Cycles of Differences of Integers

ANNE LUDINGTON FURNO

Department of Mathematics, Hamilton College, Clinton, New York 13323

Communicated by P. T. Bateman

Received November 13, 1979

Let \( A = (a_i) \) be a \( k \)-tuple of positive integers. We define a new \( k \)-tuple \( \overline{A} = ([a_i - a_{i+1}] \) by taking numerical differences. If this process is repeated, eventually repetition takes place, resulting in a cycle. We show that except for constant multiples there are only a finite number of cycles. We determine explicitly those \( k \)-tuples which are in a cycle.

1. INTRODUCTION

Let \( A = (a_0, a_1, \ldots, a_{k-1}) \) be a \( k \)-tuple of positive integers. We obtain a new \( k \)-tuple \( \overline{A} = (a'_0, a'_1, \ldots, a'_{k-1}) \) by taking numerical differences; that is, \( a'_i = |a_i - a_{i+1}| \). Subscripts are always to be reduced modulo \( k \) so that \( a'_{k-1} = |a_{k-1} - a_0| \).

If we consider tuples \( A_0, A_1, \ldots, A_n, \ldots \), where \( A_i = A_{i+1} \), then at some stage repetition must take place since \( \max A_i > \max A_{i+1} \) and there are only a finite number of arrangements of \( k \) things using numbers less than or equal to \( \max A_0 \). If \( A_n = A_0 \), then we call \( A_0, A_1, \ldots, A_{n-1} \) a cycle of length \( n \).

It is well known that when \( k = 2^r \) every \( k \)-tuple \( A \) eventually leads to the trivial or zero-tuple \( (0) = (0, 0, \ldots, 0) \) [1–7]. Thus when \( k = 2^r \) there is only one cycle, the trivial one. This is not the case when \( k = 2^r k' \), \( k' \) odd and greater than 1. A necessary but not sufficient condition that the differencing process eventually takes a tuple \( A = (a_i) \) to \( (0) \) is that

\[ a_{i+2r} \equiv a_i \pmod{2}. \]

Thus we seek to characterize the cycles of \( k \)-tuples for \( k = 2^r k' \). We will show that except for constant multiples there are only a finite number of cycles. We will explicitly determine those tuples which are in a cycle.
2. A Reduction of the Problem

The proof of the following lemma is immediate.

**Lemma 1.** For any $k$-tuple $(a_i)$ we have

$$(\lambda a_i + \delta) = \lambda(a_i), \quad \delta \in \mathbb{Z}^+, \quad \lambda \in \mathbb{Z}^+, \quad \delta \in \mathbb{Z}^+ \cup \{0\}.$$ 

By Lemma 1, $A_0, A_1, ..., A_{n-1}$ is a cycle if and only if $\lambda A_0, \lambda A_1, ..., \lambda A_{n-1}$ is a cycle. Thus in seeking to characterize cycles we need only consider tuples $A = (a_i)$ for which the nonzero terms are relatively prime. The following lemmas will help us characterize those tuples which are in a cycle.

**Lemma 2.** Suppose $A = (a_i)$ is in a cycle. Then there is some $j$ such that

(a) $a_j = \max A,$

(b) $a_{j-1} = 0$ or $a_{j+1} = 0.$

**Proof.** Let $\bar{A} = (a'_i).$ Then since $A$ is in a cycle, $\max A = \max \bar{A}.$ Suppose $a_j = \max A.$ Then $a'_j = a_j - a_{j-1}$ and $a'_{j+1} = a_j - a_{j+1}.$ Thus for some $a_j = \max A,$ $a_{j-1}$ or $a_{j+1}$ is zero.

**Lemma 3.** Suppose $A_0 = (a_i)$ is in a cycle with $\gcd(a_i | a_i \neq 0) = 1.$ Then

$$\max A_0 - 1.$$ 

**Proof.** The proof is by contradiction. Assume $\max A_0 = b$ with some $a_i \in \{0, b\}.$ We observe that the $k$-tuples $(a_1, a_2, ..., a_0), (a_2, a_3, ..., a_1), ..., (a_{k-1}, a_0, ..., a_{k-2}),$ and $(a_{k-1}, a_{k-2}, ..., a_0)$ are essentially the same with regard to the differencing process. Thus we may assume that $A_0$ is of the form $A_0 = (a_0, a_1, a_2, ..., a_{l-1}, a_{l+1}, ...,)$ where $a_0 \notin \{0, b\}; \quad a_i \notin \{0, b\}, \quad i = 1, 2, ..., l; \quad a_j = b$ and $a_{j+1} = 0$ for some $j$ between $1$ and $l - 1;$ and $l$ is as large as possible. Note that $l \geq 2;$ further, either $a_{l+1} \notin \{0, b\}$ or else $l = k.$

Taking differences we find

$$A_1 = \bar{A}_0 = (a'_0, a'_1, ..., a'_{l+1}, ...),$$

where

$$a'_0 \notin \{0, b\}; \quad a'_i \in \{0, b\}, \quad i = 1, ..., l - 1; \quad a'_l \notin \{0, b\}.$$ 

Continuing we have

$$A_{l-1} = (a''_0, a''_1, ..., a''_{l}, ...),$$

where

$$a''_0 \notin \{0, b\}, \quad a''_i \in \{0, b\}, \quad a''_l \notin \{0, b\}.$$
This is a contradiction to Lemma 2 since \( l \) was chosen as large as possible. That is, in \( A_{i-1} \) if \( a'_j = b \), then \( a'_{j-1} \) and \( a'_{j+1} \) are not zero.

As a result of Lemma 3 we need only consider tuples containing 0 and 1. This we do in the next section.

3. Characterization of Tuples in Cycles

Henceforth we will consider only tuples of 0's and 1's. Thus by \( A = (a_i) \) we will mean \( a_i \in \{0, 1\} \). Note that now the process of differencing is the same as addition in \( \mathbb{Z}_2 \) since

\[
|a_i - a_{i+1}| \equiv a_i + a_{i+1} \quad \text{(mod 2)}.
\]

Thus we shall write

\[
\overline{(a_i)} = (a_i + a_{i+1}),
\]

where it is understood that addition is modulo 2 (subscripts are of course still reduced modulo \( k \)).

For such tuples we can explicitly determine the successors, \( A_1, A_2, \ldots \), of \( A_0 \).

**Theorem 1.** Let \( A_0 = (a_i) \) and \( A_n = (b^n) \). Suppose the 2-adic expansion of \( n \) is \( n = \sum_{s=0}^{N} a_s 2^s, \ a_N \neq 0. \) Then

\[
b^n = \sum_{j \in J} a_j,
\]

where \( J \) is the set of all \( j = \sum_{s=0}^{N} \beta_s 2^s \) for which \( \beta_s = 0 \) whenever \( a_s = 0. \)

Further

\[
b^n_i = \sum_{j \in J} a_{j+i}.
\]

**Proof.** Before proving the theorem we give an example to illustrate (1). Suppose \( n = 19 = 1 + 2 + 2^4 \). Then \( b^9 = \sum_{j \in J} a_j, \) where \( J = \{0, 1, 2, 3, 16, 17, 18, 19\}. \)

The proof is by induction on \( n. \) Clearly (1) and (2) hold when \( n = 1. \) Suppose (1) and (2) hold for \( n > 1. \) Thus we have

\[
b^{n+1}_0 = b^n_0 + b^n_1 = \sum_{j \in J} a_j + \sum_{j \in J} a_{j+1}.
\]

There are three cases depending on \( n = \sum_{s=0}^{N} a_s 2^s: \)
(i) \( n = \sum_{i=1}^{N} a_i 2^i \),
(ii) \( n = \sum_{i=0}^{I-1} 2^i + \sum_{i=I+1}^{N} a_i 2^i \), \( 1 \leq I \leq N-2 \),
(iii) \( n = \sum_{i=0}^{N} 2^i \).

For each case \( n+1 \) is

(i) \( n + 1 = \sum_{i=0}^{N} a_i 2^i \), \( a_0 = 1 \),
(ii) \( n+1 = 2^I + \sum_{i=I+1}^{N} a_i 2^i \), \( 1 \leq I \leq N-2 \),
(iii) \( n + 1 = 2^N + 1 \).

Now (3) gives \( b_{n+1}^* = \sum_{j=1} J a_j \), where \( J \) is

(i) \( J = \{ j = \sum_{s=0}^{N-1} \beta_s 2^s \mid \alpha_s = 0 \Rightarrow \beta_s = 0 \text{ for } s \geq 1 \} \),
(ii) \( J = \{ j = \sum_{s=1}^{N-1} \beta_s 2^s \mid \alpha_s = 0 \Rightarrow \beta_s = 0 \text{ for } s > I \} \),
(iii) \( J = \{ 0, N+1 \} \).

Thus (1) is shown; (2) follows similarly.

**COROLLARY 1.** Let \( A_0 = (a_i) \). Then

\[ A_{2n} = (a_i + a_{i+2^n}). \]  \( (4) \)

Two \( k \)-tuples \((a_i)\) and \((b_i)\) are said to be inverses if \( a_i + b_i \equiv 1 \pmod{2} \) for \( i = 0, 1, \ldots, k-1 \). We denote the inverse of \((a_i)\) by \((a_i)^*\). The next lemma shows that inverses have the same successor.

**LEMMA 4.** For any tuple \((a_i)\), \((a_i)^* = (a_i)\).

**Proof:** The proof is immediate by considering the various possibilities \( a_i \) and \( a_{i+1} \).

A \( k \)-tuple \( A = (a_i) \) is said to be even if \( \sum_{i=0}^{k-1} a_i \equiv 0 \pmod{2} \). A tuple which is not even is odd. We can now characterize those tuples which are successors.

**LEMMA 5.** A tuple \( A_0 = (a_i) \) is a successor of a tuple \( A_{-1} = (b_i) \) if and only if \( A_0 \) is an even tuple.

**Proof:** If \( A_0 \) is a successor of \( A_{-1} \), then

\[ a_i \equiv b_i + b_{i+1}, \quad i = 0, \ldots, k-1 \]

(recall that addition is modulo 2). Thus

\[ \sum_{i=0}^{k-1} a_i \equiv \sum_{i=0}^{k-1} (b_i + b_{i+1}) = 2 \sum_{i=0}^{k-1} b_i \equiv 0 \pmod{2} \]

and \( A_0 \) is even.
Now suppose \( A_0 \) is even. We construct a predecessor \( A_{-1} \) of \( A_0 \) as follows:

\[
\begin{align*}
    b_0 &= 1, \\
    b_j &= b_{j-1} + a_{j-1}, \quad j = 1, \ldots, k - 1.
\end{align*}
\]

By definition \( a_i \equiv b_i + b_{i+1}, \ i = 0, \ldots, k - 2 \). By (5)

\[
\sum_{j=1}^{k-1} (b_j + b_{j-1}) = \sum_{j=1}^{k-1} a_{j-1}
\]

which is equivalent to

\[
b_0 + b_{k-1} \equiv \sum_{i=0}^{k-2} a_i.
\]

Since \( A_0 \) is even, \( \sum_{i=0}^{k-2} a_i \equiv a_{k-1} \) (mod 2). Thus \( b_0 + b_{k-1} \equiv a_{k-1} \) and \( (b_i) = (a_i) \). This completes the proof. Note that the inverse of \( A_{-1} \) is also a predecessor of \( A_0 \).

We seek to characterize those \( k \)-tuples which are in a cycle. In order to do this we need to generalize the idea of an even tuple. Suppose \( k = 2^r k' \), where \( k' \) is odd and greater than one. We say a \( k \)-tuple is \( r \)-even if

\[
\sum_{i=0}^{k'-1} a_{2^r i + j} \equiv 0 \pmod{2}, \quad j = 0, \ldots, 2^r - 1.
\]

For example, if \( k = 12 \), then \( A = (a_i) \) is 2-even if

\[
\begin{align*}
    a_0 + a_4 + a_8 &\equiv 0, \\
    a_1 + a_5 + a_9 &\equiv 0, \\
    a_2 + a_6 + a_{10} &\equiv 0, \\
    a_3 + a_7 + a_{11} &\equiv 0.
\end{align*}
\]

Note that if \( k \) is odd, then a tuple is 0-even if and only if it is even. It is \( r \)-even tuples which are tuples in cycles. To prove this we need the following lemma.

**Lemma 6.** Let \( k = 2^r k' \). Suppose \( A_0 = (a_i) \) is \( r \)-even. Then \( A_0 \) has a predecessor \( A_{-1} \) which is \( r \)-even.

**Proof.** First suppose \( r = 0 \). Then by Lemma 5, \( A_0 \) has two predecessors which are inverses. Since \( k \) is odd, exactly one of these predecessors is even.
Now suppose $r > 0$. Since $A_0$ is $r$-even, it is even and hence by Lemma 5 has predecessors $B = (b_i)$ and $\bar{B} = (\bar{b}_i)$. Let

$$\sigma_j = \sum_{i=0}^{k'-1} b_{2^r i + j}, \quad j = 0, \ldots, 2^r - 1.$$  \hspace{1cm} (7)

Since $a_i \equiv b_i + b_{i+1}$,

$$0 \equiv \sum_{i=0}^{k'-1} a_{2^r i} = \sigma_0 + \sigma_1.$$  

Thus either

(a) $\sigma_0 \equiv \sigma_1 \equiv 0 \mod 2$

or

(b) $\sigma_0 \equiv \sigma_1 \equiv 1 \mod 2$.

If (b) holds, then $\sigma_0 \equiv 0 \mod 2$ where $\sigma_i$ is defined as in (7) for the tuple $\bar{B}$. Thus we may assume (a) holds. By considering $\sum_{i=0}^{k'-1} a_{2^r i+1}$ we find $\sigma_1 \equiv 0 \mod 2$ and thus $B$ is $r$-even. Note that if $B$ is $r$-even, its inverse $\bar{B}$ is not $r$-even.

**Theorem 2.** Let $k = 2^r k'$. A $k$-tuple is in a cycle if and only if it is $r$-even.

**Proof.** Suppose $A_0$ is $r$-even. By Lemma 6, $A_0$ has a predecessor $A_{-1}$ which is $r$-even. Likewise $A_{-1}$ has an $r$-even predecessor $A_{-2}$, and so forth. Since there are only a finite number of $r$-even $k$-tuples, there exists an $n$ such that $A_{-n} = A_{-j}$, $0 \leq j \leq n - 1$. Let $n$ be as small as possible. Then $A_{-n}, A_{-n+1}, \ldots, A_{-j-1}$ forms a cycle. But $A_{-j-1} = A_{-j}$ and thus $A_{-n} = A_0$.

Now suppose that $A_0 = (a_i)$ is in a cycle. Then there exist $A_{-1}, A_{-2}, \ldots, A_{-2^r}$ such that $A_{-i} = A_{-i+1}$; note that the $A_{-i}$ need not be distinct. Let $A_{-2^r} = (b_i)$. Then by (4)

$$a_j = b_j + b_{j+2^r}.$$  

Thus we have

$$\sum_{i=0}^{k'-1} a_{2^r i + j} = \sum_{i=0}^{k'-1} (b_{2^r i + j} + b_{2^r (i+1) + j}) = 2 \sum_{i=0}^{k'-1} b_{2^r i + j} \equiv 0 \mod 2$$

and $A_0$ is $r$-even.

Thus for $k = 2^r k'$ exactly $2^{k-2^r}$ of the $2^k$ $k$-tuples are in a cycle. It is now relatively easy to characterize the lengths of the non-trivial cycles.
THEOREM 3. Let \( k = 2'k' \) with \( k' \) odd and greater than one; \( r \geq 0 \). Let \( m \) be the order of 2 in \( U_{k'} \), the group of units of \( \mathbb{Z}_{k'} \). Then the maximum length of any cycle is \( 2'(2^m - 1) \). Further, if a cycle has length \( l \), then \( l \) divides \( 2'(2^m - 1) \).

Proof. By (4), for any \( A_0 = (a_i) \), \( A_{2^r} = (a_i + a_{i+2^r}) \). Now \( 2^m \equiv 1 \pmod{k'} \) implies \( 2^{m+r} \equiv 2^r \pmod{k} \). Since subscripts are reduced modulo \( k \),

\[ A_{2^r} = A_{2^m+r} \]

Thus the maximum length of any cycle is \( 2^{r+m} - 2^r \) and for every cycle of length \( l \), \( l \) divides \( 2'(2^m - 1) \).

Using an observation of Zvengrowski [9], Richman has characterized the length of all cycles of \( k \)-tuples.

THEOREM 4 (Richman [8]). Let \( k \) be odd and \( F \) be a splitting field of \( x^k - 1 \) over \( \mathbb{Z}_2 \). Then \( m \) is the length of some cycle of \( k \)-tuples if and only if \( m \) is the least common multiple of some subset of

\[ \{\text{ord}_{F}(y+1) : y \in F, y^n = 1, \text{ and } y \neq 1\} \]

Here \( \text{ord}_{F}(y+1) \) denotes the order of \( y+1 \) in the multiplicative group \( F^* \).

REFERENCES