A talk given at Nanjing Univ. Inform. Sci. & Tech. (March 8, 2016)
and Central China Normal Univ. (March 13, 2016)
and Hefei Univ. Tech. (March 25, 2016)
and Workshop on Graph Theory and Comb. of Yangtze Delta
(Nanjing Normal Univ., April 16, 2016)

A new result in combinatorial number theory

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

April 16, 2016

Abstract

Let G be a finite abelian group with exponent $n > 1$. For $a_1, \ldots, a_{n-1} \in G$, we determine completely when there is a permutation σ on $\{1, \ldots, n-1\}$ such that $sa_{\sigma(s)} \neq 0$ for all $s = 1, \ldots, n-1$. When G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$, this confirms a conjecture of Z.-W. Sun motivated by his study of covering systems. The work is joint with Fan Ge, a former student of the speaker.

Part I. Covering systems and subset sums

Covering systems of residue classes

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, let

$$a(\bmod\ n) = a + n\mathbb{Z} = \{a + nq :\ q \in \mathbb{Z}\}.$$

For a finite system $A = \{a_s(\bmod\ n_s)\}_{s=1}^k$ of residue classes, if $\bigcup_{s=1}^k a_s(\bmod\ n_s) = \mathbb{Z}$ then we call A a *covering system*; if A covers each integer exactly once then A is called an *exact covering system*.

The concept of covering system was introduced by Paul Erdős in 1950's who gave the following example:

$$\{0(\bmod\ 2),\ 0(\bmod\ 3),\ 1(\bmod\ 4),\ 5(\bmod\ 6),\ 7(\bmod\ 12)\}.$$

Another Example.

$$A = \{1(\bmod\ 2), 2(\bmod\ 2^2), \ldots, 2^{k-1}(\bmod\ 2^k), 0(\bmod\ 2^k)\}$$

is an exact covering system. Note that $B = \{2^{s-1}(\bmod\ 2^s)\}_{s=1}^k$ covers $1, \ldots, 2^k - 1$ but it does not cover 0.

Erdős' conjecture

In 1965, P. Erdős offered \$25 prize for a proof of his following conjecture which is a refinement of Stein's conjecture on exact covering systems.

Erdős' Conjecture $A = \{a_s (\mathrm{mod}\ n_s)\}_{s=1}^k$ is a covering system if it covers all those integers from 1 to 2^k.

Remark. The 2^k in Erdős' conjecture is best possible because $\{2^{s-1} (\mathrm{mod}\ 2^s)\}_{s=1}^k$ covers $1, \ldots, 2^k - 1$ but does not cover any multiple of 2^k.

In 1969–1970 R. B. Crittenden and C. L. Vanden Eynden [Bull. Amer. Math. Soc. 1969; Proc. Amer. Math. Soc. 1970] supplied a long and awkward proof of the Erdős conjecture for $k \geqslant 20$, which involves some deep results concerning the distribution of primes.

A local-global theorem

As usual, the fractional part of a real number x is denoted by $\{x\}$.

For real numbers α and $\beta > 0$, we define

$$\alpha + \beta\mathbb{Z} := \{\alpha + \beta x : \ x \in \mathbb{Z}\}.$$

A Local-Global Theorem (Z.-W. Sun [Acta Arith. 72(1995)]) Let $\alpha_1, \ldots, \alpha_k$ be real numbers and $\beta_1, \ldots, \beta_k$ be positive real numbers. Then $A = \{\alpha_s + \beta_s\mathbb{Z}\}_{s=1}^k$ covers all the integers at least m times if it covers $|S|$ consecutive integers at least m times, where

$$S = \left\{ \left\{ \sum_{s \in I} \frac{1}{\beta_s} \right\} : \ I \subseteq \{1, \ldots, k\} \right\}.$$

Remark. For $1 \leqslant m \leqslant k$, clearly an integer x is covered by $A = \{\alpha_s + \beta_s\mathbb{Z}\}_{s=1}^k$ at least m times if and only if it is covered by $\{\alpha_s + \beta_s\mathbb{Z}\}_{\substack{s=1 \\ s \notin J}}^k$ for all $J \subseteq \{1, \ldots, k\}$ with $|J| = m - 1$. So the theorem is reduced to the case $m = 1$.

Proof of the Local-Global Theorem with $m = 1$

For any integer x, clearly

$$\begin{aligned} & x \text{ is covered by } A \\ \iff & e^{2\pi i(\alpha_s - x)/\beta_s} = 1 \text{ for some } s = 1, \ldots, k \\ \iff & \prod_{s=1}^{k} \left(1 - e^{2\pi i(\alpha_s - x)/\beta_s}\right) = 0 \\ \iff & \sum_{I \subseteq \{1,\ldots,k\}} (-1)^{|I|} e^{2\pi i \sum_{s\in I} \alpha_s/\beta_s} \cdot e^{-2\pi i x \sum_{s\in I} 1/\beta_s} = 0 \\ \iff & \sum_{\theta \in S} e^{-2\pi i x\theta} z_\theta = 0, \end{aligned}$$

where

$$z_\theta = \sum_{\substack{I \subseteq \{1,\ldots,k\} \\ \{\sum_{s\in I} 1/\beta_s\} = \theta}} (-1)^{|I|} e^{2\pi i \sum_{s\in I} \alpha_s/\beta_s}.$$

Proof of the Local-Global Theorem with $m = 1$

Suppose that A covers $|S|$ consecutive integers

$$a, a+1, \ldots, a+|S|-1$$

where $a \in \mathbb{Z}$. By the above,

$$\sum_{\theta \in S} (e^{-2\pi i\theta})^r (e^{-2\pi i a\theta} z_\theta) = 0$$

for $r = 0, 1, \ldots, |S|-1$. As the determinant

$$\|(e^{-2\pi i\theta})^r\|_{0 \leqslant r < |S|,\, \theta \in S}$$

is of Vandermonde's type and hence nonzero, by Cramer's rule we have $z_\theta = 0$ for all $\theta \in S$. Therefore

$$\sum_{\theta \in S} e^{-2\pi i x\theta} z_\theta = 0$$

for all $x \in \mathbb{Z}$, i.e., any $x \in \mathbb{Z}$ is covered by A.

An application of the Local-Global Theorem

Theorem. Let $m_1, \ldots, m_{n-1}$ $(n > 1)$ be integers. If there is a permutation $\sigma \in S_{n-1}$ such that $n \nmid s m_{\sigma(s)}$ for all $s = 1, \ldots, n-1$, then the set

$$\left\{ \sum_{i \in I} m_i : \ I \subseteq \{1, \ldots, n-1\} \right\}$$

contains a complete system of residues modulo n.

Proof. $A = \{s + (n/m_{\sigma(s)})\mathbb{Z}\}_{s=1}^{n-1}$ covers $1, \ldots, n-1$ but it does not cover 0. By the Local-Global Theorem, the fractional parts

$$\left\{ \sum_{s \in I} \frac{1}{n/m_{\sigma(s)}} \right\} \quad (I \subseteq \{1, \ldots, n-1\})$$

must have more than $n-1$ distinct values. Thus, the set

$$\left\{ \sum_{i \in I} m_i : \ I \subseteq \{1, \ldots, n-1\} \right\} = \left\{ \sum_{s \in I} m_{\sigma(s)} : \ I \subseteq \{1, \ldots, n-1\} \right\}$$

contains a complete system of residues modulo n.

Another Local-Global Theorem

The characteristic function of a residue class is a periodic arithmatical map. Dirichlet characters are also periodic functions. If an element a in an additive abelian group G has order n, then the map $\psi : \mathbb{Z} \to G$ given by $\psi(x) = xa$ is periodic mod n.

Another Local-Global Theorem (Z.-W. Sun [J. Algebra, 293(2005)]). Let G be any additive abelian group, and let $\psi_1, \ldots, \psi_k$ be maps from $\mathbb{Z}$ to G with periods $n_1, \ldots, n_k \in \mathbb{Z}^+$ respectively. Then the function $\psi = \psi_1 + \cdots + \psi_k$ is constant if $\psi(x)$ equals a constant for $|T|$ consecutive integers x, where

$$T = \bigcup_{s=1}^{k} \left\{ \frac{r}{n_s} : r = 0, 1, \ldots, n_s - 1 \right\}.$$

Corollary. $A = \{a_s (\mathrm{mod}\ n_s)\}_{s=1}^k$ covers any integer exactly m times if it covers $|\bigcup_{s=1}^k \{r/n_s :\ r = 0, \ldots, n_s - 1\}|$ $(\leqslant \sum_{s=1}^k n_s - k + 1)$ consecutive integers exactly m times.

A natural question

Let $m_1, \ldots, m_{n-1}$ $(n > 1)$ be integers. Now it is natural to ask when there is a permutation $\sigma \in S_{n-1}$ such that $n \nmid s m_{\sigma(s)}$ for all $s = 1, \ldots, n-1$. Clearly, this happens if $(m_s, n) = 1$ for all $s = 1, \ldots, n-1$. So we have

Corollary (Z.-W. Sun [Eletron. Res. Announc. Amer. Math. Soc., 9(2003)]). Let $m_1, \ldots, m_{n-1}$ $(n > 1)$ be integers all relatively prime to n. Then the subset sums $\sum_{i \in I} m_i$ $(I \subseteq \{1, \ldots, n-1\})$ contain a complete system of residues modulo n.

If there is such a permutation $\sigma \in S_{n-1}$ such that $n \nmid s m_{\sigma(s)}$ for all $s = 1, \ldots, n-1$, then for each positive divisor d of n we have

$$|\{1 \leqslant c < d : \ d \nmid m_{\sigma(cn/d)}\}| \geqslant \left|\left\{1 \leqslant c < d : \ n \nmid \frac{cn}{d} m_{\sigma(cn/d)}\right\}\right| = d - 1,$$

and hence the sequence $\{m_s\}_{s=1}^{n-1}$ has the following property:

$$\left|\{1 \leqslant s < n : \ d \nmid m_s\}\right| \geqslant d - 1 \ \text{ for any } d \in D(n), \qquad (*)$$

where $D(n)$ denotes the set of all positive divisors of n.

Combinatorial Nullstellensatz

Let $m_1, \ldots, m_{n-1}$ be integers with $(m_s, n) \leqslant s$ for all $s = 1, \ldots, n-1$. Then the condition $(*)$ holds since for any $d \in D(n)$ we have

$$|\{1 \leqslant s < n : \ d \nmid m_s\}| \geqslant |\{1 \leqslant s < n : \ s < d\}| = d - 1.$$

Via Alon's Combinatorial Nullstellensatz, we can prove that there is a permutation $\sigma \in S_{n-1}$ such that $n \nmid sm_{\sigma(s)}$ for all $s = 1, \ldots, n-1$.

Combinatorial Nullstellensatz (Alon [Comb. Probab. Comput, 1999]) Let $A_1, \ldots, A_n$ be finite subsets of a field F with $|A_i| > k_i$ for $i = 1, \ldots, n$ where $k_1, \ldots, k_n$ are nonnegative integers. If the coefficient of the monomial $x_1^{k_1} \cdots x_n^{k_n}$ in $P(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ is nonzero and $k_1 + \cdots + k_n$ is the total degree of P, then there are $a_1 \in A_1, \ldots, a_n \in A_n$ such that $P(a_1, \ldots, a_n) \neq 0$.

A theorem via the Combinatorial Nullstellensatz

Theorem (Fan Ge and Z.-W. Sun, arXiv:1601.04988). Let $m_1, m_2, \ldots, m_{n-1}$ $(n > 1)$ be integers with $(m_s, n) \leqslant s$ for all $s = 1, \ldots, n-1$. For any $a_1, \ldots, a_{n-1} \in \mathbb{Z}$, there is a function $f : \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ such that the sums

$$f(1) + a_1,\ \ldots,\ f(n-1) + a_{n-1}$$

are pairwise distinct modulo n and also none of the numbers

$$f(1)m_1,\ \ldots,\ f(n-1)m_{n-1}$$

is divisible by n.

Remark. In the case $a_1 = \cdots = a_{n-1}$, the function f in the theorem must be a permutation on $\{1, \ldots, n-1\}$.

Proof of the Theorem. Take a prime power $q \equiv 1 \pmod{n}$ and consider the finite field $\mathbb{F}_q$. As $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is a cyclic group of order $q-1$, and n is a divisor of $q-1$, there is an element $g \in \mathbb{F}_q^*$ of order n. For $i = 1, \ldots, n-1$ define

$$A_i := \{g^k :\ 1 \leqslant k \leqslant n-1 \text{ and } (g^k)^{m_i} \neq 1\}.$$

Proof of the Theorem (continued)

Then $|A_i| = n - (m_i, n) \geqslant n - i$ for all $i = 1, \ldots, n-1$. For

$$P(x_1, \ldots, x_{n-1}) := \prod_{1 \leqslant i < j \leqslant n-1} \left(g^{a_i} x_i - g^{a_j} x_j\right),$$

we clearly have

$$\begin{aligned} P(x_1, \ldots, x_{n-1}) &= \det \left|(g^{a_i} x_i)^{j-1}\right|_{1 \leqslant i,j \leqslant n-1} \\ &= \sum_{\sigma \in S_{n-1}} \operatorname{sign}(\sigma) \prod_{i=1}^{n-1} (g^{a_i} x_i)^{\sigma(i)-1}, \end{aligned}$$

where $\operatorname{sign}(\sigma)$, the sign of σ, takes 1 or -1 according as the permutation σ is even or odd. Choose $\sigma_0 \in S_{n-1}$ with $\sigma_0(i) = n - i$ for all $i = 1, \ldots, n-1$. Then the coefficient of the monomial $\prod_{i=1}^{n-1} x_i^{n-1-i}$ in $P(x_1, \ldots, x_{n-1})$ coincides with

$$\operatorname{sign}(\sigma_0) \prod_{i=1}^{n-1} (g^{a_i})^{n-i-1} \neq 0,$$

and $\deg P = \binom{n-1}{2} = \sum_{i=1}^{n-1} (n-1-i)$.

Proof of the Theorem (continued)

In view of the Combinatorial Nullstellensatz, there are $x_1 \in A_1, \ldots, x_{n-1} \in A_{n-1}$ such that $P(x_1, \ldots, x_{n-1}) \neq 0$.

Write $x_i = g^{f(i)}$ for all $i = 1, \ldots, n-1$, where $f(i) \in \{1, \ldots, n-1\}$. If $1 \leqslant i < j \leqslant n-1$, then

$$g^{a_i + f(i)} = g^{a_i} x_i \neq g^{a_j} x_j = g^{a_j + f(j)}$$

and hence

$$f(i) + a_i \not\equiv f(j) + a_j \pmod{n}.$$

For each $i = 1, \ldots, n-1$, as $(g^{f(i)})^{m_i} \neq 1$ we have $n \nmid f(i) m_i$.

So far we have completed the proof of the Theorem.

A Conjecture of Snevily

In 1952 M. Hall [Proc. Amer. Math. Soc.] obtained an extension of Cramer's conjecture.

M. Hall's theorem. Let $G = \{b_1, \ldots, b_n\}$ be an additive abelian group, and let $a_1, \ldots, a_n$ be elements of G with $a_1 + \ldots + a_n = 0$. Then there exists a permutation $\sigma \in S_n$ such that

$$\{a_{\sigma(1)} + b_1, \ldots, a_{\sigma(n)} + b_n\} = G.$$

Snevily's Conjecture on Addition modulo n. [Amer. Math. Monthly, 1999]. Let $0 < k < n$ and $a_1, \ldots, a_k \in \mathbb{Z}$. Then there exists $\pi \in S_k$ such that $a_1 + \pi(1), \ldots, a_k + \pi(k)$ are distinct modulo n.

Remark. A. E. Kézdy and H. S. Snevily [Combin. Probab. Comput. 2002] proved the conjecture for $k \leqslant (n+1)/2$ and found an application to tree embeddings.

Attack Snevily's conjecture on addition modulo n

A. E. Kézdy and H. S. Snevily [Combin. Probab. Comput. 2002] Let k and n be positive integers with $k \leqslant (n+1)/2$. Then, for any $a_1, \dots, a_k \in \mathbb{Z}$, there exists $\pi \in S_k$ such that $a_1 + \pi(1), \dots, a_k + \pi(k)$ are distinct modulo n.

Proof. Let $A = \{1, \dots, k\}$. For $x_i, x_j \in A$, since

$$|x_i - x_j| \leqslant k - 1 \leqslant \frac{n-1}{2} < \frac{n}{2},$$

we have

$$\begin{aligned} & x_i + a_i \not\equiv x_j + a_j \pmod{n} \\ \Longleftrightarrow\ & x_j - x_i \not\equiv a_i - a_j \pmod{n} \\ \Longleftrightarrow\ & x_j - x_i \neq r_{ij} \end{aligned}$$

where r_{ij} denotes the residue of $a_i - a_j$ in the interval $(-n/2, n/2]$.

Continue the proof

Thus, we only need to show that there are distinct $x_1, \ldots, x_k \in A = \{1, \ldots, k\}$ such that $x_j - x_i \neq r_{ij}$ for all $1 \leqslant i < j \leqslant k$. By the Combinatorial Nullstellensatz for the real field $\mathbb{R}$, it suffices to note that

$$
\begin{aligned}
&[x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)(x_j - x_i - r_{ij}) \\
=&[x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)^2 \\
=&[x_1^{k-1} \cdots x_k^{k-1}](\det(x_j^{i-1})_{1 \leqslant i,j \leqslant k})^2 \\
=&[x_1^{k-1} \cdots x_k^{k-1}] \sum_{\sigma \in S_k} \mathrm{sign}(\sigma) \prod_{j=1}^{k} x_j^{\sigma(j)-1} \sum_{\tau \in S_k} \mathrm{sign}(\tau) \prod_{j=1}^{k} x_j^{\tau(j)-1} \\
=& \sum_{\sigma \in S_k} \mathrm{sign}(\sigma)\mathrm{sign}(\sigma') = \sum_{\sigma \in S_k} (-1)^{\binom{k}{2}} = k!(-1)^{\binom{k}{2}} \neq 0.
\end{aligned}
$$

where $\sigma'(j) = k - \sigma(j) + 1$ for $j = 1, \ldots, k$.

Part II. Working with finite abelian groups

A conjecture of Sun

Conjecture (Z.-W. Sun, May 1, 2004). Let $m_1, \ldots, m_{n-1}$ ($n > 1$) be integers satisfying the condition

$$\left|\{1 \leqslant s < n : \ d \nmid m_s\}\right| \geqslant d - 1 \ \text{ for any } d \in D(n) \qquad (*)$$

(where $D(n)$ denotes the set of all positive divisors of n). Then there is a permutation $\sigma \in S_{n-1}$ such that $n \nmid sm_{\sigma(s)}$ for all $s = 1, \ldots, n-1$.

Note that

$$n \nmid sm_t \iff s\overline{m}_t \neq \bar{0},$$

where $\bar{a} = a + n\mathbb{Z}$ belongs to the additive cyclic group $\mathbb{Z}/n\mathbb{Z}$.

An extended version for finite abelian groups

For a finite multiplicative group G, its exponent $\exp(G)$ is defined to be the least positive integer such that $x^n = e$ for all $x \in G$, where e is the identity of G. For a finite abelian group G, $\exp(G)$ is known to be $\max\{o(x):\ x \in G\}$, where $o(x)$ denotes the order of x. If G is an additive group, then for $k \in \mathbb{Z}^+$ and $a \in G$ we write ka for the sum $a_1 + \ldots + a_k$ with $a_1 = \cdots = a_k = a$.

Theorem (F. Ge and Z.-W. Sun, arXiv:1601.04988). Let G be a finite additive abelian group with exponent $n > 1$. For any $a_1, \ldots, a_{n-1} \in G$, there is a permutation $\sigma \in S_{n-1}$ such that all the elements $sa_{\sigma(s)}$ $(s = 1, \ldots, n-1)$ are nonzero if and only if

$$\left|\left\{1 \leqslant s < n:\ \frac{n}{d}a_s \neq 0\right\}\right| \geqslant d-1 \ \text{ for all } d \in D(n). \qquad (\star)$$

Remark. Applying this theorem to the cyclic group $\mathbb{Z}/n\mathbb{Z}$, we immediately confirm the conjecture of Sun.

Proof of the Necessariness

Proof of the Necessariness. If there is a permutation $\sigma \in S_{n-1}$ such that $sa_{\sigma(s)} \neq 0$ for all $s = 1, \ldots, n-1$, then for any $d \in D(n)$ we have

$$\begin{aligned} &\left|\left\{1 \leqslant s < n : \ \frac{n}{d} a_s \neq 0\right\}\right| \\ \geqslant &\left|\left\{1 \leqslant c < d : \ \frac{cn}{d} a_{\sigma(cn/d)} \neq 0\right\}\right| = d - 1. \end{aligned}$$

Proof of the Sufficiency

Suppose that the sufficiency is false. Then there are $a_1, \ldots, a_{n-1} \in G$ satisfying $(\star)$ such that the set

$$I(\sigma) := \{1 \leqslant i < n : ia_{\sigma(i)} = 0\} = \{1 \leqslant i < n : o(a_{\sigma(i)}) \mid i\}$$

is nonempty for any $\sigma \in S_{n-1}$. Take such $a_1, \ldots, a_{n-1} \in G$ with $\sum_{s=1}^{n-1} o(a_s)$ maximal.

Choose $\sigma \in S_{n-1}$ with $|I(\sigma)|$ minimal. As $n = \exp(G)$, there is an element x of G with $o(x) = n$. Let $j \in I(\sigma)$, and for $s = 1, \ldots, n-1$ define

$$a_s^* = \begin{cases} x & \text{if } s = \sigma(j), \\ a_s & \text{otherwise.} \end{cases}$$

If $(n/d)a_{\sigma(j)} \neq 0$ with $d \in D(n)$, then $d > 1$ and $(n/d)x \neq 0$. As $o(a_{\sigma(j)}) \mid j$, we have $o(a_{\sigma(j)}) \leqslant j < n = o(x)$. Since $\sum_{s=1}^{n-1} o(a_s^*) > \sum_{s=1}^{n-1} o(a_s)$, by our choice of $a_1, \ldots, a_{n-1}$, for some $\tau \in S_{n-1}$ we have $sa^*_{\tau(s)} \neq 0$ for all $s = 1, \ldots, n-1$. For any $1 \leqslant s < n$ with $\tau(s) \neq \sigma(j)$, we have $sa_{\tau(s)} = sa^*_{\tau(s)} \neq 0$.

Proof of the Sufficiency (continued)

Thus $|I(\tau)| \leqslant 1 \leqslant |I(\sigma)|$. Combining this with the choice of σ, we see that $|I(\sigma)| = 1$.

For $\pi \in S_{n-1}$ with $|I(\pi)| = 1$, by i_π we denote the unique element of $I(\pi)$. Without loss of generality, below we assume that

$$i_\sigma = \min\{i_\pi : \ \pi \in S_{n-1} \text{ and } |I(\pi)| = 1\}.$$

For simplicity, now we just write i for i_σ. As $o(a_{\sigma(i)})$ divides both i and $n = \exp(G)$, we have $o(a_{\sigma(i)}) \mid i_n$, where $i_n = (i, n)$.

Now we show that $i \mid n$. Suppose that $i \nmid n$. Then $i_n \neq i$, $i_n \notin I(\sigma)$ and hence $0 \neq i_n a_{\sigma(i_n)}$. Thus $o(a_{\sigma(i_n)}) \nmid i_n$ and hence $o(a_{\sigma(i_n)}) \nmid i$. Therefore

$$i a_{\sigma(i i_n)(i)} = i a_{\sigma(i_n)} \neq 0 \ \text{ and } \ i_n a_{\sigma(i i_n)(i_n)} = i_n a_{\sigma(i)} = 0,$$

where $\sigma(i i_n)$ is the product of σ and the cyclic permutation $(i i_n)$. So we get $|I(\sigma(i i_n))| = 1$ and $i_{\sigma(i i_n)} = i_n < i = i_\sigma$, which contradicts $(\star)$.

Proof of the Sufficiency (continued)

Assume that $1 \leqslant j < n$ and $o(a_{\sigma(j)}) \nmid i$. Then $j \neq i$ since $o(a_{\sigma(i)}) \mid i$. For any $s = 1, \ldots, n-1$ with $s \neq i, j$, we have

$$sa_{\sigma(ij)(s)} = sa_{\sigma(s)} \neq 0.$$

Also, $ia_{\sigma(ij)(i)} = ia_{\sigma(j)} \neq 0$ since $o(a_{\sigma(j)}) \nmid i$. As $|I(\sigma(ij))| \geqslant |I(\sigma)| = 1$, we must have $0 = ja_{\sigma(ij)(j)} = ja_{\sigma(i)}$, i.e., $o(a_{\sigma(i)}) \mid j$. Since $I(\sigma(ij)) = \{j\}$, we have $j = i_{\sigma(ij)} > i = i_{\sigma}$.

Now suppose that $1 \leqslant k < i$. By the last paragraph, we must have $o(a_{\sigma(k)}) \mid i$. For any $s = 1, \ldots, n-1$ with $s \neq i, j, k$, we have $sa_{\sigma(kij)(s)} = sa_{\sigma(s)} \neq 0$. Note that $ia_{\sigma(kij)(i)} = ia_{\sigma(j)} \neq 0$. If $0 \neq ja_{\sigma(k)} = ja_{\sigma(kij)(j)}$, then we must have $I(\sigma(kij)) = \{k\}$ and hence $i_{\sigma(kij)} = k < i = i_{\sigma}$ which leads to a contradiction. Therefore, $0 = ja_{\sigma(k)}$, i.e., $o(a_{\sigma(k)}) \mid j$. Since $o(_{\sigma(k)})$ also divides i, we have $o(a_{\sigma(k)}) \mid (i, j)$.

Proof of the Sufficiency (continued)

Suppose that j is not divisible by i. Then $k := (i, j) < i$. By the last paragraph, $o(a_{\sigma(k)})$ divides $(i, j) = k$. This contradicts the fact that $ka_{\sigma(k)} \neq 0$.

In view of the above, $i \in D(n)$, and $i < j$ and $i \mid j$ for any $1 \leqslant j < n$ with $o(a_{\sigma(j)}) \nmid i$. Therefore

$$\begin{aligned} |\{1 \leqslant s < n : \ o(a_s) \nmid i\}| =& |\{1 \leqslant j < n : \ o(a_{\sigma(j)}) \nmid i\}| \\ \leqslant& |\{i < j < n : \ i \mid j\}| = \frac{n}{i} - 2, \end{aligned}$$

and hence for $d = n/i \in D(n)$ we have

$$\left|\left\{1 \leqslant s < n : \ \frac{n}{d} a_s \neq 0\right\}\right| < d - 1$$

which contradicts our condition $(\star)$.

Reference

For sources of the above work, you may loot at the preprint

Fan Ge and Zhi-Wei Sun, *A new result in combinatorial number theory*, arXiv:1601.04988. `http://arxiv.org/abs/1402.6641`.

Thank you!