J. Math. Soc. Japan
Vol. 31, No. 2, 1979

The non-existence of elliptic curves with everywhere good reduction over certain imaginary quadratic fields

By Hidenori ISHII

(Received Aug. 2, 1977)

Introduction.

The purpose of this paper is to prove the following theorem.

THEOREM. *Let d be a prime number such that $d=2$ or $d\equiv -1 \bmod 12$, and k be an imaginary quadratic field with the discriminant $-d$. Suppose that the class number of k is prime to 3. Let E be an elliptic curve defined over k. Then, there exists a prime ideal of k at which E does not have good reduction.*

Note that the assumptions of the Theorem imply that the class number of k is prime to 6 and $\left(\frac{-d}{3}\right)=1$ where $\left(-\right)$ denotes the Legendre symbol.

To prove the Theorem, we shall study the k-rational points of order 3 on elliptic curves with everywhere good reduction defined over k. To state our method more explicitly, let k be an arbitrary algebraic number field, $\mathfrak{o}_k$ the maximal order of k. Let E be an elliptic curve with everywhere good reduction defined over k, $\mathcal{E}$ the Neron model of E over $X=\operatorname{Spec}\mathfrak{o}_k$, and ${}_p\mathcal{E}$ the kernel of the p-multiplication on $\mathcal{E}$. In § 1-2, following Mazur [6], we obtain an estimate of the free rank of the Mordell-Weil group of E in terms of the rank of $\mathfrak{o}_k^{\times}$ under an assumption on the divisibility of ${}_p\mathcal{E}$ by $\boldsymbol{\mu}_p$ or $\boldsymbol{Z}/p\boldsymbol{Z}$, where ${}_p\mathcal{E}$ is considered as a finite flat group scheme over X. (See Proposition 4). As an application of this proposition, we shall show that E has no k-rational point of order 3 under the assumptions of the Theorem (see Lemma 3). On the other hand, we can show that such an elliptic curve has a k-rational point of order 3 in the last section, by studying the ramification of the extensions over k generated by the coordinates of the points of order 3 (see Proposition 6, Lemma 4, 5).

The author wishes to express his hearty thanks to Dr. H. Yoshida for his valuable suggestions.

§ 1. Let k be an algebraic number field of finite degree, and h_k the class number of k in the narrow sense. Let $X=\operatorname{Spec}\mathfrak{o}_k$, and $H^i(X,\ )$ denote the i-th cohomology group for the f. p. p. f. topology over X (cf. [2] Expose IV).

LEMMA 1. *Let p be a prime number and assume that p does not divide h_k. Then;*

i) $H^1(X, \boldsymbol{Z}/p\boldsymbol{Z})=0$,

ii) $H^2(X, \boldsymbol{Z}/p\boldsymbol{Z})\cong\mathfrak{o}_k^\times/(\mathfrak{o}_k^\times)^p$ *if* $p\neq 2$ *or* k *is totally imaginary,*

iii) $H^1(X, \boldsymbol{\mu}_p)\cong\mathfrak{o}_k^\times/(\mathfrak{o}_k^\times)^p$,

iv) $H^2(X, \boldsymbol{\mu}_p)=0$, *if* $p\neq 2$ *or* $s\leqq 1$, *where* s *is the number of the real archimedean places of* k.

PROOF. By virtue of the exact sequence of sheaves on the f. p. p. f. topology over X,

$$0\longrightarrow\boldsymbol{\mu}_p\longrightarrow\boldsymbol{G}_m\xrightarrow{p}\boldsymbol{G}_m\longrightarrow 0,$$

we get the exact sequence

$$H^1(X, \boldsymbol{G}_m)\xrightarrow{p}H^1(X, \boldsymbol{G}_m)\longrightarrow H^2(X, \boldsymbol{\mu}_p)\longrightarrow H^2(X, \boldsymbol{G}_m)\xrightarrow{p}H^2(X, \boldsymbol{G}_m).$$

Using the facts $H^1(X, \boldsymbol{G}_m)\cong\mathrm{Pic}\,X$ and $H^2(X, \boldsymbol{G}_m)\cong(\boldsymbol{Z}/2\boldsymbol{Z})^t$ (Grothendieck [3] III Proposition 2.4, II Corollary 2.2), where $t=\mathrm{Max}\,(0, s-1)$ we get the asssertion iv). Similarly, by the exact sequence

$$\mathfrak{o}_k^\times\xrightarrow{p}\mathfrak{o}_k^\times\longrightarrow H^1(X, \boldsymbol{\mu}_p)\longrightarrow\mathrm{Pic}\,X\xrightarrow{p}\mathrm{Pic}\,X,$$

we get the assertion iii). Next by the duality theorem announced in Mazur [6] §7 (see Remark 1), we get the assertion i) in the case $p\neq 2$, and ii).

Finally, we shall show i) in the case $p=2$. Let P be a $\boldsymbol{Z}/2\boldsymbol{Z}$-torsor over X. Then P is finite and etale over X (cf. Grothendieck [4] Chap. IV). If $\mathrm{Spec}\,R$ is an irreducible component of P, the quotient field of R is an extension over k of degree at most two. Hence it is an abelian extension over k. Since R is finite and etale over $\mathfrak{o}_k$, we have $R=\mathfrak{o}_k$ because $2\nmid h_k$. Therefore, $H^1(X, \boldsymbol{Z}/2\boldsymbol{Z})=0$.

REMARK 1. We shall use only i) and iii) of Lemma 1 in the following sections. M. Ohta has told the author the assertion i) is an immediate consequence of the fact $H^1(X, \boldsymbol{Z}/n\boldsymbol{Z})=\mathrm{Hom}\,(\pi_1(X), \boldsymbol{Z}/n\boldsymbol{Z})$, where $\pi_1(X)$ denotes the fundamental group of X (cf. [1] Chap. II. (2.1)).

Let $\mathcal{E}$ be an abelian scheme of dimension 1 over X. The ${}_p\mathcal{E}$ is a finite flat group scheme over X.

The symbols η, δ and r are defined as follows; $\eta=\dim_{\boldsymbol{F}_p}H^1(X, {}_p\mathcal{E})$, $\delta=\dim_{\boldsymbol{F}_p}{}_p\mathcal{E}(k)$ and r is the free rank of $\mathfrak{o}_k^\times$.

PROPOSITION 1. *Let p be a prime number not dividing h_k. If ${}_p\mathcal{E}$ is divisible by $\boldsymbol{\mu}_p$, then $\eta-\delta=r-1$.*

PROOF. By the assumption, we get an exact sequence (in the sense of Tate [12]),

$$(*)\qquad 0\longrightarrow\boldsymbol{\mu}_p\longrightarrow{}_p\mathcal{E}\xrightarrow{\pi}G\longrightarrow 0,$$

where G is a finite flat group scheme and π is a faithfully flat morphism. Since ${}_p\mathcal{E}$ is self-dual with respect to the Cartier duality, we can conclude $G \cong \boldsymbol{Z}/p\boldsymbol{Z}$. Moreover, we can consider (*) as an exact sequence of sheaves on f.p.p.f. topology because π is faithfully flat (cf. Oort [7] Chap. III). Let us abbreviate $H^i(X, \mathcal{F})$ to $H^i(\mathcal{F})$ for a sheaf $\mathcal{F}$. Then we get the following exact sequence by Lemma 1 i).

$$0 \longrightarrow H^0(\boldsymbol{\mu}_p) \longrightarrow H^0({}_p\mathcal{E}) \longrightarrow H^0(\boldsymbol{Z}/p\boldsymbol{Z}) \longrightarrow H^1(\boldsymbol{\mu}_p) \longrightarrow H^1({}_p\mathcal{E}) \longrightarrow 0\,.$$

By Lemma 1 iii), $\dim_{\boldsymbol{F}_p} H^1(\boldsymbol{\mu}_p) = r + \dim_{\boldsymbol{F}_p} H^0(\boldsymbol{\mu}_p)$.

Therefore, $\eta - \delta = \dim_{\boldsymbol{F}_p} H^1(\boldsymbol{\mu}_p) - \dim_{\boldsymbol{F}_p} H^0(\boldsymbol{\mu}_p) - 1 = r - 1$.

PROPOSITION 2. *Let p be a prime number not dividing h_k. If ${}_p\mathcal{E}$ is divisible by $\boldsymbol{Z}/p\boldsymbol{Z}$, then $\delta = \dim_{\boldsymbol{F}_p} H^0(\boldsymbol{\mu}_p) + 1$, $\eta - \delta \leqq r - 1$.*

PROOF. Similarly in the proof of Proposition 1, we get the exact sequence

$$0 \longrightarrow \boldsymbol{Z}/p\boldsymbol{Z} \longrightarrow {}_p\mathcal{E} \longrightarrow \boldsymbol{\mu}_p \longrightarrow 0\,.$$

Hence we get the exact sequences

$$0 \longrightarrow H^0(\boldsymbol{Z}/p\boldsymbol{Z}) \longrightarrow H^0({}_p\mathcal{E}) \longrightarrow H^0(\boldsymbol{\mu}_p) \longrightarrow 0$$

and

$$0 \longrightarrow H^1({}_p\mathcal{E}) \longrightarrow H^1(\boldsymbol{\mu}_p)\,.$$

Therefore we have $\delta = \dim_{\boldsymbol{F}_p} H^0(\boldsymbol{\mu}_p) + 1$ and $\eta \leqq \dim_{\boldsymbol{F}_p} H^1(\boldsymbol{\mu}_p)$. Hence it follows $\eta - \delta \leqq r - 1$.

Let E be the generic fibre of $\mathcal{E}$ and ${}_p\text{Ш}(E, k)$ the p-torsion part of the Shafarevich-Tate group of E over k. Let τ denote $\dim_{\boldsymbol{F}_p}({}_p\text{Ш}(E, k))$ and ρ denote the free rank of the Mordell-Weil group $E(k)$.

PROPOSITION 3. $\tau + \rho + \delta \leqq \eta$.

PROOF. We have the exact sequence

$$0 \longrightarrow {}_p\mathcal{E} \longrightarrow \mathcal{E} \xrightarrow{\ p\ } \mathcal{E} \longrightarrow 0$$

of sheaves on f.p.p.f. topology. Therefore we get the exact sequence

$$0 \longrightarrow \text{Coker}\,(H^0(\mathcal{E}) \xrightarrow{\ p\ } H^0(\mathcal{E})) \longrightarrow H^1({}_p\mathcal{E}) \longrightarrow \text{Ker}(H^1(\mathcal{E}) \xrightarrow{\ p\ } H^1(\mathcal{E})) \longrightarrow 0\,,$$

and we conclude $\eta = \rho + \delta + \tau'$, where $\tau' = \dim_{\boldsymbol{F}_p}(\text{Ker}\,(H^1(\mathcal{E}) \xrightarrow{p} H^1(\mathcal{E}))$. Using the fact $\tau \leqq \tau'$ (cf. Mazur [6] Appendix), we have $\eta \geqq \rho + \delta + \tau$.

PROPOSITION 4. *The assumption on p being as in Lemma 1, suppose that ${}_p\mathcal{E}$ is divisible by $\boldsymbol{Z}/p\boldsymbol{Z}$ or $\boldsymbol{\mu}_p$. Then $\rho + \tau \leqq r - 1$.*

PROOF. The assertion is an immediate consequence of the previous three propositions.

The following two corollaries are immediate from Proposition 4.

COROLLARY 1. *Let k be an imaginary quadratic field, and assume that p is prime to h_k. Then ${}_p\mathcal{E}$ is divisible by neither $\boldsymbol{Z}/p\boldsymbol{Z}$ nor $\boldsymbol{\mu}_p$.*

Corollary 2. *Let k be a real quadratic field and assume that p is prime to h_k. If ${}_p\mathcal{E}$ is divisible by $\boldsymbol{Z}/p\boldsymbol{Z}$ or $\boldsymbol{\mu}_p$, then the Mordell-Weil group $E(k)$ is finite and the p-primary part of the Shafarevich-Tate group equals zero.*

§ **2.** Let k be an algebraic number field of finite degree, E an elliptic curve with everywhere good reduction defined over k and $\mathcal{E}$ the Neron model of E over $\mathfrak{o}_k$. Suppose that E has a k-rational point of order p, namely that there exists a closed immersion f from $\boldsymbol{Z}/p\boldsymbol{Z}$ to E over k. Then by the universal property of the Neron model, there exists a morphism φ from $\boldsymbol{Z}/p\boldsymbol{Z}$ to $\mathcal{E}$ over $X=\mathrm{Spec}\,\mathfrak{o}_k$ such that the generic fibre of φ is f. We denote the image of φ by G. Then G is a group scheme of order p over X in the sense of [8].

Lemma 2. *Put $d=[k:Q]$ and suppose that $p>d+1$. Then $G\cong\boldsymbol{Z}/p\boldsymbol{Z}$.*

Proof. For each finite place v of k, we denote the completion of k with respect to v by k_v and the maximal order of k_v by $\mathfrak{o}_v$. Put $G_v=G\otimes_{\mathfrak{o}_k}\mathfrak{o}_v$, then

$$\varphi_v:\ \boldsymbol{Z}/p\boldsymbol{Z}\longrightarrow G_v$$

is a morphism which is isomorphic on the generic fibres. Therefore it is an isomorphism by Raynaud's Corollary 3.3.6 in [**9**]. Finally, we conclude that φ is an isomorphism by Lemma 4 of Oort-Tate [8].

Proposition 5. *Let k be an imaginary quadratic field and $p>3$ a prime number not dividing h_k. Then any elliptic curve defined over k that has everywhere good reduction has no k-rational point of order p.*

Proof. This follows from Corollary 1 of Proposition 4.

Remark 2. Let $\mathfrak{l}$ be a prime ideal of k dividing 2. Then the number of $\boldsymbol{F}_{N(\mathfrak{l})}$-rational points of $N \bmod \mathfrak{l}$ is at most $1+N(\mathfrak{l})+2N(\mathfrak{l})^{1/2}$. Therefore, the assertion of Proposition 5 is clear for $p>1+N(\mathfrak{l})+2N(\mathfrak{l})^{1/2}$, where $N(\mathfrak{l})$ denotes the absolute norm of the ideal $\mathfrak{l}$.

In the following lemma we shall extend the previous proposition to the case $p=3$.

Lemma 3. *Let k be an imaginary quadratic field and assume that its class number h_k is prime to* 6. *If an elliptic curve E defined over k has everywhere good reduction, then E has no k-rational point of order* 3.

Proof. Assume that E has a k-rational point of order 3. Then we shall show that G is isomorphic to $\boldsymbol{Z}/3\boldsymbol{Z}$ or $\boldsymbol{\mu}_3$ under the notation in the first part of this section. Since the class number of k is odd, there exists only one prime number ramified in $k/\boldsymbol{Q}$. In the case $k\neq\boldsymbol{Q}(\sqrt{-3})$, $p=3$ is unramified in $k/\boldsymbol{Q}$, hence $G\cong\boldsymbol{Z}/3\boldsymbol{Z}$ by Corollary 3.3.6 of Raynaud [**9**] and Theorem 3 of Oort-Tate [8]. In the case $k=\boldsymbol{Q}(\sqrt{-3})$, we can also conclude that $G\cong\boldsymbol{Z}/3\boldsymbol{Z}$ or $\boldsymbol{\mu}_3$ by Theorem 3 of Oort-Tate [8]. This completes the proof of Lemma 3 by Corollary 1 of Proposition 4.

§ **3.** We will denote the group of the p-torsion points of an elliptic curve E by ${}_pE$. Let k be an algebraic number field of finite degree satisfying the following two conditions.

i) The class number of $k(\sqrt{-3})$ is odd,

ii) any prime ideal $\mathfrak{p}$ of k dividing 3 is unramified over $\boldsymbol{Q}$ and the norm $N_{k/\boldsymbol{Q}}(\mathfrak{p})$ is an odd power of 3.

PROPOSITION 6. *Let the notation and the assumptions be as above. Moreover, let E be a semi-stable elliptic curve defined over k with good reduction at any prime ideal not dividing* 3. *If the discriminant Δ of a Weierstrass model of E is a cube in k, then E has a k-rational point of order* 3, *moreover $k({}_3E)=k(\sqrt{-3})$, where $k({}_3E)$ is the field generated by the coordinates of the points in ${}_3E$.*

PROOF. Define S_1 and S_2 as follows;

$$S_1=\{\mathfrak{p}\in \operatorname{Spec}\mathfrak{o}_k\,;\ \mathfrak{p}|3 \text{ and } E \bmod \mathfrak{p} \text{ is not supersingular}\}.$$

$$S_2=\{\mathfrak{p}\in \operatorname{Spec}\mathfrak{o}_k\,;\ \mathfrak{p}|3 \text{ and } E \bmod \mathfrak{p} \text{ is supersingular}\}.$$

Since Δ is a cube in k, the degree of $k({}_3E)/k$ is a power of 2. Hence any prime ideal in $S_1\cup S_2$ is tamely ramified in $k({}_3E)/k$. Put $L=k(\sqrt{-3})$. Then any prime ideal $\mathfrak{p}$ in $S_1\cup S_2$ is necessarily ramified in this quadratic extension L/k. In the case $\mathfrak{p}$ is in S_1, the inertia group $I(\mathfrak{p})$ (which is determined up to conjugations) in $k({}_3E)/k$ is of order 2 (cf. Serre [**10**] § 1). Therefore, the prime ideal of L lying over $\mathfrak{p}$ is unramified in $k({}_3E)/L$. In the case $\mathfrak{p}$ is in S_2, the inertia group $I(\mathfrak{p})$ is a cyclic group of order 8 and the decomposition group is the normalizer of $I(\mathfrak{p})$ in $GL_2(\boldsymbol{F}_3)$ (cf. [**10**] § 1). Hence it is of order 16. On the other hand, the degree of $k({}_3E)/k$ is at most 16, therefore $\operatorname{Gal}(k({}_3E)/k)$ is a subgroup P of order 16, which is a 2-Sylow subgroup of $GL_2(\boldsymbol{F}_3)$. Since P has a unique cyclic subgroup C of order 8, $I(\mathfrak{p})=C$ and it does not depend on the choice of $\mathfrak{p}$ in S_2. This cyclic subgroup C is a non-split Cartan subgroup of $GL_2(\boldsymbol{F}_3)$. Hence it is not contained in $SL_2(\boldsymbol{F}_3)$ and we can conclude that $I(\mathfrak{p})\neq G_L$, where $G_L=\operatorname{Gal}(k({}_3E)/L)$. Let F be the subfield of $k({}_3E)$ corresponing to $I(\mathfrak{p})\cap G_L$. Then F is an unramified quadratic extension of L in $k({}_3E)$ by the fact described above and [**11**] (Proposition 18, Chap. IV). It contradicts the assumption on the class number of L. Hence $S_2=\emptyset$ and $k({}_3E)/L$ is an unramified extension whose degree is a power of 2. Thus we obtain $k({}_3E)=L$. Therefore, $\operatorname{Gal}(k({}_3E)/k)$ is of order 2. Using the fact that it is not contained in $SL_2(\boldsymbol{F}_3)$, we can conclude that it is conjugate to the subgroup generated by the element $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\in GL_2(\boldsymbol{F}_3)$. Therefore, ${}_3E\cong \boldsymbol{Z}/3\boldsymbol{Z}\oplus\boldsymbol{\mu}_3$ as Galois modules. This completes the proof of Proposition 6.

We shall continue a discussion on the assumption of Proposition 6 in the case where k is an imaginary quadratic field.

LEMMA 4. *Let k be an imaginary quadratic field different from $\boldsymbol{Q}(\sqrt{-3})$ and assume that the class number of k is prime to 6. If E is an elliptic curve with everywhere good reduction defined over k, then the discriminant Δ of a Weierstrass model of E is a cube in k.*

PROOF. Since E has everywhere good reduction, there exists an ideal $\mathfrak{a}$ such that $\mathfrak{a}^{12}=(\Delta)$. The assumption on the class number implies that $\mathfrak{a}$ is principal, namely $\mathfrak{a}=(a)$ for some $a\in k^{\times}$. Hence $\Delta=ua^{12}$ with some unit u of k. Since u is a cube in k, we get our conclusion.

LEMMA 5. *Let k be an imaginary quadratic field with the discriminant $-d$, and assume that the class number of k is odd and $\left(\frac{-d}{3}\right)=1$, where $\left(\frac{}{}\right)$ is the Legendre symbol. Then the class number of $k(\sqrt{-3})$ is odd.*

PROOF. The assumption on the class number of k implies that there exists only one prime number ramified in k. By the reciprocity law for the quadratic residues, this prime number remains prime in $\boldsymbol{Q}(\sqrt{-3})$. Since k and $\boldsymbol{Q}(\sqrt{-3})$ are linearly disjoint over $\boldsymbol{Q}$ and their discriminants are prime to each other, we can conclude that there exists only one prime ideal of $\boldsymbol{Q}(\sqrt{-3})$ ramified in $k(\sqrt{-3})$. Then the assertion is a special case of the result of Iwasawa [5].

Finally, we can prove the Theorem stated in the Introduction.

PROOF OF THEOREM. If E is an elliptic curve with everywhere good reduction defined over k, then E has a k-rational point of order 3 by Lemma 4, Lemma 5 and Proposition 6. This contradicts the conclusion of Lemma 3 in § 2.

References

[1] P. Deligne, (with J.F. Boutot, A. Grothendieck, L. Illusie and J.L. Verdier), Cohomologie Etale (SGA 4(1/2)), Lecture Notes in Math., no. 569, Springer, Berlin-Heidelberg-New York, 1977.

[2] M. Demazure and A. Grothendidck, Schémas en groupes I (SGA 3), Lecture Notes in Math., no. 151, Springer, Berlin-Heidelberg-New York, 1970.

[3] A. Grothendieck, Le groupe de Brauer II, III, Séminaire Bourbaki, 1965, no. 297, and I. H. E. S., 1966.

[4] A. Grothendieck (with J. Dieudonné), Eléments de géométrie algébrique, Publ. Math. I. H. E. S., 1961-68.

[5] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math, Sem. Univ. Hamburg, **20** (1956), 257-258.

[6] B. Mazur, Rational points on abelian varieties with values in towers of number fields, Invent. Math., **18** (1972), 183-266.

[7] F. Oort, Commutative group schemes, Lecture Notes in Math., no. 15, Springer, Berlin-Heidelberg-New York, 1966.

[8] F. Oort and J. Tate, Group schemes of prime order, Ann. Sci. École Norm. Sup., Series 4,3 (1970), 1-21.

[9] M. Raynaud, Schémas en groupes de type $(p,\cdots,p)$, Bull. Soc. Math. France, **102** (1974), 241-280.

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

[11] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, no. 6, Tokyo, 1961.

[12] I. Tate, p-divisible groups, Proceedings of a Conference on Local Fields, NUFFIC Summer School held at Driebergen, (1966), 158-183, Springer, Berlin-Heidelberg-New York, 1967.

Hidenori Ishii
Department of Mathematics
Faculty of Science
Kyoto University
Kyoto, Japan