İstanbul Üniv. Fen Fak. Mat. Der. 49 (1990), 13-20

SOME CRITERIONS FOR THE CLASS NUMBER OF A REAL QUADRATIC FIELD OF R-D TYPE TO BE ONE

M. H. DEVELİ - F. ÇALLIALP

In this study, using the properties of the indefinite form, we obtain some criterions for the class number of the real quadratic number fields to be one.

1. INTRODUCTION

Some mathematicians have obtained some criterions in R-D type of real quadratic number field for class number which is to be one ([5], [6], [7]).

Our purpose in this study, is to obtain general criterions by the help of quadratic forms for the class number one, and then to get the list of the fields with the class number one applying these conditions to the all of R-D types except of extended ones.

Under the extended Riemann Hypothesis, it has been shown the contidion of $d < 2000$ has been satisfied for the fields which are R-D types of class number one, except at most one [6]. For this reason we have studied the values of $d < 2000$.

Now, let us summarise the relations between quadratic forms and ideals of quadratic fields.

Let $\{1, w\}$ be the integral base of the field $\mathbf{Q}(\sqrt{d})$, where

$$w = \begin{cases} (1+\sqrt{d})/2 \ ; \ if \ d \equiv 1 \pmod 4 \\ \sqrt{d} \qquad\quad ; \ if \ d \equiv 2, 3 \pmod 4. \end{cases}$$

Continued fractional expansion of w is

$$w = < a_0 , \overline{a_1 , a_2 , \ldots , Tr\,(a_0 - w)} > .$$

Let us think about the quadratic form of

$$\phi_0 = x^2 - Tr\,(a_0 - w)\,xy + N\,(a_0 - w)\,y^2 .$$

ϕ_0, of which the discriminant is equal to the discriminant of the field, is reduced indefinite form, ([3], p. 54). Let ϕ_t be a form which is obtained by

applying integral transformation $\tau : \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ to ϕ_0. ϕ_1 is called "right neighboring form to ϕ_0". In this manner we obtain a chain $\phi_0, \phi_1, \phi_2, \ldots$ of equivalent, reduced forms (in strict sense). The number of the forms in this chain is finite ([4], p. 103). Let us call this chain "principal forms chain corresponding to the field".

Let us represent this chain as

$$\phi_i = ((-1)^i A_i, B_i, (-1)^{i+1} A_{i+1}). \tag{1-1}$$

There are following relations between the coefficients of (1-1) ([7], p. 108):

$$A_0 = 1, B_0 = Tr(a_0 - w), A_1 = -N(a_0 - w), A_{i+1} = (B_i + \sqrt{D})/2w_{i+1},$$
$$B_{i+1} = -B_i 2a_{i+1} A_{i+1}. \tag{1-2}$$

(D is the discriminant of the field and w_i is a convergent of w)

The set of first coefficients of principal chain is $A_d = \{A_0, A_1, \ldots, A_{k-1}\}$ (k is the period of the continued fraction expansion of w).

Let us take an integral ideal $M = (\alpha_1, \alpha_2)$ of $\mathbf{Q}(\sqrt{d})$, where $\{\alpha_1, \alpha_2\}$ is ordered basis of M.

The quadratic form $\phi(x, y) = \dfrac{(\alpha_1 x + \alpha_2 y)(\alpha_1' x + \alpha_2' y)}{N(M)}$ (1-3)

is called "form corresponding to M" and it is denoted by $\phi_M \to M$. ϕ_M has integral coefficients and it is primitive. Furthermore, the discriminant of ϕ_M is equal to the discriminant of the field. Conversely, each primitive indefinite or positive definite integral form which has the same discriminant can be obtained from integral ideal of quadratic field by (1-3) ([2], p. 200-201). Hence, equivalent classes of ideals are one to one correspondance to the equivalent classes of forms (in strict sense).

Proposition 1.1. $E_i = \left(A_i, \dfrac{1}{2}(B_i\ Tr(w)) - w\right)_{\mathbf{Z}}$ moduls are principal integral ideals in quadratic field $\mathbf{Q}(\sqrt{d})$. Moreover, $N(E_i) = A_i$ ([7], p. 119).

Proposition 1.2. Let $I = (a, b - w)$ $(a, b \in \mathbf{Z})$ be an integral ideal of real field $\mathbf{Q}(\sqrt{d})$. Moreover, let $a \mid N(b - w)$ and $2a < \sqrt{d}$. Thus, if I is principal ideal, then $a \in A_d$ ([2], p. 121).

2. GENERAL CRITERIONS

Let us think, $I = (a, b - w)$ $(a, b \in \mathbf{Z})$ integral ideal of real field $\mathbf{Q}(\sqrt{d})$.

$$\phi_I = ax^2 + Tr(b-w)xy + \frac{N(b-w)}{a}y^2 \qquad (2-1)$$

is the corresponding form to I, by (1—3).

Definition 2.1. I is called "reduced ideal" if ϕ_I is a reduced form.

Proposition 2.1. Let $I=(a, b-w)$ be an integral ideal of real quadratic field $\mathbf{Q}(\sqrt{d})$ such that $N(I)=a<\sqrt{D}/2$ and b >0. Thus, we can choose b uniquely as a class of modulo a such that I is reduced.

Proof. The conditions of which ϕ_I is reduced are $0<b<w$ and $0<\sqrt{D}-Tr(b-w)<2a<\sqrt{D}\,Tr(b-w)$ ([4], p. 100).

Moreover, considering that $a<\sqrt{D}/2$

$$\begin{cases} 0<(\sqrt{d}+1)/2-a<b\,; & \text{if } d\equiv 1 \pmod 4 \\ 0<\sqrt{d}-a<b\,; & \text{if } d\equiv 2,3 \pmod 4 \end{cases}$$

or

$$D<w-a<b<w$$

is found.

Proposition 2.2. Let $I=(a, b-w)$ be reduced integral ideal of real field $\mathbf{Q}(\sqrt{d})$. Moreover, let $N(I)=a<\sqrt{D}/2$.

(i) I is principal ideal if and only if ϕ_I belongs to principal chain.

(ii) If $\phi_I=\phi_i$, then $N(I)=A_i$.

(iii) Let I and I' are the only two ideals whose norms are equal to $N(I)$ (I' is conjugate of I). Thus, I is principal ideal if and only if $N(I)\in A_d$.

Proof.

(i) $\Leftarrow$: If $\phi_I=\phi_i$; assuming $a=A_i$, $Tr(b-w)=B_i$ and $b=\frac{1}{2}(B_i+Tr(w))$ then $I=E_i$ is found.

$\Rightarrow$: If I is principal ideal, at least one of $I\approx E_i$ or $I\approx\sqrt{D}E_i$ is true (in strict sense) ([2], p. 197). Let $I\approx E_i$. From (2—1), $\phi_i\to E_i$ is found if i is even. Let $I\approx\sqrt{D}E_i$. In the same way, $\phi_I\to E_i$ is found if i is odd. Thus, $\phi_I\approx\phi_i$ is found from both cases. This indicates that ϕ_I belongs to principal chain.

(ii) If $\phi_I=\phi_i$, taking $a=A_i$, $Tr(b-w)=B_i$ and $N(b-w)/a=-A_{i+1}$ then $I=E_i$ and $N(I)=A_i$ is found.

(iii) $\Rightarrow$: Let I be reduced principal ideal. If $N(I)=a<\sqrt{D}/2$, then $N(I)\in A_d$ (Prop. 1.2.).

$\Leftarrow$: If I and I' are only two ideals such that $N(I) \in A_d$ then at least one of them has to be equal to E_1.

Theorem 2.1 (Criterion 1). Class number of real field $\mathbf{Q}(\sqrt{d})$ is to be one ($h=1$) if and only if every prime number p belongs to

$$T=\left\{p \;\middle|\; p \text{ prime}, p<\sqrt{D}/2, \left(\frac{D}{p}\right)\neq -1\right\}$$

and also belongs to A_d.

Proof. Let us think the prime ideal $P=(p, b-w)$ which contains p as $p\in T$. In this case, it is possible to choose b as the class of mod p such that p is reduced (Prop. 2.1).

$\Rightarrow$: If $h=1$, P is principal. Then, $N(P)=p\in A_d$ (Prop. 1.2).

$\Leftarrow$: Let one of p elements of T belongs to A_d. Thus reduced prime ideal P over (p) is principal ideal (Prop. 2.2. (iii)). Hence, every prime ideal such as P is principal ideal such that $N(P)\in A_d$.

On the other hand, in each ideal class of $\mathbf{Q}(\sqrt{d})$, there is an integral ideal I such that $N(I)<\sqrt{D}/2$ ([2], p. 135). Since ideal I can be written as a product of such prime ideals P, I is principal ideal, too. Thus, it is seen that class group consists of principal ideal class. In short, $h=1$.

Theorem **2.2 (Criterion 2).** Let us think the polynomial for the real field $\mathbf{Q}(\sqrt{d})$

$$f(x)=-N(x-w)=\begin{cases}-x^2+x+(d-1)/4 & ; \text{if } d\equiv 1 \pmod 4\\ d-x^2 & ; \text{if } d\equiv 2,3 \pmod 4.\end{cases}$$

The class number of the real quadratic field $\mathbf{Q}(\sqrt{d})$ is to be one if and only if for all integers k such that $1\leq k<\sqrt{D}/2$, $f(k)$ must be a prime or every prime divisor of $f(k)$ which is less than $\sqrt{D}/2$ belongs to A_d.

Proof. 1°) Let $d\equiv 1 \pmod 4$ (case $D=d$).

If $1\leq k<\sqrt{D}/2$, $1<f(k)\leq (D-1)/4$ is found. Hence, if $f(k)$ is not prime, it has a prime divisor which is smaller than $\sqrt{D}/2$.

$\Rightarrow$: Let p be a prime divisor of $f(k)$. If $2<p<\sqrt{D}/2$, $f(k)=[d-(2k-1)^2]/4$ and $D=d\equiv(2k-1) \pmod p$ are found. If $p=2$, $D=d\equiv 1 \pmod 8$ is found. Hence, it is seen that in both cases (p) is non-inert in field ([2], p. 142-144). Thus, for prime ideals P over (p), $N(P)$ belongs to A_d.

If $f(k)$ is prime and $f(k) < \sqrt{D}/2$, same result is obtained $p = f(k)$.

$\Leftarrow$: Let prime $p < \sqrt{D}/2$ and let p be non-inert in field (Prop. 1.2). Prime ideal P over (p) can be written $P = (p, k_p - w)$ with k_p satisfying $1 \leq k_p < p$. $(N(P) = p)$. If $p \in A_d$, then $p = A_i$. For $E_i = A_i$,

$$\frac{1}{2}(B_i + Tr(w)) - w = (A_i, b_i - w)$$

and P ideals, $p = A_i \mid N(b_i - w)$ and $p \mid N(k_p - w)$. The result of $p \mid (b_i - k_p)$ or $p \mid (b_i + k_p - Tr(w))$ is obtained from these conditions. If $p \mid (b_i - k_p)$, $k_p = b_i - np$ (for $\exists\, n \in Z$). Hence, $P = (p, k_p - w) = (p, b_i - np - w) = (p, b_i - w) = (A_i, b_i - w) = E_i$ is found. If $p \mid (b_i + k_p - Tr(w))$, $P = E'$ is found by the same way. The result of $h = 1$ is obtained by the help of Criterion 1.

2°) Let $d \equiv 2, 3 \pmod 4$ (case $D = 4d$).

If $1 \leq k < \sqrt{D}/2$, $1 < f(k) \leq d$ is found. Furthermore, for odd primes p such that $p \mid f(k)$ and $p < \sqrt{D}/2$, $d \equiv k^2 \pmod p$ and for $p = 2$, $2 \mid D$ are found. Thus for prime divisors of $f(k)$ which are smaller than $\sqrt{D}/2$, $\left(\frac{D}{p}\right) \neq -1$ is understood and the result is found by the same way.

3. THE APPLICATION OF CRITERIAS TO THE R-D TYPES

In this section, R-D types will be classified in as appropriate way except extended ones. Criterions which are applied for every R-D type that we herein shall give will be only the expression of application theorems and numerical results that are obtained. The proof of almost all theorems is made by the same manner. We herein shall prove the last theorem only since it needs a different proof manner.

Note : When the theorems are organized, particular conditions that d verifies in case $h = 1$, were determined carefully. Moreover, in every theorem being shown $(i) \Leftrightarrow (ii)$, the determination of field by the help of only prime factors of $f(x)$ is easier.

Theorem 3.1. Let $d = 4m^2 + 1$ prime such that m odd prime. Class number of $\mathbf{Q}(\sqrt{d})$ is to be one if and only if one of the following equivalent conditions is satisfied:

(i) $f(k)$ is prime for all integer numbers k satisfing $2 \leq k \leq m - 1$.

(ii) $\left(\frac{d}{p}\right) = -1$, for all prime numbers p satisfing $2 \leq p \leq m - 1$.

The fields which are found : $d = 37, 101, 197, 677$.

Theorem 3.2. Let $d = n^2 + 4$ prime such that $n > 5$ and $(d-1)/4$ prime. Class number of $\mathbf{Q}(\sqrt{d})$ is to be one if and only if one of the following equivalent conditions is satisfied:

(i) $f(k)$ is prime for all integer numbers satisfying $2 \leq k \leq (n-1)/2$.

(ii) $\left(\frac{d}{p}\right) = -1$, for all prime numbers satisfying $2 \leq p \leq (n-1)/2$.

The fields which are found : $d = 29, 53, 173, 293$.

Theorem 3.3. Let $d = n^2 - 4 > 21$ such that $n \pm 2 \equiv 3 \pmod 4$ prime and $(d-1)/4$ prime.

Class number is to be one if and only if one of the following equivalent conditions is satisfied:

(i) $f(k)$ is prime for all integer numbers $2 \leq k \leq (n-1)/2$.

(ii) $\left(\frac{d}{p}\right) = -1$, for all prime numbers satisfying $2 \leq p \leq (n-1)/2$.

The fields which are found : $d = 21, 77, 437$.

Theorem 3.4. Let $d = n^2 \pm 4m$ $(1 < m \mid n, n$ is odd) such that $m \equiv \frac{d}{m} \equiv 3 \pmod 4$, $d \equiv 5 \pmod 8$ and $(d-1)/4$ odd primes. Moreover, let $(n-m-1)$ be a prime in case of $d = n^2 - 4m$.

Class number is to be one if and only if one of the following equivalent conditions is satisfied:

(i) $f(k)$ or $f(k)/2$ is prime for all integer numbers $2 \leq k \leq \sqrt{d-1}/2$.

(ii) $\left(\frac{d}{p}\right) = -1$, for all primes p satisfying $2 \leq p \leq \sqrt{d-1}/2$ and $p \neq m$.

The fields which are found : $d = 213, 237, 453, 717, 1077, 1253$.

Theorem 3.5. Let $d = n - r \equiv 5 \pmod 8$ such that $2 < n$ is even, $0 < r \equiv 3 \pmod 4$, $r \mid n\ (r < n)$, $r \equiv \frac{d}{r} \equiv 3 \pmod 4$ is odd prime, $(2n-r-1)/4$ is odd prime and less than $\sqrt{D}/2$, $r \equiv 7 \pmod 8$ in case of $n \equiv 2 \pmod 4$, $r \equiv 3 \pmod 8$ in case of $n \equiv 0 \pmod 4$, $\frac{d-1}{4}$ is odd prime.

The class number is to be one if and only if one of the following equivalent conditions is satisfied:

(i) $f(k)$ is prime or prime factors of $f(k)$ which are less than $\sqrt{d}/2$ can be equal to only r or $(2n-r-1)/4$ for all k satisfying $2 \leq k \leq \sqrt{d-1}/2$.

(ii) $\left(\frac{d}{p}\right) = -1$, for all primes p satisfying $2 \leq p \leq \sqrt{d-1}/2$ and $p \neq r(2n-r-1)/4$.

The fields which are found : $d = 141,\ 573,\ 1293,\ 1757$.

Theorem 3.6. Let $d = n^2 \pm 2$ if d is odd, then d and $(d-1)/2$ are primes if d is even, then $d/2$ and $d-1$ are primes.

The class number is to be one if and only if one of the following equivalent conditions is satisfied.

(i) $f(k)$ or $f(k)/2$ (for $\sqrt{d} < f(k)/2$) is prime for all integer numbers satisfying $2 \leq k \leq \sqrt{d-1}$.

(ii) $\left(\frac{D}{p}\right) = -1$, for all primes p satisfying $3 \leq p \leq \sqrt{d-1}$.

The fields which are found : $d = 6, 7, 11, 14, 23, 38, 47, 62, 83, 167, 227, 398$.

Theorem 3.7. Let $d = n^2 - 1 \equiv 1 \pmod 8$ such that $2 < n$ is even, $r \mid n$ and $r \equiv 3 \pmod 4$.

The class number is to be one if and only if $d = 33$.

Proof. $\Leftarrow$: If $d = 33$, $d = 6^2 - 3 \equiv 1 \pmod 8$. In addition, $h = 1$.

$\Rightarrow$: For given field, $A_d = \{1, r, (2n-r-1)/4\}$ is obtained ([3], p. 77). Moreover, if $d \equiv 1 \pmod 8$, $f(k) = -k^2 + (d-1)/4$ is even (for every integer k). If $h = 1$, $2 \in A_d$ (Criterion 2). Since $r \neq 2$, r is equal to $(2n-1)/4$ forced. Hence, $2n - r = 9$ is found. If $r \mid n$, $2r \leq n$ and $3r < 9$ are obtained. Moreover, $r \equiv 3 \pmod 4$. Thus, $r = 3$ in other words the result of $n = 6$ or $d = 33$ is obtained.

Note : Of the extended R-D types $(d = n^2 - r,\ r \mid 4n)$ the fields of which class number is one are $d = 141,\ 573,\ 1293,\ 1757$. Furthermore, of the $d = n^2 + 1$ (n odd), $d = 4m^2 - 1$ and $d = 4m^2 + 1$ types, particular three fields of which class number is one, $d = 2,\ 3,\ 17$ respectively. It was not studied to obtain these fields by the help of criterions.

REFERENCES

[1] AZUHATA, T. : *On the fundamental units and the class numbers of real quadratic fields*, Nagoya Math. J., 95 (1984), 125-135.

[2] CHON, H. : **Advanced Number Theory,** Dover Publications, Inc., New York, 1962.

[3] DEVELİ, M.H. : *Some criterias for the class number to be one in* R-D *types real quadratic number fields* (Doctoral thesis, Samsun, 1990).

[4] DICKSON, L.E. : **Introduction to the theory of numbers,** Dover Pupl. Inc., New York, 1957.

[5] LOUBOUTIN, S. : *Continued fractions and real quadratic fields*, J. of Number Theory, 30 (1988), 167-176.

[6] MOLLIN, R.A. and WILLIAMS, H.C. : *Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type* (*with one possible exception*) (To appear, in proc. of the first conference of the Canadian Number Theory Association at Banff, Canada, 1988).

[7] SASAKI, R. : *Generalized ono invariant and Rabinovitch's Theorem for real quadratic fields* (Nagoya Math. J., 109 (1988), 117-124.

M. H. DEVELİ
ONDOKUZ MAYIS ÜNİVERSİTESİ
AMASYA EĞİTİM YÜKSEKOKULU
AMASYA-TURKEY

F. ÇALLIALP
ONDOKUZ MAYIS ÜNİVERSİTESİ
FEN-EDEBİYAT FAKÜLTESİ
SAMSUN-TURKEY