COMPOSITIO MATHEMATICA

FUMIYUKI MOMOSE

Isogenies of prime degree over number fields

Compositio Mathematica, tome 97, n° 3 (1995), p. 329-348
<http://www.numdam.org/item?id=CM_1995__97_3_329_0>

Compositio Mathematica **97**: 329–348, 1995.

Isogenies of prime degree over number fields

FUMIYUKI MOMOSE

Department of Mathematics, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112, Japan

Received 19 August 1993; accepted in final form 24 December 1993

1. Introduction

We discuss the isogenies of prime degree of elliptic curves defined over algebraic number fields (cf. [Se]). For the field $\mathbf{Q}$ of rational numbers, Mazur [Ma2] solved it, completely. He also solved this problem for imaginary quadratic fields k and the prime numbers p which *remain prime* in k. In the latter case, he showed that for a given imaginary quadratic field k, there are no isogenies of prime degree p defined over k except for finitely many prime numbers p as above. An isogeny $\varphi: E \to F$ of degree p corresponds to a non-cuspidal k-rational point $(E, \ker(\varphi))$ on the modular curve $X_0(p)$ (cf. [D-R], [Ma1,2]). For a given imaginary quadratic field k of class number one and for a rational prime p which *splits* or *ramifies* in k, we have isogenies of degree p which are represented by elliptic curves with complex multiplication by $\mathcal{O}_k$ defined over k. We call a point x on $X_0(p)$ is a C.M. point if x is represented by an elliptic curve with complex multiplication. Let $\mathcal{O}$ be an order of an imaginary quadratic field L, and $H = H_{\mathcal{O}}$ be the ring class field associated with the order $\mathcal{O}$ with degree $h = h_{\mathcal{O}} = [H:L]$ (cf. [La1]). Then there are h isomorphism classes of elliptic curves E over H with ring $\mathrm{End}(E)$ of endomorphisms isomorphic to $\mathcal{O}$. If a rational prime p splits or ramifies in L, then E with a level p structure defines a C.M. point belonging to $X_0(p)(H)$. Therefore, if an algebraic number field k contains the Hilbert class field H_L of an imaginary quadratic field L, then $X_0(p)(k)$ contain non cuspidal points for the primes p as above. So, we set our problem as follows: Find a finite set $S = S(k)$ of prime numbers p such that the sets $X_0(p)(k)$ consist of the cusps 0 and ∞, and the *C.M. points* for prime numbers p not belonging to S. For arbitrary algebraic number field k of finite degree, we classify the non cuspidal k-rational points on the series of the modular curves $X_0(p)$ into three cases for the prime numbers p larger than an effective constant.

Let x be a non cuspidal k-rational point on $X_0(p)$ which is represented by a pair (E, V) for an elliptic curve E and a subgroup V of order p defined over k (cf. [D-R], §VI, Prop. 2). We denote it by $x = (E, V)_{/k}$. Let λ be the

character of $G_k = \mathrm{Gal}(\bar{k}/k)$ induced by the Galois action on $V(\bar{k})$. Then λ is called the isogeny character of $(E, V)_{/k}$ (cf. [Ma2]), and λ^{12} is independent of the choice of the representative $(E, V)_{/k}$ of x.

THEOREM A. *There exists an effective constant C_0 depending only on k such that for any prime $p > C_0$, the non cuspidal k-rational point on $X_0(p)$ is one of the following three types*:

Type 1 λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified.*
Type 2 $\lambda^{12} = \theta_p^6$ *and* $p \equiv 3 \pmod 4$.
Type 3 *k contains an imaginary quadratic field L and its Hilbert class field H_L. The rational prime p splits in L*

$$p\mathfrak{o}_L = \mathfrak{p}\bar{\mathfrak{p}}.$$

For any prime $\mathfrak{q}$ of k prime to $\mathfrak{p}$,

$$\lambda^{12}(\sigma_\mathfrak{q}) \equiv \alpha^{12} \pmod{\mathfrak{p}}$$

for any $\alpha \in L^\times$ with $\alpha\mathfrak{o}_L = N_{k/L}(\mathfrak{q})$.

For the estimate of the constant C_0, see the proof of Theorem 1. For the case of Type 1, we can apply the result of *formal immersion* of Kamienny [Ka1,2] for the algebraic number fields of degree $\leqslant 8$. For the case of Type 2 and quadratic fields k, a modification of Goldfeld's theorem ([Ma2] Appendix) can be applied.

THEOREM B. *Let k be a quadratic field which is not an imaginary quadratic field of class number one. Then the non cuspidal k-rational points on $X_0(p)$ appear only for finitely many prime numbers p.*

For each quadratic field k in Theorem B, the finite set of the exceptional prime numbers is effectively estimated, except for at most one prime number. This prime, if exists, concerns with the Siegel's zero of the L-functions of quadratic characters (cf. [Ma2] Appendix). Under the Goldfeld conjecture ([Ma2] Appendix), the case of Type 2 is solved for any algebraic number field of *odd* degree (cf. Theorem 6). The k-rational points of Type 3 are expected to be the C.M. points for almost all prime numbers p. But, even for the imaginary quadratic field k of class number one, we have not solved this case. We add a result under a strong condition on reduction. The classification of algebraic points on $X_0(p)$'s can be applied to some other cases. The condition on the reduction as above is satisfied for the *fine* objects of the Shimura curves over $\mathbf{Q}$ etc. of Type 3. We will

describe the results for the *fine* objects of the Shimura varieties in the next paper.

NOTATION. For a fractional ideal $\mathfrak{a}$ of an algebraic number field k of finite degree, $\mathbf{N}(\mathfrak{a})$ as its norm $N_{k/\mathbf{Q}}(\mathfrak{a})$ and $I_k(\mathfrak{a})$ (resp. $P_k(\mathfrak{a})$) is the ideal group consisting of the ideals (resp. principal ideals) prime to $\mathfrak{a}$. For a finite extension k of $\mathbf{Q}$ or $\mathbf{Q}_p$, o_k is the ring of integers of k, and for a prime ideal $\mathfrak{q}$ of o_k, $\kappa(\mathfrak{q}) = o_k/\mathfrak{q}$. For an elliptic curve E over k, $E_{/o_k}$ is the Néron model of E over Spec o_k.

2. Classification of algebraic points

For each prime number $p \geqslant 5$, let $X_0(p)$ be the modular curve over $\mathbf{Q}$ which is associated with the elliptic modular group $\Gamma_0(p)$. The affine open subscheme $X_0(p)\backslash\{\text{cusps } 0, \infty\}$ is the coarse moduli space of elliptic curves E with a cyclic subgroup V of order p (cf. [D-R]). For any field k of $\mathrm{char}(k) \neq p$, any non cuspidal k-rational point x is represented by a pair (E, V) defined over the field k (cf. [D-R], §VI, Prop. 3.2). Let k be an algebraic number field of finite degree, and $x = (E, V)_{/k}$ be a non cuspidal k-rational point on $X_0(p)$. Denote by λ the isogeny character which is induced by the Galois action on $V(\bar{k})$:

$$\lambda : G_k = \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}\, V(\bar{k}) = \mathbf{F}_p^{\times}.$$

The character λ^{12} is unramified outside of $\mathrm{Supp}(p)$ (cf. [Mf] p. 46). The character λ^n is independent of the choice of the representative $(E, V)_{/k}$ for $n = |\mathrm{Aut}_{\mathbf{C}}(E, V)|$ ($n = 2, 4$ or 6, and $n = 2$ unless the modular invariant $j(E) = 0$ or 1728). Denote also by λ^{12}, the corresponding character of the ideal group $I_k(p)$ consisting of the ideals of k prime to p. By the classification of the finite flat group schemes (cf. [O-T], [Ra1]) and the theory of the Tate models, we have the following lemma. This lemma is also valid even if the rational prime p ramifies in k.

LEMMA 1. *Assume that k is a Galois extension of $\mathbf{Q}$ and that the rational prime p is unramified in k. Then for a fixed prime $\mathfrak{p}$ of k lying over p, we have integers a_σ, $0 \leqslant a_\sigma \leqslant 12$, for $\sigma \in \mathrm{Gal}(k/\mathbf{Q})$ such that*

$$\lambda^{12}((\alpha)) \equiv \alpha^{\varepsilon} \pmod{\mathfrak{p}}$$

for $\varepsilon = \Sigma_\sigma a_\sigma \sigma$ and $\alpha \in k^{\times}$ prime to p.

Proof. We denote also by λ^{12} the character of the idèle group of k which corresponds to the character λ^{12} of the ideal group $I_k(p)$. We may assume

$p \geqslant 5$. Let $\mathfrak{P}$ be a prime of k lying over the rational prime p, and $\lambda_{\mathfrak{P}}$ be the restriction of λ to the group of units of $k_{\mathfrak{P}}$. Denote by F the maximal unramified extension $k_{\mathfrak{P}}^{unr}$ of $k_{\mathfrak{P}}$. Then $E \otimes F$ has semistable reduction over a cyclic extension K of degree e dividing 12 (cf. [Mf] p. 46). Using the classification of the finite flat group schemes (cf. [O-T], [Ra1]) and the Tate module (cf. loc. cit.), we see that

$$\lambda_{\mathfrak{P}}(\alpha)^{12} \equiv N_{k_{\mathfrak{P}}/\mathbf{Q}_p}(\alpha)^{a_{\mathfrak{P}}} \pmod{\mathfrak{P}}$$

for a positive divisor $a_{\mathfrak{P}}$ of 12. Rewriting it in the classical form, we get this lemma.

REMARK 1. The integers $a_{\mathfrak{P}}$'s take the values 0, 12; 4, 8 (only if the modular invariant $j(E) \equiv 0 \pmod{\mathfrak{p}}$ and $p \equiv 2 \pmod 3$); 6 (only if $j(E) \equiv 1728 \pmod{\mathfrak{p}}$ and $p \equiv 3 \pmod 4$) (cf. [Ma1], Chap. 3; [Ma2]).

REMARK 2. Let w_p be the fundamental involution of $X_0(p)$ defined by

$$(E, V) \mapsto (E/V, E[p]/V).$$

Then, for the point $w_p(x) = (E/V, E[p]/V)$, the isogeny character is $\hat{\lambda} = \theta_p \lambda^{-1}$ for the cyclotomic character θ_p (cf. loc. cit.). The corresponding sum is

$$\hat{\varepsilon} = \sum_{\sigma} (12 - a_\sigma)\sigma.$$

Let $\mathfrak{q}$ be a prime of k prime to p ($p \geqslant 5$), and F be a finite extension of $k_{\mathfrak{q}}$. If λ is unramified over F, then $E \otimes F$ has semistable reduction (cf. [S-T], [SGA7]). Hence, we can take the field F as a cyclic extension of $k_{\mathfrak{q}}$ of degree e dividing 12 (cf. [Mf] p. 46). We first consider the case when $E \otimes F$ has good reduction. Let $\mathscr{E}_s$ be the special fibre of the Néron model of $E \otimes F$ over Spec o_F. Take an element $\alpha \in k$ with $\alpha o_k = \mathfrak{q}^h$ for the class number $h = h_k$ of k. Under the same notation ε as Lemma 1,

$$\alpha^{\varepsilon} + \alpha^{\varepsilon} \equiv \mathrm{tr}(\mathrm{Frob}^{12h}) \pmod p,$$

for the Frobenius map Frob on E_s. By the Riemann–Weil condition (see e.g., [La1], [Mf]), there exists a constant C depending only on k such that for all the primes $p > C$,

$$\alpha^{\varepsilon} = \beta^{12h}$$

for a root β of Frob on E_s. Therefore the assumption of the following lemma is satisfied for the prime numbers $p > C$.

LEMMA 2. *Under the same notation and the assumption as Lemma* 1, *take a rational prime* q, $q \neq p$, *which splits completely in* k. *Take a prime* $\mathfrak{q}$ *of* k *lying over* q, *and an element* $\alpha \in k^\times$ *with* $\sigma\mathfrak{o}_k = \mathfrak{q}^h$ *for the class number* $h = h_k$ *of* k. *Assume that*

$$\alpha^\varepsilon = \beta^{12h}$$

for a root β *of the Frobenius map of an elliptic curve defined over* $\mathbf{F}_q$. *Then* ε *is one of the following forms*:

Type 2 $\varepsilon = 6N_{k/\mathbf{Q}}$ *and* $p \equiv 3 \pmod 4$.

Type 3 k *contains the imaginary quadratic field* $L = \mathbf{Q}(\beta)$, *and*

$$\varepsilon = 12N_{k/L} \text{ or } 12N_{k/L}\cdot\rho$$

for the complex conjugation ρ *of* L. *Further, if* $p \geqslant 13$ *or* $p = 7$, *the rational prime* p *splits in* L

$$p\mathfrak{o}_L = \dot{\mathfrak{p}}\bar{\mathfrak{p}}.$$

Proof. The field $L = \mathbf{Q}(\beta)$ is an imaginary quadratic field, so that α^ε is a rational number or $L = \mathbf{Q}(\alpha^\varepsilon)$. We first discuss the case when α^ε is a rational number. The principal ideal $(\alpha^\varepsilon) = \mathfrak{q}^{h\varepsilon}$ is equal to $(q)^r$ for an integer r, and for the rational prime q which splits completely in k. Then $r = 6h$ and $\varepsilon = 6N_{k/\mathbf{Q}}$. In this case, $a_\sigma = 6$ for any σ, hence $p \equiv 3 \pmod 4$ (cf. Remark 1). Now assume that $L = \mathbf{Q}(\alpha^\varepsilon)$ is an imaginary quadratic field. The ideal $(\alpha^\varepsilon) = q^{h\varepsilon}$ is $G_L = \mathrm{Gal}(\bar{L}/L)$-invariant, so that $\varepsilon = N_{k/L}\cdot(a + b\rho)$ for some integers a, b, $0 \leqslant a$, $b \leqslant 12$. Then $\mathfrak{q}^\varepsilon = \mathfrak{r}^a\mathfrak{r}^b$ for $\mathfrak{r} = N_{k/L}(\mathfrak{q})$, and $\mathfrak{q}^\varepsilon = (\beta^{12})$. Hence, $(a, b) = (12, 0)$ or $(0, 12)$. The remaining statement follows from the fact that the character λ is $\mathbf{F}_p^\times$-valued and the rational prime p is unramified in the field k.

REMARK 3. In the latter case of Type 3 of the above proof, the ideal $\mathfrak{r}$ is the principal ideal (β) or $(\bar{\beta})$.

Let $\mathfrak{q}$ be a prime of k prime to p. If $E \otimes k_\mathfrak{q}$ has potentially multiplicative reduction, then $\lambda(\sigma_\mathfrak{q})^2 = 1$ or $\mathbf{N}(\mathfrak{q})^2$ (cf. [Mf] p. 46, [Ri]). Now, we can classify the k-rational points on $X_0(p)$ by the type of the characters λ^{12}. For a given algebraic number field k of finite degree, and all prime numbers p larger than an effective constant $C_0 = C_0(k)$, we can classify the k-rational points on the modular curves $X_0(p)$ into three types. For the estimate of the constant C_0, see the proof of Theorem 1.

THEOREM 1. *Let* k *be an algebraic number field of finite degree. There exists an effective constant* $C_0 = C_0(k)$ *such that for any prime number* $p > C_0$, *the*

associating character λ^{12} *of any non cuspidal k-rational point on the modular curve* $X_0(p)$ *is one of the following three types*:

Type 1 λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified.*

Type 2 $\lambda^{12} = \theta_p^6$ *and* $p \equiv 3 \pmod 4$.

Type 3 *k contains an imaginary quadratic field L and it also contains the Hilbert class field* H_L *of L. The rational prime p splits in L*

$$p\mathfrak{o}_L = \mathfrak{p}\bar{\mathfrak{p}}.$$

For any prime $\mathfrak{q}$ *of k prime to* $\mathfrak{p}$,

$$\lambda^{12}(\sigma_\mathfrak{q}) = \alpha^{12} \pmod{\mathfrak{p}}$$

for any $\alpha \in k^\times$ *with* $\alpha\mathfrak{o}_L = N_{k/L}(\mathfrak{q})$.

Proof. We may assume that the rational prime p is unramified in k and $p \geqslant 13$. Let K be the Galois closure of the extension k of $\mathbf{Q}$. Let $x = (E, V)_{/k}$ be a non cuspidal k-rational point on $X_0(p)$ with the isogeny character λ, and $\varepsilon = \Sigma_\sigma a_\sigma \sigma$ be as in Lemma 1. If $\varepsilon = 0$ or $12N_{k/\mathbf{Q}}$, then λ^{12} is of Type 1. We discuss the other cases, so $\Sigma a_\sigma \neq 0, 12d$ for $d = [k:\mathbf{Q}]$. Take a rational prime q, $q \neq p$, which splits completely in K, and take a prime $\mathfrak{q}$ of K lying over q. If the K-rational point x has potentially multiplicative reduction at the prime $\mathfrak{q}$, then

$$\lambda(\sigma_\mathfrak{q}) \equiv \pm 1 \quad \text{or} \quad \pm q \pmod p,$$

(cf. [Mf] p. 46, [Ri]). Let h_K be the class number of K, and take an element $\alpha \in K^\times$ with $\alpha\mathfrak{o}_K = \mathfrak{q}^{h_K}$. There are only finitely many prime numbers p which divide

$$N_{K/\mathbf{Q}}(\alpha^\varepsilon - 1) \quad \text{or} \quad N_{K/\mathbf{Q}}(\alpha^\varepsilon - q^{12h_K}).$$

Therefore, we may assume that the K-rational point x has potentially good reduction at $\mathfrak{q}$. If ε is not of the Type 2, 3 of Lemma 2, then

$$\alpha^\varepsilon \neq \beta^{12h_K}$$

for any root β of the Frobenius map of any elliptic curve over $\kappa(\mathfrak{q}) = \mathbf{F}_q$. Then, there are only finitely many prime numbers p which divide a nonzero rational integer

$$N_{K(\beta)/\mathbf{Q}}(\alpha^\varepsilon - \beta^{12h_K})$$

for a root β as above. Now, we discuss the cases of Type 2 and 3 of Lemma 2 for the Galois closure K of the extension k over $\mathbf{Q}$. In the case of Type 3, the rational prime p splits in L; $p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}$. Changing $\mathfrak{p}$ by $\bar{\mathfrak{p}}$, if necessary, we may assume that λ^{12} is unramified at the primes of K lying over $\bar{\mathfrak{p}}$ and it ramifies at the primes of K lying over $\mathfrak{p}$. Then for any $\alpha \in (k \cdot L)^\times$ prime to $\mathfrak{p}$,

$$\lambda^{12}((\alpha)) \equiv N_{kL/L}(\alpha)^{12} \pmod{\mathfrak{p}}.$$

The character $\lambda^{12} \circ N_{kL/L}$ is unramified outside of Supp($\mathfrak{p}$) and ramifies at the primes lying over $\bar{\mathfrak{p}}$, so that k contains L. Then, for any $\alpha \in k^\times$ prime to p (or to $\mathfrak{p}$ in the case of Type 3),

$$\lambda^{12}((\alpha)) \equiv \begin{cases} N_{k/\mathbf{Q}}(\alpha)^6 & (\text{mod } p) \text{ Type 2} \\ N_{k/L}(\alpha)^{12} & (\text{mod } \mathfrak{p}) \text{ Type 3} \end{cases} \tag{1}$$

Let $M = M(k)$ be the set of rational primes q which split in k and are prime to $6h$ for the class number $h = h_k$ of k. Let $N = N(k)$ be the set of the primes $\mathfrak{q}$ of k lying over the rational primes q in M. Further, take a *finite* subset S of N such that ($S \bmod P_k$) generates the ideal class group $C_k = I_k/P_k$ of k. It suffices to discuss the case for the prime numbers p prime to any prime $\mathfrak{q}$ in S. By the same argument as above, we may assume that the k-rational points of Type 2 and 3 are all potentially good reduction at any prime $\mathfrak{q}$ in S for the prime numbers p larger than an effective constant which depends only on k. Further, we may assume that for each prime $\mathfrak{q}$ in S and $\alpha \in k^\times$ with $\alpha\mathcal{O}_k = \mathfrak{q}^h$,

$$\alpha^\varepsilon = \beta^{12h} \tag{2}$$

for a root $\beta = \beta_\alpha$ of the Frobenius map of an elliptic curve over $\kappa(\mathfrak{q}) = \mathbf{F}_q$ (for the prime numbers p larger than the constant as above). In the case of Type 2, $\beta = \zeta\sqrt{-q}$ for a $12h^{th}$ root ζ of unity. The prime q in S does not divide $6h$ and $\mathbf{Q}(\beta)$ is an imaginary quadratic field, so that

$$\beta = \pm\sqrt{-q}.$$

Thus,

$$\lambda^{12}(\sigma_\mathfrak{q}) \equiv \beta^{12} = N_{k/\mathbf{Q}}(\mathfrak{q})^6 \pmod{p}.$$

With the congruence (1), this gives the result for the case of Type 2. In the case of Type 3, the relation (2) gives the equalities of ideals that

$$(N_{k/L}(\mathfrak{q})^{12h}) = (N_{k/L}(\alpha))^{12} = (\beta)^{12h}.$$

Then

$$N_{k/L}(\mathfrak{q}) = (\beta),$$

which is a principal ideal of L. By our assumption, (S mod P_k) generates the ideal class group C_k of k, so that $N_{k/L}(I_k)$ is contained in the principal ideal group P_L of L. Then, by the class field theory (cf. [La2]), k contains the Hilbert class field H_L of L. If $\beta^{12h} = \gamma^{12h}$ for a root γ of the Frobenius map of an elliptic curve over $\kappa(\mathfrak{q}) = \mathbf{F}_q$, then $\gamma = \zeta\beta$ for a $12h^{th}$ root ζ of unity. As the prime q does not divide to $6h$, so that ζ belongs to the imaginary quadratic field L. Then,

$$\lambda^{12}(\sigma_{\mathfrak{q}}) \equiv \beta^{12} \pmod{\mathfrak{p}}.$$

With the congruence (1), this gives the result for the case of Type 3.

3. Algebraic points of Type 1

Kamienny [Ka1] solved the problem of the p-torsion points on elliptic curves over quadratic fields. It leads the complete result of the problem of torsion points on elliptic curves over quadratic fields (cf. [Ke1,2], [Mo], [K-Mo]). Kamienny's idea is a generalization of Mazur's *formal immersion* at the cuspidal section ∞ ([Ma2]). He also proved the *formal immersion* at the cuspidal section $(\infty, \ldots, \infty)$ for the cases of degree $\leqslant 8$ ([Ka2], [K-M]), and solved the problem of the p-torsion points on elliptic curves over the algebraic number fields of degree $\leqslant 8$. Abramovich [Ab] improved it and solved this problem for the algebraic number fields of degree $\leqslant 12$. These results solve the case of Type 1 for algebraic number fields of degree $\leqslant 12$.

We first explain the formal immersion of Kamienny (cf. loc. cit.). Let $X_{(n)}$ be the nth symmetric product of the modular curve $X = X_0(p)$:

$$X_{(n)} = \underbrace{(X \times \cdots \times X)}_{n\text{-times}}/S_n,$$

where S_n is the symmetric group of n-letters. Let $f_{(n)}$ be the morphism of $X_{(n)}$ to the jacobian variety $J = J_0(p)$ of $X_0(p)$ defined by the following morphism of nth product of X to J:

$$(x_1, \ldots, x_n) \mapsto \mathrm{cl}\left(\sum_{i=1}^{n} (x_i) - n(\infty)\right).$$

Then $f_{(n)}$ induces naturally the morphism $q_{(n)}$ of $X_{(n)}$ to the *Eisenstein quotient* $\tilde{J} = \tilde{J}_0(p)$ ([Ma1]). Let $X_{/\mathbf{Z}} = X_0(p)_{/\mathbf{Z}}$ be the modular curve over $\mathbf{Z}$ associated with $X_0(p)$ (cf. [D-R]), and $X_{(n)/\mathbf{Z}}$ be the symmetric nth product of $X_{/\mathbf{Z}}$ and $X^{\text{smooth}}_{(n)/\mathbf{Z}}$ be the smooth part (/$\mathbf{Z}$) of $X_{(n)/\mathbf{Z}}$. Then $f_{(n)}, g_{(n)}$ induce naturally the morphisms $f_{(n)}$ and $g_{(n)}$ of $X^{\text{smooth}}_{(n)/\mathbf{Z}}$ to the Néron models $J_{/\mathbf{Z}}$ and $\tilde{J}_{/\mathbf{Z}}$, respectively. For the prime numbers $q > n$, $q \neq p$,

$$X^{\text{smooth}}_{(n)/\mathbf{Z}} \otimes \mathbf{Z}_q = X_{(n)/\mathbf{Z}} \otimes \mathbf{Z}_q$$

and for the prime number $q = p > n$,

$$X^{\text{smooth}}_{(n)/\mathbf{Z}} \otimes \mathbf{Z}_p = X^{h}_{(n)/\mathbf{Z}} \otimes \mathbf{Z}_p,$$

where $X^h_{/\mathbf{Z}}$ is the open subscheme of $X_{/\mathbf{Z}}$ obtained by removing the supersingular points of characteristic p (cf. [D-R]).

THEOREM 2 (Kamienny, Abramovich). *For each integer $n \leqslant 12$, there exists prime numbers $p_{(n)}$ and $q_{(n)}$ such that $g_{(n)} \otimes \mathbf{Z}_q$ is a formal immersion at the cuspidal sections $(\infty, \ldots, \infty)$ and $(0, \ldots, 0)$ for any prime numbers $p \geqslant p_{(n)}$ and $q \geqslant q_{(n)}$.*

REMARK 4. For $n = 1$, $p_{(1)} = 17$, $q_{(1)} = 3$ and for $n = 2$, $p_{(2)} = 73$, $q_{(2)} = 7$ ([Ka1],[Ma2]). For the other cases $3 \leqslant n \leqslant 12$, the known estimates of $p_{(n)}$ and $q_{(n)}$ are not fine enough (cf. [K-M], [Ab]).

Let k be an algebraic number field of degree $n \leqslant 12$, and x be a non cuspidal k-rational point of $X_0(p)$. Then x defines a $\mathbf{Q}$-rational point $x_{(n)} = \{x^\sigma | \sigma : k \hookrightarrow \bar{\mathbf{Q}}\}$ on $X_{(n)}$, which is not the cuspidal sections $(\infty, \ldots, \infty)$ nor $(0, \ldots, 0)$.

COROLLARY 1 (Kamienny, Abramovich). *Under the same notation as above, for $n \leqslant 12$, if $p \geqslant p_{(n)}$ and $q \geqslant q_{(n)}$, then*

$$x_{(n)} \otimes \mathbf{F}_q \neq (\infty, \ldots, \infty)_{/\mathbf{F}_q} \quad \text{nor} \quad (0, \ldots, 0)_{/\mathbf{F}_q}.$$

REMARK 5. For a positive integer n, denote by $S(n)$ the set of torsion primes (cf. [K-M]), i.e., for any prime p in $S(n)$, there is an isogeny of prime degree p over an algebraic number field of degree not greater than n. Kamienny and Mazur (loc. cit.) showed that the set $S(n)$ is of (natural) density zero.

Now we can show the result for the case of Type 1.

THEOREM 3. *Let k be an algebraic number field of degree $\leqslant 12$. Then there exists an effective constant C_1 depends only on k such that $X_0(p)\backslash\{0, \infty\}$ has no k-rational points of Type 1 for any prime number $p > C_1$.*

REMARK 6. For a given algebraic number field k, it is easy to estimate the constant C_1, see the proof of Theorem 3.

Proof. Take prime numbers $p \geqslant p_{(n)}$ and $q \geqslant q_{(n)}$ with $q \neq p$. We may assume that $p \geqslant 5$ and the rational prime p is unramified in k. Let $x = (E, V)_{/k}$ be a non cuspidal k-rational point on $X_0(p)$ of Type 1. Changing x by $w_p(x) = (E/V, E[p]/V)$, if necessary, we may assume that $\lambda^{12h} = 1$ for the class number $h = h_k$ of k (cf. Remark 2). By Corollary 1, there exists a prime $\mathfrak{q}$ of k lying over the rational prime q such that $x \otimes \kappa(\mathfrak{q})$ is equal to $0_{/\kappa(\mathfrak{q})}$ or a non cuspidal point over $\kappa(\mathfrak{q})$. In the first case, E has potentially multiplicative reduction at $\mathfrak{q}$, and the restriction of λ to the inertial subgroup $I_{\mathfrak{q}}$ of $\mathfrak{q}$ is $\pm\theta_p$ (cf. [D-R]). Then,

$$1 = \lambda^{12h} | I_{\mathfrak{q}} = \theta_p^{12h},$$

so that $p - 1$ divides $12h$. In the latter case, the elliptic curve E has potentially good reduction at $\mathfrak{q}$. Then, for a root β of the Frobenius map of an elliptic curve over $\kappa(\mathfrak{q})$,

$$1 + \mathbf{N}(\mathfrak{q})^{12h} \equiv \beta^{12h} + \bar{\beta}^{12h} \pmod{p}.$$

The absolute value of R.H.S. $\leqslant 2\mathbf{N}(\mathfrak{q})^{6h}$(, by the Riemann–Weil condition (cf. [La1], [Mf])), so that the prime numbers $p > (\mathbf{N}(\mathfrak{q})^{6h} - 1)^2$ do not satisfy the above congruence.

REMARK 7. For an algebraic number field k of finite degree, denote by $T(k)$ the set of prime numbers p such that the modular curves $X_0(p)$ have non trivial k-rational points of Type 1. The result on the torsion primes [K-M] (cf. Remark 5) shows that this set $T(k)$ is of (natural) density zero.

4. Algebraic points of Type 2

Let $x = (E, V)_{/k}$ be a k-rational point on $X_0(p)$ of Type 2, and λ be its isogeny character as in Theorem 3. We first prepair several lemmas.

LEMMA 3. *The isogeny character λ is of the form*

$$\lambda = \psi\theta_p^m$$

for an integer m with $2m \equiv p + 1/2 \pmod{p-1}$, and a character ψ of order dividing 6.

Proof. Put $\psi = \lambda\theta_p^{-m}$, then $\psi^{12} = \lambda^{12}\theta_p^{-6} = 1$. Since $p \equiv 3 \pmod 4$, $\psi^6 = 1$.

LEMMA 4. *Let $\mathfrak{q}$ be a prime of k lying over a rational prime q, $q \neq p$. If E has potentially multiplicative reduction at $\mathfrak{q}$, and the rational prime q splits in*

the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$, *then*

$$\mathbf{N}(\mathfrak{q}) \equiv \psi(\sigma_{\mathfrak{q}})^{\pm 2} \pmod{p}.$$

Proof. In this case, $\lambda(\sigma_{\mathfrak{q}}) \equiv \pm 1$ or $\pm \mathbf{N}(\mathfrak{q}) \pmod{p}$ (cf. [Mf] p. 46). Then, by Lemma 3 and the assumption of this lemma,

$$\psi(\sigma_{\mathfrak{q}})^2 \mathbf{N}(\mathfrak{q})^{2m} \equiv (\sigma_{\mathfrak{q}})^2 \mathbf{N}(\mathfrak{q}) \equiv 1 \quad \text{or} \quad \mathbf{N}(\mathfrak{q})^2 \pmod{p}.$$

LEMMA 5. *Let* $\mathfrak{q}$ *be a prime of* k *lying over a rational prime* $q, q \neq p$. *Suppose that* E *has potentially good reduction at* $\mathfrak{q}$, *and that* $\mathfrak{q}$ *is of odd degree and* $\mathbf{N}(\mathfrak{q}) < p/4$. *Then the rational prime* q *remains prime in* $\mathbf{Q}(\sqrt{-p})$.

Proof. By Lemma 3,

$$\{\psi(\sigma_{\mathfrak{q}})^2 + \psi(\sigma_{\mathfrak{q}})^{-2}\}\mathbf{N}(\mathfrak{q})^{1+n-1/2} \equiv \beta^2 + \bar{\beta}^2 \pmod{p},$$

for a root β of the Frobenius map of an elliptic curve over $\kappa(\mathfrak{q}) = o_k/\mathfrak{q}$ and a 6^{th} root $\psi(\sigma_{\mathfrak{q}})$ of unity. If the rational prime q splits in $\mathbf{Q}(\sqrt{-p})$, then

$$(\beta + \bar{\beta})^2 \equiv 4\mathbf{N}(\mathfrak{q}) \quad \text{or} \quad \mathbf{N}(\mathfrak{q}) \pmod{p}.$$

Then the Riemann–Weil condition: $|\beta + \bar{\beta}| \leqslant 2\sqrt{\mathbf{N}(\mathfrak{q})}$ (cf. [La1], [Mf]) and the assumption: $\mathbf{N}(\mathfrak{q}) < p/4$ lead that $\beta + \bar{\beta} = \pm 2\sqrt{\mathbf{N}(\mathfrak{q})}$ or $\pm\sqrt{\mathbf{N}(\mathfrak{q})}$, which contradicts that $\beta + \bar{\beta}$ is a rational integer and $\mathfrak{q}$ is of odd degree.

For quadratic field k, we make use of a Goldfeld's theorem ([Ma2] Appendix). We first explain his conjecture ([Ma2]). For an algebraic number field L, denote by D_L the discriminant of L.

CONJECTURE (Goldfeld). For any algebraic number field k of finite degree, there are only finitely many quadratic fields L which satisfy the condition that any rational prime $q < |D_L|/4$ does not split in the composite $k \cdot L$.

Goldfeld (loc. cit.) proved this conjecture for quadratic fields k. The discriminants D_L of the exceptional quadratic fields L are effectively estimated, except for at most one L (cf. loc. cit). In our case, the condition C below is satisfied for any algebraic number field k of finite degree by Lemmas 3, 4 and 5.

CONDITION C. Any rational prime q with $q < p/4$ does not split in $k(\sqrt{-p})$, unless $q^2 + q + 1 \equiv 0 \pmod{p}$.

For a quadratic field k, we cannot apply the above Goldfeld's theorem to our case, directly. But, a slight modification solves our problem. His proof admits at most two exceptional primes q with $2 \leqslant q \leqslant p/4$.

PROPOSITION 1. *For any quadratic field k, there are only finitely many prime numbers p which satisfy the condition C.*

Proof. We explain here the modified parts of the Goldfeld's proof. Let S be the set of rational primes which ramify in k. It is enough to consider the prime numbers $p > |D_k|$. Let $K = k(\sqrt{-p})$, and

$$f(s) = \zeta(2s) \prod_{q \in S} (1 - q^{-2s})$$

$$g(s) = \zeta_K(s)$$

for the zeta function $\zeta_K(s)$ of K, and the Riemann zeta function $\zeta(s)$. For $t > 0$ and an integer $r \geqslant 5$, let

$$F(t) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} f(s) \frac{(t/4)^s}{s(s+1)\cdots(s+r)} \mathrm{d}s$$

$$G(t) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} g(s) \frac{(t/4)^s}{s(s+1)\cdots(s+r)} \mathrm{d}s$$

Then, Goldfeld ([Ma2] Appendix) showed that

$$F(t) = t^{1/2}(c_1 + c_2 \log t) + c_3 + \varphi(t^{-1/4}),$$

$$G(t) > c_4 t p^{-\varepsilon} - c_5 p^{3/8+\varepsilon} t^{1/2}$$

for the constants c_1, c_2 and c_3 depending only on k, and the positive constants c_4 and c_5 depending only on k and any given positive number ε, and for a function $\varphi(t) = O(t)$ which depends only on k. The last inequality as above is valid, except for at most one prime number p (see loc. cit). The condition C leads that $F(p) = G(p)$ or

$$F(p) - 2F\left(\frac{p}{q}\right) + F\left(\frac{p}{q^2}\right) = G(p) + 2G\left(\frac{p}{q}\right) + G\left(\frac{p}{q^2}\right),$$

for a prime number q with $q < p/4$ and $q^2 + q + 1 \equiv 0 \pmod{p}$. In the latter case, except for at most one prime number p,

$$\text{L.H.S.} = O(p^{1/2} \log p) + O(p^{1/4})$$

$$\text{R.H.S.} > c_4 p^{1-\varepsilon} \left(1 - \frac{1}{q}\right)^2 - c_5 p^{7/8+\varepsilon}(1 - q^{-1/2})^2$$

$$> \frac{c_4}{4} p^{1-\varepsilon} - c_5 p^{7/8+\varepsilon}$$

Taking a positive number ε with $0 < \varepsilon < \frac{1}{16}$, we get the result.

Proposition 1 and Lemmas, 3, 4 and 5 give the following Theorem 4.

THEOREM 4. *For any quadratic field k, the k-rational points on* $X_0(p)$ *of Type* 2 *appear only for finitely many prime numbers p.*

REMARK 8. K. Murty taught me that the G.R.H. leads Goldfeld conjecture. In fact, G.R.H. implies that Condition C is satisfied only for finitely many prime numbers p for a given algebraic number field k of finite degree. For any algebraic number field k of finite degree, we may expect that the modular curves $X_0(p)$ have no k-rational points of Type 2 for almost all prime numbers p.

We show that the assumption of the Goldfeld conjecture is satisfied for algebraic number fields of *odd* degree (cf. Condition C). We first study the Mordell–Weil group of the jacobian variety $J = J_0(p)$ of the modular curve $X_0(p)$. Let

$$\mathbf{T} = \mathbf{Z}[T_l, w_p]_{l \neq p}$$

be the subring of End(J) generated by the Hecke operators T_l for prime numbers l, $l \neq p$, and the automorphism w_p defined by the fundamental involution of $X_0(p)$. Then End(J) $\otimes$ **Q** is a product of totally real algebraic number fields of finite degree, and the index $[\mathrm{End}(J) : \mathbf{T}]$ is finite (see [Ri], [Ma1] Chap. 2). Let $\mathscr{I}$ be the *Eisenstein ideal* generated by $\eta_l = T_l - l - 1$ for all prime numbers l, $l \neq p$, and $w_p + 1$. Then

$$\mathbf{T}/\mathscr{I} \simeq \mathbf{Z}/n\mathbf{Z}$$

for the numerator n of $(p - 1)/12$ ([Ma1]). Let

$$A = \left(\bigcap_{n \geq 1} \mathscr{I}^n \right) J \quad \text{and} \quad \tilde{J} = \tilde{J}_0(p) = J/A.$$

The quotient $\tilde{J}$ is called the *Eisenstein quotient* of J. Let $j : J \to \tilde{J}$ be the natural map, and $C = \langle \mathrm{cl}((0) - (\infty)) \rangle$ be the cuspidal subgroup of J. Then

$$J(\mathbf{Q})_{\mathrm{tor}} = C \simeq \mathbf{Z}/n\mathbf{Z}$$

and j maps *isomorphically* the cuspidal subgroup C onto the Mordell–Weil group

$$\tilde{J}(\mathbf{Q}) = j(C)$$

(see loc. cit.). For an abelian variety B over $\mathbf{Q}$, and a subring R of $\mathbf{Q}$ not containing $1/p$, let $B_{/T} = B_{/R}$ be the Néron model of B over the base $T = \operatorname{Spec} R$, and B_s be the special fibre of $B_{/T}$ at $s = \operatorname{Spec} \mathbf{F}_p$, and B_s^0 be its connected component of the unit section. Further, denote by B^0 the open subgroup scheme of $B_{/S}$ which is obtained by removing the connected components of B_s other than B_s^0. Let

$$M = J(\mathbf{Q}) = J_{/S}(\mathbf{Z}) \quad \text{and} \quad M^0 = J^0(\mathbf{Z}),$$

which are $\mathbf{T}$-modules. Then we know that

$$J_s = J_s^0 \times C_s \quad \text{and} \quad M = M^0 \oplus C,$$

where $C_s = C \otimes \mathbf{F}_p$ (loc. cit). For each prime ideal $\mathfrak{q}$ of $\mathbf{T}$, let $\mathbf{T}_\mathfrak{q} = \varprojlim \mathbf{T}/\mathfrak{q}^m\mathbf{T}$.

PROPOSITION 2. *For any prime ideal* $\mathfrak{q}$ *over* $\mathscr{I}$, $M^0 \otimes \mathbf{T}_\mathfrak{q} = \{0\}$.

Proof. It follows from the facts that $M^0 \otimes \mathbf{T}_\mathfrak{q}$ is of finite order, and M^0 is a free $\mathbf{Z}$-module ([Ma1] Chap. 3, Th. 3.1, Lemma 3.3).

Let $A^\vee = \operatorname{Pic}^0(A)$, $J^\vee = J$ and $\tilde{J}^\vee$ be the dual abelian varieties, and

$$0 \to A \to J \to \tilde{J} \to 0$$

be the natural exact sequence. Let

$$0 \to \tilde{J}^\vee \to J \to A^\vee \to 0$$

be the dual exact sequence, and

$$D = A \cap \tilde{J}^\vee$$

which is a finite subgroup. For a finite subgroup V of J over $\mathbf{Q}$, denote by $V_{/S'}$ the flat closure of V in the Néron model $J_{/S'}$ for $S' = \operatorname{Spec} \mathbf{Z}[1/2]$ (cf. [Ra2]).

LEMMA 6

(1) *For each prime ideal* $\mathfrak{q}$ *over* I, $D \otimes \mathbf{T}_\mathfrak{q} = \{0\}$.
(2) $D_{/S'}$ *is contained in* $J^0_{/S'}$.
(3) $0 \to D_{/S'} \to J^0_{/S'} \to \tilde{J}^0_{/S'} \times A^{\vee 0}_{/S'} \to 0$ *is exact.*

Proof. The first statement (1) follows from the fact that the natural map

$$J \otimes \mathbf{T}_\mathfrak{q} \tilde{\to} \tilde{J} \otimes \mathbf{T}_\mathfrak{q}$$

is an isomorphism (see [Ma1] Chap. 3, Cor. 1.4). The natural map of J onto $\tilde{J} \times A^{\vee}$ is an isogeny with kernel D. Then kernel of the induced map φ of $J_{/S'}$ to $\tilde{J}_{/S'} \times A^{\vee}_{/S'}$ is contained in $J_{/S'}[N]$ for an integer $N \geqslant 1$. Applying the specialization lemma of finite flat group schemes (cf. [Ra2], [Ma2]) to the finite part $D^{f}_{/S'}$ (loc. cit), we see that the quasi-finite flat subgroup scheme $D_{/S'}$ is the kernel of the induced map φ. Let $\mathrm{Gr}(D)$ be the graded module of D as $\mathbf{T}$-module. Then by (1), $\mathrm{Gr}(D) \otimes \mathbf{T}_{\mathfrak{q}} = \{0\}$ for any prime $\mathfrak{q}$ over I. The quotient group J_s/J°_s is naturally isomorphic to the cuspidal subgroup C as $\mathbf{T}$-module. This proves (2) and (3).

THEOREM 5

$$\tilde{J}^{\circ}(\mathbf{Z}) = \{0\}.$$

Proof. By Lemma 6(1) and (3), we have the long exact sequence

$$0 \to D(S') \to M^{\circ} \to \tilde{J}^{\circ}(S') \times A^{\vee\circ}(S') \to \mathrm{H}^1(S', D_{/S'}) \to \cdots.$$

For each prime ideal $\mathfrak{q}$ over I, by Proposition 2 and Lemma 6(1), we get

$$\tilde{J}^{\circ}(S') \otimes \mathbf{T}_{\mathfrak{q}} = \{0\}.$$

While $\tilde{J}(\mathbf{Z}) = \tilde{J}(S') = \tilde{J}(\mathbf{Q}) = C$ as $\mathbf{T}$-modules. This gives the result.

COROLLARY 2

(1) $M^{\circ} = A(\mathbf{Q})$.
(2) $j(C)_s \cap \tilde{J}^{\circ}_s = \{0\}$.
(3) *The image of* A_s *in* J_s *is contained in* J°_s.

Proof. Lemma 6 gives (2) and (3), directly. Then M° is contained in $A(\mathbf{Q})$, and $M^{\circ} \oplus C = M = A(\mathbf{Q}) \oplus C$ ([Ma1] Chap. 3). This shows (1).

We now discuss the algebraic points of Type 2. Let k be an algebraic number field of degree d, and K be its Galois closure over $\mathbf{Q}$. Let $x = (E, V)_{/k}$ be a k-rational point on $X_0(p)$ of Type 2. Assume that p is unramified in k and $p \geqslant 5$. Then $p \equiv 3 \pmod 4$, and the special fibre $x \otimes \kappa(\mathfrak{p})$ is a section of the supersingular point with modular invariant $=$ 1728. Let $X_{/\mathbf{Z}} = X_0(p)_{/\mathbf{Z}}$ be the canonical model of $X_0(p)$ over $\mathbf{Z}$, and $\mathscr{X}$ be the minimal model of $X = X_0(p)$ over $\mathbf{Z}$ (cf. [D-R]). Then natural morphism

$$\mathscr{X} \to X_{/\mathbf{Z}}$$

is obtained by blowing up at the supersingular point(s) of characteristic p with modular invariant = 1728 (and 0 if $p \equiv 2 \pmod 3$). Denote by F the fibre over the supersingular point with modular invariant = 1728. Let $\mathfrak{P}$ be a prime of K lying over the prime p. Then x^σ defines the section of the minimal model $\mathscr{X}$ whose special fibre at $\mathfrak{P}$ is a section of $F - \{\text{nodes}\}$ (see [D-R] [Ma2]). Let

$$P = \mathrm{cl}((0) - (\infty))$$

be the generator of the cuspidal subgroup C. Let

$$f(x) = \mathrm{cl}\left(\sum_\sigma (x^\sigma) - d(\infty)\right)$$

be the $\mathbf{Q}$-rational point of the jacobian variety $J = J_0(p)$ for the embeddings σ of k into K. We denote by $f(x)_s$ etc. the special fibre at $s = \mathrm{Spec}\,\mathbf{F}_p$. Let $j: J \to \tilde{J}$ be the natural map, and $g(x) = j(f(x))$.

LEMMA 7. *Assume that p is unramified in k. Then, for $d = [k:\mathbf{Q}]$*

$$2f(x) \equiv dP \pmod{J_s^\circ}.$$

Proof. Let $o_{\mathfrak{P}}$ be the ring of integers of $K_{\mathfrak{P}}$. The construction of the Néron models commutes with the étale base change $\mathrm{Spec}\, o_{\mathfrak{P}} \to \mathrm{Spec}\, \mathbf{Z}_p$ (cf. [Ra2], [SGA7]). The quotient group J_s/J_s° is described by the vertical divisor group of $\mathscr{X}$ at p and the intersection matrix (cf. [Ma2] Appendix, [Ra2]). Then an elementally calculation gives the result.

For a rational prime q, let $e(q)$ be the maximal value of the ramification indices of all primes of K lying over q.

LEMMA 8. *Let q be a rational prime with*

$$e(q) < q - 1 \quad \text{or} \quad \left(q, \mathrm{num}\left(\frac{p-1}{12}\right)\right) = 1,$$

and $\mathfrak{q}$ be a prime of K lying over q. Assume that p is unramified in k, and that the special fibres of x^σ at $\mathfrak{q}$ are all cusps, and d_1 of them are the 0 cusps, and $d_2 = d - d_1$ are the ∞ cusps, then

$$g(x) = d_1 j(P).$$

Proof. The special fibre $f(x)_{\kappa(\mathfrak{q})} = d_1 P_{\kappa(\mathfrak{q})}$. The cuspidal subgroup $j(C) = \tilde{J}(\mathbf{Q})$ is a finite group of order $n = \mathrm{num}((p-1)/12)$ ([Ma2]). Then lemma follows from the specialization lemma (cf. loc. cit. [Ra1]).

PROPOSITION 3. *Assume that p is unramified in k and $p > 12d + 1$ for $d = [k:\mathbf{Q}]$ and that $x_{/k(\mathfrak{q})}$ are cusps for all primes lying over a rational prime $q, q > d$. Then the degree d is even.*

Proof. Under the same notation of Lemma 8, by Corollary 2 and Lemmas 7 and 8, $d_1 - d_2 \equiv 0 \pmod{(p-1)/12}$. Then by our assumption on p, $d_1 = d_2$.

PROPOSITION 4. *Let k be an algebraic number field of odd degree. Under the Goldfeld conjecture* [Ma2], *the k-rational points on $X_0(p)$ of Type 2 exist only for finitely many prime numbers p.*

Proof. By Lemma 5 and Proposition 3, the assumption of Goldfeld conjecture is satisfied.

5. Algebraic points of Type 3

For a given algebraic number field k of finite degree, the k-rational points of Type 3 are excepted to be the C.M. points for large prime numbers p. We discuss this case under a strong condition on reduction at primes. Let $x = (E, V)_{/k}$ be a k-rational point on $X_0(p)$ of Type 3 with the isogeny character λ. For our problem, it suffices to discuss the case when $p \geqslant 5$ and the modular invariant $j(x) = j(E) \neq 0, 1728$. Then λ^2 is independent of the choice of the representative $(E, V)_{/k}$ of x. Let L, H_L and $\mathfrak{p}$ be as in Theorem 3 for this x. Then, for any ideal $\mathfrak{q}$ of k prime to $\mathfrak{p}$, and $\alpha \in L^\times$ with $\alpha o_L = N_{k/L}(\mathfrak{q})$,

$$\lambda(\mathfrak{q})^{12} \equiv \alpha^{12} \pmod{\mathfrak{p}}.$$

Let ζ be a primitive 12^{th} root of unity, and $L' = L(\zeta)$, and take a prime $\mathfrak{P}$ of L' over $\mathfrak{p}$. Then we can lift λ uniquely to a (primitive) $L'^\times$-valued Hecke characters φ_λ of Type A_0 of k:

$$\varphi_\lambda \pmod{\mathfrak{P}} = \lambda \quad \text{and} \quad \varphi_\lambda(\alpha) = \alpha$$

for $\alpha \in k^\times$ with $\alpha \equiv 1 \pmod{c_\lambda}$. Denote by k^λ the class field of k which corresponds to the ideal group

$$\{\mathfrak{a} \in I_k(c_\lambda) \mid \varphi_\lambda(\mathfrak{a}) \in L\}.$$

Then there exists an elliptic curve which has complex multiplication by o_L over k^λ and whose l-adic representations are induced from $\varphi_\lambda \circ N_{k^\lambda/k}$ (cf. [La1]). Now take an elliptic curve E_L with complex multiplication by o_L over the class field H_L, and denote by φ_L its associating Hecke character. Denote by $w(L)$ the number of the roots of unit of L.

LEMMA 9. *If $p \geqslant 5$ and the modular invariant $j(x) \neq 0, 1728$, then*

(1) *k^{λ} is independent of the choice of the representative $(E, V)_{/k}$ of x.*
(2) $(\varphi_{\lambda} \circ N_{k^{\lambda}/k})^{w(L)} = (\varphi_L \circ N_{k^{\lambda}/H_L})^{w(L)}$.

Proof. Let $(E', V')_{/k}$ be another representative of x with isogeny character λ'. Then $\lambda' = \lambda \otimes \chi$ for a character χ with $\chi^2 = 1$, since $\mathrm{Aut}(E) = \{\pm 1\}$. Then $\varphi_{\lambda'} = \varphi_{\lambda} \otimes \chi$, so that $k^{\lambda'} = k^{\lambda}$. For any ideal $\mathfrak{a}$ of k^{λ} prime to the conductors of φ_{λ} and φ_L, the principal ideals $\varphi_{\lambda}(N_{k^{\lambda}/k}(\mathfrak{a}))\mathcal{O}_L = \varphi_L(N_{k^{\lambda}/H_L}(\mathfrak{a}))\mathcal{O}_L$.

COROLLARY 3. *If $k^{\lambda} = k$ and $w(L) = 2$, we can choose a representative $(E, V)_{/k}$ of x whose associating Hecke character is $\varphi_L \circ N_{k/H_L}$.*

Let $\tilde{H}_L$ be the minimal class field of L such that $\varphi_L \circ N_{\tilde{H}_L/H_L}$ is unramified, and $k_L = k \cdot \tilde{H}_L$. Then the chosen elliptic curve E_L has everywhere good reduction over H_L. Let $e(p)$ be the maximal value of the ramification indices of the primes $\mathfrak{P}$ of k_L lying over the rational prime p.

LEMMA 10. *Assume that $p \geqslant 5$, $6e(p) < p - 1$, $k^{\lambda} = k$ and $w(L) = 2$. Let $(E, V)_{/k}$ be the representative of x as in Corollary 3. Then E has everywhere semistable reduction over k_L.*

Proof. The isogeny character of $(E, V)_{/k_L}$ is $\varphi_L \circ N_{k_L/H_L} \pmod{\mathfrak{p}}$, which is unramified outside of $\mathrm{Supp}(\mathfrak{p})$ and $p \geqslant 5$. Then $E_{/k_L}$ has semistable reduction outside of $\mathrm{Supp}(p)$ (cf. [Mf]). Let $\mathfrak{P}$ be a prime of k_L lying over p, and R be the ring of integers of $(k_L)_{\mathfrak{P}}$. We first consider the case when $\mathfrak{P}$ divides $\bar{\mathfrak{p}}$. The finite group $V_{/k_L}$ extends to a finite étale group scheme $\mathbf{V}$ over R. By the universal property of the Néron model (cf. [SGA7], [Ra2]), the embedding $V_{/k_L} \hookrightarrow E_{/k_L}$ extends to a morphism $\mathbf{V} \to E_{/R}$. Since $e(p) < p - 1$, the specialization lemma of finite flat group schemes (cf. [Ra1], [Ma2]) shows that the $E_{/R} \otimes \kappa(\mathfrak{P})$ contains the étale group $\mathbf{V} \otimes \kappa(\mathfrak{P})$. E has semistable reduction over extension K of degree $\leqq 6$, and the natural morphism of $E_{/R} \otimes \mathcal{O}_K$ to $E_{/\mathcal{O}_K}$ sends isomorphically, since $6e(p) < p - 1$. Then $E_{/R}$ is semistable (cf. [Mf] p. 46). For the prime $\mathfrak{P}$ dividing the prime $\mathfrak{p}$, applying the same argument to $(E/V)_{/k_L}$, we see that $(E/V)_{/R}$ is semistable, hence $E_{/R}$ is semistable.

The elliptic curves with complex multiplication have everywhere potentially good reduction. The Kamienny's result for quadratic fields L [Ka1] shows that any L-rational point on $X_0(p)$ (for $p \geqslant 73$) has potentially good reduction at remain primes $q, q \geqslant 7$. But, we have a little information for splitting primes. We here add a strong condition on the reduction. Let S be a finite set of primes of k, and L be an imaginary quadratic field whose Hilbert class field H_L is contained in the given algebraic number field k. For a positive constant C, let $M(k, L, C, S)$ be the set of k-rational points x on the modular curves $X_0(p)$ of Type 3 for prime numbers $p \geqslant C$ which satisfy the conditions below:

(1) x has potentially good reduction outside of S.
(2) The associating Hecke character is $L^{\times}$-valued.

PROPOSITION 5. *If L is not either of $\mathbf{Q}(\sqrt{-1})$ or $\mathbf{Q}(\sqrt{-3})$, then for a constant C, $M(k, L, C, S)$ consists of C.M. points.*

Proof. Choose a constant $C' \geqslant 5$ such that any rational prime $\geqslant C'$ does not ramify in the field k_L of Lemma 10. By Lemma 10, any point x in $M(k, L, C, S)$ is represented by an object $(E, V)_{/k}$ such that $E_{/k_L}$ has everywhere semistable reduction, and good reduction outside of S. There are only finitely many such elliptic curves $E_{/k_L}$ up to isomorphism over k_L (cf. [Fa] Chap. 5, [C-S] Chap. 2). If E does not have complex multiplication, then E does not have any cyclic subgroup of order p over k for large p ([Se]).

For a finite set S of primes of k, denote by $X_0(p)(k, S)$ the subset of $X_0(p)(k)$ consisting of the points which have potentially good reduction outside of S.

COROLLARY 4. *For a constant C, the k-rational points in $X_0(p)(k, S)$ of Type 3 are the C.M. points for the prime numbers p with $p > C$, $p \equiv 11 \pmod{12}$.*

Proof. Let x be a k-rational point on $X_0(p)$ of Type 3, and λ, L and φ_λ be as before. Then the rational prime p splits in L, and φ_λ is $L(\zeta_m)^\times$-valued for a primitive $m = (12, p-1)^{th}$ root of unity. If $p \equiv 11 \pmod{12}$, then $L = \mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-3})$ and $m = 2$.

References

[Ab] Abramovich, D.: Formal finiteness and the uniform boundedness conjecture. A footnote to a paper of Kamienny and Mazur, preprint.

[C-S] Cornell, G. and Silverman, J. H.: *Arithmetic Geometry*. Springer-Verlag, Berlin (1985).

[D-R] Deligne, P. and Rapoport, M.: 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, Springer-Verlag, Berlin (1973).

[Fa] Falting, G. and Wüstholz et al.: Rational Points, Seminar Bonn/Wuppertal 1983–84, Aspects of Math., Friedr. Vieweg and Sohn (1984).

[Ka1] Kamienny, S.: Torsion points on elliptic curves and q-coefficients of modular forms, *Invent. Math.* 109(2) (1992) 221–230.

[Ka2] Kamienny, S.: A letter to B. Mazur.

[K-M] Kamienny, S. and Mazur B.: Rational torsion of prime order in elliptic curves over number fields, preprint.

[Ke1] Kenku, M. A.: On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$, *J. Lond. Math. Soc.* 23 (1981) 415–427.

[Ke2] Kenku, M. A.: Certain torsion points on elliptic curves defined over quadratic fields, *J. Lond. Math. Soc.* 2 (1978) 233–240.

[K-Mo] Kenku, M.A. and Momose, F.: Torsion points on elliptic curves defined over quadratic fields, *Nagoya Math. J.* 109 (1988) 125–149.

[La1] Lang, S.: *Elliptic Functions*, Addison-Wesley, Reading Math. (1973).

[La2] Lang, S.: *Algebraic Number Theory*, GTM 110, Springer-Verlag (1970).

[Ma1] Mazur, B.: Modular curves and the Eisenstein ideal, *Publ. Math. I.H.E.S.* 47 (1977) 33–186.

[Ma2] Mazur, B.: Rational isogenies of prime degree, *Invent. Math.* 44 (1978) 129–162.

[Mo] Momose, F.: p-Torsion points on elliptic curves defined over quadratic fields, *Nagoya Math. J.*, 96 (1984) 139–165.

[O-T] Oort, F. and Tate, J.: Group schemes of prime order, Ann. Scient. Éc. Nórm. Sup., série 4, 3, 1–21 (1970).

[Ra1] Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$, *Bull. Math. France* 102 (1974) 241–280.

[Ra2] Raynaud, M.: Spécialisation du fonctuer de Picard, *Publ. Math. I.H.E.S.* 38 (1970) 27–76.

[Ri] Ribet, K. A.: Endomorphisms of semistable abelian varieties over number fields, *Ann. of Math.* 101 (1975) 552–562.

[Se] Serre, J. P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972) 259–331

[S-T] Serre, J. P. and Tate, J.: Good reduction of abelian varieties, *Ann. Math.* 88 (1968) 492–517.

[Mf] Modular functions of one variable IV, Lecture Notes in Math. 476, Springer-Verlag, Berlin (1975).

[SGA7] Groupes de Monodromie en Géométrie Algébrique (dirigé par A. Grothendieck avec collaboratiob de M. Raynaud et D. S. Rim), Lecture Notes in Math. 288, Springer-Verlag, Berlin (1972).