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.