H. Yokoi
Nagoya Math. J.
Vol. 33 (1968), 139–152

ON REAL QUADRATIC FIELDS CONTAINING UNITS WITH NORM -1

HIDEO YOKOI

Let $\boldsymbol{Q}$ be the rational number field, and let $K=\boldsymbol{Q}(\sqrt{D})$ ($D>0$ a rational integer) be a real quadratic field. Then, throughout this paper, we shall understand by the fundamental unit ε_D of $\boldsymbol{Q}(\sqrt{D})$ the normalized fundamental unit $\varepsilon_D>1$.

Recently H. Hasse investigated variously real quadratic fields with the genus 1, but with the class number more than one[1]. However, since he needed there to know a explicit form of the fundamental unit of a real quadratic field, his investigation had naturally to be restricted within the case of real quadratic fields of Richaud-Degert type whose fundamental units were already given explicitly.

In this paper, we shall give explicitly the fundamental units of real quadratic fields of the more general type than Richaud-Degert's in the case of real quadratic fields with the fundamental unit ε satisfying $N\varepsilon=-1$, and consider the class number of real quadratic fields of this type as Hasse did in the case of Richaud-Degert type.

In §1, by means of expressing any unit $\varepsilon=(t+u\sqrt{D})/2$ of $\boldsymbol{Q}(\sqrt{D})$ as a function of t, we shall give first a generating function of all real quadratic fields with the fundamental unit whose norm is equal to -1 (Theorem 1). In §2, by means of classifying all units $\varepsilon=(t+u\sqrt{D})/2$ with $N\varepsilon=-1$ by the positive value of u, we shall prove that in the class of $u=p$ or $2p$ (p is 1 or prime congruent to 1 mod 4) the unit $\varepsilon=(t+u\sqrt{D})/2>1$ becomes the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$ except for at most finite number of values of D (Theorem 2 and its Corollary). Moreover, we shall show that real quadratic fields of Richaud-Degert type essentially correspond to real quadratic fields with the fundamental unit belonging to the class of $u=1$ or 2 in such classification (Proposition 2). In §3, we shall give an estima-

Received February 21, 1968.

1) Cf. H. Hasse [3].

tion formula from below of the class number of real quadratic fields with the fundamental unit belonging to the class of $u=p$ or $2p$ (Theorem 3). Finally, in §4 we shall show a few examples in concrete cases of $p=5$, 13.

§1. Generating function

In order to investigate real quadratic fields with the fundamental unit whose norm is equal to -1, we first give a generating function of those real quadratic fields. The following theorem may be already known, but since by using the theorem we can easily draw up a list of the fundamental unit ε_D of real quadratic fields $\boldsymbol{Q}(\sqrt{D})$ satisfying $N\varepsilon_D=-1$[2] and our investigation in this note is based on it, we dare add a simple proof of it.

THEOREM 1. *Let $\boldsymbol{Q}(\sqrt{D})$ $(D>0$ square-free) be a real quadratic field, then any unit ε of $\boldsymbol{Q}(\sqrt{D})$ satisfying $N\varepsilon=-1$ is of the form $\varepsilon=(t+\sqrt{t^2+4})/2$ for some integer t, and the reverse is also true.*

In particular, all real quadratic fields with the fundamental unit ε satisfying $N\varepsilon=-1$ are generated by the function $\sqrt{t^2+4}$ over $\boldsymbol{Q}$, and conversely any field $\boldsymbol{Q}(\sqrt{t^2+4})$ $(t\neq 0)$ generated by $\sqrt{t^2+4}$ over $\boldsymbol{Q}$ is a real quadratic field with the fundamental unit ε satisfying $N\varepsilon=-1$.

Proof. Since an unit ε of a real quadratic field $\boldsymbol{Q}(\sqrt{D})$ $(D>0$ square-free) is an integer whose norm is equal to ± 1, ε is of the form $\varepsilon=(t+u\sqrt{D})/2$; $t\equiv u \pmod 2$, moreover $t\equiv u\equiv 0 \pmod 2$ for the special case of $D\equiv 2, 3 \pmod 4$, and (t, u) satisfies Pell's equation $x^2-Dy^2=\pm 4$ because of $\pm 1=N\varepsilon=(t^2-Du^2)/4$.

Conversely, if a pair of integers (t, u) satisfies Pell's equation $t^2-Du^2=-4$, then clearly $t\equiv u \pmod 2$ and moreover $t\equiv u\equiv 0 \pmod 2$ for the special case of $D\equiv 2, 3 \pmod 4$. For, if we assume $t\equiv u\equiv 1 \pmod 2$, then we have $t^2\equiv u^2\equiv 1 \pmod 4$, and hence $t^2-Du^2=-4$ implies $D\equiv 1 \pmod 4$. Therefore, $\varepsilon=(t+u\sqrt{D})/2=(t\pm\sqrt{Du^2})/2=(t\pm\sqrt{t^2+4})/2$ is a unit of $\boldsymbol{Q}(\sqrt{D})$ satisfying $N\varepsilon=-1$.

The following lemma may be partly known, but it is useful throughout this note.

LEMMA 1. *If Pell's equation $t^2-Du^2=-4$ is solvable for a positive square-free integer D, then the prime decompositions of D, u are of the following form:*

2) Cf. Table 1.

$$D = 2^{\delta_1} \prod_i p_i, \quad u = 2^{\delta_2} \prod_j q_j^{e_j},$$

where δ_1, δ_2 *take the value* 0 *or* 1, p_i, q_j *are congruent to* 1 *mod* 4, *and* e_j *are positive integers. Moreover,* $D \equiv 2$ (*mod* 4) *implies* $t \equiv 0$ (*mod* 2), *which is equivalent to* $u \equiv 0$ (*mod* 2).

Proof. If Pell's equation $t^2 - Du^2 = -4$ is solvable, then $t^2 \equiv -4$ (mod Du^2) holds, and hence for any odd prime factor p of Du^2, we have $t^2 \equiv -4$ (mod p). Therefore, we get $1 = \left(\frac{-4}{p}\right) = (-1)^{\frac{p-1}{2}}$, which implies $p \equiv 1$ (mod 4).

Next, if $u \equiv 0$ (mod 4) holds, then $t^2 - Du^2 = -4$ implies $t \equiv 0$ (mod 2), and hence we may put $u = 4u_0$, $t = 2t_0$, and we have $t_0^2 - 4Du_0^2 = -1$. Therefore, we get $t_0^2 \equiv -1$ (mod 4), which is a contradiction. The remaining part is clear from $t^2 - Du^2 = -4$.

§2. Fundamental unit

We first give the fundamental unit of real quadratic fields of two types.

PROPOSITION 1. (i) *If* $D = t^2 + 4$ $(t > 0)$ *is square-free, then* $\varepsilon_D = (t + \sqrt{t^2+4})/2$ *is the fundamental unit of the real quadratic field* $\boldsymbol{Q}(\sqrt{D})$ *and* $N\varepsilon_D = -1$.

(ii) *If* $D = t_0^2 + 1$ $(0 < t_0 \neq 2)$ *is square-free, then* $\varepsilon_D = t_0 + \sqrt{t_0^2+1}$ *is the fundamental unit of the real quadratic field* $\boldsymbol{Q}(\sqrt{D})$ *and* $N\varepsilon_D = -1$.

Proof. Let $(x, y) = (t, u)$ be the least positive integral solution of Pell's equation $x^2 - Dy^2 = -4$ (if exists), then $\varepsilon_D = (t + u\sqrt{D})/2$ is the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{D})$ and $N\varepsilon_D = -1$. Therefore, in the special case of $y = u = 1$, i.e. $t^2 - D = -4$, $\varepsilon_D = (t + u\sqrt{D})/2 = (t + \sqrt{t^2+4})/2$ is certainly the fundamental unit of $\boldsymbol{Q}(\sqrt{t^2+4})$ provided that $D = t^2 + 4$ is square-free. In the case of $y = u = 2$, we get $t \equiv 0$ (mod 2) from lemma 1, and hence we may put $t = 2t_0$, and $t_0^2 - D = -1$ holds. Hence, $\varepsilon_D = (t + u\sqrt{D})/2 = t_0 + \sqrt{t_0^2+1}$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{t_0^2+1})$ provided that $D = t_0^2 + 1$ is square-free and D is not of the above mentioned type (i). However, $D = t_0^2 + 1 = t^2 + 4$ holds for some integers t_0, t if and only if t_0 is equal to 2, i.e. $D = 5 = 2^2 + 1 = 1^2 + 4$. Thus, the proposition 1 is proved in both cases.

Probably, the following result of Richaud-Degert[3] is only one that gives explicitly the fundamental unit of real quadratic fields of certain type.

LEMMA 2 (*Richaud-Degert*). *Let* $\boldsymbol{Q}(\sqrt{D})$ $(D>0$ *square-free) be a real quadratic field, and put* $D=n^2+r\,(-n<r\leqq n)$. *Then, if* $4n\equiv 0 \pmod r$ *holds, the fundamental unit* ε_D *of* $\boldsymbol{Q}(\sqrt{D})$ *is of the following form:*

$$\varepsilon_D = n+\sqrt{D} \text{ with } N\varepsilon_D = -\operatorname{sgn} r \text{ for } |r|=1,$$
$$(\text{except for } D=5,\ n=2,\ r=1),$$
$$\varepsilon_D = (n+\sqrt{D})/2 \text{ with } N\varepsilon_D = -\operatorname{sgn} r \text{ for } |r|=4,$$
$$\varepsilon_D = [(2n^2+r)+2n\sqrt{D}]/r \text{ with } N\varepsilon_D = 1 \text{ for } |r|\neq 1,\ 4.$$

Such type of real quadratic fields that the assumption of this lemma is satisfied we shall call simply R-D type. Then the following proposition shows a relation between the type of real quadratic fields in proposition 1 and R-D type in the case of real quadratic fields with the fundamental unit whose norm is equal to -1.

PROPOSITION 2. *A real quadratic field* $\boldsymbol{Q}(\sqrt{D})$ $(D>0$ square-free) *with the fundamental unit whose norm is equal to* -1 *is of R-D type if and only if* D *is of the form* $D=t^2+4$ *or* t_0^2+1 $(t,\ t_0>0$ *integer) except for* $D=5,\ 13$; *in other words, if and only if* u *in the least positive integral solution* $(x,y)=(t,u)$ *of Pell's equation* $x^2-Dy^2=-4$ *is equal to* 1 *or* 2.

Proof. Let $\boldsymbol{Q}(\sqrt{D})$ $(D>0$ square-free) be a real quadratic field with the fundamental unit whose norm is equal to -1. Then, if $\boldsymbol{Q}(\sqrt{D})$ is of R-D type, D is of the form $D=t^2+4$ or t_0^2+1, $(t,\ t_0>0$ integers) by lemma 2, and hence it follows from proposition 1 that in the least positive integral solution $(x,y)=(t,u)$ of Pell's equation $x^2-Dy^2=-4$ is equal to 1 or 2.

Conversely, if $u=2$, i.e. $D=t_0^2+1$, then $\boldsymbol{Q}(\sqrt{D})$ is clearly of R-D type. On the other hand, in the case of $u=1$, i.e. $D=t^2+4$, $\boldsymbol{Q}(\sqrt{D})$ is of R-D type if and only if $t\geqq 4$ holds. However, in the case of $t=2$, D is equal to 8 and is not square-free.

Therefore, except for $D=5$ with $t=1$ and $D=13$ with $t=3$, it is equivalent to $u=1$ or 2 that the real quadratic field $\boldsymbol{Q}(\sqrt{D})$ with the fundamental unit whose norm is equal to -1 is of R-D type.

3) Cf. G. Degert [2] and C. Richaud [6].

Thus, both $\boldsymbol{Q}(\sqrt{5})$ and $\boldsymbol{Q}(\sqrt{13})$ are not of R-D type, but both values of u in the least positive integral solution $(x, y) = (t, u)$ of Pell's equation $x^2 - Dy^2 = -4$ are equal to 1. Hence, from now, we shall understand R-D type in such a wide sense that it contains both $\boldsymbol{Q}(\sqrt{5})$ and $\boldsymbol{Q}(\sqrt{13})$.

In order to give explicitly the fundamental unit of real quadratic fields of a new type different from R-D's, we must prepare the following three lemmas:

LEMMA 3. *For any prime p satisfying $p \equiv 1$ (mod 4), an unit ε of a real quadratic field $\boldsymbol{Q}(\sqrt{D})$ that is of the form $(t + p\sqrt{D})/2$ or $t + p\sqrt{D}$ $(D > 0$ square-free) and that satisfies $N\varepsilon = -1$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$ if and only if the real quadratic field $\boldsymbol{Q}\sqrt{D})$ is not of R-D type.*

Proof. Let $\varepsilon_0 = (t_0 + u_0\sqrt{D})/2$ $(D > 0$ square-free) be the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{D})$, then the norm of ε_0 is equal to -1 and there exists an odd integer n satisfying $\varepsilon = \varepsilon_0^n$. If we put for this odd integer n $2^n\varepsilon_0^n = (t_0 + u_0\sqrt{D})^n = T + U\sqrt{D}$, then we have $U = {}_nC_1 t_0^{n-1}u_0 + {}_nC_3 t_0^{n-3}u_0^3 D + \cdots + {}_nC_{n-2} t_0^2 u_0^{n-2} D^{\frac{n-3}{2}} + {}_nC_n u_0^n D^{\frac{n-1}{2}} \equiv 0 \pmod{u_0}$, while we have $U = 2^{n-1}p$ or $2^n p$. Hence, in the case of $u_0 \equiv 1$ (mod 4), we get $p \equiv 0 \pmod{u_0}$, which implies $u_0 \equiv 1$ or p. In the case of $u_0 \equiv 1$ (mod 4), we may put by lemma 1 $u_0 = 2u_0'$, $u_0' \equiv 1$ (mod 4). Hence, we get $p \equiv 0 \pmod{u_0'}$, which implies $u_0' = 1$ or p. Therefore, the condition $u_0 = p$ or $2p$ is equivalent to $u_0 \neq 1, 2$. On the other hand, since the condition $\varepsilon_0 = \varepsilon$ is equivalent to $u_0 = p$ or $2p$, it follows from proposition 2 that $\varepsilon = \varepsilon_0$ holds if and only if the real quadratic field $\boldsymbol{Q}(\sqrt{D})$ is not of R-D type.

LEMMA 4. *For any prime p satisfying $p \equiv 1$ (mod 4), there are two uniquely determined integers a, b such that $a^2 + 4 = bp^2$, $0 < a < p^2$. Moreover, for these p, a, b, $D = p^2m^2 \pm 2am + b$ $(m > 0)$ is congruent to 1 mod 4 or congruent to 4 or 8 mod 16, and Pell's equation $t^2 - Du^2 = -4$ is always solvable.*[4)]

Proof. Since for any prime p congruent to 1 mod 4 we get $\left(\frac{-4}{p}\right) = 1$, congruence $x^2 \equiv -4 \pmod{p}$ is solvable, and hence congruence $x^2 \equiv -4$ $(\mathrm{mod}\ p^2)$ is also solvable. Among the solutions of this congruence $x^2 \equiv -4$

4) L. Rédei notes in [5] that if Pell's equation $t^2 - du^2 = -1$ is solvable for some integer $d = d_0$, then the Pell's equation is also solvable for $d = u_0^2m^2 + 2t_0m + d_0$, where (t_0, u_0) is any positive integral solution of $t^2 - d_0u^2 = -1$ and m is any integer.

(mod p^2), there exists only one solution $x \equiv \pm a$ (mod p^2) satisfying $0 < a < p^2$. For this positive integer a, there is a unique integer b satisfying $a^2 + 4 = bp^2$. Conversely, if $a^2 + 4 = bp^2$ holds, then $x \equiv \pm a$ (mod p^2) is a solution of congruence $x^2 \equiv -4$ (mod p^2).

Next, set $D = p^2m^2 \pm 2am + b$, $t = p^2m \pm a$, $u = p$ $(m > 0)$, then Pell's equation $t^2 - Du^2 = -4$ is certainly satisfied by these D, t, u. Therefore, if we note only that $p^2 \equiv 1$ (mod 4) and $t^2 + 4 = Dp^2$, it is easy to see that $D \equiv 1$ (mod 4) for odd t, and $D \equiv 0$ (mod 4) for even t. In the case of $D \equiv 0$ (mod 4), we may put $D = 4D_0$, $t = 2t_0$, and get $t_0^2 + 1 = D_0p^2$. Hence, we obtain similarly $D_0 \equiv 2$ (mod 4) for odd t_0 and $D_0 \equiv 1$ (mod 4) for even t. Thus, we have $D = 4D_0 \equiv 4$ or 8 (mod 16).

In order to prove theorem 2 we require another lemma, which is itself of some interest.

LEMMA 5. *For any integers $a > 0$, b, c satisfying $b \not\equiv 0$ (mod a), there exist at most a finite number of such natural n that $f(n) = a^2n^2 + bn + c$ is square.*

Proof. It follows from the assumption $b \not\equiv 0$ (mod a) that an integer k satisfying $\left|\frac{b}{2a} - k\right| < \frac{1}{2}$ is uniquely determined. By using this integer k, we rewrite $f(n)$ in the following form:

$$f(n) = a^2n^2 + bn + c = (an + k)^2 + (b - 2ak)n + (c - k^2).$$

Then, since $|b - 2ak| < a$, the inequality

$$-(an + k) < (b - 2ak)n + (c - k^2) < an + k$$

holds for all natural n except at most finite number of cases. Moreover, since $b - 2ak \neq 0$, we know that

$$(b - 2ak)n + (c - k^2) \neq 0$$

holds for all natural n except for at most one.

On the other hand, the above inequality shows that $(b - 2ak)n + (c - k^2)$ is the nearest integer to $\sqrt{f(n)}$ in absolute value. Therefore, $f(n) = a^2n^2 + bn + c$ does not become square for any natural n apart from a finite number of exceptions. The lemma is thus proved.

THEOREM 2. *For any prime p congruent to 1 mod 4, let, a, b denote the integer in lemma 4 satisfying $a^2 + 4 = bp^2$ $(0 < a < p^2)$. Then, there exists an integer $D_0 = D_0(p)$ such that if $D = p^2m^2 \pm 2am + b$ $(m \geqq 0)$ has no square factor* *except* 4, *and if* $D \geqq D_0$, *the real quadratic field* $\boldsymbol{Q}(\sqrt{D})$ *is not of R-D type. Therefore, the fundamental unit* ε_D *of* $\boldsymbol{Q}(\sqrt{D})$ *is of the following form*:

$$\varepsilon_D = \begin{cases} [(p^2m \pm a) + p\sqrt{D}]/2 \cdots\cdots\cdots D\text{: } \textit{square-free}, \\ (p^2m \pm a)/2 + p\sqrt{D/4} \cdots\cdots \textit{otherwise}, \end{cases}$$

and $N\varepsilon_D = -1$.

Proof. Since Pell's equation $t^2 - Du^2 = -4$ is satisfied by $D = p^2m^2 \pm 2am + b$, $t = p^2m \pm a$, $u = p$, $\varepsilon = [(p^2m \pm a) + p\sqrt{D}]/2$ is an unit of the real quadratic field $\boldsymbol{Q}(\sqrt{D})$, and $N\varepsilon = -1$. Moreover, by our assumptions $a^2 + 4 = bp^2$ and $p \equiv 1 \pmod 4$ we have $2a \equiv 0 \pmod p$. Therefore, in the case that D is square-free, it follows from lemma 5 that both $D - 1 = p^2m^2 \pm 2am + b - 1$ and $D - 4 = p^2m^2 \pm 2am + b - 4$ are never square for any natural m except at most a finite number, and hence by lemma 2 the quadratic field $\boldsymbol{Q}(\sqrt{D})$ is not of R-D type for any natural m except at most a finite number. In the case of $D = 4D_0$($D_0 > 0$ square-free), we have $t = p^2m \pm a \equiv 0 \pmod 2$ by lemma 1, and hence $m \equiv a \pmod 2$. By our assumptions $a^2 + 4 = bp^2$, $p \equiv 1 \pmod 4$, $a \equiv 0 \pmod 2$ is equivalent to $b \equiv 0 \pmod 4$, and $a \equiv 1 \pmod 2$ is equivalent to $b \equiv 1 \pmod 4$.

Therefore, in the case of $m \equiv 0 \pmod 2$, we may put $m = 2m_0$, $b = 4b_0$ and get $D_0 = D/4 = p^2m_0^2 \pm am_0 + b_0$. Since $a \not\equiv 0 \pmod p$, it follows from lemma 5 that both $D_0 - 1$ and $D_0 - 4$ are never square for any natural m except at most a finite number. In the case of $m \equiv 1 \pmod 2$, we may put $m = 2m_0 + 1$, $b = 4b_0 + 1$ and get $D_0 = D/4 = p^2m_0^2 + (p^2 \pm a)m_0 + (b_0 + (p^2 + 1 \pm 2a)/4)$. Since $p^2 \pm a \equiv \pm a \not\equiv 0 \pmod p$, it follows from lemma 5 that both $D_0 - 1$ and $D_0 - 4$ are never square for any natural m_0 except at most a finite number. Thus, for both types of m, we see at once from lemma 2 that the quadratic field $\boldsymbol{Q}(\sqrt{D}) = \boldsymbol{Q}(\sqrt{D/4})$ is never of R-D type for any natural m up to at most a finite number of exceptions.

Therefore, it was proved by lemma 3 for both types of D that there exists an integer $D_0 = D_0(p)$ such that the above mentioned unit $\varepsilon = [(mp^2 \pm a) + p\sqrt{D}]/2$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$ provided that D has no square factor except 4, and that $D \geqq D_0(p)$.

This theorem implies the following sufficient condition for an unit ε of a real quadratic field $\boldsymbol{Q}(\sqrt{D})$ ($D > 0$ square-free) satisfying $N\varepsilon = -1$ to be the fundamental unit.

COROLLARY. *For any prime p congruent to 1 mod 4, there exists an integer $D_0 = D_0(p)$ such that if for some square-free D satisfying $D \geqq D_0$ the real quadratic field $\boldsymbol{Q}(\sqrt{D})$ contains an unit ε of the form $\varepsilon = (t_0 + p\sqrt{D})/2$ or $t_0 + p\sqrt{D}$ and $N\varepsilon = -1$ holds, then the unit ε is the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$.*

Proof. In the case of $\varepsilon = (t_0 + p\sqrt{D})/2$, $-1 = N\varepsilon = (t_0^2 - Dp^2)/4$ implies $t_0^2 + 4 = Dp^2$. Hence, $x \equiv t_0 \pmod{p^2}$ is a solution of $x^2 \equiv -4 \pmod{p^2}$. On the other hand, let a, b be as in lemma 4 satisfying $a^2 + 4 = bp^2$, then we get $t_0 = p^2 m_1 \pm a$ for some integer $m_1 \geqq 0$. Therefore, $Dp^2 = t_0^2 + 4 = (p^2 m_1 \pm a)^2 + 4 = p^2(p^2 m_1^2 \pm 2am_1 + b)$ implies $D = p^2 m_1^2 \pm 2am_1 + b$ $(m_1 \geqq 0)$. If we choose D_0 in theorem 2 as $D_0 = D_0(p)$ in question, and consider square-free D satisfying $D \geqq D_0$, then it follows from theorem 2 that the unit $\varepsilon = (t_0 + p\sqrt{D})/2$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$.

In the case of $\varepsilon = t_0 + p\sqrt{D}$, $-1 = t_0^2 - Dp^2$ implies $t_0^2 + 1 = Dp^2$. Hence, there exists an integer $m_2 \geqq 0$ satisfying $2t_0 = p^2 m_2 \pm a$, because $x \equiv 2t_0 \pmod{p^2}$ is a solution of $x^2 \equiv -4 \pmod{p^2}$. Therefore, $(4D)p^2 = (2t_0)^2 + 4 = (p^2 m_2 \pm a)^2 + 4 = p^2(p^2 m_2^2 \pm 2am_2 + b)$ implies $4D = p^2 m_2^2 \pm 2am_2 + b$ $(m_2 \geqq 0)$. If we choose D_0 in theorem 2 as $D_0 = D_0(p)$ in question and consider square-free D satisfying $D_0 \leqq 4D$, it follows from theorem 2 that the unit $\varepsilon = t_0 + p\sqrt{D}$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$. Thus, in both cases the corollary is proved.

§3. Class number

In this §, we give an estimation formula from below of the class number of those real quadratic fields whose fundamental unit was given in §2. To this purpose we require the following lemma of Davenport-Ankeny-Hasse:

LEMMA 6. *(Davenport-Ankeny-Hasse)*[5] *Let $\boldsymbol{Q}(\sqrt{D})$ $(D > 0$ square-free) be a real quadratic field with the fundamental unit $\varepsilon_D = (t + u\sqrt{D})/2$ $(t, u > 0)$. Then, if Pell's equation $(x^2 - Du^2)/4 = \pm m$ (m not square) is solvable, the following inequality holds:*

$$\begin{cases} m \geqq (t-2)/u^2 & \text{for} \quad N\varepsilon_D = 1, \\ m \geqq t/u^2 & \text{for} \quad N\varepsilon_D = -1. \end{cases}$$

[5] Cf. N.C. Ankeny, S. Chowla and H. Hasse [1] and H. Hasse [3].

Let us quote this boundary $s = t/u^2$ for $N\varepsilon_D = -1$ in lemma 6 as Hasse's boundary (in the lemma of D-A-H).

THEOREM 3. *For any prime p congruent to 1 mod 4, let a, b denote the integers in lemma 4 satisfying $a^2+4=bp^2$ $(0<a<p^2)$, and let $D_0 = D_0(p)$ be the integer in theorem 2. Furthermore, set $D = p^2m^2 \pm 2am + b$ for any integer m bigger than $4p$, and consider D bigger than $D_0(p)$. Then, if D has no square factor except 4 and p splits in the real quadratic field $\boldsymbol{Q}(\sqrt{D})$ into two conjugate prime ideals with the degree one, these prime ideals are not principal. Therefore, the class number h of $\boldsymbol{Q}(\sqrt{D})$ is bigger than one and the following estimation from below holds:*

$$h \geqq \frac{\log\sqrt{Dp^2-4}}{\log p} - 2 \quad \textit{for} \quad D \equiv 1 \quad (\textit{mod } 2),$$

$$h \geqq \frac{\log\frac{1}{4}\sqrt{Dp^2-4}}{\log p} - 2 \quad \textit{for} \quad D \equiv 0 \quad (\textit{mod } 2).$$

Proof. In the case of $D\equiv 1$ (mod 2), D is square-free from the assumption, and hence by theorem 2 the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$ is $\varepsilon_D = [(mp^2 \pm a) + p\sqrt{D}]/2$ provided $D \geqq D_0(p)$. Therefore, it follows from lemma 6 that Hasse's boundary is $s = (mp^2 \pm a)/p^2 = m \pm a/p^2$ $(0 < a/p^2 < 1)$. In the case of $D\equiv 0$ (mod 2), we have $D \equiv 0$ (mod 4) by lemma 4, and $D_0 = 4/D$ is square-free. Therefore, by theorem 2 the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$ is $\varepsilon_D = (mp^2 \pm a)/2 + p\sqrt{D/4}$ provided $D \geqq D_0(p)$, and hence by lemma 6 Hasse's boundary is $s = (mp^2 \pm a)/4p^2 = m/4 \pm a/4p^2$ $(0 < a/4p^2 < 1/4)$. For any integer m bigger than p (in the first case) or $4p$ (in the second case), the prime p is smaller than Hasse's boundary s i.e. $p < s$.

If we assume that the prime p splits into two conjugate principal ideals $\mathfrak{p}$, $\mathfrak{p}'$ with the degree one in $\boldsymbol{Q}(\sqrt{D})$, then Pell's equation $(x^2 - Dy^2)/4 = \pm p$ is solvable, and hence lemma 6 implies $p > s$, which is contrary to the above assertion $p < s$. Therefore, if the prime p splits into two conjugate prime ideals $\mathfrak{p}$, $\mathfrak{p}'$ with the degree one in $\boldsymbol{Q}(\sqrt{D})$, then the prime $\mathfrak{p}$, $\mathfrak{p}'$ are not principal. Moreover, the order of those prime ideals $\mathfrak{p}$, $\mathfrak{p}'$ in the ideal class group of $\boldsymbol{Q}(\sqrt{D})$ is bigger than one and it is a factor of the ideal class number h of $\boldsymbol{Q}(\sqrt{D})$. Hence, in the case of $D\equiv 1$ (mod 2), we have

$$p^h \geqq s = \frac{mp^2 \pm a}{p^2} = \frac{\sqrt{Dp^2-4}}{p^2},$$

which implies

$$h \geqq \frac{\log \sqrt{Dp^2 - 4}}{\log p} - 2,$$

and similarly in the case of $D \equiv 0 \pmod 2$, we have

$$p^h \geqq s = \frac{mp^2 \pm a}{4p^2} = \frac{\sqrt{Dp^2 - 4}}{4p^2},$$

which implies

$$h \geqq \frac{\log \frac{1}{4}\sqrt{Dp^2 - 4}}{\log p} - 2.$$

Thus, the theorem is completely proved.

Remark 1. In the case of $D \ngeqq D_0(p)$, $\varepsilon = [(mp^2 \pm a)/2 + p\sqrt{D}]$ and $\varepsilon = (mp^2 \pm a)/2 + p\sqrt{D/4}$ are not always the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{D})$, but they are always an unit of $\boldsymbol{Q}(\sqrt{D})$ satisfying $N\varepsilon = -1$. On the other hand, it is not always necessary in lemma 6 that the unit ε is the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$; it is sufficient that ε is an unit, as we can see easily from proof of lemma 6. Therefore, we can remove the condition $D \geqq D_0(p)$ in theorem 3.

Remark 2. In the case of real quadratic fields of R-D type, H. Hasse obtained already in [3] an explicit estimation formula as in theorem 3, and in the case of $\boldsymbol{Q}(\sqrt{a^2+1})$ T. Nagell also treated in [4] a similar problem.

§4. Examples

[I] *The case of* $p = 5$.

$a = 11$, $b = 5$, $D_0(p) = 61$,

$t = 25m \pm 11$, $D = 25m^2 \pm 22m + 5$.

(1) If $m \equiv 0 \pmod 2$, then $D \equiv 1 \pmod 4$, and hence the fundamental unit is

$$\varepsilon = [(25m \pm 11) + 5\sqrt{25m^2 \pm 22m + 5}]/2.$$

Hasse's boundary is $s = m \pm 11/25$.

Hence $s > 5 \Longleftrightarrow m \geqq 6$.

(2) If $m \equiv 1 \pmod 2$, then $D \equiv 0 \pmod 4$, and hence the fundamental unit is

$$\varepsilon = (25m \pm 11)/2 + 5\sqrt{(25m^2 \pm 22m + 5)/4},$$

Hasse's boundary is $s = m/4 \pm 11/100$.
Hence $s > 5 \Longleftrightarrow m \geqq 21$.
$D_0 = D/4 \equiv 2 \pmod 4 \Longleftrightarrow m \equiv 1 \pmod 4$,
$D_0 = D/4 \equiv 1 \pmod 4 \Longleftrightarrow m \equiv -1 \pmod 4$.

[II] *The case of* $p = 13$.
$a = 29$, $b = 5$, $D_0(p) = 58$,
$t = 169m \pm 29$, $D = 169m^2 \pm 58m + 5$.

(1) If $m \equiv 0 \pmod 2$, then $D \equiv 1 \pmod 4$, and hence the fundamental unit is

$$\varepsilon = [(199m \pm 29) + 13\sqrt{169m^2 \pm 58m + 5}]/2,$$

Hasse's boundary is $s = m \pm 29/169$.
Hence $s > 13 \Longleftrightarrow m \geqq 14$.

(2) If $m \equiv 1 \pmod 2$, then $D \equiv 0 \pmod 4$, and hence the fundamental unit is

$$\varepsilon = (169m \pm 29)/2 + 13\sqrt{(169m^2 \pm 58m + 5)/4},$$

Hasse's boundary is $s = m/4 \pm 29/676$.
Hence $s > 13 \Longleftrightarrow m \geqq 53$
$D_0 = D/4 \equiv 2 \pmod 4 \Longleftrightarrow m \equiv 1 \pmod 4$,
$D_0 = D/4 \equiv 1 \pmod 4 \Longleftrightarrow m \equiv -1 \pmod 4$.

References

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

[2] G. Degert, Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper. Abh. math. Sem. Univ. Hamburg **22** (1958), 92–97.

[3] H. Hasse, Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper. Elemente der Mathematik **20** (1965), 49–59.

[4] T. Nagell, Bemerkung über die Klassenzahl reell-quadratischer Zahlkörper. Det Kongelige Norske Videnskabens Selskab, Forhandlinger **11** (1938), 7–10.

[5] L. Rédei, Über die Pellsche Gleichung $t^2 - du^2 = -1$. J. reine angew. Math. **173** (1935), 193–221.

[6] C. Richaud, Sur la résolution des équations $x^2 - Ay^2 = \pm 1$. Atti Accad. pontif. Nuovi Lincei (1866), 177–182.

Table 1

$\varepsilon_D=(t+u\sqrt{D})/2$

t	D	u		t	D	u	
1	5	1		31	965=5·193	1	
2	2	2		32	257	2	
3	13	1		33	1093	1	
4	5	2	ε_5^3[6]	34	290=2·5·29	2	
5	29	1		35	1229	1	
6	10=2·5	2		36	13	10	ε_{13}^3
7	53	1		37	1373	1	
8	17	2		38	362=2·181	2	
9	85=5·17	1		39	61	5	
10	26=2·13	2		40	401	2	
11	5	5	ε_5^5	41	1685=5·337	1	
12	37	2		42	442=2·13·17	2	
13	173	1		43	1853=17·109	1	
14	2	10	ε_2^3	44	485=5·97	2	
15	229	1		45	2029	1	
16	65=5·13	2		46	530=2·5·53	2	
17	293	1		47	2213	1	
18	82=2·41	2		48	577	2	
19	365=5·73	1		49	2405=5·13·37	1	
20	101	2		50	626=2·313	2	
21	445=5·89	1		51	2605=5·521	1	
22	122=2·61	2		52	677	2	
23	533=13·41	1		53	2813=29·97	1	
24	145=5·29	2		54	730=2·5·73	2	
25	629=17·37	1		55	3029=13·233	1	
26	170=2·5·17	2		56	785=5. 157	2	
27	733	1		57	3253	1	
28	197	2		58	842=2·421	2	
29	5	13	ε_5^7	59	3485=5·17·41	1	
30	226=2·113	2		60	901=17·53	2	

6) $\varepsilon_5^3=(4+2\sqrt{5})/2$ means the third power of the fundamental unit ε_5 of the real quadratic field $Q(\sqrt{5})$, and etc.

Table 2

The case of $p=5$.

$t=25m-11$, $D=25m^2-22m+5$ (left) $\qquad$ $t=25m+11$, $D=25m^2+22m+5$ (right)

t	D	u	m	t	D	u
			0	11	5 ; ε_5^5	5
14	2 ; ε_2^3	10	1	36	13 ; ε_{13}^3	10
39	61	5	2	61	149	5
64	41	10	3	86	74=2·37	10
89	317	5	4	111	493=17·29	5
114	130=2·5·13	10	5	136	185=5·37	10
139	773	5	6	161	1037=17·61	5
164	269	10	7	186	346=2·173	10
189	1429	5	8	211	1781=13·137	5
214	458=2·229	10	9	236	1129	10
239	2285=5·457	5	10	261	109 ;	25
264	697=17·41	10	11	286	818=2·409	10
289	3341=13·257	5	12	311	3869=53·73	5
314	986=2·17·29	10	13	336	1129	10
339	4597	5	14	361	5213=13·401	5
364	53 ;	50	15	386	1490=2·5·149	10
389	6053	5	16	411	6757=29·233	5
414	1714=2·857	10	17	436	1901	10
439	7709=13·593	5	18	461	8501	5
464	2153	10	19	486	2362=2·1181	10
489	9565=5·1913	5	20	511	10445=5·2089	5
514	2642=2·1321	10	21	536	17 ;	130
539	11621	5	22	561	12589	5
564	3181	10	23	586	3434=2·17·101	10
589	13877	5	24	611	14933=109·137	5
614	3770=2·5·13·29	10	25	636	4045=5·809	10
639	16337	5	26	661	17477	5
664	4409	10	27	686	4706=2·13·181	10
689	18989=17·1117	5	28	711	20221=73·277	5
714	5098=2·2549	10	29	736	5417	10

Table 3

The case of $p=13$.

$t=169m-29$, $D=169m^2-58m+5$ (left); $t=169m+29$, $D=169m^2+58m+5$ (right)

t	D	u	m	t	D	u
			0	29	5; ε_5^7	13
140	29 ; ε_{29}^3	26	1	198	$58=2\cdot29$	26
309	$565=5\cdot113$	13	2	367	797	13
478	2 ;	338	3	536	17 ;	130
647	2477	13	4	705	$2941=17\cdot173$	13
816	$985=5\cdot197$	26	5	874	$1130=2\cdot5\cdot113$	26
985	5741	13	6	1043	$6437=41\cdot157$	13
1154	$1970=2\cdot5\cdot197$	26	7	1212	$2173=41\cdot53$	26
1323	10357	13	8	1381	$11285=5\cdot37\cdot61$	13
1492	$3293=37\cdot89$	26	9	1550	$3554=2\cdot1777$	26
1661	653 ;	65	10	1719	$17485=5\cdot13\cdot269$	13
1830	$4954=2\cdot2477$	26	11	1888	5273	26
1999	$23645=5\cdot4729$	13	12	2057	25037	13
2168	$6953=17\cdot409$	26	13	2226	$7330=2\cdot5\cdot733$	26

Mathematical Institute
Nagoya University

The author wishes to express his hearty thanks to Professor H. Hasse who kindly pointed out that it had been forgotten to add in Lemma 4 the condition $0 < a < p^2$, which establishes uniqueness. (27, August 1968)