COMPOSITIO MATHEMATICA

M. A. KENKU
FUMIYUKI MOMOSE

Automorphism groups of the modular curves $X_0(N)$

Compositio Mathematica, tome 65, nº 1 (1988), p. 51-80
<http://www.numdam.org/item?id=CM_1988__65_1_51_0>

Compositio Mathematica 65: 51–80 (1988)

Automorphism groups of the modular curves $X_0(N)$

M.A. KENKU[1] & FUMIYUKI MOMOSE[2,*]
[1]*Department of Mathematics, Faculty of Science, University of Lagos, Lagos, Nigeria;*
[2]*Department of Mathematics, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112, Japan (*author for correspondence)*

Received 15 December 1986; accepted in revised form 31 July 1987

Let $N \geqslant 1$ be an integer and $X_0(N)$ be the modular curve $/\mathbb{Q}$ which corresponds to the modular group $\Gamma_0(N)$. We here discuss the group Aut $X_0(N)$ of automorphisms of $X_0(N) \otimes \mathbb{C}$ (for curves of genus $g_0(N) \geqslant 2$). Ogg [23] determined them for square free integers N. The determination of Aut $X_0(N)$ has applications to study on the rational points on some modular curves, e.g., [10, 19–21]. Let $\Gamma_0^*(N)$ be the normalization of $\Gamma_0(N)/\pm 1$ in $\mathrm{PGL}_2^+(\mathbb{Q})$, and put $B_0(N) = \Gamma_0^*(N)/\Gamma_0(N)$ ($\subset$ Aut $X_0(N)$), which is determined in [1] §4. The known example such that Aut $X_0(N) \neq B_0(N)$ is $X_0(37)$ [16] §5 [22]. The modular curve $X_0(37)$ has the hyperelliptic involution which sends the cusps to non cuspidal $\mathbb{Q}$-rational points, and Aut $X_0(37) \simeq (\mathbb{Z}/2\mathbb{Z})^2$, $B_0(37) \simeq \mathbb{Z}/2\mathbb{Z}$. Our result is the following.

THEOREM 0.1. *For $X_0(N)$ with $g_0(N) \geqslant 2$,* Aut $X_0(N) = B_0(N)$, *provided $N \neq 37, 63$.*

We have not determined Aut $X_0(63)$. The index of $B_0(63)$ in Aut $X_0(63)$ is one or two, see proposition 2.18. The automorphisms of $X_0(N)$ are not defined over $\mathbb{Q}$, in the general case, and it is not easy to get the minimal models of $X_0(N)$ over the base Spec $\mathcal{O}_K$ for finite extensions K of $\mathbb{Q}$. By the facts as above, the proof of the above theorem becomes complicated. In the first place, using the description of the ring End $J_0(N)$ ($\otimes\mathbb{Q}$) of endomorphisms of the jacobian variety $J_0(N)$ of $X_0(N)$ [18, 29], we show that the automorphisms of $X_0(N)$ are defined over the composite $k(N)$ of quadratic fields with discriminant D such that $D^2 | N$, except for $N = 2^8, 2^9, 2^2 3^3, 2^3 3^3$, see corollary 1.11, remark 1.12. For the sake of the simplicity, we here treat the cases for $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3, 37$. Using corollary 2.5 [20], we show that automorphisms of $X_0(N)$ are defined over a subfield $F(N)$ which contained in $k(N) \cap \mathbb{Q}(\zeta_8, \sqrt{-3}, \sqrt{5}, \sqrt{-7})$. In the second place, for an automorphism u of $X_0(N)$, we show that if $u(\mathbf{0})$ or $u(\infty)$ is a cusp, then u belongs to $B_0(N)$, see corollary 2.4, where $\mathbf{0}$ and ∞ are the $\mathbb{Q}$-rational cusps cf. §1. Further we show that if u is defined over $\mathbb{Q}$, then u belongs to $B_0(N)$, see proposition 2.8. Now assume that $u(\mathbf{0})$ and $u(\infty)$ are not cusps and that $F(N) \neq \mathbb{Q}$. Let $l = l(N)$ be the least prime number not dividing N, and $D = D_l = (l+1)(u(\mathbf{0})) + (T_l u^\sigma(\infty)) - (l+1)(u(\infty)) - (T_l u^\sigma(\mathbf{0}))$ be the divisor of $X_0(N)$, where $\sigma = \sigma_l$ is the Frobenius element of the rational prime l and T_l is the Hecke operator associating to l. Under the assumption on u as above, we show that $0 \neq D \sim 0$ (linearly equivalent), and that $w_N^*(D) \neq D$, where w_N is the fundamental involution of $X_0(N)$, see lemma 2.7, 2.10. Let S_N be the number of the fixed points of w_N, which can be easily described, see (1.16). Then we get the inequality that $S_N \leqslant 4(l+1)$, see corollary 2.11. Let p_n be the n-th prime number. Then using the estimate $p_n < 1.4 \times n \log n$ for $n \geqslant 4$ [30] theorem 3, we get $l \geqslant 19$, see lemma 2.13. In the last place, applying an Ogg's idea in [22, 23], we get Aut $X_0(N) = B_0(N)$, except for some integers, see lemma 2.14, 2.15. For the remaining cases, because of the finiteness of the cuspidal subgroup of $J_0(N)$ [13], we can apply lemma 2.16. We apply the other methods to the cases for $N = 50, 75, 125, 175, 108, 117$ and 63.

The authors thank L. Murata who informed us the estimate of prime numbers [30].

NOTATION. For a prime number p, $\mathbb{Q}_p^{ur}$ denotes the maximal unramified extension of $\mathbb{Q}_p$, and $\mathbf{W}(\bar{\mathbb{F}}_p)$ is the ring of Witt vectors with coefficients in $\bar{\mathbb{F}}_p$. For a finite extension K of $\mathbb{Q}$, $\mathbb{Q}_p$ of $\mathbb{Q}_p^{ur}$, $\mathcal{O}_K$ denotes the ring of integers of K. For an abelian variety A defined over K, $A_{/\mathcal{O}_K}$ denotes the Néron model of A over the base Spec $\mathcal{O}_K$. For a commutative ring R, $\mu_n(R)$ denotes the group of n-th roots of unity belonging to R.

§1. Preliminaries

Let $N \geqslant 1$ be an integer, and $X_0(N)$ be the modular curve $/\mathbb{Q}$ which corresponds to the modular group $\Gamma_0(N)$. Let $\mathcal{X}_0(N)$ denote the normalization of the projective j-line $\mathcal{X}_0(1) \simeq \mathbb{P}^1_{\mathbb{Z}}$ in the function field of $X_0(N)$. For a positive divisor M of N prime to N/M, denotes the canonical involution of $\mathcal{X}_0(N)$ which is defined by $(E, A) \mapsto (E/A_M, (E_M + A)/A_M)$ (at the generic fibre), where A is a cyclic subgroup of order N and A_M is the cyclic subgroup of A of order M. Let $\mathfrak{H}$ be the complex upper half plane $\{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}$. Under the canonical identification of $X_0(N) \otimes \mathbb{C}$ with $\Gamma_0(N)\backslash\mathfrak{H} \cup \{i\infty, \mathbb{Q}\}$, w_M is represented by a matrix $\begin{pmatrix} Ma & b \\ Nc & Md \end{pmatrix}$ for integers a, b, c and d with $M^2ad - Nbc = M$. For a fixed rational prime p, and a subscheme Y of $\mathcal{X}_0(N)$, Y^h denotes the open subscheme of Y obtained by excluding the supersingular points on $Y \otimes \mathbb{F}_p$. For a prime divisor p with

$p^r \| N$, the special fibre $\mathscr{X}_0(N) \otimes \mathbb{F}_p$ has $r + 1$ irreducible components $E_0, E_1, \ldots, E_r$. We choose $Z' = E_0$ (resp. $Z = E_r$) so that Z'^h (resp. Z^h) is the coarse moduli space $/\mathbb{F}_p$ of the isomorphism classes of the generalized elliptic curves E with a cyclic subgroup A isomorphic to $\mathbb{Z}/N\mathbb{Z}$ (resp. μ_N), locally for the étale topology [4]V, VI. then Z'^h and Z^h are smooth over spec $\mathbb{F}_p$. For a prime number p with $p \| N$, $\mathscr{X}_0(N) \otimes \mathbb{F}_p$ is reduced, and Z and Z' intersect transversally at the supersingular points on $\mathscr{X}_0(N) \otimes \mathbb{F}_p$. For a supersingular points x on $\mathscr{X}_0(N) \otimes \mathbb{F}_p$ with $p \| N$, let y be the image of x under the natural morphism of $\mathscr{X}_0(N) \mapsto \mathscr{X}_0(N/p)$: $(E, A) \mapsto (E, A_{M/p})$, and (F, B) be an object associating to y. Then the completion of the local ring $\mathcal{O}_{\mathscr{X}_0(N),x} \otimes \mathbf{W}(\bar{\mathbb{F}}_p)$ along the section x is isomorphic to $\mathbf{W}(\bar{\mathbb{F}}_p)[[X, Y]]/(XY - p^m)$ for $m = \frac{1}{2}|\mathrm{Aut}\,(F, B)|$ [4]VI (6.9). Let $\mathbf{0} = \binom{0}{1}$ and $\infty = \binom{1}{0}$ denote the $\mathbb{Q}$-rational cusps of $\mathscr{X}_0(N)$ which are represented by $(\mathbb{G}_m \times \mathbb{Z}/N\mathbb{Z}, \mathbb{Z}/N\mathbb{Z})$ and $(\mathbb{G}_m, \mu_N)$, respectively.

(1.1) Let $S_2(\Gamma_0(N))$ be the $\mathbb{C}$-vector space of holomorphic cusp forms of weight 2 belonging to $\Gamma_0(N)$. Then $S_2(\Gamma_0(N))$ is spanned by the eigen forms of the Hecke ring $\mathbb{Q}[T_m]_{(m,N)=1}$ e.g., [1] [33] Chap. 3 (3.5). Let $f = \Sigma\, a_n q^n$, $a_1 = 1$, be a normalized new form belonging to $S_2(\Gamma_0(N))$ cf. [1]. Put $K_f = \mathbb{Q}(\{a_n\}_{n \geqslant 1})$, which is a totally real algebraic number field of finite degree, see loc.cit. . For each isomorphism σ of K_f into $\mathbb{C}$, put $\sigma f = \Sigma\, a_n^\sigma q^n$, which is also a normalized new form belonging to $S_2(\Gamma_0(N))$ [33] Chap. 7 (7.9). For a positive divisor d of $N/$(level of f), put $f|e_d = \Sigma\, a_n q^{dn}$, which belongs to $S_2(\Gamma_0(N))$ and has the eigen values a_n of T_n for integers n prime to N [1]. The set $\{f|e_d\}_{f,d}$ becomes a basis of $S_2(\Gamma_0(N))$, where f runs over the set of all the normalized new forms belonging to $S_2(\Gamma_0(N))$, and d are the positive divisors of $N/$(level of f). To the set $\{\sigma f\}$, $\sigma \in \mathrm{Isom}\,(K_f, \mathbb{C})$, of the normalized new forms, there corresponds a factor $J_{\{\sigma f\}}$ $(/\mathbb{Q})$ of the jacobian variety $J_0(N)$ of $X_0(N)$ [35] §4. Let $m(f)$ $(=m(\sigma f))$ be the number of the positive divisors of $N/$(level of f). Then $J_0(N)$ is isogenous over $\mathbb{Q}$ to the product of the abelian varieties

$$\prod_{\{\sigma f\}} J_{\{\sigma f\}}^{m(f)},$$

where σf runs over the set of the normalized new forms belonging to $S_2(\Gamma_0(N))$. For each normalized new form f belonging to $S_2(\Gamma_0(N))$, let $V(f)$ be the $\mathbb{C}$-vector space spanned by $\{f|e_d\}$, $d|N/$(level of f). Then $S_2(\Gamma_0(N))$ is decomposed into the direct sum $\oplus_f V(f)$ of the eigen spaces $V(f)$ of the Hecke ring $\mathbb{Q}[T_m]_{(m,N)=1}$, where f runs over the set of the normalized new forms belonging to $S_2(\Gamma_0(N))$.

Let $\mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field with discriminant D. Let λ be a Hecke character of $\mathbb{Q}(\sqrt{-D})$ with conductor $\mathfrak{r}$ which satisfies the following conditions:

$$\begin{cases} \lambda((\alpha)) = \alpha & \text{for} \quad \alpha \in \mathbb{Q}(\sqrt{-D})^\times \quad \text{with } \alpha \equiv 1 \bmod^\times \mathfrak{r}, \\ \lambda((a)) = \left(\dfrac{-D}{a}\right) a & \text{for} \quad a \in \mathbb{Z} \quad \text{prime to } D\mathrm{N}(\mathfrak{r}), \end{cases}$$

where $\mathrm{N}(c) = \mathrm{Norm}_{\mathbb{Q}(\sqrt{-D})/\mathbb{Q}}(\mathfrak{r})$. Put

$$f(z) = \sum_{\mathfrak{A}} \lambda(\mathfrak{A}) \exp(2\pi\sqrt{-1}\,\mathrm{N}(\mathfrak{A})z),$$

where $\mathfrak{A} \neq (0)$ runs over the set of all the integral ideals prime to $\mathfrak{r}$. Then f is an eigen form of $\mathbb{Q}[T_m]_{(m, D\mathrm{N}(\mathfrak{r}))=1}$ belonging to $S_2(\Gamma_0(D\mathrm{N}(\mathfrak{r})))$ [34]. We call such a form f a form with complex multiplication. The form f is a normalized new form if and only if λ is a primitive character. In such a case, $\bar{\mathfrak{r}} = \mathfrak{r}$ and D divides $\mathrm{N}(\mathfrak{r})$, where $\bar{\mathfrak{r}}$ is the complex conjugate of $\mathfrak{r}$ loc.cit. . The $\mathbb{C}$-vector space $S_2(\Gamma_0(N))$ is identified with $\mathrm{H}^0(X_0(N) \otimes \mathbb{C}, \Omega^1)$ by $f \mapsto f(z)\,dz$. Let $V_C = V_C(N)$ (resp. $V_H = V_H(N)$) be the subspace of $\mathrm{H}^0(X_0(N), \Omega^1) \simeq \mathrm{H}^0(J_0(N), \Omega^1)$ such that $V_C \otimes \mathbb{C}$ (resp. $V_H \otimes \mathbb{C}$) is spanned by the eigen forms with complex multiplication (resp. without complex multiplication). Let T_C and T_H be the subspaces of the tangent space of $J_0(N)$ at the unit section which are associated with V_C and V_H, respectively. Let $J_C = J_C(N)$ and $J_H = J_H(N)$ denote the abelian subvarieties $/\mathbb{Q}$ of $J_0(N)$ whose tangent spaces are T_C and T_H, respectively. Then $J_0(N)$ is isogeneous over $\mathbb{Q}$ to the product $J_C \times J_H$, and $\mathrm{End}\, J_0(N) \otimes \mathbb{Q} = \mathrm{End}\, J_C \otimes \mathbb{Q} \times \mathrm{End}\, J_H \otimes \mathbb{Q}$ [28] (4.4) (4.5). Let $k(N)$ be *the composite of the quadratic fields with discriminant D whose square divides N*. For a modular form f of weight 2 and for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$, put

$$f\|[g]_2 = (ad - bc)(cz + d)^{-2} f\left(\frac{az + b}{cz + d}\right).$$

For a normalized new form $f = \Sigma\, a_n q^n$ and for a Dirichlet character χ, $f_{(\chi)}$ denotes the new form with eigen values $a_n\chi(n)$ of T_n for integers n prime to (level of f) $\times$ (conductor of χ).

PROPOSITION 1.3. *Any endomorphism of $J_H = J_H(N)$ is defined over $K(N)$.*

Proof. Let k' be the smallest algebraic number field over which all endomorphisms of J_H are defined. Then k' is a composite of quadratic fields, and any rational prime p with $p \| N$ is unramified in k', see [27] lemma 1, [32] lemma (1.2), [3]VI, see also [18, 29]. There remains to discuss the *2-primary part* of N. Let $f = \Sigma\, a_n q^n$ and $g = \Sigma\, b_n q^n$ be normalized new forms belonging to V_H. If Hom $(J_{\{\sigma f\}}, J_{\{\sigma g\}}) \neq \{0\}$, then there exists a primitive Dirichlet character χ of degree one or two such that $a_n \chi(n) = b(n)^\tau$ for an isomorphism τ of K_g into $\mathbb{C}$ and for all integers n prime to N, see [28] (4.4) (4.5). If $\chi = id.$, then $f = \tau g$. The ring End $J_{\{\sigma f\}} \otimes \mathbb{Q}$ is spanned by the twisting operators as a (left) K_f-vector space [18, 29]. If moreover End $J_0(N) \otimes \mathbb{Q} \simeq K_f$, then all endomorphisms of $J_{\{\sigma f\}}$ are defined over $\mathbb{Q}$. In the other case, let $\eta = \eta_\lambda$ be the twisting operator associated with a primitive Dirichlet character λ of order two, then $a_n^\varrho = a_n \lambda(n)$ for an isomorphism ϱ of K_f into $\mathbb{C}$ and for all integers n, see [18] remark (2.19). Then $f_{(\lambda)} = \varrho f$ is a normalized new form. If $\chi \neq id.$, then $\tau g = f_{(\chi)}$ belongs to $S_2(\Gamma_0(N))$. Therefore it is enough to show that for a primitive Dirichlet character χ of order 2, if $f_{(\chi)}$ belongs to $S_2(\Gamma_0(N))$, then the square of the conductor of χ divides N. We may assume that $\mathrm{ord}_2(\text{level of} f) \leqslant \mathrm{ord}_2(\text{level of } f_{(\chi)})$. Let $r = 2^m t$ be the conductor of χ for an odd integer t, and put $\chi = \chi_1 \chi_2$ for the primitive Dirichlet characters χ_1 and χ_2 with conductors 2^m and t, respectively. As noted as above, t^2 divides N, so that $(f_{(\chi)})_{(\chi_2)} = f_{(\chi_1)}$ belongs to $S_2(\Gamma_0(N))$. If $m \neq 0$, then $4|N$ and the second Fouriere coefficient of $f_{(\chi_1)}$ is zero [1]. Further we have the following relation:

$$f_{(\chi_1)} = \frac{1}{\sqrt{\chi_1(-1)2^m}} \sum_{u \bmod 2^m} \chi_1(u) f \left| \left[\begin{pmatrix} 1 & u/2^m \\ 0 & 1 \end{pmatrix} \right]_2 \right., \quad \text{see [35] §5.} \tag{$*$}$$

Put $N = 2^s M$ for an odd integer M. If $2m < s$, then

$$f_{(\chi_1)} \left| \left[\begin{pmatrix} 1 & 0 \\ 2^{2m-1} & 1 \end{pmatrix} \right]_2 \right. = f_{(\chi_1)}. \tag{$**$}$$

But using the above relation ($*$), we can see that the equality ($**$) can not be sattisfied. □

Put $g_C = g_C(N) = \dim J_C(N)$ and $g_H = g_H(N) = \dim J_H(N)$.

LEMMA 1.4. *If $g_0(N) > 1 + 2g_C(N)$, then all the automorphisms of $X_0(N)$ are defined over $k(N)$.*

Proof. Let u be an automorphism of $X_0(N)$, and put $v = u^\sigma u^{-1}$ for $1 \neq \sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}/k(N))$. Then the automorphism of $J_0(N)$ induced by v acts trivially on J_H by proposition 1.3. Assume that $v \neq id.$ Then $g_C \geqslant 1$. Let

$d\,(\geqslant 2)$ be the degree of v and $Y = X_0(N)/\langle v\rangle$ be the quotient of genus g_Y. Then $g_Y \geqslant g_H$ and $g_0(N) = g_H + g_C$. If $g_H = 0$, then $g_0(N) = g_C < 1 + 2g_C$. If $g_H \geqslant 1$, then the Riemann–Hurwitz formula leads the inequality that $g_0(N) - 1 \geqslant d(g_Y - 1)\ (\geqslant 1(g_H - 1))$. Then $g_0(N) \leqslant 2g_C + 1$. □

Let D be the discriminant of an imaginary quadratic field, and $\mathfrak{r} \neq (0)$ be an integral ideal of $\mathbb{Q}(\sqrt{-D})$ with $\mathfrak{r} = \bar{\mathfrak{r}}$. Let $\nu(D, \mathfrak{r})$ denote the number of the primitive Hecke characters of $\mathbb{Q}(\sqrt{-D})$ with conductor $\mathfrak{r}$ which satisfies the condition (1.2). For an integer $n \geqslant 1$, $\psi(n)$ denotes the number of the positive divisors of n. We know the following.

LEMMA 1.5 [34]. $g_C = \Sigma_D \Sigma_{\mathfrak{r}}\, \nu(D, \mathfrak{r})\psi(N/D\mathbf{N}(\mathfrak{r}))$, *where D runs over the set of the discriminants of imaginary quadratic fields whose squares divide N, and $\mathfrak{r} \neq (0)$ are the integral ideals of $\mathbb{Q}(\sqrt{-D})$ such that $D|\mathbf{N}(\mathfrak{r})$, $D\mathbf{N}(\mathfrak{r})|N$ and $\mathfrak{r} = \bar{\mathfrak{r}}$.*

LEMMA 1.6. *If $g_0(N) \geqslant 2$, then $g_0(N) > 1 + 2g_C$, provide $N \neq 2^6, 2^7, 2^8, 2^9, 3^4, 2\cdot 3^3, 2\cdot 3^2, 2^3\cdot 3^3$.*

Proof. For the sake of simplicity, we here denote $g = g_0(N)$. For a rational prime p, put $r_p = \mathrm{ord}_p N$. The genus formula of $X_0(N)$ is well known:

$$g - 1 = \frac{1}{12}\prod_{p|N} p^{r_p - 1}(p + 1) - e_2 - e_3$$

$$- \frac{1}{2}\prod_{r_p \geqslant 2\,\mathrm{even}} \frac{r_p}{p^2} - 1\,(p + 1)\prod_{r_p\mathrm{odd}} \frac{r_p - 1}{p^2},$$

where

$$e_2 = \begin{cases} 0 & \text{if } 4|N \\ \dfrac{1}{2}\displaystyle\prod_{p|N}\left(1 + \left(\frac{-4}{p}\right)\right) & \text{otherwise} \end{cases}$$

$$e_3 = \begin{cases} 0 & \text{if } 9|N \\ \dfrac{1}{3}\displaystyle\prod_{p|N}\left(1 + \left(\frac{-3}{p}\right)\right) & \text{otherwise.} \end{cases}$$

We estimate g_C. Let D be the discriminant of the imaginary quadratic field $k = \mathbb{Q}(\sqrt{-D})$, and $\mathcal{O} = \mathcal{O}_k$ be the ring of integers of k. For an integer

$n \geqslant 1$ and a rational prime p, put $\psi_p(n) = 1 + \mathrm{ord}_p(n)$. Put $(\frac{-D}{\cdot}) = \chi_p \mu_p$ for primitive characters χ_p and μ_p with conductors p^r and D/p^r for $r = \mathrm{ord}_p D$, respectively. For an integral ideal $\mathfrak{m} \neq (0)$ of $k = \mathbb{Q}(\sqrt{-D})$, let $v_p(D, \mathfrak{m})$ denote the number of the primitive characters λ_p of $(\mathcal{O} \otimes \mathbb{Z}_p)^\times$ which satisfy the following condition: for $a \in \mathbb{Z}_p^\times$,

$$\lambda_p(a) = \begin{cases} \chi_p(a) & \text{if } p \mid D \\ 1 & \text{otherwise.} \end{cases} \tag{1.7}$$

Let $h(-D)$ be the class number of $k = \mathbb{Q}(\sqrt{-D})$, and $\mathfrak{r} \neq \{0\}$ be an integral ideal of k with $\mathfrak{r} = \bar{\mathfrak{r}}$. Let N_p, D_p and $\mathfrak{r}_p$ be the p-primary parts of N, D and $\mathfrak{r}$. Put

$$e_D = \begin{cases} 2 & \text{if } D = 4 \\ 3 & \text{if } D = 3 \\ 1 & \text{otherwise.} \end{cases}$$

Put $\mu(D, p) = \Sigma_{\mathfrak{r}_p} v_p(D, p)\psi_p(N/D\mathbf{N}(\mathfrak{r}))$, where $\mathfrak{r}_p \neq (0)$ runs over the set of the ideals of $\mathcal{O}_k$ such that $\mathfrak{r}_p = \bar{\mathfrak{r}}_p$, $D_p | \mathfrak{r}_p$ and $D\mathfrak{r}_p | N$. Then the formula in lemma 1.5. gives the following inequality:

$$g_C \leqslant \sum_D \frac{h(-D)}{e_D} \sum_{\mathfrak{r}} v_p(D, \mathfrak{r})\psi_p(N/D\mathbf{N}(\mathfrak{r})) = \sum_D \frac{h(-D)}{e_D} \prod_{p|N} \mu(D, p). \tag{1.8}$$

For a positive integer m, $\varphi(m)$ denotes the Euler's number of m. By the well known formula of the class number of $\mathbb{Q}(\sqrt{-D})$: $h(-D) = 1/[2 - (\frac{-D}{2})] \Sigma_{0<a<D/2} (-D/a)$ for $D \neq 4,3$ e.g., [2], we get the following inequality: for $D \neq 4$ nor 3,

$$h(-D) \leqslant \frac{1}{2 - (-D/2)} \cdot \frac{1}{2} \varrho(D) = \begin{cases} \prod_{p|D} (p - 1) & \text{if } 8 \| D \\ \frac{1}{6} \prod_{p|D} (p - 1) & \text{if} \left(\frac{-D}{2}\right) = -1 \\ \frac{1}{2} \prod_{p|D} (p - 1) & \text{otherwise.} \end{cases}$$

For a prime divisor p of N with $p \| N$, $\mu(D, p) = 2$. If $8 \| D$ and $\mathrm{ord}_2 N \leqslant 7$, then $\mu(D, 2) = 0$, see (1.7). For an odd prime divisor p of N with $p^2 | N$, put

$$\mu'(D, p) = \begin{cases} (p-1)\mu(D, p) & \text{if } p \| D \\ \mu(D, p) & \text{otherwise.} \end{cases}$$

If $4|N$, put

$$\mu'(D, 2) = \begin{cases} 2\mu(d, 2) & \text{if } 8 \| D \\ \frac{1}{3}\mu(D, 2) & \text{if} \left(-\frac{D}{2}\right) = -1 \\ \mu(D, 2) & \text{otherwise.} \end{cases}$$

Further let $\mu(p)$ be the maximal value of $\mu'(D, p)$ for discriminants D whose squares divide N. Then by (1.9),

$$\frac{h(-D)}{e_D} \prod_{p|N} \mu(D, p) \leqslant \frac{1}{2} \prod_{p^2|N} \mu(p) \prod_{p\|N} 2.$$

Then the inequalities (1.8) and (1.9) gives the following estimates of g_C:

$$2g_C \leqslant \begin{cases} \prod_{p^2|N} 2\mu(p) \prod_{p\|N} 2 & \text{if } 2^8|N \\ \frac{1}{2} \prod_{p^2|N} 2\mu(p) \prod_{p\|N} 2 & \text{otherwise.} \end{cases} \tag{1.10}$$

One can easily calculate $\mu(D, p)$: Put $r = \mathrm{ord}_p N$ for a fixed rational prime p.

Cast $p \neq 2$:

	$p\|D$	$(-D/p) = 1$	$(-D/p) = -1$
$n = 2r$ $(\geqslant 2)$	$1 + 2 \cdot \frac{p^r - 1}{p - 1}$	$p^r + p^{r-1} + 2r - 1$	$\frac{p^r + 1}{p - 1}(p^r + p^{r-1} - 2) + 2r + 1$
$n = 2r + 1$ $(\geqslant 3)$	$-1 + p^r + 2 \cdot \frac{p^r - 1}{p - 1}$	$2p^r + 2r$	$2 \cdot \frac{p + 1}{p - 1}(p^r - 1) + 2r + 2$

Case $p = 2$:

	$8 \| D$	$4 \| D$	$(-D/2) = 1$	$(-D/2) = -1$
$n = 2r$ $(\geqslant 2)$	$2^r - 12$ $(r \geqslant 4)$	$2^r + 2^{r-1} - 4$ $(r \geqslant 2)$	$2^r + 2^{r-1} + 2r - 1$	$3(2^r + 2^{r-1} - 2)$ $+ 2r + 1$
$n = 2r + 1$ $(\geqslant 3)$	$2^r + 2^{r-1} - 12$ $(r \geqslant 4)$	$2^{r+1} - 4$ $(r \geqslant 2)$	$2^{r+1} + 2r$	$6(2^r - 1) + 2r + 2$

Using the genus formula of $X_0(N)$ and the estimate (1.10) of g_C, one can see that $g > 1 + 2g_C$, except for some integers N. For the remaining cases, a direct calculation makes complete this lemma. □

COROLLARY 1.11. *Any automorphism of $X_0(N)$ ($g_0(N) \geqslant 2$) is defined over the field $k(N)$ provided $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3$.*

Proof. Lemma 1.3, 1.4 and 1.6 give this lemma, except for $N = 2^6, 2^7, 3^4, 2 \cdot 3^3, 2^3 3^2$. The ring End $J_C \otimes \mathbb{Q}$ is determined by the associated Hecke characters [3, 34]. Considering the condition (1.2), we get the result also for the remaining cases. □

REMARK 1.12. We here add the results on the fields of definition of endomorphisms of J_C for $N = 2^8, 2^9, 2^2 3^3, 2^3 3^3$.
(1) $N = 2^8, 2^9$: Let χ be a character of the ideal group of $\mathbb{Q}(\sqrt{-1})$ of order 4 which satisfies the following conditions:

(i) $\chi((\alpha)) = 1$ for $\alpha \in \mathbb{Q}(\sqrt{-1})$ with $\alpha \equiv 1 \bmod^{\times} 8$.
(ii) $\chi((\alpha)) = 1$ for $\alpha \in \mathbb{Z}$ prime to 2.

Let $J_{C(-1)}$ and $J_{C(-2)}$ be the abelian subvarieties $/\mathbb{Q}$ of J_C whose tangent spaces $\otimes\mathbb{C}$ correspond to the subspaces spanned by the eigen forms induced by the Hecke characters of $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$, respectively. Let $k'(N)$ be the class field of $\mathbb{Q}(\sqrt{-1})$ associated with ker (χ). Then any endomorphisms of $J_{C(-1)}$ is defined over $k'(N)$ and End $J_C \otimes \mathbb{Q} \simeq$ End $J_{C(-1)} \otimes \mathbb{Q} \times$ End $J_{C(-2)} \otimes \mathbb{Q}$. The same argument as in lemma 1.4 shows that any automorphism of $X_0(N)$ is defined over $k'(N)$. Note that $\zeta_{16} = \exp(2\pi\sqrt{-1}/16)$ does not belong to $k'(N)$.
(2) $N = 2^2 3^3, 2^3 3^3$: Let $\chi \neq 1$ be a character of the ideal group of $\mathbb{Q}(\sqrt{-3})$ which satisfies the following conditions:

(i) $\chi((\alpha)) = 1$ for $\alpha \in \mathbb{Q}(\sqrt{-3})^{\times}$ with $\alpha \equiv 1 \bmod^{\times} 6$.
(ii) $\chi((\alpha)) = 1$ for $a \in \mathbb{Z}$ prime to 6.

Then any endomorphism of J_C is defined over the class field $k'(N)$ associated with ker (χ). Note that ζ_9 and ζ_8 do not belong to $k(N)$.

Let $p \geqslant 5$ be a prime number and K be a finite extension of $\mathbb{Q}_p^{ur}$ of degree e_K. For an elliptic curve E defined over K, and an integer $m \geqslant 3$ prime to p, let ϱ_m be the representation of $G_K = \mathrm{Gal}(\bar{K}/K)$ induced by the Galois action of G_K on the m-torsion points $E_m(\bar{K})$. Then $\varrho_m(G_K)$ becomes a subgroup of $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$, and ker (ϱ_m) is independent of the integer $m \geqslant 3$ prime to p. Let K' be the extension of K associated with ker (ϱ_m), and e be the degree of the extension K'/K. Let $\pi = \pi_K$ be a prime element of the ring $R = \mathcal{O}_K$ of integers of K. Then we know that (i) If the modular invariant $j(E) \not\equiv 0$, $1728 \bmod \pi$, then $e = 1$ or 2, (ii) If $e = 4$, then $j(E) \equiv 1728 \bmod \pi$, (iii) If $e = 3$ or 6, then $j(E) \equiv 0 \bmod \pi$ e.g., [31] §5 (5.6) [36] p. 46. Now assume that E has a cyclic subgroup $A(/K)$ of order N for an integer N divisible by p^2. Put $e' = e$ if e is odd, and $e' = e/2$ if e is even.

LEMMA 1.13 ([20] § lemma (2.2), (2.3)). *If $e_K e' < p - 1$, then the pair (E, A) defines a R-valued section of the smooth part of $\mathscr{X}_0(N)$.*

COROLLARY 1.14. *Let x: Spec $R \to \mathscr{X}_0(N)$ be a section of an integer N divisible by p^2. If $e_K = 1$ and $p \geqslant 5$, then x is a section of the smooth part of $\mathscr{X}_0(N)$. If $e_K = 2$ and $p \geqslant 7$, then x is a section of the smooth part of $\mathscr{X}_0(N)$.*

REMARK 1.15. Under the notation as above, we here consider the cases for $e_K = 2$ and $p = 5, 7$. Put $N = p^r m$ for coprime integers p^r and m $(r \geqslant 2)$. Under one of the following conditions (i), (ii) on m, $e' = 1$ for $p = 5$, and $e' \leqslant 2$ for $p = 7$.

$p = 5$: Conditions on m.
- (i) 4, 6 or 9 divides m.
- (ii) 2 or a rational prime q with $q = 2 \bmod 3$ divides m, and a rational prime q' with $q' \equiv 3 \bmod 4$ divides m.

$p = 7$:
- (i) 2 or 9 divides m.
- (ii) A rational prime q with $q \equiv 2 \bmod 3$ divides m.

(1.16) The fixed points of w_N.

Let w_N be the fundamental involution of $X_0(N)$: $(E, A) \mapsto (E/A, E_N/A)$. Put $N = N_1^2 N_2$ for the square free integer N_2. Let k_N be the class field of $\mathbb{Q}(\sqrt{-N_2})$ which is associated with the order of $\mathbb{Q}(\sqrt{-N_2})$ with conductor

N_1. Put $h_N = |k_N: \mathbb{Q}(\sqrt{-N_2})|$. Then as well known (see e.g. [12] Chapter 8 theorem 7)

$$h_N = h(-N_2)\frac{N_1}{|\mathcal{O}^\times : \mathcal{O}_{N_1}^\times|}\sum_{p|N_1}\left(1 - \left(\frac{-N_2}{p}\right)\frac{1}{p}\right),$$

where $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(\sqrt{-N_2})$ and $\mathcal{O}_{N_1} = \mathbb{Z} + N_1\mathcal{O}$. Let S_N be the number of the fixed points of w_N. Then

$$S_N = \begin{cases} h_N & \text{if } N_2 \equiv 1 \quad \text{or} \quad 2 \bmod 4 \\ h_N + h_{4N} & \text{if } N_2 \equiv 3 \bmod 4. \end{cases}$$

Let $p \leqslant 13$ (or $p = 17, 19, 23$ or 29 etc.) be a rational prime and M be an integer prime to p. Then supersingular points on $\mathscr{X}_0(1) \otimes \mathbb{F}_p$ are all $\mathbb{F}_p$-rational and the supersingular points on $\mathscr{X}_0(M) \otimes \mathbb{F}_p$, hence those on $\mathscr{X}_0(pM) \otimes \mathbb{F}_p$ are all $\mathbb{F}_{p^2}$-rational [3]V theorem 4.17, [36] table 6 p. 142–144. Let $m(M, p) = g_0(pM) - 2g_0(M) + 1$. For a prime divisor q of M, put $r_q = \mathrm{ord}_q M$. Put

$$m(2) = \begin{cases} \sum_{i=0}^{r_2} \varphi((2^i, 2^{r_2 - i})) & \text{if } r_2 \leqslant 6 \\ 16 & \text{if } r_2 \geqslant 6, \quad \text{and} \end{cases}$$

$$m(3) = \begin{cases} \sum_{i=0}^{r_3} \varphi((3^i, 3^{r_3 - i})) & \text{if } r_3 \leqslant 2 \\ 4 & \text{if } r_3 \geqslant 2, \end{cases}$$

where φ is the Euler's function. The number of the $\mathbb{F}_{p^2}$-rational cusps on $\mathscr{X}_0(M) \otimes \mathbb{F}_p = m(2)m(3)\prod_{\substack{q|M \\ q\neq 2,3}} 2$. Therefore

$$\#\mathscr{X}_0(M)(\mathbb{F}_{p^2}) \geqslant g_0(pM) - 2g_0(M) + 1 + m(2)m(3)\prod_{\substack{q|M \\ q\neq 2,3}} 2. \tag{1.17}$$

§2. Automorphisms of $X_0(N)$

In this section, we discuss the automorphisms of the modular curves $X_0(N)$ of genus $g_0(N) \geqslant 2$. For an automorphism u of $X_0(N)$, u denotes also the induced automorphism of the jacobian variety $J_0(N)$. Let $k(N)$ be the composite of the quadratic fields with discriminants D whose squares divide N. For the integers $N = 2^8, 2^9, 2^3 3^3$ and $2^3 3^3$, let $k'(N)$ be the fields defined in remark 1.12.

(2.1) (see [1] §4). Let $A_\infty = A_\infty(N)$ denote the subgroup of Aut $X_0(N)$ consisting of the automorphisms which fix the cusp $\infty = \binom{1}{0}$, and put $B_\infty = A_\infty \cap B_0(N)$. Then A_∞ is a cyclic group. Let $\mathbb{Q}[[q]]$ be the completion of the local ring $\mathcal{O}_{X_0(N),\infty}$ with the canonical local parameter q see [4] VII. For $\gamma \in A_\infty$, $\gamma * (q) = \zeta_m q + c_2 q^2 + \cdots$ for a primitive m-th root ζ_m of unity and $c_i \in \bar{\mathbb{Q}}$. Then we see easily that the field of definition of γ is $\mathbb{Q}(\zeta_m)$. Put $r_2 = \min\{3, [\frac{1}{2} \operatorname{ord}_2 N]\}$, $r_3 = \{1, [\frac{1}{2} \operatorname{ord}_3 N]\}$ and $m = 2^{r_2} 3^{r_3}$. Then A_∞ is generated by $\begin{pmatrix} 1 & 1/m \\ 0 & 1 \end{pmatrix} \bmod \Gamma_0(N)$.

LEMMA 2.2. *Under the notation as above, suppose that an involution u belongs to A_∞. Then u is defined over $\mathbb{Q}$ and it is not the hyperelliptic involution. Moreover* $4|N$.

Proof. Let $\mathbb{Q}[[q]]$ be the completion of the local ring at the cusp ∞ with the canonical local parameter q [3] VII. Put $u * (q) = c_1 q + c_2 q^2 + \cdots$ for $c_i \in \bar{\mathbb{Q}}$. Then one sees easily that $c_1 = -1$ and that u is defined over $\mathbb{Q}$. The hyperelliptic modular curves of type $X_0(N)$ are all known [22] theorem 2. In all cases, the hyperelliptic involution of $X_0(N)$ do not fix the cusp ∞. Using the congruence relation [3] [33] Chapter 7 (7.4), one sees that u commutes with the Hecke operators T_l for prime numbers l prime to N. For a normalized new form g belonging to $S_2(\Gamma_0(N))$, let $V(g)$ be the subspace spanned by $g|e_d$ for positive divisors d of N/(level of g) cf. (1.1). Then $S_2(\Gamma_0(N)) = \oplus V(g)$ as $\mathbb{Q}[T_l]_{(l,N)=1}$-modules, where g runs over the set of the normalized new forms belonging to $S_2(\Gamma_0(N))$. If N/(level of g) is odd, then $u * | V(g)$ becomes a triangular matrix with the eigen values -1 for a choice of the basis of $V(g)$. Hence $u * | V(g) = -1_{V(g)}$. If N is odd, then $u * = -1$ on $S_2(\Gamma_0(N))$. Then $u = -1$ on $J_0(N)$, and it is a contradiction. Now consider the case $2 \| N$. Let $K(/\mathbb{Q})$ be the abelian subvariety of $J_0(N)$ whose tangent space $\operatorname{Tan}_0 K \otimes \mathbb{C}$ corresponds to the subspace $\oplus' V(g)$ for the normalized new forms g with even level. Then as noted as above, u acts on K under -1. Let $\tilde{\mathscr{X}}_0(N) \to \operatorname{Spec} \mathbf{W}(\bar{\mathbb{F}}_2)$ be the minimal model of $X_0(N) \otimes \mathbb{Q}_2^{ur}$, and Σ be the dual graph of the special fibre $\tilde{\mathscr{X}}_0(N) \otimes \bar{\mathbb{F}}_2$. Let Z and Z' be the irreducible components of $\tilde{\mathscr{X}}_0(N) \otimes \bar{\mathbb{F}}_2$ which contains the cusps $\infty \otimes \bar{\mathbb{F}}_2$ and $\mathbf{0} \otimes \bar{\mathbb{F}}_2$, respectively cf. §1. Since the genus $g_0(N) \geqslant 2$, the self-intersection numbers of Z and Z' are $\leqslant -3$, and those of the other irreducible components are all -2. Denote also by u the induced automorphism of the minimal model $\tilde{\mathscr{X}}_0(N)$. Note that u is defined over $\mathbb{Q}$. Then u send $Z \cup Z'$ to itself. By the condition $u(\infty) = \infty$, u fixes Z and Z'. Let P^τ be the kernel of the degree map Pic $\tilde{\mathscr{X}}_0(N) \to \mathbb{Z}$, P^0 be the connected component of the unit section of P^τ, and E be the Zariski closure of the unit section of the generic fibre $P^\tau \otimes \mathbb{Q}_2^{ur}$. Then the Néron model $J_0(N)_{/\mathrm{W}(\bar{\mathbb{F}}_2)} = P^\tau/E$ and $P^0 \cap E = \{0\}$, see [25] §8 (8.1), [4] VI. Let l be an odd prime number and T_l, $V_l = T_l \otimes \mathbb{Q}_l$ be the Tate modules. Then $V_l(\mathrm{H}^1(\Sigma, \mathbb{Z}) \otimes \mathbb{G}_m) = V_l(P^0) = V_l(K)^I$, where I is the inertia subgroup Gal $(\bar{\mathbb{Q}}_2/\mathbb{Q}_2^{ur})$ [32] lemma 1. Then one sees that u acts under -1 on $\mathrm{H}^1(\Sigma, \mathbb{Z})$. Since u fixes Z and Z', considering the action of u on the dual graph Σ, one sees that $\mathrm{H}^1(\Sigma, \mathbb{Z}) = \{0\}$ or $\mathbb{Z}$, i.e., $g_0(N) = 2g_0(N/2)$ or $= 2g_0(N/2) + 1$. By the result [23], it suffices to discuss the case when $N/2$ is not square free. Then there are at least six cusps on $X_0(N/2)$, since $g_0(N/2) \geqslant 1$. Then the Riemann–Hurwitz relation

$$g_0(N) - 1 \geqslant 3\{g_0(N/2) - 1\} + \tfrac{1}{2}\,\#\{\text{cusps on } X_0(N/2)\}.$$

gives a contradiction. □

COROLLARY 2.3. $A_\infty = B_\infty$.

Proof. Let $\mathbb{Q}[[q]]$ be the completion of the local ring at the cusp ∞ with the canonical local parameter q. Put $u*(q) = c_1 q + c_2 q + \cdots$ for $c_i \in \bar{\mathbb{Q}}$. Then c_1 is a root of unity belonging to the field $k(N)$, or $k'(N)$ for $N = 2^8$, 2^9, $2^2 3^3$ and $2^3 3^3$ cf. corollary 1.11, remark 1.12. Hence $c_1 \in \mu_{24}(k(N))$, see loc.cit. For the case $\mathrm{ord}_2 N \leqslant 1$, by (2.1) and lemma 2.2, $A_\infty = B_\infty$. For the case $\mathrm{ord}_2 N \geqslant 2$, by (2.1), $A_\infty = B_\infty$. □

COROLLARY 2.4. *Let C be a $k(N)$ or $k'(N)$-rational cusp, and u be an automorphism of $X_0(N)$ such that $u(C)$ is a cusp. Then u belongs to the subgroup $B_0(N)$.*

Proof. It suffices to note that $B_0(N)$ acts transitively on the set of the $k(N)$ or $k'(N)$-rational cusps on $X_0(N)$. □

Let "$F(N)$" be the subfield of $k(N) \cap \mathbb{Q}(\zeta_8, \sqrt{-3}, \sqrt{5}, \sqrt{-7})$ which contains $k(N) \cap \mathbb{Q}(\zeta_8, \sqrt{-3})$ and satisfies the following conditions for $p = 5$ and 7: the rational prime $p = 5$ (resp. $p = 7$) is unramified in $F(N)$ if one of the conditions (i), (ii) in (1.15) for p is satisfied.

LEMMA 2.5. *If an automorphism u of $X_0(N)$ is defined over $k(N)$, then u is defined over $F(N)$.*

Proof. It is enough to show that for each rational prime $p \geqslant 5$ with $p^2|N$, if p is unramified in $F(N)$, then u is defined over $\mathbb{Q}_p^{ur}$, see corollary 1.11, remark 1.12. First note that the $k(N)$-rational cusps on $\mathscr{X}_0(N) \otimes \mathbb{Z}[1/6]$ are the sections of the smooth part $\mathscr{X}_0(N)^{smooth} \otimes \mathbb{Z}[1/6]$ see lemma 1.13, corollary 1.14, remark 1.15, [4]. Let p be a rational prime which is unramified in $F(N)$. Then we know that any $k(N)$-rational point on $X_0(N)$ defines a $\mathcal{O}_{k(N)} \otimes \mathbb{Z}_p$-section of $\mathscr{X}_0(N)^{smooth}$, see loc.cit. For $1 \neq \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{ur})$, let x be the section of $J_0(N)$ defined by

$$x = cl((u(\mathbf{0})) - (u(\infty)) - (u^\sigma(\mathbf{0})) + (u^\sigma(\infty))).$$

Since $cl((\mathbf{0}) - (\infty))$ is of finite order [13], x is of finite order and is defined over $k(N) \otimes \mathbb{Q}_p^{ur}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O} = \mathcal{O}_{k(N)}$ lying over the rational prime p, and $\mathcal{O}_\mathfrak{p}$ be the completion along $\mathfrak{p}$. As noted as above, $u(\mathbf{0})$, $u(\infty)$, $u^\sigma(\mathbf{0})$ and $u^\sigma(\infty)$ define the $\mathcal{O}_\mathfrak{p}$-sections of $\mathscr{X}_0(N)^{smooth}$ such that $u(\mathbf{0}) \otimes \kappa(\mathfrak{p}) = u^\sigma(\mathbf{0}) \otimes \kappa(\mathfrak{p})$ and $u(\infty) \otimes \kappa(\mathfrak{p}) = u^\sigma(\infty) \otimes \kappa(\mathfrak{p})$. Then by the universal property of the Néron model, we see that $x \otimes \kappa(\mathfrak{p}) = 0$ (= the unit section). Further by the conditions that x is of finite order and that $p > \mathrm{ord}_\mathfrak{p}(p) + 1$, we see that x is the unit section [26] §3 (3.3.2), [15] proposition 1.1. Thus we get the linearly equivalent relation: $(u(\mathbf{0})) + (u^\sigma(\infty)) \sim (u(\infty)) + (u^\sigma(\mathbf{0}))$. Now suppose that $u^\sigma \neq u$.

Case $u(\infty) = u^\sigma(\infty)$: Put $v = u^\sigma u^{-1}$ ($\neq$ id.). Then v fixes the cusps $\mathbf{0}$ and ∞, so that v belongs to $B_0(N)$, corollary 2.3. But any non trivial automorphism belonging to $B_0(N)$ does not fix both of $\mathbf{0}$ and ∞ [1] §4.

Case $u(\infty) \neq u^\sigma(\infty)$: By the above linear equivalence, there exists the hyperelliptic involution γ of $X_0(N)$ with $\gamma u(\mathbf{0}) = u^\sigma(\mathbf{0})$. Then by the condition on p as above and by the classification of hyperelliptic modular curves of type $X_0(N)$ [23] theorem 2, there remains the case for $N = 50$. But $k(50) = F(50) = \mathbb{Q}(\sqrt{5})$, corollary 1.11. □

Let l be a prime number prime to N, and T_l be the Hecke operator associated with l.

LEMMA 2.6. *Let u be an automorphism of $X_0(N)$ defined over a composite of quadratic fields, and σ_l be a Frobenius element of the rational prime l. Then*

$$uT_l = T_l u^{\sigma_l} \quad \text{on} \quad J_0(N).$$

Proof. On $J_0(N) \otimes \mathbb{F}_l$, we have the congruence relation [3, 33] Chapter 7 (7.4):

$$T_l = F + V, \quad FV = VF = l,$$

where F is the Frobenius map and V is the Verschiebung. Put $u^{(l)} = u^{\sigma_l}$ on $J_0(N) \otimes \mathbb{F}_l$. Then the assumption on u as above shows that $uF = Fu^{(l)}$ and $uV = Vu^{(l)}$. □

Let $\mathscr{D}$ (resp. $\mathscr{D}_0$, resp. $\mathscr{D}_l$) be the group of divisors of $X_0(N)$ (resp. of degree 0, resp. which are linearly equivalent to 0). For a prime number l prime to N, and for an automorphism u of $X_0(N)$, T_l and u, u^{σ_l} act on $\mathscr{D}$, $\mathscr{D}_0$ and $\mathscr{D}_l$. Put $\alpha_l = uT_l - T_lu^{\sigma_l}$ on $J_0(N)$. Then by lemma 2.6, $\alpha_l = 0$ on $J_0(N) \otimes \mathbb{C} = \mathscr{D}_0/\mathscr{D}_l$. Put $D_l = \alpha_l((\mathbf{0}) - (\infty))$ $(= (l+1)(u(\mathbf{0})) + (T_lu^{\sigma_l}(\infty)) - (l+1)(u(\infty)) - (T_lu^{\sigma_l}(\mathbf{0})))$. Then $D_l \sim 0$, linearly equivalent to the zero divisor.

LEMMA 2.7. *Under the notation as above, let u be an automorphism of $X_0(N)$ defined over the field $F(N)$. Then if $u(\mathbf{0})$ or $u(\infty)$ is not a cusp, then $D_l \neq 0$.*

Proof. If $D_l = 0$, then $(l+1)(u(\mathbf{0})) = (T_lu^{\sigma_l}(\mathbf{0}))$ and $(l+1)(u(\infty)) = (T_lu^{\sigma_l}(\infty))$. Suppose that $D_l = 0$ and that $u(\mathbf{0})$ is not a cusp. Let $z \in \mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ be the point which corresponds to $u^{\sigma_l}(\mathbf{0})$ under the canonical identification of $X_0(N) \otimes \mathbb{C}$ with $\Gamma_0(N)\backslash\mathfrak{H} \cup \{i\infty, \mathbb{Q}\}$. Then

$$T_lu^{\sigma_l}(\mathbf{0}) \equiv (lz) + \sum_{i=0}^{l-1} \left(\frac{z+i}{l}\right) \bmod \Gamma_0(N).$$

The corresponding points on $X_0(N) \otimes \mathbb{C}$ to (lz) and $(z + i/l)$ are represented by elliptic curves $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}lz$ and $\mathbb{C}/\mathbb{Z} + \mathbb{Z}(z + i/l)$ with level structures, respectively. Then by the assumption $D_l = 0$, $E \simeq \mathbb{C}/\mathbb{Z} + \mathbb{Z}(z + i/l)$ for the integers i, $0 \leqslant i \leqslant l-1$. Consider the following homomorphisms f_i with kernel C_i:

$$f_i\colon E \xrightarrow{\text{can.}} \mathbb{C}/\mathbb{Z} + \mathbb{Z}\frac{z+i}{l} \xrightarrow{\sim} E.$$

Then $C_i = \mathbb{Z}((i/l) + (1/l^2)lz) \bmod L = \mathbb{Z} + \mathbb{Z}lz$ are cyclic subgroups of order l^2, and $(C_i)_l$ $(= \ker(l\colon C_i \to C_i)) = (1/l)\mathbb{Z}lz \bmod L$. This is a contradiction. (Because, there are at most two cyclic subgroups A_i of order l^2 with $E/A_i \simeq E$. If $l = 2$ and there are such subgroups A_i $(i = 1, 2)$, then $2A_1 \neq 2A_2$. □

PROPOSITION 2.8. *Let u be an automorphism of $X_0(N)$ defined over $\mathbb{Q}$. Then u belongs to the subgroup $B_0(N)$, provided $N \neq 37$.*

Proof. By the results on the rational points on $X_0(N)$ [10, 15, 17], we know that $u(\mathbf{0})$ is a cusp, provided $N \neq 37, 43, 67, 163$. The rest of the proof owes to corollary 2.4 and [23] Satz 1. □

The following result is immediate from corollary 1.11, remark 1.12 and lemma 2.5.

COROLLARY 2.9. *If $F(N) = \mathbb{Q}$, then* Aut $X_0(N) = B_0(N)$, *provided $N \neq 37$.*

Now consider the case $F(N) \neq \mathbb{Q}$. In this case N are divisible by the square of 2, 3, 5 or 7, see lemma 2.5. Let u be an automorphism of $X_0(N)$ which is not defined over $\mathbb{Q}$. If $u(\mathbf{0})$ or $u(\infty)$ is a cusp, then u belongs to the subgroup $B_0(N)$, see corollary 2.4. So we assume that $u(\mathbf{0})$ and $u(\infty)$ are not cusps. Let l be a prime number prime to N, $\sigma = \sigma_l$ be a Frobenius element of the rational prime l, and $D_l = (l+1)(u(\mathbf{0})) + (T_l u^\sigma(\infty)) - (l+1)(u(\infty)) - (T_l u^\sigma(\mathbf{0}))$ (~ 0) be the divisor of $X_0(N)$ defined as above, see lemma 2.7, for $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3$ cf. corollary 1.11, remark 1.12. Under the assumption on u as above, $D_l \neq 0$ by lemma 2.7.

LEMMA 2.10. *Under the assumption as above for $N \neq 37, 2^8, 2^9, 2^2 3^3, 2^3 3^3$, assumes that $D_l \neq 0$ and $l \geqslant 5$. Then $w_N * (D_l) \neq D_l$, and $u(\mathbf{0})$, $u(\infty)$ are not the fixed points of w_N.*

Proof. If $D_l = w_N * (D_l)$, then

$$(l+1)(u(\mathbf{0})) + (T_l u^\sigma(\infty)) + (l+1)(w_N u(\infty)) + (T_l w_N u^\sigma(\mathbf{0}))$$

$$= (l+1)(w_N u(\mathbf{0})) + (T_l w_N u^\sigma(\infty)) + (l+1)(u(\infty)) + (T_l u^\sigma(\mathbf{0})).$$

(Note that $w_N T_l = T_l w_N$ on $J_0(N)$, since w_N is defined over $\mathbb{Q}$, see lemma 2.6.) The assumption $D_l \neq 0$ shows that $(l+1)(u(\mathbf{0})) \neq (T_l w_N u^\sigma(\infty))$ nor $(T_l u^\sigma(\mathbf{0}))$, see the proof in lemma 2.7. Suppose that $w_N * (D_l) = D_l$. Then the similar argument as in the proof of lemma 2.7 shows that $u(\mathbf{0})$ and $u(\infty)$ are the fixed points of w_N, since $l \geqslant 5$. Let p be a prime divisor of N with $p \| N$ or $p \geqslant 11$. Then u defines an automorphism of the minimal model $\mathscr{X}_0(N) \to \operatorname{Spec} \mathbf{W}(\bar{\mathbb{F}}_p)$, see lemma 2.5. If $p \| N$, then $u(\mathbf{0}) \otimes \bar{\mathbb{F}}_p$ and $u(\infty) \otimes \bar{\mathbb{F}}_p$ are not the supersingular points (, because $g_0(N) \geqslant 2$). By our assumption and corollary 2.9, the automorphism u is not defined over $\mathbb{Q}$, and N is divisible by the square of a prime $q \leqslant 7$ see lemma 2.5. Therefore if $p \geqslant 11$, then $\mathscr{X}_0(N) \otimes \bar{\mathbb{F}}_p$ has at least three supersingular points, and the points $u(\mathbf{0})$ and $u(\infty)$ define the sections of different irreducible components of $\tilde{\mathscr{X}}_0(N) \otimes \bar{\mathbb{F}}_p$ see corollary 1.14. Hence N is a form $2^a 3^b 5^c 7^d$ for integers $a, b, c, d = 0$ or $\geqslant 2$. Let S be the set of rational primes which ramify in $F(N)$. Then we see that $S = \{2, 3\}, \{2\}, \{3\}, \{5\}$ or $\{7\}$, see corollary 1.14, remark 1.15, lemma 2.5, proposition 2.8. Put $N = N_1^2 N_2$ for the square free integer N_2. Let k_N be the class field of $\mathbb{Q}(\sqrt{-N_2})$ associated with the order with conductor N_1. Then the condition $w_N u(\mathbf{0}) = u(\mathbf{0})$ gives the inequality that $[F(N)\colon \mathbb{Q}] \leqslant [k(N)\colon \mathbb{Q}(\sqrt{-N_2})]$, which is satisfied only for $N = 2^6$, see (1.16). For $N = 2^6$, $F(N) = \mathbb{Q}(\zeta_8)$ and k_N is the class field of $\mathbb{Q}(\sqrt{-1})$ of degree 4, see loc.cit. Thus $u(\mathbf{0})$ is not a fixed point of w_N. □

COROLLARY 2.11. *Under the notation and assumption as in lemma 2.10, let S_N be the number of the fixed points of w_N on $X_0(N)$. Then $S_N \leqslant 4(l+1)$.*

Proof. Put $D_+ = (l+1)(u(\mathbf{0})) + (T_l u^\sigma(\infty))$ and $D_- = (l+1)(u(\infty)) + (T_l u^\sigma(\mathbf{0}))$ for a Frobenius element $\sigma = \sigma_l$ of the rational prime l. Let n_+, n_- be the numbers of the fixed points of w_N belonging to Supp (D_+) and Supp (D_-), respectively. Then Supp $(w_N * (D_+))$ (resp. Supp $(w_N * (D_-))$) contains exactly n_+ (resp. n_-) fixed points of w_N. Consider the rational function f on $X_0(N)$ whose divisor $(f) = D_l = D_+ - D_-$ ($\neq 0$, by our assumption). Put $g = w_N * (f)/f - 1$, which is not a constant function, see lemma 2.10. For a fixed point x of w_N not belonging to Supp $(D_+) \cup$ Supp (D_-), $g(x) = 0$. Then $4(l+1) - (n_+ + n_-) \geqslant$ the degree of $g \geqslant S_N - (n_+ + n_-)$. □

Now under the assumption that $u(\mathbf{0})$ and $u(\infty)$ are not cusps, we estimate the least prime number l not dividing N. Let p_n be the n-th prime number. We know the following estimate of p_n for $n \geqslant 4$ [30] theorem 3:

$$p_n < 1.4 \times n \log(n), \tag{2.12}$$

Let $l(N)$ be the least prime number not dividing N.

LEMMA 2.13. *Under the notation and the assumption as above, $l(N) \leqslant 19$.*

Proof. We may assume that $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3$. Put $N = N_1^2 N_2$ for the square free integer N_2. Let n_i $(i = 1, 2)$ be the numbers of the prime divisors of N_i, and n be the number of the prime divisors of N. We will show that $n \leqslant 7$, applying lemma 2.10. We know the following (1.16):

$$S_N = \begin{cases} \frac{1}{2}N_1 \prod_{p|N_1}\left(1 - \left(\frac{-1}{p}\right)\frac{1}{p}\right) & \text{if } N_2 = 1 \\ \frac{4}{3}N_1 \prod_{p|N_1}\left(1 - \left(\frac{-3}{p}\right)\frac{1}{p}\right) & \text{if } N_2 = 3 \\ h(-N_2) \prod_{p|N_1}\left(1 - \left(\frac{-N_2}{p}\right)\frac{1}{p}\right) & \text{if } N_2 \neq 1 \text{ and } N_2 \equiv -1 \bmod 4 \\ \geqslant 2h(-N_2) \prod_{p|N_1}\left(1 - \left(\frac{-N_2}{p}\right)\frac{1}{p}\right) & \text{if } N_2 \neq 3 \text{ and } N_2 \equiv -1 \bmod 4 \end{cases}$$

As well known, $n_2 \leqslant \mathrm{ord}_2\, h(-N_2)$ if $N_2 \equiv 1 \bmod 4$, and $n_2 - 1 \leqslant \mathrm{ord}_2\, h(-N_2)$ if $N_2 \not\equiv 1 \bmod 4$ (see e.g., [2]). Then the above formula of S_N gives the estimate that $S_N \geqslant 2^n$ for $n \geqslant 7$. Then corollary 2.11 and (2.12) give the following estimate of S_N for $n \geqslant 7$:

$$S_N \leqslant 4(1 + p_{n+1}) < 4\{1 + 1.4 \times (n + 1) \log (n + 1)\}.$$

Then by a calculation, we get $n \leqslant 7$. □

Let p be a prime divisor of N with $r = \mathrm{ord}_p N$. Put $M = M/p^r$, and let $\pi = \pi_{N,M}: \mathscr{X}_0(N) \to \mathscr{X}_0(M)$ be the natural morphism. For a prime number l not dividing N, let D_l be the divisor defined in lemma 2.7. For $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3$, $cl(D_l) = 0$ on $J_0(N)$, so that the image $\pi(cl(D_l)) = 0$ under the natural homomorphism $\pi: J_0(N) \to J_0(M)$ of jacobian varieties. Let $E_l = (l + 1)(\pi u(\mathbf{0})) + (T_l \pi u^\sigma(\infty)) - (l + 1)(\pi u(\infty)) - (T_l \pi u^\sigma(\mathbf{0}))$ be a divisor of $X_0(M)$. Then $E_l \sim 0$ (for $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3$), since $\pi(T_l | J_0(N)) = (T_l | J_0(M))\pi$. We give a criterion for $E_l \neq 0$.

LEMMA 2.14. *Under the notation as above, assume that $u(\mathbf{0})$ and $u(\infty)$ are not cusps. If the following conditions are satisfied, then $E_l \neq 0$: There exists a prime divisor q of N with $t = \mathrm{ord}_q N$ such that $g_0(N/q^t) \geqslant 1$ and that q satisfies the following conditions* (i), (ii) *and* (iii):

(i) $q \| N$.
(ii) $q \geqslant 11$.
(iii) $q = 5$ *or* 7 *which satisfies one of the conditions* (i), (ii) *for q in lemma* 1.15.

Proof. It suffices to show that under the conditions as above $\pi u(\mathbf{0}) \neq \pi u(\infty)$, see the proof of lemma 2.7. Any automorphisms u of

$X_0(N)$ is defined over the field $F(N)$, see corollary 1.11, lemma 2.5. Let $\mathfrak{q}$ be a prime of $F(N)$ lying over the rational prime q which satisfies the above conditions. Then u defines the automorphism u of the minimal model $\tilde{\mathscr{Y}} \to \operatorname{Spec} \mathcal{O}_{\mathfrak{q}}$ of $X_0(N) \otimes F(N)_{\mathfrak{q}}$, where $\mathcal{O}_{\mathfrak{q}}$ is the completion of the ring of integers of $F(N)$ along $\mathfrak{q}$. Let $Z' = E_0$ and $Z = E_t$ be the irreducible components of $\mathscr{X}_0(N) \otimes \mathbb{F}_q$ cf. §1. Then $Z \simeq Z' \simeq \mathscr{X}_0(N/q^t) \otimes \mathbb{F}_q$, see [4] VI, which are smooth over $\mathbb{F}_q$. By our assumption $g_0(N/q^t) \geqslant 1$. Then by the construction of the minimal model $\tilde{\mathscr{Y}} \dashrightarrow \mathscr{X}_0(N) \otimes \mathcal{O}_{\mathfrak{q}}$ (birational map), Z and Z' do not become points on $\tilde{\mathscr{Y}}$. Denote also by Z and Z' the proper transforms of Z and Z' by the birational map $\tilde{\mathscr{Y}} \dashrightarrow \mathscr{X}_0(N) \otimes \mathcal{O}_{\mathfrak{q}}$. Then $u(\mathbf{0}) \otimes \kappa(\mathfrak{q})$ and $u(\infty) \otimes \kappa(\mathfrak{q})$ are sections of $(Z \cup Z')^h$ $(= Z \cup Z'$-{supersingular points}), see corollary 1.14, remark 1.15 and the conditions on q as above. As $\mathbf{0} \otimes \kappa(\mathfrak{q})$ belongs to Z'^h and $\infty \otimes \kappa(\mathfrak{q})$ belongs to Z^h, so that $u(\mathbf{0}) \otimes \kappa(\mathfrak{q})$ and $u(\infty) \otimes \kappa(\mathfrak{q})$ are the sections of the different irreducible components $\subset Z \cup Z'$. Denote also by Z and Z' the images of Z and Z' under the natural morphism of $\mathscr{X}_0(N)$ to $\mathscr{X}_0(M)$. Then $\pi u(\mathbf{0}) \otimes \kappa(\mathfrak{q})$ and $\pi u(\infty)' \otimes \kappa(\mathfrak{q})$ are the sections of the different irreducible components. Hence $\pi u(\mathbf{0}) \neq \pi(u(\infty)$. □

LEMMA 2.15 (see [22, 23]). *Let $M > 1$ be an integer and p be a prime number not dividing M. Let $D = \Sigma_i n_i(x_i)$ be a divisor of $X_0(M)$ of degree $d = \Sigma_i n_i$ with $n_i \geqslant 1$. Assume that D is defined over a composite of quadratic fields and that* $\dim H^0(X_0(M), \mathcal{O}(D)) > 1$. *Then*

$$\# \mathfrak{X}_0(M)(\mathbb{F}_{p^2}) \leqslant d(p^2 - 1) - \sum_i (n_i - 1).$$

Proof. It is immediate from the upper semicontinuity, see E.G.A. IV (7.7.5) 1. □

LEMMA 2.16. *Let $p \geqslant 3$ be a prime number which satisfies one of the following conditions* (i) $\operatorname{ord}_p N \leqslant 1$, (ii) $p \geqslant 11$, *or* (iii) $p = 5$ *or* 7 *satisfies one of the conditions* (i), (ii) *in Remark 1.15. Then for any automorphism u of $X_0(N)$, if $u(\mathbf{0})$ and $u(\infty)$ are not cusps, then $u(\mathbf{0}) \otimes \bar{\mathbb{F}}_p$ or $u(\infty) \otimes \bar{\mathbb{F}}_p$ is not a cusp.*

Proof. Under the assumption on p as above, $u(\mathbf{0}) \otimes \bar{\mathbb{F}}_p$ and $u(\infty) \otimes \bar{\mathbb{F}}_p$ are the sections of the smooth part $\mathscr{X}_0(N)^{smooth}$, and u is defined over $\mathbb{Q}_p^{ur}$, see corollary 1.11, Remark 1.12, 1.15, lemma 2.5. Suppose that $u(\mathbf{0}) \otimes \bar{\mathbb{F}}_p$ and $u(\infty) \otimes \bar{\mathbb{F}}_p$ are cusps. Let C_1 and C_2 be the cusps on $\mathscr{X}_0(N)$ such that $C_1 \otimes \bar{\mathbb{F}}_p = u(\mathbf{0}) \otimes \bar{\mathbb{F}}_p$ and $C_2 \otimes \bar{\mathbb{F}}_p = u(\infty) \otimes \bar{\mathbb{F}}_p$. Consider the section x

the Néron model $J_0(N)_{/\mathbf{W}(\mathbb{F}_p)}$ defined by

$$x = cl((u(\mathbf{0})) - (u(\infty)) - (C_1) + (C_2)).$$

(Note that under the condition on p as above, C_i are defined over $\mathbb{Q}_p^{ur}$). By the choice of C_i, $x \otimes \bar{\mathbb{F}}_p = 0$. The classes $u(cl(\mathbf{0}) - (\infty)) = cl((u(\mathbf{0})) - (u(\infty)))$ and $cl((C_1) - (C_2))$ are of finite order, see [13] proposition 3.2. Then by the specialization lemma [26] §3 (3.3.2), [15] lemma 1.1, x is the unit section. If $F(N) = \mathbb{Q}$ and $N \neq 37$, then $u(\mathbf{0})$ and $u(\infty)$ are cusps, see corollary 2.9. For the case $N = 37$, see [16] §5. If $u(\mathbf{0})$ and $u(\infty)$ are not cusps and $N \neq 37$, then $X_0(N)$ must be hyperelliptic and the hyperelliptic involution sends $\mathbf{0}$ to a cusp, see [22] theorem 2. □

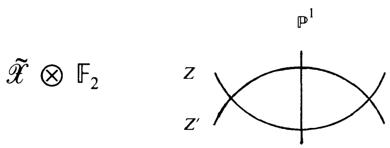
Now applying (1.17), lemma 2.13, 2.14, 2.15, 2.16, we can prove main theorem.

THEOREM 2.17. *For the modular curves $X_0(N)$ with $g_0(N) \geqslant 2$*, Aut $X_0(N) =$ $B_0(N)$, *provided* $N \neq 37, 63$.

Proof. It is enough to discuss the case $F(N) \neq \mathbb{Q}$, see remark 1.15, corollary 2.9. Suppose that Aut $X_0(N) \neq B_0(N)$. Then there exists an automorphism u of $X_0(N)$ such that $u(\mathbf{0})$ and $u(\infty)$ are not cusps, see corollary 2.4. At first, we treat the cases for $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3$. Let $l = l(N)$ be the least prime number not dividing N, and $D = D_l = (l+1)(u(\mathbf{0})) + (T_l u^\sigma(\infty)) - (l+1)(u(\infty)) - (l+1)(u(\infty)) - (T_l u^\sigma(\mathbf{0}))$ $(\neq 0)$ be the divisor of $X_0(N)$ defined in lemma 2.7 for $\sigma = \sigma_l$. Then D is defined over $F(N)$ (corollary 1.11, lemma 2.5), $0 \neq D$ and $l \leqslant 19$ by lemma 2.7, 2.13. We apply lemma 2.14. For $l = 13$, 17 and 19, applying lemma 2.14, 2.15 to $p = 2$, we see that $l \leqslant 11$. For $l = 11$, applying the above lemmas to $p = 2$, we see $N = 2 \cdot 3^2 \cdot 5 \cdot 7, 2^3 \cdot 3^2 \cdot 5 \cdot 7, 2^3 \cdot 3^2 \cdot 5 \cdot 7, 2^4 \cdot 3^2 \cdot 5 \cdot 7, 2^5 \cdot 3^2 \cdot 5 \cdot 7, 2^4 \cdot 3 \cdot 5 \cdot 7$ or $2^5 \cdot 3 \cdot 5 \cdot 7$. Further applying lemma 2.14, 2.15 to $p = 3$ and 5, we see $N \neq 2^4 \cdot 3^2 \cdot 5 \cdot 7, 2^5 \cdot 3^2 \cdot 5^7 \cdot 7, 2^5 \cdot 3 \cdot 5 \cdot 7$. For $l = 7$, the same argument as above shows that $N = 2 \cdot 3^2 \cdot 5, 2^2 \cdot 3^2 \cdot 5, 2^3 \cdot 3^2 \cdot 5, 2^4 \cdot 3 \cdot 5, 2^5 \cdot 3 \cdot 5, 2 \cdot 3^3 \cdot 5, 2^2 \cdot 3^3 \cdot 5$ or $2 \cdot 3^2 \cdot 5^2$. For $l = 5$, $N = 2^4 \cdot 3 \cdot 7, 2^4 \cdot 3 \cdot 11, 2^4 \cdot 3 \cdot 13, 2^4 \cdot 3^2 \cdot 7, 2^2 \cdot 3^2 \cdot 11, 2 \cdot 3^3 \cdot 7, 2 \cdot 3^2 \cdot 7, 2 \cdot 3^2 \cdot 11, 2 \cdot 3^2 \cdot 13, 2 \cdot 3^2 \cdot 17, 2 \cdot 3^2 \cdot 19, 2 \cdot 3^2 \cdot 23, 2^7 \cdot 3, 2^6 \cdot 3, 2^5 \cdot 3^2, 2^5 \cdot 3, 2^4 \cdot 3^2, 2^4 \cdot 3^2, 2^4 \cdot 3, 2^3 \cdot 3^2, 2^2 \cdot 3^4, 2^2 \cdot 3^3, 2 \cdot 2^4$ or $2 \cdot 3^3$. For $l = 3$, $N = 2^6, 2^7, 2^5 \cdot 5, 2^4 \cdot 5, 2^4 \cdot 7, 2^4 \cdot 13$ or $2 \cdot 5^2$. For $l = 2$, $N = 3^4, 3^2 \cdot 5, 3^2 \cdot 7, 3^2 \cdot 7, 3^2 \cdot 11, 3^2 \cdot 13, 3^2 \cdot 17, 3 \cdot 5^2, 5^3$ or $5^2 \cdot 7$. For the remaining cases, we apply lemma 2.16. Choose a prime number $p \geqslant 3$ which satisfies one of the conditions (i), (ii), (iii) in lemma 2.16, and splits in $F(N)$ for $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3$, and in $k'(N)$ for $N = 2^8, 2^9, 2^2 3^3, 2^3 3^3$ (see corollary 1.11, remark 1.12, lemma 2.5). By a calculation, we see that there is a prime number $p \geqslant 3$ as above such that $\mathscr{X}_0(N)(\mathbb{F}_p)$ consists of the cusps (and the supersingular points if $p \| N$), provided $N \neq 2^2 \cdot 3^3, 3^2 \cdot 7, 3^2 \cdot 13, 2 \cdot 5^2, 3 \cdot 5^2, 5^2 \cdot 7, 5^3$. Thus lemma 2.16 gives the result, except for $N = 2^2 \cdot 3^2, 3^2 \cdot 7, 3^2 \cdot 13$, $2 \cdot 5^2, 3 \cdot 5^2$ and 5^3.

In the following, we give the proofs for $N = 50, 75, 125, 175, 108$ and 117. Let $\tilde{\mathscr{X}} = \tilde{\mathscr{X}}_0(N) \to \operatorname{Spec} \mathbb{Z}$ be the minimal model of $X_0(N)$. For a prime divisor p of N with $p \| N$, Aut $X_0(N)$ becomes a subgroup of Aut $\tilde{\mathscr{X}} \otimes \bar{\mathbb{F}}_p$. Let Z, Z' be the irreducible components of $\tilde{\mathscr{X}}_0(N) \otimes \mathbb{F}_p$ ($p \| N$), and $\operatorname{Aut}_Z \tilde{\mathscr{X}} \otimes \bar{\mathbb{F}}_p$ be the subgroup of Aut $\tilde{\mathscr{X}} \otimes \bar{\mathbb{F}}_p$ consisting the automorphisms which fix Z (, hence fix Z'). We denote also by Z, Z' the proper transforms of Z and Z' under the quadratic transformation $\tilde{\mathscr{X}} \to \mathscr{X} = \mathscr{X}_0(N)$. For the pairs $(N, p) = (50, 2), (75, 3), (175, 7), (63, 7)$ and $(117, 13)$, $X_0(N/p) \simeq \mathbb{P}^1_{\mathbb{Q}}$. For a pair (N, p) as above, if an automorphism u fixes Z and has more than three fixed points on Z, then $u = \mathrm{id}$. For N as above and an automorphism u of $X_0(N)$, u or uw_N fixes Z and Z'. Let $J = J_0(N)$ be the jacobian variety of $X_0(N)$, and u be an automorphism of $X_0(N)$ which fixes Z for (N, p) as above.

Proof for $N = 50$: $\operatorname{Aut}_Z \tilde{\mathscr{X}} \otimes \bar{\mathbb{F}}_p \simeq \mathbb{Z}/2\mathbb{Z}$ and it is generated by the canonical involution w_{25}, see below:



Proof for $N = 75$: The set of the $\mathbb{F}_9$-rational points on Z ($\simeq \mathscr{X}_0(25) \otimes \mathbb{F}_3$) consists of the $\mathbb{F}_3$-rational cusps C_1, C_2, non cuspidal $\mathbb{F}_3$-rational points C_3, C_4, and the supersingular points. Then u acts on the set $\{C_1, C_2, C_3, C_4\}$. For $1 \neq \sigma \in \operatorname{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$, $u^\sigma(C_i) = (u(C_i))^{(3)} = u(C_i)$, where $(u(C_i))^{(3)}$ is the image of $u(C_i)$ under the Frobenius map $Z \to Z$. Then $u^{-1}u^\sigma$ has more than four fixed points on Z, so that $u^\sigma = u$. Then by lemma 2.5, 2.8, u belongs to the subgroup $B_0(75)$.

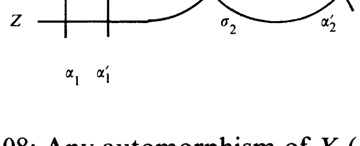
Proof for $N = 125$: Put $J_1 = J_+ = (w + 1)J$ and $J_- = (w - 1)J$, where $w = w_{125}$. Then J_- is isogenous over $\mathbb{Q}$ to a product of two $\mathbb{Q}$-simple abelian varieties J_2 and J_3 with $\dim J_2 = 4$, $\dim J_3 = 2$, see [5, 36] table 5. The abelian varieties J_1 and J_3 are simple over $\mathbb{C}$, and they are isogenous with each other over $\mathbb{Q}(\sqrt{5})$, see [18] [29]. The abelian variety J_2 is isogenous over $\mathbb{Q}(\sqrt{5})$ to a product of two abelian varieties, loc.cit. Let $V = V_J$, $V_i = V_{J_i}$ be the tangent spaces of J and J_i at the unit sections. Suppose that an automorphism u of $X_0(125)$ is not defined over $\mathbb{Q}$.

Claim $uw = wu$: Put $v = wuwu^{-1}$. Then v acts trivially on J_2, since u acts on J_2 (see above) and $w = -1$ on J_2. Suppose $v \neq$ id. Let Y be the quotient $X_0(125)/\langle v\rangle$ with genus g_Y, and $(2 \leqslant)d$ be the degree of v. Then $g_Y \geqslant 4$ and the Riemann–Hurwitz formula yields $d = 2$ and $g_Y = 4$. Thus v acts on $V_1 \oplus V_2$ under -1, hence $v = -1$ on $J_1 + J_2$. Then $v(\neq w)$ is defined over $\mathbb{Q}$. But the non trivial automorphism of $X_0(125)$ defined over $\mathbb{Q}$ is w, proposition 2.8.

The above claim shows that the action of u is compatible with the decomposition $V = V_1 \oplus V_2 \otimes V_3$, hence with $J = J_1 + J_2 + J_3$. Put $v = u^\sigma u^{-1}$ ($\neq$ id.) for $1 \neq \sigma \in \mathrm{Gal}\,(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$. Let Y be the quotient $X_0(125)/\langle v\rangle$ with genus g_Y, and $(2 \leqslant)$d be the degree of v. As noted as above, all endomorphisms of J_1 and J_3 are defined over $\mathbb{Q}$, so that v acts trivially on $J_1 + J_3$. Then the Riemann–Hurwitz formula shows that $d = 2$ and $g_Y = 4$. Then $v = -1$ on J_2, and v is defined over $\mathbb{Q}$. But $w \neq v$.

Proof for $N = 175$: Let $\alpha_i, \alpha_i' = \alpha_i^{(7)}$ $(1 \leqslant i \leqslant 8)$ be the supersingular points on $\mathscr{X}_0(175) \otimes \mathbb{F}_7$. Let E $(/\bar{\mathbb{F}}_7)$ be an elliptic curve with modular invariant $j(E) = 1728$, and A, A' be the independent cyclic subgroups of order 25 which are fixed by Aut $E \simeq \mathbb{Z}/4\mathbb{Z}$. Then $(E, A') \simeq (E/A, E_{25}/A)$, and the pairs (E, A), (E, A') represent the supersingular points, say α_1 and α_1', and $w_{25}(\alpha_1) = \alpha_1'$, $u(\{\alpha_1, \alpha_1'\}) = \{\alpha_1, \alpha_1'\}$, see below. Since u and w_{25} fix the irreducible components Z and Z', $v = u$ or w_{25} fixes α_1, α_1' and Z. Let T be the subgroup of Aut Z $(\simeq \mathrm{PGL}_2)$ consisting of automorphisms which fix α_1, α_1'. Then T is the non split torus. If v does not belong to the subgroup $B_0(175)$, then u is not defined over $\mathbb{F}_7$, and the order of v is 16 or divisible by 3, see lemma 2.5, proposition 2.8. In both cases as above, v acts on the set $\{\alpha_i, \alpha_i'\}_{2 \leqslant i \leqslant 8}$. Then v have more than three fixed points on Z. Therefore $v =$ id., and it contradicts to our assumption.

$\tilde{\mathscr{X}} \otimes \mathbb{F}_7$



Proof for $N = 108$: Any automorphism of $X_0(108)$ is defined over the class field $k' = k(108)'$ of $\mathbb{Q}(\sqrt{-3})$, see Remark 1.12. The rational prime 31 splits in k', and $\mathscr{X}(\mathbb{F}_{31})$ consists of the cusps C_i ($1 \leqslant i \leqslant 18$) and non cuspidal points x_i ($1 \leqslant i \leqslant 18$). Let u be an automorphism of $X_0(108)$. If u is defined over $\mathbb{Q}(\sqrt{-3})$, applying lemma 2.16 to $p = 7$, we see that u belongs to $B_0(108)$. Suppose that u is not defined over $\mathbb{Q}(\sqrt{-3})$, and let $1 \neq \sigma \in \mathrm{Gal}\,(k'/\mathbb{Q}(\sqrt{-3}))$. Applying lemma 2.16 to $p = 7$, we see that $\#\,\{\{u(C_i)\}_i \cap \{C_i\}_i\} \leqslant 1$ and $\#\,\{\{u^\sigma(C_i)\}_i \cap \{C_i\}_i\} \leqslant 1$, see corollary 2.4. Then $\#\,\{\{u(C_i)\}_i \cap \{u^\sigma(C_i)\}_i\} \geqslant 16$, hence $\#\,\{\{u^\sigma u^{-1}(C_i)\}_i \cap \{C_i\}_i\} \geqslant 16$. Put $\gamma = u^\sigma u^{-1}$ ($\neq$id.). Then there are cusps P_1, P_1', P_2, P_2' such that $\gamma(P_1) \otimes \mathbb{F}_{31} = P_1' \otimes \mathbb{F}_{31}$ and $\gamma(P_2) \otimes \mathbb{F}_{31} = P_2' \otimes \mathbb{F}_{31}$. Consider the section $x = cl((\gamma(P_1)) - (\gamma(P_2)) - (P_1') + (P_2'))$ of the jacobian variety $J = J_0(108)$. Then x is of finite order [13] proposition 3.2, and $x \otimes \mathbb{F}_{31}$ is the unit section. By the specialization lemma [26] §3 (3.3.2), [15] lemma 1.1, x is the unit section, so that $\gamma(P_i)$ are cusps, since $X_0(108)$ is not hyperelliptic [22]. Therefore γ belongs to $B_0(108)$, see corollary 2.4. Let J_C be the abelian subvariety ($/\mathbb{Q}$) of J with complex multiplication, and J_H be the abelian subvariety ($/\mathbb{Q}$) without complex multiplication. Then $\dim J_C = 6$ and $\dim J_H = 4$ [36] table 5. All endomorphisms of J_H are defined over $\mathbb{Q}(\sqrt{-3})$ (proposition 1.3), so that $\gamma =$ id. on J_H. Let Y be the quotient $X_0(108)/\langle\gamma\rangle$ with genus $g_Y \geqslant 4$, and $(2 \leqslant)d$ be the degree of γ. The Riemann–Hurwitz formula shows that (i) $d = 2, g_Y = 4, 5$ or (ii) $d = 3, g_Y = 4$. Let J_{C_1} (resp. J_{C_2}) be the abelian subvariety ($/\mathbb{Q}$) of J_C associated with the eigen forms of T_l ($l \times 6$) which have same eigen values with the new forms of level 36 and 108 (resp. 27). Then $J_C = J_{C_1} + J_{C_2}$, $\dim J_{C_1} = \dim J_{C_2} = 3$, and $\mathrm{End}_{\mathbb{Q}(\sqrt{-3})} J_C \otimes \mathbb{Q} \simeq \mathrm{End}\, J_{C_1} \otimes \mathbb{Q} \times \mathrm{End}\, J_{C_2} \otimes \mathbb{Q}$, where $\mathrm{End}_{\mathbb{Q}(\sqrt{-3})}$ is the subring consisting of endomorphisms defined over $\mathbb{Q}(\sqrt{-3})$.

sign of the eigen values of (w_4, w_{27})	$+\,+$	$+\,-$	$-\,+$	$-\,-$	
	1	1	1	1	J_H
dimensions of	0	0	$1 + 1$	1	J_{C_1}
the factors	0	$1 + 1$	0	1	J_{C_2}

The automorphism γ acts trivially on J_H, w_4 acts on J_{C_1} under -1, and w_{27} acts on J_{C_2} under -1. Then $\dim \ker\,(w_m\gamma w_m\gamma^{-1} - 1\colon J \to J) \geqslant 7$ for $m = 4$ and 27. Then the Riemann–Hurwitz formula shows that $\gamma w_4 = w_4\gamma$ and $\gamma w_{27} = w_{27}\gamma$. Put $E = (w_{27} - 1)J_{C_1}$, which is an elliptic curve ($/\mathbb{Q}$) with conductor 36, see above. Then γ acts on E under ± 1. Therefore the second case (ii) as above does not occur. In the first case, $\dim\,(w_m\gamma + 1)J \geqslant 6$ for $m = 4$, 27 or 108, see the above table. The same argument as above yields $\gamma = w_m$ for $m = 4$, 27 or 108. But w_m do not act trivially on J_H, see above, Thus we get a contradiction.

For points x_i, $1 \leqslant i \leqslant r$, let $\mathrm{Aut}_{(x_i)} Z$ be the subgroup of Aut Z consisting of automorphisms which fix x_i's.

Proof for $N = 117$: Let α_i, $\alpha_i' = \alpha_i^{(13)}$ $(1 \leqslant i \leqslant 6)$ be the supersingular points on $\mathscr{X}_0(117) \otimes \mathbb{F}_{13}$. The subgroup $B_0(117) \cap \mathrm{Aut}_Z \tilde{\mathscr{X}} \otimes \mathbb{F}_{13}$ acts transitively on the set $\{\alpha_i, \alpha_i'\}_{1 \leqslant i \leqslant 6}$. There are two pairs of the supersingular points, say $\{\alpha_1, \alpha_1'\}$ and $\{\alpha_2, \alpha_2'\}$, such that $\alpha_1' = w_9(\alpha_1)$ and $\alpha_2' = w_9(\alpha_9)$. For any $u \in \mathrm{Aut}\, X_0(117) \cap \mathrm{Aut}_Z \tilde{\mathscr{X}} \otimes \mathbb{F}_{13}$, there is an automorphism $\gamma \in B_0(117)$ such that $v = u\gamma$ fixes Z, α_1 and α_1'. Note that any automorphism of $X_0(117)$ is defined over $\mathbb{Q}(\sqrt{-3})$ cf. lemma 2.5. The subgroup $T = \mathrm{Aut}_{(\alpha_1, \alpha_1')} Z$ is the non split torus, and v belongs to $T(\mathbb{F}_{13}) \simeq \mathbb{Z}/14\mathbb{Z}$. If the order of v is divisible by 7, then v^2 acts on the set $\{\alpha_i, \alpha_i'\}_{2 \leqslant i \leqslant 6}$, and it has the other fixed points α_i, α_i' for an integer $i \geqslant 2$. Therefore $v^2 = \mathrm{id}$. The automorphisms $w_{13} v w_{13} v$ and $w_9 v w_9 v$ fix Z and α_1, α_1', since $w_{13}(\alpha_i) = \alpha_i'$. If $v \neq \mathrm{id.}$, then $T \cap \mathrm{Aut}\, X_0(117) = \langle v \rangle$, see above. Therefore v commutes with w_9 and w_{13}. For $1 \neq \sigma \in \mathrm{Gal}\,(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$ and $m = 9, 13$, $v^\sigma w_m = (v w_m)^\sigma = w_m v^\sigma$. For $\varepsilon, \varepsilon' = \pm$, put $J_{\varepsilon,\varepsilon'} = (w_9 + \varepsilon 1)(w_{13} + \varepsilon' 1) J$. Then we have the following table cf. [36] table 5.

$(\varepsilon, \varepsilon')$	$+\,+$	$+\,-$	$-\,+$	$-\,-$
$\dim J_{\varepsilon,\varepsilon'}$	2	$1 + 2$	$2 + 2$	$1 + 1$
$\dim (J_{\varepsilon,\varepsilon'})^{\mathrm{new}}$	0	2	2	1

The old part J^{old} of J is isogenous to $J_0(39) \times J_0(39)$ [1], so that the $\mathbb{Q}$-simple factors of J^{old} have multiplicative reduction at the rational prime 3 and 13 [4], and the ring of endomorphisms of such a factor is generated by Hecke operators [18] [29]. Let $\gamma_j = \left(\begin{smallmatrix} 1 & j/3 \\ 0 & 1 \end{smallmatrix}\right) \bmod \Gamma_0(117)$, which commutes with w_{13}. Then the twisting operator $\eta = \gamma_1 - \gamma_2$ acts on $(w_{13} + 1) J = J_{++} + J_{-+}$ [35] §4, [18, 29]. Since $\eta(J_{++})$ does not have multiplicative reduction at the rational prime 3 [18, 29], J_{-+} is isogenous over $\mathbb{Q}$ to the product $J_{++} \times \eta(J_{++})$. Put $J_{+-} = A_{+-} + E_{+-}$ for $\mathbb{Q}$-rational abelian subvariety A_{+-} of dimension two and an elliptic curve E_{+-}. Then we see that η acts on A_{+-} (see above table) and that A_{+-} is isogenous to a product to two elliptic curves. We here note that any abelian subvariety of J has multiplicutive reduction at 13 [4] (above table). Now consider the automorphisms u and v. If $v = \mathrm{id.}$, the u belongs to $B_0(117)$. Suppose $v \neq \mathrm{id.}$.

Claim: The action of v on $J_{++} + J_{+-}$ is $\mathbb{Q}$-rational: As noted as above, v acts $\mathbb{Q}$-rationally on J_{++} and E_{+-}, so that v acts on J_{++} and E_{+-} under ± 1. Denote also by v the involution of $X_+ = X_0(117)/\langle w_9 \rangle$ (Note that v

commutes with w_9). Let $\mathscr{X}_+ \to \operatorname{Spec} \mathbb{Z}$ be the minimal model of X_+, and β_i = image of $\{\alpha_i, \alpha_i'\}$ ($i = 1, 2$) be the $\mathbb{F}_{13}$-rational supersingular points of $\mathscr{X}_+ \otimes \mathbb{F}_{13}$. The other supersingular points on $\mathscr{X}_+ \otimes \mathbb{F}_{13}$ are not defined over $\mathbb{F}_{13}$. By lemma 2.5, v is defined over $\mathbb{Q}(\sqrt{-3})$, so that $v \otimes \mathbb{F}_{13}$ is defined over $\mathbb{F}_{13}$. As v fixes β_1, so that v fixes also β_2, and does not fix the other supersingular points. Let Σ be the dual graph of the special fibre $\mathscr{X}_+ \otimes \bar{\mathbb{F}}_{13}$. Then $\mathrm{H}^1(\Sigma, \mathbb{Z}) \otimes \mathbb{G}_m$ is canonically isogenous to the connected component of $J_{+/\mathbb{Z}} \otimes \mathbb{F}_{13}$ of the unit section, where J_+ is the jacobian variety of X_+ [4] VI, [25] §8 (8.1). Denote also by v the involution of $\mathscr{X}_+ \otimes \mathbb{Z}_{13}$ induced by v. The action of v on $\mathrm{H}^1(\Sigma, \mathbb{Z})$ is represented by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The jacobian variety J_+ is canonically isomorphic to $(w_9 + 1)J$, since the double covering $X_0(117) \to X_+$ has ramification points. Then $(v + 1)(w_9 + 1)J$ is of dimension three. As noted as above, v acts on J_{++}, A_{+-} and E_{+-}, and it acts under ± 1 on J_{++} and E_{+-}. If $v = -1$ on J_{++}, then $v = \text{id.}$ on $J_{+-} = A_{+-} + E_{+-}$ (see above representation). Then v acts $\mathbb{Q}$-rationally on $(w_9 + 1)J = J_{++} + J_{+-}$. Now consider the case $v = \text{id.}$ on J_{++}. If v acts trivially on E_{+-}, then v acts on A_{+-} under -1, and its action is $\mathbb{Q}$-rational. Now suppose that $v = -1$ on E_{+-}. Then $(v + 1)A_{+-}$ is an elliptic curve. The involution vw_{13} acts trivially on $J_{++} + E_{+-}$, and $(vw_{13} + 1)A_{+-}$ is an elliptic curve. Then the Riemann–Hurwitz formula gives a contradiction.

The above claim shows that v acts $\mathbb{Q}$-rationally on $X_+ = X_0(117)/\langle w_9 \rangle$. Let C_i, $w_9(C_i)$ ($1 \leqslant i \leqslant 4$) be the cusps on $X_0(117)$, and D_i = image of $\{C_i, w_9(C_i)\}$ be the ($\mathbb{Q}$-rational) cusps on X_+. As $\mathscr{X}_+(\mathbb{F}_5)$ consists of the cusps $D_i \otimes \mathbb{F}_5$ cf. [4] VI 3.2, so that v sends the set $\{D_i \otimes \mathbb{F}_5\}_i$ to itself. Then v sends the set $\{C_i \otimes \mathbb{F}_5\}_i$ to itself. Therefore by the lemma 2.16, we see that v, hence u also, belongs to $B_0(117)$. □

We add a result on Aut $X_0(63)$ below. It seems that Aut $X_0(63)$ will be determined by using the defining equation of $X_0(63)$ with an explicit representation of $B_0(63)$.

PROPOSITION 2.18. *The index of* $B_0(63)$ *in* Aut $X_0(63)$ *is one or two. If* Aut $X_0(63) \neq B_0(63)$, *then there exists an automorphism* u *such that* $u^2 = w_9$, $w_7 u = w_7 u$. *The representation of* Aut $X_0(63)$ *on the tangent space of* $J_0(63)$ *is as follows*:

$$\begin{pmatrix} 1 & 1/3 \\ 0 & 1 \end{pmatrix} \bmod \Gamma_0(63) = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\left(u = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix} \right)$$

$$w_9 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \quad w_7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Proof. The modular curve $Z \simeq \mathscr{X}_0(9) \otimes \mathbb{F}_7$ is defined by the equation

$$j - 1728 = \frac{\{(t^2 - 3)(t^2 - 2t + 3)(t^2 + t + 3)\}^2}{t(t^2 + 3t + 3)}$$

with $w_9 * (t) = 3/t$ [6] IV §2. The cusps are defined by C_∞: $t = 0$, C_0: $t = \infty$, C_1: $t = 1$, C_2: $t = 3$. Let γ_∞ be the automorphism of $X_0(63)$ represented by the matrix $(\begin{smallmatrix} 1 & 1/3 \\ 0 & 1 \end{smallmatrix})$ (or $(\begin{smallmatrix} 1 & -1/3 \\ 0 & 1 \end{smallmatrix})$). Then $\gamma_\infty * (t) = t/(t + 4)$, since $\gamma_\infty(C_\infty) = C_\infty$, $\gamma_\infty(C_0) = C_1$ and $\gamma_\infty(C_1) = C_2$. Let α_i, $\alpha_i' = \alpha_i^{(7)}$ be the supersingular points on Z defined by α_1: $t = 2\sqrt{-1}$, $\alpha_2 = \gamma_\infty(\alpha_1)$ and

$\alpha_3 = \gamma_\infty(\alpha_2)$. Then w_9 fixes α_1 and α'_1, and exchanges α_i with α'_i for $i = 2, 3$. On $\mathscr{X} \otimes \mathbb{F}_7 = \mathscr{X}_0(63) \otimes \mathbb{F}_7$, w_7 exchanges α_i with α'_i for $i = 1, 2, 3$. The automorphism groups of the objects associating to the points α_i, α'_i are all $\{\pm 1\}$, so that $\mathscr{X} \otimes \mathbb{Z}_7 \to \operatorname{Spec} \mathbb{Z}_7$ is the minimal model of $X_0(63) \otimes \mathbb{Q}_7$, see [4] VI §6. For any $u \in \operatorname{Aut} X_0(63) \cap \operatorname{Aut} Z$, there exists an element $\gamma \in B_0(63)$ such that $v = \gamma u$ fixes Z, Z', α_1 and α'_1. The subgroup $T = \operatorname{Aut}_{(\alpha_1, \alpha'_1)} Z$ is the non split torus, and w_9 belongs to $T(\mathbb{F}_7) \simeq \mathbb{Z}/8\mathbb{Z}$. Note that for any automorphisms g of $X_0(63)$, $g \otimes \mathbb{F}_7$ is defined over $\mathbb{F}_7$, see lemma 2.5. The automorphism v acts on the set $\{\alpha_2, \alpha'_2, \alpha_3, \alpha'_3\}$, and it has no fixed point on this set if $v \neq \mathrm{id}$. Therefore the order of v divides 4. If v is of order four, then for $w = v$ or v^{-1}, $w*(t) = (2t + 4)/(-t + 2)$, $w(\alpha_2) = \alpha_3$, $w(\alpha_3) = \alpha'_2$ and $v^2 = w_9$. Let Σ be the dual graph of the special fibre $\mathscr{X} \otimes \mathbb{F}_7$, and e_{2i-1}, e_{2i} $(1 \leqslant i \leqslant 3)$ be the paths which are associated with the points α_i and α'_i with the orientation from Z to Z'. The representation of the automorphisms on $\mathrm{H}^1(\Sigma, \mathbb{Z})$ for the basis $x_i = e_{i+1} - e_1$ $(1 \leqslant i \leqslant 5)$ is as follows:

$$\left(v \text{ or } v^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \; v^2 = w_9 \right) w_9 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$w_7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 & 0 \end{pmatrix}, \quad \gamma_\infty = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \end{pmatrix}.$$

Then $w_7 v = v w_7$. Put $J_{\varepsilon, \varepsilon'} = (w_9 + \varepsilon 1)(w_7 + \varepsilon' 1) J$ for $\varepsilon, \varepsilon' = \pm$. Then we have the following table [36] table 5.

$(\varepsilon, \varepsilon')$	$+\,+$	$+\,-$	$-\,+$	$-\,-$
$\dim J_{\varepsilon, \varepsilon'}$	1	2	1 + 1	0
$\dim (J_{\varepsilon, \varepsilon'})^{\text{new}}$	0	2	1	0

The abelian subvariety J_{+-} is isogenous over $\mathbb{Q}(\sqrt{-3})$ to a product of two elliptic curves. Note that any abelian subvariety of $J = J_0(63)$ has multiplicative reduction at the rational prime 7. Changing the basis (from $\{x_i\}_{1 \leqslant i \leqslant 5}$ to $\{x_i' = 2x_1 + \Sigma_{i=2}^{5} x_i, x_2' = x_2 + x_3, x_3' = x_4 + x_5, x_4' = x_2 - x_3, x_5' = x_4 - x_5\}$), we get the representation as in this proposition. □

REMARK 2.19. Let $\Gamma = \Gamma(3) \cap \Gamma_0(7)$ be the modular group, and X_Γ be the modular curve $/\mathbb{Q}(\sqrt{-3})$ associated with Γ:

$$\Gamma = \left\{ \begin{pmatrix} a & d \\ c & d \end{pmatrix} \in \Gamma_0(7) | a - 1 \equiv b \equiv c \equiv d - 1 \equiv 0 \bmod 3 \right\}.$$

Then X_Γ is isomorphic to $X_0(63)$ over $\mathbb{Q}(\sqrt{-3})$, since $\Gamma_0(63) = \langle g^{-1}\Gamma g, \pm 1 \rangle$ for $g = \left(\begin{smallmatrix} 3a & b \\ 21c & 3d \end{smallmatrix}\right)$ for integers a, b, c, d with $3ad - 7bc = 1$. Let $B = B_\Gamma$ be the subgroup of Aut X_Γ generated by 2×2 matrices, and H be the subgroup generated by the elements $g \in \Gamma_0(7)$ with $g \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)$ mod 3. Then H is a normal subgroup of Aut X_Γ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ cf. proposition 2.18. Let $Y = X_\Gamma/H$ be the modular group (, $\to X_0(1)$), which is of genus two. Then the function field of Y is generated by the functions x and y with the relations:

$$yx^3 = y^2 + 13y + 49, \quad \text{and} \quad \sqrt[3]{j} = x(y^2 + 5y + 1)$$

see [6] IV §2. Using the minimal model of Y over the base $\mathbb{Z}_7$, by the similar argument as in the proof of the proposition 2.18, we see that the index of the subgroup B/H in Aut Y is two. Further we see that exists an automorphism g of Y which is not represented by any 2×2 matrix defined by

$$g*(x) = -3/x, \quad g*(y) = \lambda \frac{y - \bar{\lambda}}{y - \lambda},$$

for λ, $\bar{\lambda}$ with $\lambda + \bar{\lambda} = -13$, $\lambda\bar{\lambda} = 49$, see loc. cit.. Further if $B_0(63) \neq$ Aut $X_0(63)$, then Aut $Y = \{\text{Aut } X_0(63)\}/H$.

References

1. A.O.L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* 1985 (1970) 134–160.
2. Z.I. Borevich and I.R. Safarevich, *Number Theory*, Academic Press, New York and London (1966).

3. P. Deligne, Formes modulaires et représentation l-adiques, Sém. Bourbaki 1968/69, exposé n°355, *Lecture Notes in Math.* 189 (1971).
4. 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.
5. K. Doi and M. Yamauchi, On the Hecke operators for $\Gamma_0(N)$ and class fields over quadratic fields, *J. Math. Soc. Japan* 25 (1973) 629–643.
6. R. Fricke, *Die Elliptischen Functionen und ihre Anwendungen*, Leipzig-Berlin, Teubner 1922.
7. M.A. Kenku, The modular curve $X_0(39)$ and rational isogeny, *Math. Proc. Cambridge Philos. Soc.* 85 (1979) 21–23.
8. M.A. Kenku, The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny, *Math. Proc. Cambridge Philos.* 87 (1980) 15–20.
9. M.A. Kenku, The modular curve $X_0(169)$ and rational isogeny, *J. London Math. Soc.* (2), 22 (1981) 239–244.
10. 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.
11. M.A. Kenku, Rational torsion points on elliptic curves defined over quadratic fields, to appear.
12. S. Lang, *Elliptic Functions*. Addison-Wesley, Reading Math.
13. Y. Manin, Parabolic points and zeta functions of modular forms, Math. *USSR-Izvestija*, Vol. 6, No. 1 (1972) 19–64.
14. B. Mazur, Modular curves and the Eisenstein ideals, *Publ. Math. I.H.E.S.* 47 (1977).
15. B. Mazur, Rational isogenies of prime degree, *Inv. Math.* 44 (1978) 129–162.
16. B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Inv. Math.* 25 (1974) 1–61.
17. J.F. Mestre, Points rationnels de la courbe modulaire $X_0(169)$, *Ann. Inst. Fourier, Grenoble* 30, 2 (1980) 17–27.
18. F. Momose, On the l-adic representations attached to modular forms, *J. Facult. Sci. Univ. Tokyo*, Vol. 28, No. 1 (1981) 89–109.
19. F. Momose, Rational points on the modular curves $X_{\mathrm{split}}(p)$, *Comp. Math.* 52 (1984) 115–137.
20. F. Momose, Rational points on the modular curves $X_0(p^r)$, *J. Facult. Sci. Univ. Tokyo*, 33 (1986) 585–631.
21. F. Momose, p-torsion points on elliptic curves defined over quadratic fields, *Nagoya Math. J.* Vol. 96 (1984), 139–165.
22. A. Ogg, Hyperelliptic modular curves, *Bull. Soc. Math. France* 102 (1974) 449–462.
23. A. Ogg, Über die Automorphismengruppe von $X_0(N)$, *Math. Ann.* 228 (1977) 279–292.
24. F. Oort and J. Tate, Group schemes of prime order, *Ann. Scient. Ec. Norm. Sup.* série 4, 3 (1970), 1–21.
25. M. Raynaud, Spécialisation du foncteur de Picard, *Publ. Math. I.H.E.S.* 38 (1970) 27–76.
26. M. Raynaud, Schémas en groupes de type $(p, \ldots, p)$ *Bull. Soc. Math. France* 102 (1974) 241–280.
27. K.A. Ribet, Endomorphisms of semi-stable abelian varieties over number fields, *Ann. Math.* 101 (1975) 555–562.
28. K.A. Ribet, On l-adic representations attached to modular forms, *Inv. Math.* 28 (1975) 245–275.
29. K.A. Ribet, Twists of modular forms and endomorphisms of abelian varieties, *Math. Ann.* 253 (1980) 43–62.
30. J.B. Rossor and L. Schoenfeld, Approximate formula for some functions of prime numbers, *Illinois J. Math.* Vol. 6 (1962) 64–94.

31. J.P. Serre, Propriétés galoissiennes des points d'ordre fini des courbes elliptiques, *Inv. Math.* 15 (1972) 259–331.
32. J.P. Serre and J. Tate, Good reduction of abelian varieties, *Ann. Math.* 88 (1968) 429–517.
33. G. Shimura, Introduction to the Arithmetic theory of Automorphic functions, *Publ. Math. Soc.* No. 11, Tokyo-Princeton 1970.
34. G. Shimura, On elliptic curves with complex multiplication as factors of the jacobians of modular function fields, *Nagoya Math. J* 43 (1971) 199–208.
35. G. Shimura, On the factors of jacobian variety of a modular function field, *J. Math. Soc. Japan* 25 (1973) 525–544.
36. Modular functions of one variable IV, *Lecture Notes in Math.* 476.