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 $X=\mathrm{Spec}\,\mathfrak{o}_k$, 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 $X=\mathrm{Spec}\,\mathfrak{o}_k$, and $H^i(X,\ )$ denote the i-th cohomology group for the f. p. p. f. topology over X (cf. [2] Expose IV).