F. Momose
Nagoya Math. J.
Vol. 96 (1984), 139-165

p-TORSION POINTS ON ELLIPTIC CURVES DEFINED OVER QUADRATIC FIELDS

FUMIYUKI MOMOSE*

Let p be a prime number and k an algebraic number field of finite degree d. Manin [14] showed that there exists an integer $n = n(k,p)$ $(\geqq 0)$ which satisfies the condition

$$E(k)_{p^\infty} \subseteq \ker(p^n : E \longrightarrow E)$$

for all elliptic curves E defined over k. Here, $E_{p^\infty} = \bigcup_{m \geqq 1} E_{p^m}$ and $E_{p^m} = \ker(p^m : E \to E)$. We denote by $n = n(k,p)$ the least non-negative integer satisfying the above condition. For $k = \boldsymbol{Q}$, we know that $n(\boldsymbol{Q}, 2) = 3$, $n(\boldsymbol{Q}, 3) = 2$, $n(\boldsymbol{Q}, 5) = n(\boldsymbol{Q}, 7) = 1$ and $n(\boldsymbol{Q}, p) = 0$ for $p \geqq 11$ (cf. [10], [16, 17], [20], [22]). For quadratic fields k, Kenku [6, 8, 9] showed that $n(k,2) \leqq 4$, $n(k,3) = 2$, $n(k,5) = n(k,7) = 1$, $n(k,17) = n(k,19) = n(k,23) = 0$ and $n(k,p) = 0$ for the primes p; $p \geqq 181$, $p \neq 191$ and $\sharp J_0^-(p)(\boldsymbol{Q}) < \infty$. Here $J_0(p)$ is the jacobian variety of the modular curve $X_0(p)$, w_p is the automorphism of $J_0(p)$ induced by the fundamental involution $w_p : (E, A) \mapsto (E/A, E_p/A)$ of $X_0(p)$ and $J_0^-(p) = J_0(p)/(1 + w_p)J_0(p)$ (see [17]). Our result for quadratic fields k is the following.

THEOREM A. *Let k be any quadratic field and $n = n(k,p)$ as above. Then*

$$n(k, 11) \leqq 1$$
$$n(k, 13) \leqq 1$$

and $n(k,p) = 0$ for the primes $p \geqq 17$ satisfying the condition $\sharp J_0^-(p)(\boldsymbol{Q}) < \infty$.

For $p = 2, 11$ and 13, $n(k,p)$ depends on k (see (3.3)). For the primes p, $17 \leqq p < 300$, except for $p = 151$, 199, 227 and 277, the condition $\sharp J_0^-(p)(\boldsymbol{Q}) < \infty$ is satisfied ([17] p. 40, [35] Table 5 pp. 135–141). We conjecture $n(k,p) = 0$ for $p \geqq 17$. Our method used for quadratic fields can

Received December 1, 1983.
* Supported in part by Japan-U.S. exchange fund.

be applied to some other number fields. For example we get the following.

THEOREM B. *Let k be any cubic field and $n = n(k, p)$ as above. Then*

$$n(k, 2) \leqq 5$$
$$n(k, 3) = 2$$
$$n(k, 17) \leqq 1$$

and $n(k, p) = 0$ for $p = 19, 23, 41, 47, 59, 71$ and the primes p; $p \geqq 79$, $p \neq 79$, $p \neq 109$ and $\# J_0^-(p)(\boldsymbol{Q}) < \infty$.

We here give a sketch of the proof of Theorem A above for the case $p \geqq 23$, $p \neq 37$. Suppose that there exists a non cuspidal k-rational point x on $X_1(p)$. Under the condition as in Theorem A, one gets a rational function g on $X_0(p)$ defined over $\boldsymbol{Q}$ such that

$$(g) = (x) + (x^\sigma) + 2(\infty) - (w_p(x)) - (w_p(x^\sigma)) - 2(0),$$

where $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$ and 0, ∞ are the cusps on $X_0(p)$, Section 2. For $p \geqq 181$ ($p \neq 191$), Kenku [9] proved that such function g does not exist, using an Ogg's idea [22, 24]: The upper semicontinuity gives a non constant rational function $h(/\boldsymbol{F}_2)$ on $\mathscr{X}_0(p) \otimes \boldsymbol{F}_2$ with $(h)_\infty <$ an effective divisor of degree 4, which leads the inequality $\# \mathscr{X}_0(p)(\boldsymbol{F}_p) \leqq 10$. For the remaining p, we use the following two methods: (1) The condition $(w_p^* g) = -(g)$ $(\neq 0)$ shows that $w_p^*(g) = a/g$ for $a \in \boldsymbol{Q}^\times$. Let y_i be the fixed points of w_p on $X_0(p)$ and put $D = \Sigma_i(y_i)$. Then one sees that $(g - \sqrt{a})_0 > \Sigma'(y_i)$ and $(g + \sqrt{a})_0 > \Sigma''(y_i)$ with $D = \Sigma'(y_i) + \Sigma''(y_i)$. This notion and a study on y_i give the inequality that the degree of $D \leqq 4$, (2.3). This criterion gives the proof, except for $p = 43, 67, 73, 97$ and 163. (2) The upper semicontinuity and a study on the action of w_p on $\mathscr{X}_0(p) \otimes \boldsymbol{F}_2$ give a non constant rational function $h(/\boldsymbol{F}_2)$ on $\mathscr{X}_0^+(p) \otimes \boldsymbol{F}_2$ with $(h)_\infty < 2(\mathrm{cusp})$ (2.4), where $\mathscr{X}_0^+(p) = \mathscr{X}_0(p)/\langle w_p \rangle$. Then $\# \mathscr{X}_0^+(p)(\boldsymbol{F}_2) \leqq 5$ and $\# \mathscr{X}_0^+(p)(\boldsymbol{F}_4) \leqq 9$, which complete the remaining case. For $p = 13$ and 37, we apply other methods.

For the case $p < 300$, we get an estimate of $n = n(k, p)$ by an integer which depends only on k and p (see § 2). We add the table in Section 4.

The author thanks to B. Mazur, T. Sekiguchi and K. Cho for their useful remarks on curves.

Notation. For a prime number q, $\boldsymbol{Q}_q^{\mathrm{ur}}$ denotes the maximal unramified extension of $\boldsymbol{Q}_q$. Let K be a finite extension of $\boldsymbol{Q}$, $\boldsymbol{Q}_q$ or $\boldsymbol{Q}_q^{\mathrm{ur}}$, and A an abelian variety defined over K. Then $\mathcal{O}_K$ denotes the ring of integers of K, $A_{/\mathcal{O}_K}$ denotes the Néron model of A over the base $\mathcal{O}_K$.

§1. Preliminaries

Let p be a prime number, $X_1(p^r)$ (resp. $X_0(p^r)$) the modular curve (defined over $\boldsymbol{Q}$) which corresponds to the modular group $\Gamma_1(p^r)$ (resp. $\Gamma_0(p^r)$). For $p^r \geqq 5$, $X_1(p^r)$ is the coarse moduli space $(/\boldsymbol{Q})$ of the isomorphism classes of the generalized elliptic curves E with a torsion point P of order p^r up to the isomorphism $(-1)_E\colon E \rightleftarrows E$. We denote by $Y_1(p^r)$, $Y_0(p^r)$ the affine open subschemes $X_1(p^r)\backslash\{\text{cusps}\}$ and $X_0(p^r)\backslash\{\text{cusps}\}$, respectively. Let k be a number field and x a k-rational point on $Y_1(p^r)$ (resp. $Y_0(p^r)$). Then there exists an elliptic curve E defined over k with a torsion point P of order p^r (resp. a cyclic subgroup A of rank p^r) defined over k (see [2] VI Proposition (3.2)). Let $f\colon X_1(p^r) \to X_0(p^r)$ be the natural morphism: $(E, \pm p) \to (E, \langle P\rangle)$, where $\langle P\rangle$ is the cyclic subgroup generated by P. Then f is a Galois covering with the Galois group $\bar{\Gamma}(p^r) = \Gamma_0(p^r)/\pm\,\Gamma_1(p^r)$ $(\simeq (\boldsymbol{Z}/p^r\boldsymbol{Z})^\times/\pm 1)$. For an integer i prime to p, $[i]$ $(=[-i])$ denotes the element of $\bar{\Gamma}(p^r)$ respresented by $g \in \Gamma_0(p^r)$, $g \equiv \begin{pmatrix} i & * \\ 0 & * \end{pmatrix} \bmod p^r$. The action of $[i]$ is defined by $(E, \pm P) \to (E, \pm\, i\cdot P)$. Let $w = w_{p^r}$ be the fundamental involution of $X_0(p^r)$: $(E, A) \mapsto (E/A, E_{p^r}/A)$ and $X_0^+(p^r)$ the quotient $X_0(p^r)/\langle w\rangle$. For a point on a modular curve, $\to X_0(1)$ (= the projective j-line$/\boldsymbol{Q}$), $j(x)$ denotes the modular invariant of x. We here explain the fixed points of w_p on $X_0(p)$ and add a table of the Mordell-Weil groups of subcoverings $X\colon X_1(p^r) \to X \to X_0(p^r)$. Further we discuss the fixed points of w_p on $\mathscr{X}_0(p) \otimes \boldsymbol{Z}_2$ and prepare some lemmas on curves, which will be used in Section 2.

(1.1) The ramification points of $Y_1(p^r) \longrightarrow Y_0(p)$ $(p^r \geqq 5)$.

$j(x)$	# {ramification points}	
1728	2	if $p \equiv 1 \bmod 4$
0	2	if $p \equiv 1 \bmod 3$.

(1.2) The ramification points of $X_0(p) \longrightarrow X_0^+(p)$ $(p \geqq 5)$ and $X_0(11^2) \longrightarrow X_0^+(11^2)$.

Let $h = h(-p)$ be the class number of $\boldsymbol{Q}(\sqrt{-p})$, and $h' = h'(p)$ the class number of the order $\boldsymbol{Z}[\sqrt{-p}]$ for $p \equiv 1 \bmod 4$. Then $h' = h$ if $p \equiv -1 \bmod 8$, $h' \equiv 3h$ if $p \equiv 3 \bmod 8$ (see e.g., [12] Part 8). Denote by $s = s(p)$

the number of the ramification points of $X_0(p) \to X_0^+(p)$ $(p \geqq 5)$. Then

$$s = \begin{cases} h & \text{if } p \equiv 1 \bmod 4 \\ h + h' & \text{if } p \equiv 1 \bmod 4 \end{cases}$$

(loc. cit.). Let H (resp. H') be the Hilbert class field of $\boldsymbol{Q}(\sqrt{-p})$ (resp. of the order $\boldsymbol{Z}[\sqrt{-p}]$ if $p \equiv 1 \bmod 4$) and $x_1, \cdots, x_h, \cdots, x_s$ the ramification points. Let $H \xhookrightarrow{\iota} \boldsymbol{C}$ (resp. $H' \xhookrightarrow{\iota'} \boldsymbol{C}$) be an embedding, ρ the complex conjugation of H (resp. H') induced by this embedding, and H^+ (resp. H'^+) the fixed field by ρ. For i, $1 \leqq i \leqq h$, x_i is defined over H and cojugate over $\boldsymbol{Q}(\sqrt{-p})$. One of them, say x_1, is defined over H^+. (Under the embedding ι of H into $\boldsymbol{C}$, x_1 is represented by the elliptic curve $\boldsymbol{C}/\mathfrak{a}$ for an ideal $\mathfrak{a}$ of the ring of integers of $\boldsymbol{Q}(\sqrt{-p})$ which satisfies $(\mathfrak{a}^\rho) \sim (\mathfrak{a})$ in the ideal class group of $\boldsymbol{Q}(\sqrt{-p})$. If $p \equiv -1 \bmod 4$, $x_{h+i} (1 \leqq i \leqq h')$ are defined over H' and conjugate over $\boldsymbol{Q}(\sqrt{-p})$. One of them, say x_{h+1}, is defined over H'^+. (Under the embedding ι' of H' into $\boldsymbol{C}$, x_{h+1} is represented by the elliptic curve $\boldsymbol{C}/\boldsymbol{Z} + \boldsymbol{Z}\sqrt{-p}$).

There are six ramification points of $X_0(11^2) \to X_0^+(11^2)$, which are conjugate over $\boldsymbol{Q}$, and the set of the ramification points is a disjoint union of two orbits of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\sqrt{-1}))$ of length three.

(1.3) The cuspidal sections of $X_0(p^r)$ ([2]) .

For integers k, $1 \leqq k \leqq r$, and i prime to p, let $\binom{i}{p^k}$ be the cuspidal section of $X_0(p^r)$ represented by the pair $(\boldsymbol{G}_m \times \boldsymbol{Z}/p^{r-k}\boldsymbol{Z}, \boldsymbol{Z}/p^r\boldsymbol{Z}(\zeta^i, p^k))$. Here, $\boldsymbol{Z}/p^r\boldsymbol{Z}(\zeta^i, p^k)$ is the cyclic subgroup of $\mu_{p^r} \times \boldsymbol{Z}/p^r\boldsymbol{Z}$ generated by (ζ^i, p^k), $\zeta = \zeta_{p^r}$ is a primitive p^r-th root of 1. We denote $0 = \binom{0}{1}$ and $\infty = \binom{1}{0}$. The ramification index of the covering $X_1(p^r) \to X_0(p^r)$ at $\binom{i}{p^k}$ is $\min\{p^k, p^{r-k}\}$. Let 0_i, $1 \leqq i \leqq p^{r-1}(p-1)$, be the cuspidal sections of $X_1(p^r)$ lying over $0 = \binom{0}{1}$, which are $\boldsymbol{Q}$-rational. We call them the 0-cusps.

(1.4) We will use the following coverings. Here γ is the generator of $\Gamma_0(p^r) \simeq (\boldsymbol{Z}/p^r\boldsymbol{Z})^\times/\pm 1$, $s = s(p)$ is the number of the ramification points of $X \to Y$, and $g(X)$ and $g(Y)$ are respectively the genuses of X and Y. If $X = X_0(p)$ and $Y = X_0^+(p)$, put $g_0(p) = g(X)$, $g_+(p) = g(Y)$.

Table 1.

prime p	covering	s	$g(X)$	$g(Y)$
2	$X = X_1(32)/\langle\gamma^4\rangle \xrightarrow{2} Y = X_1(32)/\langle\gamma^2\rangle$	8	5	1
3	$X = X_1(27) \xrightarrow{3} Y = X_1(27)/\langle\gamma^3\rangle$	12	13	1
5	$X = X_1(25)/\langle\gamma^5\rangle \xrightarrow{5} Y = X_0(25)$	4	4	0
(7	$X = X_1(49)/\langle\gamma^3\rangle \xrightarrow{3} Y = X_0(49)$	2	3	1)
11	$X = X_1(121) \xrightarrow{2} Y = X_0^+(121)$	6	6	2
13	$X = X_1(13) \xrightarrow{2} Y = X_1(13)/\langle\gamma^3\rangle$	6	2	0
17	$X = X_1(17) \xrightarrow{2} Y = X_1(17)/\langle\gamma^4\rangle$	8	5	1
19	$X = X_1(19) \xrightarrow{3} Y = X_1(19)/\langle\gamma^3\rangle$	6	7	1
23	$X = X_1(23) \xrightarrow{11} Y = X_0(23)$	0	12	2
or	$X = X_0(23) \xrightarrow{2} Y = X_0^+(23)$	6	2	0
$p \geqq 29$ $\neq 37$	$X = X_0(p) \xrightarrow{2} Y = X_0^+(p)$			

For $p = 37$, let $(X_1(37) \xrightarrow{9}) X \xrightarrow{2} Y = X_0(37)$ be the double covering. Then $s = 2$, $g(X) = 4$ and $g(Y) = 2$.

(1.5) Let $J = J(X)$ be the jacobian variety of the modular curve X above. On the Mordell-Weil groups of J or $J_0^-(p)$ ($p \geqq 11$), we know the following (Kenku [6, 8, 9], Mazur and Tate [20], Mazur [17], [35] Table 1, 3, 5).

Table 2.

p	$\# J(\boldsymbol{Q})$ or $\# J_0^+(p)(\boldsymbol{Q})_{\text{tor}}$
2	$2\cdot 5 \mid \# J(\boldsymbol{Q}) \mid 2^9\cdot 5^2$
3	$3\cdot 19 \mid \# J(\boldsymbol{Q}) \mid 3^4\cdot 19\cdot 307$
5	$J(\boldsymbol{Q}) \simeq \boldsymbol{Z}/71\boldsymbol{Z}$
7	$J(\boldsymbol{Q}) \simeq \boldsymbol{Z}/14\boldsymbol{Z}$
11	$2\cdot 5 \mid \# J_0^-(121)(\boldsymbol{Q}) \mid 2^a\cdot 5^2$ for an integer $a \geqq 1$
13	$J(\boldsymbol{Q}) \simeq \boldsymbol{Z}/19\boldsymbol{Z}$
17	$2\cdot 73 \mid \# J(\boldsymbol{Q}) \mid 2^3\cdot 73$
19	$3 \mid \# J(\boldsymbol{Q}) \mid 3^2\cdot 387$
23	$11 \mid \# J_1(23)(\boldsymbol{Q}) \mid 11\cdot 37181$
$p \geqq 11$	$J_0^-(p)(\boldsymbol{Q})_{\text{tor}} \simeq \boldsymbol{Z}/m\boldsymbol{Z}$, where $m = \text{num}((p-1)/12)$.

For $p = 37$, we will see that the Mordell-Weil group of Coker $(J_0(37) \to J(X))$ is isomorphic to $Z/5Z$. (The double covering $X \to X_0(37)$ has two ramification points with the modular invariant $j = 1728$).

(1.6) Let $\mathscr{X}_1(p^r)$, $\mathscr{X}_0(p^r)$ be the normalizations of the projective j-line $\mathscr{X}_0(1) \simeq \boldsymbol{P}^1{}_{\boldsymbol{Z}}$ in $X_1(p^r)$ and $X_0(p^r)$, respectively. These are smooth over $\boldsymbol{Z}[1/p]$ ([2]VI Proposition (6.7)). The special fibre $\mathscr{X}_1(p^r) \otimes \boldsymbol{F}_p$ (also $\mathscr{X}_0(p^r) \otimes \boldsymbol{F}_p$) has $r+1$ irreducible components $E_0, \cdots, E_r$. The 0-cusps $\otimes \boldsymbol{F}_p$ are the sections of the smooth component $E_0^h = E_0 \backslash$ {supersingular points on $\mathscr{X}_1(p^r) \otimes \boldsymbol{F}_p$}. Put $\mathscr{V}_1(p^r) = \mathscr{X}_1(p^r) \backslash \sum_{i=0}^{r-1} E_{i+1}$, which is smooth over $\boldsymbol{Z}$. The 0-cusps are the sections of $\mathscr{V}_1(p^r)$ ([2] V §2, §4, VI).

N.B. (loc. cit.). Let $\mathscr{C}' = \mathscr{C}_1'(p^r)$ be the algebraic stack which represents the functor: for a scheme $S/\boldsymbol{Z}$, $\mathscr{C}'(S)$ is the set of the isomorphism classes of the generalized elliptic curves C with a S-section P of order p^r such that $\langle P \rangle \simeq (\boldsymbol{Z}/p^r\boldsymbol{Z})/S$, isomorphic locally for the étale topology. Here $\langle P \rangle$ is the finite étale subgroup generated by the section P (see loc. cit. V §2, §4). Let $\mathscr{V}_1(p^r)$ be the scheme induced by $\mathscr{C}'$ (= "schéma grossier", loc. cit. VI, VII p. 300). Then $\mathscr{V}_1(p^r)$ is an open subscheme of $\mathscr{X}_1(p^r)$ and smooth over $\boldsymbol{Z}$ (see loc. cit. V §2, §4, I (8.22)). The 0-cusps are the sections of $\mathscr{V}_1(p^r)$ represented by the pairs $(\boldsymbol{G}_m \times \boldsymbol{Z}/p^r\boldsymbol{Z}, \pm P)$ for $P \in \boldsymbol{Z}/p^r\boldsymbol{Z}$.

Let k be an algebraic number field of degree d, $\tilde{k}$ the smallest Galois extension of $\boldsymbol{Q}$ containing k. For a rational prime q, let $\mathfrak{q}$ be a prime of $\tilde{k}$ lying over q. We denote by f_q, e_q the degree of $\mathfrak{q}$ and the ramification index of q in $\tilde{k}$, respectively. Let $C = C(k, p)$ be the set of rational primes q as follows:

$$(1.7)\qquad \begin{aligned} C(k,p) = \{q \neq 2, p\} &\cup \{q = p \quad \text{if } e_p < p-1\} \\ &\cup \{q = 2 \quad \text{if } p \neq 2,\ 11,\ 17 \text{ or } p \equiv 1 \bmod 8\}\,. \end{aligned}$$

Define an integer $n' = n'(k, p)$ as the least non-negative integer subjects to

$$(1.8)\qquad p^{n'} > \min_{q \in C(k,p)} \{1 + q^{f_q} + 2\sqrt{q^{f_q}}\}$$

and

$$n' > 4 \quad \text{if } p = 2,\ n' > 2 \quad \text{if } p = 3,\ n' > 1 \quad \text{if } p = 5,\ 7.$$

For $p \geqq 23$, let $n'' = n''(k, p)$ be the least integer such that $n'' \geqq n'$ and $p^{n''} > 1 + 2^{f_2} + 2\sqrt{2^{f_2}}$. For the prime $p \equiv 1 \bmod 8$ $(p \geqq 23)$, $n' = n''$ (see (1.7)).

For a $\tilde{k}$-rational point x on $X_1(p^r)$ (resp. $X_0(p^r)$), by x we denote the $\mathcal{O}_{\tilde{k}}$-section: $\operatorname{Spec} \mathcal{O}_{\tilde{k}} \to \mathcal{X}_1(p^r)$ (resp. $\to \mathcal{X}_0(p^r)$) which is the unique extension of x. Let E be an elliptic curve defined over k with a k-rational point P of order p^r, and x the point on $Y_1(p^r)$ represented by the pair $(E, \pm P)$.

LEMMA (1.9). *Let q be a rational prime such that $q \neq p$, or $q = p$ and $e_q < p - 1$, and $\mathfrak{q}$ a prime of $\tilde{k}$ lying over q. If $p^r > 1 + q^{f_q} + 2\sqrt{q^{f_q}}$, then $x^\sigma \otimes \mathcal{O}/\mathfrak{p}$ is a 0-cusp for any $\sigma \in \operatorname{Isom}_{\boldsymbol{Q}}(k, \overline{\boldsymbol{Q}})$, where $\mathcal{O}$ is the ring of integers of $\tilde{k}$.*

Proof. We denote f_q by f, and $\mathcal{O}^{\mathrm{ur}}$ the ring of integers of $\tilde{k} \otimes \boldsymbol{Q}_q^{\mathrm{ur}}$. The point x^σ is represented by (E^σ, P^σ) which is defined over $\tilde{k}$. By the universal property of the Néron model $E_{/\mathcal{O}}$, there exists a homomorphism $f\colon (\boldsymbol{Z}/p^r\boldsymbol{Z})_{/\mathcal{O}} \to E_{/\mathcal{O}}$ such that $f \otimes \tilde{k}$ is an isomorphism into E. Let A be the flat closure of $f((\boldsymbol{Z}/p^r\boldsymbol{Z})_{/\mathcal{O}} \otimes \tilde{k})$ in the Néron model $E_{/\mathcal{O}}$, which is a finite flat group scheme of rank p^r. If $q \neq p$, f is an isomorphism. If $q = p$ and $e_p < p - 1$, by the fundamental property of the finite flat group schemes ([26] § 3 Proposition (3.3.2)), f is also an isomorphism $(\colon f \otimes \mathcal{O}^{\mathrm{ur}}$ is an isomorphism, then $\ker(f \otimes \boldsymbol{F}_{q^f}) = \{0\})$. Since $p^r > 1 + q^f + 2\sqrt{q^f}$ $(\geqq 5)$, E has semistable reduction at $\mathfrak{q}$ (Tate [35] p. 46), and has multiplicative reduction (e.g., [16] Lemma 2). Fix an embedding of $\tilde{k}$ into $\overline{\boldsymbol{Q}}_q$. Then the connected component $(E^\sigma{}_{/\mathcal{O}} \otimes \boldsymbol{F}_{q^f})^0$ of the unity is a torus T and $T \otimes_{\boldsymbol{F}_{q^f}} \boldsymbol{F}_{q^{2f}} \simeq \boldsymbol{G}_{m/\boldsymbol{F}_{q^{2f}}}$. So if $x^\sigma \otimes \boldsymbol{F}_{q^f}$ is not a 0-cusp, then $\boldsymbol{Z}/p^r\boldsymbol{Z} \subset T(\boldsymbol{F}_{q^f}), \simeq \boldsymbol{Z}/(q^f - 1)\boldsymbol{Z}$ or $\simeq \boldsymbol{Z}/(q^f + 1)\boldsymbol{Z}$. Therefore the condition $p^r > 1 + q^f + 2\sqrt{q^f}$ shows that $x^\sigma \otimes \boldsymbol{F}_{q^f}$ is a 0-cusp. □

(1.10) Now we describe the fixed points of $w = w_p$ of $\mathcal{X}_0(p) \otimes \boldsymbol{Z}[1/p]$ $(p \geqq 5)$.

Let $\mathcal{X}_0^+(p)$ be the quotient $\mathcal{X}_0(p)/\langle w \rangle$, which is smooth over $\boldsymbol{Z}[1/p]$. ($\mathcal{X}_0(p)$ is smooth over $\boldsymbol{Z}_2$ and the action of w on $\mathcal{X}_0(p) \otimes \boldsymbol{F}_2$ is generically étale of degree two, see [2] VI Proposition (6.7)). Let $q, \neq p$, be a rational prime, y a fixed point of w on $\mathcal{X}_0(p) \otimes \boldsymbol{F}_q$. Then y is represented by an elliptic curve $(/\overline{\boldsymbol{F}}_q)$ with a subgroup A of rank p such that $(E, A) \simeq (E/A, E_p/A)$ (see [2]). There exists an endomorphism α of E such that

$\alpha(A) = \{0\}$ and $\alpha^2 = -p$. The pair (E, α) is lifted to characteristic zero (over a finite extension of $\boldsymbol{Q}_q^{\mathrm{ur}}$), see e.g., [12] Part 12 § 5 Theorem 14). Thus y is the special fibre of a fixed point x_i for an integer i, $1 \leqq i \leqq s = s(p)$ (see (1.2)). Let x be a fixed point of w on $X_0(p)$ and $\mathcal{O}$ the ring of integers of $\boldsymbol{Q}_q^{\mathrm{ur}}$. Let $\widehat{\mathcal{O}_{\mathscr{X}_0(p),x}} = \mathcal{O}[[t]]$ be the completion along the $\mathcal{O}$-section x ([2] VI Proposition (6.7)). Then, $\sigma = w^*$ is of the form $\sigma(t) = -t + a_2t^2 + \cdots$ for $a_i \in \mathcal{O}$ and $a_j \in \mathcal{O}^\times$ for some j if $q = 2$. If $q \neq 2$, p, it is easily seen that $x_i \otimes \bar{\boldsymbol{F}}_q \neq x_j \otimes \bar{\boldsymbol{F}}_q$ for $x_i \neq x_j$.

Now assume $q = 2$ $(p \geqq 5)$. The double covering $\mathscr{X}_0(p) \otimes \boldsymbol{F}_2 \to \mathscr{X}_0^+(p) \otimes \boldsymbol{F}_2$ has wild ramifications at the fixed points of $w = w \otimes \boldsymbol{F}_2$ (see e.g., [29] Chapitre IV). By the Riemann-Hurwitz formula, $2g_0(p) - 2 = 2(2g_+(p) - 2) + \sum_y(1 + i(y))$, where y are the ramification points and $i(y)$ is the index of wild ramification at y (see loc. cit., [17] Chapter II). Therefore, there are at most $s(p)/2$ ramification points on $\mathscr{X}_0(p) \otimes \bar{\boldsymbol{F}}_2$. Let $v = v_2$ be the normalized valuation of $\bar{\boldsymbol{Q}}_2$ such that $v(2) = 1$.

SUBLEMMA. *Let x, σ and $\mathcal{O}$ be as above, and π a prime element of $\mathcal{O}$. Let $\mathcal{O}'$ be the ring of integers of the cyclic extension of $\boldsymbol{Q}_2^{\mathrm{ur}}(x)$ of degree three, and π' a prime element of $\mathcal{O}'$.*

(i) *If $v(\pi) = 1$ $(\mathcal{O} \simeq W(\bar{\boldsymbol{F}}_2))$, there are at most two solutions $t = \alpha \in \pi\mathcal{O}$ of $t = \sigma(t)$, and at most three solutions $t = \alpha \in \pi'\mathcal{O}'$ of the same equation.*

(ii) *If $v(\pi) = 1/2$, $t = \sigma(t)$ has at most two solutions in $\pi\mathcal{O}$.*

Proof. The relation $\sigma^2 = 1$ implies $a_3 = -a_2^2$. The remaining part is elementary. □

Case $p \equiv 1 \bmod 8$. The ramification index of the rational prime 2 in H is 2 (see (1.2)). By (ii) above we see that the map $\{x_i\} \to \{x_i \otimes \bar{\boldsymbol{F}}_2\}$ is two to one. Two of $x_i \otimes \bar{\boldsymbol{F}}_2$ are $\boldsymbol{F}_2$-rational (see [24] Theorem 3).

Case $p \equiv 5 \bmod 8$. By the same reason as above, the map $\{x_i\} \to \{x_i \otimes \bar{\boldsymbol{F}}_2\}$ is two to one. One of $x_i \otimes \bar{\boldsymbol{F}}_2$ is $\boldsymbol{F}_2$-rational (loc. cit.).

Case $p \equiv -1 \bmod 8$. In this case $H = H'$ (see (1.2)), the rational prime 2 splits in $\boldsymbol{Q}(\sqrt{-p})$ and $x_i \otimes \bar{\boldsymbol{F}}_2$ are not the supersingular points (e.g., [13] Chapter 8, [30]). By the uniqueness of the Deuring lifting (e.g., [12] Part 13, § 4 Theorem 13), $\{x_i\}_{1 \leqq i \leqq h} \to \{x_i \otimes \bar{\boldsymbol{F}}_2\}$ is injective. Hence (i) above shows that the map $\{x_i\}_{1 \leqq i \leqq 2h} \to \{x_i \otimes \bar{\boldsymbol{F}}_2\}$ is two to one. Let $\mathfrak{p} = \mathfrak{p}_2$ be a prime of H lying over 2. Then these $\{x_i \otimes \bar{\boldsymbol{F}}_2\}$ is the disjoint union of orbits of the action of $\mathrm{Gal}(H_{\mathfrak{p}}/\boldsymbol{Q}(\sqrt{-p})) \simeq \mathrm{Gal}(\kappa(\mathfrak{p})/\boldsymbol{F}_2)$. Here $H_{\mathfrak{p}}$ is the

$\mathfrak{p}$-adic completion of H and $\kappa(\mathfrak{p}) = \mathcal{O}_H/\mathfrak{p}$. Note that the degree of $\mathfrak{p}$ is odd $\geqq 3$ for $p \geqq 23$, $p \equiv -1 \bmod 8$.

Case $p \equiv 3 \bmod 8$. The rational prime 2 does not ramify in H and the degree of the prime $\mathfrak{p}|2$ of H is two. H' is a cyclic extension of H of degree 3, which ramifies totally at the primes lying over 2 (e.g., [12] Part 8 Theorem 7). Then $x_i^\sigma \otimes \kappa(\mathfrak{p}') = x_i \otimes \kappa(\mathfrak{p}')$ for a prime $\mathfrak{p}'|2$ of H' and $\sigma \in \mathrm{Gal}(H'/H)$, where $\kappa(\mathfrak{p}') = \mathcal{O}_{H'}/\mathfrak{p}'$. Let $E/\boldsymbol{F}_2$ be a supersingular elliptic curve. Then $x_i \otimes \bar{\boldsymbol{F}}_2$ is represented by the pair (E, A) for $A = \ker(\alpha\colon E \to E)$, $\alpha^2 = -p$. Under the isomorphism

$$\mathrm{End}(E) \xrightarrow{\sim} \left\{\frac{a+bi+cj+dk}{2} \,\middle|\, a, b, c, d \in \boldsymbol{Z}, a \equiv b \equiv c \equiv d \bmod 2\right\}$$

(e.g., [35] § 7), α is represented by $ai + bj + ck$ for $a, b, c \in \boldsymbol{Z}$. Then, as $p \equiv 3 \bmod 8$, a, b, c must be odd. Therefore A is invariant under the action of $(1+\alpha)/2 \in \mathrm{End}(E)$. Let $(\tilde{E}, \tilde{\beta})$ be a lifting of $(E, (1+\alpha)/2)$ (e.g., [12] Part 13, § 5 Theorem 14). Then $x_i \otimes \bar{\boldsymbol{F}}_2$ is the special fibre of x_j for a j, $1 \leqq j \leqq h$, see (1.2). x_j is represented by $(\tilde{E}, \ker(2\tilde{\beta} - 1))$. Thus we see that the map $\{x_i\}_{1 \leqq i \leqq h} \to \{x_i \otimes \bar{\boldsymbol{F}}_2\}$ is one to one (see (i) above), and $\{x_{i+h}\}_{1 \leqq i \leqq 3h} \to \{x_i \otimes \bar{\boldsymbol{F}}_2\}$ is three to one. One of $x_i \otimes \bar{\boldsymbol{F}}_2$ is $\boldsymbol{F}_2$-rational ([24] Theorem 3).

Let y_j be the fixed point of $w = w \otimes \boldsymbol{F}_2$ on $\mathscr{X}_0(p) \otimes \boldsymbol{F}_2$ ($p \geqq 5$), $i(y)$ be the index of the wild ramification at y_j of the natural morphism $\mathscr{X}_0(p) \otimes \boldsymbol{F}_2 \to \mathscr{X}_0^+(p) \otimes \boldsymbol{F}_2$.

Table 3.

$p \bmod 8$	$i(y_j)$	$\#\{\boldsymbol{F}_2$-rational fixed points$\}$	$\#\{$non $\boldsymbol{F}_2$-rational fixed points$\}$
1	1	2	$h/2 - 2$
5	1	1	$h/2 - 1$
-1	1	0 ($p \geqq 23$)	h ($p \geqq 23$)
3	3	1	$h - 1$

Let K be a field, X a proper smooth curve defined over K. Let $\sigma \neq 1$ be an automorphism of X defined over K, $\{x_i\}_{1 \leqq i \leqq s}$ the set of the fixed points of σ, and set $D = \sum_{i=1}^{s}(x_i)$ a divisor of X. It is easy to see the following.

LEMMA (1.11). *If g is a rational function on X of degree m defined over K such that $(\sigma^* g) \neq (g)$ (= the divisor of g) and $g(x_i) \neq 0, \infty$. Then*

$$(\sigma^* g/g - 1)_0 > D.$$

In particular, $s \leqq 2m$. *If, moreover,* $\sigma^2 = 1$,

$$(\sigma^* g/g - 1)_0 = \sum_{i=1}^{s} m_i(x_i) + \sum_j \{(y_j) + (\sigma y_j)\}$$

for some positive integers m_i *such that* $\sum_{i=1}^{s} m_i(x_i)$ *is* K*-rational and* $y_j \neq \sigma y_j$.

Now let K be a finite extension of $\boldsymbol{Q}_2$, R the ring of integers of K with the residue field $\boldsymbol{F}_q$ for $q = 2^r$. Suppose that X is the generic fibre of a smooth projective curve $\mathscr{X} \to \operatorname{Spec} R$, and σ an involution of $\mathscr{X}$ defined over R such that $\mathscr{Y}_{\mathrm{dfn}} = \mathscr{X}/\langle\sigma\rangle \to \operatorname{Spec} R$ is smooth and that the natural morphism f: $\mathscr{X} \otimes \boldsymbol{F}_q \to \mathscr{Y} \otimes \boldsymbol{F}_q$ is not radicial. Let $E = \sum m_i(z_i)$, $m_i > 0$, be a K-rational divisor of X such that $1 < \dim_K H^0(X, \mathcal{O}(E))$. Then we have

LEMMA (1.12). *Assume further that* $\sigma = \sigma \otimes \boldsymbol{F}_q$ *has fixed points,* $z_i \otimes \boldsymbol{F}_q$ *are not fixed points and that* $\sigma^*(\sum m_i(z_i \otimes \boldsymbol{F}_q)) = \sum m_i(z_i \otimes \boldsymbol{F}_q)$. *Then there exists a covering* g: $\mathscr{Y} \otimes \boldsymbol{F}_q \to \boldsymbol{P}^1{}_{/\boldsymbol{F}_q}$ *defined over* $\boldsymbol{F}_q$ *such* $f^*((g)_\infty) > \sum m_i(z_i \otimes \boldsymbol{F}_q)$.

Proof. Let K' be a finite extension of K over which the z_i's are defined, and R', $\boldsymbol{F}_{q'}$ the ring of integers of K' and the residue field of R', respectively. Let $\mathscr{L} = \overset{i}{\otimes}\, \mathcal{O}(z_i)^{\otimes m_i}$ be the Cartier divisor of $\mathscr{X} \otimes R'$. Then $\dim_{\boldsymbol{F}_{q'}} H^0(\mathscr{X} \otimes \boldsymbol{F}_{q'}, \mathscr{L}) > 1$ by the upper semicontinuity ([34] (7.7.5)1). Then $\dim_{\boldsymbol{F}_q} H^0(\mathscr{X} \otimes \boldsymbol{F}_q, \mathcal{O}(E)) > 1$, because $\mathscr{L} \simeq \mathcal{O}(E) \otimes R'$ over $\mathscr{X} \otimes R'$. By the assumption $\sigma^*(E \otimes \boldsymbol{F}_q) = E \otimes \boldsymbol{F}_q$, there exists a non-constant section h of $H^0(\mathscr{X} \otimes \boldsymbol{F}_q, \mathcal{O}(E))$ such that $\boldsymbol{F}_q \oplus \boldsymbol{F}_q h$ is a σ-invariant subspace. So $\sigma^* h = h + a$ for an $a \in \boldsymbol{F}_q$. The proof is completed if $a = 0$ is shown (because $\mathscr{X} \otimes \boldsymbol{F}_q \to \mathscr{Y} \otimes \boldsymbol{F}_q$ is generically étale of degree 2). Suppose $a \neq 0$. For each point x on $\mathscr{X} \otimes \boldsymbol{F}_q \backslash \operatorname{Supp}(E \otimes \boldsymbol{F}_q)$, $h \in \mathcal{O}_{\mathscr{X} \otimes \boldsymbol{F}_q, x}$. The covering $\mathscr{X} \otimes \boldsymbol{F}_q \to \mathscr{Y} \otimes \boldsymbol{F}_q$ is then factored by $\operatorname{Spec} \mathcal{O}_{\mathscr{Y} \otimes \boldsymbol{F}_q, f(x)}[h]$ at x:

$$\begin{tikzcd} \operatorname{Spec} \mathcal{O}_{\mathscr{X} \otimes \boldsymbol{F}_q, x} \arrow[rr, "f"] \arrow[dr] & \arrow[d, phantom, "\circlearrowleft"] & \operatorname{Spec} \mathcal{O}_{\mathscr{Y} \otimes \boldsymbol{F}_q, f(x)} \\ & \operatorname{Spec} \mathcal{O}_{\mathscr{Y} \otimes \boldsymbol{F}_q, f(x)}[h] \arrow[ur] & \end{tikzcd}$$

The morphism f is finite of degree 2, and $\operatorname{Spec} \mathcal{O}_{\mathscr{Y} \otimes \boldsymbol{F}_q, f(x)}[h] \to \operatorname{Spec} \mathcal{O}_{\mathscr{Y} \otimes \boldsymbol{F}_q, f(x)}$ is étale of degree 2, since $\sigma^* h(z) \neq h(z)$ for any point z on $\mathscr{X} \otimes \boldsymbol{F}_q \backslash \operatorname{Supp}(E \otimes \boldsymbol{F}_q)$. Therefore f is étale at any point $x \in \mathscr{X} \otimes \boldsymbol{F}_q \backslash \operatorname{Supp}(E \otimes \boldsymbol{F}_q)$.

This contradicts to our assumption. $\square$

§2. The rational points on $Y_1(p^r)$

Let k be an algebraic number field of degree d; $\tilde{k}$, e_q, f_q, $C = C(k, p)$, $n' = n'(k, p)$ and $n'' = n''(k, p)$ be as in the last section. Assuming the existence of a k-rational point on $Y_1(p^r)$ with $r > n(k, p)$, we here introduce a rational function g on a modular curve whose divisor is determined by the k-rational point as above. Further we prepare propositions which concern g and the fixed points of w_p ($p \geqq 23$). Let x be a k-rational point on $Y_1(p^r) = X_1(p^r)\backslash\{\text{cusps}\}$ for $r \geqq n'(k, p)$. By x we denote also the image of x by the natural morphism $X_1(p^r) \to X$, see (1.4). We consider only the primes p with $p \leqq 23$ or ($p \geqq 29$ and) $\sharp J_0^-(p)(\boldsymbol{Q}) < \infty$. For each $\sigma \in \mathrm{Isom}_{\boldsymbol{Q}}(k, \bar{\boldsymbol{Q}})$, Lemma (1.9) shows that $x^\sigma \otimes \kappa(\mathfrak{q}) = 0_{i_\sigma} \otimes \kappa(\mathfrak{q})$ for an integer i_σ and a prime $\mathfrak{q}$ of $\tilde{k}$ lying over the rational prime $q \in C = C(k, p)$ which attains the minimal value of $1 + q^{f_q} + 2\sqrt{q^{f_q}}$, where $\kappa(\mathfrak{q}) = \mathcal{O}_{\tilde{k}}/\mathfrak{q}$. Consider the $\boldsymbol{Q}$-rational section

$$i(x) = \mathrm{cl}\left(\textstyle\sum_\sigma (x^\sigma) - \sum_\sigma (0_{i_\sigma})\right)$$

of $A = J(X)$ for $p \leqq 23$, $p \neq 11$; of $A = \mathrm{Coker}\,(J_0(37) \to J(X))$ for $p = 37$; of $A = J_0^-(121)$ for $p = 11$; and of $A = J_0^-(p)$ for $p \geqq 29$ (see (1.4)). Let $\mathscr{X}$ be the normalization of the projective j-line $\mathscr{X}_0(1)$ in X (see (1.4)). Let $\boldsymbol{Z}_{(q)}$ be the localization of $\boldsymbol{Z}$ at the prime q and $\mathcal{O}_{(q)} = \mathcal{O}_{\tilde{k}} \otimes \boldsymbol{Z}_{(q)}$. Then $x^\sigma \otimes \mathcal{O}_{(q)}$, $0_{i_\sigma} \otimes \mathcal{O}_{(q)}$ are the sections of the smooth part of $\mathscr{X} \otimes \boldsymbol{Z}_{(q)}$, see (1.6), (1.9). Let

$$i(x^\sigma)\colon \mathrm{Spec}\,\mathcal{O}_{(q)} \xrightarrow{x^\sigma} \mathscr{X}^{\mathrm{smooth}} \otimes \boldsymbol{Z}_{(q)} \longrightarrow A_{/\boldsymbol{Z}_{(q)}} \qquad z \longrightarrow \mathrm{cl}((z) - (0_{i_\sigma}))\,.$$

Then by our assumptions on q and r (see (1.8), (1.9)), $i(x_\sigma) \otimes \kappa(\mathfrak{q}) = 0$. Then $i(x) \otimes \kappa(\mathfrak{q}) = (\sum_\sigma i(x^\sigma)) \otimes \kappa(\mathfrak{q}) = 0$, i.e., $i(x) \otimes \boldsymbol{F}_q = 0$. The $\boldsymbol{Q}$-rational section $i(x) \otimes \boldsymbol{Z}_{(q)}$ is of finite order for $p \neq 37$, see (1.5). The specialization lemma of the finite flat group schemes ([26] Proposition (3.3.2), [18] Proposition (1.2)) leads that $i(x) = 0$ for $p \neq 37$ (, note: $1 < 3 - 1 \leqq q - 1$, (1.7)). Then there is a rational function g on X such that (see (1.4))

$$(2.1)\quad (g) = \begin{cases} \sum (x^\sigma) - \sum (0_{i_\sigma}) & \text{for } p \leqq 23,\ p \neq 11 \\ \sum (x^\sigma) - d(0) & \text{for } p = (23), 29, 31, 41, 47, 59, 71 \\ & \qquad (\text{Case } X_0^+(p) \simeq \boldsymbol{P}^1); \\ \sum (x^\sigma) + d(\infty) - \sum (\gamma(x^\sigma)) - d(0) & \text{for } p = 11,\ p > 29 \\ & \qquad \text{with } \sharp J_0^-(p)(\boldsymbol{Q}) < \infty\,. \end{cases}$$

For $p=37$, we will show $\mathrm{Coker}\,(J_0(37)\to J(X))(\boldsymbol{Q})\simeq \boldsymbol{Z}/5\boldsymbol{Z}$, see (3.4.2). Then we get a rational function g on X such that

$$(2.1)' \qquad (g)=\sum(x^{\sigma})+\sum(\gamma(0_{i_\sigma}))-\sum(\gamma(x^{\sigma}))-\sum(0_{i_\sigma}),$$

where $1\neq\gamma\in\mathrm{Aut}\,(X/X_0(37))$, see (1.4). As (g) is $\boldsymbol{Q}$-rational, we may assume that g is defined over $\boldsymbol{Q}$. If $p=11$ or p is the last case in (2.1), $(w^*g)=-(g)$ $(\neq 0)$; and if $p=37$, $(\gamma^*g)=-(g)$. So we may assume

$$(2.2) \qquad \begin{cases} w^*g=\dfrac{a}{g} \\ \gamma^*g=\dfrac{a}{g} \quad (\text{for } p=37) \end{cases}$$

for a square free integer a $(\neq 0)$. For $p\neq 37$, as $\boldsymbol{Q}(x_i)$ is not totally imaginary (see (1.2)), $a>0$.

PROPOSITION (2.3). *Let x be a k-rational point on $Y_1(p^r)$, g the rational function as above and $p=2, 3, 11, 17$, or $p\geqq 23$, $\neq 37$, with $\sharp J_0^-(p)(\boldsymbol{Q})<\infty$. In the case $p\equiv 5 \bmod 8$ and the class number $h=h(-p)$ of $\boldsymbol{Q}(\sqrt{-p})$ is divisible by 4, we further assume $p^r>1+q^{f_q}+2\sqrt{q^{f_q}}$ for an odd prime $q\neq p$. Then we have*

$$s=s(p)\leqq 2d\,.$$

Proof. *Case $p\geqq 23$ and $X_0^+(p)\simeq \boldsymbol{P}^1$.*

The rational function g is of degree d and $(g)\neq(w^*g)$. So the conditions of Lemma (1.11) are satisfied.

Case $p\geqq 23$, $\neq 37$, and $X_0^+(p)\neq \boldsymbol{P}^1$.

Let $x_1,\cdots,x_h,\cdots,x_s$ be the fixed points of $w=w_p$. Then $g(x_i)=\pm\sqrt{a}$ (see (2.2)). We may assume $g(x_1)=+\sqrt{a}$. First, we consider the case $p\equiv -1 \bmod 4$. Then $s=s(p)=h+h'$ (see (1.4)) is even, and $h(\leqq h')$ is odd. x_1 is defined over H^+ (see (1.4)) and $[H^+:\boldsymbol{Q}]$ is odd, so that $a=1$ (by our choice of a, see (2.2)). The points $x_1,\cdots,x_h$ (resp. $x_{h+1},\cdots,x_{h+h'}$) are conjugate to each other over $\boldsymbol{Q}$, so that

$$(g-1)_0>\textstyle\sum_{i=1}^{h}(x_i)$$

and

$$(g-1)_0>\textstyle\sum_{i=1}^{h'}(x_{h+i}) \qquad \text{or } (g+1)_0>\sum_{i=1}^{h'}(x_{h+i})\,.$$

In the first case $s=h+h'\leqq 2d$. In the second case, Lemma (1.11) and

and the fact that h and h' are odd integers show

$$(g-1)_0 > 2\textstyle\sum_{i=1}^{h}(x_i)$$

and

$$(g+1)_0 > 2\textstyle\sum_{i=1}^{h'}(x_{h+i}) .$$

Thus $2d \geqq 2h' \geqq s$.

Next, we consider the case $p \equiv 1 \bmod 4$. If $2d < h = s$, then

$$(g-\sqrt{a})_0 > \textstyle\sum'(x_i)$$
$$(g+\sqrt{a})_0 > \textstyle\sum''(x_i)$$

where $\sum' + \sum'' = \sum_{i=1}^{s}$ and $a > 1$ (because x_i are conjugate to each other over $\boldsymbol{Q}$). If $h \not\equiv 0 \bmod 4$, our assumption and Lemma (1.11) show $(g-\sqrt{a})_0 > 2\sum'(x_i)$ and $(g+\sqrt{a})_0 > 2\sum''(x_i)$. This contradicts that $s > 2d$. If $h \equiv 0 \bmod 4$, $a = p$. Set $D' = \sum'(x_i)$. D' is a divisor of degree $s/2$ and

$$(g-\sqrt{p}) = D' + E - \textstyle\sum_\sigma(w(x^\sigma)) - d(0) ,$$

for an effective divisor E. We have $w^*E = E$. By the assumption, there is an odd prime $q \neq p$ such that $p^r > 1 + q^{f_q} + 2\sqrt{q^{f_q}}$. Using the upper semicontinuity ([34] (7.7.5), 1), we get a rational function f on $\mathscr{X}_0(p) \otimes \bar{\boldsymbol{F}}_q$ such that

$$(f) = D' + E - d(\infty) - d(0) .$$

Then $(w^*f) = (f)$ so $w^*f = \pm f$. If $w^*f = +f$, $E > D'$. If $w^*f = -f$, $(f)_0 > D = \sum_{i=1}^{s}(x_i)$ (see (1.11)). Thus $s \leqq 2d$.

Case $p = 11$. The number of the fixed points of $w = w_{121}$ on $X_0(121)$ is six. Using g in (2.1), (2.2), we get $d \geqq 3 = s/2$ by the same way as above.

Case $p = 2, 17$. Let $f = \gamma^*g/g$ for $1 \neq \gamma \in \mathrm{Gal}(X/Y)$ (see (1.4)). Then $\gamma^*f = 1/f$ and $(f) = \sum(\gamma(x^\sigma)) + \sum(0_{i_\sigma}) - \sum(x^\sigma) - \sum(\gamma(0_{i_\sigma}))$. If $(\gamma^*g) = (g)$, then $\gamma(x^\sigma) = x^{\iota\sigma}$ for an $\iota \in \mathrm{Isom}_{\boldsymbol{Q}}(k, \bar{\boldsymbol{Q}})$ and any $\sigma \in \mathrm{Isom}_{\boldsymbol{Q}}(k, \bar{\boldsymbol{Q}})$. If $d = 2$, we see that $\{x, x^\sigma = \gamma(x)\}$ defines a $\boldsymbol{Q}$-rational point on Y. But we know that the $\boldsymbol{Q}$-rational points on $X_0(32)$, and on $X_0(17)$ are the cuspidal points ([35] table 1). If $d = 3$, one of the x^σ becomes a fixed point of γ. But we know that a ramification point of $X \to Y$ is either a cuspidal point or a point with the modular invariant $j = 1728$, see (1.1), (1.4). Therefore

$(\gamma^* g) \neq (g)$ for $d = 2$ and 3. The rest then follows from Lemma (1.11).

Case $p = 3$. Let $f = \gamma^* g/g$ for $1 \neq \gamma \in \mathrm{Gal}(X/Y)$ (see (1.4)). Then $(f) = \sum(\gamma(x^\sigma)) + \sum(0_{i_\sigma})) - \sum(x^\sigma) - \sum(\gamma(0_{i_\sigma}))$. For $d < 6 = s/2$, if $(\gamma^* g) = (g)$, $\gamma(x^\sigma) = x^{\iota\sigma}$ for an $\iota \in \mathrm{Isom}_{\boldsymbol{Q}}(k, \bar{\boldsymbol{Q}})$ and any $\sigma \in \mathrm{Isom}_{\boldsymbol{Q}}(k, \bar{\boldsymbol{Q}})$. Any fixed point of γ is a cuspidal point or a point with the modular invariant $j = 0$, so that $\gamma(x^\sigma) \neq x^\sigma$ for any $\sigma \in \mathrm{Isom}_{\boldsymbol{Q}}(k, \bar{\boldsymbol{Q}})$, see (1.4). Then $\{x^\sigma\}_\sigma$ is a disjoint union of $\langle\gamma\rangle$-orbits of length 3. If $d = 3$, $\{x^\sigma\}_\sigma = \{x, \gamma(x), \gamma^2(x)\}$ defines a $\boldsymbol{Q}$-rational point on Y. But a $\boldsymbol{Q}$-rational point on $X_0(27)$ is a cuspidal point or a point with the modular invariant $j = 0$ (see (1.4), [35] table 1). Therefore $(\gamma^* g) \neq (g)$ for $d < 6$. Then by Lemma (1.11) we get the result. $\square$

Let $\mathscr{X}^+ = \mathscr{X}_0^+(p)$ be the quotient $\mathscr{X}_0(p)/\langle w_p\rangle$, which is smooth over $\boldsymbol{Z}[1/p]$ (see (1.10)).

PROPOSITION (2.4). *Let $p \geqq 23$, $\neq 37$ be a prime number satisfying the condition $\sharp J_0^-(p)(\boldsymbol{Q}) < \infty$, g the rational function on $X_0(p)$ in* (2.2). *If $p^r > 1 + 2^{f_2} + 2\sqrt{2^{f_2}}$, then there is a covering f defined over $\boldsymbol{F}_2$,*

$$\mathscr{X}^+ \otimes \boldsymbol{F}_2 \xrightarrow{f} \boldsymbol{P}^1{}_{/\boldsymbol{F}_2}$$

such that $(f)_\infty = d'$ (cusp) for an integer d', $1 \leqq d' \leqq d$.

Proof. Let $\mathscr{L} = (\otimes^\sigma \mathscr{O}(x^\sigma)) \otimes \mathscr{O}(d(\infty))$ be the Cartier divisor on $\mathscr{X}_0(p) \otimes \mathscr{O}_{\tilde{k}}$, where $\mathscr{O}_{\tilde{k}}$ is the ring of integers of $\tilde{k}$. By our assumption, $\dim_{\bar{\boldsymbol{F}}_2} H^0(\mathscr{X}_0(p) \otimes \bar{\boldsymbol{F}}_2, \mathscr{L}) > 1$ (see [34] (7.7.5), 1), and $\mathscr{L} \otimes \bar{\boldsymbol{F}}_2 = \mathscr{O}(d(0) + d(\infty))$, see (1.9). The cusps $0 = 0 \otimes \boldsymbol{F}_2$ and $\infty = \infty \otimes \boldsymbol{F}_2$ are not the fixed points of $w = w \otimes \boldsymbol{F}_2$, while $\mathscr{X}_0 \otimes \boldsymbol{F}_2 \to \mathscr{X}^+ \otimes \boldsymbol{F}_2$ has ramifications points. The divisor $d(0) + d(\infty)$ is $\boldsymbol{F}_2$-rational, and is w-invariant. So Lemma (1.12) yields the desired covering f. $\square$

COROLLARY (2.5). *Under the assumption of* (2.4),

$$\sharp \mathscr{X}_0^+(p)(\boldsymbol{F}_{2^m}) < 1 + 2^m d$$
$$\sharp \mathscr{X}_0(p)(\boldsymbol{F}_4) \leqq 2 + 8d - s(p)\,.$$

PROPOSITION (2.6). *Let $p \geqq 23$, $\neq 37$, be a prime number such that $\sharp J_0^-(p)(\boldsymbol{Q}) < \infty$. Assume that $r \geqq n'' = n''(k, p)$ (see* (1.8)) *and let g be the rational function on $X_0(p)$ in* (2.2). *Then we get the following estimates of $\sharp \mathscr{X}_0^+(p)(\boldsymbol{F}_{2^m})$.*

(i) $p \equiv 1 \bmod 8$; $\sharp \mathscr{X}_0^+(p)(\boldsymbol{F}_2) \leqq 2 + 2d - h/4$.

(ii) $p \equiv 5 \bmod 8$ and $h = h(-p) \not\equiv 0 \bmod 4$;

$$\sharp\, \mathscr{X}_0^+(p)(F_2) \leqq 2 + 2d - h/2$$

or

$$\sharp\, \mathscr{X}_0^+(p)(F_4) \leqq 1 + 4d - (h-2)/4.$$

(iii) $p \equiv -1 \bmod 8$; $\sharp\, \mathscr{X}_0^+(p)(F_2) \leqq 1 + 2d - h$

and

$$\sharp\, \mathscr{X}_0^+(p)(F_4) \leqq 1 + 4d - h\,.$$

(iv) $p \equiv 3 \bmod 8$; $\sharp\, \mathscr{X}_0^+(p)(F_2) \leqq 2 + 2d - 2h$

and

$$\sharp\, \mathscr{X}_0^+(p)(F_4) \leqq 1 + 4d - h\,.$$

Proof. Let $x_1, \cdots, x_s$ (resp. $y_1 = x_1 \otimes \boldsymbol{F}_2, y_2, \cdots, y_{h/2}$ if $p \equiv 1 \bmod 4$; $y_1, y_2, \cdots, y_h$ if $p \equiv -1 \bmod 4$) be the fixed points of $w = w_p$ on $X_0(p)$ (resp. $\mathscr{X}_0(p) \otimes \boldsymbol{F}_2$), see (1.10). Then $g(x_i) = \pm\sqrt{a}$ (see (2.3)). We may assume $g(x_1) = +\sqrt{a} \in H^+$ (see (1.2)). As in the proof of (2.3), $a = 1$, or $a = p$ if $p \equiv 1 \bmod 4$. Set $D = \sum_{i=1}^{s}(x_i)$.

Case $p \equiv 1 \bmod 4$ and $a = 1$. The divisor of $g - 1$ is

$$(g-1) = D + E - \sum (w(x^{\sigma})) - d(0)\,,$$

for a w-invariant $\boldsymbol{Q}$-rational divisor $E > 0$ (see (1.11)). Let $\mathscr{L} = \mathcal{O}(D+E) \otimes \mathcal{O}(\sum (wx^{\sigma}) + d(0))^{\otimes(-1)}$ be the invertible sheaf on $\mathscr{X}_0(p) \otimes \mathcal{O}_K$ for a finite extension K of $\boldsymbol{Q}$. By the upper semicontinuity ([34] (7.7.5), 1), there is a rational function f on $\mathscr{X}_0(p) \otimes \bar{\boldsymbol{F}}_2$ such that

$$(f) = 2\sum_{i=1}^{h/2}(y_i) + E - d(0) - d(\infty) \quad (\neq 0)$$

for the effective divisor $E = E \otimes \boldsymbol{F}_2$ (see (1.10)). The divisor (f) is $\boldsymbol{F}_2$-rational and w-invariant. Then $w^*f = f$ and we may assume that f is defined over $\boldsymbol{F}_2$. Then we get a covering f^+ defined over $\boldsymbol{F}_2$:

$$\mathscr{X}_0^+(p) \otimes \boldsymbol{F}_2 \xrightarrow{f^+} \boldsymbol{P}^1{}_{/\boldsymbol{F}_2}$$

such that $(f^+) = \sum_{1=i}^{h/2}(y_i) + E' - d'(\text{cusp})$ for an effective divisor E' and an integer d', $1 \leqq d' \leqq d$. Here by y_i we denote the images of y_i by the natural morphism of $\mathscr{X}_0(p) \otimes \boldsymbol{F}_2$ to $\mathscr{X}_0^+(p) \otimes \boldsymbol{F}_2$, Then $\sharp\, \mathscr{X}_0^+(p)(\boldsymbol{F}_2) \leqq 3 + 2d - h/2$ if $p \equiv 1 \bmod 8$; $\leqq 2 + 2d - h/2$ if $p \equiv 5 \bmod 8$ (see (1.9)).

Case $p \equiv 1 \bmod 8$ and $a = p$. Let $D = D_1 + D_2$, $D_1 > (x_1)$, be the decomposition into the sum of $\mathrm{Gal}(H/\boldsymbol{Q}(\sqrt{p}))$-orbits D_i of length $h/2$. Then

$$(g-\sqrt{p}) = D_1 + E_1 - \sum (w(x^\sigma)) - d(0)$$
$$(g+\sqrt{p}) = D_2 + E_2 - \sum (w(x^\sigma)) - d(0)\,,$$

for $\boldsymbol{Q}(\sqrt{p})$-rational, w-invariant divisors $E_i>0$. Let $1 \neq \sigma$ be an element of the inertia subgroup of a prime of H lying over 2, and $H^+ = H^{\langle\sigma\rangle}$ the fixed field of $\langle\sigma\rangle$ ($\simeq \boldsymbol{Z}/2\boldsymbol{Z}$). Then $\sigma^* D_i = D_i$ for $i = 1, 2$. There are only two fixed points of w defined over H^+ (see (1.10)). Therefore $D_2 \otimes \boldsymbol{F}_2 = 2\sum'(y_i)$. In the same way as above, we get a rational function f^+ on $\mathscr{X}_0^+(p) \otimes \boldsymbol{F}_2$ defined over $\boldsymbol{F}_2$ such that $(f^+) = \sum'(y_i) + E' - d'(\text{cusp})$, for an effective divisor E' and an integer d', $1 \leqq d' \leqq d$. So $\sharp \mathscr{X}_0^+(p)(\boldsymbol{F}_2) \leqq 2 + 2d - h/4$ (see (1.10)).

Case $p \equiv 5 \bmod 8$ and $a = p$. Let $D = D_1 + D_2$, $D_1 > (x_1)$, be the decomposition into the sum of $\mathrm{Gal}(H/\boldsymbol{Q}(\sqrt{p}))$-orbits D_i of length $h/2$. Here we assume $h = h(-p) \not\equiv 0 \bmod 4$. Then by Lemma (1.11)

$$(g-\sqrt{p}) = 2D_1 + E_1 - \sum (w(x^\sigma)) - d(0)$$
$$(g+\sqrt{p}) = 2D_2 + E_2 - \sum (w(x^\sigma)) - d(0)\,,$$

for $\boldsymbol{Q}(\sqrt{p})$-rational, w-invariant divisors $D_i > 0$. Let $\sigma = \sigma_2$ be the Frobenius element of the rational prime 2. Then $\sigma(D_1) = D_2$, i.e., $(D_1 \otimes \boldsymbol{F}_4)^{(2)} = D_2 \otimes \boldsymbol{F}_4$. By (1.10), we see that $D_1 \otimes \boldsymbol{F}_4 = (y_1) + \sum_{i=2}^{(h-2)/4}(y_i)$, y_1 is the $\boldsymbol{F}_2$-rational fixed point of w (see (1.10)). By the same way as above, we get a rational function f^+ on $\mathscr{X}_0^+(p) \otimes \boldsymbol{F}_4$ such that $(f^+) = (y_1) + 2\sum_{i=2}^{(h-2)/4}(y_i) + E' - d'(\text{cusp})$, for an effective divisor E' and an integer d', $1 \leqq d' \leqq d$ (see (1.10)). Then $\sharp \mathscr{X}_0^+(p)(\boldsymbol{F}_4) \leqq 1 + 4d - (h-2)/4$.

Case $p \equiv -1 \bmod 8$. Set $D_1 = \sum_{i=1}^{h}(x_i)$, $D_2 = \sum_{i=1}^{h}(x_{h+i})$. Then

$$(g-1) = \begin{cases} D + E - \sum (w(x^\sigma)) - d(0) \\ \quad \text{or} \\ 2D_1 + E_1 - \sum (w(x^\sigma)) - d(0) \end{cases}$$

for $\boldsymbol{Q}$-rational, w-invariant divisors $E > 0$, $E_1 > 0$. In both cases, by the same way as above, we get a rational function f^+ on $\mathscr{X}_0^+(p) \otimes \boldsymbol{F}_2$ defined over $\boldsymbol{F}_2$ such that $(f^+) = \sum_{i=1}^{h}(y_i) + E' - d'(\text{cusp})$ for an effective divisor E' and an integer d', $1 \leqq d' \leqq d$. Then $\sharp \mathscr{X}_0^+(p)(\boldsymbol{F}_2) \leqq 1 + 2d - h$ and $\sharp \mathscr{X}_0^+(p)(\boldsymbol{F}_4) \leqq 1 + 4d - h$ (see (1.10)).

Case $p \equiv 3 \bmod 8$. Set $D_1 = \sum_{i=1}^{h}(x_i)$, $D_2 = \sum_{i=1}^{3h}(x_i)$. Then

$$(g-1) = D + E - \sum (w(x^\sigma)) - d(0)$$

or

$$(g+1) = 2D_2 + E_2 - \sum (w(x^\sigma)) - d(0)\,,$$

for $\boldsymbol{Q}$-rational, w-invariant divisors $E>0$, $E_2>0$. In the first case, the same argument as above shows that there is a rational function f^+ on $\mathscr{X}_0^+(p)\otimes \boldsymbol{F}_2$ defined over $\boldsymbol{F}_2$ such that $(f^+) = 2\sum_{i=1}^{h}(y_i) + E' - d'$ (cusp), for an effective divisor E' and an integer d', $1\leqq d'\leqq d$. Then $\sharp\,\mathscr{X}_0^+(p)(\boldsymbol{F}_2)\leqq 2+2d-2h$, and $\sharp\,\mathscr{X}_0^+(p)(\boldsymbol{F}_4)\leqq 1+4d-h$ (see (1.10)). The second case yields better estimates. □

§3. Rational points on $Y_1(p^r)$ defined over quadratic fields

In this section we prove Theorem A in the introduction. Let k be a quadratic field, x a k-rational point on $Y_1(p^r)$ for $r\geqq n' = n''(k,p)$ (see (1.8)). In this case, it is easy to see that $n'(k,p)=n''(k,p)$ (see (1.7), (1.8)). So we can apply the propositions in Section 2. Moreover, we see that we have only to show $n(k,p) < n'(k,p)$ (see Section 0). Applying Proposition (2.3), we get the result of the theorem except for $p=13$, 37, 43, 67, 97, 163 and 193 ($p<300$, $\neq 5, 7, 151, 199, 227, 277$). See table (4.3).

(3.1). *Proof for* $p = 43, 67, 73, 97, 163$ *and* 193. We can apply (2.4), (2.5) and (2.6) in the last section to these cases. Wada [32] shows that the characteristic polynomials of the Hecke operator T_2 on the $\boldsymbol{C}$-vector space of holomorphic cusp forms of weight 2 belonging to $\left\langle \Gamma_0(p), \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}\right\rangle$ for $p<250$. According to his table, we get

Table 4.

p	characteristic polynomial of T_2	$\sharp\,\mathscr{X}_0^+(p)(\boldsymbol{F}_2)$	$\sharp\,\mathscr{X}_0^+(p)(\boldsymbol{F}_4)$	$h(-p)$
43	$x+2$	5	5	1
67	x^2+3x+1	6	6	1
73	x^2+3x+1	6	6	4
97	x^3+4x^2+3x-1	7	7	4
163	$x(x^5+5x^4+3x^3-15x^2-16x+3)$	8	10	1
193	$(x^2+3x+1)\times$ $(x^5+2x^4-5x^3-7x^2+7x+1)$	8	12	4

With these and Proposition (2.6), we get the proof.

(3.2). *Proof for* $p = 13$.

(3.2.1). Rational points on $Y_1(13)$ defined over quadratic fields k.

Let x be a k-rational point on $Y_1(13)$. There is an elliptic curve E defined over k with a k-rational point P of order 13 such that the pair $(E, \pm P)$ represents x ([2] VI Proposition (3.2)). By (1.5), (1.7), we can apply Lemma (1.9). So there is a rational function g (defined over $\boldsymbol{Q}$) on $X_1(13)$ such that

$$(g) = (x) + (x^\sigma) - (0_i) - (0_{i_\sigma}) \ (\neq 0)$$

for $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$ see (2.1). g defines an involution γ of $X_1(13)$ such that $X_1(13)/\langle\gamma\rangle \simeq \boldsymbol{P}^1$. The automorphism $[5] \in \bar{\Gamma}(13)$ (see § 1) of $X_1(13)$ is of degree 2, and $X_1(13)/\langle[5]\rangle \simeq \boldsymbol{P}^1$ (see (1.4)). Hence $\gamma = [5]$, and so $x^\sigma = \gamma(x)$, $0_{i_\sigma} = \gamma(0_i)$ $(\neq 0_i)$. (Note that if a proper smooth curve X defined over a field is hyperelliptic of genus $\geqq 2$, the involution γ satisfying $X/\langle\gamma\rangle \simeq \boldsymbol{P}^1$ is unique.) Then $\{x, x^\sigma = \gamma(x)\}$ defines a $\boldsymbol{Q}$-rational point on $Y_1(13)/\langle\gamma\rangle$ and $0_i \otimes \boldsymbol{F}_q \neq \gamma(0_i) \otimes \boldsymbol{F}_q$ for any rational prime q. There exists an elliptic curve F defined over $\boldsymbol{Q}$ such that the image of $G_{\boldsymbol{Q}} = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ of the Galois representation on $F_{13}(\bar{\boldsymbol{Q}})$ is contained in $\left\{\begin{pmatrix}\langle 5\rangle & * \\ 0 & *\end{pmatrix}\right\}$ $(\subset GL_2(\boldsymbol{F}_{13}))$, and $F \simeq E$ over $\boldsymbol{C}$.

(3.2.2). Suppose that there is a k-rational point x on $Y_1(169)$. There is an elliptic curve E defined over k with a k-rational point P of order 13^2 such that the pair $(E, \pm P)$ represents x ([2] VI Proposition (3.2)). Let x' be a k-rational point on $Y_1(13)$ which is represented by the pair $(E', \pm P')_{/k} \underset{\mathrm{dfn}}{=} (E/\langle 13\cdot P\rangle, \pm P \bmod \langle 13\cdot P\rangle)_{/k}$, and ρ' the Galois representation on $E'_{13}(\bar{k})$. Then

$$\rho'(G_k) \hookrightarrow \left\{\begin{pmatrix}1 & 0 \\ 0 & *\end{pmatrix}\right\}.$$

As was seen in (3.2.1), there is an elliptic curve F defined over $\boldsymbol{Q}$ such that the image of $G_{\boldsymbol{Q}}$ under the Galois representation ρ on $F_{13}(\bar{\boldsymbol{Q}})$ is contained in $\left\{\begin{pmatrix}\langle 5\rangle & * \\ 0 & *\end{pmatrix}\right\}$ and $E' \simeq F$ over $\boldsymbol{C}$. Since F has multiplicative reduction at $q = 2$ (see (1.9)), there exists a quadratic extension K of k over which $E' \simeq F$. Thus

$$\rho(G_K) \hookrightarrow \left\{\begin{pmatrix}1 & 0 \\ 0 & *\end{pmatrix}\right\}.$$

So $\rho(G_Q) \hookrightarrow \left\{\begin{pmatrix}* & 0 \\ 0 & *\end{pmatrix}\right\}$, which contradicts to the fact that $X_{\mathrm{sp.Car}}(13)(\boldsymbol{Q})$

consists of the cusps 0, ∞($; X_{\mathrm{sp.Car}}(p) \simeq X_0(p^2)$, see [7], [21]).

Remarks (3.3). (3.3.1). The modular curve $X = X_1(16)$ is of genus 2 and $\# J_1(16)(\boldsymbol{Q}) = 20$ (see [6]). Let $X \xrightarrow{2} Y \xrightarrow{2} X_0(16)$ be the natural covering, γ the generator of $\mathrm{Gal}(X/Y)$. Then $Y = X/\langle\gamma\rangle \simeq \boldsymbol{P}^1$. Let x be a k-rational point on $Y_1(16)$. If $q = 3$ (resp. $=5$) does not remain prime in k, then $x \otimes \kappa(\mathfrak{q})$ and $x^\sigma \otimes \kappa(\mathfrak{q})$ are 0-cusps for a prime $\mathfrak{q}$ of k lying over q (see (1.9)). Then we get a rational function g on X, defined over $\boldsymbol{Q}$, such that $(g) = (x) + (x^\sigma) - (0_i) - (0_{i_\sigma})$ (see (2.2)). Thus $x^\sigma = \gamma(x)$ and $0_{i_\sigma} = \gamma(0_i)$ $(\neq 0_i)$ (see (3.2)). Therefore if $q = 3$ or 5 ramifies in k, $Y_1(16)(k) = \phi$. Let k be an imaginary quadratic field such that the class number of k is prime to 5 and that the rational prime 2 does not split in k. Then the fact that $\boldsymbol{Z}/5\boldsymbol{Z} \subset J_1(16)(\boldsymbol{Q})$ and the descent ([17] Chapter III) show $\# J_1(16)(k) < \infty$. Moreover, if 3 splits in k or 5 does not remain prime in k, using Mazur's idea "formal immersion" [18], we see $Y_1(16)(k) = \phi$.

(3.3.2). The modular curve $X_1(11)$ is an elliptic curve with conductor (11). The defining equation of $X_1(11)$ is

$$y^2 + y = x^3 - x^2$$

and $X_1(11)(\boldsymbol{Q}) \simeq \boldsymbol{Z}/5\boldsymbol{Z}$ (see [35] p. 82). The numbers of the $\boldsymbol{F}_{q^i}$-rational points for $q = 2, 3$ of $\mathscr{X} = \mathscr{X}_1(11)$ are as follows:

$$\# \mathscr{X}(\boldsymbol{F}_2) = 5, \qquad \# \mathscr{X}(\boldsymbol{F}_4) = 5$$
$$\# \mathscr{X}(\boldsymbol{F}_3) = 5, \qquad \# \mathscr{X}(\boldsymbol{F}_9) = 15$$

(loc. cit.). Therefore $X_1(11)(k)_{\mathrm{tor}} \simeq \boldsymbol{Z}/5\boldsymbol{Z}$ for quadratic fields k. So we have $Y_1(11)(k) = \phi$ if and only if the rank of $X_1(11)(k)$ is 0. For example if k is an imaginary quadratic field such that the class number of k is prime to 5 and the rational prime 11 does not split in k, then $Y_1(11)(k) = \phi$. This can be shown by the descent; see [17] Chapter III.

(3.3.3). By the argument in (3.2.1), we have already known that the k-rational points on $Y_1(13)$ are parametrized by the $\boldsymbol{Q} \cup \{\infty\}$-values of a rational function on $X_1(13)/\langle\gamma\rangle \simeq \boldsymbol{P}^1_{\boldsymbol{Q}}$ of degree 1. If the rational prime $q = 2$ does not split in k or $q = 3$ ramifies in k, then $x \otimes \kappa(\mathfrak{q}) = x^\sigma \otimes \kappa(\mathfrak{q})$ for a k-rational point x on $X_1(13)$ and a prime $\mathfrak{q}$ of k lying over q. Therefore by (3.2.1) in such a case $Y_1(13)(k) = \phi$.

(3.4). *Proof for* $p = 37$. Let $X_1(37) \xrightarrow{9} X \xrightarrow{2} X_0(37)$ be the natural coverings, $J = J(X)$ the jacobian variety of X and $A = \mathrm{Coker}\,(J_0(37) \to J)$

(see (1.4)). Then A has everywhere good reduction over $\boldsymbol{Q}(\sqrt{37})$ ([2] V).

LEMMA (3.4.1). *Let p be a prime number congruent to* $1 \bmod 4$, $X_1(p) \xrightarrow{(p-1)/4} X \xrightarrow{2} X_0(p)$ *the natural coverings, and $J = J(X)$ the jacobian variety of X. If there is a prime factor of $(1/4)B_{2,(\frac{p}{})}$ which is prime to the class number of $\boldsymbol{Q}(\sqrt{p})$, then there is a factor $(\ /\boldsymbol{Q}(\sqrt{p}))$ of* Coker $(J_0(p) \to J)$ *with finite Mordell-Weil group $(\ /\boldsymbol{Q}(\sqrt{p}))$. Here $B_{2,(\frac{p}{})}$ is the (second) generalized Bernoulli number associated to the quadratic residue symbol $(\frac{p}{})$ (see* [13]).

Proof. Let $0', 0''$ be the 0-cusps of X. The order of $\mathrm{cl}((0') - (0''))$ is $(1/4)B_{2,(\frac{p}{})}$ [11]. Let q be a prime number which is prime to the class number of $\boldsymbol{Q}(\sqrt{p})$ and divides $(1/4)B_{2,(\frac{p}{})}$. Let B be a quotient $(\ /\boldsymbol{Q})$ of Coker $(J_0(p) \to J)$ such that B is $\boldsymbol{Q}$-simple and the order of the image $\mathrm{cl}((0') - (0''))$ on B is divisible by q, then $\boldsymbol{Z}/q\boldsymbol{Z} \subset B$. B has everywhere good reduction over $\boldsymbol{Q}(\sqrt{p})$, see [2] V, and is isogenous to a product $C \times C^{\sigma}$ of an abelian variety C over $\boldsymbol{Q}(\sqrt{p})$. Further C is isogenous over $\boldsymbol{Q}(\sqrt{p})$ to C^{σ} for $1 \neq \sigma \in \mathrm{Gal}(\boldsymbol{Q}(\sqrt{p})/\boldsymbol{Q})$, see [31] Chapter 7. Then B is isogenous over $\boldsymbol{Q}$ to $\mathrm{Re}_{\boldsymbol{Q}(\sqrt{p})/\boldsymbol{Q}}(C)$, where $\mathrm{Re}_{\boldsymbol{Q}(\sqrt{p})/\boldsymbol{Q}}$ is the restriction of scalars (see [4], [33]). Hence $\mathrm{rk}\, B(\boldsymbol{Q}) = \mathrm{rk}\, C(\boldsymbol{Q}(\sqrt{p}))$. Applying the descent to $C(\ /\boldsymbol{Q}(\sqrt{p}))$ (see [17] Chapter III), we have $\sharp\, C(\boldsymbol{Q}(\sqrt{p})) < \infty$.$\square$

LEMMA (3.4.2). *Let $A =$* Coker $(J_0(37) \to J)$ *as above. Then $A(\boldsymbol{Q}) \simeq \boldsymbol{Z}/5\boldsymbol{Z}$.*

Proof. $(1/4)B_{2,(\frac{37}{})} = 5$ and the class number of $\boldsymbol{Q}(\sqrt{37}) = 1$. A is isogenous over $\boldsymbol{Q}(\sqrt{37})$ to a product of two elliptic curves, so that A is $\boldsymbol{Q}$-simple. Using the table of the characteristic polynomials of the Hecke operators on the $\boldsymbol{C}$-vector space $S_2(\Gamma_0(37), (\frac{37}{}))$ of the holomorphic cusp forms of weight 2 with the neben character $(\frac{37}{})$ belonging to $\Gamma_0(37)$, p. 207 of [31], we see that $\sharp\, A(\boldsymbol{Q})_{\mathrm{tor}} = 5$. Then Lemma (3.4.1) is applied to yield $A(\boldsymbol{Q}) \simeq \boldsymbol{Z}/5\boldsymbol{Z}$. $\square$

Suppose that there is a k-rational point x on $Y_1(37)$. Consider the $\boldsymbol{Q}$-rational section $i(x) = \mathrm{cl}((x) + (x^{\sigma}) - (0_i) - (0_{i_\sigma}))$ of A, where $1 \neq \sigma \in \mathrm{Gal}(k/\boldsymbol{Q})$, see Section 2. Then $i(x) \otimes \boldsymbol{F}_q = 0$ for $q = 2, 3$ and 5 (see (1.9)), so we get $i(x) = 0$, see (3.4.2). There is a rational function g on X (defined over $\boldsymbol{Q}$) such that $(g) = (x) + (x^{\sigma}) + (\gamma(0_i)) + (\gamma(0_{i_\sigma})) - (\gamma(x)) - (\gamma(x^{\sigma})) - (0_i) - (0_{i_\sigma})$, where $1 \neq \sigma \in \mathrm{Aut}(X/X_0(37))$, see (2.1′).

Claim. $x \neq \gamma(x), \neq \gamma(x^\sigma)$.

Proof. If $x = \gamma(x)$, then x is a fixed point of γ with the modular invariant $j(x) = 1728$. This contradicts that $x \otimes \kappa(\mathfrak{q}) = 0_i \otimes \kappa(\mathfrak{q})$ for the primes $\mathfrak{q} \mid 2$ of k. If $x = \gamma(x^\sigma)$, then $\{x, x^\sigma = \gamma(x)\}$ defines a $\boldsymbol{Q}$-rational point on $(Y_0(37))$. But we know that the non-cuspidal $\boldsymbol{Q}$-rational points on $X_0(37)$ have everywhere potentially good reduction, [19] Section 5, p. 32. $\square$

Let $\mathscr{X}$ be the normalization of the projective j-line $\mathscr{X}_0(1) \simeq \boldsymbol{P}^1_{\boldsymbol{Z}}$ in X. Then $\mathscr{X}$ is smooth over $\boldsymbol{Z}[1/37]$, see [2].

Case $0_i \neq 0_{i_\sigma}$. In this case $\gamma(0_i) = 0_i$ and $(g) = (x) + (x^\sigma) - (\gamma(x)) - (\gamma(x^\sigma))$ $(\neq 0)$. Let $E_\eta = (x) + (x^\sigma)$ and E be the flat closure of E_η on $\mathscr{X} \otimes \boldsymbol{Z}_2$. Then $E \otimes \boldsymbol{F}_2 = (0_i \otimes \boldsymbol{F}_2) + (\gamma(0_i \otimes \boldsymbol{F}_2))$. The argument similar to Lemma (1.11) shows that there is a rational function on $\mathscr{X}_0(37) \otimes \boldsymbol{F}_2$ of degree one. This is a contradiction.

Case $0_i = 0_{i_\sigma}$. Let $E_\eta = (x) + (x^\sigma) + 2(\gamma(0_i))$ and E be the flat closure of E_η on $\mathscr{X} \otimes \boldsymbol{Z}_2$. Then $E \otimes \boldsymbol{F}_2 = 2(0_i \otimes \boldsymbol{F}_2) + 2(\gamma(0_i \otimes \boldsymbol{F}_2))$. The argument as in Lemma (1.11) shows that there is a double covering $g' : \mathscr{X}_0(37) \otimes \boldsymbol{F}_2 \to \boldsymbol{P}^1_{\boldsymbol{F}_2}$, such that $(g')_\infty = 2(0 \otimes \boldsymbol{F}_2)$. Then $0 = 0 \otimes \boldsymbol{F}_2$ is a fixed point of the (unique) hyperelliptic involution $\bar{S}$ of $\mathscr{X}_0(37) \otimes \boldsymbol{F}_2$. The hyperelliptic involution S of $X_0(37)$ sends the cusp $0 = \binom{0}{1}$ to a non cuspidal $\boldsymbol{Q}$-rational point, see [19] Section 5. As noted as before, $S(0) \otimes \boldsymbol{F}_2$ is not a cusp (see loc. cit.), so that $\bar{S} = S \otimes \boldsymbol{F}_2$ does not fix $0 = 0 \otimes \boldsymbol{F}_2$. Thus we get a contradiction.

For an imaginary quadratic field k, $Y_1(p)(k) = \phi$ if a rational prime p remains prime in k, except for finitely many p ([18] § 4). For a real quadratic field k, we use Mazur's idea "formal immersion" (loc. cit.) to show the following. $\square$

PROPOSITION (3.5). *Let $p \geqq 17$ be a rational prime congruent to* $1 \bmod 4$. *If there exists a prime factor of* $(1/4)B_{2,\left(\frac{p}{\cdot}\right)}$ *which is prime to the class number of* $\boldsymbol{Q}(\sqrt{p})$, *then* $Y_1(p)(\boldsymbol{Q}(\sqrt{p})) = \phi$.

Proof. Let $X_1(p) \xrightarrow{(p-1)/4} X \xrightarrow{2} X_0(p)$ be the natural coverings, $J = J(X)$ the jacobian variety of X, and $A = \operatorname{Coker}(J_0(p) \to J)$. Then by Lemma (3.4.1), there exists a quotient B ($/\boldsymbol{Q}$) of A with finite Mordell-Weil group over $\boldsymbol{Q}(\sqrt{p})$. As $p > (1+3)^2$, Lemma (1.8) is applied for $q = 3$. The rest owes to [18] Section 4. $\square$

COROLLARY (3.6). *Let p be a prime number congruent to* $1 \bmod 8$. *Then* $Y_1(p)(\boldsymbol{Q}(\sqrt{p})) = \phi$.

Proof. $(1/4)B_{2,\left(\frac{p}{\cdot}\right)} \equiv 0 \bmod 2$ (see, e.g. [17] Chapter II § 12). □

§ 4. Further results

Let k be an algebraic number field of degree d, $n = n(k, p)$ and $n'' = n''(k, p)$ as in Section 1 (1.8). Applying propositions in Section 2, we can estimate n in some cases.

THEOREM (4.1). *Let k be any cubic field. Then*

$$n(k, 2) \leqq 5,$$
$$n(k, 3) = 2,$$
$$n(k, 17) \leqq 1\,.$$

For $p = 19, 23, 41, 47, 59, 71$ *and the primes* $p \leqq 79, \neq 97, \neq 109$, *satisfying* $\# J_0^-(p)(\boldsymbol{Q}) < \infty$, *we have* $n(k, p) = 0$.

Proof. For $p < 300$, the result follows from Proposition (2.3), (1.4), (1.8), Lemma (1.12), except for $p = 19, 23, 157, 163, 193$, (277) (see table (4.3)). Using Corollary (2.5), we get the result for $p = 157, 163, 193$ (see (3.1)). The characteristic polynomial of the Hecke operator T_2 on $S_2\left(\left\langle \Gamma_0(157), \begin{bmatrix} 0 & -1 \\ 157 & 0 \end{bmatrix} \right\rangle\right)$ (see (3.1)) is $x^5 + 5x^4 + 5x^3 - 6x^2 - 7x + 1$ (see [32]). Thus $\# \mathscr{X}_0^+(157)(\boldsymbol{F}_2) = 8$ and $\# \mathscr{X}_0^+(157)(\boldsymbol{F}_4) = 10$. For $p = 19, 23$, if there exists a k-rational point x on $Y_1(p)$, then there exists a rational function g on $X = X_1(p)$, defined over $\boldsymbol{Q}$, such that $(g) = \sum (x^\sigma) - \sum (0_{i_\sigma})$, see (1.9), (2.1)). For $p = 23$, we know $\# \mathscr{X}_1(23)(\boldsymbol{F}_2) = 11$ ([9] § 4). Using the upper semicontinuity (see [34] (7.7.1)1), we get a contradiction.

(4.1.1) *Proof for* $p = 19$. Let $1 \neq \gamma \in \mathrm{Aut}\,(X/Y)$ (see (1.4)). If $(\gamma^* g) = (g)$, then $\gamma(x) = x^\tau$ for a $\tau \in \mathrm{Isom}_{\boldsymbol{Q}}(k, \bar{\boldsymbol{Q}})$. Then x is a fixed point if $\tau = 1$, or $\{x^\sigma\}_\sigma = \{\gamma^i(x)\}_{i=0,1,2}$ if $\tau \neq 1$. The fixed points of γ have the modular invariant $j = 0$ (see (1.1), (1.4)). So by Lemma (1.9) the first case above does not occur. In the second case, $\{x^\sigma\}_\sigma$ defines a $\boldsymbol{Q}$-rational point on Y, hence on $X_0(19)$. But the $\boldsymbol{Q}$-rational points on $X_0(19)$ are the cusps and the points represented by the elliptic curve $\boldsymbol{C}/\boldsymbol{Z}[(1 + \sqrt{-19})/2]$. So $(\gamma^* g) \neq (g)$ is shown. Let $D = \sum_{i=1}^{6} (x_i)$ be the $\boldsymbol{Q}$-rational divisor of $X_1(19)$, where x_i are the fixed points of γ on $X_1(19)$ (see (1.4)). Then by Lemma (1.11), $1/(\gamma^* g/g - 1) \in H^0(X_1(19), \mathcal{O}(D))$. The Riemann-Roch theorem and a theorem of Clifford (see below) then show $\dim_{\boldsymbol{Q}} H^0(X_1(19), \mathcal{O}(D)) < 1 + 3$.

(4.1.2) THEOREM (Clifford; see e.g. [5]). *Let X be a proper smooth curve $/\boldsymbol{C}$ of genus $\geqq 1$, E an effective divisor such that $\dim_{\boldsymbol{C}} H^0(X, \mathcal{O}(K - E)) > 0$, where K is the canonical divisor. Then*

$$\dim_{\boldsymbol{C}} H^0(X, \mathcal{O}(E)) \leqq 1 + \frac{1}{2} \deg (E) .$$

The equality holds if and only if $E = 0$, $E \sim K$ or $E \sim \pi^* F$ if X is hyperelliptic, where $\pi: X \to \boldsymbol{P}^1$ is a double covering and F is a divisor of $\boldsymbol{P}^1$.

It is easy to see the following.

(4.1.3). Let X be a proper smooth curve and γ an automorphism of X of degree m ($\geqq 1$) defined over $\boldsymbol{Q}$. Let E be an effective, $\boldsymbol{Q}$-rational divisor of X such that $\gamma^* E = E$ and γ^* acts faithfully on $H^0(X, \mathcal{O}(E))$. Then $\dim_{\boldsymbol{Q}} H^0(X, \mathcal{O}(E)) \geqq 1 + \varphi(m)$, where $\varphi(m)$ is the Euler number of m.

Let $\tilde{\gamma}$ be the generator of $\bar{\Gamma}_0(19) = \Gamma_0(19)/\pm \Gamma_1(19)$ (see (1.4)), which is of order 9. Then D is $\tilde{\gamma}^*$-invariant and $H^0(X_1(19), \mathcal{O}(D))^{\langle \tilde{\gamma}^* \rangle} = \boldsymbol{Q} \cdot 1$. If $\dim_{\boldsymbol{Q}} H^0(X_1(19), \mathcal{O}(D)) \geqq 2$, then $\tilde{\gamma}^*$ acts faithfully on $H^0(X_1(19), \mathcal{O}(D))$ and $\dim_{\boldsymbol{Q}} H^0(X_1(19), \mathcal{O}(D)) \geqq 1 + \varphi(9) = 7$ by (4.1.3). This is a contradiction.

(4.1.4) *Proof for $p > 300$* (e.g. $p = 383, 419, 429, 491$, cf. [17] p. 151]) (and for $p = 277$ if $\# J_0^-(277)(\boldsymbol{Q}) < \infty$). By Corollary (2.5), if $Y_1(p)(k) \neq \phi$, then $\# \mathscr{X}_0(p)(\boldsymbol{F}_4) \leqq 2(1 + 4 \cdot 3) - s \leqq 24$. But we know $\# \mathscr{X}_0(p)(\boldsymbol{F}_4) \geqq 2 + (p + 1)/12$ (see [24] Theorem 3). Hence $Y_1(p)(k) = \phi$ for $p > 300$ (, and p $= 277$) if $\# J_0^-(p) < \infty$. □

Remark (4.2). The above method used for $(p, d) = (19, 3)$ can be applied to some other cases. For example, it gives an alternating proof for $(p, d) = (5, 2)$. In this case, under the notation in (4.1.1), (4.1.2) and the Riemann-Roch theorem show $\dim_{\boldsymbol{Q}} H^0(X, \mathcal{O}(D)) \leqq 1 + 2$. But if $\dim_{\boldsymbol{Q}} H^0(X, \mathcal{O}(D)) \geqq 2$, then it must be $\geqq 1 + 4$ by (4.1.3).

(4.3). Table for $p < 300$.

Let k be an algebraic number field of degree d. For the pairs (p, d) in the following table, we get $n(k, p) < n''(k, p)$. See (1.4), (1.8), [32], [35] table 5, pp. 135–141.

Table 5.

p	d	$s(p)$	$h(-p)$ (for $p \geqq 23$)
2	2, 3	8	
3	2, 3, 4, 5	12	
5	2	4	
7	2	2	
11	2	6	
13	2	6	
17	2, 3	8	
19	2, 3	8	
23	2, 3	6	3
29	2	6	6
31	2	6	3
37	2	2	2
41	2, 3	8	8
43	2	4	1
47	2, 3, 4	10	5
53	2	6	6
59	2, 3, 4, 5	12	3
61	2	6	6
67	2	4	1
71	2, 3, 4, 5, 6	14	7
73	2	4	4
79	2, 3, 4	10	5
83	2, 3, 4, 5	12	3
89	2, 3, 4, 5	12	12
97	2	4	4
101	2, 3, 4, 5, 6	14	14
103	2, 3, 4	10	5
107	2, 3, 4, 5	12	3
109	2	6	6
113	2, 3	8	8
127	2, 3, 4	10	5
131	2, 3, $\cdots$, 9	20	5
137	2, 3	8	8
139	2, 3, 4, 5	12	3
149	2, 3, 4, 5, 6	14	14
151	?	14	7
157	2, 3	6	6
163	2, 3	4	1

Table 5. Continued

p	d	$s(p)$	$h(-p)$ (for $p \geqq 23$)
167	$2, 3, \cdots, 10$	22	11
173	$2, 3, 4, 5, 6$	14	14
179	$2, 3, \cdots, 9$	20	5
181	$2, 3, 4$	10	10
191	$2, 3, \cdots, 12$	26	13
193	$2, 3$	4	4
197	$2, 3, 4$	10	10
199	?	18	9
211	$2, 3, 4, 5$	12	3
223	$2, 3, 4, 5, 6$	14	7
227	?	20	5
229	$2, 3, 4$	10	10
233	$2, 3, 4, 5$	12	12
239	$2, 3, \cdots, 14$	30	15
241	$2, 3, 4, 5$	12	12
251	$2, 3, \cdots, 13$	28	7
257	$2, 3, 4, 5, 6, 7$	16	16
263	$2, 3, \cdots, 12$	26	13
269	$2, 3, \cdots, 10$	22	22
271	$2, 3, \cdots, 10$	22	11
277	?	6	6
281	$2, 3, \cdots, 9$	20	20
283	$2, 3, 4, 5$	12	3
293	$2, 3, \cdots, 8$	18	18

References

[1] Z. I. Borevich, I. R. Shafarevich, Number theory, Academic Press, New York and London (1966).

[2] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, Proceedings of the International Summer School on Modular functions of one variable, vol. II, Lecture Notes in Math., **349**, Springer-Verlag, Berlin-Heiderberg-New York (1973).

[3] B. H. Gross, Arithmetic on elliptic curves with complex multiplication, Lecture Notes in Math., **776**, Springer-Verlag, Berlin-Heiderberg-New York (1980).

[4] A. Grothendieck, Fondements de la géométrie algébrique, Sém. Bourbaki, 1957–1962.

[5] R. Hartshorne, Algebraic Geometry, Springer-Verlag, New York (1977).

[6] M. A. Kenku, Certain torsion points on elliptic curves defined over quadratic fields, J. London Math. Soc., (2) **19** (1979), 233–240.

[7] ——, The modular curve $X_0(169)$ and rational isogeny, J. London Math. Soc., (2) **22** (1980), 239–244.

[8] ——, On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$, J. London Math. Soc., (2) **23** (1981), 415–427.
[9] ——, Rational torsion points on elliptic curves defined over quadratic fields, to appear.
[10] D. Kubert, Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc., (3) **33** (1976), 193–237.
[11] D. Kubert, S. Lang, Units in the modular function fields I, II, III, Math. Ann., **218** (1975), 67–96, 175–189, 273–285.
[12] S. Lang, Elliptic Functions, Addison-Wesley, Reading Math. (1973).
[13] ——, Cyclotomic Fields, Addison-Wesley, Reading Math. (1973).
[14] Yu. I. Manin, The p-torsion of elliptic curves is uniformly bounded, Math. USSR-Izv., **3** (1969), 433–438.
[15] ——, Parabolic points and zeta functions of modular curves, Math. USSR-Izv., **6** (1972), 19–64.
[16] B. Mazur, Rational points on modular curves, Proceedings of Conference on Modular Functions held in Bonn, Lecture Notes in Math., **601**, Springer-Verlag, Berlin-Heiderberg-New York (1977).
[17] ——, Modular curves and the Eisenstein ideal, I.H.E.S. Publ. Math., **47** (1977), 33–186.
[18] ——, Rational isogenies of prime degree, Invent. Math., **44** (1978), 129–162.
[19] ——, P. Swinnerton-Dyer, Arithmetic of Weil curves, Invent. Math., **25** (1974), 1–61.
[20] ——, J. Tate, Points of order 13 on elliptic curves, Invent. Math., **22** (1973), 41–49.
[21] J. F. Mestre, Points rationnels de la courbe modulaire $X_0(169)$, Ann. Inst. Fourier, **30**, 2 (1980), 17–27.
[22] A. Ogg, Rational points on certain elliptic modular curves, Proc. Symposia in Pure Math. XXIV, AMS (1973), 221–231.
[23] ——, Hyperelliptic modular curves, Bull. Soc. Math. France, **102** (1974), 449–462.
[24] ——, Diophantine equation and modular forms, Bull. Amer. Math. Soc., **81** (1975), 14–27.
[25] F. Oort, J. Tate, Group schemes of prime order, Ann. Sci. Ecole Norm. Sup. série 4,**3** (1970), 1–21.
[26] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$, Bull. Soc. Math. France, **102** (1974), 241–280.
[27] K. A. Ribet, Endomorphisms of semi-stable abelian varieties over number fields, Ann. of Math., **101** (1975), 555–562.
[28] J. P. Serre, p-torsion des courbes elliptiques (d'àpres Y. Manin), Sém. Bourbaki 1969/70 pp. 281–294, Lecture Notes in Math., **180**, Springer-Verlag, Berlin-Heiderberg-New York (1971).
[29] J. P. Serre, Corps Locaux, Publ. Inst. de Math. de Univ. de Nancago Hermann, Paris (1968).
[30] G. Shimura, On elliptic curves with complex multiplication as factors of jacobians of modular function fields, Nagoya Math. J., **43** (1971), 199–208.
[31] ——, Introduction to the Arithmetic theory of Automorphic Functions, Publ. Math. Soc. Japan 11, Iwanami Shoten, Tokyo-Princeton Univ. Press, Princeton, N.J.
[32] H. Wada, A table of Hecke operators II, Proc. Japan Acad., **49** (1973) 380–384.
[33] A. Weil, Adèles and Algebraic Groups, Lecture Notes, Inst. for Advanced Study, Princeton, N.J.

[34] Éléments de Géométrie Algébrique III (par A. Grothendieck), I.H.E.S. Publ. Math., **17** (1963).
[35] Modular Functions of One Variable IV (Ed. By B. J. Birch and W. Kuyk), Lecture Notes in Math., **476**, Springer-Verlag, Berlin-Heiderberg-New York (1975).

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