A SIMPLE RECURRENCE RELATION IN FINITE ABELIAN GROUPS

H. P. YAP
University of Singapore, Singapore 10

A finite abelian group G is said to have a simple recurrence relation of length n if there exist distinct nonzero elements $a_1, a_2, \cdots, a_n$ of G such that $a_1 + a_2 = a_3$, $a_2 + a_3 = a_4$, $\cdots$, $a_{n-2} + a_{n-1} = a_n$, $a_{n-1} + a_n = a_1$ and $a_n + a_1 = a_2$. It is proved that if $n = 6m$ or $n = 2^\alpha 3^\beta m$ (≥ 3), where $(6, m) = 1$, $\alpha = 0, 2$, or 3 and $\beta = 0, 1$, or 2, then there exists a finite abelian group which has a simple recurrence relation of length n.

Let G be a finite abelian group written additively and $a_1, a_2, \cdots, a_n$ be distinct nonzero elements of G. If

$$a_1 + a_2 = a_3,\ a_2 + a_3 = a_4,\ \cdots,\ a_{n-2} + a_{n-1} = a_n,$$
$$a_{n-1} + a_n = a_1 \quad \text{and} \quad a_n + a_1 = a_2,$$

then we say that the ordered set

$$A = \{a_1, a_2, \cdots, a_n\}$$

has a simple recurrence relation (SRR). If G has an ordered subset A such that the cardinal of A is n (≥ 3) and A has a SRR, then we say that G has a SRR of length n. We use the notation $\ell(G) = n$ to mean that G has a SRR of length n.

Suppose

$$A = \{a_1, a_2, \cdots, a_n\}$$

has a SRR; then we have

$$a_3 = a_1 + a_2,\ a_4 = a_1 + 2a_2,\ a_5 = 2a_1 + 3a_2,\ \cdots .$$

Let

$$U_0 = 0,\ U_1 = 1,\ U_2 = 1,\ U_3 = 2,\ U_4 = 3,\ U_5 = 5, \cdots,\ U_{i+2} = U_i + U_{i+1}, \cdots,$$

be a Fibonacci sequence ([1], p. 148). Then

$$\text{(1)} \qquad U_i = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^i - \left(\frac{1-\sqrt{5}}{2}\right)^i\right], \quad i \geq 0 .$$

Thus

$$\text{(2)} \qquad a_{2+i} = U_i a_1 + U_{i+1} a_2 , \quad i \geq 0 .$$

From $a_{n-1} + a_n = a_1$ and $a_n + a_1 = a_2$, we have

$$\text{(3)} \qquad (U_{n-1} - 1)a_1 + U_n a_2 = 0$$

and

$$\text{(4)} \qquad (U_{n-2} + 1)a_1 + (u_{n-1} - 1)a_2 = 0 .$$

Let

$$h(n) = (U_{n-2} + 1)U_n - (U_{n-1} - 1)^2, \quad n \geq 2 ,$$
$$d = (U_{n-1} - 1), \; U_n) ,$$

the g.c.d. of U_{n-1} and U_n, and

$$f(n) = \frac{1}{d} h(n) .$$

Using (1), we can verify

$$\text{(5)} \qquad U_j U_n - U_{n+1}U_{n-1} = (-1)^{j+1} U_{n-j-1}, \quad j < n .$$

Now

$$
\begin{aligned}
h(n) &= (U_{n-2} + 1)(U_{n-2} + U_{n-1}) - (U_{n-1} - 1)^2 \\
&= U_{n-2}^2 - U_{n-1}^2 + U_{n-2}U_{n-1} + U_{n-2} + 3U_{n-1} - 1 \\
&= (U_{n-2} + U_{n-1})(U_{n-2} - U_{n-1}) + U_{n-2}U_{n-1} + U_{n-1} + U_{n+1} - 1 \\
&= -U_{n-3}U_n + U_{n-2}U_{n-1} + U_{n-1} + U_{n+1} - 1 \\
&= (-1)^{n-1}U_2 + U_{n-1} + U_{n+1} - 1 \quad \text{(by (5))}
\end{aligned}
$$

Define

$$\delta_n = \begin{cases} 1 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$$

Then we have

$$h(n) = U_{n-1} + U_{n+1} - 2\delta_n \tag{6}$$

Eliminate a_2 from (3) and (4), and we have $f(n)a_1 = 0$ and thus by permutation, we have

$$f(n)a_i = 0 \quad \text{for every} \quad i = 1, 2, \cdots, n. \tag{7}$$

Before we proceed further, we list some examples below. We use C_m to denote the cyclic group of order m and $C_m \times C_n$ as the cartesian product of C_m and C_n.

(E1) $A = \{(0,1), (1,0), (1,1)\}$ has a SRR in $C_2 \times C_2$;

(E2) $A = \{1, 3, 4, 2\}$ has a SRR in C_5;

(E3) $A = \{1, 4, 5, 9, 3\}$ has a SRR in C_{11};

(E4) $A = \{(1, 0), (1,1), (0,1), (1,2), (1,3), (0,1)\}$ has a SRR in $C_2 \times C_4$;

(E5) $A = \{1, -5, -4, -9, -13, 7, -6\}$ has a SRR in C_{29};

(E6) $A = \{(1,2,1), (1,1,3), (2,0,4), (0,1,2), (2,1,1), (2,2,3), (1,0,4), (0,2,2)\}$ has a SRR in $C_3 \times C_3 \times C_5$;

(E7) $A = \{1, 5, 6, 11, 17, 9, 7, 16, 4\}$ has a SRR in C_{19};

(E8) $A = \{1, 8, 9, 6, 4, 10, 3, 2, 5, 7\}$ has a SRR in C_{11}.

We write $\ell(G) \neq n$ if G does not contain any subset A whose cardinal is n, such that A has a SRR. We note that

(i) because of (7), $\ell(C_4) \neq 3$, $\ell(C_8) \neq 6$;

(ii) since $(7, f(i)) = 1$ for $i = 3, 4, 5, 6$ and $(13, f(i)) = 1$ for $i = 3, 4, \cdots, 12$, therefore both C_7 and C_{13} have no SRR of any length;

(iii) although $f(8) = 15$, $\ell(C_{15}) \neq 8$; if $\{a_1, a_2, \cdots, a_8\}$ has a SRR in C_{15}, then from (4), we have $3a_2 \equiv 9a_1 \pmod{15}$ and thus $a_2 \equiv -2a_1, 3a_1$, or $8a_1 \pmod{15}$.

<u>Case 1</u>: If $a_2 = -2a_1$, then $a_3 = -a_1, \cdots, a_8 = -3a_1 = a_4$, which is impossible.

<u>Case 2</u>: If $a_2 = 3a_1$, then $a_3 = 4a_1, \cdots, a_6 = 3a_1 = a_2$, which is impossible.

<u>Case 3</u>: If $a_2 = 8a_1$, then $a_3 = 9a_1, \cdots, a_7 = 9a_1 = a_3$, which is impossible.

Now we prove

<u>Lemma 1</u>: If

$$(U_n, f(n)) = 1, \quad n \neq 2(2m+1),$$

then $\ell(C_f(n)) = n$.

<u>Proof</u>: Since $(U_n, f(n)) = 1$, therefore

$$d = (U_{n-1} - 1, U_n) = 1,$$

and thus

$$f(n) = h(n) = U_{n-1} + U_{n+1} - 2\delta_n. \tag{8}$$

Also, there exist r and t such that

$$rU_n + tf(n) = 1 \quad . \tag{9}$$

From (3), we have

$$r(U_{n-1} - 1)a_1 + rU_n a_2 = 0 \, .$$

Substitute $rU_n = 1 - tf(n)$ into the above equation and make use of the result of (7); we have

$$a_2 = r(1 - U_{n-1})a_1 \quad . \tag{10}$$

Thus

$$a_3 = a_1 + a_2 = [r(1 - U_{n-1}) + 1]a_1 \, ,$$

and in general,

$$a_{2+i} = [rU_{i+1}(1 - U_{n-1}) + U_i]a_1, \quad 0 \le i \le n - 2 \quad . \tag{11}$$

Now we prove that $A = \{a_1, a_2, \cdots, a_n\}$, where a_1 is chosen such that $(a_1, f(n)) = 1$ and a_{2+i}, $0 \le i \le n - 2$ is given by (11), has a SRR.

We need to verify

(I) $a_1, a_2, \cdots, a_n$ considered as elements in $C_{f(n)}$, are distinct and nonzero;

(II) $a_1 + a_2 = a_3$, $a_2 + a_3 = a_4$, $\cdots$, $a_{n-2} + a_{n-1} = a_n$, $a_{n-1} + a_n = a_1$, and $a_n + a_1 = a_2$.

First we prove (II):

For this part, we need only to verify that $a_{n-1} + a_n = a_1$ and $a_n + a_1 = a_2$. In fact,

$$\begin{aligned} a_{n-1} + a_n = [rU_n(1 - U_{n-1}) + U_{n-1}]a_1 &= [(1 - U_{n-1}) + U_{n-1}]a_1 \quad \text{(by (9))} \\ &= a_1 \, ; \end{aligned}$$

$$a_n + a_1 = [rU_{n-1}(1 - U_{n-1}) + U_{n-2} + 1]a_1$$
$$= U_{n-1}a_2 + (U_{n-2} + 1)a_1 .$$

Since

$$f(n) = (U_{n-2} + 1)U_n - (U_{n-1} - 1)^2 ,$$

therefore,

$$rU_n(U_{n-2} + 1)a_1 + r(1 - U_{n-1})(U_{n-1} - 1)a_1 = 0 ,$$

from which it follows that

$$(U_{n-2} + 1)a_1 + (U_{n-1} - 1)a_2 = 0 .$$

Hence $a_n + a_1 = a_2$.

To prove (I), we shall show that

(12) $$rU_{i+1}(1 - U_{n-1}) + U_i \neq rU_{j+1}(1 - U_{n-1}) + U_j, \quad 0 \leq i < j \leq n - 2 ,$$

(13) $$rU_{i+1}(1 - U_{n-1}) + U_i \neq 1, \quad 0 \leq i \leq n - 2 ;$$

and

(14) $$rU_{i+1}(1 - U_{n-1}) + U_i \neq 0, \quad 0 \leq i \leq n - 2 .$$

Suppose for some i,j such that $0 \leq i < j \leq n - 2$,

$$rU_{i+1}(1 - U_{n-1}) + U_i = rU_{j+1}(1 - U_{n-1}) + U_j .$$

then

$$r(U_{j+1} - U_{i+1})(1 - U_{n-1}) + (U_j - U_i) = 0$$

and thus

$$rU_n(U_{j+1} - U_{i+1})(1 - U_{n-1}) + U_n(U_j - U_i) = 0 ,$$

from which it follows that

$$(U_{j+1} - U_{i+1})(1 - U_{n-1}) + U_n(U_j - U_i) = 0 ,$$

i.e.,

$$(U_jU_n - U_{j+1}U_{n-1}) - (U_iU_n - U_{i+1}U_{n-1}) + U_{j+1} - U_{i+1} = 0 .$$

Applying (5), we have

$$g(i,j) \equiv (-1)^{j+1}U_{n-j-1} + (-1)^iU_{n-i-1} + U_{j+1} - U_{i+1} = 0, \quad 0 \le i < j \le n - 2 . \tag{15}$$

We can verify that

$$-f(n) \le g(i,j)(\ne 0) \le f(n) .$$

Hence (15) cannot be true.

Similarly, if

$$rU_{i+1}(1 - U_{n-1}) + U_i = 1, \quad 0 \le i \le n - 2 ,$$

then

$$rU_nU_{i+1}(1 - U_{n-1}) + U_n(U_i - 1) = 0 ,$$

which implies that

$$U_{i+1}(1 - U_{n-1}) + U_n(U_i - 1) = 0 ,$$

i.e.,

$$(U_iU_n - U_{i+1}U_{n-1}) + U_{i+1} - U_n = 0$$

or

(16) $$k(i) = (-1)^{i+1}U_{n-i-1} + U_{i+1} - U_n = 0, \quad 0 \le i \le n - 2 .$$

We can also verify that

$$-f(n) < k(i)(\neq 0) < f(n) .$$

Hence (16) cannot be true.

Finally, if

$$rU_{i+1}(1 - U_{n-1}) + U_i = 0, \quad 0 \le i \le n - 2 ,$$

then

(17) $$w(i) \equiv (-1)^{i+1}U_{n-i-1} + U_{i+1} = 0, \quad 0 \le i \le n - 2 .$$

But for $n \neq 2(2m + 1)$, $w(i) \neq 0$, and $-f(n) < w(i) < f(n)$. Hence (17) cannot be true.

The proof of Lemma 1 is complete.

Lemma 2. Let G_1, G_2 be two finite abelian groups. If

$$\ell(G_1) = m, \quad \ell(G_2) = n, \quad m < n, \quad (m,n) = d,$$

then

$$\ell(G_1 \times G_2) = \frac{1}{d}mn .$$

Proof: Let

$$A = \{a_1, a_2, \cdots, a_m\}$$

be a subset of G_1 such that A has a SRR and

$$B = \{b_1, b_2, \cdots, b_n\}$$

be a subset of G_2 such that B has a SRR. Then we can prove that

$$A \otimes B = \{c_1, c_2, \cdots, c_s\}$$

where

$$s = \frac{1}{d} mn$$

and

$$c_1 = (a_1, b_1), \ c_2 = (a_2, b_2), \ c_3 = c_1 + c_2 = (a_3, b_3), \cdots, c_m = (a_m, b_m),$$
$$c_{m+1} = (a_1, b_{m+1}), \cdots, c_s = (a_m, b_n),$$

has a SRR in $G_1 \times G_2$.

Lemma 3: If $(n, 6) = 1$, then $(U_n, f(n)) = 1$.

Proof: We observe that U_n is even if and only if $n = 3m$. Hence if $(n, 3) = 1$, then U_n is odd.

Now, $(n, 2) = 1$ implies that

$$f(n) = \frac{1}{d} (U_{n-1} + U_{n+1}).$$

It can be proved that if U_n is odd, then $(U_n, U_{n=1} + U_{n+1}) = 1$ ([1], p. 148).

It is clear that $(U_n, h(n)) = 1$ implies that $d = 1$. Hence $f(n) = U_{n-1} + U_{n+1}$, and thus $(U_n, f(n)) = 1$.

From Lemmas 1 and 3, we have

Lemma 4: If $(n, 6) = 1$, then $\ell(C_{f(n)}) = n$.

From (E1), (E2), (E6), (E7), Lemmas 2 and 4, we have

Theorem 1: If

$$n = 6m \quad \text{or} \quad n = 2^{\alpha}3^{\beta}m \ (\geq 3),$$

where $(6, m) = 1$, $\alpha = 0, 2$, or 3 and $\beta = 0, 1$, or 3, then there exists a finite abelian group G such that $\ell(G) = n$.

REFERENCE

1. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Clarendon Press, Oxford, 4th Ed., 1960.