Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

# A computational technique for determining the fundamental unit in explicit types of real quadratic number fields

Özen Özer [1, *], Abdel Badeh M. Salem [2]

[1]Department of Mathematics, Faculty of Science and Arts, Kırklareli University, 39100, Kırklareli, Turkey
[2]Faculty of Computer and Informatic Science, Ain Shams University, Cairo, Egypt

ARTICLE INFO

*Article history:*
Received 24 October 2016
Received in revised form
10 January 2017
Accepted 10 January 2017

*Keywords:*
Quadratic fields
Continued fractions
Fundamental units
Yokoi's invariants

ABSTRACT

In real quadratic number field $Q(\sqrt{d})$, integral basis element is denoted by $w_d = [\, a_0; \overline{a_1, a_2, \dots, a_{\ell(d)-1}, a_{\ell(d)}}\,]$ for the period length $\ell(d)$. The fundamental unit $\varepsilon_d$ of real quadratic number field is also denoted by $\varepsilon_d = \frac{t_d + u_d\sqrt{d}}{2} > 1$. The Unit Theorem for real quadratic fields says that every unit in the integer ring of a quadratic field is generated by the fundamental unit. Also, regulator in real quadratic cryptography is outstanding. We have seen that the regulator $R = \log \varepsilon_d$ plays the role of a group order. The regulator problem is to find an integer $R'$ satisfies $|R' - R| < 1$ where $R'$ *is* an approximation of $R$ with any given precision can be computed in polynomial time for discriminant. However, some of the fundamental units can not be calculated by computer programme in short time because of the big numbers or long calculations of usual algorithm. This is also the main problem from the computing/informatics point of view. So, determining of the fundamental units is of great importance. In this paper, we construct a theorem to determine the some certain real quadratic fields $Q(\sqrt{d})$ having specific form of continued fraction expansion of $w_d$ where $d \equiv 1(mod4)$ is a square-free integer. We also present the general context and obtain new certain parametric representation of fundamental unit $\varepsilon_d$ for such types of fields.By specialization, we get a fix on Yokoi's invariants and support all results with tables.



## 1. Introduction

Development of the theory of quadratic fields is not easy task. Tools of the infrastructure of quadratic fields have rendered numerous results in algebraic and computational number theory with cryptography as well as algebraic geometry, especially when applied to quadratic order. For example, Public Key Cryptography is one of the main techniques for making the internet secure in the cryptography and computer science. Most public key crypto-systems are based on intractable computational problems in number theory such as factoring integers. One source for computationally hard problems is algebraic number theory. Since the Diffie-Hellman key exchange protocol was presented in class groups of imaginary quadratic orders in 1988, many public key crypto-systems have been suggested whose security is based on difficult problems in quadratic number fields. Since then it has been started to state of the art of real and imaginary quadratic field crypto-systems.

Also, there are many different approach from that of most authors who use genus theory, composition of binary quadratic forms, and who use class field theory as a developmental tool. Also, many books and papers on the number theory include(use) continued fraction, ideal, class number, quadratic residue, prime producing quadratic polynomials, binary quadratic forms, elliptic curves, algorithms in cryptography based upon ideals with continued fraction algorithms, regulators in the class group, etc.

Because of the importance of the class number, the problem of determining the class number is of central interest in algebraic number theory. In general, the determination of the class number of an arbitrary algebraic number field is not an easy task. There exist some formulaes for determining the class numbers of real and imaginary quadratic fields, but the problem of determining the class number of an arbitrary number field is still beyond the scope of

* Corresponding Author.
Email Address: ozenozer39@gmail.com (Ö. Özer)
https://doi.org/10.21833/ijaas.2017.02.004

contemporary number theory.For example, to determine the class number (Dirichlet class number formulae), we need regulator, values of $L$- function, discriminant etc. So, real quadratic fields have great importance in many branches of mathematics, even computer science.

It is also well known that the fundamental units play an important role in studying the class number problem, unit group, pell equations, cryptology, network security and even computer science. Most of present and past works focused on the lower bound of fundamental units and the number of some special types of polynomials with fixed period of continued fraction expansions, certain class number and some types of continued fraction expansions, relations between the coefficients of fundamental units, comparison between the period length, quadratic fields and cryptology and Yokoi's invariants (Buchmann, 2004; Badziahin and Shallit, 2016; Benamar et al., 2015; Clemens et al., 1995; Elezovi´, 1997; Kawamoto and Tomita, 2008; Louboutin, 1988; Özer, 2016a; 2016b; Sasaki, 1986; Tomita, 1995; Tomita and Yamamuro, 2002; Williams and Buck, 1994; Yokoi, 1990; 1993a; 1991; 1993b; Zhang and Yue, 2014). For the history and main results on infrastructures of quadratic fields, we refer to the reader to (Mollin,1996; Olds, 1963; Perron, 1950; Sierpinski, 1964).

The focal point of this paper is to determine the some specific types of the real quadratic fields $\mathrm{Q}(\sqrt{\mathrm{d}})$ and the representation of fundamental units $\varepsilon_d = \frac{t_d + u_d\sqrt{d}}{2}$ where $\mathrm{d} \equiv 1(\mathrm{mod}4)$ is a square free positive integer. By using this practical way, obtained results on fundamental units, Yokoi's invariants, continued fraction expansions, period length are given with tables as illustrates. Also, present paper completes (Özer, 2016b) in the case of $\mathrm{d} \equiv 1(\mathrm{mod}4)$.

## 2. Preliminaries

Now, we recall some definitions and lemmas which will be used later.

### 2.1. Quadratic fields

**Definition 1.** If $k$ is an extension of $Q$ of degree two, then $k$ is called a quadratic field and represents as $k = \mathrm{Q}(\sqrt{\mathrm{d}})$ where d is a square free integer.

**Definition 2**. If $\mathrm{d} > 0$ square free integer, then $\mathrm{Q}(\sqrt{\mathrm{d}})$ is called a real quadratic field, and if $\mathrm{d} < 0$ then $\mathrm{Q}(\sqrt{\mathrm{d}})$ is called a imaginary (complex) quadratic field.

**Note 1.** There is a one to one correspondence between quadratic fields and square free rational integer for $\mathrm{d} \neq 1$. Also, $\mathcal{O}_d$ is called integral ring is the ring of integers of the quadratic field $k$. The ring of integer of quadratic field has two integral basis elements. One of is the trivial identity element 1, another is the non trivial basis element $w_d$. In real quadratic fields, $w_d$ is defined $w_d = \frac{1+\sqrt{\mathrm{d}}}{2}$ in the case of $\mathrm{d} \equiv 1(\mathrm{mod}4)$ and also $w_d = \sqrt{\mathrm{d}}$ in the case of $\mathrm{d} \equiv 2,3(\mathrm{mod}4)$.

### 2.2. Continued fraction expansions

There are many types of continued fraction expansions, but in our work, we use the quadratic irrational numbers and reduced quadratic irrationals, which indicate the periodic continued fraction expansion and purely periodic continued fraction expansion, respectively.

**Definition 3.** Let $a_0, a_1, a_2, \dots, a_{\mathrm{j}}, \dots$ are integers and $a_{\mathrm{j}} > 0$ for $0 < j$. Then

$$[\, a_0; a_1, a_2, \dots, a_{\mathrm{j}}, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{j-1} + \cfrac{1}{a_j + \ddots}}}}$$

is called simple continued fraction expansion.

**Definition 4.** A real number $\gamma$ is called a quadratic irrational, if $\gamma$ can be written as $\gamma = \frac{P+\sqrt{d}}{Q}$ where $P, Q, d$ are integers, $d > 0$, $Q \neq 0$, and $P^2 \equiv d(\mathrm{mod}\ Q)$.

**Definition 5.** Quadratic $\gamma$ is called periodic if $\gamma = [\, a_0; a_1, a_2, \dots]$ where $a_{\mathrm{n}} = a_{\ell(\mathrm{d})+n}$ for all $n \geq k$ with $\ell(\mathrm{d}), k \in N$. We use the notation $\gamma = \left[\, a_0; a_1, a_2, \dots, a_{k-1}, \overline{a_k, a_{k+1}, \dots, a_{\ell(\mathrm{d})+k-1}}\right]$ where $\ell(\mathrm{d})$ is period length of $\gamma$.

**Definition 6.** Quadratic $\gamma$ is called purely periodic if $\gamma = \left[\overline{a_0; a_1, a_2, \dots, a_{\ell(\mathrm{d})-1}}\right]$.

**Example 1.** Let $d = 145$. if we consider $\gamma = \frac{9+\sqrt{145}}{8}$, then continued fraction expansion of $\gamma$ is given by $[\overline{2; 1, 1, 1, 2}]$ with period $\ell(\mathrm{d}) = 5$.

### 2.3. Fundamental units

**Definition 7.** Let $Q(\sqrt{d})$ be a real quadratic number field and $U_d$ be a unit group. In real quadratic fields, positive units in $U_d$ have a generator, which is the smallest unit exceeds 1. This selection is unique and is called the fundamental unit of $Q(\sqrt{d})$ and denoted by $\varepsilon_d = \frac{1}{2}(t_d + u_d\sqrt{d})$.

**Note 2.** When $d < 0$, then $U_d$ unit group is finite cyclic and when $d > 0$ then the positive units of $U_d$ form a multiplicative group isomorphic to $\mathcal{Z}$, and so $U_d$ contains exactly one generator larger than 1 describing as fundamental unit.

**Proposition 1.** Let $Q(\sqrt{d})$ be a real quadratic number field, then there is a fundamental unit $\varepsilon_d > 1$ where the unit group of $Q(\sqrt{d})$ is $U_d = \{\mp \varepsilon_d^s | \, s \in Z\}$.

To illustrate to notion of fundamental unit, we have followings:

**Example 2.** Let $d = 5$, then the fundamental unit is $\varepsilon_d = (1+\sqrt{5})/2$ since $(1+\sqrt{5})/2 > 1$ and $((1+\sqrt{5})/2)((1-\sqrt{5})/2) = -1$. Powers of $(1+\sqrt{5})/2$ are also units and there are infinitely many of them since $(1+\sqrt{5})/2 > 1$.

**Remark 1.** Not all fundamental units are so easy to calculate practically, even for small values of $d$. So, this is very important to find a practical method so as to easily and rapidly determine fundamental unit $\varepsilon_d$.

**Example 3**. If we take $d = 1969 \equiv 1(\text{mod}4)$ ,then $w_d = \frac{1+\sqrt{\text{d}}}{2}$ and the fundamental unit is

$\varepsilon_d = 4582840784247572232077488714645 1 + 211320263122040749213888265460 0 w_d$

**Note 3.** Additionaly, Yokoi's invariants, which were defined by H.Yokoi are determined by the coefficient of fundamental unit $\varepsilon_d = \frac{t_d + u_d\sqrt{d}}{2}$ as $m_d = \left[\left[\frac{u_d^2}{t_d}\right]\right]$ and $n_d = \left[\left[\frac{t_d}{u_d^2}\right]\right]$ have got great importance in class number problem and in the solvability of Pell equations where $[\![x]\!]$ represents the greatest integer not greater than $x$.

In this section we also give some fundamental concepts as follows for the proof of our main theorem defined in the next section.

**Note 4.** For the set $I(d)$ of all quadratic irrational numbers in $Q(\sqrt{d})$, we say that $\alpha$ in $I(d)$ is reduced if $\alpha > 1, -1 < \alpha' < 0$ ($\alpha'$ is the conjugate of $\alpha$ with respect to $Q$), and $R(d)$ denotes the set of all reduced quadratic irrational numbers in $I(d)$.Then, it is well known that any number $\alpha$ in $R(d)$ is purely periodic in the continued fraction expansion and the denominator of its modular automorphism is equal to fundamental unit $\varepsilon_d$ of $Q(\sqrt{d})$.

**Definition 8.** (Özer, 2016a) $\{Y_i\}$ is called a sequence defined by the recurrence relation

$Y_i = 5Y_{i-1} + Y_{i-2}$

with seed values $Y_0 = 0$ and $Y_1 = 1$ for $i \geq 2$.

**Lemma 1.** (Tomita, 1995) Let $d$ be a square-free positive integer such that $d$ congruent to 1 modulo 4. If we put $w_d = \frac{1+\sqrt{d}}{2}, a_0 = [\![w_d]\!]$ into the $w_R = (a_0 - 1) + w_d$, then $w_d \notin R(d)$ but $w_R \in R(d)$holds. Moreover, for the period $l = \ell(\text{d})$ of $w_R$, we get $w_R = \overline{[2a_0 - 1, a_1, \ldots\ldots, a_{l-1}]}$ and $w_d = \overline{[a_0, a_1, \ldots\ldots, a_{l-1}, 2a_0 - 1]}$.

Let $w_R = \frac{(P_l w_R + P_{l-1})}{(Q_l w_R + Q_{l-1})} = \overline{[2a_0 - 1, a_1, \ldots\ldots, a_{l-1}, w_R]}$ be a modular automorphism of $w_R$, then the fundamental unit $\varepsilon_d$ of $Q(\sqrt{d})$ is given by the formulae

$\varepsilon_d = \frac{t_d + u_d\sqrt{d}}{2}, \quad t_d = (2a_0 - 1).Q_{\ell(d)} + 2Q_{\ell(d)-1}, \; u_d = Q_{\ell(d)}$

where $Q_i$ is determined by $\text{Q}_0 = 0$ , $\text{Q}_1 = 1$ and $Q_{i+1} = a_i Q_i + Q_{i-1}$, $(i \geq 1)$.

## 3. Main theorem and results

**Main Theorem.** Let $d$ be square free positive integer and $\ell \geq 2$ be a positive integer.

(1) We suppose that

$d = (2\delta Y_\ell + 5)^2 + 8\delta Y_{\ell-1} + 4$

where $\delta > 0$ is a positive integer. In this case, we obtain that $\text{d} \equiv 1(\text{mod}4)$ and

$w_d = \left[3 + \delta Y_\ell; \overline{\underbrace{5,5,\ldots,5}_{\ell-1}, 5 + 2\delta Y_\ell}\right]$

with $\ell = \ell(d)$. Moreover, we get

$t_d = 2\delta Y_\ell^2 + 5Y_\ell + 2Y_{\ell-1}$ and $u_d = Y_\ell$ for $\varepsilon_d = \frac{t_d + u_d\sqrt{d}}{2}$.

(2) If $\ell \equiv 0(mod3)$, and

$d = (\delta Y_\ell + 5)^2 + 4\delta Y_{\ell-1} + 4$

for $\delta > 0$ positive odd integer, then $\text{d} \equiv 1(\text{mod}4)$ and

$w_d = \left[3 + \frac{\delta Y_\ell}{2}; \overline{\underbrace{5,5,\ldots,5}_{\ell-1}, 5 + \delta Y_\ell}\right]$

Also, in this case

$t_d = \delta Y_\ell^2 + 5Y_\ell + 2Y_{\ell-1}$ and $u_d = Y_\ell$ hold for $\varepsilon_d = \frac{t_d + u_d\sqrt{d}}{2}$.

**Remark.** it is clear that $Y_\ell$ is odd number if $\ell \not\equiv 0(mod3)$. $\frac{\delta Y_\ell}{2}$ is not integer if we substitue $\delta$ odd numbers into the parametrization of d for $\ell \not\equiv 0(mod3)$. So, we assume that $\ell$ is divided by 3 in the case of (2). Also, if we choose $\delta$ is even integer, the parametrization of $d$ in (2) coincides with the case of (1). That's why we assume $\ell \equiv 0(mod3)$ and $\delta > 0$ positive odd integer in the case of (2).

**Proof.** (1) For any $\ell \geq 2$ and $\delta > 0$ positive integer, $d \equiv 1(mod4)$ holds since $(2\delta Y_\ell + 5)$ is odd integer.

From Lemma 1, we know that $w_d = \frac{1+\sqrt{d}}{2}, a_0 = [\![w_d]\!]$ and $w_R = (a_0 - 1) + w_d$.

By using these equations, we obtain

$$w_R = (2 + \delta Y_\ell) + \left[3 + \delta Y_\ell; \underbrace{\overline{5,5,\dots,5}}_{\ell-1}, 5 + 2\delta Y_\ell\right]$$

$$\Rightarrow \quad w_R = (5 + 2\delta Y_\ell) + \cfrac{1}{5+\cfrac{1}{5+\cfrac{1}{\ddots\,+\cfrac{1}{5+\cfrac{1}{w_R}}}}}$$

$$= (5 + 2\delta Y_\ell) + \frac{1}{5} + \dots + \frac{1}{5} + \frac{1}{w_R}$$

By a straight forward induction argument, we have

$$w_R = (5 + 2\delta Y_\ell) + \frac{Y_{\ell-1}w_R + Y_{\ell-2}}{Y_\ell w_R + Y_{\ell-1}}$$

Using Definition 8 and put $Y_{\ell+1} + Y_{\ell-1} = 5Y_\ell + 2Y_{\ell-1}$ equation into the above equality, we obtain

$$w_R^2 - (5 + 2\delta Y_\ell)w_R - (1 + 2\delta Y_{\ell-1}) = 0$$

This implies that $w_R = \frac{(5+2\delta Y_\ell)+\sqrt{d}}{2}$ since $w_R > 0$. If we consider Lemma 1, we get $\frac{1+\sqrt{d}}{2} = \left[3 + \delta Y_\ell; \underbrace{\overline{5,5,\dots,5}}_{\ell-1}, 5 + 2\delta Y_\ell\right]$ and $\ell = \ell(d)$. Proof of the first part of (1) is completed.

Now, we have to determine $\varepsilon_d$, $t_d$ and $u_d$ using Lemma 1. We have known that $Q_i = Y_i$ from (Özer, 2016a) by induction for $\forall i \geq 0$.

If we substitute the values of sequence into the coefficients of fundamental unit

$t_d = 2\delta Y_\ell^2 + 5Y_\ell + 2Y_{\ell-1}$ and $u_d = Y_\ell$ holds for $\varepsilon_d = \frac{t_d + u_d\sqrt{d}}{2}$.

(2) In the case of $\ell \equiv 0(mod3)$, $Y_\ell \equiv 0(mod2)$ holds. By subsituting this equivalence into the parametrization of $d$, we have $d \equiv 1(mod4)$ for $\delta > 0$ positive odd integer.

By using Lemma 1 and the parametrization of $d = (\delta Y_\ell + 5)^2 + 4\delta Y_{\ell-1} + 4$, we have

$$w_R = (a_0 - 1) + w_d \Rightarrow \qquad w_R = \left(2 + \frac{\delta Y_\ell}{2}\right) + \left[3 + \frac{\delta Y_\ell}{2}; \underbrace{\overline{5,5,\dots,5}}_{\ell-1}, 5 + \delta Y_\ell\right]$$

$$\Rightarrow \quad w_R = (5 + \delta Y_\ell) + \cfrac{1}{5+\cfrac{1}{5+\cfrac{1}{\ddots\,+\cfrac{1}{5+\cfrac{1}{w_R}}}}}$$

$$= (5 + \delta Y_\ell) + \frac{1}{5} + \dots + \frac{1}{5} + \frac{1}{w_R}$$

By a straight forward induction argument, we get

$$w_R = (5 + \delta Y_\ell) + \frac{Y_{\ell-1}w_R + Y_{\ell-2}}{Y_\ell w_R + Y_{\ell-1}}$$

Using Definition 8 and put $Y_{\ell+1} + Y_{\ell-1} = 5Y_\ell + 2Y_{\ell-1}$ equation into the above equality, we obtain

$$w_R^2 - (5 + \delta Y_\ell)w_R - (1 + \delta Y_{\ell-1}) = 0$$

This implies that $w_R = \left(2 + \frac{\delta Y_\ell}{2}\right) + \frac{1+\sqrt{d}}{2}$ since $w_R > 0$. If we consider Lemma 1, we get

$\frac{1+\sqrt{d}}{2} = \left[3 + \frac{\delta Y_\ell}{2}; \underbrace{\overline{5,5,\dots,5}}_{\ell-1}, 5 + \delta Y_\ell\right]$ and $\ell = \ell(d)$.

Using $Q_i = Y_i$ for $\forall i \geq 0$, we obtain the coefficients of fundamental unit as follows:

$t_d = \delta Y_\ell^2 + 5Y_\ell + 2Y_{\ell-1}$ and $u_d = Y_\ell$ for $\varepsilon_d = \frac{t_d + u_d\sqrt{d}}{2}$.

We can obtain following conclusions from Main Theorem.

**Corollary 1.** Let d be a square free positive integer congruent to 1 modulo 4. If we assume that $d$ is satisfying the conditions in Main Theorem, then it always hold Yokoi's invariant $m_d$=0.

**Proof.** Yokoi's invariant $m_d$ is defined $m_d = \left[\!\left[\frac{u_d^2}{t_d}\right]\!\right]$ by Yokoi (1990, 1991, 1993a, 1993b). In the case of (1), if we substitue $t_d$ and $u_d$ into the $m_d$, then we obtain

$$m_d = \left[\!\left[\frac{u_d^2}{t_d}\right]\!\right] = \left[\!\left[\frac{Y_\ell^2}{2\delta Y_\ell^2 + 5Y_\ell + 2Y_{\ell-1}}\right]\!\right]$$

So, we get $m_d$=0 since $\delta > 0$ is positive integer.

In a similar way, we obtain $m_d = \left[\!\left[\frac{u_d^2}{t_d}\right]\!\right] = \left[\!\left[\frac{Y_\ell^2}{\delta Y_\ell^2 + 5Y_\ell + 2Y_{\ell-1}}\right]\!\right]$ =0 since $t_d > u_d^2$ for $\delta > 0$ positive odd integer in the case of (2).

**Corollary 2.** Let $d$ be the square free positive integer positive integer corresponding to $Q(\sqrt{d})$ holding (1) in the Main Theorem. We state the following Table 1 where fundamental unit is $\varepsilon_d$, integral basis element is $w_d$ and Yokoi's invariant is $n_d$ for $\delta = 1,2$ and $2 \leq \ell(d) \leq 11$. (In Table 1, we rule out $\ell(d)$ = 7,8 for $\delta =$ 2 since d is not a square free positive integer.)

**Proof.** This Corollary is obtained from main theorem by taking $\delta = 1$ or 2 in the case of (1) of Main Theorem. We know $n_d$ is defined $n_d = \left[\!\left[\frac{t_d}{u_d^2}\right]\!\right]$. If we substitue $t_d$ and $u_d$ into the $n_d$, then we get

$$n_d = \left[\!\left[\frac{t_d}{u_d^2}\right]\!\right] = \left[\!\left[\frac{2Y_\ell^2 + 5Y_\ell + 2Y_{\ell-1}}{Y_\ell^2}\right]\!\right] = 2 + \left[\!\left[\frac{5Y_\ell + 2Y_{\ell-1}}{Y_\ell^2}\right]\!\right]$$

for $\delta = 1$. For $\ell = 2$, we get $n_d = 3$. Since $Y_\ell$ is increasing sequence, we obtain

$$2{,}208 > \left(\frac{2Y_\ell^2 + 5Y_\ell + 2Y_{\ell-1}}{Y_\ell^2}\right) > 2$$

**Table 1:** Square-free positive integers d with $2 \leq \ell(d) \leq 11$

| $d$ | $\delta$ | $\ell(d)$ | $n_d$ | $w_d$ | $\varepsilon_d$ |
|---|---|---|---|---|---|
| 237 | 1 | 2 | 3 | $[8;\overline{5,15}]$ | $(77+5\sqrt{237})/2$ |
| 3293 | 1 | 3 | 2 | $[29;\overline{5,5,57}]$ | $(1492+26\sqrt{3293})/2$ |
| 75837 | 1 | 4 | 2 | $[138;\overline{5,5,275}]$ | $(37177+135\sqrt{75837})/2$ |
| 1980733 | 1 | 5 | 2 | $[704;\overline{5,\ldots,5,1407}]$ | $(986577+701\sqrt{1980733})/2$ |
| 53076837 | 1 | 6 | 2 | $[3643;\overline{5,\ldots,5,7285}]$ | $(26518802+3640\sqrt{53076837})/2$ |
| 1429398373 | 1 | 7 | 2 | $[18904;\overline{5,\ldots,5,37807}]$ | $(714597387+18901\sqrt{1429398373})/2$ |
| 38531878237 | 1 | 8 | 2 | $[98148;\overline{5,\ldots,5,196295}]$ | $(19265410577+98145\sqrt{38531878237})/2$ |
| 1038885617213 | 1 | 9 | 2 | $[509629;\overline{5,\ldots,5,1019257}]$ | $(519440064172+509626\sqrt{1038885617213})/2$ |
| 28011142505037 | 1 | 10 | 2 | $[2646278;\overline{5,\ldots,5,5292555}]$ | $(14005557001877+2646275\sqrt{28011142505037})/2$ |
| 755260729918253 | 1 | 11 | 2 | $[13741004;\overline{5,\ldots,5,27482007}]$ | $(377630290961557+13741001\sqrt{755260729918253})/2$ |
| 645 | 2 | 2 | 5 | $[13;\overline{5,25}]$ | $(127+5\sqrt{645})/2$ |
| 11965 | 2 | 3 | 4 | $[55;\overline{5,5,109}]$ | $(2844+26\sqrt{11965})/2$ |
| 297445 | 2 | 4 | 4 | $[273;\overline{5,\ldots,5,545}]$ | $(73627+135\sqrt{297445})/2$ |
| 7892645 | 2 | 5 | 4 | $[1405;\overline{5,\ldots,5,2809}]$ | $(1969379+701\sqrt{7892645})/2$ |
| 212150445 | 2 | 6 | 4 | $[7283;\overline{5,\ldots,5,14565}]$ | $(53018002+3640\sqrt{212150445})/2$ |
| 4155520513405 | 2 | 9 | 4 | $[1019255;\overline{5,\ldots,5,2038509}]$ | $(1038877383924+509626\sqrt{4155520513405})/2$ |
| 112044456015045 | 2 | 10 | 4 | $[5292553;\overline{5,\ldots,5,10585105}]$ | $(28011099753127+2646275\sqrt{112044456015045})/2$ |
| 3021042327692485 | 2 | 11 | 4 | $[27482005;\overline{5,\ldots,5,54964009}]$ | $(755260507925559+13741001\sqrt{3021042327692485})/2$ |

for $\ell \geq 3$. Therefore, we obtain $n_d = 2$ for $\ell \geq 3$. Also, in the case of $\delta = 2$, we get $n_d = 5$ for $\ell = 2$ as well as $n_d = 4$ for $\ell \geq 3$ by using similar way. The proof of Corollary 2 is completed.

**Corollary 3.** Let $d$ be the square free positive integer corresponding to $Q(\sqrt{d})$ holding (2) in the Main Theorem. We state the following Table 2 where fundamental unit is $\varepsilon_d$, integral basis element is $w_d$ and Yokoi's invariant is $n_d$ for $\delta = 1,3$ and $3 \leq \ell(d) \leq 12$. (In Table 2, we rule out $\ell(d) = 6$ for $\delta = 1$ since d is not a square free positive integer.)

**Table 2:** Square-free positive integers d with $3 \leq \ell(d) \leq 12$

| $d$ | $\delta$ | $\ell(d)$ | $n_d$ | $w_d$ | $\varepsilon_d$ |
|---|---|---|---|---|---|
| 985 | 1 | 3 | 1 | $[16;\overline{5,5,31}]$ | $(816+26\sqrt{985})/2$ |
| 259724148745 | 1 | 9 | 1 | $[254816;\overline{5,\ldots 5,509631}]$ | $(259721404296+509626\sqrt{259724148745})/2$ |
| 5091005926115233 | 1 | 12 | 1 | $[35675643;\overline{5,\ldots 5,71351285}]$ | $(5091005541876802+71351280\sqrt{5091005926115233})/2$ |
| 6953 | 3 | 3 | 3 | $[42;\overline{5,5,83}]$ | $(2168+26\sqrt{6953})/2$ |
| 119364041 | 3 | 6 | 3 | $[5463;\overline{5,\ldots,5,10925}]$ | $(39768402+3640\sqrt{119364041})/2$ |
| 2337484405433 | 3 | 9 | 3 | $[764442;\overline{5,\ldots 5,1528883}]$ | $(779158724048+509626\sqrt{2337484405433})/2$ |
| 45819048724176041 | 3 | 12 | 3 | $[107026923;\overline{5,\ldots 5,214053845}]$ | $(15273015857153602+71351280\sqrt{45819048724176041})/2$ |

**Proof.** By subsituting $\delta = 1$ or 3 into the (2) of Main Theorem, we get this corallary and the table in the case of (2) of Main Theorem. If we substitue $t_d$ and $u_d$ into the $n_d = \left[\left[\frac{t_d}{u_d^2}\right]\right]$, then we get

$$n_d = \left[\left[\frac{t_d}{u_d^2}\right]\right] = \left[\left[\frac{Y_\ell^2+5Y_\ell+2Y_{\ell-1}}{Y_\ell^2}\right]\right] = 1 + \left[\left[\frac{5Y_\ell+2Y_{\ell-1}}{Y_\ell^2}\right]\right]$$

for $\delta = 1$. Since $Y_\ell$ is increasing sequence, we obtain

$$1{,}208 > \left(\frac{Y_\ell^2+5Y_\ell+2Y_{\ell-1}}{Y_\ell^2}\right) > 1$$

for $\ell \geq 3$. Therefore, we obtain $n_d = 1$ for $\ell \geq 3$. Also, we get $n_d = 3$ for $\ell \geq 3$ in a similar way for $\delta = 3$.

## 4. Conclusıon and future works

There are a lot of applications for quadratic fields in many different fields of mathematics which include algebraic number theory, algebraic geometry, algebra, cryptology, and also other scientific fields like computer science.

In this paper, we introduced the notion of real quadratic field structures such as continued fraction expansions, fundamental unit and Yokoi invariants. We established general interesting and significant results for that. Results obtained in this paper provide us a useful and practical method in order to rapidly determine continued fraction expansion of $w_d$ fundamental unit $\varepsilon_d$ and and Yokoi invariants $n_d$ for such real quadratic number fields.

Findings in this paper will help the researchers to enhance and promote their studies on quadratic fields to carry out a general framework for their applications in life.

Future researches will be related to the application of our developed model/theory in crypto inteligent/smart systems.

## References


Badziahin D and Shallit J (2016). An unusual continued fraction. Proceedings of the American Mathematical Society, 144(5): 1887-1896.

Benamar H, Chandoul A, and Mkaouar M (2015). On the continued fraction expansion of fixed period in finite fields. Canadian Mathematical Bulletin-Bulletin Canadien De Mathematiques, 58(4): 704-712.

Buchmann J (2004). Introduction to cryptography. 2nd Edition, Springer-Verlag, New York, USA.

Clemens LE, Merill KD, and Roeder DW (1995). Continued fractions and series. Journal of Number Theory, 54(2): 309-317.

Elezovi´ N (1997). A note on continued fractions of quadratic irrationals. Mathematical Communications, 2(1): 27-33.

Kawamoto F and Tomita K (2008). Continued fractions and certain real quadratic fields of minimal type. Journal of the Mathematical Society of Japan, 60(3): 865-903.

Louboutin S (1988). Continued fractions and real quadratic fields. Journal of Number Theory, 30(2): 167-176.

Mollin RA (1996). Quadratics. CRC Press, Boca Rato, FL.

Olds CD (1963). Continued fractions. Random House, New York, USA

Özer Ö (2016a). Notes on especial continued fraction expansions and real quadratic number fields. Kirklareli University Journal of Engineering and Science, 2(1): 74-89.

Özer Ö (2016b). On real quadratic number fields related with specific type of continued fractions. Journal of Analysis and Number Theory, 4(2): 85-90.

Perron O (1950). Die Lehre von den Kettenbrichen. Chelsea, reprint from teubner leipzig, New York, USA.

Sasaki R (1986). A characterization of certain real quadratic fields. Proceedings of the Japan Academy, Series A, Mathematical Sciences, 62(3): 97-100.

Sierpinski W (1964). Elementary theory of numbers. Monografi Matematyczne, Warsaw.

Tomita K (1995). Explicit representation of fundamental units of some quadratic fields. Proceedings of the Japan Academy, Series A, Mathematical Sciences, 71(2): 41-43.

Tomita K and Yamamuro K (2002). Lower bounds for fundamental units of real quadratic fields. Nagoya Mathematical Journal, 166: 29-37.

Williams KS and Buck N (1994). Comparison of the lengths of the continued fractions of $\sqrt{D}$ and fraction $\frac{1}{2}(1+\sqrt{D})$. Proceedings of the American Mathematical Society, 120(4): 995-1002.

Yokoi H (1990). The fundamental unit and class number one problem of real quadratic fields with prime discriminant. Nagoya Mathematical Journal, 120: 51-59.

Yokoi H (1991). The fundamental unit and bounds for class numbers of real quadratic fields. Nagoya Mathematical Journal, 124: 181-197.

Yokoi H (1993a). A note on class number one problem for real quadratic fields. Proceedings of the Japan Academy, Series A, Mathematical Sciences, 69(1): 22-26.

Yokoi H (1993b). New invariants and class number problem in real quadratic fields. Nagoya Mathematical Journal, 132: 175-197.

Zhang Z and Yue Q (2014). Fundamental units of real quadratic fields of odd class number. Journal of Number Theory, 137: 122-129.