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 $\mathfrak{p}_0 = \mathfrak{P} \cap \mathfrak{o}$ and we denote by n_0 the number of elements of the cyclic subgroup of the proper $\mathfrak{o}$-ideal class group generated by the proper $\mathfrak{o}$-ideal class $\{\mathfrak{p}_0\}$. Clearly, n_0 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 $M(p,f) \ni \mathfrak{o} \to n_0 \in N$.

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.

$8 \nmid f$ *(resp.* $4 \nmid f$*) in the case* $p \equiv 5 \pmod 8$ *(resp.* $p \equiv 3 \pmod 4$*), the complement* $N - N(p,f)$ *is a finite set,* (ii) *otherwise,* $N(p,f) \subset 2N$*, and the complement* $2N - N(p,f)$ *is a finite set.*

THEOREM 2. $N(p, 1) = N$.

Further, for real quadratic fields, we show a fact similar to (but not as sharp as) Theorem 1, 2.

Ankeny and Chowla [1] proved $|N - N(3, 1)| < \infty$ (a special case of Theorem 1). For a fixed natural number n, set $m(p, n) = |\{\mathfrak{o} \in M(p, 1); n_{\mathfrak{o}} = n\}|$. Humbert [4] and Kuroda [5] proved that $m(p, n) \to \infty$ as $p \to \infty$. By these facts, they showed the existence of infinitely many imaginary quadratic fields with class number divisible by a given integer. Theorem 1 is proved by using the method of [4], [1] and [5]. To prove Theorem 2, we first calculate a number n_p such that $n \in N(p, 1)$ if $n \geq n_p$, with the help of an approximation formula of Rosser and Schoenfeld [8] for $\pi(x)$, the number of prime numbers $\leq x$. Next, we construct orders $\mathfrak{o} \in M(p, 1)$ with $n_{\mathfrak{o}} = n$ for "small" n explicitly.

NOTATIONS. $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$ and $\boldsymbol{F}_p$ denote, respectively, the set of natural numbers, the ring of rational integers, the field of rational numbers and the finite field with p elements. For a field $\boldsymbol{K}$, $\bar{\boldsymbol{K}}$ denotes the algebraic closure of $\boldsymbol{K}$. For an element a of a quadratic field, a' and $N(a)$ denotes its conjugate and its norm respectively.

§2. Proof of Theorem 1

Let p be a fixed prime number and f a fixed natural number prime to p. There are two possible cases.

[I] $(p/l) = 1$ for any odd prime divisor l of f, and $8 \nmid f$ (resp. $4 \nmid f$) in the case $p \equiv 5 \pmod 8$ (resp. $p \equiv 3 \pmod 4$),

[II] otherwise.

First, we show the following

LEMMA 1. *In case* [II], $N(p,f) \subset 2N$.

Proof. The condition [II] means that $(p/l) = -1$ for some odd prime divisor l of f, or $8 | f$ and $p \equiv 5 \pmod 8$, or $4 | f$ and $p \equiv 3 \pmod 4$. Let $\mathfrak{o}$ be an order of an imaginary quadratic field with $(\mathfrak{o}/p) = 1$ and conductor f. Let d be the discriminant of the imaginary quadratic field $\mathfrak{o} \otimes_{\boldsymbol{Z}} \boldsymbol{Q}$. First, assume that $(p/l) = -1$ for some odd prime divisor l of f and $d \equiv 0$

(mod 4). Then, $\mathfrak{o} = [1, f\sqrt{d/4}]$. By the definition of n_0, $\mathfrak{p}_0^{n_0} = (a + bf\sqrt{d/4})$ for some $a, b \in \boldsymbol{Z}$. Taking norms of both sides, $p^{n_0} = a^2 - b^2f^2(d/4)$. Therefore, if n_0 is odd, $(p/l) = 1$ for any odd prime divisor l of f, which is a contradiction. So, n_0 must be even. It is proved similarly in the other cases.

Now, we prove that $N - N(p, f)$ (resp. $2N - N(p, f)$) is a finite set in case [I] (resp. [III]). First, we deal with the case where f is odd and satisfying the condition [I].

The following lemma is easily proved.

LEMMA 2. *Assume f is odd. Let n be a natural number, and let x be a rational integer, prime to $2p$ and satisfying the following conditions:*

(i) $x^2 \equiv 4p^n \pmod{f^2}$,

(ii) $\dfrac{x^2 - 4p^n}{f^2}$ *is square free,*

(iii) $0 < x < 2\sqrt{p^n - p^{n/2}}$.

Let $\mathfrak{o}$ be the order the imaginary quadratic field $\boldsymbol{K} = \boldsymbol{Q}(\sqrt{x^2 - 4p^n})$ with conductor f. Then, $(\mathfrak{o}/p) = 1$ and $n_0 = n$.

Let $f = \prod_i l_i^{e_i}$ be the prime decomposition of f, and set $f_0 = \prod_i l_i$. Since f is odd and satisfies the condition [I], there exists an odd integer $x(n)$ such that $x(n)^2 \equiv 4p^n \pmod{f^2}$ and $x(n)^2 \not\equiv 4p^n \pmod{l^2f^2}$ for any prime divisor l of f. Set $A(n) = \{x(n) + 2f_0^2f^2k;\ k \in \boldsymbol{Z}\}$ and $B(n) = \{x \in A(n);\ x$ is prime to p, $x^2 \not\equiv 4p^n \pmod{l^2}$ for any odd prime number l with $l \nmid f$, and $0 < x < 2\sqrt{p^n - p^{n/2}}\}$. By Lemma 2, it suffices to show that $|B(n)| \to \infty$ as $n \to \infty$. The number of $x \in A(n)$ such that x is prime to p and $0 < x < 2\sqrt{p^n - p^{n/2}}$ is at least $[(1 - 1/p)((\sqrt{p^n - p^{n/2}})/f_0^2f^2)] - 2$ if $p \neq 2$, and $[(\sqrt{p^n - p^{n/2}})/f_0^2f^2]$ if $p = 2$, where $[a]$ denotes the largest integer $\leq a$.

Let l be an odd prime number with $l \nmid pf$. Since the congruence $x^2 \equiv 4p^n \pmod{l^2}$ has at most two solutions, the number of $x \in A(n)$ such that $x^2 \equiv 4p^n \pmod{l^2}$ and $0 < x < 2\sqrt{p^n - p^{n/2}}$ is at most $2\{[(\sqrt{p^n - p^{n/2}})/f_0^2f^2l^2] + 1\}$ if $l < 2p^{n/2}$, and is zero if $l \geq 2p^{n/2}$.

Therefore,

$$(1)\quad |B(n)| > \begin{cases} \left[\left(1 - \dfrac{1}{p}\right)\dfrac{\sqrt{p^n - p^{n/2}}}{f_0^2f^2}\right] - 2 - \sum_l{}' \left\{2\left[\dfrac{\sqrt{p^n - p^{n/2}}}{f_0^2f^2l^2}\right] + 2\right\} & \text{if } p \neq 2 \\ \left[\dfrac{\sqrt{p^n - p^{n/2}}}{f_0^2f^2}\right] - \sum_l{}' \left\{2\left[\dfrac{\sqrt{p^n - p^{n/2}}}{f_0^2f^2l^2}\right] + 2\right\} & \text{if } p = 2 \end{cases}$$

$$
> \begin{cases} \dfrac{1}{f_0^2 f^2}\left\{\left(1-\dfrac{1}{p}\right) - 2\sum{}'\dfrac{1}{l^2}\right\}\sqrt{p^n - p^{n/2}} - 3 - 2\sum\limits_l{}'' 1 & \text{if } p \neq 2 \\ \dfrac{1}{f_0^2 f^2}\left\{1 - 2\sum\limits_l{}'\right\}\sqrt{p^n - p^{n/2}} - 1 - 2\sum\limits_l{}'' 1 & \text{if } p = 2\,, \end{cases}
$$

where the sum $\sum_l'$ is taken over all prime numbers l prime to $2pf$ with $0 < l < 2p^{n/2}$, and the sum $\sum_l''$ is taken over all prime numbers l with $0 < l < 2p^{n/2}$.

Note that $\sum_l' 1/l^2 < \log \zeta(2) - 1/4 - 1/p^2$ (resp. $\log \zeta(2) - 1/4$) when $p \neq 2$ (resp. $p = 2$), where $\zeta(s)$ is the Riemann zeta function. Therefore, by $\zeta(2) = \pi^2/6$, we see that the coefficient of $\sqrt{p^n - p^{n/2}}$ is larger than the positive constant $c_p/f_0^2 f^2$, where c_p is the positive constant given as follows:

(Table 1)

p	$p \geq 11$	7	5	3	2
c_p	0.429	0.401	0.384	0.392	0.504

On the other hand, by the prime number theorem,

$$
\sum_l{}'' 1 = O\left(\frac{2p^{n/2}}{(n/2)\log p}\right).
$$

Therefore, $|B(n)| \to \infty$ as $n \to \infty$. This completes the proof of Theorem 1 when f is odd and satisfies the condition [I].

It is proved similarly in the other cases.

§3. Proof of Theorem 2

Let $\pi(x)$ be the number of prime numbers $\leq x$. Rosser and Schoenfeld [8] (Theorem 2) showed

$$
(2) \qquad \pi(x) < \frac{x}{\log x - 3/2} \qquad \text{for } x > e^{3/2}\,.
$$

By a simple calculation using (1), (2) and Table 1, we obtain

LEMMA 3. *The set $N(p, 1)$ contains all natural numbers n with $n \geq n_p$, where n_p is the natural number given in the following table.*

p	$p \geq 11$	7	5	3	2
n_p	10	12	16	21	26

By this lemma, it suffices to construct orders $\mathfrak{o} \in M(p, 1)$ with $n_{\mathfrak{o}} = n$ for "small" n.

LEMMA 4. *The set* $N(p, 1)$ *contains all natural numbers of the form* $n = 2^{\lambda}3^{\mu}5^{\nu}7^{\chi}$ *with* $\lambda, \mu, \nu, \chi \geq 0$.

Proof. First, we prove our lemma when $p \neq 3$. Fix a natural number k and set $m = p^k$. Set $\boldsymbol{K}_{1,l} = \boldsymbol{Q}(\sqrt{1-4m^l})$ and $\boldsymbol{K}_{2,l} = \boldsymbol{Q}(\sqrt{9-4m^l})$ for $l = 1, 2, 3, 5, 7$. When $p \neq 3$, $(\boldsymbol{K}_{i,l}/p) = 1$ and we denote by $\mathfrak{p}_{i,l}$ a prime ideal(*) of $\boldsymbol{K}_{i,l}$ over p ($i = 1, 2$, $l = 1, 2, 3, 5, 7$). We show

CLAIM 1. *Assume* $p \neq 3$. *The ideal class*(*) *of* $\mathfrak{p}_{1,2}^k$ (*in* $\boldsymbol{K}_{1,2}$) *or that of* $\mathfrak{p}_{2,2}^k$ (*in* $\boldsymbol{K}_{2,2}$) *is of order* 2.

This is proved as follows. Write $1 - 4m^2 = f_1^2 d_1$ and $9 - 4m^2 = f_2^2 d_2$ with natural numbers f_1, f_2 and square free integers d_1, d_2. Then, $d_i \equiv 1 \pmod 4$ and 1, $(1 + \sqrt{d_i})/2$ is an integral basis of $\boldsymbol{K}_{i,2}$. Note that $\boldsymbol{K}_{i,2} \neq \boldsymbol{Q}(\sqrt{-1})$ because $d_i \equiv 1 \pmod 4$. Set $\alpha_1 = (1 + \sqrt{1-4m^2})/2$ and $\alpha_2 = (3 + \sqrt{9-4m^2})/2$. Then, we easily see that α_i is an integer of $\boldsymbol{K}_{i,2}$, $(\alpha_i, \alpha_i') = 1$ and $N(\alpha_i) = p^{2k}$. Hence, we may assume, without loss of generality, that $\mathfrak{p}_{i,2}^{2k} = (\alpha_i)$. Assume that $\mathfrak{p}_{1,2}^k$ is principal. Then, since $\boldsymbol{K}_{1,2} \neq \boldsymbol{Q}(\sqrt{-1})$, $\alpha_1 = \pm((a + b\sqrt{d_1})/2)^2$ for some a, $b \in \boldsymbol{Z}$. Therefore, $1 = \pm(a^2 + b^2 d_1)/2$ and $f_1 = \pm ab$. Hence, $1 - 4m^2 = f_1^2 d_1 = a^2(\pm 2 - a^2)$, from which we obtain $2m = a^2 \pm 1$. By considering both sides modulo 4, we see that a is odd and $2m = a^2 + 1$ (resp. $2m = a^2 - 1$) when m is odd (resp. even). Next, assume that $\mathfrak{p}_{2,2}^k$ is principal. Then, similarly, for some odd integer c, $2m = c^2 - 3$ (resp. $2m = c^2 + 3$) when m is odd (resp. even). Therefore, if both of $\mathfrak{p}_{1,2}^k$ and $\mathfrak{p}_{2,2}^k$ are principal, $c^2 = a^2 + 4$ for some odd integers a and c. But this is impossible because the square of an odd integer is congruent to 1 modulo 8. Hence, we obtain our claim. Similarly and more easily, we can prove

CLAIM 2(**). *Assume* $p \neq 3$. *For* $l = 1, 3, 5, 7$, *the ideal class of* $\mathfrak{p}_{i,l}^k$ *is of order* l ($i = 1, 2$).

Now, set $n = 2^{\lambda}3^{\mu}5^{\nu}7^{\chi}$ with $\lambda, \mu, \nu, \chi \geq 0$. By the above claims, we see that for the maximal order $\mathfrak{o}$ of the imaginary quadratic field $\boldsymbol{Q}(\sqrt{1-4p^n})$

(*) In this section, an ideal (class) is one with respect to the maximal order of an imaginary quadratic field.

(**) Further, we can show that for any prime number l (≥ 7), the ideal class of $\mathfrak{p}_{i,l}^k$ is of order l for *sufficiently large p*.

or that of $\boldsymbol{Q}(\sqrt{9-4p^n})$, $(\mathfrak{o}/p)=1$ and $n_{\mathfrak{o}}=n$. This proves our lemma when $p\neq 3$. When $p=3$, we can prove our lemma similarly by considering imaginary quadratic fields of type $K'_{2,l}=\boldsymbol{Q}(\sqrt{25-4m^l})$ in place of $K_{2,l}$.

LEMMA 5. *Assume p is odd. Then, the set $N(p,1)$ contains all odd natural numbers prime to p.*

Proof. Let n be an odd natural number prime to p. Let n_1 be the largest square free integer $|\,n$. Note that $n_1^2<p^n$. We easily see that for the maximal order $\mathfrak{o}$ of the imaginary quadratic field $\boldsymbol{Q}(\sqrt{n_1^2-p^n})$, $(\mathfrak{o}/p)=1$ and $n_{\mathfrak{o}}=n$, by the following

THEOREM (Nagel [7], Satz V). *Let n be an odd natural number. Let x and z be natural numbers such that $(x,z)=1$, $x^2<z^n$, $2\nmid z$, and $q\,\|\,x$ for any prime divisor q of n. Let $z=\prod_i q_i^{e_i}$ be the prime decomposition of z. Set $K=\boldsymbol{Q}(\sqrt{x^2-z^n})$. Then, $(K/q_i)=1$ and $\mathfrak{q}_i=(q_i,x+\sqrt{x^2-z^n})$ is a prime ideal of K over q_i. Set $\mathfrak{a}=\prod_i\mathfrak{q}_i^{e_i}$. Then, the ideal class of $\mathfrak{a}$ is of order n.*

Hence, we obtain our assertion.

By Lemmas 3, 4, 5, it remains to construct orders $\mathfrak{o}\in M(p,1)$ with $n_{\mathfrak{o}}=n$ when $(p,n)=(2,11)$, $(2,13)$, (2.17), $(2,19)$, $(2,22)$, $(2,23)$.

Using the table of Wada [9], we see, by a simple calculation, that the maximal order of the following imaginary quadratic field $K(p,n)$ is an example of such an order for the above (p,n).

(p,n)	$(2,11)$	$(2,13)$	$(2,17)$
$K(p,n)$	$\boldsymbol{Q}(\sqrt{-167})$	$\boldsymbol{Q}(\sqrt{-263})$	$\boldsymbol{Q}(\sqrt{-383})$
$h(p,n)$	11	13	17
(p,n)	$(2,19)$	$(2,22)$	$(2,23)$
$K(p,n)$	$\boldsymbol{Q}(\sqrt{-311})$	$\boldsymbol{Q}(\sqrt{-591})$	$\boldsymbol{Q}(\sqrt{-647})$
$h(p,n)$	19	22	25

($h(p,n)$ denotes the class number of $K(p,n)$.)

This completes the proof of Theorem 2.

§4. Real quadratic fields

Set $M(p)$ (resp. $M(p)_+$) $= \{\mathfrak{o}$; orders of imaginary (resp. real) quadratic fields with $(\mathfrak{o}/p) = 1\}$. Let $N(p)$ (resp. $N(p)_+$) be the image of the map $\partial(p)$ (resp. $\partial(p)_+$):

$$M(p) \text{ (resp. } M(p)_+) \ni \mathfrak{o} \longrightarrow n_0 \in \boldsymbol{N}\,.$$

By Theorem 2, $N(p) = \boldsymbol{N}$. In this section, we prove the following

PROPOSITION. $N(p)_+ = \boldsymbol{N}$.

First, we give a definition.

DEFINITION. Let $d(>1)$ be a square free integer, and let $m(>1)$ and g be natural numbers. Let $(X, Y) = (u, v)$ be a rational integral solution of the diophantine equation

$$X^2 - dg^2Y^2 = \pm 4m\,. \tag{3}$$

We say that (u, v) is a trivial solution if $m = n^2$ is a square and $n \mid u$, $n \mid vg$.

LEMMA 6. *Let $d(>1)$ be a square free integer and g a natural number. Set $K = \boldsymbol{Q}(\sqrt{d})$. Let $\varepsilon = (1/2)(s + tg\sqrt{d})$ be a nontrivial unit of the order of K with conductor g such that $\varepsilon > 1$ and $N(\varepsilon) = -1$* (resp. $N(\varepsilon) = 1$). *For a natural number $m(>1)$, if the diophantine equation* (3) *has a nontrivial solution, an inequality $m \geq s/t^2$ (resp. $m \geq (s-2)/t^2$) holds.*

When m is not a square and $g = 1$, this lemma was proved in Ankeny, Chowla and Hasse [2] and Hasse [3]. The proof of the general case goes through similarly and we shall not give the proof.

Now, we shall prove our proposition. Let n be a natural number. We see easily that $p^{2n} + 4$ is not a square. Let $K = \boldsymbol{Q}(\sqrt{p^{2n} + 4})$. First, we deal with the case $p \neq 2$. Write $p^{2n} + 4 = g^2d$ with a natural number g and a square free integer d. Let $\mathfrak{o}$ be the order of K with conductor g. We claim that $(\mathfrak{o}/p) = 1$ and $n_0 = n$. We easily see that $(\mathfrak{o}/p) = 1$, $\mathfrak{o} = [1, (1 + \sqrt{p^{2n} + 4})/2]$ and $\varepsilon = (1/2)(p^n + \sqrt{p^{2n} + 4})$ is a nontrivial unit of $\mathfrak{o}$ with $N(\varepsilon) = -1$. Set $\alpha = 1 - \varepsilon$. Then, $\alpha \in \mathfrak{o}$, $N(a) = -p^n$ and $(\alpha, \alpha') = 1$. Therefore, $\mathfrak{p}_0^n = (\alpha)$ or $\mathfrak{p}_0^n = (\alpha')$, hence by the definition of n_0, $n_0 \mid n$. On the other hand, $\mathfrak{p}_0^{n_0} = (a + b(1 + \sqrt{p^{2n} + 4})/2)$ for some a, $b \in \boldsymbol{Z}$. Taking norms of both sides, we obtain $\pm 4p^{n_0} = (2a + b)^2 - b^2(p^{2n} + 4) = (2a + b)^2 - dg^2b^2$. Since $(\mathfrak{p}_0, \mathfrak{p}_0') = 1$, $(X, Y) = (2a + b, b)$ is a nontrivial solution of the diophantine equation $X^2 - dg^2Y^2 = \pm 4p^{n_\mathfrak{o}}$. Therefore, by Lemma 6 and the fact that ε is a unit of $\mathfrak{o}$ with $N(\varepsilon) = -1$, we get $p^{n_\mathfrak{o}} \geq p^n$, i.e. $n_\mathfrak{o} \geq n$. Hence $n_\mathfrak{o} = n$, which proves our claim. Next, we deal with the case $p = 2$. Assume $n \geq 3$ and set $m = n - 2$ (≥ 1). Then, $p^{2n} + 4 = 4g^2d$ for an odd natural number g and a square free integer d with $d \equiv 1$ (mod 8). We claim that for the order $\mathfrak{o}$ of K with conductor g, $(\mathfrak{o}/2) = 1$ and $n_\mathfrak{o} = m$. Since g is odd and $d \equiv 1$ (mod 8), $(\mathfrak{o}/p) = 1$. Set $\alpha = (1/2)(2^{n-1} + 1 + \sqrt{2^{2n-2} + 1})$. Then, $a \in \mathfrak{o}$, $N(\alpha) = 2^m$ and $(\alpha, \alpha') = 1$. Therefore, $\mathfrak{p}_\mathfrak{o}^m = (\alpha)$ or $\mathfrak{p}_\mathfrak{o}^m = (\alpha')$, hence $n_\mathfrak{o} | m$. Then, similarly to the case $p \neq 2$, we see that $n_\mathfrak{o} = m$ by Lemma 6 and the fact that $\varepsilon = (1/2)(2^n + 2\sqrt{2^{2n-2} + 1})$ is a unit of $\mathfrak{o}$ with $N(\varepsilon) = -1$.

This completes the proof of our proposition.

Remark 1. The fact that $N(p) = N$ is also proved as follows. Let n be a natural number. Set $K = \boldsymbol{Q}(\sqrt{1 - 4p^n})$. Write $1 - 4p^n = g^2d$ for a natural number g and a square free integer d. Then, by Lemma 2, $(\mathfrak{o}/p) = 1$ and $n_\mathfrak{o} = n$, for the order $\mathfrak{o}$ of K with conductor g.

Remark 2. We have seen that the maps $\partial(p)$, $\partial(p)_+$ are surjective. For any $n \in N$, the inverse image $\partial(p)^{-1}(n)$ is a finite set, but $\partial(p)_+^{-1}(n)$ is an infinite set. This is shown as follows.

The imaginary quadratic case: Obvious.

The real quadratic case: (The notations being as in the proof of Proposition.) First, we deal with the case $p \neq 2$. Let $(1/2)(s + tg\sqrt{d})$ be a nontrivial unit of $\mathfrak{o}$ with $s, t > 0$. Let $\mathfrak{o}_1$ be the order of K with conductor $(((p^n - 2)t + s)/2)g$. Then, we easily see that $(\mathfrak{o}_1/p) = 1$ and $n_{\mathfrak{o}_1} = n$. Since there are infinitely many units of $\mathfrak{o}$, there exist infinitely many $\mathfrak{o}_1$'s with $(\mathfrak{o}_1/p) = 1$ and $n_{\mathfrak{o}_1} = n$. It is proved similarly when $p = 2$.

Remark 3. Set $M(p, 1)_+ = \{\mathfrak{o}$; maximal orders of real quadratic fields with $(\mathfrak{o}/p) = 1\}$. Let $N(p, 1)_+$ be the image of the map $\partial(p, 1)_+ : M(p, 1)_+ \ni \mathfrak{o} \to n_\mathfrak{o} \in N$. We see that $n = 1, 2 \in N(p, 1)_+$ and the inverse images $\partial(p, 1)_+^{-1}(1)$, $\partial(p, 1)_+^{-1}(2)$ are infinite sets by considering the following real quadratic fields:

$n = 1$; $K = \boldsymbol{Q}(\sqrt{x^2 + 4p})$ where x is a rational integer prime to $2p$. (Fields of this type were considered in Yamamoto [10].)

$n = 2$; $K = \boldsymbol{Q}(\sqrt{q(q - 4p)})$ where q is a prime number such that $q > 4p$, $(-1/q) = 1$ and $(p/q) = -1$.

In view of this, we can raise questions: (1) *for any* $n \in N(p, 1)_+$, *is* *the inverse image* $\partial(p, 1)_{+}^{-1}(n)$ *an infinite set?* (2) *does* $N(p, 1)_{+}$ *coincide with* N?

REFERENCES

[1] N. C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, Pacific J. Math., **5** (1955), 321–324.

[2] N. C. Ankeny, S. Chowla and H. Hasse, On the class number of the maximal real subfields of a cyclotomic field, J. reine angew. Math., **217** (1965), 217–220.

[3] H. Hasse, Über die mehrklassige, aber einegeschlechtige reell-quadratische Zahkl-körper, Elem. Math., **20** (1965), 49–58.

[4] P. Humbert, Sur les nombres de classes de certains corps quadratiques, Comment. Math. Helv., **12** (1939/40), 233–245.

[5] S.-N. Kuroda, On the class number of imaginary quadratic number fields, Proc. Japan Acad., **40** (1964), 365–367.

[6] S. Lang, Elliptic functions, Addison Wesley (1973).

[7] T. Nagel, Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. Humburg, **1** (1922), 140–150.

[8] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math., **6** (1962), 64–94.

[9] H. Wada, The table of the class number of the quadratic field $\boldsymbol{Q}(\sqrt{-m})$, $1 \leq m < 24000$, RIMS Kokyuroku, **89** (1970), 90–114.

[10] Y. Yamamoto, Real quadratic number fields with large fundamental units, Osaka J. Math., **8** (1971), 261–270.

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo, 113 Japan