

**THE FUNDAMENTAL UNIT AND CLASS NUMBER ONE
PROBLEM OF REAL QUADRATIC FIELDS WITH
PRIME DISCRIMINANT**

HIDEO YOKOI

§ 0. Introduction

Class number one problem for imaginary quadratic fields was solved in 1966 by A. Baker and H.M. Stark independently. However, the problem for real quadratic fields is still unsolved. It seems to us that one of the most essential difficulties of the problem for real quadratic fields comes from deep connection of the class number with the fundamental unit.

In this paper, we shall first in § 1 concern ourselves with real quadratic fields of prime discriminant $F = \mathbf{Q}(\sqrt{p})$ (prime $p \equiv 1 \pmod{4}$), and give a sufficient condition for an unit $\varepsilon = (t + u\sqrt{p})/2$ corresponding to a positive integral solution $(x, y) = (t, u)$ of the diophantine equation $x^2 - py^2 = -4$ to be the fundamental unit (Theorem 1).

In § 2, for the p -invariant n_p defined by using the fundamental unit of F

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

in the case $n_p \neq 0$, i.e. $t_p/u_p^2 > 1/2$, the class number one problem is considered, and it will be proved that if $n_p \neq 0$ and $h_p = 1$ then $p < 4.1 \times 10^6$ holds with one possible exception of p and that under the assumption of the generalized Riemann hypothesis this is true without any exception (Theorem 2).

Finally, we shall show that for real quadratic fields $\mathbf{Q}(\sqrt{d})$ with discriminant d not necessarily prime the same result is proved (Theorem 3). Moreover, we shall give three kinds of tables, one of which consists of 30 primes p congruent to 1 mod 4 satisfying $h_p = 1$ and $n_p \geq 1$.

§ 1. Fundamental unit

In real quadratic fields $\mathbf{Q}(\sqrt{p})$ with prime discriminant, p is prime

Received November 17, 1989.

congruent to 1 mod 4. Therefore, the fundamental unit of $\mathbb{Q}(\sqrt{p})$

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

has the norm $N\varepsilon_p = -1$, and hence (t_p, u_p) is the smallest positive integral solution of $x^2 - py^2 = -4$.

Conversely, we can prove the following theorem:

THEOREM 1. *For any fixed prime p ($\neq 5$) congruent to 1 mod 4, if a non-trivial positive integral solution $(x, y) = (t, u)$ ($t > 0, u > 0$) of diophantine equation $x^2 - py^2 = -4$ satisfies any one of the following:*

- (i) $t/u^2 > 1/2$,
- (ii) $t < 2p$,
- (iii) $u^2 < 4p$,

then $\varepsilon = (t + u\sqrt{p})/2$ is the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$.

To prove this theorem, we need several lemmas. First we prove the following:

LEMMA 1. *For any prime p congruent to 1 mod 4, let (t, u) be a positive integral solution of diophantine equation $x^2 - py^2 = -4$.*

Then the following are equivalent:

- (i) $t/u^2 > 1/2$,
- (ii) $t < 2p$,
- (iii) $u^2 < 4p$.

Proof. In the case $u = 1$, we have $p = t^2 + 4$, and hence $t = \sqrt{p-4} < 2p$, $u^2 = 1 < 4p$, $t/u^2 \geq 1$.

In the case $u = 2$, we have $p = t^2/4 + 1$, and hence $t = 2\sqrt{p-1} < 2p$, $u^2 = 4 < 4p$, $t/u^2 \geq 1$.

Now we suppose $u > 2$. Then $t^2 - pu^2 = -4$ implies $t \neq 2p$, $0 < 8/u^2 < 1$ and $p > p - 4/u^2 = t^2/u^2$. Therefore,

$$t/u^2 < 1/2 \quad \text{if and only if} \quad p - 4/u^2 < t/2,$$

which is equivalent to $t > 2p$.

Next, $p \geq 5$ implies $0 < 4/p < 1$. Therefore,

$$t > 2p \quad \text{if and only if} \quad pu^2 - 4 > 4p^2,$$

which is equivalent to $u^2 > 4p$.

LEMMA 2. For any prime p congruent to $1 \pmod 4$, let $(x, y) = (t_0, u_0)$ be any positive integral solution of diophantine equation $x^2 - py^2 = -4$. If we put

$$\left(\frac{t_0 + u_0\sqrt{p}}{2}\right)^{2n+1} = \frac{t_n + u_n\sqrt{p}}{2} \quad (n = 1, 2, \dots),$$

then sequences of natural numbers $\{t_n\}$, $\{u_n\}$ are monotonically increasing in narrow sense.

Proof. If we put

$$\frac{t + u\sqrt{p}}{2} = \left(\frac{t_0 + u_0\sqrt{p}}{2}\right)^2,$$

then we get easily

$$t = (t_0^2 + pu_0^2)/2 \geq 3,$$

and hence we have $t/2 > 1$.

On the other hand, from the definition, we have

$$\begin{aligned} \frac{t_{n+1} + u_{n+1}\sqrt{p}}{2} &= \frac{t_n + u_n\sqrt{p}}{2} \cdot \frac{t + u\sqrt{p}}{2} \\ &= \{(tt_n + puu_n) + (tu_n + ut_n)\sqrt{p}\}/4. \end{aligned}$$

Therefore, we get

$$t_{n+1} = (t/2)t_n + (p/2)uu_n > t_n,$$

and

$$u_{n+1} = (t/2)u_n + (u/2)t_n > u_n$$

for any $n = 1, 2, 3, \dots$.

LEMMA 3. For any prime p congruent to $1 \pmod 4$, let

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

be the fundamental unit of real quadratic field $\mathbf{Q}(\sqrt{p})$. If we put

$$\varepsilon_p^3 = (\bar{t}_p + \bar{u}_p\sqrt{p})/2,$$

then

$$\bar{t}_p > 2p \quad \text{and} \quad \bar{u}_p^2 > 4p$$

hold except for $p = 5$.

Proof. Since

$$\begin{aligned} (\bar{t}_p + \bar{u}_p\sqrt{p})/2 &= \{(t_p + u_p\sqrt{p})/2\}^3 \\ &= [(t_p^3 + 3pt_pu_p^2) + (pu_p^3 + 3t_p^2u_p)\sqrt{p}]/4/2. \end{aligned}$$

we have

$$\bar{t}_p = t_p(t_p^2 + 3pu_p^2)/4$$

and

$$\bar{u}_p = u_p(pu_p^2 + 3t_p^2)/4.$$

Hence, $2p < \bar{t}_p$ holds if and only if

$$p(8 - 3t_pu_p^2) < t_p^3,$$

which follows from

$$8 - 3t_pu_p^2 < 0, \quad \text{i.e.} \quad u_p^2t_p \geq 3.$$

However, $u_p^2t_p \geq 3$ holds if and only if $u_p \neq 1$ or $t_p \neq 1, 2$, which is equivalent to $p \neq 5$.

On the other hand, since (\bar{t}_p, \bar{u}_p) is a positive integral solution of $x^2 - py^2 = -4$, by Lemma 1

$$\bar{t}_p > 2p \quad \text{if and only if} \quad \bar{u}_p^2 > 4p.$$

Proof of Theorem 1. First, we note that three conditions of our theorem are equivalent by Lemma 1.

Next, we suppose that $\varepsilon = (t + u\sqrt{p})/2$ is not equal to the fundamental unit $\varepsilon_p = (t_p + u_p\sqrt{p})/2 (>1)$ of $\mathbf{Q}(\sqrt{p})$, and put

$$\left(\frac{t_p + u_p\sqrt{p}}{2}\right)^{2n+1} = \frac{t_n + u_n\sqrt{p}}{2} \quad (n = 1, 2, \dots).$$

Then there is a uniquely determined positive integer m such that

$$t = t_m \quad \text{and} \quad u = u_m,$$

and by Lemma 2, we have

$$t_p < t_1 \leq t_m \quad \text{and} \quad u_p < u_1 \leq u_m.$$

On the other hand, by Lemma 3, we obtain

$$t_1 > 2p \quad \text{and} \quad u_1^2 > 4p,$$

which contradict with the assumption of our theorem.

§ 2. Class number

For any prime p congruent to 1 mod 4, denote by

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

the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$ with prime discriminant.

We now define p -invariant as a mapping from the set of all rational primes congruent to 1 mod 4 to the set of non-negative rational integers.

In our recent papers ([6], [7], [8]), we defined some new p -invariant, above all n_p , which is defined by the inequality

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

and obtained several interesting results regarding its property. Especially as a result closely related to class number one problem, we proved in [8] that in the case $n_p \neq 0$, there exists only a finite number of prime p congruent to 1 mod 4 with class number one.

In this section, we prove more precisely the following:

THEOREM 2. *If prime p congruent to 1 mod 4 satisfies*

$$p > 4.1 \times 10^6 \quad \text{and} \quad n_p \neq 0 \quad \text{i.e.} \quad \varepsilon_p < 2p,$$

then $h_p > 1$ holds with one possible exception of p .

Moreover, if we assume the generalized Riemann Hypothesis, this is true without any exception.

The proof of this theorem depends upon the following lemma:

LEMMA 4. *If prime p congruent to 1 mod 4 satisfies $n_p \neq 0$, then*

$$\varepsilon_p < 2p \quad \text{and} \quad h_p > \frac{0.3275}{m} \times \frac{p^{(m-2)/2m}}{\log 2p}$$

hold for any $p > e^m$, $m \geq 11.2$ with one possible exception of p .

Assuming the generalized Riemann Hypothesis, this is true without any exception.

Proof. The first part of this lemma follows from Dirichlet's class number formula by applying the Siegel-Tatuzawa theorem (cf. [1], [5]) and Lemma 1.

For the second part, Kim [3] shows that if we assume the generalized

Riemann Hypothesis, the Siegel-Tatuzawa theorem is true without any exception (cf. [4]).

Proof of Theorem. Put

$$f_m(x) = \frac{x^a}{\log 2x}, \quad a = a(m) = (m - 2)/2m \quad (> 0)$$

for any fixed $m \geq 11.2$. Then, since

$$f'_m(x) = \frac{(a \log 2x) - 1}{x^{1-a} (\log 2x)^2} > 0$$

for any $x \geq 6$, $f(x)$ is increasing on $[6, \infty)$.

Moreover, put

$$g_m(x) = \frac{0.3275}{m} \times f_m(x).$$

Then, for $m = 15$ (> 11.2) we have

$$g_{15}(4.1 \times 10^6) > 1, \quad \text{and} \quad e^m = e^{15} < 4.1 \times 10^6.$$

This establishes by Lemma 4 that $h_p > 1$ holds for all $p > 4.1 \times 10^6$ except possibly one p , and without any exception under the assumption of the generalized Riemann Hypothesis.

For any prime p satisfying $3533 < p < 4.1 \times 10^6$, we may confirm that $n_p \neq 0$ implies $h_p > 1$ by using Kida's **UBASIC 86**. We owe to Y. Tanigawa such better upper bound of p and this confirmation. Moreover, in primes p satisfying $5 \leq p \leq 3533$, we find exactly 30 primes p such that $n_p \neq 0$ and $h_p = 1$. Therefore, from Theorem 2 we obtain the following corollary, which is a generalization of Kim, Leu and Ono's result (cf. [2]):

COROLLARY. *There exist exactly 30 primes p congruent to 1 mod 4 satisfying $n_p \geq 1$ and $h_p = 1$ with one more possible exception of p .*

All such primes are listed in the following table I. Furthermore, Y. Tanigawa kindly informed me that by the same way the following general result is proved for discriminant d , not necessarily prime:

THEOREM 3. *There exist exactly 54 discriminants d of real quadratic fields $\mathbf{Q}(\sqrt{d})$ satisfying $\varepsilon_d < 2d$ and $h_d = 1$ with one more possible exception of d .*

All such discriminants except primes are listed in the table III.

Table I
 $(n_p \geq 1, h_p = 1)$

Table II
 $(t_p/u_p^2 > 1/2, h_p > 1)$

p	t_p	u_p	n_p	p	t_p	u_p	t_p/u_p^2	h_p
5	1	1	1	229	15	1	15	3
13	3	1	3	257	32	2	8	3
17	8	2	2	401	40	2	10	5
29	5	1	5	577	48	2	12	7
37	12	2	3	733	27	1	27	3
41	64	10	1	1009	1080	34	0.93	7
53	7	1	7	1093	33	1	33	5
61	39	5	2	1129	336	10	3.36	9
101	20	2	5	1229	35	1	35	3
149	61	5	2	1297	72	2	18	11
157	213	17	1	1373	37	1	37	3
173	13	1	13	1429	189	5	7.56	5
197	28	2	7	1601	80	2	20	7
269	164	10	2	1901	436	10	4.36	3
293	17	1	17	2029	45	1	45	7
317	89	5	4	2153	464	10	4.64	5
461	365	17	1	2213	47	1	47	3
509	925	41	1	2677	3777	73	0.70	3
557	236	10	2	2917	108	2	27	3
677	52	2	13	3137	112	2	28	9
773	139	5	6	3181	564	10	5.64	5
797	367	13	2	3221	3689	65	0.87	3
941	1135	37	1	3253	57	1	57	5
1013	923	29	1	4229	65	1	65	7
1493	2357	61	1	4357	132	2	33	5
1613	2972	74	1	4409	664	10	6.64	9
1877	1603	37	1	4493	67	1	67	3
2477	647	13	4	4597	339	5	13.5	3
2693	4411	85	1	4933	2388	34	2	3
3533	2437	41	1	5273	1888	26	3	7

p : prime congruent to 1 mod 4.

$\epsilon_p = (t_p + u_p\sqrt{p}) > 1$: fundamental unit of $\mathbb{Q}(\sqrt{p})$.

n_p : p -invariant defined by $|t_p/u_p^2 - n_p| < 1/2$.

h_p : class number of $\mathbb{Q}(\sqrt{p})$.

Table III

($d \neq p$, $t_d/u_d^2 > 1/2$ i.e. $n_d \geq 1$, $h_d = 1$)

d	t_d	u_d	t_d/u_d^2	n_d
21 = 3·7	5	1	5	5
33 = 3·11	46	8	0.71	1
69 = 3·23	25	3	2.77	3
77 = 7·11	9	1	9	9
93 = 3·31	29	3	3.20	3
133 = 7·19	173	15	0.76	1
141 = 3·47	190	16	0.74	1
213 = 3·71	73	5	2.92	3
237 = 3·79	77	5	3.08	3
341 = 11·31	277	15	1.23	1
413 = 7·59	61	3	6.77	7
437 = 19·23	21	1	21	21
453 = 3·151	149	7	3.04	3
573 = 3·191	766	32	0.74	1
717 = 3·239	241	9	2.97	3
917 = 7·131	1181	39	0.77	1
1077 = 3·359	361	11	2.98	3
1133 = 11·103	101	3	11.22	11
1253 = 7·179	177	5	7.08	7
1293 = 3·431	1726	48	0.74	1
1757 = 7·251	1006	24	1.74	2
2453 = 11·223	3566	72	0.68	1
3053 = 43·71	3481	63	0.87	1
3317 = 31·107	5241	91	0.63	1

d : discriminant of real quadratic $Q(\sqrt{d})$.

$\varepsilon_d = (t_d + u_d\sqrt{d})/2 > 1$: fundamental unit of $Q(\sqrt{d})$.

n_d : invariant defined by $|t_d/n_d^2 - n_d| < 1/2$.

h_d : class number of $Q(\sqrt{d})$.

REFERENCES

- [1] J. Hoffstein, On the Siegel-Tatuzawa theorem, *Acta Arith.*, **33** (1980), 167–174.
- [2] H. K. Kim, M.-G. Leu and T. Ono, On two conjectures on real quadratic fields, *Proc. Japan Acad.*, **63** (1987), 222–224.
- [3] H. K. Kim, A conjecture of S. Chowla and related topics in analytic number theory, thesis, Johns Hopkins University, 1988.
- [4] R. A. Mollin and H. C. Williams, A conjecture of S. Chowla via the generalized Riemann hypothesis, *Proc. A. M. S.*, **102** (1988), 794–796.
- [5] T. Tatuzawa, On a theorem of Siegel, *Japan. J. Math.*, **21** (1951), 163–178.
- [6] H. Yokoi, Some relations among new invariants of prime number p congruent to 1 mod 4, *Advances in pure Math.*, **13** (1988), 493–501.
- [7] ———, New invariants of real quadratic fields, *Proc. 1st Conf. Canadian Number Theory Assoc.*, April, 18–27, 1988, Banff, Canada, 635–639.
- [8] ———, Bounds for fundamental units and class numbers of real quadratic fields with prime discriminant, *Dept. of Math., Coll. Gen. Educ., Nagoya Univ., Prep. ser.*, 1989, No. 2.

*Department of Mathematics
College of General Education
Nagoya University
Chikusa-ku, Nagoya 464-01
Japan*