Connections between power integral bases and radix representations in algebraic number fields

Attila Pethő*
Institute of Informatics, University of Debrecen,
P.O. Box 12, H-4010 Debrecen, HUNGARY
email:pethoe@inf.unideb.hu

November 19, 2009

1 Radix representation in algebraic number fields

Let $g \geq 2$ be an integer. Then every $n \in \mathbb{Z}$ can be represented in the form

$$n = \pm \sum_{j=0}^{\ell} n_i g^i, \quad 0 \leq n_i < g.$$

This classical representation has a disadvantage that it cannot be generalized to more general algebraic structures (e.g. to algebraic number fields), because there exists no natural separation between positive and negative elements. V. Grünwald [7] introduced the radix representation with respect to negative bases on the following way: Let $g \leq -2$ be an integer. Then every $n \in \mathbb{Z}$ can be represented in the form

$$n = \sum_{j=0}^{\ell} n_i g^i, \quad 0 \leq n_i < |g|.$$

This concept does not use the dichotomy of positive and negative numbers and allows a far reaching generalization, which was started by Knuth [12], see also [13] and worked out by Kátai and Szabó [11], Kátai and B. Kovács [9, 10] and by Gilbert [6]. Let $\mathbb{Z}_{\mathbb{K}}$ be the ring of integers of the algebraic number field $\mathbb{K}$.

$$\{\alpha, \mathcal{N}\}; \quad \alpha \in \mathbb{Z}_{\mathbb{K}}, \quad \mathcal{N} = \{0, \ldots, |Norm(\alpha)| - 1\}$$

*The author was supported partially by the Hungarian National Foundation for Scientific Research Grant Nos. T42985 and T38225, as well as HAS-JSPS bilateral project RC20318007

is called a *canonical number system*, in short CNS, if every $\nu \in \mathbb{Z}_{\mathbb{K}}$ can be represented in the form

$$\nu = \sum_{j=0}^{\ell} n_i \alpha^i, \quad n_i \in \mathcal{N}.$$

Remark that Gilbert used the notion of radix representation instead of canonical number system. In this note we follow the Hungarian tradition.

2 CNS polynomials

To characterize bases of canonical number systems it is useful to generalize the concept. Observe that if $\mathbb{Z}_{\mathbb{K}}$ is monogenic then $\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathbb{Z}_{\mathbb{K}}$. This means $\mathbb{Z}_{\mathbb{K}}$ is isomorphic to the quotient ring $\mathbb{Z}[x]/P(x)\mathbb{Z}[x]$, where $P(x)$ is the minimal polynomial of α. Moreover, $\{\alpha, \mathcal{N}\}$ is a CNS in $\mathbb{Z}_{\mathbb{Q}(\alpha)}$ means nothing else that every coset of $\mathbb{Z}[x]/P(x)\mathbb{Z}[x]$ has an element (a representative) such that its coefficients belong to the interval $[0, |p_0| - 1]$. This point of view does not depend on the algebraic number field $\mathbb{Q}(\alpha)$, but only on the polynomial $P(x)$!

A monic polynomial $P(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_0$ is called CNS polynomial if every coset of $\mathbb{Z}[x]/P(x)\mathbb{Z}[x]$ has an element

$$a_0 + a_1 x + \cdots + a_k x^k \tag{1}$$

such that $0 \leq a_i < |p_0|$.

The set of CNS polynomials of degree d will be denoted by $\mathcal{C}_d$ and (1) will be called a *CNS representation*.

3 Algorithmic properties of $\mathcal{C}_d$.

The first problem is to find a method, with which it is possible to compute the CNS representation of elements $\mathbb{Z}[x]/P(x)\mathbb{Z}[x]$ with respect to a given polynomial $P(x) = p_d x^d + p_{d-1}x^{d-1} + \cdots + p_0 \in \mathbb{Z}[x]$ with $p_d = 1$. As every coset of $\mathbb{Z}[x]/P(x)\mathbb{Z}[x]$ has a unique element of degree $d-1$ with integer coefficients say

$$A_0 + A_1 x + \cdots + A_{d-1} x^{d-1} \tag{2}$$

it is natural to use the following process. Let $\mathbb{Z}'[x] = \{A(x) \in \mathbb{Z}[x] \ : \ \deg A < d\}$ and

$$T_P(A) = \sum_{i=0}^{d-1} (A_{i+1} - q p_{i+1}) x^i,$$

where $A_d = 0$ and $q = [A_0/p_0]$. Then $T_P \ : \ \mathbb{Z}'[x] \to \mathbb{Z}'[x]$ and

$$A = a_0 + x T_P(A), \text{ with } a_0 = A_0 - q p_0 \in \{0, \ldots, |p_0| - 1\}.$$

A polynomial $A \in \mathbb{Z}'[x]$ is called a periodic point of T_P, if there exists an integer $k > 0$ such that $T_P^k(A) = A$. It is very easy to prove our first statement.

Theorem 1. *$P(x) \in \mathcal{C}_d$ if and only if the only periodic point of the mapping T_P is the zero polynomial.*

Hence it is enough to study the map $T_P : \mathbb{Z}^d \to \mathbb{Z}^d$ defined as

$$T_P((A_0, \ldots, A_{d-1})) = (A_1 - qp_1, \ldots, A_d - qp_d).$$

The next theorem gives sufficient conditions for $P(x)$ to be an element of $\mathcal{C}_d$.

Theorem 2 (Analytical conditions)**.** *If $P(x) \in \mathcal{C}_d$ then*

(i) $|\alpha| > 1$ *for all roots of $P(x)$ and*

(ii) $\alpha < -1$ *for all real roots of $P(x)$.*

Proof (i) If $|\alpha| < 1$ for a root of $P(x)$ then the sum

$$|n_0 + n_1\alpha + \cdots + n_k\alpha^k|,\ n_i \in \mathcal{N}$$

is bounded.
(ii) If $\alpha > 0$ for a real root of $P(x)$ then the sum

$$n_0 + n_1\alpha + \cdots + n_k\alpha^k,\ n_i \in \mathcal{N}$$

is always non-negative.

Corollary 1. *If $P(x) \in \mathcal{C}_d$ then $p_0 \geq 2$ and for given d and p_0 there exist only finitely many CNS polynomials of degree d and with constant term p_0.*

4 Early characterization results

The next theorem is due to Kátai and Szabó [11] for the ring of Gaussian integers and Kátai and B. Kovács [9, 10] in the general case. It was proved independently by Gilbert [6]. Thuswaldner [22] gave a different proof based on the theory of automata.

Theorem 3. *Let $x^2+p_1x+p_0$ be the minimal polynomial of α. The pair $\{\alpha, \mathcal{N}\}$ is a CNS in $\mathbb{Z}_{\mathbb{Q}(\alpha)}$ if and only if $p_0 \geq 2$ and $0 \leq p_1 \leq p_0$.*

Later B. Kovács [15] proved the following useful theorem. A different proof was given by Scheicher [20] using the theory of transducer automata.

Theorem 4. *Let $P(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_0$ be the minimal polynomial of α. If $p_0 \geq 2$ and $p_{d-1} \leq \cdots \leq p_1 \leq p_0$ then $\{\alpha, \mathcal{N}\}$ is a CNS in $\mathbb{Z}_{\mathbb{Q}(\alpha)}$.*

Proof: Let $A(x) \in \mathbb{Z}[x]/P\mathbb{Z}[x]$ be of degree at most d. Adding a suitable multiple of $P(x)$ to $A(x)$ we can achieve that all of the coefficients of $A(x)$ are non-negative, which we will assume in the sequel. Let $A(x) = a_0+a_1x+\cdots+a_dx^d$ and $q = [a_0/p_0]$. Then

$$A(x) - qP(x) + xqP(x) = (a_0 - qp_0) + \sum_{i=1}^{d}(a_i - qp_i + qp_{i-1})x^i + qx^{d+1}$$

and $a_0 - qp_0 \in \mathcal{N}$. Let

$$\tilde{T}_P(A) = \sum_{i=1}^{d} (a_i - qp_i + qp_{i-1}) x^{i-1} + qx^d.$$

Then $A \equiv a_0 - qp_0 + x\tilde{T}_P(A) \pmod{P}$, the degree of $\tilde{T}_P(A)$ is d and the coefficients of $\tilde{T}_P(A)$ are non-negative. Moreover the sum of the coefficients of $\tilde{T}(A)$ is equal to the sum of the coefficients of A minus $a_0 - qp_0$. Hence this function is decreasing whenever $a_0 - qp_0 > 0$. Iterating this process we arrive after finitely many steps the zero polynomial. □

The next theorem gives a qualitative characterization of canonical number systems.

Theorem 5 (B. Kovács [15])**.** *There exists in $\mathbb{Z}_\mathbb{K}$ a CNS if and only if $\mathbb{Z}_\mathbb{K}$ is monogenic, i.e. there exists an $\alpha \in \mathbb{Z}_\mathbb{K}$ such that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an integral basis in $\mathbb{Z}_\mathbb{K}$.*

Proof: If $\{\alpha, \mathcal{N}\}$ is a CNS in $\mathbb{Z}_\mathbb{K}$ then $\mathbb{Z}_\mathbb{K}$ is obviously monogenic.
Let α be a basis element of a power integral basis in $\mathbb{Z}_\mathbb{K}$ and denote by $P(x)$ its minimal polynomial. Then there exists a k_0 such that the coefficients of $P(x+k)$ for $k \geq k_0$ are positive and monotonically increasing. By the last theorem $\{\alpha - k, \mathcal{N}_{\alpha-k}\}$ is a CNS in $\mathbb{Z}_\mathbb{K}$. □

Combining this theorem with a deep result of Győry [8] B. Kovács obtained.

Corollary 2. *Up to translation by integers there exist only finitely many CNS in $\mathbb{Z}_\mathbb{K}$.*

Based on this result the following strategy was proposed by Kovács and Pethő [16] to find all CNS in $\mathbb{Z}_\mathbb{K}$ for a given $\mathbb{K}$:

(i) Find, up to translation, the bases of power integral bases of $\mathbb{Z}_\mathbb{K}$. Let α one of them with minimal polynomial $P(x)$.

(ii) Find the smallest k_1 such that the coefficients of $P(x+k)$ are positive and increasing for all $k \geq k_1$.

(iii) Find the largest $k_0 \leq k_1$ such that the roots of $P(x+k_0)$ satisfy the analytical conditions, i.e. they are in absolute value larger than one and the real roots are less than -1.

(iv) Test the remaining, finitely many polynomials, whether they are CNS.

To test conditions (i)-(iii) is easy, therefore we concentrate in the sequel to condition (iv). For monic $P(x) \in \mathbb{Z}[x]$ and for $c > 0$ let

$$P_c = \{A(x) = \sum_{i=0}^{d-1} A_i x^i \in \mathbb{Z}'[x] \ : \ |A_i| \leq c, 0 \leq d-1\}.$$

Theorem 6 (Kovács and Pethő [16]). *Let $P(x)$ be irreducible and square-free for which the analytical conditions hold. Then there exists a computable constant $c > 0$ such that $P(x) \in \mathcal{C}_d$ if and only if every $A(x) \in P_c$ has a CNS representation.*

Pethő [19] generalized this theorem for the case when $P(x)$ is not necessarily irreducible and Akiyama and Rao [3] removed the square-freeness too. The last theorem means that the CNS property is algorithmically decidable. On the other hand the decision procedure can be, and often is, very time consuming.

5 CNS polynomials with large p_0

At the end of the 20-th century Akiyama and Pethő [2] realized that if p_0 is dominating among the other coefficients, then the polynomial is CNS. More precisely they proved the following theorems:

Theorem 7 (Akiyama and Pethő [2]). *For polynomials with $p_0 \geq \sum_{i=1}^{d} |p_i|$ the CNS property can be decided in polynomial time.*

Theorem 8 (Akiyama and Pethő [2]). *Assume that $p_2, \ldots, p_{d-1}, \sum_{i=1}^{d} p_i \geq 0$ and $p_0 > 2\sum_{i=1}^{d} |p_i|$ then $P(x) \in \mathcal{C}_d$.*

The statement of the last theorem was refined by Scheicher and Thuswaldner [21] and Akiyama and H. Rao [3] to $p_0 > \sum_{i=1}^{d} |p_i|$.

6 Affect of a new representation

Brunotte [5] and independently Scheicher and Thuswaldner [21] observed that the basis transformation

$$\begin{aligned} \{1, x, \ldots, x^{d-1}\} &\rightarrow \{w_1, \ldots, w_d\}, \\ w_j &= \sum_{i=j}^{d} p_i x^{i-j}, j = 1, \ldots, d \end{aligned}$$

implies a simpler and much nicer transformation. Indeed, if

$$\begin{aligned} A(x) &= \sum_{j=1}^{d} \bar{A}_j w_j \quad \text{then} \\ T_P(A) &= -qw_1 + \sum_{j=2}^{d} \bar{A}_{j-1} w_j. \end{aligned}$$

Hence T_P implies the mapping

$$\begin{aligned} \tau_P &= \tau : \mathbb{Z}^d \rightarrow \mathbb{Z}^d \\ \tau(\underline{A}) &= \left(-\left[\frac{p_1 A_1 + \cdots + p_d A_d}{p_0} \right], A_1, \ldots, A_{d-1} \right), \end{aligned}$$

where $\underline{A} = (A_1, \ldots, A_d)$. This will be called in the sequel **Brunotte's mapping**.
Brunotte [5] proved the following theorem.

Theorem 9. *Assume that $E \subseteq \mathbb{Z}^d$ has the following properties*

- $(1, 0, \ldots, 0) \in E$,
- $-E \subseteq E$,
- $\tau(E) \subseteq E$,
- *for every $e \in E$ there exists some $\ell > 0$ with $\tau^\ell(e) = 0$*

then $P(x) \in \mathcal{C}_d$.

Such a set E will be called the **set of witnesses** of $P \in \mathcal{C}_d$.

7 Trinomials

The quadratic CNS polynomials were characterized by Kátai and B. Kovács [9, 10] and independently by Gilbert [6]. Scheicher [20] and Brunotte [5] gave new proofs.

Theorem 10. *We have $x^2+p_1x+p_0 \in \mathcal{C}_2$ if and only if $p_0 \geq 2$ and $0 \leq p_1 \leq p_0$.*

Brunotte [5] generalized this statement to higher degree trinomials.

Theorem 11. *Let $d > 2$. Then*
(i) $x^d + bx + c$ belongs to $\mathcal{C}_d$ if and only if $-1 \leq b \leq c - 2$,
(ii) if $1 \leq q \leq d$ and $q \not| d$ then $x^d + bx^q + c \in \mathcal{C}_d$ if and only if $0 \leq b \leq c - 2$.

8 Cubic polynomials

After characterizing the CNS in quadratic number fields and trinomials, whose roots are bases of CNS in the corresponding number fields it is straightforward to analyze the situation for cubic fields. We will show that this problem is much more complicated as the trinomial case and is far from a complete solution.

Let $P(x) = x^3+p_2x^2+p_1x+p_0$. In 1981 Gilbert [6] formulated the following conjecture.

Conjecture 1. *We have $P \in \mathcal{C}_3$ if and only if*
(i) $p_0 \geq 2$,
(ii) $p_2 \geq 0$,
(iii) $p_1 + p_2 \geq -1$,
(iv) $p_1 - p_2 \leq p_0 - 2$,
(v) $p_2 \leq \begin{cases} p_0 - 2, & \text{if } p_1 \leq 0, \\ p_0 - 1, & \text{if } 1 \leq p_1 \leq p_0 - 1, \\ p_0, & \text{if } p_1 \geq p_0. \end{cases}$

Akiyama, Brunotte and Pethő [1] confirmed his conjecture in several cases. For example they proved the following statement.

Proposition 1. *Let*
(i) $p_1 \leq -1$, $p_2 \leq p_0 - 2$ *and* $-1 \leq p_1 + p_2 \leq 0$ *or*
(ii) $p_1 \leq -1$, $0 \leq p_2 < \min\{p_0 - 1, 2p_0/3\}$ *and* $1 + p_1 + p_2 \geq 0$ *or*
(iii) $1 + p_1 + p_2 \geq 0$, $-p_0 + p_2 + 1 \leq p_1 \leq -1$
then $P \in \mathcal{C}_3$.

Summarizing we obtain that Gilbert's conjecture holds if $p_1 = -1$. On the other hand they realized (see also [4]) that Gilbert's conditions are **not sufficient**. They presented the following counterexamples.

Counterexamples. *(i)* $\mathbf{p_1 \leq 0}$.
Let $2 \leq p_1 + p_2 \leq -p_1$ and $p_0 \leq \min\{p_2 - p_1, p_1 + 2p_2 + 1\}$ then $(1, -1, -1)$ is periodic and the period is always $(1, -1, -1); 2, 1, -1, -1$.

(ii) $\mathbf{1 \leq p_1 \leq p_0 - 1}$.
Let $\frac{7p_0 - 5p_2}{6} + 1 \leq p_1 \leq -p_0 + \frac{3}{2}p_2$. Then $(1, -3, 1)$ is periodic with period $(1, -3, 1); 3, -2, -2, 3, 1, -3$ provided that $p_0 \geq 28$.

(iii) $\mathbf{p_1 > p_0}$.
Let $p_0 + \frac{1}{2}p_2 + 1 \leq p_1 < p_0 + \frac{2}{3}p_2 - \frac{1}{3}$. Then $(3, -2, 1)$ is periodic with period $(3, -2, 1); -2, 1, 1, -2$. The same point is periodic, but with period $(3, -2, 1); -3, 3, -2, 1, 1, -2$, provided that $p_0 + \frac{2}{3}p_2 - \frac{1}{3} \leq p_1 \leq 2p_2 - 4$.

9 Binary CNS polynomials

A CNS polynomial is called *binary* if its constant term is 2. A. Kovács [14] computed all binary CNS polynomial up to degree 8. His results are summarized in the next table.

Degree	3	4	5	6	7	8
Number of CNS Polynomials	4	12	7	25	12	20

He proved for example that $x^8+2x^7+3x^6+3x^5+3x^4+3x^3+3x^2+3x+2 \in \mathcal{C}_8$. In this case the number of elements of the set of witnesses E is 241719.

10 CNS in cubic number fields

Combining results of diophantine equations and the strategy described in Section 3 Akiyama, Brunotte and Pethő [1] described in two infinite classes of cubic number fields all CNS.

Simplest cubic fields: Let $t > 0$, let $\vartheta = \vartheta_1$ be the root of $X^3 - tX^2 - (t + 3)X - 1$ with $t + 1 < \vartheta < t + 1 + 1/t$.

Theorem 12. *An element $\gamma \in \mathbb{Z}[\vartheta]$ is the basis of a CNS in $\mathbb{Z}[\vartheta]$ if and only if*
$\gamma = \vartheta + n, n \leq -t - 3$,
$\gamma = -\vartheta + n, n \leq -3$,
$\gamma = \vartheta^2 - t\vartheta + n, n \leq -t - 5$,
$\gamma = -\vartheta^2 + t\vartheta + n, n \leq -1$,
$\gamma = \vartheta^2 - (t+1)\vartheta + n, n \leq -t - 5$,
$\gamma = -\vartheta^2 + (t+1)\vartheta + n, n \leq -1$.

Pure cubic fields:

Theorem 13. *Let m be a positive integer not divisible by 3 such that $d = m^3 + 1$ is square-free. Put $\vartheta = \sqrt[3]{d}$. Then $\gamma \in \mathbb{Z}[\vartheta]$ is the basis of a CNS in $\mathbb{Z}[\vartheta]$ if and only if*
$\gamma = \vartheta + n, n \leq -m - 2$,
$\gamma = -\vartheta + n, n \leq 0$,
$\gamma = \vartheta^2 + m\vartheta + n, n \leq -2m^2 - 2$,
$\gamma = -(\vartheta^2 + m\vartheta) + n, n \leq -m^2 - 2$.

The last theorem is a generalization of a statement of Körmendi [17], where he considered the case $m = 1$. His result was completed by Brunotte [5].

11 CNS in a family of quartic number fields

For a class of quartic number fields Y. Motoda [18] established all power integral bases.

Theorem 14. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with $m = f^2 + 2, n = f^2 - 2$ and $f > 0$ odd. Then the generators of a power integral basis of $\mathbb{Z}_{\mathbb{K}}$ are equivalent to*
$\vartheta_1 = \frac{\sqrt{m}+\sqrt{n}}{2}$ *or*
$\vartheta_2 = f\frac{1+\sqrt{mn}}{2} + \sqrt{n} + (f^2 - 1)\frac{\sqrt{m}+\sqrt{n}}{2}$.

Using this theorem and the general strategy described in Section 3 to find all CNS in $\mathbb{Z}_{\mathbb{K}}$ we proved during our stay in Japan in 2003 the following result.

Theorem 15. *Let $\mathbb{K}$ as above. Then $\{\alpha, \mathcal{N}\}$ is a CNS in $\mathbb{Z}_{\mathbb{K}}$ if and only if*
(i) $\alpha = \vartheta_1 - k, k \geq f + 1$,
(ii) $\alpha = \vartheta_2 - k, k \geq \frac{3f^3+f}{2} + 1$,
(iii) $\alpha = -\vartheta_2 - k, k \geq \frac{f^3-f}{2} + 2$,

Proof: (i) We have $P_{\vartheta_1}(x) = x^4 - f^2x^2 + 1$. If $k \geq f + 1$ then $\vartheta_1^{(i)} - k < -1$. A simple computation leads to

$$\begin{aligned} P_{\vartheta_1}(x + f + 1) &= x^4 + (4f+4)x^3 + (5f^2 + 12f + 6)x^2 + (2f^3 + 10f^2 + 12f + 4)x \\ &+ 2f^3 + 5f^2 + 4f + 2. \end{aligned}$$

Let $p_i, i = 0, 1, 2, 3$ denote the coefficient of x^i in the last expression. Observing that $p_0 = p_1 - p_2 + p_3$ it is easy to see that if $a \geq 1$ then

$$\tau(-a, a-1, -a+2, a-3) = \begin{cases} (a+1, -a, a-1, -a+2), & \text{if } a < p_2 - 2p_3 + 3 \\ (a, -a, a-1, -a+2), & \text{otherwise.} \end{cases}$$

Starting from $(-1, 0, 0, 0)$ we arrive after some steps, which depend on f, the case $a \geq p_2 - 2p_3 + 3$. Later the first coordinate of the argument vector does not grow in absolute value. Finally it is easy to see that applying the iterates of τ to the vector $(a, -a, a-1, -a+2)$ we obtain after finitely many steps the zero vector. By Theorem 9 of Brunotte $P_{\vartheta_1}(x + f + 1)$ is a CNS polynomial.

(ii) This is obvious.

(iii) With $P(x) = P_{\vartheta_2}(-x - \frac{f^3-f}{2} - 1)$ we have

$$\begin{aligned} P(x) &= x^4 + (2f^3 + 4)x^3 + (6f^3 + 5f^2 + 6)x^2 + (6f^3 + 10f^2 + 4f + 4)x \\ &+ 2f^3 + 5f^2 + 4f + 2. \end{aligned}$$

This polynomial is not CNS, because τ has a period

$$(-2, 2, -1, 0); 2, -1, 0, 1, -1, 1, -1, 1, 0, -1, 2, -2$$

.

However with $P(x) = P_{\vartheta_2}(-x - \frac{f^3-f}{2} - 2)$ we have

$$\begin{aligned} P(x) &= x^4 + (2f^3 + 8)x^3 + (12f^3 + 5f^2 + 24)x^2 + (24f^3 + 20f^2 + 4f + 52)x \\ &+ 16f^3 + 20f^2 + 8f + 17. \end{aligned}$$

This is already a CNS polynomial with a set of witnesses, which is independent from f.

References

[1] S. Akiyama, H. Brunotte and A. Pethő, *Cubic CNS polynomials, notes on a conjecture of W.J. Gilbert*, J. Math. Anal. and Appl., **281** (2003), 402–415.

[2] S. Akiyama and A. Pethő, *On canonical number systems*, Theoret. Comput. Sci., **270** (2002), 921 - 933.

[3] S. Akiyama and H. Rao, *New criteria for canonical number systems*, Acta Arith., to appear.

[4] T. Borbély, *Generalized number systems*, (in Hungarian), Master Thesis, University of Debrecen, 2003.

[5] H. Brunotte, *On trinomial bases of radix representations of algebraic integers*, Acta Sci. Math. (Szeged), **67** (2001), 521-527.

[6] W. J. Gilbert, *Radix representations of quadratic fields*, J. Math. Anal. Appl., **83** (1981), 264-274.

[7] V. Grünwald, *Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale)*, Giornale di matematiche di Battaglini, **23** (1885), 203-221, 367.

[8] K. Győry, *Sur les polynomes a coefficients entiers et de discriminant donne, III*, Publ. Math. (Debrecen), **23** (1976), 141-165.

[9] I. Kátai and B. Kovács, *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*, Acta Sci. Math. (Szeged), **42** (1980), 99-107.

[10] I. Kátai and B. Kovács, *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar., **37** (1981), 159-164.

[11] I. Kátai and J. Szabó, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged), **37** (1975), 255-260.

[12] D. E. Knuth, *An imaginary number system*, Comm. ACM, **3** (1960), 245-247.

[13] D. E. Knuth, *The Art of Computer Programming, Vol. 2 Semi-numerical Algorithms*, Addison Wesley (1998) London 3rd-edition.

[14] A. Kovács, *Generalized binary number systems*, Ann. Univ. Sci. Budap. Rolando Etvös, Sect. Comput., **20** (2001), 195-206.

[15] B. Kovács, *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar., **37** (1981), 405-407.

[16] B. Kovács and A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields,* Acta Sci. Math. (Szeged), **55** (1991) 287–299.

[17] S. Körmendi, *Canonical number systems in* $\mathbb{Q}(\sqrt[3]{2})$, Acta Sci. Math. (Szeged), **50** (1986), 351-357.

[18] Y. Motoda, *On the Power Bases of Trivial Real Monogenic Biquadratic Fields*, manuscript, 2003.

[19] A. Pethő, *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. Pethő, M. Pohst, H.G. Zimmer and H.C. Williams, 1991, pp 31-43.

[20] K. Scheicher, *Kanonische Ziffernsysteme und Automaten,* Grazer Math. Ber., **333** (1997), 1-17.

[21] K. Scheicher and J. M. Thuswaldner, *On the characterization of canonical number systems*, Osaka J. Math., to appear.

[22] J. M. Thuswaldner, *Elementary properties of canonical number systems in quadratic fields*, Applications of Fibonacci Numbers, Volume 7, G. E. Bergum et al. (eds.), Kluwer Academic Publishers (1998) 405–414.