H. Ichimura
Nagoya Math. J.
Vol. 99 (1985), 63-71

A NOTE ON QUADRATIC FIELDS IN WHICH A FIXED PRIME NUMBER SPLITS COMPLETELY

HUMIO ICHIMURA

§1. Introduction

Throughout this note, p denotes a fixed prime number and f denotes a fixed natural number prime to p.

It is easy to see and more or less known that(*) for any natural number n, there exists an elliptic curve over $\bar{F}_p$ whose j-invariant is of degree n over F_p and whose endomorphism ring is isomorphic to an order of an imaginary quadratic field. In this note, we consider a more precise problem: *for any natural number n, decide whether or not there exists an elliptic curve over $\bar{F}_p$ whose j-invariant is of degree n over F_p and whose endomorphism ring is isomorphic to an order of an imaginary quadratic field with conductor f.*

To state our results, we introduce some notations. For an order $\mathfrak{o}$ of a quadratic field K, we write $(\mathfrak{o}/p) = 1$ when $(K/p) = 1$ and the conductor of $\mathfrak{o}$ is prime to p, where (K/p) denotes the Legendre symbol. Let $\mathfrak{P}$ be a prime divisor of p in $\bar{Q}$. For an order $\mathfrak{o}$ of a quadratic field with $(\mathfrak{o}/p) = 1$, we set $\mathfrak{p}_{\mathfrak{o}} = \mathfrak{P} \cap \mathfrak{o}$ and we denote by $n_{\mathfrak{o}}$ the number of elements of the cyclic subgroup of the proper $\mathfrak{o}$-ideal class group generated by the proper $\mathfrak{o}$-ideal class $\{\mathfrak{p}_{\mathfrak{o}}\}$. Clearly, $n_{\mathfrak{o}}$ does not depend on the choice of $\mathfrak{P}$.

Set $M(p, f) = \{\mathfrak{o};$ orders of imaginary quadratic fields with $(\mathfrak{o}/p) = 1$ and conductor $f\}$. Let $N(p, f)$ be the image of the map $M(p, f) \ni \mathfrak{o} \to n_{\mathfrak{o}} \in N$.

By some results of Deuring on elliptic curves (see e.g. Lang [6]; Chap. 13, Theorem 11, 12, and Chap. 14, Theorem 1), the preceding problem is equivalent to a problem: decide the image $N(p, f)$.

Our results are as follows.

THEOREM 1. (i) *When $(p/l) = 1$ for any odd prime divisor l of f, and*

Received March 26, 1984.

(*) We give a simple proof in Remark 1 of § 4.