78. A Note on the Class-number of Real Quadratic Fields with Prime Discriminants

By Hideo YOKOI
College of General Education, Nagoya University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1991)

Introduction. In recent papers [6], [7], [8], we defined some new integer-valued p-invariants for any rational prime p congruent to 1 mod 4 and studied relationships among them. In particular, we defined in [6] the new p-invariant n_p by

$$|t_p/u_p^2-n_p|<1/2$$

through the fundamental unit

$$\varepsilon_p=(t_p+u_p\sqrt{p})/2 \quad (>1)$$

of real quadratic field $\boldsymbol{Q}(\sqrt{p})$ with prime discriminant, which turned out to be very useful as far as $n_p\neq 0$ (i.e. $2t_p>u_p^2$).

In this paper, we shall introduce some more new p-invariants q_p, r_p, r_p^*, a_p, b_p and provide lower bounds for the class-number h_p of $\boldsymbol{Q}(\sqrt{p})$ (Theorems 1, 2). Moreover, we shall show that if $\boldsymbol{Q}(\sqrt{p})$ is of R-D type and $h_p=1$, 3 or 5, then n_p has certain simple multiplicative structures (Theorem 3).

§ **1.** We first prove the following theorem which is fundamental throughout this paper, providing a lower bound for the class-number h_p of real quadratic field $\boldsymbol{Q}(\sqrt{p})$ with prime discriminant.

Theorem 1. *For any prime p congruent to* 1 mod 4, *we denote by q_p the least prime number which splits completely in $\boldsymbol{Q}(\sqrt{p})$, i.e. $(p/q_p)=1$, where (/) means Legendre's symbol.*

Then if $n_p\neq 0$, $h_p\geqq \log n_p/\log q_p$ holds.

Proof. In the case $q_p\neq 2$, we proved this already in [6]. In the case $q_p=2$, we can prove the following lemma in a similar way as in Lemma 2 in [6]:

Lemma. *For any square-free positive integer D congruent to* 1 mod 8, *we denote by e the order of prime factors of* 2 *in the ideal class group of $\boldsymbol{Q}(\sqrt{D})$.*

Then, the diophantine equation $x^2-Dy^2=\pm 4\cdot 2^e$ has at least one non-trivial solution, while for any integer e' such that $1\leqq e'<e$ the diophantine equation $x^2-Dy^2=\pm 4\cdot 2^{e'}$ has no non-trivial integral solution.

By using this lemma together with Lemma 1 in [6], in a similar way as in the proof of Theorem in [6] we can prove

$$q_p=2 \quad \text{and} \quad h_p\geqq \log n_p/\log 2$$

for any prime $p\equiv 1 \bmod 8$.

We next provide a lower bound r_p for the class-number of $Q(\sqrt{p})$

which is also a new p-invariant.

Theorem 2. *If $n_p \neq 0$, then we denote by r_p the sum of multiplicities of all prime factors in n_p which completely split in $\boldsymbol{Q}(\sqrt{p})$.*

Then $h_p \geqq r_p$ holds.

Proof. Let $q_1, q_2, \cdots, q_r$ be all distinct prime factors of n_p which completely split in $Q(\sqrt{p})$, and put

$$n_p = n_0 \cdot \Pi_i q_i^{e_i}, \quad (n_0, q_i) = 1.$$

Then, $r_p = \Sigma_i e_i$ is clearly p-invariant.

On the other hand, since $q_p \leqq q_i$, we have easily

$$\begin{aligned} \log n_p / \log q_p &= (\log n_0 / \log q_p) + \Sigma_i (e_i \log q_i / \log q_p) \\ &\geqq \Sigma_i e_i \\ &= r_p. \end{aligned}$$

Hence from Theorem 1 we obtain

$$h_p \geqq \log n_p / \log q_p \geqq r_p$$

provided $n_p \neq 0$.

Remark. Especially, if there is at least one prime factor of n_p which does not split in $Q(\sqrt{p})$, or which splits in $\boldsymbol{Q}(\sqrt{p})$ but is greater than q_p, then $h_p > r_p$ holds.

If we put

$$t_p = u_p^2 n_p \pm a_p \quad (a_p \geqq 0),$$

then we get

$$0 \leqq a_p < u_p^2/2 \quad \text{and} \quad a_p^2 + 4 \equiv 0 \pmod{u_p^2}.$$

Hence if we put moreover $a_p^2 + 4 = b_p u_p^2$, then both a_p and b_p are also p-invariants, and we can describe p as follows:

$$p = u_p^2 n_p^2 \pm 2 a_p n_p + b_p.$$

Here, $a_p = 0$ if and only if $u_p = 1$ or 2 (cf. [6]).

On the other hand, for a square-free positive integer D, we put

$$D = m^2 + r, \quad -m < r \leqq m.$$

Then if $4m \equiv 0 \pmod{r}$ holds, $\boldsymbol{Q}(\sqrt{D})$ is called of Richaud-Degert type (or simply R-D type). A real quadratic field $\boldsymbol{Q}(\sqrt{p})$ with prime discriminant is of R-D type if and only if $a_p = 0$ (cf. [1], [3], [4]).

Under these circumstances, we have first the following application of Theorem 2:

Corollary 2.1. *If $\boldsymbol{Q}(\sqrt{p})$ is of R-D type and $n_p \neq 0$, then $h_p \geqq r_p^*$, where r_p^* is the sum of multiplicities of all prime factors in n_p.*

Proof. For real quadratic fields $\boldsymbol{Q}(\sqrt{p})$ of R-D type,

$$p = n_p^2 + 4 \quad (u_p = 1,\ b_p = 4)$$

or

$$p = 4 n_p^2 + 1 \quad (u_p = 2,\ b_p = 1)$$

(cf. [1], [3], [4]). Hence, in both cases we know $(p/q) = 1$ for any prime factor q of n_p, i.e. q splits always in $Q(\sqrt{p})$. Therefore, Corollary 2.1 follows immediately from Theorem 2.

For real quadratic fields $\boldsymbol{Q}(\sqrt{p})$ which are not of R-D type, we have similarly next two applications:

Corollary 2.2. *If prime p congruent to* 1 mod 4 *is described in one of the following three forms*:

(1) $p=25n^2\pm 22n+5$,

(2) $p=169n^2\pm 58n+5$,

(3) $p=289n^2\pm 152n+20$,

then $h_p\geqq r_p^*$,

where r_p^* is the sum of multiplicities of all prime factors q of n_p such that $q\equiv\pm 1$ (mod 10).

Proof. In these cases, $u_p=5, 13, 17$, $a_p=11, 29, 76$, $b_p=5, 5, 20$ respectively. Hence, in any case we know for any prime factor q of n $(p/q)=(b_p/q)=(5/q)$. Therefore, the prime q splits completely in $\boldsymbol{Q}(\sqrt{p})$ if and only if $q\equiv\pm 1$ (mod 10).

Corollary 2.3. *If prime p congruent to* 1 mod 4 *is described in the following form*: $p=841n^2\pm 164n+8$,

then $h_p\geqq r_p^*$,

where r_p^* is the sum of multiplicities of all prime factors q of n such that $q\equiv\pm 1$ (mod 8).

Proof. In this case, $u_p=29$, $a_p=82$ and $b_p=8$. Since $(p/q)=(b_p/q)=(2/q)$, the prime q splits completely in $\boldsymbol{Q}(\sqrt{p})$ if and only if $q\equiv\pm 1$ (mod 8).

§ 2. For real quadratic fields $\boldsymbol{Q}(\sqrt{p})$ of R-D type, we already obtained a necessary and sufficient condition for the class-number h_p to be one in terms of p-invariants n_p and q_p (cf. [5]). Similarly, by considering the structure of n_p from such point of view as r_p^* we provide a necessary condition for the class-number to be three or five respectively in terms of p-invariants n_p and q_p as follows:

Theorem 3. *Let $\boldsymbol{Q}(\sqrt{p})$ be a real quadratic field of R-D type with prime discriminant. For the class-number h_p of $\boldsymbol{Q}(\sqrt{p})$,*

(1) *$h_p=1$ if and only if $n_p=q_p$.*

(2) *If $h_p=3$, then n_p is one of the following three forms*:

1) $n_p=q$ (*prime* $>q_p$),

2) $n_p=q_1q_2$ (*primes* $\geqq q_p$),

3) $n_p=q_p^3$.

(3) *If $h_p=5$, then n_p is one of the following five forms*:

1) $n_p=q$ (*prime* $>q_p$),

2) $n_p=q_1q_2$ (*primes* $\geqq q_p$),

3) $n_p=q_1^2q_2$ (*primes* $\geqq q_p$),

4) $n_p=q^4$ (*prime* $\geqq q_p$),

5) $n_p=q_p^5$.

Proof. The assertion (1) was already obtained in [5] as above mentioned. In the case $h_p=3$, we get $r_p^*\leqq 3$ from Corollary 2.1. Hence, if we assume $r_p^*=3$ and n_p has at least two distinct prime factors q_1, q_2, then the value of the divisor function is $\tau(n_p)\geqq 6$.

On the other hand, we have $h_p\geqq\tau(n_p)-1$ from Mollin's result (cf. [2]), which implies a contradiction with $h_p=3$. Therefore, from the Remark of

Theorem 2, we get $n_p=q_p^3$, and hence assertion (2) also.

Assertion (3) is obtained similarly by using Mollin's results.

Examples. (1) $p=1{,}373$: $h_p=3$, $u_p=1$, $n_p=37$, $q_p=3$, $r_p^*=1$.

(2) $p=229$: $h_p=3$, $u_p=1$, $n_p=3\cdot 5$, $q_p=3$, $r_p^*=2$.

(3) $p=257$: $h_p=3$, $u_p=2$, $n_p=2^3$, $q_p=2$, $r_p^*=3$.

(4) $p=10{,}613$: $h_p=5$, $u_p=1$, $n_p=103$, $q_p=7$, $r_p^*=1$.

(5) $p=401$: $h_p=5$, $u_p=2$, $n_p=2\cdot 5$, $q_p=2$, $r_p^*=2$.

Finally, we provide a table of all primes $p=n_p^2+4$ for $n_p\leqq 135$ and $p=4n_p^2+1$ for $n_p\leqq 75$ together with p-invariants h_p, q_p, n_p and r_p^*. From

$p=n^2+4$	h_p	q_p	n_p	r_p^*
5	1		1	1
13	1	3	3	1
29	1	5	5	1
53	1	7	7	1
173	1	13	13	1
229	3	3	$15=3\cdot 5$	2
293	1	17	17	1
733	3	3	$27=3^3$	3
1,093	5	3	$33=3\cdot 11$	2
1,229	3	5	$35=5\cdot 7$	2
1,373	3	7	37	1
2,029	7	3	$45=3^2\cdot 5$	3
2,213	3	7	47	1
3,253	5	3	$57=3\cdot 19$	2
4,229	7	5	$65=5\cdot 13$	2
4,493	3	11	67	1
5,333	3	11	73	1
7,229	5	5	$85=5\cdot 17$	2
7,573	9	3	$87=3\cdot 29$	2
9,029	7	5	$95=5\cdot 19$	2
9,413	3	13	97	1
10,613	5	7	103	1
13,229	5	5	$115=5\cdot 23$	2
13,693	15	3	$117=3^2\cdot 13$	3
15,629	9	5	$125=5^3$	3
18,229	19	3	$135=3^3\cdot 5$	4

$p=4n^2+1$	h_p	q_p	n_p^*	r_p^*
17	1	2	2	1
37	1	3	3	1
101	1	5	5	1
197	1	7	7	1
257	3	2	$8=2^3$	3
401	5	2	$10=2\cdot 5$	2
577	7	2	$12=2^2\cdot 3$	3
677	1	13	13	1
1,297	11	2	$18=2\cdot 3^2$	3
1,601	7	2	$20=2^2\cdot 5$	3
2,917	3	3	$27=3^3$	3
3,137	9	2	$28=2^2\cdot 7$	3
4,357	5	3	$33=3\cdot 11$	2
5,477	3	13	37	1
7,057	21	2	$42=2\cdot 3\cdot 7$	3
8,101	13	3	$45=3^2\cdot 5$	3
8,837	3	11	47	1
12,101	5	5	$55=5\cdot 11$	2
13,457	13	2	$58=2\cdot 29$	2
14,401	43	2	$60=2^2\cdot 3\cdot 5$	4
15,377	13	2	$62=2\cdot 31$	2
15,877	13	3	$63=3^2\cdot 7$	3
16,901	7	5	$65=5\cdot 13$	2
17,957	7		67	1
21,317	5	7	73	1
22,501	11	3	$75=3\cdot 5^2$	3

these tables, we may conjecture the following, which shows that it would be very interesting to investigate q_p: if n_p is not prime, then $n_p \equiv 0 \pmod{q_p}$.

References

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

[2] R. A. Mollin: On the divisor function and class numbers of real quadratic fields. I. Proc. Japan Acad., **66**A, 109–111 (1990).

[3] C. Richaud: Sur la résolution des équation $x^2 - Ay^2 = \pm 1$. Atti Accad. Pontif. Nuovi Lincei, pp. 177–182 (1866).

[4] H. Yokoi: On real quadratic fields containing units with norm -1. Nagoya Math. J., **33**, 139–152 (1968).

[5] ——: Class-number one problem for certain kind of real quadratic fields. Proc. Int. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields, June 24–28, 1986, Katata, Japan, pp. 125–137.

[6] ——: Some relations among new invariants of prime number p congruent to 1 mod 4. Advanced Studies in pure Math., **13**, 493–501 (1988).

[7] ——: The fundamental unit and class number one problem of real quadratic fields with prime discriminant. Nagoya Math. J., **120**, 51–59 (1990).

[8] ——: The fundamental unit and bounds for class numbers of real quadratic fields. ibid., **124**, 181–197 (1991).