East Asian Mathematical Journal
Vol. 31 (2015), No. 3, pp. 357–362
http://dx.doi.org/10.7858/eamj.2015.027

NUMBER SYSTEMS PERTAINING TO EUCLIDEAN RINGS OF IMAGINARY QUADRATIC INTEGERS

Hyo-Seob Sim and Hyun-Jong Song*

Abstract. For a ring R of imaginary quadratic integers, using a concept of a unitary number system in place of the Motzkin's universal side divisor, we show that the following statements are equivalent:
(1) R is Euclidean.
(2) R has a unitary number system.
(3) R is norm-Euclidean.
Through an application of the above theorem we see that R admits binary or ternary number systems if and only if R is Euclidean.

1. Introduction

It is well known that among rings of imaginary quadratic integers, only nine rings

$$\mathbb{Z}\left[\sqrt{-1}\right],\ \mathbb{Z}\left[\sqrt{-2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right],$$

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$$

are principal ideal domains, which was conjectured by Gauss and settled completely by Stark [15]. Furthermore, only the first five examples of those are Euclidean domains, whose Euclidean functions are induced by the norms; whereas, the other four have no Euclidean functions whatsoever. A brilliant proof for the latter claim was presented by Motzkin [12] around 1949, who came up with a criterion for an integral domain to be Euclidean. But the proof seems too terse for laymen. And filling details of Motzkin's proof especially for non-existence of Euclidean algorithm of ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ was presented by many researchers; for

Received September 1, 2014; Accepted April 20, 2015.
2010 *Mathematics Subject Classification.* Primary 11A63, 11R04, 11R27, 13F07 57M27, Secondary 28A80, 52C20.
Key words and phrases. Euclidean rings, imaginary quadratic integers,Complex base number systems,Fractals.
* This work was supported by a Research Grant of Pukyong National University (2014 year).

(pISSN 1226-6973, eISSN 2287-2833)

examples, see [2], [6], [18] and [19]. Most of their proofs are based on a concept of the universal side divisor induced by the Motzkin's criterion.

Complex base number systems received wide attention due to various reasons such as data processing [8], [9] construction of Haar-typed wavelets [7], public key cryptosystems [14],[11] and fractal figures rendered by the fractional parts of number systems [1], [5] and [16]. In particular, Khmeinik [8] and Penny [13] independently showed that a number system with a base $b = -1+\sqrt{-1}$ and a digit set $D = \{0, 1\}$ in $\mathbb{Z}\left[\sqrt{-1}\right]$ yields so called *the twin dragon*. Knuth [10] proposed another binary number system with a base $b = \sqrt{-2}$ and a digit set $D = \{0, 1\}$. For applications in data processing Khmeinik [9] introduced a rather mysterious binary number system $\left(\frac{1+\sqrt{-7}}{2},\ D = \{0, 1\}\right)$ which yields so called the *the tamed dragon*. Similarly, we can get fractal figures by considering ternary number systems with the same digit set $D = \{-1, 0, 1\}$ and bases $1 + \sqrt{-2}$, $\frac{3+\sqrt{-3}}{2}$ and $\frac{3+\sqrt{-11}}{2}$ respectively. Two well known number systems in fractal geometry are added in a family of number systems which we are interested in, namely, $(b = -2 + i,\ D = \{0, \pm 1, \pm i\})$ and $\left(b = 2 + \omega,\ D = \{0, \pm 1, \pm\omega, \pm \omega^2\}\right)$ where $i = \sqrt{-1}$ and $\omega = \frac{1+\sqrt{-3}}{2}$.

All number systems introduced in the above have common characteristics:

Each digit set D consists of zero and units of the ring R.

Such a number system is said to be *unitary*. Indeed, bases of unitary number systems are referred to as *the universal side divisors* by Motzkin [12]. However, it seems rather a unfamiliar expression (c.f. Remark 5.11 in [3]). Thus we hopefully propose to use more tractable term, unitary number systems rather than universal side divisors.

By way of the concept of 'norm-Euclidean' we may more transparently restate the Motzkin's contribution to Euclidean rings of imaginary quadratic integers as follows:

Theorem 1.1.

Let R be a ring of imaginary quadratic integers. Then the following statements are equivalent.

(1) *R is Euclidean.*

(2) *R has a unitary number system.*

(3) *R is norm-Euclidean.*

Novelty of the proof for implication from (2) to (3) in Theorem 1.1 lies in the elementary observation that $N(b)$, the norm of b, is equal to the number of residue classes of $R/(b)$. One would immediately realize that it is much simpler and rudimentary than known proofs for the latter four principal ideal domains to be non-Euclidean.

Observing that any binary or ternary number systems in a Euclidean ring R of imaginary quadratic integers is necessarily unitary, we have a following characterization of R:

Theorem 1.2. *A ring R of imaginary quadratic integers admits binary or ternary number system if and only if R is Euclidean.*

The proofs of the theorems will be presented at the end of section 2.

2. Revisit to the Motzkin's contribution to Euclidean rings of imaginary quadratic integers

Let R be a ring of imaginary quadratic integers. It is well known that either

$$R = \mathbb{Z}\left[\sqrt{-d}\right] \text{ when } d \equiv 1, 2 \mod 4$$

or

$$R = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] \text{ when } d \equiv 3 \mod 4$$

for some square free positive integer d. For every $r \in R$, let N denote the norm defined by $N(r) = |r|^2 = r\bar{r}$ where $\bar{r}$ is the complex conjugate of r.

Let $R^\times$ be the multiplicative group of units of a ring R and $R_0^\times = R^\times \cup \{0\}$.

The following basic fact is well known; one can find the proof, some standard textbooks in algebraic number theory, for example [17].

Lemma 2.1. *Let R be a ring of imaginary quadratic integers. The group $R^\times$ of unities in R is listed as follow:*

(i) $R^\times = \{\pm 1, \pm i\}$ *for $R = \mathbb{Z}[i]$, where $i = \sqrt{-1}$;*

(ii) $R^\times = \{\pm 1, \pm\omega, \pm \omega^2\}$ *for $R = \mathbb{Z}[\omega]$, where $\omega = \frac{1+\sqrt{-3}}{2}$;*

(iii) *except for the above two cases, $R^\times = \{\pm 1\}$.*

Lemma 2.2. *Let R be a ring of imaginary quadratic integers. If $b \in R \setminus R_0^\times$, then the number of cosets modulo (b) equals to $N(b)$.*

Proof. Note that R forms a lattice, a discrete additive subgroup of $\mathbb{C}$ generated by an integral base $\{1, \theta\}$ where $\theta = \sqrt{-d}$ or $\frac{1+\sqrt{-d}}{2}$. Then an ideal $(b) = \{rb \,|\, r \in R\}$ forms a sub-lattice of generated by $\{b, b\theta\}$. Let T be a torus, namely a quotient group $\mathbb{C}/(b)$ and let F be the fundamental domain of T, a choice of representatives of T in $\mathbb{C}$. Then $R \cap F$ forms all residue classes modulo b. Thus the number of all residue classes modulo b equals to the area of F which equals to $N(b)$. □

For a ring R of imaginary quadratic integers, each element $b \in R \setminus R_0^\times$ contributes a base of a number system (b, D) by choosing a digit set

$$D = \{d_i \in R \,|\, d_1 = 0, d_2, \cdots, d_{N(b)}\}$$

consisting of a complete set of coset representatives of $R/(b)$. In particular, if D can be chosen to be a subset of $R_0^\times$, then a number system (b, D) is said to be *unitary*.

An integral domain R is said to be *Euclidean* if there exists a function ϕ from $R \setminus \{0\}$ to the set of positive integers such that for every $a, b \in R$, there exist $q, r \in R$ such that $a = qr + b$ with $r = 0$ or $\phi(r) < \phi(b)$. Such a function ϕ is called a *Euclidean function*. In particular, R is said to be *norm-Euclidean* if the norm $N(\cdot)$ of R is a Euclidean function. From the classifications of Euclidean rings of imaginary quadratic integers, the following result is well known; for example see [17].

Lemma 2.3. *Among the rings of imaginary quadratic integers, the five rings*

$$\mathbb{Z}\left[\sqrt{-1}\right],\ \mathbb{Z}\left[\sqrt{-2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right],\ \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right],$$

are norm-Euclidean.

We here briefly recall Motzkin's idea of dealing with Euclidean rings. Let $A_0 = \{0\}$. And inductively define A_n by the set of elements $r \in R$ such that every class modulo r has a representative in A_j for some $j < n$. Thus $A_1 = R^\times$. Then the Motzkin's criterion is that R is Euclidean if and only if $R = \cup_{n=0}^{\infty} A_n$.

We are now ready to give the proof of Theorem 1.1.

Proof. (1) $\Longrightarrow$ (2) : By Motzkin's criterion, we observe that there must be b in $R - R_0^\times = R - A_0 \cup A_1$ whose modulo classes have representatives in $R_0^\times$. Thus b forms a base of a unitary number system.

(2) $\Longrightarrow$ (3) : Suppose that R is not norm-Euclidean. Then, in the case when $R = \mathbb{Z}\left[\sqrt{-d}\right]$, we have $d > 3$ from Lemma 2.3. Thus for each $b = p + q\sqrt{-d} \in R \setminus R_0^\times$, since either $q \neq 0$ or $p \neq \pm 1$ we have

$$N(b) = p^2 + dq^2 > 3$$

in this case. In the other case when $R = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$, we have $d > 12$ also from Lemma 2.3. Therefore, in this case, for each $b = p + q\sqrt{-d} \in R \setminus R_0^\times$, since either $q \neq 0$ or $p \neq \pm 1$ it follows that

$$N(b) = \left(p + \frac{q}{2}\right)^2 + \frac{d}{4}q^2 > 3.$$

From Lemma 2.3, neither $R = \mathbb{Z}[i]$ nor $R = \mathbb{Z}[\omega]$. Therefore, $R^\times = \{\pm 1\}$ from Lemma 2.1. It follows from Lemma 2.2 that R has no unitary number systems.

(3) $\Longrightarrow$ (1) : Obvious. □

Lemma 2.4. *Let R be a ring of imaginary quadratic integers. If b is a base of a unitary number system in R, then $R/(b)$ is a finite field, whose order is one of* $2, 3, 4, 5$ *and* 7.

Proof. Let b be a base of a unitary number system in R. Each nonzero element of $R/(b)$ is of the form $u + (b)$ for some unit element u in $R^\times$. Then $1/u + (b)$ is the inverse of $u + (b)$. Therefore, the commutative ring $R/(b)$ is a field. It follows from Lemma 2.1 that the order of $R/(b)$ is not greater than 7. □

Lemma 2.5. (i) $\mathbb{Z}[i]$ *has a binary unitary number system.*

(ii) $\mathbb{Z}[\omega]$ *has a ternary unitary number system.*

Proof. (i) If $b = p + qi, (p, q \in \mathbb{Z})$ is a base of a unitary number system, then $N(b) = p^2 + q^2$ should be one of $2, 4$ or 5. Equation $N(b) = p^2 + q^2 = 2$ yields a solution $b = 1 + i$; $(p, q) = (1, 1)$. For any binary number system (b, D) in

$R = \mathbb{Z}[i]$, a digit set D, representatives of $R/(b)$ can be replaced by a subset of $R_0^\times$.

(ii) If $b = p + q\omega, (p, q \in \mathbb{Z})$ is a base of a unitary number system ,then $N(b) = p^2+pq+q^2$ should be one of $3, 4$ or 7. Equation $N(b) = p^2+pq+q^2 = 3$ yields a solution $b = 1 + \omega$; $(p, q) = (1, 1)$. For any ternary number system (b, D) in $R = \mathbb{Z}[\omega]$ representatives D of $R/(b)$ can be replaced by a subset of $R_0^\times$ because there are no elements $r \in R$ with $N(r) = 2$. □

Remark 1. All quaternary number systems in $\mathbb{Z}[i]$ are not unitary.

Proof. Note that equation $N(b) = p^2 + q^2 = 4$ yields a solution $b = 2; (p, q) = (2, 0)$ and the other solutions yield the associates of b. Since 2 is not prime in $\mathbb{Z}[i]$, $\mathbb{Z}[i]/(2)$ is not a field by Lemma 2.4. □

Observing that any binary or ternary number systems in a Euclidean ring of imaginary quadratic integers is necessarily unitary, we can now give a proof of Theorem 1.2.

Proof. Since 'only if' part follows from Theorem 1.1, we assume that R is Euclidean for 'if' part. If R is one of $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$, then it has binary or ternary number systems by Lemma 2.5. If R is none of the two examples, then $R^\times = \{\pm 1\}$ from Lemma 2.1 (iii). Since R is Euclidean, from Theorem 1.1 it follow that there exists a base b of a unitary number system. By Lemma 2.2, $N(b) \leq 3$, and so the number system is binary or ternary. □

References

[1] S. Akiyama and J.M. Thuswalender, *A Survey on Topological Properties of Tiles Related to Number Systems*, Geom. Dedica. **109** (2004), 89-105.

[2] O.A. Campoli, *A principal ideal domain that is not a Euclidean domain*, Amer. Math. Monthly, **95** (1988), no. 9, 868-871.

[3] K. Conrad, *Remarks about Euclidean domains*, an expository paper in Ring Thery.

[4] K. Falconer, *Fractal Geometry, Mathematical Foundations and Applications*, Wiley, (1990).

[5] D. Goffinet, *Number systems with a complex base: a fractal tool for teaching topology*, Amer. Math. Monthly **98** (1991), no. 3, 249255.

[6] L. Guillen, *A principal ideal domain that is not a Euclidean domain*, a personal note in website.

[7] K. Groechenig and W.R. Madych, *Multiresolution Analysis, Haar bases and self-similar tilings of R^n*, IEEE Trans. Inform. Th. **38(2)** Part2 (2)(1992), 556-568.

[8] S.I. Khmelnik, *Specialized digital computer for operations with complex numbers*, Questions of Radio Electronics (in Russian) XII (2)(1964).

[9] S.I. Khmelnik, *Positional coding of complex numbers*, Questions of Radio Electronics (in Russian) XII (9)(1966).

[10] D.E. Knuth, *An Imaginary Number System*, Communication of the ACM-3 (4) (1960).

[11] N. Koblitz, *CM-curves with good cryptographic properties*, Advances in Cryptology-CRYPTO '91', LNCS **576**, 1992, 279-287.

[12] T. Motzkin, *The Euclidean Algorithm*, Bull. Amer. Math. Soc., **55** (1949), 1142-1146.

[13] W. Penney, *A "binary" system for complex numbers*, JACM **12** (1965) 247-248.

[14] A. Petho, *On a polynomial transformation and its application to the construction of a public key cryptosystem*, Computational Number Theory, Proc., Walter de Gruyter Publ. Comp., Eds.: A. Petho and etals, (1991), 31-44.

[15] H.M. Stark, *A complete determination of the complex quadratic fields of class number one*, Michigan Math. J. **14** (1967), 1-27.

[16] H.J. Song and B.S. Kang, *Disclike Lattice Reptiles induced by Exact Polyominos*, Fractals , **7** (1999), no. 1, 9-22.

[17] I. Stewart, D. Tall, *Algebraic Number Theory*, Chapman and Hall Mathematics Series, Second Edition.

[18] K.S. Williams, *Note on non-Euclidean principal ideal domains*, Amer. Math. Monthly , **48**(1975), no. 3, 176-177.

[19] Jack C. Wilson, *A Principal Ring that is Not a Euclidean Ring*, Math. Mag. **46** (Jan 1973), 34-38.

Hyo-Seob Sim

Department of Applied Mathematics, Pukyong National University, Pusan 608-737, Korea

E-mail address: hsim@pknu.ac.kr

Hyun-Jong Song

Department of Applied Mathematics, Pukyong National University, Pusan 608-737, Korea

E-mail address: hjsong@pknu.ac.kr