ker(Frob) and B = ker(Ver). Then (E, A) represents $\pi(x) \otimes \mathbb{F}_p$ and $(E/B, E_p/B)$ represents $w_p \pi w(x) \otimes \mathbb{F}_p$. The following diagram is commutative:



i.e., $(E, A) \xrightarrow{\simeq} (E/B, E_p/B)$. Therefore $\pi(x) \otimes \mathbb{F}_p = w_p \pi w(x) \otimes \mathbb{F}_p$. Then $g(x) \otimes \mathbb{F}_p = g(w(x)) \otimes \mathbb{F}_p = 0$. □

COROLLARY (3.4): *Under the notation and the assumption on p as above. Let g, $\tilde{g}$ be the morphisms defined in* §2. *Then $\tilde{g}(y) = 0$. If the Mordell-Weil group of J^- is finite, then $g^-(y) = 0$.*

PROOF: By Theorem (2.1), $\tilde{g}(y) \otimes \mathbb{Z}_p$ is a section of the finte étale subgroup which is the image of $C_{/\mathbb{Z}_p} \xrightarrow{\simeq} (\mathbb{Z}/n\mathbb{Z})_{/\mathbb{Z}_p}$, see (2.1). Then $\tilde{g}(y) = 0$, see (3.3) above. If the Mordell-Weil group of J^- is finite, then $g^-(y) \otimes \mathbb{Z}_p$ is a secton of the image of $C_{/\mathbb{Z}_p}$ see (2.1). □

REMARK (3.5): By this corollary (3.4), we see that $y \otimes \mathbb{F}_p \neq y_i \otimes \mathbb{F}_p$ for all rational primes q. Because, $g(y_i)$ = the image of the generator $cl((0) - (\infty))$ of C, which is of order $n = \text{num}((p-1))/12)$, see (2.1).

COROLLARY (3.6): *If $p \equiv 1$ mod 8, then y has potentially good reduction at $q = 2$.*

PROOF: If y does not have potentially good reduction at $q=2$, then $y \otimes \mathbb{F}_2 = 0 \otimes \mathbb{F}_2$. The morphism $\mathrm{Cot}(\pi)$; $\mathrm{Cot}_0\mathscr{X} \otimes \mathbb{Z}_2 \xrightarrow{\sim} \mathrm{Cot}_0\mathscr{X}_{\mathrm{sp.Car}} \otimes \mathbb{Z}_2$ is an isomorphism and $\mathrm{Cot}(w_p\pi w)$: $\mathrm{Cot}_0\mathscr{X} \otimes \mathbb{Z}_2 \longrightarrow \mathrm{Cot}_0\mathscr{X}_{\mathrm{sp.Car}} \otimes \mathbb{Z}_2$ is a 0-map, see (2.5). It is enough to show that there exists a form $\omega \in u^*(\mathrm{Cot}\ \tilde{J}_{/\mathbb{Z}_2})$ such that $\omega(0 \otimes \mathbb{F}_2) \neq 0$, where u: $J_{/\mathbb{Z}_2} \longrightarrow \tilde{J}_{/\mathbb{Z}_2}$ is the natural morphism. The cyclic subgroup $C_{/\mathbb{Z}_2}$ contains the multiplicative group $\mu_{p/\mathbb{Z}_2}$, see (2.2). Consider the morphism $u \otimes \mathbb{Z}_2$:

$$\begin{array}{ccc} J_{/\mathbb{Z}_2} & \longrightarrow & \tilde{J}_{/\mathbb{Z}_2} \\ \cup & & \cup \\ \mu_{2/\mathbb{Z}_2} & \xrightarrow{\sim} & \mu_{2/\mathbb{Z}_2}. \end{array}$$

By Theorem (1.2) and (2.1), $u|\mu_{2/\mathbb{Z}_2}$ is an isomorphism. Then $u^*(\mathrm{Cot}\ \tilde{J}_{/\mathbb{Z}_2}) \otimes \mathbb{F}_2 \neq \{0\}$, which is a $\mathbb{T} = \mathbb{Z}[T_l, w_p]_{l \neq p}$-module. Using the q-expansion principle (see [11] §3), we get a desired form. □

To prove the main theorem, we need the following result of Ogg [14] Satz 1.

THEOREM (3.7) (Ogg, loc. cit.): *Let p be a prime number such that the genus $g_0(p)$ of $X = X_0(p) \geqslant 2$. Then the group* Aut $X_0(p)$ *of automorphisms of $X \otimes \mathbb{C} = \langle w_p \rangle$, provided $p \neq 37$.*

REMARK (3.8): Aut $X_0(37) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, see loc.cit., [12] §5.

THEOREM (3.9): *Let $p = 11$ or $p \geqslant 17$ be a prime number such that the Mordell-Weil group of $J^- = J_0^-(p)$ is of finite order. Then $X_{\mathrm{split}}(p)(\mathbb{Q})$ consists of the cusps and the C.M. points.*

PROOF: Let y be a non cuspidal $\mathbb{Z}$-section of $\mathscr{X}_{\mathrm{split}} = \mathscr{X}_{\mathrm{split}}(p)$ and x a section of the fibre $(\mathscr{X}_{\mathrm{sp.Car}})_y$. Let $(E, \{A, B\})$ $(/\mathbb{Q})$ be a pair which represents y (see [3] VI Proposition (3.2)). Denote by $g_+ = g_+(p)$ the genus of $X_0^+(p) = X_0(p)/\langle w_p \rangle$. If $g_+ = 0$, then $J = J^-$, which has the Mordell-Weil group of finite order (see [10] p. 40, [21] Table 5 pp. 135–141). By Corollary (3.4), $0 = g(x) = cl((\pi(x)) - (w_p\pi w(x)))$. Then $\pi(x) = w_p\pi w(x)$, because $g_0(p) \geqslant 1$ for $p = 11$ and $p \geqslant 17$. Then $E \xrightarrow{\sim} E/B$ $(/\mathbb{Q})$, hence E is an elliptic curve with complex multiplication. If $g_+ > 0$, by Corollary (3.4), $0 = (1 - w_p)g(x) = cl((\pi(x)) + (\pi w(x)) - (w_p(\pi(x)) - (w_p\pi w(x)))$. Then there exists a rational function f on $X_0(p)$ whose divisor $(f) = (\pi(x)) + (\pi w(x)) - (w_p\pi(x)) - (w_p\pi w(x))$. If the degree of $f \leqslant 1$, by the same way as above, we see that y is a C.M. point. If the degree of $f = 2$, then $X_0(p)$ has the hyperelliptic involution γ such that $\gamma\pi(x) = \pi w(x)$. By Theorem (3.7) above, such a γ exists only when $p = 37$ (, $g_0(p) \geqslant 2$). □

§4. Effective bound of rational points

In this section, we estimate the number of the $\mathbb{Q}$-rational points on $X_{\mathrm{split}} = X_{\mathrm{split}}(p)$ for $p \geqslant 17$. Let y be a non cuspidal $\mathbb{Q}$-rational point on X_{split} ($p \geqslant 17$) and x, $w(x)$ the sections of the fibre $(X_{\mathrm{sp.Car}})_y$, which are defined over a quadratic field k. The rational prime p splits in k and x, $w(x)$ become $\mathbb{Z}_p$-sections of the smooth part of $\mathscr{X}_{\mathrm{sp.Car}}$, see (1.4), (3.2). Let $\tilde{g}$ (resp. g) be the morphism of $\mathscr{X}_{\mathrm{split}}^{\mathrm{smooth}}$ (resp. $\mathscr{X}_{\mathrm{sp.Car}}^{\mathrm{smooth}}$) to the Néron $\tilde{J}_{/\mathbb{Z}}$ (resp. $J_{/\mathbb{Z}}$) and u: $J_{/\mathbb{Z}} \longrightarrow \tilde{J}_{/\mathbb{Z}}$ the natural morphism as in §2. Then $\tilde{g}(y) = ug(x) = ug(w(x)) = 0$, see (3.4). Denote by $l(p)$ the number of the $\mathbb{Z}_p$-sections x of $\mathscr{X}_{\mathrm{sp.Car}}$ which satisfy the following conditions (C_1), (C_2):

(C_1) $x \otimes \mathbb{Q}_p$ are neither cusps nor C.M. points.

(C_2) $x \otimes \mathbb{F}_p$ are sections of $Z_1'^h$ (see §1(1.1)) and $ug(x) = 0$.

One of the sections x and $w(x)$ of the fibre $(\mathscr{X}_{\mathrm{sp.Car}})_y$ satisfies the condition (C_2). If a $\mathbb{Z}_p$-section x of $\mathscr{X}_{\mathrm{sp.Car}}$ satisfies the condition (C_2) and $x \otimes \mathbb{F}_p = 0 \otimes \mathbb{F}_p$, then x is the cusp 0, see (2.5). Denote by $n(p)$ the number of the $\mathbb{Z}$-sections of $\mathscr{X}_{\mathrm{split}}$ whose generic fibres are neither cusps nor C.M. points. Then $n(p) \leqslant l(p)$. Estimating $l(p)$, we get the following.

THEOREM (4.1): *$n(p) \leqslant \dim J - \dim \tilde{J}$ for $p \geqslant 17$.*

Example: $l(37) = 1$, see (5.A).
For a point $z \in Z'^h(\mathbb{F}_p)$, $z \neq 0 \otimes \mathbb{F}_p$,

$$m(z) = \underset{\omega \in \mathrm{Cot}\, \tilde{J}_{/\mathbb{Z}_p} \otimes \mathbb{F}_p}{\mathrm{Minimum}} \{\text{the order of zero of } \omega \text{ at } z\}.$$

Let $l(z) = l(p, z)$ be the number of the $\mathbb{Z}_p$-sections of $\mathscr{X}_{\mathrm{sp.Car}}$ which satisfy the conditions (C_1), (C_2) above and

$$(C_z)\ \pi(x) \otimes \mathbb{F}_p = z,$$

where π: $\mathscr{X}_{\mathrm{sp.Car}} \longrightarrow \mathscr{X} = \mathscr{X}_0(p)$ is the canonical morphism (see §1). We estimate $l(p)$ by the following way. Firstly, we show that there exist at most $m(z) + 1$ $\mathbb{Z}_p$-sections of $\mathscr{X}_{\mathrm{sp.Car}}$ which satisfy the conditions (C_2), (C_z) above. Secondly, we show that the Deuring lifting (see e.g., [8] Part 13§5) satisfies the conditions (C_2), (C_z) above. Then $l(z) \leqslant m(z)$ for $z \in Z'^h(\mathbb{F}_p)$, $z \neq 0 \otimes \mathbb{F}_p$. Finally, using the Riemann-Roch theorem, we estimate $\Sigma_z m(z)$.

LEMMA (4.2): *$\ell(z) \leqslant m(z)$.*

PROOF: Let x be a $\mathbb{Z}_p$-section of $\mathscr{X}_{\mathrm{sp.Car}}$ which satisfies the conditions (C_2), (C_z) for $z \in Z'^h(\mathbb{F}_p)$, $z \neq 0 \otimes \mathbb{F}_p$. The morphism $ug = uC_1 - uC_p$ (see

§2) is defined by

$$\mathscr{X}_{\text{sp.Car}} \otimes \mathbb{Z}_p^{\text{smooth}} \xrightarrow[\pi \times w_p \pi w]{} \mathscr{X} \otimes \mathbb{Z}_p^{\text{smooth}} \times \mathscr{X} \otimes \mathbb{Z}_p^{\text{smooth}}$$

$$\to \tilde{J}_{/\mathbb{Z}_p} \times \tilde{J}_{/\mathbb{Z}_p} \to \tilde{J}_{/\mathbb{Z}_p}$$

$$(\text{the cusp } 0) \mapsto 0, \ (x_1, x_2) \mapsto x_1 - x_2$$

Consider the morphism uC_1 of $\mathscr{X}_{\text{sp.Car}} \otimes \mathbb{Z}_p^{\text{smooth}}$ to $\tilde{J}_{/\mathbb{Z}_p}$:

$$\begin{array}{ccc} (uC_1)^*: \widehat{\mathcal{O}_{\tilde{J}_{/\mathbb{Z}_p}, uC_1(x)}} & \to & \widehat{\mathcal{O}_{\mathscr{X}_{\text{sp.Car}} \otimes \mathbb{Z}_p, x}} \\ \| & & \| \\ \mathbb{Z}_p[[t_1, \dots, t_{\tilde{g}}]] & & \mathbb{Z}_p[[q]] \end{array}$$

where $\tilde{g} = \dim \tilde{J}$. By Proposition (2.3) and by the fact that π is isomorphic formally along the section x (see §1), we see that for an integer i, $1 \leqslant i \leqslant \tilde{g}$,

$$(uC_1)^*(t_i) \equiv a_m q^m + a_{m+1} q^{m+1} + \dots (\text{mod } p)$$

with $m = m(z) + 1$ and $a_m \in \mathbb{Z}_p^\times$. Similarly, we see that $(uC_p)^*(t_i) \equiv a'_{pm} q^{pm} + a'_{pm+1} q^{pm+1} + \dots$ (mod p) with $a'_{pm} \in \mathbb{Z}_p^\times$, see (1.1), (2.5). By the condition (C_2), $uC_1(x) = uC_p(x)$. $\tilde{J}_{/\mathbb{Z}_p} \otimes \mathbb{F}_p$ is a split torus $\mathbb{G}_m \times \dots \times \mathbb{G}_m = \text{Spec } \mathbb{F}_p[u_1, u_1^{-1}, \dots, u_{\tilde{g}}, u_{\tilde{g}}^{-1}]$ (see [15], [10] Appendix). The section $uC_1(x) \otimes \mathbb{F}_p = uC_p(x) \otimes \mathbb{F}_p$ is defined by $(u_1, \dots, u_{\tilde{g}}) = (c_1, \dots, c_{\tilde{g}})$ for $c_i \in \mathbb{F}_p^\times$. Let v be the morphism: $\tilde{J}_{/\mathbb{Z}_p} \times \tilde{J}_{/\mathbb{Z}_p} \to \tilde{J}_{/\mathbb{Z}_p}$, $(x_1, x_2) \mapsto x_1 - x_2$. Then $v^*(u_j - 1) = c_j^{-1}(u_j \otimes 1 - c_j) + c_j(1 \otimes u_j^{-1} - c_j^{-1}) + (u_j \otimes 1 - c_j)(1 \otimes u_j^{-1} - c_j^{-1})$. For an integer k, $(ug)^*(u_k - 1) = c_k^{-1} b_m q^m + \dots$ with $b_m \in \mathbb{F}_p^\times$. Then $(ug)^*(t_i) \equiv b'_m q^m + \dots$ (mod p) with $b'_m \in \mathbb{Z}_p^\times$. In the following, we show that there exists a C.M. point satisfying the conditions (C_2), (C_z). Let $E(/\mathbb{F}_p)$ be an elliptic curve with the modular invariant $j(E) = j(z)$. Then the triple (E, ker(Ver), ker(Frob)) represents $x \otimes \mathbb{F}_p$, see §1(1.1). Let F be the Deuring lifting of E (see e.g., [8] Part 13 §5), which is defined over a subfield K of $\mathbb{Q}_p^{ur}$ (see loc. cit., Theorem 13). Let α, $\bar{\alpha}$ be the endomorphisms of F such that $\alpha \otimes \overline{\mathbb{F}}_p = \text{Ver}$ and $\bar{\alpha} \otimes \overline{\mathbb{F}}_p = \text{Frob}$ (see loc.cit., Theorem 12). Put $A = \ker(\alpha: F \to F)$ and $B = \ker(\bar{\alpha}: F \to F)$. Then the triple (F, A, B) represents a $\mathcal{O}_K$-section $\tilde{x}$ of $\mathscr{X}_{\text{sp.Car}}$ such that $\tilde{x} \otimes \overline{\mathbb{F}}_p = x \otimes \overline{\mathbb{F}}_p$. By the same way as in Proposition (3.3), we can see that $(F/B, F_p/B) \xrightarrow{\sim} (F, A)$. Then, $g(\tilde{x}) \equiv 0$. The rest of this lemma owes to the following sublemma.

SUBLEMMA (4.3): *Let $f(t) = \sum_{n \geqslant 1} a_n t^n$ be a formal power series with $a_n \in W(\overline{\mathbb{F}}_p)$. Suppose that $f(t) \equiv a_r t^r + \dots (\text{mod } p)$ with $a_r \not\equiv 0$ mod p. Then there are at most r solutions of $f(t) = 0$ in $pW(\overline{\mathbb{F}}_p)$. If $r = 2$ and $a_1 \neq 0$, there exist two solutions of $f(t) = 0$ in $pW(\overline{\mathbb{F}}_p)$.* □

Proof of Theorem (4.1): By Lemma (4.2), $l(p) \leqslant m(p) = \Sigma m(z)$. Put $g = g_0(p) = \dim J$, $\tilde{g} = \tilde{g}_0(p) = \dim \tilde{J}$ and let $g_+ = g_+(p)$ be the genus of $X_0^+(p) = X_0(p)/\langle w_p \rangle$. Let α_i $(1 \leqslant i \leqslant r = g - 2g_+ + 1)$ be the $\mathbb{F}_p$-rational supersingular points and β_i, $\beta_i^{(p)}$ $(1 \leqslant i \leqslant g_+)$ the non $\mathbb{F}_p$-rational supersingular points on $\mathscr{X} \otimes \mathbb{F}_p$. Put $D_1 = \Sigma_i(\alpha_i)$, $D_2 = \Sigma_i(\beta_i) + \Sigma_i(\beta_i^{(p)})$ and $D_0 = \Sigma_z m(z)(z)$. Then $\operatorname{Cot} \tilde{J}_{/\mathbf{Z}_p} \otimes \overline{\mathbb{F}}_p$ can be regarded as a $\tilde{g}$-dimensional subspace of $H^0(Z' \otimes \overline{\mathbb{F}}_p, \Omega^1(-D_0 + D_1 + D_2))$ (see [11] Corollary (1.1), [3] p. 162 (2.3)). For an effective divisor $D < D_1 + D_2$, put $V(D) = \operatorname{Cot} \tilde{J}_{/\mathbf{Z}_p} \otimes \overline{\mathbb{F}}_p \cap H^0(Z' \otimes \overline{\mathbb{F}}_p, \Omega^1(-D_0 + D))$ and let S be the set of the divisors $\{D < D_1 + D_2 | D > 0, V(D) \neq \{0\}\}$. Take a divisor $D_{(1)} \in S$ such that $\deg D_{(1)} \leqslant \deg D$ for all $D \in S$. Then $\deg D_{(1)} \geqslant m(p) + 2$. The fundamental involution w_p acts by (-1) on $\operatorname{Cot} J^-_{/\mathbf{Z}_p} \otimes \overline{\mathbb{F}}_p$ and $w_p(\beta_i) = \beta_i^{(p)}$ (see [15], [10] Appendix), so that if $\omega \in \operatorname{Cot} J^-_{/\mathbf{Z}_p} \otimes \mathbb{F}_p$ has a pole at β_i (resp. $\beta_i^{(p)}$), then ω has also a pole at $\beta_i^{(p)}$ (resp. β_i). Therefore, $\dim V(D + (\beta_i) + (\beta_i^{(p)})) \leqslant \dim V(D) + 1$ for $D < D_1 + D_2$. We can choose the divisors $D_{(1)} < D_{(2)} < \ldots < D_{(\tilde{g})}$ such that $D_{(i)} \in S$ and $\dim V(D_{(i)}) = i$ for the integers i, $1 \leqslant i \leqslant \tilde{g}$. Put $D_{(1)} = E + F$ with $E < D_1$ and $F < D_2$, and let s, $2t$ be the degrees of E and F, respectively. Then $\tilde{g} = \dim \tilde{J}_{/\mathbf{Z}_p} \otimes \overline{\mathbb{F}}_p \leqslant (g - 2g_+ + 1) - s + (g_+ - t) + 1$. Therefore, we get the following:

$$s + t \leqslant g - g_+ - \tilde{g} + 2$$

$$0 \leqslant s \leqslant g - 2g_+ + 1$$

$$0 \leqslant t \leqslant g_+$$

$$m(p) + 2 \leqslant s + 2t$$

$$l(p) \leqslant m(p).$$

In paticular, $l(p) \leqslant g - \tilde{g}$. □

§5. Further results

We here discuss the cases for $p = 13$ and 37.

(5.A) A result for p = 37

Let $f_+ = q - 2q^2 - 3q^3 + \ldots$ (resp. $f_- = q + q^3 + \ldots$) be the new form on $\Gamma_0(37)$ of weight 2 with the eigen value $+1$ (resp. -1) of w_{37}, see [1]. Put $\omega_+ = f_+ \mathrm{d}q/q$ and $\omega_- = f_- \mathrm{d}q/q$, which are basis of $H^0(\mathscr{X}, \Omega)$ ($\mathscr{X} \longrightarrow \operatorname{Spec} \mathbf{Z}$ is regular ($p = 37$), see [3] VI §6). On $Z \xrightarrow{\sim} \mathscr{X}_0(1) \otimes \mathbb{F}_{37} = \mathbb{P}^1(j) \otimes \mathbb{F}_{37}$,

$$\omega_+ = \frac{-\mathrm{d}j}{j^2 - 6j - 6} \qquad \omega_- = \frac{-(j-6)\mathrm{d}j}{(j^2 - 6j - 6)(j - 8)}$$

(see [3] p. 162 (2.3), [21] Table 6, pp. 142–144). There are at most two $\mathbb{Z}_{37}$-section of $\mathscr{X}_{\mathrm{sp.Car}} = \mathscr{X}_{\mathrm{sp.Car}}(37)$ which satisfy the condition (C_2) and (C_z) for the point $z \in Z'^h$ with the modular invariant $j(z) = 6$. One of them is the Deuring lifting of z whose ring of endomorphisms $\mathcal{O} = \mathbb{Z}[(-1 + 7\sqrt{-3})/2]$. The class number of the order $\mathcal{O}$ is two (e.g., [8] Part 8 Theorem 7). The modular curve $X_0(37)$ is defined by the equation:

$$Z^2 = -f^6 - 9f^4 - 11f^2 + 37,$$

where $f = f_+/f_-$ and $Z = 1 + q + \dots$ (, $q = \exp(2\pi\sqrt{-1}\,z)$, see [12] §5). The fundamental involution w_{37} acts by $w_{37}^*(Z, f) = (Z, -f)$ and the hyperelliptic involution S acts by $S^*(Z, f) = (-Z, f)$, see loc.cit.. Let $\tilde{z}$ be the Deuring lifting of $z \in Z'^h$ with the modular invariant $j(\tilde{z}) \equiv 6 \bmod 37$. Let K be the Hilbert class field associated with $\mathcal{O}$. The rational prime 37 splits in K. Fix an embedding of K into $\mathbb{Q}_{37}$. For $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, $ug(\tilde{z}^\tau) = (ug(\tilde{z}))^\tau = 0$ and $\tilde{z}^\tau \otimes \mathbb{F}_{37}$ is a section of $Z_1^h \cup Z_1'^h$, see (1.1), (1.4). Choose $\tau_i \in \mathrm{Gal}(K/\mathbb{Q})$ ($\tau_1 = \mathrm{id.}$, $i = 1, 2$) such that $\tilde{z}^{\tau_i} \otimes \mathbb{F}_{37}$ are the sections of Z_1'. Then $\tilde{z}_i = \tilde{z}^{\tau_i}$ satisfy the condition (C_2) in §4. By the uniqueness of the Deuring lifting (see [8] Part 13 Theorem (13)), the modular invariant $j(\tilde{z}_2) \not\equiv 6 \bmod 37$. Put $\omega = (ug)^*(\omega_-)$. Then $\omega(\tilde{z}_1 \otimes \mathbb{F}_{37}) = 0$ and $\omega(\tilde{z}_2 \otimes \mathbb{F}_{37}) \neq 0$. Therefore, $\omega(z_1) \neq 0$ (, because if $\omega(\tilde{z}_1) = 0$, then $\omega(\tilde{z}_2) = \omega(\tilde{z}_1)^{\tau_2} = 0$). There exists a $\mathbb{Z}_{37}$-section of $\mathscr{X}_{\mathrm{sp.Car}}(37)$ which satisfies the conditions (C_1), (C_2), see (4.2), (4.3). We here discuss it. Put $\tau = \exp(2\pi\sqrt{-1}/3)$, $\tau_1 = 1 - 10\tau$, $\tau_2 = 1 + 11\tau$, $L = \mathbb{Z} + \mathbb{Z}\tau$ and $E = \mathbb{C}/L$. Denote by δ_0, δ_∞ and δ_i $(1 \leqslant i \leqslant 36)$ the points on $X_0(37)$ which are represented by the pairs $(E, (\frac{1}{37}\mathbb{Z}\tau_1 + L)/L)$, $(E, (\frac{1}{37}\mathbb{Z}\tau_2 + L)/L)$ and $(E, (\frac{1}{37}\mathbb{Z}(\tau_1 + i\tau_2) + L)/L)$, respectively. Let H be the subgroup of $(\mathbb{Z}/37\mathbb{Z})^\times$ generated by 11 mod 37. Then $\delta_i = \delta_j$ if and only if $i \equiv j \bmod H$. Let $\varepsilon_\pm$ be the points defined by $(f^{-1}, f^{-3}Z) = (0, \pm\sqrt{-1})$. The field of rational functions on $X_0(37)$ is $\mathbb{Q}(j(z), j(37z))$. The divisors of the rational functions $j(z)$, $f - 1$ and $f + 1$ are $(j(z)) = (\delta_0) + (\delta_\infty) + 3\Sigma_{i \bmod H}(\delta_i) - (\infty) - 37(0)$, $(f - 1) = (\infty) + (\gamma_\infty) - (\varepsilon_+) - (\varepsilon_-)$ and $(f + 1) = (0) + (\gamma_0) - (\varepsilon_+) - (\varepsilon_-)$, where $\gamma_\infty = S(\infty)$ and $\gamma_0 = S(0)$. We can easily see that $\mathbb{Z}[1/2 \cdot 37, X, Y]/(X^2 + Y^6 + 9Y^4 + 11Y^2 - 37)$ is smooth. Then the modular function $j(z)$ is of the form

$$j(z) = \frac{p(f) + q(f)Z}{(f-1)(f+1)^{37}}$$

with some polynominals $p(Y)$, $q(Y) \in \mathbb{Q}[Y]$. The points defined by $(Z, f) = (\pm\sqrt{37}, 0)$ correspond to the elliptic curves $(/\mathbb{Q}(\sqrt{37}))$ with complex multiplication, so that $q(0) \neq 0$. The cusps ∞, 0 are defined respectively by $(Z, f) = (4, 1)$ and $= (4, -1)$, so that $p(1) + 4q(1) \neq 0$ and $p(-1) + 4q(-1) \neq 0$. The non cuspidal points γ_∞, γ_0 are defined respectively by $(Z, f) = (-4, 1)$ and $= (-4, -1)$, so that $p(1) - 4q(1) =$

$p(-1)-4q(-1)=0$. Therefore, $q(\pm 1)\neq 0$. The special fibre $\varepsilon_{\pm}\otimes\mathbb{F}_{37}$ of the fixed points $\varepsilon_{\pm}$ of Sw_{37} is the supersingular point $(/\mathbb{F}_{37})$. $X_0(37)(\mathbb{Q})=\{0, \infty, \gamma_0, \gamma_\infty\}$, see [12] §5. For the rational points on $X_{split}(37)$, we get the following.

PROPOSITION (5.1): *If $n(37)=1$, then there exists a $\mathbb{Q}$-rational solution of the equation $q(Y)=0$. Conversely, if $q(Y)=0$ has a $\mathbb{Q}$-rational solution, then $n(37)=1$.*

PROOF: Firstly, suppose that there exists a $\mathbb{Q}$-rational point y on X_{split} (37) which is neither a cusp nor a C.M.point. Let x, $w(x)$ be the sections of the fibre $(X_{sp.Car})_y$, which are defined over a quadratic field k and $w(x)=x^\sigma$ for $1\neq\sigma\in \mathrm{Gal}(k/\mathbb{Q})$, see (3.2). As was seen in the proof of Theorem (3.9), there exists a rational function $g(/\mathbb{Q})$ on $X_0(37)$ of degree 2 whose divisor $(g)=(\pi(x))+(\pi w(x))-(w_{37}\pi(x))-(w_{37}\pi w(x))$. Then $S\pi(x)=\pi w(x)(=\pi(x)^\sigma)$, so that $a=f(\pi(x))\in\mathbb{Q}$ (and $a\neq\pm 1$). Let $b(\in k)$ be the square root of $-a^6-9a^4-11a^2+37$. We may assume that the points $\pi(x)$, $\pi w(x)$ are defined by $(Z,f)=(b,a)$ and $=(-b,a)$, respectively. The modular invariant $j(\pi(x))=j(\pi w(x))$ of $\pi(x)$ and $\pi w(x)=S\pi(x)$ is written by $\{p(a)+q(a)b\}/(a-1)(a+1)^{37}=\{p(a)-q(a)b\}/(a-1)(a+1)^{37}$. Hence, $q(a)=0$. Conversely, suppose that the equation $q(Y)=0$ has a solution $Y=a\in\mathbb{Q}$. Let z, $S(z)$ be the points on $X_0(37)$ which are defined by $(Z,f)=(b,a)$ and $=(-b,a)$ for a square root b of $-a^6-9a^4-11a^2+37$. As $a\neq\pm 1$, so that $\mathbb{Q}(b)$ is a quadratic field and $z\neq S(z)$, $S(z)=z^\sigma$ for $1\neq\sigma\in \mathrm{Gal}(\mathbb{Q}(b)/\mathbb{Q})$. The modular invariant $j(z)=j(z^\sigma)\in\mathbb{Q}$. If z is a C.M. point, then z is represented by an elliptic curve E $(/\mathbb{Q})$ with $\mathbb{Q}(b)$-rational subgroup A of rank 37. Then z^σ is represented by the pair (E, A^σ), and $(E, A^\sigma)\xrightarrow{\sim}(E/A, E_{37}/A)$, i.e., $z^\sigma=w_{37}(z)$. As noted before, $a\neq 0$, so that z is not a C.M. point. Let F be an elliptic curve defined over $\mathbb{Q}$ with the modular invariant $j(F)=j(z)$, and ρ the representation of the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the 37-torsion points $F_{37}(\overline{\mathbb{Q}})$. There is a quadratic extension K of $\mathbb{Q}(b)$ such that $\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is contained in a Borel subgroup $(\subset GL_2(\mathbb{F}_{37}))$. Then $\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is contained in a Borel subgroup or in the normalizer of a split Cartan subgroup, see [19] §2, [9] §2 p. 120. The first case does not occur, because z is not $\mathbb{Q}$-rational. □

(5.B) Some results for p = 13

Because of the fact that $X_0(13)\xrightarrow{\sim}\mathbb{P}^1$, we can not apply the same method as for the other primes $p\geqslant 11$. We here discuss the case $p=13$ under additional conditions. Let y be a non cuspidal $\mathbb{Q}$-rational point on $X_{split}(13)$, which is represented by a pair $(E, \{A, B\})$ for an elliptic curve defined over $\mathbb{Q}$. Then the triple (E, A, B) represents a point on $X_{sp.Car}(13)$, which is defined over a quadratic field k, see (3.2). Consider the representation ρ_2 of the Galois action of $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the 2-torsion points $E_2(\overline{\mathbb{Q}})$. If y is a C.M.point, then $\rho_2(G_k) \not\twoheadrightarrow GL_2(\mathbb{F}_2)$, where $G_k = \mathrm{Gal}(\overline{\mathbb{Q}}/k)$. We set the following condition (C):

$$(C) \quad \rho_2(G_k) \not\twoheadrightarrow GL_2(\mathbb{F}_2).$$

Under the condition (C) above, there occur the following three cases:

$$(C\text{-}1) \quad \rho_2(G) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}.$$

$$(C\text{-}2) \quad \rho_2(G) \subsetneq \mathbb{Z}/3\mathbb{Z}.$$

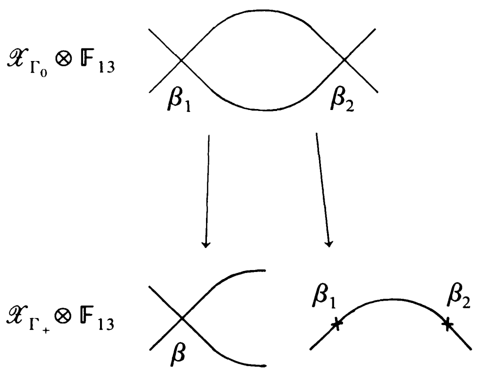
$$(C\text{-}3) \quad \rho_2(G) \xrightarrow{\sim} GL_2(\mathbb{F}_2) \quad \text{and} \quad \rho_2(G_k) \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z}.$$

Denote by $\mathscr{X}_\Gamma$ the modular curve $(/\mathbb{Z})$ corresponding to the finite adèlic modular group $\Gamma \subset GL_2(\hat{\mathbb{Z}})$ (see §1(1.1)), and put $X_\Gamma = \mathscr{X}_\Gamma \otimes \mathbb{Q}$. In the case $(C\text{-}1)$, let Γ_0, Γ_1 and Γ respectively the modular groups $\Gamma_0 = \Gamma_0(26)$, $\Gamma_1 = \Gamma_0(2) \cap \Gamma_{\mathrm{sp.Car}}(13)$ and $\Gamma = \Gamma_0(2) \cap \Gamma_{\mathrm{split}}(13)$. In the case $(C\text{-}2)$ (resp. $(C\text{-}3)$), let Γ_0, Γ_1 and Γ respectively the modular groups $\Gamma_0 = \Gamma_{\mathrm{non.sp.Car}}(2) \cap \Gamma_0(13)$, $\Gamma_1 = \Gamma_{\mathrm{non.sp.Car}}(2) \cap \Gamma_{\mathrm{sp.Car}}(13)$ and $\Gamma = \Gamma_{\mathrm{non.sp.Car}}(2) \cap \Gamma_{\mathrm{split}}(13)$ $\left(\textit{resp}.\ \Gamma = \left\langle \Gamma_1, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle\right)$, where $\Gamma_{\mathrm{non.sp.Car}}(2) = \{ g \in GL_2(\hat{\mathbb{Z}}) | g^3 \equiv 1 \bmod 2\}$. Under the condition $(C\text{-}i)$, (y, E) represents a non cuspidal $\mathbb{Q}$-rational point on X_Γ. In the rest of this section, we prove the following.

Theorem (5.2): *Let X_Γ be as above. Then $X_\Gamma(\mathbb{Q})$ consists of the cusps and the C.M. points.*

Define the involutions w of X_{Γ_1} by: Case $(C\text{-}1)$: $(E, A, B, C) \longmapsto (E, B, A, C)$, Case $(C\text{-}2)$: $(E, A, B, \alpha \bmod \mathbb{F}_4^\times) \longmapsto (E, B, A, \alpha \bmod \mathbb{F}_4^\times)$, Case $(C\text{-}3)$: $(E, A, B, \alpha \bmod \mathbb{F}_4^\times) \longmapsto (E, B, A, \alpha' \bmod \mathbb{F}_4^\times)$, where A, B are subgroups of rank 13, $C \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$ and α, α' are the 2-level structures such that $\alpha \not\equiv \alpha' \bmod \mathbb{F}_4^\times(, \mathbb{F}_4^\times \subsetneq GL_2(\mathbb{F}_2))$. Then $X_\Gamma = X_{\Gamma_1}/\langle w \rangle$. Define the involution w_0 of X_{Γ_0} by: Case $(C\text{-}1)$: $(E, A, C) \longmapsto (E/A, E_{13}/A, (C+A)/A)$, Case $(C\text{-}2)$: $(E, A, \alpha \bmod \mathbb{F}_4^\times) \longmapsto (E, A, \alpha' \bmod \mathbb{F}_4^\times)$, Case $(C\text{-}3)$: $(E, A, \alpha \bmod \mathbb{F}_4^\times) \longmapsto (E/A, E_{13}/A, \alpha' \bmod \mathbb{F}_4^\times)$, where α, α' are the 2-level structures such that $\alpha \not\equiv \alpha' \bmod \mathbb{F}_4^\times$. Let J be the jacobian variety of X_{Γ_0}, π the canonical morphism of $\mathscr{X}_{\Gamma_1}$ to $\mathscr{X}_{\Gamma_0}$ and put $J^- = J/(1 + w_0)J$. In the case $(C\text{-}1)$, X_{Γ_0} is of genus 2 and $J^-(\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z}$ (see [21] Table 1, pp. 81–113). In the cases $(C\text{-}2)$ and $(C\text{-}3)$, X_{Γ_0} is of genus 1. The modular curve $X_{\Gamma(2) \cap \Gamma_0(13)}$ is isomorphic over $\mathbb{Q}$ to $X_0(4 \cdot 13)$ (see [3] IV Proposition (3.16): $\Gamma_0(4 \cdot 13) = g\{\Gamma(2) \cap \Gamma_0(13)\} g^{-1}$ for $g = \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix} h$

with $h \in GL_2(\hat{\mathbb{Z}})$ such that $h \equiv 1 \bmod 4$ and $h \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \bmod 13$). In the cases $(C\text{-}2)$ and $(C\text{-}3)$, the double covering $X_{\Gamma_0} \to X_0(13)$ ramifies at the cusps 0 and ∞. The class $cl((0)-(\infty))$ is of order 2 and $J(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ (see [21] Table 1). Let ω be the base of $H^0(X_{\Gamma_0}, \Omega^1)$ (in the cases $(C\text{-}2)$, $(C\text{-}3)$), then $w_0^*\omega = -\omega$ (see [21] Table 3 pp. 116–122), so that $J^- = J$.



Case(C-2) Case(C-3)

where $\mathscr{X}_{\Gamma_+} = \mathscr{X}_{\Gamma_0}/\langle w_0 \rangle$. Define the morphism g of X_{Γ_1} to J by $\longmapsto cl((\pi(x)) - (w_0 \pi w(x)))$. Then g induces the morphism g^- of X_Γ to J^-:

$$\begin{array}{ccc} X_{\Gamma_1} & \xrightarrow{\text{can.}} & X_\Gamma \\ g \downarrow & \circlearrowleft & \downarrow g^- \\ J & \xrightarrow{\text{can.}} & J^- . \end{array}$$

Denote also by g (resp. g^-) the morphism of $\mathscr{X}_{\Gamma_1}^{\mathrm{smooth}}$ (resp. $\mathscr{X}_{\Gamma}^{\mathrm{smooth}}$) to the Néron model $J_{/\mathbb{Z}}$ (resp. $J^-_{/\mathbb{Z}}$). The modular curve $X_0(13) \xrightarrow{j} X_0(1)$ is defined by the following equation (Fricke, see [13]):

$$j(X) = (X^2 + 5X + 13)(X^4 + 7X^3 + 20X^2 + 19X + 1)^3/X. \quad (5.3)$$

The modular curve $X_{\mathrm{sp.Car}}(13)$ is the normalization of the curve defined by the equation:

$$0 = \frac{j(X) - j(Y)}{X - Y}. \quad (5.4)$$

Let y be a non cuspidal $\mathbb{Q}$-rational point on $X_{\mathrm{split}}(13)$ and x, $w(x)$ the sections of the fibre $(X_{\mathrm{sp.Car}}(13))_y$, which are defined over a quadratic field k. Then $w(x) = x^\sigma$ for $1 \neq \sigma \in \mathrm{Gal}(k/\mathbb{Q})$ (see (3.2)) and x, $w(x)$

correspond to the points defined by $(X, Y) = (a, a^\sigma)$ and (a^σ, a) for $a \in k$, respectively.

LEMMA (5.5): *Under the notation as above. Suppose that y has potentially good reduction at a prime $\mathfrak{q}$ of k. Then* $(ord_{\mathfrak{q}} a, ord_{\mathfrak{q}} a^\sigma) = (0, 0)$ *if* $\mathfrak{q} \nmid 13$, $=$ $(0, 0)$, $(1, 0)$ *or* $(0, 1)$ *if* $\mathfrak{q} | 13$.

PROOF: By the assumption, $\mathrm{ord}_{\mathfrak{q}}\, j(y) \geqslant 0$. If $\mathfrak{q} \nmid 13$, by the equation (5.3) above, we can easily see that $\mathrm{ord}_{\mathfrak{q}} a = \mathrm{ord}_{\mathfrak{q}} a^\sigma = 0$. The rational prime 13 splits in k, see (3.2). If $\mathfrak{q} | 13$, $\mathrm{ord}_{\mathfrak{q}} a$, $\mathrm{ord}_{\mathfrak{q}} a^\sigma = 0$ or 1. By the equation (5.4) above, $(\mathrm{ord}_{\mathfrak{q}} a, \mathrm{ord}_{\mathfrak{q}} a^\sigma) \neq (1, 1)$. □

For a rational prime q, let I_q be the inertia subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q^{ur})$. There exists an elliptic curve E defined over $\mathbb{Q}$ with independent subgroups A, B of rank 13 such that the set $\{A, B\}$ is $\mathbb{Q}$-rational and the pair $(E, \{A, B\})$ represents y. Let ρ_4 be the representation of the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the 4-torsion points $E_4(\overline{\mathbb{Q}})$.

LEMMA (5.6): *Under the notation as above. If a rational prime q ramifies in k, then the modular invariant* $j(y) \equiv 1728 \bmod q$. *If moreover* $q \neq 2$, $\rho_4(I_q)$ *contains a subgroup isomorphic to* $\mathbb{Z}/4\mathbb{Z}$.

PROOF: If q ramifies in k, then $q \neq 13$ (see (3.2)) and $y \otimes \mathbb{F}_q$ is a ramification point of the double covering $\mathscr{X}_{\mathrm{sp.Car}}(13) \otimes \mathbb{F}_q \longrightarrow \mathscr{X}_{\mathrm{split}}(13) \otimes \mathbb{F}_q$. Then $j(y) \equiv 1728$ mod q. Let ρ be the representation of the Galois action on the 13-torsion points $E_{13}(\overline{\mathbb{Q}})$. Then for a rational prime $q \neq 2$, 13, $\rho_4(I_q) \xrightarrow{\sim} \rho(I_q) (\subsetneq SL_2(\mathbb{F}_{13}))$ (see [19] §5). Let $q \neq 2$ be a rational prime which ramifies in k and $\mathfrak{q}$ the prime of k lying over q with the inertial subgroup $I_{\mathfrak{q}} = \mathrm{Gal}(\bar{k}_{\mathfrak{q}}/k_{\mathfrak{q}}^{ur})$. For $\tau \in I_q \backslash I_{\mathfrak{q}}$, $\rho(\tau)$ is not contained in the split Cartan subgroup $\mathrm{Aut}\, A(\overline{\mathbb{Q}}) \times \mathrm{Aut}\, B(\overline{\mathbb{Q}})$ and $\det \rho(\tau) = 1$. Then the order of $\rho_4(\tau)$($=$ the order of $\rho(\tau)$) $= 4$. □

PROOF OF THEOREM (5.2): Let y be a non cuspidal $\mathbb{Q}$-rational point on X_Γ and x, $w(x)$ the sections of the fibre $(X_{\Gamma_1})_y$, which are defined over a quadratic field k. By the same way as in Proposition (2.5), (3.1), we see that y has potentially good reduction at the rational prime $q = 13$.

Case (C-1): Changing x by $w(x)$, if necessary, we may assume that $x \otimes \mathbb{F}_{13}$ is represented by $(F$, ker(Frob), ker(Ver), $C)$, where F is an elliptic curve defined over $\mathbb{F}_{13}$ and C is a subgroup of order 2 such that $\mathrm{Frob}(C) = C$, see (1.1), (1.4), (3.2). Let $(\tilde{F}, \tilde{A}, \tilde{B})$ be the Deuring lifting of $(F$, ker(Frob), Ker(Ver)$)$ and α the endomorphism of $\tilde{F}$ corresponding to Frob by the reduction map, see (4.2). Let $\tilde{C}$ be the subgroup of $\tilde{F}$ of rank 2 whose reduction (mod 13) $= C$. Then the reductions of $\tilde{C}$ and $\alpha(\tilde{C})$ (mod 13) are $C = \mathrm{Frob}(C)$. Then $\alpha(\tilde{C}) = \tilde{C}$. Let $\tilde{x}$ be the point on

X_{Γ_1} which is represented by $(\tilde{F}, \tilde{A}, \tilde{B}, \tilde{C})$. By the same way as in Lemma (4.2), we see that $\pi(\tilde{x}) = w_0 \pi w(\tilde{x})$, hence $g(\tilde{x}) = 0$. Because $J^-(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, $g^-(y) = 0$, see (3.4). The form $0 \neq \omega \in \operatorname{Cot} J^-_{/\mathbb{Z}} \otimes \mathbb{F}_{13}$ has one simple zero on each irreducible component of $x_0(26) \otimes \mathbb{F}_{13}$ (see [11] Corollary (1.1), [3] p. 162 (2.3)). Therefore, there exists at most one $\mathbb{Q}$-rational point on X_Γ which is neither a cusp nor a C.M. point, see the proof of Theorem (4.1). Let w_2 be the involution of X_Γ defined by $(E, \{A, B\}, C) \longmapsto (E/C, \{(A + C)/C, (B + C)/C\}, E_2/C)$. If y is not a C.M.point, then $w_2(y) \neq y$. Therefore, y is a C.M. point.

Case (C-3): There exists an elliptic curve F defined over $\mathbb{F}_{13}$ such that (F, ker(Frob), ker(Ver), α mod $\mathbb{F}_4^\times$) represents $x \otimes \mathbb{F}_{13}$, where α is a 2-level structure and $\mathbb{F}_4^\times \subsetneq GL_2(\mathbb{F}_2)$. The rational prime 13 splits in k (see (3.2)) and $\rho_2(G_k) \subset \mathbb{F}_4^\times$. Then $(F, A, \alpha \bmod \mathbb{F}_4^\times) \simeq (F/B, F_{13}/B, \alpha \bmod \mathbb{F}_4^\times)$, i.e., $\pi(x) \otimes \mathbb{F}_{13} = w_0 \pi w(x) \otimes \mathbb{F}_{13}$, see (3.3). Because $J = J^-$ has the Mordell-Weil group $\simeq \mathbb{Z}/2\mathbb{Z}$, $g^-(y) = 0$. Then y is a C.M. point, see the proof of Theorem (3.9).

Case (C-2): There corresponds to y an elliptic curve E defined over $\mathbb{Q}$ which satisfies the condition (C-2). The double covering $X_{\Gamma_0} \to X_0(13)$ ramifies at the cusps and $J = J^-$ has the Mordell-Weil group $\simeq \mathbb{Z}/2\mathbb{Z}$. Let 0, ∞ and z_i be the cusps on X_{Γ_1} lying over respectively 0, ∞ and x_i on $X_{\text{sp.Car}}(13)$, see (2.5). Let J_s^0 be the connected component of $J_{/\mathbb{Z}_{13}} \otimes \mathbb{F}_{13}$ of the unity. We see that $\pi(x) \otimes \mathbb{F}_{13} \neq w_0 \pi w(x) \otimes \mathbb{F}_{13}$ and $g(x) \bmod J_s^0 = cl((0) - (\infty)) \bmod J_s^0$ $(\neq J_s^0)$. For a rational prime $q \nmid 26$, if $x \otimes \overline{\mathbb{F}}_q = z_i \otimes \overline{\mathbb{F}}_q$, then $g(x) = g(z_i) = 0$. Let $\omega \in H^0(\tilde{\mathscr{X}}_{\Gamma_0} \otimes \mathbb{Z}[1/2], \Omega) \simeq \operatorname{Cot} J_{/\mathbb{Z}[1/2]}$ (see [11] Corollary (1.1), (2.3)), where $\mathscr{X}_{\Gamma_0} \to \operatorname{Spec} \mathbb{Z}$ is the minimal model. Then $\omega(0) = -\omega(\infty)$ is a unit of $\mathbb{Z}[1/2]$. For a rational prime $q \neq 2$, $g^*\omega(0) \neq 0 \bmod q$, $g^*\omega(\infty) \not\equiv 0 \bmod q$ (cf. the proof of (2.5)). Therefore, y has potentially good reduction at the primes $q \neq 2$, see (2.5), (3.1). By Lemma (5.6), only the prime $q = 2$ ramifies in k and E has potentially good reduction at $q = 2$. Hence, E has everywhere potentially good reduction. Then $k = \mathbb{Q}(\sqrt{-1})$, because the prime 13 splits in k. Then y corresponds to a point defined by $(X, Y) = (a, a^\sigma)$ for $a \in \mathbb{Z}[\sqrt{-1}]$, see (5.5). As y is a $\mathbb{Q}$-rational point, so the modular invariant $j(y) = j(a) \in \mathbb{Q}$. Using Lemma (5.5), (5.3), we see that y is a C.M. point corresponding to one of the points defined by $a = -3 \pm 2\sqrt{-1}$ and $-2 \pm 3\sqrt{-1}$. $\square$

References

[1] A.O.L. Atkin and J. Lehner: Hecke operators on $\Gamma_0(m)$. *Math. Ann. 185* (1970) 134–160.

[2] B.G. Berkovic: Rational points on the jacobians of modular curves. *Math. USSR Sbornik 30* (4) (1976) 478–500.

[3] P. Deligne and M. Rapoport: 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. 349.* Berlin-Heidelberg-New York: Springer 1973.

[4] M.W. KENKU: The modular curve $X_0(39)$ and rational isogeny. *Math. Proc. Cambridge Philos. Soc. 85* (1979) 21–23.
[5] M.A. KENKU: The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny. *Math. Proc. Cambridge Philos. Soc. 87* (1980) 15–20.
[6] M.A. KENKU: The modular curve $X_0(169)$ and rational isogeny. *J. London Math. Soc. (2) 22* (1980) 239–244.
[7] M.A. KENKU: On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. *J. London Math. Soc. (2) 23* (1981) 415–427.
[8] S. LANG: *Elliptic functions.* Reading, Mass.: Addison-Wesley.
[9] B. MAZUR: Rational points on modular curves. Proceedings of a conference on modular functions held in Bonn 1976. *Lecture Notes in Math. 601*. Berlin-Heidelberg-New York: Springer 1977.
[10] B. MAZUR: Modular curves and the Eisenstein ideal. *Publ. Math. I.H.E.S. 47* (1977).
[11] B. MAZUR: Rational isogenies of prime degree. *Inv. Math. 44* (1978) 129–162.
[12] B. MAZUR and H.P.F. SWINNERTON-DYER: Arithmetic of Weil curves. *Inv. Math. 25* (1974) 1–61.
[13] J.F. MESTRE: Points rationnels de la courbe modulaire $X_0(169)$. *Ann. Inst. Fourier, Grenoble* 30-2 (1980) 17–27.
[14] A. OGG: Über die Automorphismengruppe von $X_0(N)$. *Math. Ann. 228* (1977) 279–292.
[15] M. OHTA: On reduction and zeta functions of varieties obtained from $\Gamma_0(N)$ (to appear).
[16] F. OORT and J. TATE: Group schemes of prime order. *Ann. Scient. Éc. Norm. Sup. Série 4, 3* (1970) 1–21.
[17] M. RAYNAUD: Schémas en groupes de type $(p,\dots,p)$. *Bull. Soc. Math. France 102* (1974) 241–280.
[18] K. RIBET: Endomorphisms of semi-stable abelian varieties over number fields. *Ann. Math. 101* (1975) 555–562.
[19] J.S. SERRE: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inv. Math. 15 (1970) 259–331.
[20] J. Tate: p-divisible groups. *Proceedings of a conference on local fields, Driebergen, 1966.* Berlin: Springer-Verlag (1967), pp. 158–183.
[21] B.J. BIRCH and W. KUYK (eds.): Modular functions of one variable IV. *Lecture Notes in Math. 476.*

(Oblatum 6-I-1982 & 22-II-1983)

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo 113
Japan

Appendix

Here, we give an another proof of the theorems of Kenku in [4,5].

THEOREM (Kenku, loc. cit.): *The* $\mathbf{Q}$*-rational points on* X_0 *(p.* 13) *are the cusps, for* $p = 3$, 5 *and* 7.

PROOF: We use the following results.

(A.1) (Berkovic [2]). There exists a factor $(/\mathbf{Q})$ of the jacobian variety of $X_0(N)$ whose Mordell-Weil group is of finite order, for $N = 39$, 65 and 91.

(A.2) (see [11] §4). If x is a non cuspidal $\mathbf{Q}$-rational point on $X_0(N)$ for the integer as above, then x has potentially good reduction at the primes $q \neq 2$.

Let x be a non cuspidal $\mathbf{Q}$ − rational point on $X_0(\mathrm{p}\cdot 13)$ for $p = 3$, 5 or 7. Then x is represented by an elliptic curve E defined over $\mathbf{Q}$ with subgroup A of rank 13 and C of rank p which are defined over $\mathbf{Q}$ (see [3] VI Proposition (3.2)). Let λ (resp. ρ_p) be the representation of the Galois action of $G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $A(\overline{\mathbf{Q}})$ (resp. on the p-torsion points $E_p(\overline{\mathbf{Q}})$). For a rational prime q, let I_q be the inertia subgroup $\mathrm{Gal}(\overline{\mathbf{Q}}_q/\mathbf{Q}_q^{ur})$ and λ_q the restriction of λ to I_q. If $q \nmid 6\cdot p\cdot 13$, $\rho_p(I_q) \xrightarrow{\sim} \lambda(I_q)$ is isomorphic to a subgroup of $\mathbf{Z}/4\mathbf{Z}$ or $\mathbf{Z}/6\mathbf{Z}$ (see [19] §5). If $q = 3$ and $p \neq 3$, $\rho_p(I_3) \xrightarrow{\sim} \lambda(I_3)$ is isomorphic to a subgroup of $SL_2(\mathbf{Z}/4\mathbf{Z})$ (see loc.cit.), so that $\lambda(I_3)$ is isomorphic to a subgroup of $\mathbf{Z}/4\mathbf{Z}$ or $\mathbf{Z}/6\mathbf{Z}$. If x has potentially multiplicative reduction at $q = 2$, then $\lambda_2^2 = 1$. If x has potentially good reduction at $q = 2$, then $\rho_p(I_2) \xrightarrow{\sim} \lambda(I_2)$ is isomorphic to a subgroup of $SL_2(\mathbf{F}_3)$ (see loc.cit.), so that $\lambda(I_2)$ is isomorphic to a subgroup of $\mathbf{Z}/4\mathbf{Z}$ or $\mathbf{Z}/6\mathbf{Z}$. By our assumption, $\rho_p(G)$ is contained in a Borel subgroup of $GL_2(\mathbf{F}_p)$, so that for any rational prime $q \neq p$, $\rho_p(I_q)$ is isomorphic to a subgroup of $\mathbf{Z}/6\mathbf{Z}$ if $p = 3$ or 7, and to one of $\mathbf{Z}/4\mathbf{Z}$ if $p = 5$. Further, as λ is a character of G, so $\lambda_p^6 = 1$ if $p = 3$ or 7, and $\lambda_p^4 = 1$ if $p = 5$. Therefore, $\lambda_q^6 = 1$ if $p = 3$ or 7, and $\lambda_q^4 = 1$ if $p = 5$ for the rational primes $q \neq 13$. Put $e = 6$ if $p = 3$ or 7, and $e = 4$ if $p = 5$. Then the order of $\lambda_p(I_{13})$ divides e, so that E has good reduction over the extension of $\mathbf{Q}_{13}^{ur}$ of degree e, (A.2), loc.cit. Let θ_{13} be the cyclotomic character induced by the Galois action of G on $\mu_{13}(\overline{\mathbf{Q}})$. Put $\chi_{13} = \theta_{13}^r$ for an integer r. Then by the fundamental property of the finite flat group schemes (see (1.2)), $\chi_{13}^e = \theta_{13}^a$ for an integer a, $0 \leqslant a \leqslant e$. Therefore, $re \equiv a \bmod 12$, so $a = 0$ or e (see [11] §5). Changing E by E/A, if necessary, we may assume that $\lambda_{13}^e = 1$. Then $\lambda^6 = 1$ if $p = 3$ or 7, and $\chi^4 = 1$ if $p = 5$. Denote also by λ the corresponding character of the idèle group $\mathbf{Q}_A^\times$ of $\mathbf{Q}$. For a rational prime $q \nmid 26$, put $\nu_q = \lambda\ \mathrm{proj}(\mathbf{Q}_A^\times \xrightarrow{\sim} \mathbf{Z}_q^\times \times \mathbf{Z} \longrightarrow \mathbf{Z}_q^\times)$. Let k_q be the subfield of $\overline{\mathbf{Q}}_q$ corresponding to the character ν_q. Then k_q is a totally ramified extension of $\mathbf{Q}_q$. Let $\mathcal{O}_q$ be the ring of integers of k_q. Then $E_{/\mathcal{O}_q}$ is an elliptic curve (see (A.2)). Therefore, for each rational prime $q \nmid 26$, we have the relation: $\lambda(\sigma_q) + q\lambda(\sigma_q)^{-1} \equiv \mathrm{Tr}(\sigma_q) \bmod 13$, where σ_q is the Frobenius element of the prime of k_q and $\mathrm{Tr}(\sigma_q)$ is the trace of σ_q on the Tate module $T_{13}(E_{/\mathcal{O}_q})(\overline{\mathbf{F}}_q)$ (see [11] §6). Then we should have the following congreuences

$$1 + q^6 \equiv \mathrm{Tr}\left(\sigma_q^6\right) \bmod 13 \text{ if } p = 3 \text{ or } 7,$$

$$1 + q^4 \equiv \mathrm{Tr}\left(\sigma_q^4\right) \bmod 13 \text{ if } p = 5,$$

for any rational prime $q \nmid 26$. But, the congruences above are not satisfied for $q = 3$ if $p = 3$ or 7, and for $q = 5$ if $p = 5$. □