Internat. J. Math. & Math. Sci.
Vol. 3 No. 1 (1980) 15-28

ON BLOCK IRREDUCIBLE FORMS OVER EUCLIDEAN DOMAINS

W. EDWIN CLARK and J.J. LIANG
Department of Mathematics
University of South Florida
Tampa, Florida 33620 U.S.A.

(Received December 11, 1978)

ABSTRACT. In this paper a general canonical form for elements in a ring Euclidean with respect to a real valuation is established. It is also shown that this form is unique and minimal thus gives the arithmetical weight of an element with respect to a radix.

KEY WORDS AND PHRASES. *Euclidean Domains, Canonical Forms, Arithmetical Coding.*
1980 MATHEMATICS SUBJECT CLASSIFICATION CODES. 94A10.

1. INTRODUCTION.

In this paper we shall establish a general canonical form for elements in a ring Euclidean with respect to a real valuation. We show this form is unique and minimal and thus gives us the arithmetical weight of an element with respect to a radix r.

Throughout R will denote a commutative ring Euclidean for a real valuation v satisfying:

(i) $v(R)$ is well-ordered by the usual ordering of the real numbers.

(ii) for $a, b \neq 0$ in R, there exists q, r in R such that $a = bq + r$ and $v(r) < v(b)$.

For completeness we recall that an element r of R is called a radix (or a base) for R if every element a of R can be represented as a finite sum of the form

$$a = \sum a_i r^i \qquad \text{where } v(a_i) < v(r) \tag{1.1}$$

and we call such a representation a weak radix-r form (or representation) for a. For convénience we often write $a = (a_{n-1},\ldots,a_0)$ or $a_{n-1},\ldots,a_1 a_0$ in lieu of (1.1). The form (1.1) is said to be a minimal weak radix form for a if the number of indices i with $a_i \neq 0$ is minimal. The weight of a relative to the radix-r form is the number of nonzero a_i's in a minimal weak radix-r form. Some canonical minimal forms were given by Reitwiesner [1] for integers with radix $r = 2$, Clark and Liang [2], Boyarinov [3], Kabatyanskii [4] for integers with general radis r and Clark and Liang [5] for Gaussian integers with radix $r = \pm 1 \pm i$.

We shall establish here a more general canonical minimal form for radix r of R which we call a block irreducible form.

LEMMA 1. Let r be an element of R such that $v(r) \geq 3$. Then $(a_m,\ldots,a_1,a_0) = (b_m,\ldots,b_1,b_0)$ if and only if there exists $c_0,\ldots,c_j,\ldots$ in R such that

$$b_0 = a_0 - c_0 r$$
$$b_j = a_j + c_{j-1} - c_j r, \qquad \text{for } 0 < j < m$$
$$b_m = a_m - c_{m-1}$$

and

$$v(c_i) < 3 \qquad \text{for all } i$$

$$v(c_0) < 2$$

PROOF. Assume $(a_m,\ldots,a_1,a_0) = (b_m,\ldots,b_1,b_0)$. This implies $a_0 \equiv b_0 \bmod r$ hence $b_0 = a_0 - c_0 r$. Now, $c_0 r = a_0 - b_0$ implies $v(c_0) < \frac{v(r) + v(r)}{v(r)} = 2$. Therefore, $(a_m,\ldots,a_1,a_0) = (a_m,\ldots,a_1 + c_0, b_0) = (b_m,\ldots,b_1,b_0)$ which implies $(b_m,\ldots,b_1) = (a_m,\ldots,a_1 + c_0)$. We thus have $b_1 \equiv a_1 + c_0 \bmod r$. Again, let $b_1 = a_1 + c_0 - c_1 r$ or $c_1 r = a_1 - b_1 + c_0$. Hence,

$$v(c_1) < \frac{v(r) + v(r) + 2}{v(r)} < 2 + \frac{2}{v(r)} < 3$$

since $v(r) \geq 3$. Now, $(a_m,\ldots,a_2,a_1 + c_0) = (a_m,\ldots,a_2 + c_1,b_1) = (b_m,\ldots,b_2,b_1)$. Therefore, $(a_m,\ldots,a_2 + c_1) = (b_m,\ldots,b_2)$. As before $a_2 + c_1 - c_2 r = b_2$ or $c_2 r = a_2 - b_2 + c_1$. We have $v(c_2) < \frac{2v(r) + 3}{v(r)} < 3$. Proceeding in this way we get

$$a_j + c_{j-1} - c_j r = b_j, \qquad v(c_j) < 3 \text{ for all } j.$$

If $a_j = b_j = 0$, we have $c_{j-1} = 0$ since $c_{j-1} = c_j r$ implies $v(c_{j-1}) > v(r) \geq 3$, a contradiction.

For the converse, we must assume $v(a_i)$ and $v(b_i)$ are both less than $v(r)$.

DEFINITION 0. We call the a_i in (1.1) and in Lemma 1 digits, and the c_i in Lemma 1 carries. Note that if $v(r) \geq 3$ then all carries c_j satisfy $v(c_j) < 3$ thus all carries are digits. However if $v(r) < 3$ then a carry may not be a digit. To avoid this complication we make the following

ASSUMPTION. Henceforth all carries are assumed to be digits.

DEFINITION 1. The form $(a_n,\ldots,a_0)$ is reducible if there exists a form $(b_m,\ldots,b_0)$ such that

(1) $b_i = 0$ for some $i \in \{0,1,\ldots,n\}$

and

(2) $(b_m,\ldots,b_0) = (a_n,\ldots,a_0)$

Otherwise the form $(a_n,\ldots,a_0)$ is called irreducible.

LEMMA 2. The form $(a_n,\ldots a_0)$ is irreducible if and only if

(1) $a_i \neq 0$ for all $i = 0,\ldots,n$

and

(2) there exists no $k \leq n$ such that $(a_k,\ldots,a_1,a_0) = (b_{k+1},0,b_{k-1},\ldots,b_0)$ where $(b_{k-1},\ldots,b_0)$ is irreducible.

PROOF. Let $(a_n,\ldots,a_0)$ be irreducible then clearly (1) holds. If (2) fails then

$$(a_k,\ldots,a_0) = (b_{k+1},0,b_{k-1},\ldots,b_0) \quad \text{for some } k \leq n.$$

If $k = n$ we get a contradiction so we may assume $k + 1 \leq n$. We can write

$$a_n r^n + \ldots + a_{k+1} r^{k+1} + b_{k+1} r^{k+1} = c_m r^m + \ldots + c_{k+1} r^{k+1}.$$

Therefore, $(a_n,\ldots,a_{k+1},a_k,\ldots,a_0) + (a_n r^n + \ldots + a_{k+1} r^{k+1}) + (a_k,\ldots,a_0)$

$= a_n r^n + \ldots + a_{k+1} r^{k+1} + (b_{k+1},0,b_{k-1},\ldots,b_0) = a_n r^n + \ldots + a_{k+1} r^{k+1} + b_{k+1} r^{k+1}$

$+ (0,b_{k-1},\ldots,b_0) = c_m r^m + \ldots + c_{k+1} r^{k+1} + (0,b_{k-1},\ldots,b_0)$

$= (c_m,\ldots,c_{k+1},0,b_{k-1},\ldots,b_0)$, a contradiction. Conversely, let $a = (a_n,\ldots,a_1,a_0)$ satisfy (1) and (2) and being reducible. Then

$$(a_n,\ldots,a_1,a_0) = (b_m,\ldots,b_j,\ldots,b_0)$$

where $b_j = 0$ for some j, $0 \leq j \leq n$ and j being smallest possible. Now

$$b_0 = a_0 - c_0 r$$
$$b_1 = a_1 + c_0 - c_1 r$$
$$\vdots$$
$$0 = b_j = a_j + c_{j-1} - c_j r$$
$$c_j = 0 + c_j - 0 \cdot r$$

We have $(a_j, a_{j-1}, \ldots, a_0) = (c_j, 0, b_{j-1}, \ldots, b_0)$. By the choice of j, $b_{j-1}, \ldots b_0$ must be irreducible otherwise we would have $(c_j, 0, b_{j-1}, \ldots, b_0) = (b'_m, \ldots, b'_{j-1}, \ldots, b'_s = 0, \ldots, b_0)$ and we could use this to find a smaller "j". If $(a_j, a_{j-1}, \ldots, a_0) = (b_m, \ldots, b_s, 0, b_{s-2}, \ldots, b_0)$, then we can write $(a_n, \ldots, a_0) = (b'_t, \ldots, b'_s, 0, b_{s-2}, \ldots, b_0)$. By "addition", $(a_n, \ldots, a_{j+1}, 0, 0, \ldots, 0) + (0, \ldots, 0, a_j, a_{j-1}, \ldots, a_0) = (a_n, \ldots, a_{j+1}, 0, \ldots, 0) + (\ldots, b_s, 0, b_{s-2}, \ldots, b_0) = (b'_t, \ldots, b'_s, 0, b_{s-2}, \ldots, b_0)$.

DEFINITION 2. The form $(a_n, \ldots, a_1, a_0)$ is called block irreducible if whenever $a_j \neq 0$ for all j, $t < j < s$ but $a_s = a_t = 0$, we must have $(a_{s-1}, \ldots, a_{t+1})$ irreducible. In otherwords $(a_n, \ldots, a_1, a_0)$ is composed of irreducible sequences (or blocks) separated by sequences (or blocks) of zeros.

LEMMA 3. If $a = qr + c$ where $v(c) < v(r)$ and $v(a) \geq v(r) \geq 2$, then $v(q) < \frac{2}{v(r)} v(a)$.

The following corollary is an immediate consequence of lemma 3.

COROLLARY. If $v(r) \geq 2$, then the sequence

$$a = q_1 r + a_0,$$
$$q_1 = q_2 r + a_1,$$
$$\cdots$$
$$q_i = q_i r + a_i, \qquad \text{where } v(a_i) < v(r),$$

contains an element q_k such that $v(q_k) < v(r)$.

REMARK. The sequence given above need not be bounded since e.g. in the ring of integers for base $r = 3$, we have $(-1,2) = (-1,2,2) = (-1,2,2,2) = \ldots = -1$ since $2 = (1,-1)$, $(2,2) = (1,0,-1)$, $(2,2,2) = (1,0,0,-1)$, etc.

DEFINITION. Let $a = (a_n,\ldots,a_1,a_0) = a_n r^n + \ldots + a_1 r + a_0$. Then

$$\begin{aligned}
a &= q_0 r + a_0, & q_0 &= a_n r^{n-1} + \ldots + a_1 \\
q_0 &= q_1 r + a_1, & q_1 &= a_n r^{n-2} + \ldots + a_2 \\
&\vdots \\
q_i &= q_{i+1} r + a_i, & q_{i+1} &= a_n r^{n-(i+2)} + \ldots + a_{i+2} \\
&\vdots \\
q_n &= 0 \cdot r + a_n
\end{aligned}$$

Suppose $a_0 \neq 0$. We shall say that $a_i = 0$ is the soonest possible zero after a_0 if $a_0 \neq 0$, $a_1 \neq 0,\ldots,$ $a_{i-1} \neq 0$, $a_i = 0$ and for no smaller i is it possible to find a representation for a with $a_j = 0$, $j < i$.

REMARK. $a = (a_n,\ldots,a_0)$ is irreducible if and only if $a_0 \neq 0$ and $a_{n+1} = 0$ is the soonest possible zero after a_0.

REMARK. If $a = \ldots,a_{s+2},0,a_s,\ldots,a_t,0,a_{t-1},\ldots,$ then the sequence corresponds to the following

$$\begin{aligned}
a &= q_0 r + a_0 \\
&\vdots \\
q_{t-2} &= q_{t-1} r + a_{t-2} \\
q_{t-1} &= q_t r + 0 \\
q_t &= q_{t+1} r + a_t
\end{aligned}$$

$$q_{s-1} = q_s r + a_s$$
$$q_s = q_{s+1} r + 0$$
$$\vdots$$

Clearly, $(a_s,\ldots,a_t)$ is irreducible if and only if a_{s+1} is the soonest possible zero after a_t and $a_t \neq 0$. We shall show in theorem 3 that this process must stop (at or before $n+2$ where $v(q_n) < v(r)$).

LEMMA 4. If $a = (a_n,\ldots,a_k,0,0,\ldots,0) = (b_m,\ldots,b_k,\ldots,b_0)$ then $b_i = 0$ for $i = 0, 1,\ldots, k-1$.

PROOF. Since $b_0 \equiv 0 \bmod r$ and $v(b_0) < r$, this implies $b_0 = 0$. Thus $\frac{a}{r} = (a_n,\ldots,a_k,0,\ldots,0) = (b_m,\ldots,b_k,\ldots,b_1)$ and $b_1 = 0$. By induction, $b_0 = b_1 = \ldots = b_k = 0$.

THEOREM 1. (Uniqueness of Block Irreducible Form) Let $v(r) \geq 3$ and $a = (a_n,\ldots,a_1,a_0)$ be a block irreducible form with non zero blocks.

$$(a_{k_2},\ldots,a_{k_1})$$
$$(a_{k_4},\ldots,a_{k_3})$$
$$\vdots$$
etc.

Then these blocks are unique in the sense that if $(a_\ell,\ldots,a_k)$ and $(b_m,\ldots,b_t)$ are the i-th irreducible blocks in two different block irreducible representations, then $k = t$, $\ell = m$ and

$$\sum_{j=k}^{m} a_j r^j = \sum_{j=k}^{m} b_j r^j$$

PROOF. Let $a = (\ldots,0,a_\ell,\ldots,a_k, 0,\ldots,0)$ and $a = (\ldots,0,b_m,\ldots,b_t,0,\ldots,0)$ where $(a_\ell,\ldots,a_k)$ and $(b_m,\ldots,b_t)$ are both irreducible. By lemma 4, $a_k \neq 0$ iff $b_t \neq 0$, hence $t = k$ and if $\ell < m$, then $(b_m,\ldots,b_k) = (\ldots,0,a_\ell,\ldots,a_k)$ not irreducible. Therefore, $\ell = m$. We may assume $k = 0$. Then we have

$$\sum_{j=0}^{m} b_j r^j \equiv \sum_{j=0}^{m} a_j r^j \bmod r^{m+2}$$

or

$$\sum_{j=0}^{m} (b_j - a_j) r^j \equiv 0 \bmod r^{m+2}$$

Therefore, either

$$\sum_{j=0}^{m} (b_j - a_j) r^j = 0$$

in which case we have

$$\sum_{j=0}^{m} b_j r^j = \sum_{j=0}^{m} a_j r^j$$

or

$$2\left(\sum_{j=0}^{m} (b_j - a_j) r^j\right) \geq v(r)^{m+2}$$

which implies

$$2[v(r)^{m+1} + \ldots + v(r)] > v(r)^{m+2}$$

or

$$2v(r)\left(\frac{v(r)^{m+1} - 1}{v(r) - 1}\right) > v(r)^{m+2}$$

or

$$v(r)^{m+1} - 1 = \frac{2(v(r)^{m+1} - 1)}{2} \geq 2\left(\frac{v(r)^{m+1} - 1}{v(r) - 1}\right) > v(r)^{m+1}$$

a contradiction. Therefore,

$$\sum_{j=k}^{m} a_j r^j = \sum_{j=k}^{m} b_j r^j .$$

By induction one may show that the next irreducible block is also unique and all blocks are unique.

THEOREM 2. (Minimality of Block Irreducible Form) If $a = (a_n,\ldots,a_0)$ is a block irreducible form, then it is minimal. Furthermore for each i, if $a = (b_m,\ldots,b_i,\ldots,b_0)$ then $(b_i,\ldots,b_0)$ has weight at least the weight of $(a_i,\ldots,a_0)$.

PROOF. It suffices to show that for each i, $(b_i,\ldots,b_0)$ has no more zero terms than $(a_i,\ldots,a_0)$. By lemma 4, we may assume $a_0 \neq 0$, $b_0 \neq 0$. Thus we have $a = (\ldots,0,a_k,\ldots,a_0)$ where $(a_k,\ldots,a_0)$ is irreducible. If $b = (\ldots,b_k,\ldots,b_0)$ then $b_j \neq 0$ for $j = 0,\ldots,k$, for suppose not, let $b_j = 0$, some $j \in \{1,2,\ldots,k\}$. By lemma 1

$$\begin{aligned}
b_0 &= a_0 - c_0 r \\
b_s &= a_s + c_{s-1} - c_s r, \qquad 0 < s \leq j - 1 \\
0 &= a_j + c_{j-1} - c_j r \\
c_j &= 0 + c_j - 0 \cdot r \\
(a_j,\ldots,a_0) &= (c_j,0,b_{j-1},\ldots,b_0)
\end{aligned}$$

which cannot happen since $(a_k,\ldots,a_0)$ is irreducible. Now, suppose we have a 1 - 1 mapping of zeros of $(b_p,\ldots,b_0)$ into zeros of $(a_p,\ldots,a_0)$ for some p where p is beyond the first irreducible block of $(a_n,\ldots,a_0)$. If $b_p = 0$ and $a_p = 0$, we map b_p to a_p. However, if $a_p \neq 0$ and $b_p = 0$, we then have the following situation:

$$
\begin{aligned}
&(a_p,\ldots,a_\ell) \text{ is irreducible} \\
0 &= a_p + c_{p-1} - c_p r \\
b_{p-1} &= a_{p-1} + c_{p-2} - c_{p-1} r \\
&\vdots \\
b_j &= a_j + c_{j-1} - c_j r \\
&\vdots \\
b_\ell &= a_\ell + c_{\ell-1} - c_\ell r \\
b_{\ell-1} &= 0 + c_{\ell-2} - c_{\ell-1} r
\end{aligned}
$$

Suppose $b_j = 0$ for some $j \in \{p-1,\ldots,\ell\}$, we have $a_j - c_j r = -c_{j-1}$. Hence $(c_p,0,b'_{p-1},\ldots,b'_\ell) = (a_p,\ldots,a_\ell)$. Since we can begin the carrying at a_j [with $a_j - c_j r$] and this will allow us to get 0 at the p-th digit, we obtain a contradiction to the fact that $(a_p,\ldots,a_\ell)$ is irreducible. Hence $b_{p-1} \neq 0$, $b_{p-2} \neq 0,\ldots,b_\ell \neq 0$. Now if $b_{\ell-1} = 0$ we have $c_{\ell-2} = c_{\ell-1} r$ which implies $c_{\ell-2} = c_{\ell-1} = 0$ and so we have $(0,b_{p-1},\ldots,b_\ell) = (a_p,\ldots,a_\ell)$ since we do not need the carry from $(\ell-1)$st digit (it is zero). Therefore $b_p = 0$ can be mapped to $a_{\ell-1} = 0$.

THEOREM 3. (Existence of Block Irreducible Form) Every element a in R has a block irreducible form with respect to a radix r if $v(r) \geq 2$.

PROOF. Let $a = (a_\ell,\ldots,a_0)$ be any weak radix-r form for a. Assume that $a_j \neq 0$ but $a_t = 0$, $t < j$, also $(a_k,\ldots,a_j)$ irreducible but $(a_{k+1},a_k,\ldots,a_j)$ reducible. Then $(a_{k+1},a_k,\ldots,a_j) = (a'_{k+2},0,a'_k,\ldots,a'_j)$ where $(a'_k,\ldots,a'_j)$ is irreducible. Now, we can rewrite a as $a = (a''_{n+1},\ldots,a''_{K+2},0,a'_k,\ldots,a'_j,0,\ldots,0)$. Applying the above to $(a''_n,\ldots,a''_{k+2})$ and induction yield for n as large as desired, $a = (a_m,\ldots,a_n,\ldots,a_0)$ where $(a_n,\ldots,a_0)$ is block irreducible. Now we want to show the process will stop. Note that $a = (a_m,\ldots,a_n,\ldots,a_0)$ leads to the sequence of

$$a = q_0r + a_0$$

$$q_0 = q_1r + a_1$$

$$\vdots$$

$$q_n = q_{n+1}r + a_n$$

and at some point $v(q_n) < v(r)$ which implies that $v(q_j) < v(r)$ for all $j \geq n$ since $q_{n+1}r = q_n - a_n$ so $v(q_{n+1}) < \frac{2v(r)}{v(r)} = 2 \leq v(r)$ and by induction. Now pick any n such that $v(q_n) < v(r)$ and $a = (\ldots,a_n,\ldots,a_0)$ where $(a_n,\ldots,a_0)$ is block irreducible. Suppose $a_n \neq 0$. We then have $q_n = rq_{n+1} + a_n$, $q_{n+1} = r \cdot 0 + q_{n+1}$ and $0 = r \cdot 0 + 0$. So $a = (0,q_{n+1},a_n,\ldots,a_\ell,0,\ldots)$ where $a_n \neq 0$, $a_\ell \neq 0$ and $(a_n,\ldots,a_\ell)$ is irreducible. If $(q_{n+1},a_n,\ldots,a_\ell)$ is irreducible, we are done. If not $(0, q_{n+1},a_n,\ldots,a_\ell) = (a'_{n+2},0,a'_n,\ldots,a'_\ell)$ and $(a'_n,\ldots,a'_\ell)$ is irreducible so $a = (a'_{n+2},0,a'_n,\ldots,a'_\ell,0,\ldots,a_1,a_0)$ is block irreducible. Now if $a_n = 0$ we claim $a_j = 0$ for $j \geq n$. Otherwise for smallest $n < j$ such that $a_j \neq 0$ we have

$$q_n = q_{n+1}r + 0$$
$$\vdots$$
$$q_{j-1} = q_j r + 0$$
$$q_j = q_{j+1}r + a_j$$

but $q_{j-1} = q_j r$ implies $q_j = 0$ and $a_j = -q_{j+1}r$ implies $a_j = 0$, a contradiction.

In what follows we shall give an algorithm for finding the block irreducible form for $v(r) \geq 3$. Actually these are just some ideas on how to possibly simplify the search for block irreducible forms.

LEMMA 5. Let A_k be the set of all representatives of the form $(a_k,a_{k-1},\ldots,a_0)$ where all proper subsequences are irreducible but the sequence itself is reducible. Let $A = A_1 \cup A_2 \ldots \cup A_k \ldots$. If $(a_{k-1},\ldots,a_0)$ is irreducible then $(a_k,a_{k-1},\ldots,a_0)$ is irreducible iff $(a_k,a_{k-1},\ldots,a_{k-j}) \notin A_j$ for all $j \in \{1,2,\ldots,k\}$, $a_k \neq 0$.

PROOF. Since $(a_{k-1},\ldots,a_0)$ is irreducible so are all proper subsequences. Thus, if $(a_k,\ldots,a_0)$ were reducible then ther is a smallest j such that $(a_k,\ldots,a_{k-j})$ is reducible. No proper subsequences will be reducible since it would contradict to the choice of j.

ALGORITHM. (For finding block irreducible form) We may assume $a_0 \neq 0$, $a_1 \neq 0$. By definition $(a_1,a_0) \notin A_1$ iff (a_1,a_1) is irreducible. If $(a_1,a_0) \notin A$, consider (a_2,a_1,a_0). WOLG, assume $a_i \neq 0$, $i = 0, 1, 2$. It is irreducible iff $(a_2,a_1) \notin A$, and $(a_2,a_1,a_0) \in A_2$. In general if we have chosen $(a_{k-1},\ldots,a_1)$ irreducible then $(a_k,\ldots,a_1)$ is also irreducible iff $(a_k,a_{k-1}) \notin A_1$, $(a_k,a_{k-1},a_{k-2}) \notin A_2,\ldots,(a_k,\ldots,a_0) \notin A_k$. Thus if we find

$(a_k,\ldots,a_j) \in A_t$, then we replace $(a_k,\ldots,a_0)$ by $(b_{k+1},0,b_{k-1},\ldots,b_j,a_{j-1},\ldots,a_0)$ and we know $(b_{k-1},\ldots,b_j,a_{j-1},\ldots,a_0)$ is irreducible. Reduce the rest of a by carring b_{k+1} to the left as necessary and then begin the same process with the new $(k+1)$st term if it is non zero (or the next non zero term).

LEMMA 6. If the form $(a_{k+1},\ldots,a_0) \in A_{k+1}$, then there exist carries c_j, $j = 0,1,\ldots,k+1$ such that

(1) $$a_{k+1} = c_{k+1}r - c_k$$

(2) $$v(a_\theta - c_0 r) < v(r)$$

and (3) for $j \in \{1,\ldots,k\}$

$$v(a_j - c_j r) \geq v(r)$$

but $$v(a_j - c_j r + c_{j-1}) < v(r)$$

PROOF. Let $(a_{k+1},\ldots,a_0) \in A_{k+1}$ then $(a_{k+1},\ldots,a_0) = (b_{k+2},0,b_k,\ldots,b_0)$ with $b_j = a_j + c_{j-1} - c_j r$, $j = k+1,\ldots,1$ and $b_0 = a_0 - c_0 r$. Now $0 < v(b_j) < v(r)$ for $j \leq k$ otherwise $b_j = 0$ would imply $(a_j,\ldots,0)$ being reducible, a contradiction. Also, $v(a_j - c_j r) \geq v(r)$ for $1 \leq j \leq k$. Since if $v(a_j - c_j) < v(r)$ then $(a_{k+1},a_k,\ldots,a_j)$ would be reducible, again a contradiction since no proper subsequence of $(a_{k+1},a_k,\ldots,a_0)$ is reducible.

EXAMPLE. Let R be the ring of Gaussian integers and $r = 100$. The element $a = [-(1+i),4 + 71i,50 + 50i] \in A_2$ because $a = (0,-95 - 28i, -50 - 50i)$ and $(4 + 71i, 50 + 50i)$ is irreducible since $4 + 71i + u_1 + u_2 i \neq 100(v_1 + v_2 i)$ for any u_i, $v_i \in \{0,\pm 1\}$.

REFERENCES

1. Reiwiesner, G. H. Advances in Computers (F. L. Alt, ed.), Vol. 1, Academic Press, New York, 1960.

2. Clark, W. E. and J. J. Liang. On arithmetic weight for a general radix presentation of integers, IEEE Trans. Information Theory (Nov. 1973) 823-826.

3. Boyarinov, I. M. Nonbinary arithmetic codes with large minimum distance, Vol. 11, No. 1, Problemy Peredachi Informatsii (Jan. - March 1975) 57-63. (Russian)

4. Kabatyanskii, G. A. Bounds on the number of code words in binary arithmetic codes, Vol. 12, No. 4, Problemy Peredachi Informatsii (Oct. - Dec. 1976) 46-54. (Russian)

5. Clark, W. E. and J. J. Liang. Weak radix representation and cyclic codes over Euclidean domains, Communications in Algebra 4(11) (1976) 999-1028.