Acta Mathematica Academiae Scientiarum Hungaricae
Tomus 37 (1—3), (1981), 159—164.

CANONICAL NUMBER SYSTEMS IN IMAGINARY QUADRATIC FIELDS

By

I. KÁTAI (Budapest), corresponding member of the Academy and B. KOVÁCS (Debrecen)

Dedicated to A. Rapcsák on his 65th anniversary

1. Let R be the field of rational numbers, $R(\vartheta)$ its extension generated by ϑ; let $R[\vartheta]$ denote the integers of $R(\vartheta)$. For an integer $\gamma \in R[\vartheta]$ let $\mathcal{N}_0 = \mathcal{N}_0(\gamma)$ denote the set $\{0, 1, \ldots, |N(\gamma)|-1\}$, $N(\cdot)$ is the norm function.

We say that $\{\gamma, \mathcal{N}_0\}$ is a canonical number system (CNS), if for every $\alpha \in R[\vartheta]$ there exists a unique representation of the form

$$\alpha = a_0 + a_1\gamma + \ldots + a_n\gamma^n \quad (a_i \in \mathcal{N}_0, \quad i = 0, \ldots, n). \tag{1.1}$$

The problem of characterizing the CNS in various rings seems to be quite interesting. Previously this problem was considered and settled for rational integers [1], for Gaussian integers [2] and for the quadratic real fields [3].

Now we determine all the CNS in imaginary quadratic fields.

THEOREM 1. *Let* $N \geqq 2$, $-N \not\equiv 1 \pmod 4$. $\{\alpha, \mathcal{N}_0\}$ *is a* CNS *in* $R(i\sqrt{N})$ *if and only if*

$$\alpha = A \pm i\sqrt{N}, \quad 0 \leqq -2A \leqq A^2 + N \geqq 2, \quad A \text{ is integer.} \tag{1.2}$$

Let $N \geqq 2$, $-N \equiv 1 \pmod 4$. $\{\alpha, \mathcal{N}_0\}$ *is a* CNS *if and only if*

$$\alpha = \frac{1}{2}(B \pm i\sqrt{N}), \quad -1 \leqq -B \leqq \frac{1}{4}(B^2 + N) \geqq 2, \quad B \text{ is an odd integer.} \tag{1.3}$$

THEOREM 2. *If* $\{\alpha, \mathcal{N}_0\}$ *is a* CNS *in* $R[\sqrt{N}]$, *then every complex number* z *can be written as*

$$z = \sum_{i=k}^{-\infty} a_i \alpha^i \quad (a_i \in \mathcal{N}_0, \ i = k, k-1, \ldots). \tag{1.4}$$

2. Lemmas. For square-free M the discriminant D of $R(\sqrt{M})$ is $4M$ or M according to $M \not\equiv 1 \pmod 4$ or $M \equiv 1 \pmod 4$, respectively.

If $\{\alpha, \mathcal{N}_0\}$ is a CNS, then $\{1, \alpha\}$ has to be a basis there and $|N(\alpha)| > 1$, as it is easy to see.

LEMMA 1. *If* $\{\alpha, \mathcal{N}_0\}$ *is a* CNS, *then* $\{1, \alpha\}$ *is an integer basis in* $R(i\sqrt{N})$.

The proof is the same as the proof of Lemma 1 in [3], and so we omit it. By an easy computation of the discriminant of the basis $\{1, \alpha\}$ we get, that $\{1, \alpha\}$

is an integer basis (IB) in $R(i\sqrt{N})$ if and only if:

(2.1) $\alpha=A\pm i\sqrt{N}$, A integer (in the case $-N\equiv 1 \bmod 4$);

(2.2) $\alpha=\frac{1}{2}(B\pm i\sqrt{N})$, B odd integer (in the case $-N\equiv 1 \bmod 4$).

In these cases α is a root of the corresponding polynomial

(2.1)′ $$x^2-2Ax+(A^2+N),$$

(2.2)′ $$x^2-Bx+\frac{1}{4}(B^2+N).$$

LEMMA 2. *Let* $\{1, \alpha\}$ *be an* IB *in* $R(i\sqrt{N})$, α *a root of* x^2+Ux+V, *where* $0<U\leqq V\geqq 2$, U, V *rational integers. Then* $\{\alpha, \mathcal{N}_0\}$ *is a* CNS.

PROOF. See the proof of Lemma 5 in [3].

LEMMA 3. $\{\alpha, \mathcal{N}_0\}$ *is a* CNS *in* $R(i\sqrt{N})$ *if and only if* $\{\bar{\alpha}, \mathcal{N}_0\}$ *is a* CNS.

PROOF. See the proof of Lemma 6 in [3].

LEMMA 4. *Let* γ *be an integer such that every* $\beta\in R(i\sqrt{N})$ *has at least one representation of the form*

(2.3) $$\beta=\sum_{i=0}^{n} a_i\gamma^i, \quad a_i\in\mathcal{N}_0.$$

Then $\{\gamma, \mathcal{N}_0\}$ *is a* CNS.

PROOF. We have to prove only that (2.3) is unique. Suppose in the contrary that there exists a β having two representations

$$\beta=r_0+r_1\gamma+\ldots+r_k\gamma^k \quad \text{and} \quad \beta=s_0+s_1\gamma+\ldots+s_l\gamma^l.$$

Assuming that $r_0\geqq s_0$, we get

(2.4) $$0=(r_0-s_0)+(r_1-s_1)\gamma+\ldots.$$

Since $\gamma|(r_0-s_0)$ and $r_0-s_0\in\mathcal{N}_0$, therefore $r_0=s_0$. After dividing by γ in (2.4) we get $r_1=s_1$, etc.

LEMMA 5. *Let* $N>3$ *be square-free,* $-N\equiv 1 \pmod 4$. *Then* $\left\{\frac{1}{2}(1\pm i\sqrt{N}), \mathcal{N}_0\right\}$ *is a* CNS *in* $R\left[\frac{1}{2}(1+i\sqrt{N})\right]$, *i.e. in* $R[i\sqrt{N}]$.

PROOF. Let $\alpha=\frac{1}{2}(1+i\sqrt{N})$, $k=\frac{1}{4}(1+N)$. We have $k\geqq 2$, since $N>3$. It is obvious that $\alpha^2-\alpha+k=0$ and $\{1, \alpha\}$ is an IB in $R(\alpha)$. So we have $R[\alpha]=R[i\sqrt{N}]$. We define $a(\gamma)$ for $\gamma=A+B\alpha\in R[\alpha]$ by $|A|+|B|$. So $a(\gamma)\geqq 0$ takes on integer values and $a(\gamma)=0$ iff $\gamma=0$.