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

On units of real quadratic number fields

By Ryozo MORIKAWA

(Received June 6, 1977)

1. In this paper we try to construct fundamental units of real quadratic number fields of certain type, and apply those results to the theory of diophantine equations.

We take an odd positive integer b and a square free odd positive integer D_1, and decompose the number

$$D_1b^2+2=r^2D_2\,, \tag{1}$$

where D_2 is square free and r is a positive integer. Then D_2 satisfies the congruence relation $D_2\equiv -D_1 (\mathrm{mod}\ 4)$, and r is an odd positive integer. Put $D_0=D_1D_2$, and $4D_0=D$. Then D_0 is square free and $D_0\equiv 3\ (\mathrm{mod}\ 4)$.

Here we define a number η by

$$\eta=(2(D_1b^2+1)+brD^{1/2})/2\,. \tag{2}$$

Then η is a unit of the real quadratic number field $\boldsymbol{Q}(D^{1/2})$. We put $\eta=[D_1, b\,;+]$. If we take the minus sign in (1) (i.e. $D_1b^2-2=r^2D_2$), and proceed in a similar way, we obtain the unit $(2(D_1b^2-1)+brD^{1/2})/2$ of $\boldsymbol{Q}(D^{1/2})$. We denote this unit by $[D_1, b\,; -]$.

Now we fix an odd positive integer s and a square free odd positive integer D_1, and let the number q run through all odd prime numbers.

Our main result is as follows.

THEOREM 1. *If $q>s$, then the unit $[D_1, sq\,; +]$ (or $[D_1, sq\,; -]$) is either a fundamental unit or a power of a unit $[D_1, s'\,; +]$ ($[D_1, s'\,; -]$ respectively), where s' is a divisor of s.*

In the following, we first prove Theorem 1, and study the excluding cases of Theorem 1 more precisely (Theorem 2). In §5 we give two applications of those results. In brief, they are

(A) *The diophantine equation $D_1s^2X^2-D_2Y^2=2$ (or -2) has, excluding special cases, at most one solution with a prime number X (Theorem 3).*

(B) *Let d be the square free factor of $q^2\pm 2$ where q is a prime number. If $d\neq 3$, then $d>\log q$ (Theorem 4).*

We use the following notation:

$\boldsymbol{Q}$, the field of rational numbers;

$\boldsymbol{N}$, the set of positive rational integers;

(a, b) the greatest common divisor of a and b;

$a|b$ means that a divides b.

2. For the proof of Theorem 1, we define some notations and prove some lemmas.

Let D_0 be a square free positive integer, and $D_0 \equiv 3 \pmod 4$. Put $4D_0 = D$. Take some unit η (>1) of $\boldsymbol{Q}(D^{1/2})$, and write $\eta = (T+UD^{1/2})/2$. Then $T \in \boldsymbol{N}$ and $U \in \boldsymbol{N}$. We call T the *t-part* of the unit η and U the *u-part* of η. Since the norm of a unit of $\boldsymbol{Q}(D^{1/2})$ is always 1, we have

$$T^2 - U^2 D = 4, \quad \text{or} \quad U^2 D = (T-2)(T+2).$$

We assume that U is an odd number, then $T \equiv 0 \pmod 4$, and we have $T-2 = 2v^2 D_1$ and $T+2 = 2w^2 D_2$, where D_1, D_2 are square free and $v, w \in \boldsymbol{N}$. In these situations, we say that the unit η is of the type $\{D_1, D_2\}$.

LEMMA 1. *Take a unit η (>1) of $\boldsymbol{Q}(D^{1/2})$, whose norm$=1$, and let T_n and U_n be the t-part and the u-part of η^n respectively $(n \in \boldsymbol{N})$. (We write $T_1 = T$, $U_1 = U$.)*

(i) *If $n = 2m-1$, then $T_n - 2 = (T-2)((U_m + U_{m-1})/U)^2$, and*

$$T_n + 2 = (T+2)((U_m - U_{m-1})/U)^2. \tag{3}$$

Here $(U_m + U_{m-1})/U$ and $(U_m - U_{m-1})/U$ are positive integers.

(ii) *If $n = 2m$, then $T_n - 2 = (T^2-4)(U_m/U)^2$ and $T_n + 2 = T_m^2$.* (4)

PROOF. Let $n = 2m-1$. Since $\mathrm{Norm}(\eta^m) = 1$, $T_n = \eta^n + \eta^{-n}$ and $U_m/U = (\eta^m - \eta^{-m})/(\eta - \eta^{-1}) \in \boldsymbol{N}$. Hence $(T_n - 2)/(T-2) = (\eta^m - \eta^{-m+1})^2/(\eta - 1)^2$ and $(T_n + 2)/(T-2) = (\eta^m + \eta^{-m+1})^2/(\eta+1)^2$. Thus we have (3). In case $n = 2m$, $(T_n - 2)/(T^2-4) = (\eta^m - \eta^{-m})^2/(\eta - \eta^{-1})^2 = (U_m/U)^2$ and $T_n + 2 = (\eta^m + \eta^{-m})^2$.

LEMMA 2. *Let $D = 4D_0$, where D_0 is a square free positive integer and $D_0 \equiv 3 \pmod 4$. Assume that the u-part of a unit η (>1) of $\boldsymbol{Q}(D^{1/2})$ is an odd integer. Then*

(i) *η can not be the square of another unit of $\boldsymbol{Q}(D^{1/2})$.*

(ii) *If $\eta = \varepsilon^{2m+1}$ $(m \in \boldsymbol{N})$, where ε is a unit of $\boldsymbol{Q}(D^{1/2})$, then the u-part of ε is also an odd integer.*

(iii) *If η is a unit of type $\{D_1, D_2\}$, then the type of ε is also $\{D_1, D_2\}$.*

PROOF. Let $\varepsilon = (t+uD^{1/2})/2$ be a unit whose norm$=1$, and write $\varepsilon^n = (t_n + u_n D^{1/2})/2$. Then u_n satisfies the following recurrent relations (cf. [**1**]).

$$u_n = uP_n,\ P_1 = 1,\ P_2 = t,\ P_n = tP_{n-1} - P_{n-2} \qquad (n \geqq 3). \tag{5}$$

Since $D \equiv 0 \pmod 4$, we have $t \equiv 0 \pmod 2$. Hence $P_n \equiv P_{n-2} \pmod 2$. This proves (i) and (ii). The assertion (iii) follows from Lemma 1, (i).

LEMMA 3. *Let the numbers* b, D_1, D_2, r, D_0, D *be as in* § 1. *If the unit* $\eta=[D_1, b; +]$ (*or* $[D_1, b; -]$) *is a power of another unit* ε *of* $Q(D^{1/2})$, *then* $\eta=\varepsilon^{2m+1}$ *with* $m\in N$, *and* ε *is expressible as* $\varepsilon=[D_1, b'; +]$ ($[D_1, b'; -]$ *respectively*), *where* $b'\in N$ *and* $b'|b$.

PROOF. The t-part of $[D_1, b; +]$ is $2(D_1b^2+1)$ and the u-part is br. η is of type $\{D_1, D_2\}$. Since br is an odd number, η is not the square of another unit of $Q(D^{1/2})$ (Lemma 2, (i)). Let $\eta=\varepsilon^{2m+1}$, then ε is of type $\{D_1, D_2\}$. Hence if we write $\varepsilon=(t+uD^{1/2})/2$, then u is odd and $t-2=2v^2D_1$, $t+2=2w^2D_2$ with $v, w\in N$. By Lemma 1, (i), we obtain $v|b$. $D_1v^2+2=w^2D_2$ means $\varepsilon=[D_1, v; +]$. The same reasoning works in case we take the minus sign.

3. Now we prove Theorem 1. Let $D_1(sq)^2+2=r^2D_2$ and $\eta=[D_1, sq; +]$. If η is not fundamental, then by Lemma 3, $\eta=\varepsilon^{2m+1}$ with $\varepsilon=[D_1, v; +]$ where $v|sq$. We write $\varepsilon=(t+uD^{1/2})/2$, and $\varepsilon^n=(t_n+u_nD^{1/2})/2$, then $t-2=2v^2D_1$, $t+2=2w^2D_2$ with $v, w\in N$. Now $sqr=u_{2m+1}\geqq u_3=u(t^2-1)=u(u^2D+3)>vw(v^2w^2D)>D_1^2v^5$. On the other hand, since $s<q$, we have $sqr<D_1(sq)^2<D_1q^4$. Hence $v<q$. This means $v|s$. The same reasoning works with respect to $[D_1, sq; -]$.

COROLLARY 1. *If* q *is an odd prime number, then the unit* $[1, q; -]$ *is a fundamental unit, and the unit* $[1, q; +]$ *is either fundamental or a power of* $2+(3)^{1/2}$.

RROOF. $[1, 1; +]=2+(3)^{1/2}$, and $[1, 1; -]=(-1)^{1/2}$.

COROLLARY 2. *Let* D *be the discriminant of the real quadratic number field which contains the unit* $[D_1, sq; +]$ (*or* $[D_1, sq; -]$). *If* $D>4(D_1s^2+2)D_1$ *and* $q>s$, *then the unit* $[D_1, sq; +]$ ($[D_1, sq; -]$ *respectively*) *is fundamental.*

PROOF. Among the units $[D_1, s'; +]$ with $s'|s$, the discriminant D has the maximum value in case $s=s'$ and D_1s^2+2 is square free. In that case $D=4D_1D_2=4(D_1s^2+2)D_1$.

Now we give some numerical examples.

(A) $[1, 8807; +]=77563250+6578829(139)^{1/2}$, $[19, 67; +]=85292+5427(247)^{1/2}$ are the fundamental units of $Q((556)^{1/2})$, $Q((988)^{1/2})$ respectively. (8807 is a prime number.)

(B) $[1, 71; +]$ is the 7-th power of $[1, 1; +]$, $[1, 3\cdot 239; -]$ is the 5-th power of $[1, 3; -]$, $[5, 3\cdot 673553; -]$ is the 7-th power of $[5, 3; -]$. (239 and 673553 are prime numbers.)

4. We shall study more precisely the case when the unit $[D_1, sq; +]$ is not fundamental. Namely we have

THEOREM 2. *Let* s *and* D_1 *be as in Theorem* 1. *Assume that a real quadratic number field* K *contains two units* $\eta_1=[D_1, sq_1; +]$ *and* $\eta_2=[D_1, sq_2; +]$, *where* q_1 *and* q_2 *are different odd prime numbers. Then* K *contains also the unit* $\eta_0=[D_1, s; +]$, *and* η_1 *and* η_2 *are powers of* η_0. *A similar proposition holds if we take the minus sign respectively.*

REMARK. If we take $\eta=[1, 39\cdot 293; -]$ and $\varepsilon=[1, 3; -]$, then $\eta=\varepsilon^7$. Theorem 2 means that no unit $[1, 39q; -]$ with odd prime number $q\neq 293$ is a power of ε.

We first prove two lemmas.

LEMMA 4. *Let s, D_1 be as above, and $\eta=[D_1, s; +]$. Then $\eta^{2m-1}=[D_1, sr_m; +]$, where r_m satisfies the following recurrent relations ($m\in\boldsymbol{N}$).*

$$\begin{aligned} &r_1=1, \quad r_2=2D_1s^2+3, \\ &r_{m+2}=2(D_1s^2+1)r_{m+1}-r_m, \quad (m\geqq 1). \end{aligned} \tag{6}$$

If we take the minus sign, the relation satisfied is

$$\begin{aligned} &r_1=1, \quad r_2=2D_1s^2-3, \\ &r_{m+2}=2(D_1s^2-1)r_{m+1}-r_m, \quad (m\geqq 1). \end{aligned} \tag{7}$$

PROOF. Let $D_1s^2+2=D_2r^2$ where D_2 is square free, and denote $\eta=(T+UD^{1/2})/2$ and $\eta^n=(T_n+U_nD^{1/2})/2$ ($n\in\boldsymbol{N}$). Then $T=2D_1s^2+2$ and $U=sr$. By Lemma 1, if we put $r_m=(U_m+U_{m-1})/U$, then $D_1(sr_m)^2+2=D_2(r(U_m-U_{m-1})/U)^2$ and $\eta^{2m-1}=[D_1, sr_m; +]$. Since the numbers U_m satisfy (5), we have (6). A similar reasoning works for (7).

DEFINITION. We call the sequence defined in Lemma 4 the sequence attached to $[D_1, s; +]$ (or $[D_1, s; -]$ respectively).

LEMMA 5. *Let $\{r_n\}$ ($n\in\boldsymbol{N}$) be the linear recurrent sequence which satisfies*

$$\begin{aligned} &r_1=1, \quad r_2=a+1\ (or\ a-1), \\ &r_{m+2}=ar_{m+1}-r_m, \quad (m\geqq 1) \quad (a\in\boldsymbol{N},\ a\geqq 4). \end{aligned} \tag{8}$$

Then

(i) $r_m \mid r_{(2m-1)k+m}$ *for* $k\in\boldsymbol{N}$ *and* $m\in\boldsymbol{N}$.

(ii) *If $2n-1$ is a composite number, then r_n is also a composite number.*

(iii) *For $t\in\boldsymbol{N}$, we define $m=\mathrm{Min}\,\{n\in\boldsymbol{N};\ t\mid r_n\}$. Then $t\mid r_n$ if and only if $n=(2m-1)(k-1)+m$ with some $k\in\boldsymbol{N}$.*

(iv) *If $n=(p+1)/2$ where p is a prime number, then $(r_n, r_m)=1$ for $1\leqq m<n$.*

PROOF. We note the following three facts.

(A) The relation considered is reflective, i.e, $r_m=ar_{m+1}-r_{m+2}$, so we can extend the sequence r_n for a negative integer n. Then $r_m=-r_{-m+1}$ (or r_{-m+1} respectively) for $m\in\boldsymbol{N}$.

(B) If we consider (8) modulo h with a fixed integer h, then the reduced sequence is also reflective.

(C) If a reflective sequence have a term $0\,(=r_d)$, then $-r_{d-f}=r_{d+f}$ for all $f\in\boldsymbol{N}$.

The assertions (i) and (iii) follow easily from these facts. If we put $n=(2m-1)k+m$, then $2n-1=(2m-1)(2k+1)$. Since $r_m<r_n$ for $m<n$, we obtain

(ii). (iv) follows from (iii).

PROOF OF THEOREM 2. Let $\eta_1=[D_1, sq_1; +]$ and $\eta_2=[D_1, sq_2; +]$, where q_1 and q_2 are different two prime numbers. Assume that two units η_1 and η_2 are contained in a real quadratic number field $\boldsymbol{K}$. Then by Lemma 3, the fundamental unit $\varepsilon(>1)$ of $\boldsymbol{K}$ is of the form $[D_1, s'; +]$ where $s'|s$, and $\eta_1=\varepsilon^{2m_1-1}$, $\eta_2=\varepsilon^{2m_2-1}$ with $m_1, m_2\in\boldsymbol{N}$. Put $s''=(s/s')$. By Lemma 4, $r_{m_1}=s''q_1$, and $r_{m_2}=s''q_2$ where $\{r_m\}$ is the linear recurrent sequence attached to $[D_1, s'; +]$. Let $m_0=\mathrm{Min}\,\{m\in\boldsymbol{N};\ s''|r_m\}$, then by Lemma 5 (i), (iii), we obtain $s''=r_{m_0}$. That means $\varepsilon^{2m_0-1}=[D_1, s; +]$, and again by Lemma 5 (iii), η_1 and η_2 are powers of $[D_1, s; +]$. The same reasoning works in case we take the minus sign.

Now it is natural to ask how many units of the form $[D_1, sq; +]$ with prime number q appear in the sequence of powers of $[D_1, s; +]$. This problem is equivalent to count prime numbers which appear in the sequence attached to $[D_1, s; +]$. It seems plausible that there exist infinitely many primes in that sequence. But it is difficult to prove the conjecture.

5. We give two applications of the above results.

(A) If we take a diophantine equation with infinitely many integer solutions, the question arises whether there exist also infinitely many solutions in prime numbers. It is difficult in general to answer the question. As a minor example we have

THEOREM 3. *Let D_1, D_2 be square free odd positive integers, and s be an odd positive integer. Then the diophantine equation*

$$D_1s^2X^2-D_2Y^2=2\,, \qquad (or\ D_1s^2X^2-D_2Y^2=-2)\,, \tag{9}$$

has at most one solution with prime number X, and $Y\in\boldsymbol{N}$, excluding the case that the number $(D_1s^2-2)/D_2((D_1s^2+2)/D_2$ respectively) is the square of an integer.

PROOF. It is obvious that $X=2$ is not a solution. From a solution $X=q$, $Y=r$, we can construct a unit $[D_1, sq; -]$. Hence the assertion is an easy corollary of Theorem 2.

(B) There is a thema to construct a real quadratic number field which has a large fundamental unit in comparison with the discriminant of the field (cf. e.g. [2]). If we try to apply our result to this problem, it is necessary to find a prime number q such as the number $q^2\pm2$, or in general $D_1(sq)^2\pm2$ has a large square factor. In numerical table we find such numbers, for example;

$$q=8807\,, \qquad (8807)^2+2=139(747)^2\,,$$

$$q=1601\,, \qquad (5\cdot1601)^2+2=163(627)^2\,.$$

And the class number of the corresponding real quadratic number field is 1.

It is doubtful whether we can get in the same way an infinite sequence of real quadratic number fields with class number 1.

On the other hand we obtain an inequality with respect to the square factor of that type of number $D_1(sq)^2\pm 2$. For simplicity, we treat only the number $q^2\pm 2$.

THEOREM 4. *Let q run through prime numbers, and decompose $q^2\pm 2=r^2d$, where d is square free. If $d\neq 3$, we have the inequality $d>\log q$.*

PROOF. Let $\varepsilon_D(>1)$ be the fundamental unit of $\boldsymbol{Q}(D^{1/2})$, where D is the discriminant of the field. Assume that $4|D$. It is known that $(1/2)\log D<\log\varepsilon_D<(D^{1/2})((1/2)\log D+1)$ (cf. [3], [4]). Put $D=4d$. Then by Corollary 1 of Theorem 1, $(2(q^2\pm 1)+qrD^{1/2})/2$ is the fundamental unit (>1) of $\boldsymbol{Q}(D^{1/2})$, excluding the case $d=3$. Hence $\varepsilon_D>q^2$. Thus we have the inequality $\log q<(d^{1/2})((1/2)\log d+2)$. If $d\geqq 11$, we have $(d^{1/2})>((1/2)\log d+2)$. If $d=7$, then $q=3$. Hence we have $\log q<d$.

REMARK 1. The fundamental unit (>1) of a real quadratic number field is unique. Hence if we let q run through all prime numbers, the square free factor d of $q^2\pm 2$ appears only once except $d=3$.

REMARK 2. Theorem 4 seems to suggest the fact that a number near to the square of a prime number can not have a very large square factor. But in studying the numbers $q^2\pm 3$ or $q^2\pm 5$, we are led to the contrary opinion. These problems are also equivalent to count prime numbers which appear in some linear recurrent sequences of second order.

References

[1] R. Morikawa, On units of real quadratic fields, J. Number Theory, 4 (1972), 503-507.

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

[3] L.K. Hua, On the least solution of Pell's equation, Bull. Amer. Math. Soc., 48 (1942), 731-735.

[4] M. Newman, Bounds for class numbers, Proc. Sympo. pure Math., 8 (1965), 70-77.

Ryozo MORIKAWA
Department of Mathematics
Nagasaki University
1-14, Bunkyo, Nagasaki.
852 Japan