J. Korean Math. Soc. **36** (1999), No. 5, pp. 945–958

DEGREE OF ISOGENIES OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

SOONHAK KWON

ABSTRACT. Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication. Suppose that E is defined over $F = \mathbb{Q}(j(E))$. We study possible degrees of F–isogenies of E.

1. Introduction

Let E be an elliptic curve over $\mathbb{C}$, the field of complex numbers, with complex multiplication. Then the ring, $End\,E$, of endomorphism of E is isomorphic to an order $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ of a maximal order $\mathcal{O}_K$ of an imaginary quadratic field $K \cong End\,E \otimes \mathbb{Q}$. Write $K = \mathbb{Q}(\sqrt{D})$ where D is a squarefree integer. The discriminant d_K of K is $4D$ when $D \equiv 2, 3 \mod 4$ and is D when $D \equiv 1 \mod 4$. Let $j(E)$ be the j-invariant of E. Then the field $K_f = K(j(E))$ is the ring class field of K with conductor f. We may assume that E is defined over $F = \mathbb{Q}(j(E))$ which is a minimal field of definition of E. We are mainly interested in the classification of all possible degrees N of cyclic isogeny $E' \to E$ where both E' and the isogeny are defined over F. Furthermore, we will classify all elliptic curves E' defined over F which are F–isogenous to E. Note that such E' is necessarily a CM–curve. Classification of degrees of cyclic isogenies of elliptic curves without the restriction of complex multiplication for a given number field is a very interesting problem and the case for $\mathbb{Q}$ is settled by Mazur [11] (See also [9]). There has been some progress in the case of quadratic fields (See [11] [5] [12]). In particular it is proved in [12] that for a given quadratic field k which is not an imaginary field of class number one, there is an effective constant C such that no elliptic curve over k has a k–isogeny of prime degree p

Received April 7, 1999.
1991 Mathematics Subject Classification: Primary 11G05; Secondary 11G15.
Key words and phrases: isogeny, complex multiplication.

when p is greater than C. Frey [5] also showed that for a given prime p greater than 240, there is no elliptic curve having a rational isogeny of degree p over almost all quadratic fields. But it seems to me that there is no satisfactory result available at this moment concerning the degrees of isogenies of CM-curves over F. If we restrict our attention to K_f-isogenies, then it is well known that E has a cyclic isogeny of degree p defined over K_f for infinitely many primes p. And those primes p are well understood. However, it will turn out that there are only finitely many integers N such that N is a degree of cyclic isogeny $E' \to E$ where both E' and the isogeny are defined over F. In fact we will prove that those N should be (roughly speaking) a divisor of $f^2 d_K$.

Regarding torsion subgroups of CM-curves, Parish [14] classified all possible types of torsion subgroups over K_f and F. In particular he showed that if P is a torsion point of order N in K_f, then N must be $1, 2, 3, 4$ or 6.

2. Ring class fields and isogenies over their subfields

From now on, we assume $D \neq -1, -3$ so that the group of units of $\mathcal{O}_K$ is $\{\pm 1\}$. Those exceptional cases, $D = -1, -3$, can be treated in a similar manner by slightly adjusting some of the statements, i.e. Proposition 2.1 and Theorem 4.1 should be modified appropriately for each case. Let us review some of the basic facts of the class field theory. We have an isomorphism between the ideal class group $Cl(\mathcal{O}_f)$ and $Gal(K_f/K)$ via the Artin map. Letting $\langle \tau \rangle = Gal(K_f/F)$, the galois group of K_f over $\mathbb{Q}$ is a generalized dihedral group generated by $\sigma \in Gal(K_f/K)$ and τ with the relation $\sigma\tau = \tau\sigma^{-1}$. The class number h of $\mathcal{O}_f$ is related to the class number of the maximal order by the well known formula,

$$h(\mathcal{O}_f) = h(\mathcal{O}_K) f \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right), \tag{2.1}$$

where p denotes a prime and $\left(\frac{d_K}{p}\right)$ is the Kronecker symbol. We also have the following equality [17],

$$\sigma_{\mathfrak{b}}(j(\mathfrak{a})) = j(\mathfrak{a}\overline{\mathcal{O}_f \cap \mathfrak{b}}), \tag{2.2}$$

where $\mathfrak{a}, \mathfrak{b}$ are proper (or invertible) ideals of $\mathcal{O}_f, \mathcal{O}_K$ respectively and $\sigma_{\mathfrak{b}}$ is an Artin symbol $\left(\frac{K_f/K}{\mathfrak{b}}\right)$ in $Gal(K_f/K)$.

PROPOSITION 2.1. *Suppose that $K_{f'}$ is a subfield of K_f. Then f' divides $2f$ when f is an odd integer and 2 splits in K, and f' divides f for all other cases. Conversely if f and f' satisfy the above conditions, then $K_{f'}$ is a subfield of K_f.*

Proof. The proof of converse statement is easily derived from the definition of ring class fields. Now suppose that we have number fields H and L such that L is a finite abelian extension of H. Then there is a conductor $\mathfrak{f}(L/H)$ which is (excluding infinite part) an integral ideal of H and satisfies certain conditions in the class field theory. Suppose that we have another finite abelian extension M of H such that L is also a subfield of M. We claim that $\mathfrak{f}(L/H)$ divides $\mathfrak{f}(M/H)$. By the theorem of Hasse on conductor and discriminant, we have the following [1],

$$\mathfrak{f}(L/H) = lcm\ \mathfrak{f}_\chi,$$

where χ runs over all characters $\chi : Gal(L/H) \to \mathbb{C}$ and $\mathfrak{f}_\chi$ is $\mathfrak{f}(H_\chi/H)$ for which H_χ is the fixed field of $ker\ \chi$. Viewing $Gal(L/H)$ as the quotient group $Gal(M/H)/Gal(M/L)$, χ can be lifted to a character $\widetilde{\chi} : Gal(M/H) \to \mathbb{C}$ such that

$$ker\ \widetilde{\chi}/Gal(M/L) = ker\ \chi,$$

which shows that $ker\ \chi$ and $ker\ \widetilde{\chi}$ have the same fixed field. Thus we have $\mathfrak{f}_\chi = \mathfrak{f}_{\widetilde{\chi}}$ for all χ and $\mathfrak{f}(L/H)$ divides $\mathfrak{f}(M/H)$, which finishes the proof of the claim. Suppose we have inclusions $K \subset K_{f'} \subset K_f$. Since it can be shown that $\mathfrak{f}(K_f/K)$ is $g\mathcal{O}_K$ only when $f = 2g$ where g is an odd integer and 2 splits in K and the conductor is $f\mathcal{O}_K$ for all other cases [4, pp. 195–198], our proposition naturally follows from the claim. □

Let $\mathcal{H}$ be the upper half plane and $\Gamma_0(N)$, where N is a positive integer, be the set of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$ with $c \equiv 0 \mod N$. Then the space $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$, where $\mathcal{H}^* = \mathcal{H} \cup \mathbf{P}^1(\mathbb{Q})$, is a compact Riemann surface which has a structure of algebraic curve defined over $\mathbb{Q}$. Every non-cuspidal point of $X_0(N)$ corresponds to a pair (E, C), where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of $E(\mathbb{C})$ of order N. (E, C) and (E', C') give the same point in $X_0(N)$ if and only if there is an isomorphism ϕ such that $\phi E = E'$ and $\phi C = C'$.

By a suitable choice of basis, we may express the corresponding lattice Λ of E as $[\omega_1, \omega_2]$ and C as $\langle \omega_2/N \rangle$ where ω_2/ω_1 is in $\mathcal{H}$. Sometimes we use the notation $([\omega_1, \omega_2], \langle \omega_2/N \rangle)$ to denote the pair (E, C). If E is a CM–curve, then by the theory of complex multiplication, (E, C) is defined over $K(j(E), j(E/C))$ where $K \cong End\, E \otimes \mathbb{Q}$. Note that we have an analytic isomorphism, $\mathbb{C}/\Lambda \cong E$ by sending z to $(\mathcal{P}(z), \mathcal{P}'(z))$, where

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - 0} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

is the Weierstrass $\mathcal{P}$-function corresponding to the lattice Λ. Now let $\mathcal{P}_1(z)$ be the Weierstrass $\mathcal{P}$-function corresponding to the lattice $[\omega_1, \omega_2/N]$. Then we have the following formula due to Keiport [18],

$$\mathcal{P}_1(z) = \mathcal{P}(z) + \sum_{n=1}^{N-1} \mathcal{P}(z + \frac{n\omega_2}{N}) - \mathcal{P}(\frac{n\omega_2}{N}).$$

Using the above formula and elementary properties of symmetric functions, we get the following (See also [13]).

LEMMA 2.2. *Let E be an elliptic curve defined over a number field L. Let $[\omega_1, \omega_2]$ be the corresponding lattice for E and $C = \langle \mathcal{P}(\omega_2/N), \mathcal{P}'(\omega_2/N)) \rangle$ be a cyclic subgroup of order N. Then, $\sigma C = C$ for all σ in $Gal(\overline{L}/L)$ if and only if E/C and the isogeny $E \to E/C$ are defined over L.*

For a given lattice Λ in $\mathbb{C}$, the corresponding elliptic curve $E \cong \mathbb{C}/\Lambda$ can be written as

$$E : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

where,

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda - 0} \frac{1}{\omega^4}, \quad g_3(\Lambda) = 140 \sum_{\omega \in \Lambda - 0} \frac{1}{\omega^6}.$$

Examining the q-expansions of corresponding modular forms for g_2 and g_3, we get $\overline{g_2(\Lambda)} = g_2(\overline{\Lambda})$ and $\overline{g_3(\Lambda)} = g_3(\overline{\Lambda})$, where $\overline{\Lambda}$ is the complex conjugation of Λ. Thus we have $\overline{j(\Lambda)} = j(\overline{\Lambda})$ and since two lattices are homothetic if and only if they have the same j-invariant, we find that $\overline{\Lambda} = \Lambda$ if and only if $g_2(\Lambda)$ and $g_3(\Lambda)$ are real numbers. The author would like to thank D. Rohrlich for providing crucial hints for the proof of the following proposition.

PROPOSITION 2.3. *Let $\mathcal{O}_f$ be the order of conductor f in an imaginary quadratic field K. Let $\mathfrak{a}$ and $\mathfrak{b}$ be proper integral ideals of $\mathcal{O}_f$.*

1. *$\mathfrak{b} \to \mathfrak{b}\mathfrak{a}^{-1}$ gives a $\mathbb{Q}(j(\mathfrak{b}))$-isogeny between elliptic curves defined over $\mathbb{Q}(j(\mathfrak{b}))$ if and only if $\mathfrak{a} = \bar{\mathfrak{a}}$.*
2. *Let f' be a positive integer which divides f. Then $\mathfrak{b} \to \mathfrak{b}\mathcal{O}_{f'}$ gives a $\mathbb{Q}(j(\mathfrak{b}))$-isogeny between elliptic curves defined over $\mathbb{Q}(j(\mathfrak{b}))$.*

Proof. **1.** First we prove that $\mathcal{O}_f \to \mathcal{O}_f\mathfrak{a}^{-1}$ is defined over $\mathbb{Q}(j(\mathcal{O}_f))$ when $\mathfrak{a} = \bar{\mathfrak{a}}$. Without loss of generality, we may assume $\mathfrak{a}$ is a primitive ideal, i.e. $\mathfrak{a}$ is not divisible by any integer greater than one. Then there exist elliptic curves E and E' defined over $K(j(\mathcal{O}_f))$ such that $E \cong \mathbb{C}/\lambda\mathcal{O}_f$, $E' \cong \mathbb{C}/\lambda\mathcal{O}_f\mathfrak{a}^{-1}$ for some complex number λ and an isogeny $\varphi : E \to E'$ defined over $K(j(\mathcal{O}_f))$ which is cyclic and of degree $|\mathcal{O}_f/\mathfrak{a}|$. Now choose μ such that $E_{\frac{1}{\mu^2}} \cong \mathbb{C}/\mu\lambda\mathcal{O}_f$ is defined over $\mathbb{Q}(j(\mathcal{O}_f))$. By the remark just before this proposition, we get $\mu\lambda = \pm\overline{\mu\lambda}$. Write E' as $y^2 = 4x^3 - g_2x - g_3$. Then $E'_{\frac{1}{\mu^2}} : y^2 = 4x^3 - \frac{1}{\mu^4}g_2x - \frac{1}{\mu^6}g_3$ has real coefficients because $\mu\lambda = \pm\overline{\mu\lambda}$ and they are in $K(j(\mathcal{O}_f))$ because μ^2 is in $K(j(\mathcal{O}_f))$. Since $\mathbb{Q}(j(\mathcal{O}_f))$ is the maximal real subfield of $K(j(\mathcal{O}_f))$, we find that $E'_{\frac{1}{\mu^2}}$ is also defined over $\mathbb{Q}(j(\mathcal{O}_f))$ and we have an isogeny $\varphi' : E_{\frac{1}{\mu^2}} \to E'_{\frac{1}{\mu^2}}$ between elliptic curves defined over $\mathbb{Q}(j(\mathcal{O}_f))$, where φ' is induced by the twist of E. Now it is easy to check $\overline{\varphi'} = \varphi'$ which shows that the isogeny is also defined over $\mathbb{Q}(j(\mathcal{O}_f))$. Conversely if $\mathcal{O}_f \to \mathcal{O}_f\mathfrak{a}^{-1}$ is defined over $\mathbb{Q}(j(\mathcal{O}_f))$, then we have $\overline{\mathcal{O}_f\mathfrak{a}^{-1}} = \mathcal{O}_f\mathfrak{a}^{-1}$, which implies $\bar{\mathfrak{a}} = \mathfrak{a}$. Now let us prove the general case. Again assume $\bar{\mathfrak{a}} = \mathfrak{a}$. Note that, by the previous argument and by the Lemma 2.2, we have an elliptic curve defined over $\mathbb{Q}(j(\mathcal{O}_f))$ and a cyclic subgroup C of order $|\mathcal{O}_f/\mathfrak{a}|$ such that C is invariant under galois action by $Gal(\overline{\mathbb{Q}(j(\mathcal{O}_f))}/\mathbb{Q}(j(\mathcal{O}_f))$. Thus we have an isogeny $\varphi : E \to E/C$ where everything is defined over $\mathbb{Q}(j(\mathcal{O}_f))$. Up to a homothety of $\mathfrak{b}$, we may assume that $\mathfrak{b}$ and f are relatively prime. Then $\mathfrak{b}\mathcal{O}_K = \mathfrak{b}_1$ is an ideal of $\mathcal{O}_K$ such that $\mathcal{O}_f \cap \mathfrak{b}_1 = \mathfrak{b}$. Now letting $\sigma_{\mathfrak{b}_1}$ be the Artin symbol $\left(\frac{K_f/K}{\mathfrak{b}_1}\right)$, by the formula (2.2) we have

$$\sigma_{\mathfrak{b}_1^{-1}}(j(E)) = \sigma_{\mathfrak{b}_1^{-1}}(j(\mathcal{O}_f)) = j(\mathcal{O}_f \cap \mathfrak{b}_1) = j(\mathfrak{b}),$$

and

$$\sigma_{\mathfrak{b}_1^{-1}}(j(E/C)) = \sigma_{\mathfrak{b}_1^{-1}}(j(\mathfrak{a}^{-1})) = j(\mathfrak{a}^{-1}\mathcal{O}_f \cap \mathfrak{b}_1) = j(\mathfrak{b}\mathfrak{a}^{-1}).$$

Now writing $\sigma = \sigma_{\mathfrak{b}_1^{-1}}$, $\varphi^\sigma : E^\sigma \to (E/C)^\sigma$ gives an isogeny defined over $\mathbb{Q}(j(\mathfrak{b}))$ which corresponds to the lattice inclusion $\mathfrak{b} \to \mathfrak{b}\mathfrak{a}^{-1}$. Note that, letting $C' = ker\ \varphi^\sigma$, we have $(E/C)^\sigma = E^\sigma/C'$. Conversely, if we have an isogeny $\mathfrak{b} \to \mathfrak{b}\mathfrak{a}^{-1}$ defined over $\mathbb{Q}(j(\mathfrak{b}))$, then by applying the formula (2.2) again, we get an isogeny $\mathcal{O}_f \to \mathcal{O}_f\mathfrak{a}^{-1}$ defined over $\mathbb{Q}(j(\mathcal{O}_f))$ and therefore $\overline{\mathfrak{a}} = \mathfrak{a}$.

2. Since $\mathcal{O}_f$ and $\mathcal{O}_{f'}$ are invariant under complex conjugation, using the same idea, it is easy to show $\mathcal{O}_f \to \mathcal{O}_{f'}$ is defined over $\mathbb{Q}(j(\mathcal{O}_f))$. Then writing $\mathfrak{b}\mathcal{O}_{f'} = \mathfrak{b}_1$ and $\mathfrak{b}\mathcal{O}_K = \mathfrak{b}_2$, we get $\mathfrak{b} = \mathcal{O}_f \cap \mathfrak{b}_2$ and $\mathfrak{b}_1 = \mathcal{O}_{f'} \cap \mathfrak{b}_2$. Now we have

$$\sigma_{\mathfrak{b}_2^{-1}}(j(\mathcal{O}_f)) = j(\mathcal{O}_f \cap \mathfrak{b}_2) = j(\mathfrak{b}),$$

and

$$\sigma_{\mathfrak{b}_2^{-1}}(j(\mathcal{O}_{f'})) = j(\mathcal{O}_{f'} \cap \mathfrak{b}_2) = j(\mathfrak{b}\mathcal{O}_{f'}),$$

and the rest of the proof is similar to the first case. □

3. Proper ideals of the order $\mathcal{O}_f$

Let $\mathfrak{a}$ be a primitive proper ideal of $\mathcal{O}_f$ with index N. Then as a $\mathbb{Z}$–module, $\mathfrak{a}$ can be written as $[N, b + fw_K]$ for a suitable choice of integer b, where $w_K = \dfrac{d_K + \sqrt{d_K}}{2}$. Writing $B = -(2b + fd_K)$, we get $b + fw_K = \dfrac{-B + f\sqrt{d_K}}{2}$ and

$$\begin{aligned}\frac{1}{4}(B^2 - f^2 d_K) &= \frac{1}{4}\{(2b + fd_K)^2 - f^2 d_K\} \\ &= b^2 + bfd_K + \frac{f^2}{4}(d_K^2 - d_K) \\ &= (b + fw_K)(b + f\overline{w_K}),\end{aligned}$$

which is divisible by N. Thus we have $B^2 - 4NC = f^2 d_K$ for some integer C. Since $\dfrac{b + fw_K}{N}$ is a root of $Nx^2 + Bx + C = 0$ and $End\,\mathfrak{a} = \mathcal{O}_f$, we get $(N, B, C) = 1$. Now assume $\overline{\mathfrak{a}} = \mathfrak{a}$. Then from the relation $b + fw_K + b + f\overline{w_K} = 2b + fd_K$, we find that N divides B. Therefore, if $\mathfrak{a}$ is a proper ideal of $\mathcal{O}_f$ with $\mathcal{O}_f/\mathfrak{a}$ cyclic of order N and $\overline{\mathfrak{a}} = \mathfrak{a}$, then there exist integers N, B, C with $(N, B, C) = 1$ such that $B^2 - 4NC = f^2 d_K$ and N divides B. Conversely if there exist N, B, C satisfying the above condition, then the module $\mathfrak{a} = [N, \dfrac{-B + f\sqrt{d_K}}{2}]$ gives a primitive

proper ideal of $\mathcal{O}_f$ with index N and $\bar{\mathfrak{a}} = \mathfrak{a}$. Thus we only need to solve the following equation,

$$B^2 - 4NC = f^2 d_K, \qquad N|B, \quad (N, B, C) = 1,$$

to find such proper ideals we want. Suppose we have an ideal $\mathfrak{a}$ with $\mathcal{O}_f/\mathfrak{a}$ cyclic of order N and invariant under complex conjugation. Let p be a prime which divides N. Write $N = p^n N'$ with $n \geq 1$ and $(p, N') = 1$. Then there is a proper ideal $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, $|\mathcal{O}_f/\mathfrak{b}| = p^n$ and $\bar{\mathfrak{b}} = \mathfrak{b}$, which implies that it is enough to solve the equation when N is a power of p for every prime p.

PROPOSITION 3.1. *Let $\mathcal{O}_f = [1, fw_K]$ be the order of conductor f of an imaginary quadratic field K. Let p be a prime which divides $f^2 d_K$ and s be the highest power of p such that p^s divides $f^2 d_K$. Then all primitive proper ideals $\mathfrak{a}$ of $\mathcal{O}_f$ with index $|\mathcal{O}_f/\mathfrak{a}|$ a power of p and $\bar{\mathfrak{a}} = \mathfrak{a}$ can be classified as follows.*

1. *When $p \neq 2$, there is a unique $\mathfrak{a}$ for which*

$$\begin{aligned} \mathfrak{a} &= \left[p^s, \frac{f\sqrt{d_K}}{2}\right] && \text{if } \frac{f^2 d_K}{p^s} \text{ is even,} \\ &= \left[p^s, \frac{-p^s + f\sqrt{d_K}}{2}\right] && \text{if } \frac{f^2 d_K}{p^s} \text{ is odd.} \end{aligned}$$

2. *When $p = 2$,*
   (a) *if 16 divides $f^2 d_K$, there are two possible cases, $|\mathcal{O}_f/\mathfrak{a}| = 4$ or 2^{s-2}. There is a unique $\mathfrak{a}$ with $|\mathcal{O}_f/\mathfrak{a}| = 4$, and*

$$\begin{aligned} \mathfrak{a} &= \left[4, \frac{-4 + f\sqrt{d_K}}{2}\right] && \text{if } \frac{f^2 d_K}{16} \text{ is even,} \\ &= \left[4, \frac{f\sqrt{d_K}}{2}\right] && \text{if } \frac{f^2 d_K}{16} \text{ is odd.} \end{aligned}$$

   There are two different (non homothetic) ideals $\mathfrak{a}$ with $|\mathcal{O}_f/\mathfrak{a}| = 2^{s-2}$ and $s > 4$, which can be described as

$$\mathfrak{a} = \left[2^{s-2}, \frac{f\sqrt{d_K}}{2}\right], \quad \left[2^{s-2}, \frac{-2^{s-2} + f\sqrt{d_K}}{2}\right].$$

(*b*) *if* 16 *does not divide* f^2d_K, *the only possible case is*

$$\begin{aligned} \mathfrak{a} &= \left[2, \frac{f\sqrt{d_K}}{2}\right] && \text{when } D \equiv 2\ (4) \text{ and } f = \text{ odd}, \\ &= \left[2, \frac{-2+f\sqrt{d_K}}{2}\right] && \text{when } D \equiv 3\ (4) \text{ and } f = \text{ odd}. \end{aligned}$$

Proof. **1.** When $p \neq 2$, letting $N = p^n$ and $B = p^nB_1$ where $n \geq 1$, we get

$$p^nB_1^2 - 4C = \frac{f^2d_K}{p^n}.$$

If $\dfrac{f^2d_K}{p^n}$ is divisible by p, then p divides C which is impossible. Thus $n = s$ where s is the highest power of p such that p^s divides f^2d_K. Now if $\dfrac{f^2d_K}{p^s}$ is even, then $B_1 = 2k$ for an integer k and the corresponding ideal is

$$\left[N, \frac{-B+f\sqrt{d_K}}{2}\right] = \left[p^s, \frac{-2p^sk+f\sqrt{d_K}}{2}\right] = \left[p^s, \frac{f\sqrt{d_K}}{2}\right].$$

If $\dfrac{f^2d_K}{p^s}$ is odd, then $B_1 = 2k+1$ and the ideal is

$$\left[p^s, \frac{-p^s(2k+1)+f\sqrt{d_K}}{2}\right] = \left[p^s, \frac{-p^s+f\sqrt{d_K}}{2}\right].$$

2. The case when $p = 2$. Write $N = 2^n$ and $B = 2^nB_1$. Then we have

$$2^{2n}B_1^2 - 2^{n+2}C = f^2d_K.$$

When 16 divides f^2d_K, we easily conclude that n is either 2 or $s-2$. Suppose $N = 4$. Then we get a unique ideal $\mathfrak{a}$ using the same technique as in the first case. Now suppose $N = 2^{s-2}$ and $s > 4$. Then we have

$$2^{s-4}B_1^2 - C = \frac{f^2d_K}{2^s}.$$

Since $\dfrac{f^2d_K}{2^s}$ is odd, any integer B_1 gives a solution of above equation. When $B_1 = 2k$, the corresponding ideal is

$$\left[2^{s-2}, \frac{-2^{s-2}\cdot 2k+f\sqrt{d_K}}{2}\right] = \left[2^{s-2}, \frac{f\sqrt{d_K}}{2}\right].$$

When $B_1 = 2k+1$, we have

$$\left[2^{s-2}, \frac{-2^{s-2}(2k+1)+f\sqrt{d_K}}{2}\right] = \left[2^{s-2}, \frac{-2^{s-2}+f\sqrt{d_K}}{2}\right].$$

Note that they are different elements in the ideal class group of $\mathcal{O}_f$. When 16 does not divide $f^2 d_K$, it is easy to check that there exists an ideal $\mathfrak{a}$ in $\mathcal{O}_f$ with $\bar{\mathfrak{a}} = \mathfrak{a}$ and $\mathcal{O}_f/\mathfrak{a}$ cyclic of order power of 2 only when f is odd and 2 is ramified in K. It is an intersection of the prime ideal of $\mathcal{O}_K$ lying above 2 with $\mathcal{O}_f$. □

4. Restriction to the degrees of isogenies

Let Λ be a lattice with complex multiplication. Then for any oriented basis $[\omega_1, \omega_2]$ for Λ, writing $\tau = \omega_2/\omega_1 \in \mathcal{H}$, τ is a root of a quadratic equation

$$Ax^2 + Bx + C = 0,$$

where A, B and C are integers with $(A, B, C) = 1$. Letting d_K be the discriminant of the quadratic field $K = \mathbb{Q}(\tau)$, we may write

$$B^2 - 4AC = f^2 d_K,$$

for some integer $f \geq 1$. Then $End\,\Lambda$ is equal to $\mathcal{O}_f$. Now suppose that Λ is a cyclic sublattice of Λ' with index N. Then for a suitable choice of basis, we have $\Lambda = [\omega_1, \omega_2]$ and $\Lambda' = [\omega_1, \omega_2/N]$. Since τ/N is a root of the following quadratic equation

$$N^2 Ax^2 + NBx + C = 0,$$

we find that $End\,\Lambda' = \mathcal{O}_{f'}$ where f' divides Nf. In particular, if $N = p$ is a prime and does not divide f, then we have $End\,\Lambda' = \mathcal{O}_f$ or $\mathcal{O}_{pf}$.

THEOREM 4.1. *Let E be an elliptic curve with complex multiplication such that $End\,E \cong \mathcal{O}_f$ where $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ and $K = \mathbb{Q}(\sqrt{D})$. Let $F = \mathbb{Q}(j(E))$ and suppose that E is defined over F. Let S_f be the set of all positive divisors of f and S'_f be the set of all integers which are indexes of primitive proper ideals of $\mathcal{O}_f$ invariant under complex conjugation.*

1. *If f is even or 2 does not split in K, then there is an elliptic curve E' defined over F and a cyclic F–isogeny $E' \to E$ of degree N if and only if $N = ab$ where a is in S_f and b in $S'_{f/a}$.*

2. *If f is odd and 2 splits in K, then there exists such E' if and only if N is either ab or $2ab$ where a is in S_f and b in $S'_{f/a}$.*

Proof. **1.** Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_f$ with $(\mathfrak{a}, f) = 1$ which represents E up to homothety. Then E' (up to isomorphism over F) corresponds to a lattice $L \supset \mathfrak{a}$ such that $\mathfrak{a} \to L$ is cyclic of index N. Since $\mathbb{Q}(j(L))$ is a subfield of F, we find, by Proposition 2.1, that $End\, L = \mathcal{O}_{f'}$ where f' divides f. Thus we have the following inclusions,

$$\mathfrak{a} \to \mathfrak{a}\mathcal{O}_{f'} \to L,$$

where $\mathfrak{a} \to \mathfrak{a}\mathcal{O}_{f'}$ is cyclic of index $a = f/f'$ and both $\mathfrak{a}\mathcal{O}_{f'}$ and L are proper ideals of $\mathcal{O}_{f'}$. Write $L = \mathfrak{a}\mathcal{O}_{f'}\mathfrak{b}^{-1}$ where $\mathfrak{b}$ is a primitive ideal and $|\mathcal{O}_{f'}/\mathfrak{b}| = N/a = b$. Since $\mathfrak{a} \to \mathfrak{a}\mathcal{O}_{f'}$ is defined over F by Proposition 2.3 and $\mathfrak{a} \to L$ is also defined over F from the assumption, $\mathfrak{a}\mathcal{O}_{f'} \to L$ must be defined over the same field. Again by Proposition 2.3, we have $\overline{\mathfrak{b}} = \mathfrak{b}$. Conversely, for a given $N = ab$ where $a \in S_f$ and $b \in S'_{f/a}$, we have the following inclusions

$$\mathfrak{a} \to \mathfrak{a}\mathcal{O}_{f/a} \to \mathfrak{a}\mathcal{O}_{f/a}\mathfrak{b}^{-1},$$

where $\mathfrak{b}$ is a primitive ideal of $\mathcal{O}_{f/a}$ with index b and $\overline{\mathfrak{b}} = \mathfrak{b}$. Though each inclusion is cyclic, we need to prove that $\mathfrak{a} \to \mathfrak{a}\mathcal{O}_{f/a}\mathfrak{b}^{-1}$ is cyclic. If not, the quotient group has a p torsion part which is not cyclic for some prime p. Therefore we have a proper ideal J dividing $\mathfrak{b}$ such that

$$J^2 = J\overline{J} = p^m\mathcal{O}_{f/a},$$

where $m \geq 1$ and we have an integer $n \geq 1$ such that p^n divides a with $(p, a/p^n) = 1$. Since $\mathfrak{a} \to \mathfrak{a}\mathcal{O}_{f/a}J^{-1}$ is not cyclic, $\mathfrak{a}\mathcal{O}_{f/a}J^{-1}/\mathfrak{a}$ is annihilated by the multiplication ap^{m-1}. Thus

$$\mathfrak{a} \supset ap^{m-1}J^{-1}\mathfrak{a}\mathcal{O}_{f/a} = \frac{a}{p}J\mathfrak{a}\mathcal{O}_{f/a} = \frac{a}{p}J\mathcal{O}_{f/a}\mathfrak{a}.$$

Since $End\, \mathfrak{a} = \mathcal{O}_f$, we have $\dfrac{a}{p}J\mathcal{O}_{f/a} \subset \mathcal{O}_f$ and

$$\frac{a}{p}J\mathcal{O}_{f/a} \subset \frac{a}{p}\mathcal{O}_{f/a} \cap \mathcal{O}_f = \frac{a}{p}\mathcal{O}_{pf/a}.$$

Thus we have $J\mathcal{O}_{f/a} \subset \mathcal{O}_{pf/a}$, which is easily seen to be impossible in view of the expression of J as a $\mathbb{Z}$–module.

2. Let $\mathfrak{a} \subset L$ with index N and $End\, L = \mathcal{O}_{f'}$. By Proposition 2.1, f' divides $2f$. If f' is odd, then f' divides f and the same argument with previous case can be applied. Thus let us assume $f' = 2f''$ and f'' divides

f. By the remark before the statement of this theorem, we find that f' divides Nf. Since f is an odd integer, N must be even. Therefore we have another lattice $\mathfrak{a}'$ such that $\mathfrak{a} \to \mathfrak{a}' \to L$ are inclusions and $\mathfrak{a} \to \mathfrak{a}'$ has index 2. Again by the same remark, $End\,\mathfrak{a}'$ is either $\mathcal{O}_f$ or $\mathcal{O}_{2f}$. If it is $\mathcal{O}_f$, we have a proper ideal $\mathfrak{p}$ of $\mathcal{O}_f$ such that $\mathfrak{a}' = \mathfrak{a}\mathfrak{p}^{-1}$. Therefore the elliptic curve corresponding to the ideal $\mathfrak{a}$ has a cyclic subgroup of order 2 which is not defined over F because 2 splits in K, which gives a contradiction. Thus we have $End\,\mathfrak{a}' = \mathcal{O}_{2f}$ and the following inclusions,

$$\mathfrak{a} \to \mathfrak{a}' \to \mathfrak{a}'\mathcal{O}_{2f''} \to L.$$

Since $\mathfrak{a}' \to L$ can be dealt with in a similar way, we are done. Conversely, assume $N = 2ab$ where $a \in S_f$ and $b \in S'_{f/a}$. Then for a given proper ideal $\mathfrak{a}$ of $\mathcal{O}_f$, there is a unique lattice $\mathfrak{a}'$ such that $\mathfrak{a} \subset \mathfrak{a}'$ has index 2 and $End\,\mathfrak{a}' = \mathcal{O}_{2f}$. (The other two lattices which contain $\mathfrak{a}$ as a sublattice of index 2 are $\mathfrak{a}\mathfrak{p}^{-1}$ and $\mathfrak{a}\overline{\mathfrak{p}}^{-1}$ where $\mathfrak{p}$ is a proper ideal of $\mathcal{O}_f$ such that $\mathfrak{p}\overline{\mathfrak{p}} = 2\mathcal{O}_f$.) Thus we have the following inclusions,

$$\mathfrak{a} \to \mathfrak{a}' \to \mathfrak{a}'\mathcal{O}_{2f/a} \to \mathfrak{a}'\mathcal{O}_{2f/a}\mathfrak{b}^{-1},$$

where $\overline{\mathfrak{b}} = \mathfrak{b}$ and $\mathcal{O}_{2f/a}/\mathfrak{b}$ is cyclic of order b. Therefore we have a cyclic isogeny of degree $2ab$ defined over F. □

The above Theorem when combined with Proposition 3.1, gives a complete description of those elliptic curves E' which are F–isogenous to E. It gives an explicit basis for the corresponding lattice of E' for every such E'. An almost immediate corollary is the following.

COROLLARY 4.2. *Let $K, F, \mathcal{O}_f$ and E be as in the* Theorem 4.1.

1. *When f is even and $d_K \equiv 0$ (4) or when $f \equiv 0$ (4) and $d_K \equiv 1$ (4), there exists a cyclic F–isogeny $E' \to E$ of degree N if and only if N divides $\dfrac{f^2 d_K}{4}$. Furthermore for those N, there are exactly two elliptic curves (up to j–invariants) E' if $N \equiv 0$ (4) and there is only one E' if $N \not\equiv 0$ (4).*
2. *When $f \equiv 2$ (4) and $d_K \equiv 1$ (4) or when f is odd and $d_K \not\equiv 5$ (8), there exists such E' if and only if $N = N'$ or $2N'$ where N' is an odd integer dividing $f^2 d_K$. And there is a unique E' for such N.*
3. *When f is odd and $d_K \equiv 5$ (8), there exists such E' if and only if N divides $f^2 d_K$. Here, the existence of E' is unique for such N.*

Proof. It is enough to consider p-power degrees only for each prime p. If p is an odd prime then for every p^r dividing $f^2 d_K$, there are only one f' which divides f and one proper ideal $\mathfrak{b}$ in $\mathcal{O}_{f'}$ with $\overline{\mathfrak{b}} = \mathfrak{b}$ such that $\mathfrak{a} \to \mathfrak{a}\mathcal{O}_{f'} \to \mathfrak{a}\mathcal{O}_{f'}\mathfrak{b}^{-1}$ gives a cyclic isogeny of degree p^r. The case when $p = 2$ can be treated in a similar manner though in this case, Proposition 3.1 implies that there are exactly two isogenies if the degree 2^r is greater than 2. □

Let us give some examples. We fix an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d_K})$ where $d_K = -35$. We will consider those elliptic curves defined over $\mathbb{Q}(j(\mathcal{O}_f))$ when f is $1, 2$ or 4. It is known [2] that the class number of K is two and $j(\mathcal{O}_K) = -2^{15} \cdot 5\sqrt{5} \cdot \epsilon^{12}$ where $\epsilon = \frac{1+\sqrt{5}}{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{5})$. Let $j_1 = j(\mathfrak{p}_5) = j(\mathfrak{p}_7) = 2^{15} \cdot 5\sqrt{5} \cdot \epsilon^{-12}$ where $\mathfrak{p}_5$ (resp. $\mathfrak{p}_7$) is the prime ideal of K lying above 5 (resp. 7). Let E be an elliptic curve defined over $F = \mathbb{Q}(j(\mathcal{O}_K))$ with $j(E) = j(\mathcal{O}_K)$. Then there is an elliptic curve E_1 defined over F with $j(E_1) = j_1$ such that E is F–isogenous to E_1 with degree 5. E is F–isogenous to the d_K–quadratic twist of E_1 (resp. E) with cyclic kernel of order 7 (resp. 35).
Now let E' be an elliptic curve defined over $F' = \mathbb{Q}(j(\mathcal{O}_2))$ with $j(E') = j(\mathcal{O}_2)$ such that E' is F'–isogenous to E with degree 2. Since 2 is inert in $K(\sqrt{d_K})$, we find that the class number $h(\mathcal{O}_2)$ is 6 by the formula (2.1). Since $\mathcal{O}_2 \to \mathcal{O}_K$ gives an isogeny of degree two, $j(\mathcal{O}_2)$ and $j(\mathcal{O}_K)$ satisfy the modular equation $\Phi_2(j(\mathcal{O}_2), j(\mathcal{O}_K)) = 0$ where (See [2] or [17])

$$\begin{aligned}\Phi_2(X,Y) &= X^3 + Y^3 - X^2Y^2 + 2^4 \cdot 3 \cdot 31(X^2Y + XY^2) \\ &\quad -2^4 \cdot 3^4 \cdot 5^3(X^2 + Y^2) + 3^4 \cdot 5^3 \cdot 4027XY \\ &\quad +2^8 \cdot 3^7 \cdot 5^6(X + Y) - 2^{12} \cdot 3^9 \cdot 5^9.\end{aligned}$$

Letting $f(X) = \Phi_2(X, j(\mathcal{O}_K))$, $j(\mathcal{O}_2)$ is a unique real root of the cubic equation $f(X) = 0$, because the other sublattices of $\mathcal{O}_K$ with index two are $[2, w_K], [2, w_K + 1]$ and none of them is homothetic to the complex conjugation of itself. Let $\mathfrak{p}_5' = [5, \sqrt{d_K}], \mathfrak{p}_7' = [7, \sqrt{d_K}]$. Then we have $\mathfrak{p}_5'\mathfrak{p}_7' = \sqrt{d_K}\mathcal{O}_2$. Let $j_1' = j(\mathfrak{p}_5') = j(\mathfrak{p}_7')$. Note that j_1' is the only real conjugate of $j(\mathcal{O}_2)$ of the galois extension K_2 over K. There is an elliptic curve E_1' defined over F' with $j(E_1') = j_1'$ such that E' is F'–isogenous to E_1' with degree 5. E' is F'–isogenous to the d_K–quadratic twist of E_1' (resp. E') with cyclic kernel of order 7 (resp. 35). All other F'–isogenies $E' \to E_0$ are factored as $E' \to E \to E_0$ where $E \to E_0$ are defined over F.

Let E'' be an elliptic curve defined over $F'' = \mathbb{Q}(j(\mathcal{O}_4))$ with $j(E'') = j(\mathcal{O}_4)$ such that E'' is F''–isogenous to E' with degree 2. Note that $j(E'')$ is a root of the cubic equation $g(X) = 0$ where $g(X) = \Phi_2(X, j(\mathcal{O}_2))$. In this case, g has three real roots and the other two roots are $j(\mathcal{O}_K)$ and $j(\mathfrak{p}_4'')$ where $\mathfrak{p}_4'' = [4, 2\sqrt{d_K}]$ is a primitive ideal of $\mathcal{O}_4$ with index 4. Let $\mathfrak{p}_5'' = [5, 2\sqrt{d_K}]$ and $\mathfrak{p}_7'' = [7, 2\sqrt{d_K}]$. An easy computation shows that $\mathfrak{p}_5''\mathfrak{p}_7''\mathfrak{p}_4'' = 2\sqrt{d_K}\mathcal{O}_4$ and from which we deduce that the ideal class group of $\mathcal{O}_4$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. There are elliptic curves E_1'', E_2'', E_3'' defined over F'' with j–invariants $j(\mathfrak{p}_5''), j(\mathfrak{p}_7''), j(\mathfrak{p}_4'')$ respectively such that E'' is F''–isogenous to E_1'' (resp. E_2'', E_3'') with cyclic kernel of order 5 (resp. 7, 4). E'' is F''–isogenous to the $4d_K$–quadratic twist of E_1'' (resp. E_2'', E_3'', E'') with cyclic kernel of order 28 (resp. 20, 35, 140). All other F''–isogenies $E'' \to E_0$ are factored as $E'' \to E' \to E_0$ where $E' \to E_0$ are defined over F'. Note that E'' has two cyclic F''–isogenies of degree 4, and the corresponding curves are E_3'' and E.

References

[1] E. Artin and J. Tate, *Class field theory*, Benjamin notes, New York, 1968.

[2] W. E. H. Berwick, *Modular invariants expressible in terms of quadratic and cubic irrationalities*, Proc. London Math. Soc. **28** (1927), 53–69.

[3] B. J. Birch and W. Kyuk ed., *Modular functions of one variables IV*, Lecture notes in math. no. 476, Springer-Verlag, New York, 1975.

[4] D. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley Press, New York, 1989.

[5] G. Frey, *A remark about isogenies of elliptic curves over quadratic fields*, Compositio Math. **58** (1986), 133–134.

[6] ———, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), 79–83.

[7] B. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture notes in math. no. 776, Springer-Verlag, New York, 1980.

[8] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

[9] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20.

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

[11] ———, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[12] F. Momose, *Isogenies of prime degree over number fields*, Compositio Math. **97** (1995), 329–348.

[13] A. Ogg, *Diophantine equations and modular curves*, Bull. Amer. Math. Soc. **81** (1975), 14–27.

[14] J. L. Parish, *Rational torsion in complex-multiplication elliptic curves*, J. of Number Theory **33** (1989), 257–265.
[15] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
[16] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
[17] ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.
[18] E. T. Whittaker, *A course of modern analysis*, Cambridge Univ. Press, Cambridge, 1962.

Department of Mathematics
Sungkyunkwan University
Suwon 440-746, Korea
E-mail: shkwon@math.skku.ac.kr