Journal of Number Theory 130 (2010) 815–827

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

An application of Fourier transforms on finite Abelian groups to an enumeration arising from the Josephus problem

Gregory L. Wilson [a,*,1], Christopher L. Morgan [b]

[a] BerrieHill Research Corporation, Dayton, OH 45459, United States
[b] California State University East Bay, Hayward, CA 94542, United States

ARTICLE INFO

Article history:
Received 7 April 2006
Revised 3 October 2009
Available online 4 February 2010
Communicated by Ronald Graham

MSC:
05A15
11D45
11D79
43A25

Keywords:
Fourier transform on groups
Josephus problem
Hermite normal form
Smith normal form

ABSTRACT

Text. We analyze an enumeration associated with the Josephus problem by applying a Fourier transform to a multivariate generating function. This yields a formula for the enumeration that reduces to a simple expression under a condition we call local prime abundance. Under this widely held condition, we prove (Corollary 3.4) that the proportion of Josephus permutations in the symmetric group S_n that map t to k (independent of the choice of t and k) is $1/n$. Local prime abundance is intimately connected with a well-known result of S.S. Pillai, which we exploit for the purpose of determining when it holds and when it fails to hold. We pursue the first case where it fails, reducing an intractable DFT computation of the enumeration to a tractable one. A resulting computation shows that the enumeration is nontrivial for this case.

Video. For a video summary of this paper, please click here or visit http://www.youtube.com/watch?v=DnZi-Znuk-A.

1. Introduction

The ancient problem of Josephus[2] begins with an arrangement of the first n positive integers in numerical order clockwise around a circle. These are eliminated from the circle one at a time through

* Corresponding author.
E-mail addresses: glwilson@berriehill.com (G.L. Wilson), christopher.morgan@csueastbay.edu (C.L. Morgan).

[1] Thanks to Peter L. Montgomery who provided a key reference and helped with Proposition 3.2.

[2] Flavius Josephus was a Jewish historian (ca. 37 CE–ca. 95 CE) and is frequently referenced by biblical scholars, although never actually mentioned in the Bible.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2009.11.004

the use of a counting parameter denoted here by d. The first integer eliminated is determined by counting d integers in sequence starting at 1. Beginning again from the integer previously eliminated, subsequent integers are eliminated by continuing to count d integers in sequence among those remaining. The order of elimination determines a permutation of S_n, which following I. Kaplansky [10] we denote by $J_{n,d}$. For example,

$$J_{8,2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 3 & 7 & 5 & 1 \end{pmatrix}.$$

The Josephus problem is to determine the last integer eliminated, which in the above example is $J_{8,2}(8) = 1$.

Although the passage is somewhat vague, Josephus claims his life was saved by an application of the problem which now bears his name [9,15]. Apparently, Josephus and his comrades were holed up during a Jewish revolt against Rome, just after Rome had captured Jotapat. The consensus among these men was to commit mass suicide rather than surrender and risk becoming slaves to the Roman empire or worse. Accordingly, they determined their deaths "by lot" and a sequence of elimination somewhat resembling that described in the opening paragraph was employed. Josephus managed through chance, fate, or providence to be among the last two left alive as the others were killed when their number was up (literally). Having surrendered to the Romans, Josephus lived to report the events that took place.

Several algorithms have been devised [1,2,7,11,18] to determine where one should stand to be the last selected in a circle of size n and counting parameter d. In terms of the notation of this article, these algorithms compute the last selected $J_{n,d}(n)$ or more generally the tth selected $J_{n,d}(t)$ for an integer t with $1 \leqslant t \leqslant n$. Other investigations have studied: when an arbitrary permutation in S_n is a Josephus permutation [4], the cycle structure of $J_{n,d}$ [10], an asymptotic approximation for the survivor [13], and when the Josephus permutations form a subgroup of S_n [18].

A related problem assumes that you find yourself in a position along the Josephus circle and asks if a counting parameter can be found making you the last selected. That is, given n and k, does there always exist d such that $J_{n,d}(n) = k$? The answer is affirmative and the existence proof is found in [7] or [15]. This and Proposition 1.1 below prove that there are in fact infinitely many such d: given one, any other positive integer residing in the same congruence class modulo $\operatorname{lcm}(n, n-1, \ldots, 1)$ will be another. Proposition 1.1, whose proof is left to the reader, is a straightforward extension of an exercise found in [10].

Proposition 1.1. *$J_{n,d_1}(i) = J_{n,d_2}(i)$ for $1 \leqslant i \leqslant t$ if and only if $d_1 \equiv d_2 \bmod L_{n,t}$, where*

$$L_{n,t} = \operatorname{lcm}(n, n-1, \ldots, n-t+1).$$

The problem addressed in this article is to find the number of parameters d that make a given integer k the last eliminated when d is restricted to integers between 1 and $\operatorname{lcm}(n, n-1, \ldots, 1)$. More generally, given an integer t with $1 \leqslant t \leqslant n$, we are interested in determining the number of parameters d (appropriately restricted) such that $J_{n,d}(t) = k$. Due to Proposition 1.1, an appropriate restriction is $1 \leqslant d \leqslant L_{n,t}$ and the set to be enumerated is:

$$D(n,t,k) = \left\{ d\colon\ 1 \leqslant d \leqslant L_{n,t},\ \ J_{n,d}(t) = k \right\}. \tag{1.1}$$

For convenience and brevity, we sometimes denote $D(n,t,k)$ by D.

The conciseness of the theorems given in this article is facilitated by introducing a notion of *local* primeness:

Definition 1.2. An element in a set of consecutive positive integers is locally prime if it is relatively prime to every other integer in the set.

Another useful concept is that of *local prime abundance*:

Definition 1.3. A set of consecutive positive integers $\{n, n-1, \ldots, n-t+1\}$ $(1 \leqslant t \leqslant n)$, is local prime abundant if $\{n, n-1, \ldots, n-s+1\}$ contains a local prime for $s = 1, 2, \ldots, t$.

We will see in Theorem 3.3 that $|D| = L_{n,t}/n$ provided that $\{n, n-1, \ldots, n-t+1\}$ is local prime abundant. As a corollary (Corollary 3.4), we will prove that if $\{n, n-1, \ldots, 1\}$ is local prime abundant, then the number of Josephus permutations mapping t to k is $L_{n,n}/n$, for any t and k.

Based on the work of S.S. Pillai [14], it will be seen that $\{n, n-1, \ldots, n-t+1\}$ is local prime abundant for any n whenever $1 \leqslant t \leqslant 16$. We will also see that $\{n, n-1, \ldots, n-t+1\}$ is local prime abundant for any $t \leqslant n$ whenever at least one of $n, n-1, \ldots, n-16$ is prime.

The enumeration of D is much more complex whenever $\{n, n-1, \ldots, n-t+1\}$ is not local prime abundant, that is, whenever $\{n, n-1, \ldots, n-s+1\}$ is free of local primes for some $s \leqslant t$. As described in Section 5, the enumeration in its full generality (absent of any conditions) requires the evaluation of a DFT over a finite Abelian group. We examine the first case (smallest n) for which local prime abundance fails, namely $n = 2200$ with $t = s = 17$. For this case, the enumeration of D varies with k, as verified by a computer program that evaluates the DFT. By necessity, the algorithm cannot be a simple exhaustive search, since there are $\operatorname{lcm}(2200, 2199, \ldots, 2184) \approx 5.95 \times 10^{43}$ cases to check. In Section 6, we outline a technique that drastically reduces this complexity.

2. Derivation of an enumeration expression

The following recursion dates back at least as far as 1898 in a paper of P.G. Tait [16]. Proofs are given in [15] and [18].

Proposition 2.1. *For any positive integers n, d, and t with* $t \leqslant n$:

$$J_{n,d}(t) \equiv \big(J_{n-1,d}(t-1) + d\big) \bmod n. \tag{2.1}$$

An algorithm for the computation of $J_{n,d}(t)$ is specified by successive applications of (2.1). The order of computation is $J_{n-t+1,d}(1)$, $J_{n-t+2,d}(2)$, $\ldots$, $J_{n,d}(t)$ where $J_{n-t+1,d}(1)$ is obtained by taking $J_{n-t,d}(0) = 0$. This also determines a finite integer sequence $x_1, x_2, \ldots, x_{t-1}$ (the above sequence in reverse order with $J_{n,d}(t)$ excluded), that leads to an alternate characterization of D. We will see that the alternate characterization lends itself to the construction of a multivariate generating function.

Lemma 2.2. *For each element* $d \in D$, *there exist unique integers* $x_1, x_2, \ldots, x_{t-1}$ *with* $1 \leqslant x_i \leqslant n-i$ *such that the following linear system of congruences is satisfied*:

$$d + x_1 \equiv k \bmod n, \tag{2.2}$$

$$d + x_i - x_{i-1} \equiv 0 \bmod (n-i+1) \quad i = 2, 3, \ldots, t, \tag{2.3}$$

where $x_t = 0$. *Conversely, an integer d with* $1 \leqslant d \leqslant L_{n,t}$ *satisfying* (2.2) *and* (2.3) *for integers* $x_1, x_2, \ldots, x_{t-1}$ *with* $1 \leqslant x_i \leqslant n-i$ *is necessarily a member of D.*

Proof. Given $d \in D$, the existence of $x_1, x_2, \ldots, x_{t-1}$ is established by taking $x_i = J_{n-i,d}(t-i)$ as described in the paragraph following recursion (2.1). Making use of the observation that $x_i \equiv \tilde{x}_i \bmod (n-i+1)$ and $1 \leqslant x_i, \tilde{x}_i \leqslant n-i$ necessarily imply $x_i = \tilde{x}_i$, the uniqueness of the x_i follows from a simple induction argument.

Let d be any integer between 1 and $L_{n,t}$. Assuming the existence of $x_1, x_2, \ldots, x_{t-1}$ $(1 \leqslant x_i \leqslant n-i)$ satisfying (2.2) and (2.3), we now prove that $J_{n,d}(t) = k$. Since both $J_{n-t+1,d}(1)$ and x_{t-1} are congruent to d modulo $n-t+1$, they must be congruent to each other. Since both lie in the interval

$[1, n-t+1]$, they must in fact be equal. Applying the same argument, $J_{n-t+2,d}(2)$ and x_{t-2} are both congruent to $(x_{t-1}+d)$ modulo $n-t+2$, implying that they are equal as well. Ignoring the details of a formal induction, this process leads to $J_{n-1,d}(t-1) = x_1$. From (2.2) it follows that $d + J_{n-1,d}(t-1) \equiv k \bmod n$, which by the recurrence (2.1) implies $J_{n,d}(t) = k$. □

The system of congruences (2.2) and (2.3) is used to establish a multivariate generating function in which a sum of coefficients yields the desired enumeration. The relevant theorem making the connection between the enumeration and the generating function is given by Proposition 2.3 below. This proposition generalizes the enumeration technique used in [19] and is essentially an application of Fourier analysis on finite groups. The underlying group is detailed in Section 5.

Proposition 2.3. *Let $f(z_1, z_2, \ldots, z_t)$ be a polynomial in $z_1, z_2, \ldots, z_t$ with integer coefficients. Let $m_1, m_2, \ldots, m_t$ be positive integers and $r_1, r_2, \ldots, r_t$ be nonnegative integers. Then, the sum of coefficients of terms $\prod_{i=1}^{t} z_i^{r_i+q_i m_i}$ in f over all integers $q_1, q_2, \ldots, q_t$ is given by the following Fourier transform*:

$$\frac{1}{\prod_1^t m_i} \sum_{\rho_1} \sum_{\rho_2} \cdots \sum_{\rho_t} \left(\prod_{i=1}^{t} \rho_i^{-r_i} \right) f(\rho_1, \rho_2, \ldots, \rho_t), \tag{2.4}$$

where in the ith sum, ρ_i runs over the m_ith roots of unity.

Proof. For clarity of exposition, the case of $t = 2$ is proved below. The general case is a straightforward extension of this. To help with the notation, define:

$$\delta(k, m) = \begin{cases} 1 & \text{if } k \equiv 0 \bmod m, \\ 0 & \text{otherwise.} \end{cases} \tag{2.5}$$

The proof makes use of the well-known result:

$$\frac{1}{m} \sum_{\rho} \rho^k = \delta(k, m),$$

where ρ runs over the mth roots of unity. By assumption, f may be expressed as a finite sum of the form $f(z_1, z_2) = \sum_{i,j} a_{ij} z_1^i z_2^j$, where the a_{ij} are integers. The expression (2.4) becomes:

$$\begin{aligned} \frac{1}{m_1 m_2} \sum_{\rho_1} \sum_{\rho_2} \rho_1^{-r_1} \rho_2^{-r_2} f(\rho_1, \rho_2) &= \frac{1}{m_1 m_2} \sum_{\rho_1} \sum_{\rho_2} \rho_1^{-r_1} \rho_2^{-r_2} \sum_{i,j} a_{ij} \rho_1^i \rho_2^j \\ &= \sum_{i,j} a_{ij} \left[\frac{1}{m_1} \sum_{\rho_1} \rho_1^{i-r_1} \right] \left[\frac{1}{m_2} \sum_{\rho_2} \rho_2^{j-r_2} \right] \\ &= \sum_{i,j} a_{ij} \delta(i - r_1, m_1) \delta(j - r_2, m_2). \end{aligned}$$

It is readily seen that this last expression is the sum of coefficients of terms $z_1^{r_1+q_1 m_1} z_2^{r_2+q_2 m_2}$ in f over all integers q_1 and q_2. □

Theorem 2.4. *For positive integers n, t, and k ($t \leqslant n$, $k \leqslant n$),*

$$\left| D(n, t, k) \right| = \frac{1}{\prod_{i=1}^{t} (n - i + 1)} \sum_{\rho_1} \sum_{\rho_2} \cdots \sum_{\rho_t} \rho_1^{-k} f(\vec{\rho}), \tag{2.6}$$

where ρ_j runs over the $(n-j+1)$th roots of unity, $\vec{\rho} = (\rho_1, \rho_2, \ldots, \rho_t)$, and f is the multivariate generating function given by:

$$f(\vec{z}) = \left[\sum_{x_1=1}^{n-1} z_1^{x_1} z_2^{(n-2)x_1}\right]\left[\sum_{x_2=1}^{n-2} z_2^{x_2} z_3^{(n-3)x_2}\right]\cdots\left[\sum_{x_{t-1}=1}^{n-t+1} z_{t-1}^{x_{t-1}} z_t^{(n-t)x_{t-1}}\right]\left[\sum_{d=1}^{L_{n,t}} \prod_{j=1}^{t} z_j^d\right]. \quad (2.7)$$

Proof. Introducing integer quotients $q_1, q_2, \ldots, q_t$ into (2.2) and (2.3) and making all coefficients non-negative yield the following system of linear equations:

$$d + x_1 = k + q_1 n, \quad (2.8)$$

$$d + x_i + (n-i)x_{i-1} = q_i(n-i+1) \quad i = 2, 3, \ldots, t, \quad (2.9)$$

where $x_t = 0$. By Lemma 2.2, $|D|$ is the number of integers d $(1 \leqslant d \leqslant L_{n,t})$ that satisfy (2.8) and (2.9) for some set of integers $x_1, x_2, \ldots, x_{t-1}$ with $1 \leqslant x_i \leqslant n-i$ and some set of quotients $q_1, q_2, \ldots, q_t$, where the x_i and q_i are uniquely determined for each $d \in D$.

An associated generating polynomial is:

$$f(\vec{z}) = \sum z_1^{d+x_1} z_2^{d+x_2+(n-2)x_1} \cdots z_{t-1}^{d+x_{t-1}+(n-t+1)x_{t-2}} z_t^{d+(n-t)x_{t-1}} \quad (2.10)$$

where the sum runs over integers $d, x_1, \ldots, x_{t-1}$ with $1 \leqslant d \leqslant L_{n,t}$ and $1 \leqslant x_i \leqslant n-i$. We see the terms of the left-hand sides of (2.8) and (2.9) appear as exponents in Eq. (2.10). For a given set of quotients, the coefficient of $z_1^{k+q_1 n} \prod_{i=2}^{t} z_i^{q_i(n-i+1)}$ of f is the number of solutions d of the system of Eqs. (2.8) and (2.9). Therefore, the number of solutions over all possible quotients is the sum of such coefficients over all possible quotients. By Proposition 2.3, (2.6) holds. Eq. (2.7) is obtained by factoring (2.10). □

The generating function evaluated at $\vec{\rho}$ may be written as $f(\vec{\rho}) = L_{n,t} \prod_{j=1}^{t} h_j$ where

$$h_j = \sum_{x_j=1}^{n-j} \left(\frac{\rho_j}{\rho_{j+1}}\right)^{x_j} \quad (1 \leqslant j \leqslant t-1), \qquad h_t = \frac{1}{L_{n,t}} \sum_{d=1}^{L_{n,t}} \left(\prod_{j=1}^{t} \rho_j\right)^d.$$

Applying the identity

$$x + x^2 + \cdots + x^N = \begin{cases} N & x = 1, \\ \frac{x(1-x^N)}{1-x} & x \neq 1, \end{cases}$$

we have

$$h_j = \begin{cases} n-j, & \rho_j = \rho_{j+1} \\ \frac{\rho_j - 1}{\rho_{j+1} - \rho_j}, & \rho_j \neq \rho_{j+1} \end{cases} \quad (1 \leqslant j \leqslant t-1), \quad (2.11)$$

and

$$h_t = \begin{cases} 1, & \prod_{j=1}^{t} \rho_j = 1, \\ 0, & \prod_{j=1}^{t} \rho_j \neq 1. \end{cases} \quad (2.12)$$

3. Simplification under local prime abundance

Under the assumption of local prime abundance, we derive a simple expression for the enumeration of D. By contrast, Section 5 details a more complicated enumeration for a case where local prime abundance does not hold.

Lemma 3.1. *Given s consecutive positive integers $\gamma_{n,s} = \{n, n-1, \ldots, n-s+1\}$, if the sum $\sum_{j=1}^{s} \frac{y_j}{n-j+1}$ is an integer for some choice of integers $y_1, y_2, \ldots, y_s$ satisfying $1 \leqslant y_j \leqslant n-j$, then $\gamma_{n,s}$ does not contain a local prime.*

Proof. For $j = 1, 2, \ldots, s$, let $a_j = L_{n,s}/(n-j+1)$ so that the given sum is an integer if and only if:

$$\sum_{j=1}^{s} a_j y_j \equiv 0 \bmod L_{n,s}. \tag{3.1}$$

Suppose now that $p = n-k+1$ is a local prime of $\gamma_{n,s}$ and consider the above congruence modulo p. Since $p \mid a_j(n-j+1)$, it follows that $p \mid a_j$ whenever $j \neq k$. Therefore, the congruence (3.1) implies that $p \mid a_k y_k$. However, since p is locally prime in $\gamma_{n,s}$, we must have $(p, a_k) = 1$ so that $p \mid y_k$. This and the assumption $1 \leqslant y_k \leqslant n-k$ provide the desired contradiction. □

Although it is not needed to prove Theorem 3.3 below, the converse of Lemma 3.1 is true and is of theoretical interest on its own merit. In addition, it eliminates the possibility of constructing a stronger version of Theorem 3.3 that could be stated in terms of integers $y_1, y_2, \ldots, y_s$. We prove the converse of Lemma 3.1 in Proposition 3.2.

Proposition 3.2. *Let $\gamma_{n,s} = \{n, n-1, \ldots, n-s+1\}$ where n and s are integers with $1 \leqslant s \leqslant n$. If $\gamma_{n,s}$ does not contain a local prime then there exist integers $y_1, y_2, \ldots, y_s$ with $1 \leqslant y_j \leqslant n-j$ such that $\sum_{j=1}^{s} \frac{y_j}{n-j+1}$ is an integer.*

Proof. Assume $\gamma_{n,s}$ does not contain a local prime and let $P = \{p_1, p_2, \ldots, p_r\}$ denote the complete set of primes dividing two or more elements of $\gamma_{n,s}$. It is straightforward to prove $s \geqslant 6$ (in fact by Theorem 4.2 below, $s \geqslant 17$). Therefore, we may take $p_1 = 2$ and $p_2 = 3$. Let $D = \operatorname{diag}(p_1^{-1}, p_2^{-1}, \ldots, p_r^{-1})$ and denote $n-j+1$ by m_j. We construct an $r \times s$ nonnegative integer matrix C satisfying 4 conditions:

(1) each column is nonzero,
(2) no $c_{i,j}$ exceeds $p_i - 1$,
(3) $c_{i,j} = 0$ if $(p_i, m_j) = 1$, and
(4) the row sums of DC are integers.

The integer matrix C is constructed as follows. If $(p_i, m_j) = 1$, let $c_{i,j} = 0$. Otherwise, consider the set $N_i = \{m_j \in \gamma_{n,s} \colon p_i \mid m_j\}$. The integers c_{ij} for which $m_j \in N_i$ are determined row by row as follows. For $i \geqslant 2$ ($p_i \geqslant 3$), choose positive integers $c_{i,j}$ such that $c_{i,j} < p_i$ and $\sum_j c_{i,j}/p_i$ is an integer, where the sum is taken over indices j with $m_j \in N_i$. Since $|N_i| \geqslant 2$, we may accomplish this by grouping terms in twos and threes. For $i = 1$ ($p_i = 2$) and $|N_1|$ even, $c_{1,j}$ is chosen in the same manner. For the case of $|N_1|$ odd (hence $\geqslant 3$), choose j_0 such that $m_{j_0} \in N_1 \cap N_2$. Then, for $m_j \in N_1$ with $j \neq j_0$, choose $c_{1,j}$ as before and let $c_{1,j_0} = 0$. This construction insures that the columns of C are nonzero.

Since the columns of C are nonzero, the set $I_j = \{i \colon c_{i,j} \neq 0\}$ is not empty. Choose a prime $p_k \in P$ with $k \in I_j$ and let Δ_j be the product of all primes p_i with $i \in I_j$. For each j, choose quotient and remainder q_j and r_j such that $\sum_{i \in I_j} c_{i,j}\Delta_j/p_i = q_j\Delta_j + r_j$, where $0 \leqslant r_j < \Delta_j$. If $r_j = 0$, then p_k divides the right side of the equation but not the left. Therefore, $0 < r_j < \Delta_j$. Taking $y_j = r_j m_j/\Delta_j$,

we see that y_j is an integer satisfying the restriction $1 \leqslant y_j \leqslant n-j$. The sum of interest is now readily computed:

$$\sum_{j=1}^{s} \frac{y_j}{m_j} = \sum_{j=1}^{s} \frac{r_j}{\Delta_j} = \sum_{j=1}^{s} \frac{1}{\Delta_j}\left(-q_j\Delta_j + \sum_{i=1}^{r} c_{ij}\frac{\Delta_j}{p_i}\right) = -\sum_{j=1}^{s} q_j + \sum_{i=1}^{r}\sum_{j=1}^{s} \frac{c_{ij}}{p_i},$$

which is an integer as required. □

Theorem 3.3. *If $\{n, n-1, \ldots, n-t+1\}$ is local prime abundant then $|D| = \frac{L_{n,t}}{n}$.*

Proof. We will show that the term of (2.6) corresponding to $\rho_1 = \rho_2 = \cdots = \rho_t = 1$ gives the desired enumeration while every other term is zero. From (2.11) and (2.12), we see that the term in (2.6) corresponding to $\rho_1 = \rho_2 = \cdots = \rho_t = 1$ is given by:

$$L_{n,t}\frac{\prod_{j=1}^{t-1}(n-j)}{\prod_{i=1}^{t}(n-i+1)} = \frac{L_{n,t}}{n}.$$

The proof will be complete once it is shown that the other terms of (2.6) are 0. Equivalently, we will show that $f(\vec{\rho}) = 0$ whenever at least one ρ_j is different than 1. If there exists j $(1 \leqslant j \leqslant t-1)$ such that $\rho_j = 1$ and $\rho_{j+1} \neq 1$, then by (2.11) $h_j = 0$. Therefore, we may assume that no such j exists and choose s $(1 \leqslant s \leqslant t)$ such that $\rho_j \neq 1$ for $1 \leqslant j \leqslant s$ and $\rho_j = 1$ for $s < j \leqslant t$. Under this assumption, it remains to show that $\prod_{j=1}^{t} \rho_j \neq 1$, since from Eq. (2.12) this implies $h_t = 0$.

For $1 \leqslant j \leqslant t$, consider the primitive $(n-j+1)$th root of unity given by:

$$\xi_j = \exp\bigl[i2\pi/(n-j+1)\bigr]. \tag{3.2}$$

For each j, let $\rho_j = \xi_j^{y_j}$, where y_j is an integer between 0 and $n-j$. By the discussion above, it may be assumed that $y_j \neq 0$ for $1 \leqslant j \leqslant s$ and that $y_j = 0$ for $s < j \leqslant t$. Hence,

$$\prod_{j=1}^{t} \rho_j = \prod_{j=1}^{t} \xi_j^{y_j} = \prod_{j=1}^{s} \xi_j^{y_j} = \exp\left[i2\pi \sum_{j=1}^{s} \frac{y_j}{(n-j+1)}\right].$$

By the hypothesis, $\{n, n-1, \ldots, n-s+1\}$ contains a local prime which by Lemma 3.1 implies that $\sum_{j=1}^{s} \frac{y_j}{(n-j+1)}$ is not an integer. Therefore, $\prod_{j=1}^{t} \rho_j \neq 1$. □

Corollary 3.4. *If $\{n, n-1, \ldots, 1\}$ is local prime abundant, then for any integers t and k, with $1 \leqslant t, k \leqslant n$, the number of Josephus permutations mapping t to k is $L_{n,n}/n$.*

Proof. By Proposition 1.1, the Josephus permutations are in one-to-one correspondence with the integers $1 \leqslant d \leqslant L_{n,n}$. Therefore, it's enough to show that the number of d between 1 and $L_{n,n}$ such that $J_{n,d}(t) = k$ is $L_{n,n}/n$. By Theorem 3.3, the number of such d between 1 and $L_{n,t}$ is $L_{n,t}/n$. Denote them by $d_1, d_2, \ldots, d_\ell$, where $\ell = L_{n,t}/n$. For an integer i with $1 \leqslant i \leqslant L_{n,n}/L_{n,t}$, we may express the totality of integers d such that $(i-1)L_{n,t} + 1 \leqslant d \leqslant iL_{n,t}$, and $J_{n,d}(t) = k$ in terms of $d_1, d_2, \ldots, d_\ell$. Again by Proposition 1.1, these are easily seen to be $d_1 + (i-1)L_{n,t}, d_2 + (i-1)L_{n,t}, \ldots, d_\ell + (i-1)L_{n,t}$. Thus, for each i, there are ℓ values of d in the interval $(i-1)L_{n,t} + 1 \leqslant d \leqslant iL_{n,t}$ such that $J_{n,d}(t) = k$, implying a total of $\ell(L_{n,n}/L_{n,t}) = L_{n,n}/n$ values of d in the interval $1 \leqslant d \leqslant L_{n,n}$ such that $J_{n,d}(t) = k$. □

By taking n to be a prime, we see immediately from Theorem 3.3 that there are infinitely many n for which the enumeration $|D(n,t,k)| = \frac{L_{n,t}}{n}$ holds for all t and k. The next section extends this, providing a variety of conditions that yield the same simple enumeration.

4. Local primes in sets of consecutive integers

Throughout this section we denote the set $\{n, n-1, \ldots, n-s+1\}$ by $\gamma_{n,s}$.

Proposition 4.1. *If $\gamma_{n,s}$ contains a prime then it contains a local prime.*

Proof. We let p be the largest prime in $\gamma_{n,s}$ and show that p is locally prime in $\gamma_{n,s}$. Since integers less than p are relatively prime to p, we may restrict our attention to integers in $\gamma_{n,s}$ larger than p. Suppose that $p \mid p+i$ for some $i \in \{1, 2, \ldots, n-p\}$. Then, $p+i = qp$ for $q \geqslant 2$ so that $n \geqslant p+i = qp \geqslant 2p$ implying that $n \geqslant 2p$. However, by Bertrand's Postulate, there is a prime p_0 such that $p < p_0 < 2p$. Therefore, $n \geqslant 2p > p_0 > p$ which contradicts the choice of p. □

There are sets of consecutive positive integers that contain no local prime. By Proposition 4.1, the search for such sets may be restricted to sets of consecutive integers that do not contain a prime number. A computer program was written to search for integers n and s such that $\gamma_{n,s}$ does not contain a local prime. The two smallest values of n are $n = 2200$ (with $s = 17$) and $n = 27,846$ (with $s \in \{17, 18, 19\}$).

For these values of n, Proposition 3.2 proves that there exist integers $y_1, y_2, \ldots, y_s$ with $1 \leqslant y_j \leqslant n-j$ such that the sum $\sum_{j=1}^{s} \frac{y_j}{n-j+1}$ is an integer. For the smallest value $n = 2200$, a computer program was written to find all such solution sets $\{y_1, y_2, \ldots, y_{17}\}$. There were 274,341,150,720 solutions found. An example solution giving the minimal integer sum of 4 is $\{5, 1466, 157, 169, 122, 439, 1097, 1462, 548, 313, 73, 597, 547, 243, 1093, 437, 1\}$.

As reported in [8], the example $n = 2200$, $s = 17$ is famous. It was first discovered by S.S. Pillai while working on his M.S. thesis, attempting to show that no such integers could exist. In 1939, he published his counterexample and included a proof of the 'only if' part of Theorem 4.2 below. However, he was unable to prove the 'if' part and had to leave it as a conjecture at that time. Although A.T. Brauer published the first proof of the 'if' part in 1940, Pillai eventually produced his own proofs in 1941 and 1944. Finally, in 1969 R.J. Evans found the simplest proof of the lot and in 1972 generalized the result to consecutive integers in arithmetic progression [3,5,6,14].

Theorem 4.2. *There exists a set of s consecutive positive integers with no local prime if and only if $s \geqslant 17$.*

Corollary 4.3. *For integers n, t, and k with $1 \leqslant t, k \leqslant n$, $|D| = L_{n,t}/n$ whenever $t \leqslant 16$.*

Proof. The proof follows immediately from Theorems 3.3 and 4.2. □

Corollary 4.4. *For positive integers n, t, and k with $1 \leqslant t, k \leqslant n$, $|D| = L_{n,t}/n$ whenever at least one of $n, n-1, \ldots, n-16$ is prime.*

Proof. By Theorem 3.3, it is sufficient to show that $\gamma_{n,s}$ contains a local prime for each s $(1 \leqslant s \leqslant n)$. If $1 \leqslant s \leqslant 16$, $\gamma_{n,s}$ contains a local prime by Theorem 4.2. If $17 \leqslant s \leqslant n$, $\gamma_{n,s}$ contains a prime by hypothesis, hence a local prime by Proposition 4.1. □

5. The enumeration as a discrete Fourier transform

From Eq. (2.6), we have for general n, t, and k:

$$\left|D(n,t,k)\right| = \frac{L_{n,t}}{\prod_{i=1}^{t}(n-i+1)} \sum_{\mathbf{y}} \xi_1^{-ky_1} \prod_{j=1}^{t} h_j(\mathbf{y}), \tag{5.1}$$

where the sum runs over all integer vectors $\mathbf{y} = (y_1, y_2, \ldots, y_t)$ with $0 \leqslant y_i \leqslant n-i$, and $h_j(\mathbf{y})$ is given by (2.11) and (2.12). As before, $\rho_j = \xi_j^{y_j}$, where ξ_j is the primitive $(n-j+1)$th root of unity given

by Eq. (3.2). In this section, we recast this enumeration in terms of a finite Fourier transform over a particular finite Abelian group.

Consider the subgroup $\mathbf{L} = (\ell_1) \times (\ell_2) \times \cdots \times (\ell_t)$ of Z^t, where the ℓ_i are given by:

$$\ell_i = \operatorname{lcm}\big\{(n-i+1, n-j+1)\colon\ 1 \leqslant j \leqslant t,\ j \neq i\big\} \quad (1 \leqslant i \leqslant t). \tag{5.2}$$

We define $G_{n,t}$ as the additive subgroup of $Z^t|\mathbf{L}$ consisting of vector cosets $\mathbf{g} = \mathbf{w} + \mathbf{L}$ where $\mathbf{w} = (w_1, w_2, \ldots, w_t) \in Z^t$ satisfies:

$$w_1/\ell_1 + w_2/\ell_2 + \cdots + w_t/\ell_t \equiv 0 \bmod 1.$$

Therefore, an element $\mathbf{g}$ of $G_{n,t}$ is a coset

$$\mathbf{w} + \mathbf{L} = \Big\{(w_1 + \alpha_1\ell_1, \ldots, w_t + \alpha_t\ell_t)\colon\ \alpha_i \in Z,\ \sum w_i/\ell_i \in Z\Big\}.$$

We evaluate the enumeration given by (5.1) through the selection of a set of coset representatives $\{w_1, w_2, \ldots, w_t\}$ of each element $\mathbf{g}$ of $G_{n,t}$. Taking $y_j = w_j(n-j+1)/\ell_j$, and evaluating $h_j(\mathbf{y})$ using (2.11) and (2.12), we see that the enumeration (5.1) is independent of the particular ensemble of coset representatives chosen. This leads us to consider the enumeration as a sum over the elements of $G_{n,t}$:

$$\big|D(n,t,k)\big| = \frac{L_{n,t}}{\prod_{i=1}^{t}(n-i+1)} \sum_{\mathbf{g}\in G_{n,t}} f(\mathbf{g})\bar{\chi}_k(\mathbf{g}),$$

where[3] $f(\mathbf{g}) = \prod_{j=1}^{t} h_j(\mathbf{y})$ and $\chi_k(\mathbf{g}) = \xi_1^{ky_1}$. This formulation gives $|D(n,t,k)|$ as a discrete Fourier transform of $f \in L^2(G_{n,t})$ on the group $G_{n,t}$ (see [17]). The following proposition allows us to express the enumeration in the classical form:

$$\big|D(n,t,k)\big| = \frac{1}{|G_{n,t}|} \sum_{\mathbf{g}\in G_{n,t}} f(\mathbf{g})\bar{\chi}_k(\mathbf{g}). \tag{5.3}$$

Proposition 5.1. *For general n and t*:

$$\big|G_{n,t}\big| = \frac{1}{L_{n,t}} \prod_{i=1}^{t}(n-i+1).$$

Proof. Consider the mapping $\mu : \prod_{i=1}^{t} Z|(n-i+1) \to Z|(L_{n,t})$ defined by:

$$\mu\big([y_1]_n, [y_2]_{n-1}, \ldots, [y_t]_{n-t+1}\big) = \left[\sum_{i=1}^{t} a_i y_i\right]_{L_{n,t}},$$

where $a_i = L_{n,t}/(n-i+1)$. It's easy to establish that μ is a group homomorphism. To show that μ is a surjection, it's enough to show that $[1]_{L_{n,t}}$ is the image of an element in $\prod_{i=1}^{t} Z|(n-i+1)$. However, this easily follows from the fact that the greatest common divisor among the a_i is 1, and consequently 1 is expressible as a linear combination of the a_i with integer coefficients. Therefore,

[3] We have changed f from the definition given in the proof of Theorem 3.3 by the scale factor $L_{n,t}$.

μ is a group homomorphism from $\prod_{i=1}^{t} Z|(n-i+1)$ onto $Z|(L_{n,t})$. By the first isomorphism theorem for groups:

$$\prod_{i=1}^{t} Z|(n-i+1) \,\big|\, \ker(\mu) \cong Z|(L_{n,t}),$$

proving that $\prod_{i=1}^{t}(n-i+1)/|\ker(\mu)| = L_{n,t}$. However, $\ker(\mu)$ is isomorphic to $G_{n,t}$ through the isomorphism determined by $y_i = w_i(n-i+1)/\ell_i$. Therefore,

$$\big|G_{n,t}\big| = \big|\ker(\mu)\big| = \prod_{i=1}^{t}(n-i+1)/L_{n,t}. \qquad \square$$

We have established several other results concerning the group $G_{n,t}$, and in particular $G_{2200,17}$. These include the construction of a set of generators of $G_{n,t}$, and a corresponding minimal set of generators of $G_{2200,17}$ obtained by applying the Hermite normal form algorithm. Following [12], we have used the Smith normal form to express $G_{2200,17}$ as a cross product of cyclic groups:

$$G_{2200,17} \cong Z|(2) \times Z|(2) \times Z|(2) \times Z|(6) \times Z|(12) \times Z|(60) \times Z|(840) \times Z|(360360).$$

As a check, it is readily verified that:

$$\begin{aligned}\big|G_{2200,17}\big| &= 2^3 \cdot 6 \cdot 12 \cdot 60 \cdot 840 \cdot 360360 = 10,461,394,944,000\\ &= \prod_{i=1}^{17}(2200-i+1)/\operatorname{lcm}(2200,2199,\ldots,2184).\end{aligned}$$

The Smith normal form determines a unimodular matrix that sets up the above isomorphism. Through the isomorphism, the elements of $G_{2200,17}$ may be computed in an efficient manner. We hope to exploit this in future work by improving on our current enumeration algorithm, which is roughly sketched in the next section.

6. Computational considerations

We now consider the computation of $|D(n,t,k)|$ when $\{n, n-1, \ldots, n-t+1\}$ is not local prime abundant. As we have seen, the first such case occurs when $n = 2200$ and $t = 17$. For this case, a straight forward implementation of (5.1) has a computational complexity much too large for modern day computers. Therefore, in this section, we briefly sketch techniques to reduce computational complexity. This has resulted in a fast running computer program that we have used to confirm that $|D(n,t,k)|$ may in fact depend on k nontrivially.

For an initial simplification, we consider 4 exhaustive and mutually exclusive cases:

Case 1: for some $s < t$, $y_s = 0$ and $y_{s+1} > 0$,
Case 2: for some $s < t$, $y_j > 0$ $(1 \leqslant j \leqslant s)$ and $y_j = 0$ $(s+1 \leqslant j \leqslant t)$,
Case 3: $y_j = 0$ for $1 \leqslant j \leqslant t$,
Case 4: $y_j > 0$ for $1 \leqslant j \leqslant t$.

We may eliminate Case 1 because $h_s(\mathbf{y}) = 0$ so that $\mathbf{y}$ does not contribute to the sum. Similarly, for $t = 17$, we may eliminate Case 2 because $h_t(\mathbf{y}) = 0$. It follows that we can break up (5.1) into two respective parts corresponding to Cases 3 and 4:

$$\left|D(n,t,k)\right| = \frac{L_{n,t}}{n} + \frac{L_{n,t}}{\prod_{i=1}^{t}(n-i+1)} \sum_{\mathbf{y}\in Y(n,t)} \xi_1^{-ky_1} \prod_{j=1}^{t-1} h_j(\mathbf{y}),$$

where

$$Y(n,t) = \left\{ \mathbf{y}\colon \sum_{i=1}^{t} \frac{y_i}{n-i+1} \in Z,\ 1 \leqslant y_i \leqslant n-i \right\}.$$

Therefore, the enumeration of $D(n,t,k)$ when $t = 17$ reduces to computing the sum:

$$S(n,t,k) = \sum_{\mathbf{y}\in Y(n,t)} \xi_1^{-ky_1} \prod_{j=1}^{t-1} h_j(\mathbf{y}) = \sum_{\mathbf{y}\in Y(n,t)} \xi_1^{-ky_1} \prod_{j=1}^{t-1} \frac{\xi_j^{y_j} - 1}{\xi_{j+1}^{y_{j+1}} - \xi_j^{y_j}}.$$

To help reduce computational complexity, we define:

$$W(n,t) = \left\{ \mathbf{w}\colon \sum_{i=1}^{t} \frac{w_i}{\ell_i} \in Z,\ 1 \leqslant w_i \leqslant \ell_i - 1 \right\},$$

where

$$\ell_i = \operatorname{lcm}\left\{ (n-i+1, n-j+1)\colon 1 \leqslant j \leqslant t,\ j \neq i \right\} \quad (1 \leqslant i \leqslant t).$$

For general n and t, the elements of $Y(n,t)$ and $W(n,t)$ are in one-to-one correspondence and are related through the equation:

$$\frac{y_i}{n-i+1} = \frac{w_i}{\ell_i}.$$

Thus, for $y_i = w_i(n-i+1)/\ell_i$, we may express S as:

$$S(n,t,k) = \sum_{\mathbf{w}\in W(n,t)} \xi_1^{-ky_1} \prod_{j=1}^{t-1} \frac{\xi_j^{y_j} - 1}{\xi_{j+1}^{y_{j+1}} - \xi_j^{y_j}}. \tag{6.1}$$

The elements of $Y(n,t)$ and $W(n,t)$ may be written as:

$$Y(n,t) = \left\{ \mathbf{y}\colon \sum_{i=1}^{t} a_i y_i \equiv 0 \bmod L_{n,t},\ 1 \leqslant y_i \leqslant n-i \right\},$$

$$W(n,t) = \left\{ \mathbf{w}\colon \sum_{i=1}^{t} b_i w_i \equiv 0 \bmod \ell,\ 1 \leqslant w_i \leqslant \ell_i - 1 \right\},$$

where $a_i = L_{n,t}/(n-i+1)$, $b_i = \ell/\ell_i$, and $\ell = \operatorname{lcm}(\ell_1, \ell_2, \ldots, \ell_t)$. For $n = 2200$ and $t = 17$, $L_{n,t} \approx 6 \times 10^{43}$ and the a_i are on the order of 10^{40}. On the other hand, the b_i on the order of 10^5 or smaller. This reduction in the parameter size is one of the keys to producing a tractable computer algorithm.

Working with the smaller parameters facilitates a computationally feasible implementation. Many vectors $\mathbf{w}$ that do not belong to $W(n,t)$ need not be visited, since we can impose constraints implied

from the condition $\sum_{i=1}^{t} b_i w_i \equiv 0 \bmod \ell$. For example, computing the b_i explicitly for $n = 2200$ and $t = 17$, we discover that the odd b_i are b_1, b_9, and b_{17}. This implies the congruence $b_1 w_1 + b_9 w_9 + b_{17} w_{17} \equiv 0 \bmod 2$, which reduces to $w_1 + w_9 + w_{17} \equiv 0 \bmod 2$. Therefore, as we loop through entries of $\mathbf{w}$, we may skip those that do not satisfy $w_1 + w_9 + w_{17} \equiv 0 \bmod 2$. Other independent congruences are determined similarly and help to further reduce computational complexity.

Using these ideas, we have put together a computer program and have performed an actual computation for the case of $n = 2200$ and $t = 17$. Running the computer program verifies that the first case where local prime abundance fails to hold does in fact lead to a nontrivial enumeration that depends on k. We hope to fully document our algorithm in a follow-on publication.

7. Conclusion

After introducing the notion of a local prime, we enumerated an appropriately restricted counting parameter d of the Josephus permutation $J_{n,d}$, subject to $J_{n,d}(t) = k$ for arbitrary k and t. The enumeration, which depends on the hypothesis of local prime abundance, is given by a simple expression. It was seen that local prime abundance widely holds and that it implies an equally simple enumeration of Josephus permutations that map t to k.

Since local prime abundance holds for any $n < 2200$, the simple enumeration is valid for any Josephus circle of size $n < 2200$. Similarly, with the exception of $n = 2200$, the simple enumeration is valid for any $n < 27,846$. We saw that it is valid for infinitely many n since the condition trivially holds whenever n is prime. Based mainly on the work of S.S. Pillai, we saw that the simple enumeration holds when any one of $n, n-1, \ldots, n-16$ is prime, or for any n provided $t \leqslant 16$.

The parameters $n = 2200$ and $t = 17$, determine the first case where local prime abundance fails. This case yields an enumeration that is no longer simple, suggesting that local prime abundance is not only a sufficient condition for the simple enumeration, but probably necessary as well.

For the case of general n, t, and k, we saw how the enumeration can be cast as a discrete Fourier transform on a finite Abelian group $G_{n,t}$. For the case of $n = 2200$ and $t = 17$, we characterized $G_{n,t}$ in an explicit fashion, and described how to generate its elements in an efficient manner.

We are confident that our approach to enumerating the Josephus counting parameter is applicable to more general recursive problems. The combination of recurrence relations, multivariate generating functions, and Fourier transforms on finite groups, promises to provide a powerful technique for solving a wide class of enumeration problems.

Supplementary material

The online version of this article contains additional supplementary material. Please visit doi:10.1016/j.jnt.2009.11.004.

References

[1] W. Ahrens, Mathematische Unterhaltungen und Spiele, Teubner, Leipzig, 1901, Chapter 15, pp. 286–301.
[2] W.W.R. Ball, Mathematical Recreations and Essays, 11th ed., revised by H.S.M. Coxeter, Macmillan, New York, 1964, Section 21, pp. 124–126.
[3] A. Brauer, On a property of k consecutive integers, Bull. Amer. Math. Soc. 47 (1941) 328–331.
[4] J. Dowdy, M.E. Mays, Josephus Permutations, J. Combin. Math. Combin. Comput. 6 (1989) 125–130, http://www.math.wvu.edu/~mays/papers.htm.
[5] R.J. Evans, On blocks of N consecutive integers, Amer. Math. Monthly 76 (1969) 48–49.
[6] R.J. Evans, On N consecutive integers in arithmetic progression, Acta Sci. Math. (Szeged) 33 (1972) 295–296.
[7] R.L. Graham, D.E. Knuth, O. Patashnik, Concrete Mathematics: A Foundation for Computer Science, Addison–Wesley, 1989, pp. 8–20.
[8] R.K. Guy, Unsolved Problems in Number Theory, 2nd ed., Springer-Verlag, 1994, 83 pp.
[9] F. Josephus, The Great Roman-Jewish War: A.D. 66-70, Peter Smith, Gloucester, 1970, pp. 138–139.
[10] I. Kaplansky, I.N. Herstein, Matters Mathematical, Chelsea, New York, 1978, pp. 121–128.
[11] E.L. Lloyd, An $O(n \log m)$ algorithm for the Josephus problem, J. Algorithms 4 (1983) 262–270.
[12] M. Newman, Integral Matrices, Academic Press, New York, London, 1972.
[13] A.M. Odlyzko, H.S. Wilf, Functional iteration and the Josephus problem, Glasg. Math. J. 33 (1991) 235–240, www.dtc.umn.edu/~odlyzko/doc/arch/.

[14] S.S. Pillai, On m consecutive integers I, Proc. Indian Acad. Sci. Sect. A 11 (1940) 6–12, MR 1, 199; II, Proc. Indian Acad. Sci. Sect. A 11 (1940) 73–80, MR 1, 291; III, Proc. Indian Acad. Sci. Sect. A 13 (1941) 530–533, MR 3, 66; IV, Bull. Calcutta Math. Soc. 36 (1944) 99–101, MR 6, 170.
[15] P. Schumer, The Josephus problem: once more around, Math. Mag. 75 (1) (2002) 12–17.
[16] P.G. Tait, On the generalization of the Josephus problem, Proc. Roy. Soc. Edinburgh 22 (1898) 165–168; Collected Scientific Papers, vol. II, Cambridge, 1900, pp. 432–435.
[17] A. Terras, Fourier Analysis on Finite Groups and Applications, London Math. Soc. Stud. Texts, vol. 43, 1999.
[18] G.L. Wilson, On the Jospehus Permutation, M.S. thesis, California State University Hayward, August 1979.
[19] G.L. Wilson, Three enumeration problems for a congruence equation, Linear Multilinear Algebra 14 (1) (1983).