COLLOQUIUM MATHEMATICUM

VOL. LXIII 1992 FASC. 2

A COMPLETE GENERALIZATION OF YOKOI'S p-INVARIANTS

BY

R. A. MOLLIN (CALGARY, ALBERTA)
AND H. C. WILLIAMS (WINNIPEG, MANITOBA)

1. Introduction. In [14]–[18] Yokoi studied what he called p-invariants for certain real quadratic fields. It is the purpose of this paper to give a complete generalization of these results to *arbitrary* real quadratic fields. Moreover, the results herein allow us to generalize (and simplify the proofs of) other results of Yokoi [19]–[20], including two statements equivalent to the general Gauss conjecture concerning an infinitude of real quadratic fields of class number $h(d) = 1$ for $\mathbb{Q}(\sqrt{d})$.

We give bounds on the fundamental unit when our n_d (see §3) for $\mathbb{Q}(\sqrt{d})$ is non-zero; and we use it to show that in this case there are only finitely many such d with $h(d) = 1$. This allows us then to reformulate the Gauss conjecture. Moreover, we prove that when $n_d \neq 0$ then the Artin–Ankey–Chowla conjecture and the Mollin–Walsh conjecture hold. We also show how these results have applications for certain norm form equation solutions, and we provide examples. Furthermore, we show how certain conditional results of Yokoi which he showed to hold for all but finitely many values, in fact hold for *all* values. Finally, we actually list all $h(d) = 1$ (with one possible exception) when $n_d \neq 0$ (see §3). This completes the task begun by Yokoi [17]–[18].

2. Units. We begin with a motivation for the generalization (beyond a mere generalization of Yokoi's special prime case of p-invariants). In what follows $\varepsilon_d = (t_d + u_d\sqrt{d})/\sigma$ will be the fundamental unit of $\mathbb{Q}(\sqrt{d})$, where

$$\sigma = \begin{cases} 2 & \text{if } d \equiv 1 \pmod 4, \\ 1 & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

Throughout the paper, d will be a positive square-free integer.

THEOREM 2.1. (1) *If* $\varepsilon_d = (u^2 n - a + u\sqrt{d})/\sigma$ *then* $d = u^2n^2 - 2an + b$ *with* $a^2 - \sigma^2 N(\varepsilon_d) = bu^2$ *where* $a \geq 0$ *and* b *are unique.*

(2) *If* $d = u^2n^2 - 2an + b$ *is square-free with* $a^2 - \sigma^2 N(\varepsilon_d) = bu^2$ *then* $\varepsilon_1 = (u^2n - a + u\sqrt{d})/\sigma = \varepsilon_d^t$ *for some* $t \geq 1$.

Proof. (1) Since $t_d = u_d^2 n - a$ and $u_d = u$ we have $\sigma^2 N(\varepsilon_d) = t_d^2 - u_d^2 d = (u_d^2 n - a)^2 - u_d^2 d$; whence $d = u_d^2 n^2 - 2an + (a^2 - \sigma^2 N(\varepsilon_d))/u_d^2$; i.e., $d = u^2 n^2 - 2an + b$ where $u^2 b = a^2 - \sigma^2 N(\varepsilon_d)$. By definition $u = u_d$ is the smallest positive integer such that $u^2 d$ is of the form $l^2 - \sigma^2 N(\varepsilon_d)$. This makes a and b unique.

(2) $N(\varepsilon_1) = ((u^2 n - a)^2 - u^2 d)/\sigma^2 = N(\varepsilon_d)$. This makes ε_1 a unit. ■

The following generalizes [20, Theorem 2, pp. 144–145]. In what follows, an *ERD-type* (Extended Richaud–Degert type, see [2], [12] and [4]–[10]) is of the form $d = l^2 + r$ where $4l \equiv 0 \pmod{r}$.

Corollary 2.1. *Let $d = p^2 n^2 - 2an + b$ where $n \geq 0$, $p \equiv 3 \pmod 4$ is prime and $a^2 + 4 = bp^2$ with p being the smallest positive integer such that the latter occurs. Then $\mathbb{Q}(\sqrt{d})$ is not of ERD-type, $N(\varepsilon_d) = -1$ and $\varepsilon_d = ((p^2 n - a) + p\sqrt{d})/2$.*

Proof. From Theorem 2.1(2), $\varepsilon_1 = ((p^2 n - a) + p\sqrt{d})/2$ is either ε_d or a power of it. However, choosing p as the *smallest* value with $a^2 + 4 = bp^2$ forces $p = u_d$. Clearly $N(\varepsilon_1) = -1$. Moreover, a fundamental fact about ERD-types is that $N(\varepsilon_d) = -1$ forces $u_d = 1$ or 2. ■

In [20] Yokoi proved that the result held for all but finitely many d. What the above shows is that a proper choice of p forces that finitely many to be zero. In a similar fashion we could generalize [19, Theorem 1, p. 109].

Now we show that the converse of Theorem 2.1(1) fails without uniqueness.

Example 2.1. Let $d = 77 = 9^2 - 4 = u^2 n^2 - 2an + b$ where $a = 2$, $b = 0$, $n = 1$, $u = 9$. We have $N(\varepsilon_{77}) = 1$, $\varepsilon_{77} = (9 + \sqrt{77})/2$, and

$$\varepsilon_1 = (u^2 n - a + u\sqrt{d})/2 = (79 + 9\sqrt{77})/2 = \varepsilon_{77}^2 .$$

However, if we require that u is the *smallest* positive value such that $u^2 d = l^2 - 4$ then we get $u = 1$ with $77 = u^2 n^2 - 2an + b$ where $n = 9$, $a = 0$, $b = -4$ and $\varepsilon_1 = \varepsilon_{77} = (9 + \sqrt{77})/2$.

Remark 2.1. If we choose u to be the smallest positive value such that $u^2 b = a^2 - \sigma^2 N(\varepsilon_d)$ in Theorem 2.1(2) then $t = 1$. This was the essential problem with Yokoi's choice of p in [19, Theorem 1, p. 109] and [20, Theorem 2, p. 144]; i.e., that he did not choose the smallest such value thereby allowing for the result to fail for finitely many values.

This motivates the following.

3. Generalized Yokoi p-invariants. The following generalizes Yokoi's special case of p-invariants for primes $p \equiv 1 \pmod 4$ which he explored in [14]–[18]. We shall have occasion to generalize all of these results while at the same time simplifying the proofs. Set

$$B = (2t_d/\sigma - N(\varepsilon_d) - 1)/u_d^2\,.$$

The boundary B was explored in [4, Lemma 1.1, p. 40], [5, Lemma, p. 121] and [16, Lemma 1, p. 494] (and which we feel was the motivation for Yokoi's special case).

Let n_d be the *nearest integer* to B; i.e.,

$$n_d = \begin{cases} [B] & \text{if } B - [B] < 1/2, \\ [B] + 1 & \text{if } B - [B] > 1/2 \end{cases}$$

(where $[x]$ is the greatest integer less than or equal to x. Note that $B - [B]$ can never be $1/2$). Set

$$a_d = \begin{cases} t_d - u_d^2 n_d & \text{if } B - [B] < 1/2, \\ u_d^2 n_d - t_d & \text{if } B - [B] > 1/2, \end{cases}$$

$$b_d = (a_d^2 - \sigma^2 N(\varepsilon_d))/u_d^2\,.$$

An easy check shows that in the case where $p = d \equiv 1 \pmod 4$ is prime they reduce to Yokoi's concept of p-invariants. Moreover, our definition is more explicit and revealing, which will allow us to provide simplified proofs (over that of Yokoi) in our more general case.

First we generalize the main results of Yokoi in [14]. Moreover, Theorem 3.1(2) shows that Yokoi's claim that it holds for all but finitely many d is in fact true but with the finitely many being 0.

THEOREM 3.1. *Let d be positive square-free. Then*

(1) $\varepsilon_d = (u_d^2 n_d \pm a_d + u_d\sqrt{d})/\sigma$, *and*
(2) $d = u_d^2 n_d^2 \pm 2a_d + b_d$.

Proof. (1) Since $t_d = u_d^2 n_d \pm a_d$ the result is clear.

(2) Since $t_d^2 - u_d^2 d = N(\varepsilon_d)\sigma^2$ we have $u_d^2 d = t_d^2 - N(\varepsilon_d)\sigma^2 = (u_d^2 n_d \pm a_d)^2 - N(\varepsilon_d)\sigma^2$ so $d = u_d^2 n_d^2 \pm 2a_d + b_d$. Uniqueness of representation is clear. ∎

THEOREM 3.2. *Let $d > 0$ be square-free and let $u_d > 2$. Then the following are equivalent.*

(1) $n_d = 0$,
(2) $t_d > 4d/\sigma$,
(3) $u_d^2 > 16d/\sigma^2$.

Proof. From $t_d^2 - u_d^2 d = N(\varepsilon_d)\sigma^2$ we get $(2t_d/\sigma)^2 = 4N(\varepsilon_d) + (2/\sigma)^2 d u_d^2$ so

$$((2t_d/\sigma)^2 - (N(\varepsilon_d)+1)^2)/u_d^2 \le 4N(\varepsilon_d)/u_d^2 + (2/\sigma)^2 d$$

and

$$(2/\sigma)^2 d + (N(\varepsilon_d) - 1)/4 \le ((2t_d/\sigma)^2 - (N(\varepsilon_d)+1)^2)/u_d^2\,.$$

(1)⇔(2). $n_d = 0$ implies that $(2t_d/\sigma - N(\varepsilon_d) - 1)/u_d^2 < 1/2$. Thus

$$(2t_d/\sigma + N(\varepsilon_d) + 1)/2 > (2/\sigma)^2 d + (N(\varepsilon_d) - 1)/4\,;$$

i.e.,

$$t_d > (4/\sigma)d - (\sigma/4)(N(\varepsilon_d) + 3)\,.$$

However, a straightforward check shows that $4d/\sigma \geq t_d > 4d/\sigma - (\sigma/4)\times (N(\varepsilon_d) + 3)$ cannot occur so $4d/\sigma < t_d$.

Conversely, if $t_d > 4d/\sigma$ then

$$\begin{aligned} t_d + (N(\varepsilon_d) + 1)/4 &> (2t_d/\sigma)^2 d + (N(\varepsilon_d) + 1)/4 \\ &> (2/\sigma)^2 + 4N(\varepsilon_d)/u_d^2 \geq ((2t_d/\sigma)^2 - (N(\varepsilon_d) + 1)^2)/u_d^2 \end{aligned}$$

since $u_d > 2$. Hence

$$1 \geq ((t_d + (N(\varepsilon_d) + 1))/4)/((2t_d/\sigma) + N(\varepsilon_d) + 1) > (2t_d/\sigma - (N(\varepsilon_d) + 1))/u_d^2,$$

which implies $n_d = 0$.

(2)⇔(3). $t_d > 4d/\sigma$ and $N(\varepsilon_d)\sigma^2 = t_d^2 - u_d^2 d$ if and only if $u_d^2 > 16d/\sigma^2 - N(\varepsilon_d)\sigma^2/d$. Since $d > \sigma^2$ (unless $d = 2, 3$ for which the theorem trivially holds) we get $u_d^2 > 16d/\sigma^2$. ∎

We get as an immediate result

Corollary 3.1. *If $n_d \neq 0$ then $\varepsilon_d < 8d/\sigma^2$.*

We may now use the above to prove

Theorem 3.3. *If $n_d \neq 0$ then there are only finitely many d with $h(d) = 1$.*

Proof. By Corollary 3.1 we have $\log \varepsilon_d < \log(8d/\sigma^2)$; i.e., we have a bound for the regulator which allows us to invoke the result of Tatuzawa [13] in the same fashion as we did in [8]. A similar argument to that in [8] yields that only finitely many d have $h(d) = 1$. ∎

The above generalizes results of Yokoi [14] and [16]–[18]. The following generalizes Yokoi [14].

Theorem 3.4. *Let d_0 be a fixed positive square-free integer. Then there are only finitely many d with $u_d = u_{d_0}$ and $h(d) = 1$.*

Proof. If $n_d \neq 0$ we are done by Theorem 3.3. If $n_d = 0$ and $u_{d_0} > 2$ then by Theorem 3.2, $u_d^2 = u_{d_0}^2 > 16d/\sigma^2$ so clearly there are finitely many such d. (Here $h(d) = 1$ is not needed.) If $u_{d_0} \leq 2$ then $d = l^2 + r$ where $|r| \in \{1, 4\}$ by [2] and [12]. This case, and the general ERD case in fact, were handled in [8]. ∎

Let

(G_1) There exist infinitely many real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with $h(d) = 1$ (Gauss conjecture).

(G_2) There exist infinitely many d with $n_d = 0$ and $h(d) = 1$.

(G_3) For a given $n_0 \in \mathbb{N}_0$ there exists at least one real quadratic field with $h(d) = 1$ and $u_d \geq n_0$.

THEOREM 3.5. (G_1)$\Leftrightarrow$(G_2)$\Leftrightarrow$(G_3).

Proof. The equivalence of (G_1) and (G_2) follows from Corollary 3.1 and the equivalence of (G_1) and (G_3) follows from Theorems 3.3–3.4. ∎

In order to set the stage for the generalization of [14, Theorem 2, p. 637] we need the following:

DEFINITION. For a positive square-free integer d, the equation $x^2 - dy^2 = \pm 4t$, for t any positive integer, is said to have a *trivial solution* (u, v) in rational integers if $t = m^2$ and m divides both u and v. Any other rational integer solution is called *nontrivial*.

The following result is proved in [4]. B is as defined above.

LEMMA 3.1. *If there is a nontrivial solution to* $x^2 - dy^2 = N(\varepsilon_d)\sigma^2 t$ *then* $t \geq B$.

THEOREM 3.6. *Let* p_d *be the least prime which splits in* $\mathbb{Q}(\sqrt{d})$. *If* $n_d \neq 0$ *then* $h(d) \geq \log n_d / \log p_d$.

Proof. Clearly there is a nontrivial solution to $x^2 - dy^2 = N(\varepsilon_d)\sigma^2 p_d^{h(d)}$; so by Lemma 3.1, $p_d^{h(d)} \geq B$. Thus $h(d) \geq \log B / \log p_d \geq \log n_d / \log p_d$. ∎

The above generalizes [14, Theorem 2, p. 637]. Moreover, it shows that Yokoi's requirement that p_d be odd is unnecessary. Indeed, if $n_d \neq 0$ for $d \equiv 1 \pmod 8$ then we see that $n_d = 1$ or 2 since 2 splits in $\mathbb{Q}(\sqrt{d})$. On the other hand, if $a_d = 0$ then $n_d = t_d/u_d^2$ forcing $u_d = 1$ or 2; i.e., d is of *narrow Richaud–Degert* (R–D) type $d = l^2 + r$ where $|r| \in \{1, 4\}$. In fact, we have the following

THEOREM 3.7. *If* $n_d \geq \sqrt{d-1}/2$ *where* $d \equiv 1 \pmod 4$ *then* $h(d) = 1$ *if and only if* d *is of narrow R–D type.*

Proof. This is immediate from [5, Theorem, p. 121] and [10, Lemma 2.3, p. 148]. ∎

Remark 3.1. We found all (except possibly one value) $h(d) = 1$ for the more general ERD-types in [8]. We already know from Theorem 3.3 that when $n_d \neq 0$ there are only finitely many d with $h(d) = 1$. In the case $n_d \geq (\sqrt{d} - 1)/2$ we found the finitely many in [10], with one possible exception. Moreover, given the results in [7] and [9]–[10], this possible exceptional value would be a counterexample to the Riemann hypothesis.

Theorem 3.6 can be generalized if we know that $h(d)$ is odd.

THEOREM 3.8. *Let p_d be the least noninert prime in $\mathbb{Q}(\sqrt{d})$. If $n_d \neq 0$ and $h(d)$ is odd then $h(d) \geq \log n_d / \log p_d$.*

Proof. Since $h(d)$ is odd p_d may be ramified and we still have a nontrivial solution to $x^2 - dy^2 = N(\varepsilon_d)\sigma^2 p_d^{h(d)}$. ∎

COROLLARY 3.2. *If $d \not\equiv 5 \pmod 8$, $n_d \neq 0$ and $h(d)$ is odd then $n_d = 1$ or 2.*

Proof. 2 is noninert so the result follows. ∎

On the other hand, if $d \equiv 5 \pmod 8$ we have

THEOREM 3.9. *If $d = pq \equiv 5 \pmod 8$ where $p < q$ both primes with $p \equiv q \equiv 3 \pmod 4$ and $t_d > u_d^2 p + 1$ then $d = p^2 u_d^2 \pm 4p$ (an ERD-type).*

Proof. By [1, Corollary, p. 189] there is a nontrivial solution to $x^2 - dy^2 = \pm 4p$. If $x^2 - dy^2 = -4p$ then by [11, Theorem 108, p. 205], $0 < y \leq u_d\sqrt{4p}/\sqrt{2(t_p - 1)} < \sqrt{2}$; whence, $y = 1$ and $d = x^2 + 4p$. On the other hand, if $x^2 - dy^2 = 4p$ then by [11, Theorem 108a, p. 206], $0 < y \leq u_d\sqrt{4p}/\sqrt{2(t_d + 1)} < \sqrt{2}$, so again $y = 1$ and $d = x^2 - 4p$.

Moreover, we may invoke Lemma 3.1 to get $p \geq (t_d - 2)/u_d^2$ so $u_d^2 p + 1 \geq t_d - 1 > u_d^2 p$ whence $t_d = u_d^2 p + 2$ and so $\varepsilon_d = (u_d^2 p + 2 + u_d\sqrt{d})/2$. Thus $x = pu_d$ and $d = p^2 u_d^2 \pm 4p$. ∎

Remark 3.2. If $h(d) = 1$ in Theorem 3.9 then we note that we have found all such d (with one possible exception) in [8]. Moreover, it is well known (e.g. see Hasse [3]) that if $h(d)$ is odd and d is not prime with $d \equiv 1 \pmod 4$ then d must equal pq with $p \equiv q \equiv 3 \pmod 4$. We already know that since the hypothesis of Theorem 3.9 forces $n_d \neq 0$ there can only be finitely many d with $h(d) = 1$ from Theorem 3.3 (compare with Remark 3.1).

Now we exhibit a result which is related to Theorem 3.9 and generalizes [19, Proposition 1, p. 107] and [19, Lemma 3, p. 108]. Moreover, the following proof is more revealing as we shall illustrate.

PROPOSITION 3.1. *If $N(\varepsilon_d) = 1$, $u_d \equiv 0 \pmod n$ for some $n \geq 1$ and $g = \gcd(u_d^2, t_d \pm \sigma)$ then $t_d = n_d^2 mg \pm \sigma$ and $(u_d/n)^2 d = n^2 m^2 g^2 \pm 2\sigma mg$ where all proper divisors of m divide d.*

Proof. It is known that $\varepsilon_d = \gamma/\overline{\gamma}$ where $\gamma = (t_d + \sigma + u_d\sqrt{d})/\sigma$ (e.g. see [1, Theorem 2, p. 185]), when $N(\varepsilon_d) = 1$.

Moreover, $N((t_d \pm \sigma + u_d\sqrt{d})/\sigma) = 2 \pm 2t_d/\sigma$; whence, whenever a prime p satisfies $g \equiv 0 \pmod p$ then $2 \pm t_d/\sigma \equiv 0 \pmod{p^2}$. (Note that in the case $p = \sigma = 2$, we *cannot* have $t_d \equiv 0 \pmod 4$ and $u_d \equiv 2 \pmod 4$ since that would imply that $-1 \equiv (u_d/2)^2 \pmod 4$.) Hence, whenever p properly divides $t_d \pm \sigma$ then p does not divide u_d. Since $t^2 \equiv \sigma^2 \pmod p$ means $u_d^2 d \equiv 0 \pmod p$, this implies that $d \equiv 0 \pmod p$. Since n^2 must divide only one of $(t_d+\sigma)/g$ or $(t_d-\sigma)/g$ we get $t^2\pm\sigma = n^2mg$ where proper divisors of m divide d. Finally,

$$u_d^2 d = t_d^2 - \sigma^2 = n^2(n^2m^2g^2 \pm 2\sigma mg)\,. \ \blacksquare$$

In the proof of Proposition 3.1 we see the importance of $t_d\pm\sigma$ when $N(\varepsilon_d)=1$. We can use it to generalize [1, Theorem 7, p. 188] for example.

PROPOSITION 3.2. *If $d=p_1p_2p_3\equiv 1 \pmod 4$ and $N(\varepsilon_d)=1$ where the p_i's are distinct primes then $x^2-dy^2=\pm 4p_i$ for some $i\in\{1,2,3\}$.*

Proof. Let $\gamma=(t_d+2+u_d\sqrt{d})/2$, and set

$$g=\begin{cases}\gcd(t_d+2,u_d) & \text{if } 2\nmid u_d,\\ \gcd((t_d+2)/2,u_d/2) & \text{if } 2\mid u_d.\end{cases}$$

Thus $(\alpha)=((t_d+2+u_d\sqrt{d})/(2g))$ must have divisors which divide d; i.e., (α) must be an ideal containing only the ramified primes $\wp_i$ where $\wp_i\mid p_i$ in $\mathcal{O}_K$, the ring of integers of $K=\mathbb{Q}(\sqrt{d})$.

If $\alpha=(1)$ then α is a unit, whence $\varepsilon_d=\gamma/\overline{\gamma}=\alpha/\overline{\alpha}=\alpha^2/(\alpha\overline{\alpha})=\alpha^2$, contradicting that ε_d is fundamental. A similar argument dismisses $(\alpha)=\wp_1\wp_2\wp_3$. Hence (α) is one of $\wp_i\wp_j$ or $\wp_k$ where $i,j,k\in\{1,2,3\}$. If it is $\wp_1\wp_2$, say, then since $(\sqrt{d})=\wp_1\wp_2\wp_3$ we get $\wp_3\sim(1)$ where $\sim$ denotes equivalence in the class group. Thus $x^2-dy^2=\pm 4p_3$ has a solution. $\blacksquare$

The above result has a more general formulation and a simple proof based upon continued fractions. (However, we do not get the generator α out of it.)

First we need some notation. Let

$$w_d=\begin{cases}(1+\sqrt{d})/2 & \text{if } d\equiv 1 \pmod 4,\\ \sqrt{d} & \text{if } d\equiv 2,\,3 \pmod 4,\end{cases}$$

and let k be the period length of the continued fraction expansion of w_d denoted by $\langle a,\overline{a_1,\ldots,a_k}\rangle$. Then $a_0=a=[w_d]$. Also $a_i=[(P_i+\sqrt{d})/Q_i]$ for $i\ge 1$ where $(P_0,Q_0)=(1,\,2)$ if $d\equiv 1 \pmod 4$ and $(P_0,Q_0)=(0,1)$ if $d\equiv 2,3 \pmod 4$. Finally, $P_{i+1}=a_iQ_i-P_i$ for $i\ge 0$ and $Q_{i+1}Q_i=d-P_{i+1}^2$ for $i\ge 0$.

PROPOSITION 3.3. *Let $d\equiv 1 \pmod 4$ be a positive square-free integer with $N(\varepsilon_d)=1$. Then for some proper divisor $d'>1$ of d we have a solution of $x^2-dy^2=\pm 4d'$.*

Proof. Since $N(\varepsilon_d)=1$ it is well known (e.g. see [9]) that the period of w_d must be even. Thus $P_{k/2}=P_{k/2+1}$ so by the preamble to the proposition

$$d=P_{k/2+1}^2+Q_{k/2+1}Q_{k/2}=(a_{k/2}Q_{k/2}/2)^2+Q_{k/2+1}Q_{k/2}$$

so $(Q_{k/2}/2)\mid d$. Clearly $Q_{k/2}\ne 2$ and $Q_{k/2}/2\ne d$. The result now follows from the fact that the principal reduced ideals have norm $Q_i/2$ for some i (e.g. see [9]). $\blacksquare$

Table 3.1 ($h(d) = 1$ with $n_d \neq 0$)

d	$\log \varepsilon_d$	d	$\log \varepsilon_d$	d	$\log \varepsilon_d$
2	0.881373587	93	3.3661046429	573	6.6411804655
3	1.866264041	101	2.9982229503	677	3.9516133361
5	0.4812118251	133	5.1532581804	717	5.4847797157
6	2.2924316696	141	5.2469963702	773	4.9345256863
7	2.7686593833	149	4.1111425009	797	5.9053692725
11	2.9932228461	157	5.3613142065	917	7.0741160992
13	1.1947632173	167	5.8171023021	941	7.0343887062
14	3.4000844141	173	2.5708146781	1013	6.8276304083
17	2.0947125473	197	3.3334775869	1077	5.8888702849
21	1.5667992370	213	4.2902717358	1133	4.6150224728
23	3.8707667003	227	6.1136772851	1253	5.1761178117
29	1.6472311464	237	4.3436367167	1293	7.4535615360
33	3.8281684713	269	5.0999036060	1493	7.7651450829
37	2.4917798526	293	2.8366557290	1613	7.9969905191
38	4.3038824281	317	4.4887625925	1757	6.9137363626
41	4.1591271346	341	5.6240044731	1877	7.3796325418
47	4.5642396669	398	6.6821070271	2453	8.1791997198
53	1.9657204716	413	4.1106050108	2477	6.4723486834
61	3.6642184609	437	3.0422471121	2693	8.3918567515
62	4.8362189128	453	5.0039012599	3053	8.1550748053
69	3.2172719712	461	5.8999048596	3317	8.5642675624
77	2.1846437916	509	6.8297949062	3533	7.7985232220
83	5.0998292455	557	5.4638497592		

The following examples illustrate Propositions 3.1–3.3.

EXAMPLE 3.1. Let $d = 215$. Then $t_d = 44$, $\sigma = 1$, $N(\varepsilon_d) = 1$, $u_d = n_d = 3$ and $m = 5$. Thus $t_d = 44 = n_d^2 m - 1$ and $d = n_d^2 m^2 - 2m = 15^2 - 10$.

EXAMPLE 3.2. Let $d = 357 = 3 \cdot 7 \cdot 17$. Then $x^2 - 357y^2 = -2^2 \cdot 17$ has solution $(17, 1) = (x, y)$ since $\wp_{17}$ dividing 17 is principal, but $\wp_3 \not\sim 1$ and $\wp_7 \not\sim 1$ while $\wp_3\wp_7 \sim 1$ with $x^2 - 357y^2 = -2^2 \cdot 21$ having solution $(x, y) = (21, 1)$. Here $h(357) = 2$ and both $\wp_3$, $\wp_7$ are ambiguous ideals. Here $t_d = 19$ and $u_d = 1$.

Remark 3.3. If $u_d = p = n$ in Proposition 3.1 then d is clearly of ERD type. However, if u_d is composite we may have non-ERD types such as $d = 158$ with $N(\varepsilon_d) = 1$ and $n_d = 0$. Here $u_d = 616$.

On the other hand, if $N(\varepsilon_d) = -1$ and $u_d = p$ or $2p$ for $p > 2$ prime then d is not ERD type. If it were then $d = l^2 + r$ where $|r| \in \{1, 4\}$ since

$N(\varepsilon_d) = -1$. In this case $u_d = 1$ or 2. This generalizes Yokoi [20, Lemma 3, p. 143].

The following application of Theorem 3.2 has ramifications concerning certain conjectures in the literature. Moreover, it generalizes Yokoi [18, Corollary 2.2].

THEOREM 3.10. *If* $d > 0$ *is square-free and* $n_d \neq 0$ *then* $u_d \not\equiv 0 \pmod{d}$.

Proof. $u_d > 2$ may be assumed. By Theorem 3.2, $u_d^2 \leq 4d$. Also if $u_d \equiv 0 \pmod{d}$ then $u_d^2 \geq d^2$. Thus $4d \geq u_d^2 \geq d^2 > 4d$, a contradiction. ■

In particular, the *Artin–Ankeny–Chowla conjecture* holds if $n_d \neq 0$, i.e., $u_p \not\equiv 0 \pmod{p}$ when $p \equiv 1 \pmod{4}$ is prime. Moreover, *the Mollin–Walsh conjecture* [6] that there does not exist any square-free $d \equiv 7 \pmod{8}$ with $u_d \equiv 0 \pmod{d}$ holds when $n_d \neq 0$.

In Table 3.1 we list all $h(d) = 1$ (with one possible exception) when $n_d \neq 0$. This completes Yokoi's result (where he assumed d to be a prime congruent to 1 modulo 4). Here we used the techniques of [8] and the bound in Corollary 3.1.

Acknowledgement. The author's research is supported by NSERC Canada grants #A8484 and #A7649 respectively. Moreover, the first author's research was also supported by a Killam research award held at the University of Calgary in 1990. Finally, the authors wish to thank Gilbert Fung, a graduate student of the second author, for doing the computing involved in compiling the above table.

REFERENCES

[1] H. Cohn, *A Second Course in Number Theory*, Wiley, New York 1962.

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

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

[4] R. A. Mollin, *On the insolubility of a class of Diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud–Degert type*, Nagoya Math. J. 105 (1987), 39–47.

[5] —, *Class number one criteria for real quadratic fields I*, Proc. Japan Acad. Ser. A 63 (1987), 121–125.

[6] R. A. Mollin and P. G. Walsh, *A note on powerful numbers, quadratic fields and the pellian*, C. R. Math. Rep. Acad. Sci. Canada 8 (1986), 109–114.

[7] R. A. Mollin and H. C. Williams, *Prime producing quadratic polynomials and real quadratic fields of class number one*, in: Number Theory, J. M. De Koninck and C. Levesque (eds.), Walter de Gruyter, Berlin 1989, 654–663.

[8] R. A. Mollin and H. C. Williams, *Solution of the class number one problem for real quadratic fields of extended Richaud–Degert type* (*with one possible exception*), in: Number Theory, R. A. Mollin (ed.), Walter de Gruyter, Berlin 1990, 417–425.

[9] —, —, *Class number one for real quadratic fields, continued fractions and reduced ideals*, in: Number Theory and Applications, R. A. Mollin (ed.), NATO ASI Ser. C265, Kluwer, Dordrecht 1989, 481–496.

[10] —, —, *On prime valued polynomials and class numbers of real quadratic fields*, Nagoya Math. J. 112 (1988), 143–151.

[11] T. Nagell, *Number Theory*, Chelsea, New York 1981.

[12] C. Richaud, *Sur la résolution des équations* $x^2 - Ay^2 = \pm 1$, Atti Acad. Pontif. Nouvi Lincei (1866), 177–182.

[13] T. Tatuzawa, *On a theorem of Siegel*, Japan J. Math. 21 (1951), 163–178.

[14] H. Yokoi, *New invariants of real quadratic fields*, in: Number Theory, R. A. Mollin (ed.), Walter de Gruyter, Berlin 1990, 635–639.

[15] —, *Class number one problem for real quadratic fields* (*The conjecture of Gauss*), Proc. Japan Acad. Ser. A 64 (1988), 53–55.

[16] —, *Some relations among new invariants of prime number p congruent to* 1 (mod 4), in: Investigations in Number Theory, Adv. Stud. in Pure Math. 13, 1988, 493–501.

[17] —, *The fundamental unit and class number one problem of real quadratic fields with prime discriminant*, preprint.

[18] —, *Bounds for fundamental units and class numbers of real quadratic fields with prime discriminant*, preprint.

[19] —, *On the fundamental unit of real quadratic fields with norm* 1, J. Number Theory 2 (1970), 106–115.

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

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF CALGARY
CALGARY, ALBERTA
CANADA T2N 1N4
RAMOLLIN@ACS.UCALGARY.CA

COMPUTER SCIENCE DEPARTMENT
UNIVERSITY OF MANITOBA
WINNIPEG, MANITOBA
CANADA R3T 2N2
HUGH_WILLIAMS@CSMAIL.CS.UMANITOBA.CA

Reçu par la Rédaction le 25.5.1990;
en version modifiée le 2.5.1991