

*Pacific
Journal of
Mathematics*

STEINITZ CLASS OF MORDELL–WEIL GROUPS
OF ELLIPTIC CURVES
WITH COMPLEX MULTIPLICATION

TONG LIU AND XIANKE ZHANG

Volume 193 No. 2

April 2000

STEINITZ CLASS OF MORDELL–WEIL GROUPS
OF ELLIPTIC CURVES
WITH COMPLEX MULTIPLICATION

TONG LIU AND XIANKE ZHANG

Let E be an elliptic curve having Complex Multiplication by the ring \mathcal{O}_K of integers of $K = \mathbf{Q}(\sqrt{-D})$, let $H = K(j(E))$ be the Hilbert class field of K . Then the Mordell–Weil group $E(H)$ is an \mathcal{O}_K -module. Its Steinitz class $St(E)$ is studied here. In particular, when D is a prime number, $St(E)$ is determined: If $D \equiv 3 \pmod{4}$ then $St(E) = 1$; if $D \equiv 1 \pmod{4}$ then $St(E) = [\mathcal{P}]^t$, where \mathcal{P} is any prime-ideal factor of 2 in K , $[\mathcal{P}]$ the ideal class of K represented by \mathcal{P} , t is a fixed integer. In addition, general structure for modules over Dedekind domain is also discussed. These results develop the results by D. Dummit and W. Miller for $D = 10$ and specific elliptic curves to more general D and general elliptic curves.

1. Introduction.

Let $K = \mathbf{Q}(\sqrt{-D})$ be an imaginary quadratic number field, \mathcal{O}_K the ring of all integers of K . Let E be an elliptic curve having Complex Multiplication by the ring \mathcal{O}_K . Then E is defined over the field $F = \mathbf{Q}(j(E))$, where $j(E)$ denotes the j -invariant of E . So $H = K(j(E))$ is the Hilbert class field of K , [4], and the Mordell-Weil group $E(H)$ (i.e., all the H -rational points of E) is naturally a module over the Dedekind domain \mathcal{O}_K (operation is the complex multiplication). By the structural theorem for finitely generated modules over Dedekind domain we have

$$E(H) \cong E(H)_{\text{tor}} \oplus \mathcal{O}_K \oplus \cdots \oplus \mathcal{O}_K \oplus \mathcal{A} = E(H)_{\text{tor}} \oplus \mathcal{O}_K^{s-1} \oplus \mathcal{A},$$

where \mathcal{A} is an ideal of \mathcal{O}_K which is uniquely determined by $E(H)$ up to a multiplication by a number from K . Thus $E(H)$ determines uniquely an ideal class $[\mathcal{A}]$ of K represented by \mathcal{A} ; $[\mathcal{A}]$ is said to be the Steinitz class of E and denoted by $St(E)$. (Similarly, any module M over a Dedekind domain R defines an ideal class of R , which is said to be the Steinitz class of M and denoted by $St(M)$.) So the structure of the Mordell-Weil group $E(H)$, as a module over the Dedekind domain \mathcal{O}_K , is uniquely determined by its Steinitz class, rank s , and its torsion part. Therefore, it is important to determine the Steinitz class. D. Dummit and W. Miller, [1] in 1996

determined the Steinitz class of some specific elliptic curves when $D = 10$ and found some of their properties.

Since the Steinitz class $\text{St}(E)$ is essentially concerned only with the free part of $E(H)$, we denote

$$E(\cdot)_f = E(\cdot)/E(\cdot)_{\text{tor}},$$

that is, the quotient group of the Mordell group $E(\cdot)$ modulo its torsion part. Note that $E(\cdot)_f$ is isomorphic to the free part of $E(\cdot)$. This notation will be used also for any subgroup I of $E(\cdot)$ to define I_f . Also we can assume the Weierstrass equation of the elliptic curve E to be ([5])

$$E : y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6$$

with $a_2, a_4, a_6 \in F$.

We will first analyze the interior structure of $E(H)$, give a general theorem for the structure of modules over Dedekind domain, and then determine Steinitz classes $\text{St}(E)$ for some types of elliptic curves. In particular, when $D = p$ is a prime number and $p \equiv 3 \pmod{4}$, we will prove that $\text{St}(E)$ is the principal class of K ; And when $D = p$ is a prime number and $p \equiv 1 \pmod{4}$, we will show that

$$\text{St}(E) = [\mathcal{P}]^t, \quad \text{with } t = l + \log |H^1(G, E(H)_f)|,$$

where \mathcal{P} is any prime factor of 2 in K , $l = \text{rank}_{\mathbf{Z}}(E(F))$ is the \mathbf{Z} -rank of $E(F)$, $|H^1(G, E(H)_f)|$ is the order of the first cohomology group $H^1(G, E(H)_f)$, and $G = \text{Gal}(H/F)$.

2. The Structure of the Mordell group $E(H)$.

Lemma 1. *The degree of the extension H/F is $[H : F] = 2$, where $F = \mathbf{Q}(j(E))$, $H = K(j(E))$, $j(E)$ is the j -invariant of E .*

Proof. Obviously we have $[H : F] \leq 2$. If $[H : F] = 1$, then $K \subset F$. By a result in page 12-13 of [2] we know that $F = \mathbf{Q}(j(E))$ has a real embedding into the complex field \mathbf{C} . Since K is totally imaginary, $K \subset F$ is impossible. Thus $[H : F] = 2$. This proves the lemma. □

Based on Lemma 1, we assume throughout the Galois group of H/F to be $G = \text{Gal}(H/F) = \{1, \sigma\}$. For any $\alpha \in \mathcal{O}_K$, let $[\alpha]$ denote the endomorphism of E corresponding to the multiplication by α . The multiplication by $\sqrt{-D}$ will be important to our following proof. Associating with $E : y^2 = f(x)$, we consider the following elliptic curve

$$E_D : -Dy^2 = f(x).$$

Note that E_D and E are isomorphic via the map

$$i : E_D(\mathbf{C}) \rightarrow E(\mathbf{C}), \quad (x, y) \mapsto (x, \sqrt{-D}y).$$

Therefore we know that

$$\text{End}(E_D) \cong \text{End}(E).$$

So E_D also has complex multiplication by \mathcal{O}_K , and is defined over F . Also via the isomorphism i of E and E_D , we have

$$E_D(F) \cong I,$$

where

$$I = \{(x, \sqrt{-D}y) | (x, \sqrt{-D}y) \in E(H), x, y \in F\}.$$

The subgroup I of $E(H)$ defined here will be very important in the following analysis.

Lemma 2. *The map $i \circ [\sqrt{-D}]$ is an F -isogeny of E_D to E . Thus*

$$\text{rank}_{\mathbf{Z}}(E_D(F)) = \text{rank}_{\mathbf{Z}}(E(F)) = l.$$

Proof. By [1] we have

$$[\sqrt{-D}](x, y) = (a(x), y\sqrt{-D}b(x)),$$

with $a(x), b(x) \in F(x)$. So $i \circ [\sqrt{-D}]$ is an F -isogeny of E_D to E . □

Lemma 3. $(I_f : [\sqrt{-D}]E(F)_f)(E(F)_f : [\sqrt{-D}]I_f) = D^l$.

Proof.

$$\begin{aligned} D^l &= (E(F)_f : [D]E(F)_f) \\ &= (E(F)_f : [\sqrt{-D}]I_f)([\sqrt{-D}]I_f : [D]E(F)_f) \\ &= (E(F)_f : [\sqrt{-D}]I_f)(I_f : [\sqrt{-D}]E(F)_f). \end{aligned}$$

□

Lemma 4. $2E(H)_f \subset E(F)_f \oplus I_f \subset E(H)_f$,

$$\text{rank}_{\mathbf{Z}}(E(H)) = \text{rank}_{\mathbf{Z}}(E(F)) + \text{rank}_{\mathbf{Z}}(E_D(F)) = 2 \text{rank}_{\mathbf{Z}}(E(F)) = 2l.$$

Proof. If $P = (x, y) \in E(F)_f$ with $P \in I_f$, then $y = 0$, which means that P is a torsion point. So $P = O$ is the point at infinity, and $E(F)_f \oplus I_f = E(F)_f + I_f \subset E(H)_f$. For any $Q \in E(H)_f$, we have $2Q = (Q + Q^\sigma) + (Q - Q^\sigma)$, where $G = \text{Gal}(H/F) = \{1, \sigma\}$. Via the definition of $E(F)_f$ and I_f , we have

$$E(F)_f = \{P | P^\sigma = P, \forall P \in E(H)_f\}, \quad I_f = \{P | P^\sigma = -P, \forall P \in E(H)_f\}.$$

So $Q + Q^\sigma \in E(F)_f, Q - Q^\sigma \in I_f, 2Q \in E(F)_f \oplus I_f$. Thus $2E(H)_f \subset E(F)_f \oplus I_f \subset E(H)_f$. This completes the proof. □

As for the index of $E(F)_f \oplus I_f$ in $E(H)_f$, we have the following theorem, which could be also deduced from the cohomology theory of cyclic groups.

Theorem 1.

$$(E(H)_f : E(F)_f \oplus I_f) = \frac{2^l}{|H^1(G, E(H)_f)|},$$

where $|H^1(G, E(H)_f)|$ is the order of the cohomology group $H^1(G, E(H)_f)$.

Proof. Consider the colomology group

$$H^1(G, E(H)_f) = Z^1(G, E(H)_f)/B^1(G, E(H)_f).$$

Let $T = \{P - P^\sigma | P \in E(H)_f\}$. We will prove that $Z^1(G, E(H)_f) \cong I_f$, $B^1(G, E(H)_f) \cong T$. For any cocycle $\xi \in Z^1(G, E(H)_f)$, let $\xi \xrightarrow{\phi} \xi_\sigma$, where $\text{Gal}(H/F) = \{1, \sigma\}$. By the definition of cocycle we have that $0 = \xi_1 = \xi_{\sigma^2} = (\xi_\sigma)^\sigma + \xi_\sigma$, so $(\xi_\sigma)^\sigma = -\xi_\sigma$, thus $\xi_\sigma \in I_f$, and ϕ is a map of $Z^1(G, E(H)_f)$ to I_f . Via the map ϕ we could see that $Z^1(G, E(H)_f) \cong I_f$, $B^1(G, E(H)_f) \cong T$. Now consider the homomorphism $E(H)_f \xrightarrow{\psi=P-P^\sigma} T$. Obviously $2I_f \subset T$. Since $\psi^{-1}(2I_f) = E(F)_f \oplus I_f$, so

$$\begin{aligned} (E(H)_f : E(F)_f \oplus I_f) &= (T : 2I_f) = (I_f : 2I_f)/(I_f : T) \\ &= 2^l/|H^1(G, E(H)_f)|. \end{aligned}$$

□

3. Main Results and Their Proofs.

We will first give a general theorem on a finitely-generated module over a Dedekind domain, which establishes a relationship between the Steinitz class and the index of the module in its corresponding free module. This theorem is the key to our final results about Steinitz class.

Theorem 2. *Suppose that L is a free \mathcal{O}_K -module, and $M \subset L$ is a submodule with $(L : M) < +\infty$. Then there is an integral \mathcal{O}_K -ideal \mathcal{A} such that $[\mathcal{A}]$ is the Steinitz class of M , and $N_{\mathbf{Q}}^K(\mathcal{A}) = (L : M)$, where $N_{\mathbf{Q}}^K(\cdot)$ denotes the norm map of ideals from K to the rationals \mathbf{Q} .*

Proof. Let $L = \bigoplus_{i=1}^n \mathcal{O}_K e_i$, so $\{e_1, \dots, e_n\}$ is an \mathcal{O}_K -basis for L . We will inductively prove that there are \mathcal{O}_K -ideals \mathcal{B}_i ($i = 1, \dots, n$) such that $M \cong \bigoplus_{i=1}^n \mathcal{B}_i$, and $(L : M) = \prod_{i=1}^n (\mathcal{O}_K : \mathcal{B}_i)$.

When $n = 1$, everything is obvious. Assume then the statement is true for $n - 1$ and consider the module-homomorphism $\rho : L \rightarrow \mathcal{O}_K$, $\rho \left(\sum_{i=1}^n r_i e_i \right) = r_n$. Then $\mathcal{B} = \rho(M)$ is an ideal of \mathcal{O}_K , and the sequence

$$0 \rightarrow N \rightarrow M \xrightarrow{\rho} \mathcal{B} \rightarrow 0$$

is exact, where $N = \ker(\rho) \cap M$. Since \mathcal{B} is a projective \mathcal{O}_K -module, there exists \mathcal{O}_K -module $\mathcal{C} \subset M$ such that $\mathcal{C} \cong \mathcal{B}$, $\rho(\mathcal{C}) = \mathcal{B}$, $M = N \oplus \mathcal{C} \cong N \oplus \mathcal{B}$. Thus

$$(L : M) = (L : N \oplus \mathcal{C}) = \left(L : \bigoplus_{i=1}^{n-1} \mathcal{O}_K + \mathcal{C} \right) \left(\bigoplus_{i=1}^{n-1} \mathcal{O}_K + \mathcal{C} : N \oplus \mathcal{C} \right)$$

where $\left(L : \bigoplus_{i=1}^{n-1} \mathcal{O}_K + \mathcal{C} \right) = (\rho^{-1}(\mathcal{O}_K) : \rho^{-1}(\mathcal{B})) = (\mathcal{O}_K : \mathcal{B})$.

Consider $\mathcal{C} \cap \bigoplus_{i=1}^{n-1} \mathcal{O}_K = \mathcal{C} \cap \ker(\rho)$. When restricted on \mathcal{C} , the map ρ is injective, so we have

$$\bigoplus_{i=1}^{n-1} \mathcal{O}_K + \mathcal{C} = \bigoplus_{i=1}^{n-1} \mathcal{O}_K \oplus \mathcal{C},$$

$$\begin{aligned} \left(\bigoplus_{i=1}^{n-1} \mathcal{O}_K + \mathcal{C} : N \oplus \mathcal{C} \right) &= \left(\bigoplus_{i=1}^{n-1} \mathcal{O}_K \oplus \mathcal{C} : N \oplus \mathcal{C} \right) \\ &= \left(\bigoplus_{i=1}^{n-1} \mathcal{O}_K : N \right). \end{aligned}$$

Note that $N \subset \bigoplus_{i=1}^{n-1} \mathcal{O}_K$. So via the hypothesis of our induction, we know

that there are \mathcal{O}_K -ideals \mathcal{B}_i ($i = 1, \dots, n - 1$) such that $N \cong \bigoplus_{i=1}^{n-1} \mathcal{B}_i$, and

$\left(\bigoplus_{i=1}^{n-1} \mathcal{O}_K : N \right) = \prod_{i=1}^{n-1} (\mathcal{O}_K : \mathcal{B}_i)$. Thus we have $M \cong \bigoplus_{i=1}^n \mathcal{B}_i$ and $(L : M) = \prod_{i=1}^n (\mathcal{O}_K : \mathcal{B}_i) = \prod_{i=1}^n N_{\mathbf{Q}}^K(\mathcal{B}_i) = N_{\mathbf{Q}}^K \left(\prod_{i=1}^n \mathcal{B}_i \right)$, where $\mathcal{B}_n = \mathcal{B}$. Now the proof is completed by the following lemma.

Lemma 5. *Assume \mathcal{A}_1 and \mathcal{A}_2 are two nonzero ideals of the Dedekind domain R , then we have isomorphism of R -modules: $\mathcal{A}_1 \oplus \mathcal{A}_2 \cong R \oplus \mathcal{A}_1 \mathcal{A}_2$.*

Proof. See Lemma 13 in page 168 of [3]. □

We now intend to prove our main results via our Theorem 2. To use Theorem 2, we need first to find the corresponding L and M in the Mordell group $E(H)$. The corresponding L is given in Lemma 6. While the corresponding M is given in the proofs of Theorem 4 and 5, i.e., $M = [\sqrt{-D}]E(H)_f$ if $D \equiv 3 \pmod{4}$; $M = [2\sqrt{-D}]E(H)_f$ if $D \equiv 1 \pmod{4}$.

Lemma 6. $L = \mathcal{O}_K \cdot E(F)_f$ is a free \mathcal{O}_K -module of rank l .

Proof. Assume P_1, \dots, P_l form a \mathbf{Z} -basis of $E(F)_f$. We will prove

$$L = \mathcal{O}_K \cdot E(F)_f = \bigoplus_{i=1}^l \mathcal{O}_K P_i.$$

Now we suppose that $\sum_{i=1}^l [\alpha_i]P_i = 0$ for some $\alpha_i \in \mathcal{O}_K$ ($i = 1, \dots, l$). When $D \equiv 3 \pmod{4}$, we have $\alpha_i = s_i + t_i(1 + \sqrt{-D})/2$ ($s_i, t_i \in \mathbf{Z}$, $i = 1, \dots, l$), then via $\sum_{i=1}^l [\alpha_i]P_i = 0$ we have $\sum_{i=1}^l [2s_i + t_i]P_i = 0$ and $\sum_{i=1}^l [\sqrt{-D}t_i]P_i = 0$. Thus $t_i = 0$, $s_i = 0$, $\alpha_i = 0$ ($i = 1, \dots, l$). This proves the theorem when $D \equiv 3 \pmod{4}$. The case $D \equiv 1 \pmod{4}$ goes in the same way.

To determine our corresponding M in the case $D \equiv 3 \pmod{4}$, we need the following theorem.

Theorem 3. *For $D \equiv 3 \pmod{4}$, we have $|H^1(G, E(H)_f)| = 1$, and $E(H)_f = \mathcal{O}_K \cdot E(F)_f + I_f$.*

Proof. Let P_1, \dots, P_l form a \mathbf{Z} -basis of $E(F)_f$, and Q_1, \dots, Q_l form a \mathbf{Z} -basis of I_f . Put $\alpha = (1 + \sqrt{-D})/2$. We need only to prove that $E(H)_f/(E(F)_f \oplus I_f) = C_1 \oplus \dots \oplus C_l$, where $C_i = (\overline{[\alpha]P_i})$ is subgroup of order 2 generated by $\overline{[\alpha]P_i}$ in the quotient group $E(H)_f/(E(F)_f \oplus I_f)$. (Here \bar{a} denotes the residue class of a in this quotient group.) Obviously we have $\overline{[\alpha]P_i} \neq \bar{0}$; otherwise there would be $t_j, s_j \in \mathbf{Z}$ ($j = 1, \dots, l$) such that $[\alpha]P_i = \sum_{j=1}^l [t_j]P_j + \sum_{j=1}^l [s_j]Q_j$, then $[1 + \sqrt{-D}]P_i = \sum_{j=1}^l [2t_j]P_j + \sum_{j=1}^l [2s_j]Q_j$, and $P_i = \sum_{j=1}^l [2t_j]P_j$, giving a contradiction.

Furthermore, if $\sum_{i=1}^l [u_i]\overline{[\alpha]P_i} = \bar{0}$ for some $u_i \in \mathbf{Z}$ ($i = 1, \dots, l$), then there are $t_i, s_i \in \mathbf{Z}$ ($i = 1, \dots, l$) such that $\sum_{i=1}^l [u_i\alpha]P_i = \sum_{i=1}^l [t_i]P_i + \sum_{i=1}^l [s_i]Q_i$, so

$$\sum_{i=1}^l [u_i]P_i + \sum_{i=1}^l [u_i\sqrt{-D}]P_i = \sum_{i=1}^l [2t_i]P_i + \sum_{i=1}^l [2s_i]Q_i.$$

Thus $\sum_{i=1}^l [u_i]P_i = \sum_{i=1}^l [2t_i]P_i$, which gives $u_i = 2t_i$ ($i = 1, \dots, l$). Hence $[u_i]\overline{[\alpha]P_i} = \overline{[t_i][2\alpha]P_i} = \overline{[t_i(1 + \sqrt{-D})]P_i} = \bar{0}$. This completes the proof. \square

Now we can prove our main results via Theorem 2.

Theorem 4. *Suppose that $D = p \equiv 3 \pmod{4}$ is a prime number, and E is an elliptic curve having complex multiplication by the full ring \mathcal{O}_K of integers of $K = \mathbf{Q}(\sqrt{-D})$. Then the Steinitz class of E is the principal class, i.e., $\text{St}(E) = 1$.*

Proof. Let $L = \mathcal{O}_K \cdot E(F)_f$, $M = [\sqrt{-p}]E(H)_f$. Since $M \cong E(H)_f$, we need only to prove $\text{St}(M)$ is the principal class.

By Theorem 3 we have $E(H)_f = \mathcal{O}_K \cdot E(F)_f + I_f$. Thus

$$M = [\sqrt{-p}]E(H)_f = E(F)_f \cdot (\sqrt{-p}\mathcal{O}_K) + [\sqrt{-p}]I_f \subset \mathcal{O}_K \cdot E(F)_f = L;$$

$$\begin{aligned} (L : M) &= (\mathcal{O}_K \cdot E(F)_f : [\sqrt{-p}]E(H)_f) \\ &= \frac{(E(H)_f : [\sqrt{-p}]E(H)_f)}{(E(H)_f : \mathcal{O}_K \cdot E(F)_f)} \\ &= \frac{p^l}{(E(H)_f : \mathcal{O}_K \cdot E(F)_f)}. \end{aligned}$$

Since p is a prime number, so $(L : M) = p^t$ for some t ($0 \leq t \leq l$). By Theorem 2, the Steinitz class of M is equal to $[\mathcal{A}]$ for some \mathcal{O}_K -ideal \mathcal{A} , and $p^t = (L : M) = N_{\mathbf{Q}}^K(\mathcal{A})$. Since p is a prime number, $\mathcal{A} = (\sqrt{-p}\mathcal{O}_K)^t$ is principal. Thus $\text{St}(E) = \text{St}(M)$ is the principal class. \square

Theorem 5. *Suppose that $D = p \equiv 1 \pmod{4}$ is a prime number, and E is an elliptic curve having complex multiplication by the ring \mathcal{O}_K of all integers of $K = \mathbf{Q}(\sqrt{-D})$. Then the Steinitz class of E is $\text{St}(E) = [\mathcal{P}]^t$, where $[\mathcal{P}]$ is the ideal class of K represented by \mathcal{P} the prime factor of 2 in \mathcal{O}_K , $2^t = 2^l |H^1(G, E(H)_f)|$. In particular, the parity of t determines $\text{St}(E)$, since \mathcal{P} is not principal while $\mathcal{P}^2 = 2\mathcal{O}_K$ is principal.*

Proof. Let $L = \mathcal{O}_K \cdot E(F)_f$, $M = [2\sqrt{-p}]E(H)_f$. Since $M \cong E(H)_f$, so $\text{St}(E) = \text{St}(M)$. Note that $[2\sqrt{-p}]E(H)_f \subset [\sqrt{-p}](E(F)_f \oplus I_f)$, $[\sqrt{-p}]I_f \subset E(F)_f$. Thus we have $M \subset \mathcal{O}_K \cdot E(F)_f = L$, and

$$\begin{aligned} (L : M) &= (\mathcal{O}_K \cdot E(F)_f : [2\sqrt{-p}]E(H)_f) \\ &= \frac{(E(H)_f : [2\sqrt{-p}]E(H)_f)}{(E(H)_f : \mathcal{O}_K \cdot E(F)_f)} \\ &= \frac{(4p)^l}{(E(H)_f : E(F)_f \oplus I_f)(E(F)_f \oplus I_f : \mathcal{O}_K \cdot E(F)_f)} \\ &= \frac{(4p)^l}{2^l |H^1(G, E(H)_f)|^{-1} (I_f : [\sqrt{-p}]E(F)_f)} \\ &= 2^t |H^1(G, E(H)_f)| \cdot p^l / (I_f : [\sqrt{-p}]E(F)_f). \end{aligned}$$

Thus $(L : M) = 2^t p^r$ for some $t, r \geq 0$, since p is a prime number. By Theorem 2 we know that $N_{\mathbf{Q}}^K(\mathcal{A}) = 2^t p^r$ for some \mathcal{O}_K -ideal \mathcal{A} . Therefore $\mathcal{A} = \mathcal{P}^t([\sqrt{-p}]\mathcal{O}_K)^r$, $\text{St}(E) = [\mathcal{A}] = [\mathcal{P}]^t$. This proves the theorem. \square

Corollary 1. *Suppose as in Theorem 5. If $l = \text{rank}_{\mathbf{Z}}(E(F)) = 1$, then $H^1(G, E(H)_f)$ determines the Steinitz class of E .*

Now we analyze the examples of Dummit and Miller in [1] by utilizing the above method. For these examples, we have $K = \mathbf{Q}(\sqrt{-10})$, $D = 10$, $H = K(\sqrt{5}) = \mathbf{Q}(\sqrt{-10}, \sqrt{5})$. We consider the \mathcal{O}_K -module $L = \mathcal{O}_K \cdot E(F)_f$ and $M = 2[\sqrt{-10}]E(H)_f$. Then via the same idea in the proof of Theorem 5 we have similar ratiocination for $D = 10$:

$$\begin{aligned} (L : M) &= \frac{(E(H)_f : 2[\sqrt{-10}]E(H)_f)}{(E(H)_f : \mathcal{O}_K \cdot E(F)_f)} \\ &= \frac{(4 \cdot 10)^l}{(E(H)_f : E(F)_f \oplus I_f)(E(F)_f \oplus I_f : \mathcal{O}_K \cdot E(F)_f)} \\ &= \frac{(40)^l}{2^l |H^1(G, E(H)_f)|^{-1} (I_f : [\sqrt{-10}]E(F)_f)} \\ &= 2^l |H^1(G, E(H)_f)| 10^l / (I_f : [\sqrt{-10}]E(F)_f). \end{aligned}$$

Thus the Steinitz class of E is determined by the 2-exponent of

$$2^l |H^1(G, E(H)_f)| (I_f : [\sqrt{-10}]E(F)_f).$$

(DM1) Consider the following elliptic curve of Dummit and Miller in [1]:

$$E_1 : y^2 = x^3 + (6 + 6\sqrt{5})x^2 + (7 - 3\sqrt{5}).$$

Then $l = 1$, $|H^1(G, E(H)_f)| = 2$, $(I_f : [\sqrt{-10}]E(F)_f) = 1$. Therefore we know that $2^l |H^1(G, E(H)_f)| (I_f : [\sqrt{-10}]E(F)_f) = 4$. Thus the Steinitz class of E_1 is the principal class, i.e., $\text{St}(E_1) = 1$.

(DM2) Consider the following elliptic curve in [1]:

$$E_{1,\text{isog}} : y^2 = x^3 - (912 + 12\sqrt{5})x^2 + (188 + 84\sqrt{5})x.$$

We have $l = 1$, $|H^1(G, E(H)_f)| = 2$, $(I_f : [\sqrt{-10}]E(F)_f) = 2$, and $2^l |H^1(G, E(H)_f)| (I_f : [\sqrt{-10}]E(F)_f) = 2^3$. Thus the Steinitz class $\text{St}(E_{1,\text{isog}}) = [\mathcal{P}]$, where \mathcal{P} is a prime factor of 2 in \mathcal{O}_K .

(DM3) For $E_3 : y^2 = x^3 + 36x^2 + (162 - 72\sqrt{5})x$, in [1], we have $l = 2$, $|H^1(G, E(H)_f)| = 2$, $(I_f : [\sqrt{-10}]E(F)_f) = 1$, $2^l |H^1(G, E(H)_f)| (I_f : [\sqrt{-10}]E(F)_f) = 2^3$. Thus $\text{St}(E_3) = [\mathcal{P}]$, \mathcal{P} a prime factor of 2 in \mathcal{O}_K .

There are still many open problems about the Steinitz classes of elliptic curves. For example, we have the following conjecture.

Conjecture. *Both the cases $\text{St}(E) = 1$ and $\text{St}(E) \neq 1$ exist for some elliptic curves E having complex multiplication by \mathcal{O}_K , where $K = \mathbf{Q}(\sqrt{-D})$ with prime number $D \equiv 1 \pmod{4}$.*

References

- [1] D.S. Dummit and W.L. Miller, *The Steinitz class of the Mordell-Weil group of some CM elliptic curves*, J. Number Theory, **56** (1996), 52-78.
- [2] B. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, SLN, **776**, Springer-Verlag, Berlin, 1980.
- [3] F. Keqin, *Introduction to Commutative Algebra*, Higher Education Press, Beijing, 1985.
- [4] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, 1971.
- [5] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Spring-Verlag, New York, 1982.

Received September 3, 1998 and revised February 10, 1999.

TSINGHUA UNIVERSITY
BEIJING 100084
P.R. CHINA

TSINGHUA UNIVERSITY
BEIJING 100084
P.R. CHINA
E-mail address: xianke@tsinghua.edu.cn

