PACIFIC JOURNAL OF MATHEMATICS
Vol. 126, No. 2, 1987

NECESSARY AND SUFFICIENT CONDITIONS FOR SIMPLE A-BASES

CARL SWENSON AND CALVIN LONG

Let A be a set of m distinct integers with $m \geq 2$ and $0 \in A$. It is shown that A possesses a simple A-base if and only if A is a complete residue system modulo m and the elements of A are relatively prime.

The notions of simple and non-simple A-bases, due to de Bruijn, are defined as follows.

DEFINITION 1. Let A be as above. The integral sequence $B = \{b_i\}_{i \geq 1}$ is called an A-base for the set of integers provided that every integer n can be represented uniquely in the form

$$n = \sum_{i=1}^{r(n)} a_i b_i, \qquad a_i \in A \ \forall i.$$

If (with possible rearrangement) B can be written in the form $B = \{d_i m^{i-1}\}_{i \geq 1}$where the d_i are integers, then it is called a simple A-base.

The notion of an A-base was generalized by Long and Woo to that of an $\mathfrak{A}$-base where $\mathfrak{A} = \{A_i\}$ and each A_i is a set of m_i distinct integers with $0 \in A_i$ and $m_i \geq 2$ for all i. The definition is as follows.

DEFINITION 2. Let $\mathfrak{A}$ be as above. The integral sequence $B = \{b_i\}_{i \geq 1}$ is called an $\mathfrak{A}$-base for the set of integers provided every integer n can be written uniquely in the form

$$n = \sum_{i=1}^{r(n)} a_i b_i, \qquad a_i \in A_i \ \forall i.$$

If (with possible rearrangement) B can be written in the form $B = \{d_i M_{i-1}\}_{i \geq 1}$ where the d_i are integers and where $M_0 = 1$ and $M_i = \prod_{j=1}^{i} m_j$ for $i \geq 1$, then it is called a simple $\mathfrak{A}$-base.

De Bruijn has pointed out that it is not yet known for which A's there exist simple A-bases nor it is known for which A's there exist non-simple A-bases. He gives several examples and then observes that if A has a simple A-base it is necessary that A form a complete residue system modulo m and that the elements of A be relatively prime. He also observes that it is necessary that $(d_i, m) = 1$ for all i.

Long and Woo have given several sets of sufficient conditions for both simple and non-simple A-bases and $\mathfrak{A}$-bases, but no necessary and sufficient conditions.

In the present paper, we shown that the necessary conditions of de Bruijn for the existence of simple A-bases are also sufficient. Necessary and sufficient conditions for the existence of simple $\mathfrak{A}$-bases are still lacking.

The results of de Bruijn noted above are contained in [**1**] and those of Long and Woo appear in [**3**].

Before proving the main theorem a lemma will be needed.

LEMMA. *Let $m \geq 2$ be an integer and let A be a complete residue system modulo m. If $0 \in A$ and the elements of A are relatively prime, then every integer n can be represented in the form*

$$n = a_1d_1 + a_2d_2m + a_3d_3m^2 + \cdots + a_sd_sm^{s-1}, \tag{1}$$

where $s > 1$ and $d_1, d_2, \ldots, d_m$ are integers with $(d_i, m) = 1$ and $a_i \in A$ for all i.

Proof. Of course, zero is trivially representable in the desired form. For $n \neq 0$, we distinguish two cases.

Case 1. $(m, n) = 1$.

Since A is a complete residue system modulo m, there exists $a \in A$ such that $n \equiv a \pmod{m}$. We set $a_1 = a$ and denote the remaining elements of A by $a_2, a_3, \ldots, a_m$. Since $(n, m) = 1$ and $n \equiv a_1 \pmod{m}$, it follows that $(a_1, m) = 1$. Thus, since $(a_1, a_2, \ldots, a_m) = 1$, it follows that $(a_1, a_2m, a_3m^2, \ldots, a_mm^{m-1}) = 1$ and hence that the diophantine equation

$$n = a_1x_1 + a_2mx_2 + a_3m^2x_3 + \cdots + a_mm^{m-1}x \tag{2}$$

has a solution $(d_1', d_2', \ldots, d_m')$. This implies that $a_1d_1' \equiv n \pmod{m}$ and hence that $(d_1', m) = 1$. For $2 \leq k \leq m$, set $e_k = (d_k', a_1)$. Then

$$\left(\frac{d_k'}{e_k}, \frac{a_1}{e_k}\right) = 1$$

and it follows from Dirichlet's theorem that there exist infinitely many primes of the form

$$\frac{d_k'}{e_k} - \frac{a_1}{e_k} \cdot r$$

where r is an integer. Hence, we may choose r_k such that $d_k' - a_1 r_k = pe_k$ where p is a prime and $(pe_k, m) = 1$. Setting $d_k = d_k' - a_1 r_k$ we have that $(d_k, m) = 1$ for $2 \leq k \leq m$. Setting

$$d_1 = d_1' + a_2 r_2 m + a_3 r_3 m^2 + \cdots + a_m r_m m^{m-1},$$

it follows that $(d_1, m) = 1$ since $(d_1', m) = 1$. Thus, $(d_i, m) = 1$ for $1 \leq i \leq m$ and

$$\begin{aligned} a_1 d_1 &+ a_2 d_2 m + a_3 d_3 m^2 + \cdots + a_m d_m m^{m-1} \\ &= a_1\left(d_1' + a_2 r_2 m + a_3 r_3 m^2 + \cdots + a_m r_m m^{m-1}\right) \\ &\quad + a_2\left(d_2' - a_1 r_2\right)m + a_3\left(d_3' - a_1 r_3\right)m^2 \\ &\quad + \cdots + a_m\left(d_m' - a_1 r_m\right)m^{m-1} \\ &= a_1 d_1' + a_2 d_2' m + a_3 d_3' m^2 + \cdots + a_m d_m' m^{m-1} = n \end{aligned}$$

since, as noted above, $(d_1', d_2', \ldots, d_m')$ satisfies (2).

Case 2. $(m, n) > 1$.

It suffices to consider only the case where all prime factors of n divide m. For, if $n = n_1 n_2$ with $(n_1, m) = 1$ and

$$n_2 = a_1 d_1' + a_2 d_2' m + a_3 d_3' m^2 + \cdots + a_m d_m' m^{m-1},$$

with $(d_i', m) = 1$ for all i, then

$$\begin{aligned} n &= n_1 n_2 \\ &= a_1\left(n_1 d_1'\right) + a_2\left(n_1 d_2'\right)m + a_3\left(n_1 d_3'\right)m^2 + \cdots + a_m\left(n_1 d_m'\right)m^{m-1} \\ &= a_1 d_1 + a_2 d_2 m + a_3 d_3 m^2 + \cdots + a_m d_m m^{m-1} \end{aligned}$$

with $d_i = n_1 d_i'$ and hence $(d_i, m) = 1$ for all i. Thus, assuming that all prime factors of n divide m, there exists $t > 1$, such that $n | m^{t-1}$. Let

$$A' = a \oplus mA \oplus m^2 A \oplus \cdots \oplus m^{t-1} A,$$

where

$$kA = \{b \mid b = ka,\ a \in A\}$$

and

$$A \oplus B = \{c \mid c = a + b,\ a \in A,\ b \in B\}$$

with $|A \oplus B| = |A||B|$. It is easy to see that A' forms a complete residue system modulo m^t. Thus, we can choose $\alpha \in A'$ such that

$$n \equiv \alpha \pmod{m^t}, \tag{3}$$

and there exists an integer q such that

$$n = \alpha + qm^t. \tag{4}$$

Since $\alpha \in A'$, we can write

$$\alpha = a_{\alpha,1} + a_{\alpha,2}m + a_{\alpha,3}m^2 + \cdots + a_{\alpha,t}m^{t-1} \tag{5}$$

with $a_{\alpha,i} \in A$ for all i. Since $n \mid m^{t-1}$, (4) implies that $n \mid \alpha$ and hence that

$$1 = \frac{\alpha}{n} + \frac{m^t}{n} \cdot q$$

where α/n and m^t/n are integers. This implies that $(\alpha/n, q) = 1$ and hence, again by Dirichlet's theorem, there exists an integer s such that $q + (\alpha/n)s$ is a prime and is relatively prime to m. Thus, by case 1, there exist d_i' with $(d_i, m) = 1$ for $1 \le i \le m$ such that

$$q + \frac{\alpha}{n} \cdot s = a_1'd_1' + a_2'd_2'm + \cdots + a_m'd_m'm^{m-1} \tag{6}$$

where $a_1', a_2', \ldots, a_m'$ are the elements of A in some order. Moreover,

$$\frac{\alpha}{n}\left(1 - \frac{m^t}{n} \cdot s\right) + \frac{m^t}{n}\left(q + \frac{\alpha}{n} \cdot s\right) = \frac{\alpha}{n} + \frac{m^t}{n} \cdot q = 1$$

and hence

$$n = \alpha\left(1 - \frac{m^t}{n} \cdot s\right) + m^t\left(q + \frac{\alpha}{n} \cdot s\right). \tag{7}$$

Since $n \mid m^{t-1}$, it follows that $m \mid (m^t/n)$ and hence that

$$1 = \left(1 - \frac{m^t}{n} \cdot s, m\right).$$

Thus, from (5), (6), and (7), we have

$$\begin{aligned} n &= \alpha\left(1 - \frac{m^t}{n} \cdot s\right) + m^t\left(q + \frac{\alpha}{n} \cdot s\right) \\ &= a_{\alpha,1}\left(1 - \frac{m^t}{n} \cdot s\right) + a_{\alpha,2}\left(1 - \frac{m^t}{n} \cdot s\right) + \cdots + a_{\alpha,t}\left(1 - \frac{m^t}{n} \cdot s\right) \\ &\qquad + a_1'd_1'm^t + a_2'd_2'm^{t+1} + a_3'd_3'm^{t+2} + \cdots + a_m'd_m'm^{m+t-1} \\ &= a_1d_1 + a_2d_2m + a_3d_3m^2 + \cdots + a_{m+t}d_{m+t}m^{m+t-1} \end{aligned}$$

where $d_i = 1 - (m^t/n) \cdot s$ and $a_i = a_{\alpha,i}$ for $1 \le i \le t$ and $d_{i+t} = d_i'$ and $a_{i+t} = a_i'$ for $1 \le i \le m$. Since, $a_i \in A$ and $(d_i, m) = 1$ for all i, this is a representation in the desired form and the proof is complete.

We now prove the main result.

THEOREM. *Let A be a set of m distinct integers with $0 \in A$ and $m \geq 2$. Then A has an A-base if and only if A is a complete residue system modulo m and the elements of A are relatively prime.*

Proof. First let $A = \{a_1, a_2, \dots, a_m\}$ and assume that A has a simple A-base, $B = \{d_i m^{i-1}\}_{i \geq 1}$. Then every integer n can be represented in the form

$$n = \sum_{i=1}^{r(n)} a_{n,i} d_i m^{i-1}, \quad a_{n,i} \in A \ \forall i. \tag{8}$$

Since $n \equiv a_{n,1} d_1 \pmod{m}$ and each of $0, 1, \dots, m-1$ is represented in the form (8), it follows that $\{a_1 d_1, a_2 d_1, \dots, a_m d_1\}$ forms a complete residue system modulo m and hence that $\{a_1, a_2, \dots, a_m\}$ also forms a complete residue system modulo m and that $(d_1, m) = 1$. The argument can be repeated, and this leads to $(d_i, m) = 1$ for all $i \geq 1$. Also, if $(a_1, a_2, \dots, a_m) = d > 1$, then only multiples of d can be represented in (8). This is a contradiction and so $(a_1, a_2, \dots, a_m) = 1$ as claimed.

Now suppose that the elements of A are relatively prime and form a complete residue system modulo m. We must show that there exists an integral sequence $\{d_i\}_{i \geq 1}$ with $(d_i, m) = 1$ for all i such that every integer n is uniquely representable in the form (8). Of course, 0 is trivially representable in the desired form. Also, by the lemma, 1 can be represented in the desired form and will, in fact, appear in the sum

$$S_1 = d_1 A \oplus d_2 m A \oplus d_3 m^2 A \oplus \cdots \oplus d_{s_1} m^{s_1 - 1} A$$

for suitable integers $d_1, d_2, \dots, d_{s_1}$ and $s_1 > 1$. S_1 is easily seen to be a complete residue system modulo m^{s_1} since A is a complete residue system modulo m and $(d_i, m) = 1$ for $1 \leq i \leq s_1$. Of course, all elements of S_1 are represented in the desired form. Let r_1 be the integer of least absolute value such that $r_1 \notin S_1$. If there are two such values, r and $-r$, we set $r_1 = r$. Since S_1 is a complete residue system modulo m^{s_1}, there exists $s \in S_1$, such that $r_1 \equiv s \pmod{m^{s_1}}$. Thus, $r_1 = s + q m^{s_1}$ for some integer q and, by the lemma, there exists an integer $s_2 > 1$ and integers $d_{s_1 + i}$ with $(d_{s_1+i}, m) = 1$ for $1 \leq i \leq s_2$ such that

$$q = a_{q,1} d_{s_1+1} + a_{q,2} d_{s_1+2} m + \cdots + a_{q,s} d_{s_1+s_2} \cdot m^{s_2 - 1}$$

with $a_{q,i} \in A$ for $1 \leq i \leq s_2$. Also, since $s \in S_1$,

$$s = a_{s,1} d_1 + a_{s,2} d_2 m + \cdots + a_{s,s_1} d_{s_1} m^{s_1 - 1}$$

with $a_{s,j} \in A$ for $1 \leq j \leq s_1$. But then

$$\begin{aligned} r_1 &= s + qm^{s_1} \\ &= a_{s,1}d_1 + a_{s,2}d_2m + \cdots + a_{s,s_1}d_{s_1}m^{s_1-1} \\ &\quad + a_{q,1}d_{s_1+1}m^s + \cdots + a_{q,s_2}d_{s_1+s_2}m^{s_1+s_2-1} \end{aligned}$$

which is a representation of r_1 in the desired form. Now from the set

$$S_2 = d_1A \oplus d_2mA \oplus d_3m^2A \oplus \cdots \oplus d_{s_1+s_2}m^{s_1+s_2-1}A.$$

Note that $S_1 \subset S_2$ since $0 \in A$ and also note that all members of S_2 are represented in the desired form. We now iterate with r_2 as the integer of least absolute value not in S_2, and so on. In this way, we build our A-base step by step and it is clear that any particular integer n will be properly represented after at most $2|n|$ steps. Since it is clear that such representations are unique, the proof is complete.

References

[1] N. G. De Bruijn, *On bases for the set of integers*, Publ. Math. (Debrecen), **1** (1950), 232–242.

[2] ——, *Some direct decompositions of the set of integers*, Math. Comp., **18** (1964), 537–546.

[3] C. T. Long and N. Woo, *On bases for the set of integers*, Duke Math. J., **38** (1971), 538–590.

Received March 18, 1985 and in revised form November 21, 1985.

SEATTLE UNIVERSITY
SEATTLE, WA 98122