ARITHMETIC SUBSEQUENCES IN A RANDOM ORDERING OF AN ADDITIVE SET

Marcel K. Goh

Department of Mathematics, McGill University, Montréal, Québec, Canada

Rosie Y. Zhao

School of Computer Science, McGill University, Montréal, Québec, Canada

Abstract

For a finite set A of size n, an ordering is an injection from $\{1, 2, \ldots, n\}$ to A. We present results concerning the asymptotic properties of the length L_n of the longest arithmetic subsequence in a random ordering of an additive set A. In the torsion-free case where $A = [1, n]^d \subseteq \mathbf{Z}^d$, we prove that $L_n \sim 2d \log n / \log \log n$. We show that the case $A = \mathbf{Z}/n\mathbf{Z}$ behaves asymptotically like the torsion-free case with $d = 1$, and then use this fact to compute the expected length of the longest arithmetic subsequence in a random ordering of an arbitrary finite abelian group. We also prove that the number of orderings of $\mathbf{Z}/n\mathbf{Z}$ without any arithmetic subsequence of length 3 is 2^{n-1} when $n \geq 2$ is a power of 2, and zero otherwise. We conclude with a concrete application to elementary p-groups and a discussion of possible noncommutative generalizations.

1. Introduction

Arithmetic progressions are most often viewed as subsets of an ambient abelian group Z. Under this interpretation and with $Z = \mathbf{Z}$, the group of integers, E. Szemerédi's celebrated theorem states that any dense subset A of Z contains arbitrarily long arithmetic progressions [13]. The story is different when the elements of A are ordered in a sequence and we look for progressions in *sub-*

sequences. For example, it is always possible to permute the first n integers so that no subsequence of length 3 is an arithmetic progression [7]. Using this fact, J. A. Davis, R. C. Entringer, R. L. Graham, and G. J. Simmons showed in 1977 that there are permutations of the positive integers that do not contain any arithmetic progressions of length 5 and permutations of $\mathbf{Z}$ avoiding 7-term arithmetic progressions [5]. Whether or not there exist permutations of the positive integers not admitting any permutation of length 4 remains an open problem to this day, but J. Geneson has recently improved the result of Davis et al. for $\mathbf{Z}$ to 6-term arithmetic progressions [9].

In an arbitrary abelian group Z, an entirely different formulation of the problem studies bijections σ from Z to itself, declaring a k-term arithmetic progression to be a tuple $(z_1, z_2, \ldots, z_k) \in Z^k$ such that there exists some r for which $z_{i+1} - z_i = r$ for every $1 \le i < k$. A permutation is said to *destroy* (3-term) arithmetic progressions if for every triple $(x, y, z) \in Z^3$, either (x, y, z) is not a progression or $\big(\sigma(x), \sigma(y), \sigma(z)\big)$ is not a progression. For Z infinite, P. Hegarty showed that there exists a progression-destroying permutation of Z if and only if $Z/\Omega_2(Z)$ is equipotent to Z, where $\Omega_2(Z)$ is the subgroup of elements with even order [10]. When $Z = (\mathbf{Z}/p\mathbf{Z})^d$ for p prime, N. D. Elkies and A. A. Swaminathan proved that there exist progression-destroying permutations if and only if $(p, d) \notin \big\{(3, 1), (5, 1), (7, 1)\big\}$ and p is odd [6].

The above definition of a progression in a permutation is not the one that we will study. Instead, we will *order* the elements of an additive set A from 1 to $|A|$ and count arithmetic progressions that appear in order in the sequence. (Thus our definition is closer to the one used by Davis et al.; Hegarty's definition above is akin to requiring that the indices of an arithmetic subseqence form a progression as well.) Though it may be possible to find perverse orderings of an additive set A that admit no arithmetic subsequences of a given length k, it is natural to suspect that as the size of A gets large, this becomes more and more unlikely in some formal sense. We can then replace a difficult extremal problem with a simpler probabilistic one. In this paper, we show that when $A = \{1, 2, \ldots, n\} \subseteq \mathbf{Z}$, and the ordering is taken uniformly at random from $\mathfrak{S}_n$ (the group of permutations of an n-element set), the length of the longest arithmetic progression converges to $2 \log n / \log \log n$ in probability. We also show analogous results when Z is a finite cyclic group and A is taken to be the whole group. In the case of an arbitrary finite abelian group Z, one cannot make any sensible asymptotic statements that depend only on the order of the group, but we will see that the counting methods used in the $\mathbf{Z}^d$ and cyclic cases can be extended to give bounds on the expected number of arithmetic subsequences

of a given length k in a random ordering of Z.

Results of this type have appeared in the literature for progressions (viewed as subsets) in a random set. In the case of a random subset of $\{1, 2, \ldots, n\}$, where each element is included independently with probability $1/2$, I. Benjamini, A. Yadin, and O. Zeitouni showed that the expected length of the longest arithmetic progression is asymptotically $2 \log n / \log 2$, and that the asymptotics do not change if the integers are taken modulo n [2]. Returning to the setting of random sequences, A. Frieze proved in 1991 that the length of the longest monotone increasing subsequence of a random permutation of $\{1, 2, \ldots, n\}$ is concentrated around $2\sqrt{n}$, its asymptotic expected value [8].

We will make frequent use of the following asymptotic notation for non-negative-valued functions $f, g : \mathbf{N} \to \mathbf{R}$. We write $f(n) = O_n\big(g(n)\big)$ if there exists a constant C such that $f(n) \leq C \cdot g(n)$ for all $n \in \mathbf{N}$. When $\lim_{n \to \infty} f(n)/g(n) = 0$, we write $f(n) = o_n\big(g(n)\big)$, and if instead we have $\lim_{n \to \infty} f(n)/g(n) = \infty$, then we write $f(n) = \omega_n\big(g(n)\big)$. Lastly, if $\lim_{n \to \infty} f(n)/g(n) = 1$, then we write $f(n) \sim_n g(n)$. In all cases, we may omit the subscript when the asymptotic variable is clear from context.

In this paper, the notation $[a, b]$ will indicate the *discrete* interval $\{n \in \mathbf{Z} : a \leq n \leq b\}$, unless otherwise stated. Formally, an *additive set* is a pair (A, Z), where $(Z, +)$ is an abelian group with identity 0 and $A \subseteq Z$ is finite and nonempty. When the ambient group is evident from context, we will write A for (A, Z). For $n \in \mathbf{Z}$ and $z \in Z$, we let nz denote the iterated sum; so $2z = z + z$ and $-3z = -z - z - z$. The *order* $|z|$ of a group element z is the smallest positive integer n such that $nz = 0$. If no such integer exists, then we put $|z| = \infty$. A group all of whose elements have finite order is called a *torsion group*, while a group in which every non-identity element has infinite order is a *torsion-free group*.

For our purposes, an *ordering* σ of an additive set A is a bijection $\sigma : [1, |A|] \to A$ and we will regard such an ordering as a sequence by listing its elements $\sigma = \big(\sigma(1), \sigma(2), \ldots, \sigma(|A|)\big)$ in order. More generally, a *k-ordering* of a set A, where $k \leq |A|$, is an injection from $[1, k] \to |A|$ and it can also be regarded as a sequence. We will say that a subsequence $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}$ with $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ is an *arithmetic progression* (or simply *progression*) of length k if for some $a, r \in Z$,

$$(\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}) = \big(a, a + r, \ldots, a + (k-1)r\big).$$

The element a is called the *base point* and r is called the *step* or *common difference*. If $r = 0$, the progression is said to be *trivial*; because we will most

often be looking at progressions in sequences without repetition, a progression will be assumed to be nontrivial unless otherwise stated.

Let σ be an ordering of an additive set A of size n. We define $L(\sigma)$ to be the largest k for which there exists a subsequence of σ that is an arithmetic progression of length k. For example, if σ is the ordering $(2, 7, 1, 6, 3, 4, 5)$ of $[1, 7]$, then $L(\sigma) = 4$, due to the embedded 4-ordering $(2, 3, 4, 5)$. We can make σ random by fixing an enumeration $f : [1, n] \to A$, selecting π uniformly at random from the group $\mathfrak{S}_n$, and then letting $\sigma = f \circ \pi$. This makes $L(\sigma)$ a random variable, which we will denote by L_n. We are interested in determining how L_n grows as n gets large.

2. Torsion-free Groups

By the structure theorem of finitely-generated abelian torsion-free groups, every abelian torsion-free group is isomorphic to a lattice $\mathbf{Z}^d$ for $d \geq 0$ (when $d = 0$, this is the trivial group, so we will assume that $d \geq 1$ for the rest of this section). A natural subset of $\mathbf{Z}^d$ to consider is $A = [1, n]^d$. We first prove a lemma for the simplest case $d = 1$, then generalize the result to any value of d.

Lemma 1. *For $1 \leq k \leq n$, let P_{nk} be the number of k-orderings of $[1, n]$ that are arithmetic progressions, i.e., of the form*

$$\big(a, a + r, a + 2r, \ldots, a + (k-1)r\big)$$

for some $a, r \in \mathbf{Z}$. We have $P_{n1} = n$ and

$$P_{nk} = 2n \left\lfloor \frac{n-1}{k-1} \right\rfloor - (k-1)\left(\left\lfloor \frac{n-1}{k-1} \right\rfloor^2 + \left\lfloor \frac{n-1}{k-1} \right\rfloor \right) \tag{1}$$

for $2 \leq k \leq n$, as well as the bounds

$$\frac{(n-k+2)(n-1)}{k-1} - k + 1 \leq P_{nk} \leq \frac{(n-k+2)(n-1)}{k-1} + k - 3. \tag{2}$$

Proof. The case $k = 1$ counts the n one-element sequences (i) for $1 \leq i \leq n$. Let $2 \leq k \leq n$; here the chief constraint is that both a and $a + (k-1)r$ must belong to $[1, n]$. We sum over the possible values of the step r. It must belong

to one of the two discrete intervals $\pm\left[1, \big((n-1)/(k-1)\big)\right]$, and the number of valid choices for a decreases as $|r|$ increases. If r is positive, then it is easy to see that $1 \le a \le n - (k-1)r$ by the above constraint. Similarly, if r is negative, then $n + (k-1)r + 1 \le a \le n$. In general, with n, k, and r fixed, the number of possibilities for a is $n - (k-1)|r|$. Exploiting the symmetry of the two cases, we compute

$$P_{nk} = \sum_{r=1}^{\lfloor (n-1)/(k-1) \rfloor} 2\big(n - (k-1)r\big)$$

$$= 2n \left\lfloor \frac{n-1}{k-1} \right\rfloor - 2(k-1) \sum_{r=1}^{\lfloor (n-1)/(k-1) \rfloor} r, \tag{3}$$

yielding Equation (1). Letting $\{x\}$ denote the fractional part of x and using the identity $\lfloor x \rfloor = x - \{x\}$, from Equation (1) we obtain

$$P_{nk} = 2n \left(\frac{n-1}{k-1} - \left\{ \frac{n-1}{k-1} \right\} \right)$$

$$- (k-1)\left(\left(\frac{n-1}{k-1} - \left\{ \frac{n-1}{k-1} \right\} \right)^2 + \frac{n-1}{k-1} - \left\{ \frac{n-1}{k-1} \right\} \right)$$

$$= \left(\frac{n-1}{k-1} \right)\big(2n - (n-1) - (k-1)\big)$$

$$- \big(-2n + 2(n-1) + (k-1)\big)\left\{ \frac{n-1}{k-1} \right\} - (k-1)\left\{ \frac{n-1}{k-1} \right\}^2$$

$$= \frac{(n-k+2)(n-1)}{k-1} + (k-3)\left\{ \frac{n-1}{k-1} \right\} - (k-1)\left\{ \frac{n-1}{k-1} \right\}^2, \tag{4}$$

which, since both $\{x\}$ and $\{x\}^2$ are nonnegative and less than 1 for any x, proves Equation (2). $\qquad\square$

Lemma 2. *Let P_{nk} be the number of k-orderings of $[1,n]$ that are an arithmetic progression. The number of k-orderings of $[1,n]^d$ that form an arithmetic progression is*

$$P_{nkd} = (P_{nk} + n)^d - n^d. \tag{5}$$

Proof. Let $a, r \in [1,n]^d$. Writing $a = (a_1, a_2, \ldots, a_d)$ and $r = (r_1, r_2, \ldots, r_d)$, the arithmetic progression

$$\big(a, a + r, a + 2r, \ldots, a + (k-1)r\big)$$

has entries in $[1, n]^d$ if and only if the projection onto the jth coordinate

$$\left(a_j, a_j + r_j, a_j + 2r_j, \ldots, a_j + (k-1)r_j\right)$$

is an arithmetic progression and has entries in $[1, n]^d$ for every $1 \leq j \leq d$. All but one of the projections may be a trivial progression, with $r = 0$. We did not count the trivial progressions in Lemma 1 because we were counting sequences without repetition, so by including the n trivial progressions, the number of valid pairs (a_j, r_j) increases to $P_{nk} + n$ for any j. Forming the product over all j, we arrive at $(P_{nk} + n)^d$, but we also counted n^d undesirable trivial progressions in $\mathbf{Z}^d$. Subtracting them proves the lemma. $\qquad\square$

We were quite careful with the calculations in these lemmas, but to prove our first main result, we will only need the fact that $P_{nkd} \sim_n n^{2d}/(k-1)^d$. The bulk of the work is done in the next lemma, which has been formulated more generally so that it may be reused in later sections. We will require the *gamma function* $\Gamma(z) = \int_0^\infty x^{z-1} e^{-x}\, dx$, which, in this form, is defined for all complex numbers with $\Re z > 0$ and for all nonnegative integers, $\Gamma(n+1) = n!$ (a classic treatment can be found in [15]). Our main result relies on the fact that for any $f : \mathbf{N} \to \mathbf{R}$, there exists a function $g : \mathbf{R} \to \mathbf{R}$, analytic on all of $\mathbf{R}$, such that $g(n) = f(n)$ for all $n \in \mathbf{N}$. (This is a special case of a result of basic complex analysis; see for example, [1], page 197.)

Lemma 3. *Let (A_n, Z_n) be a family of nonempty additive sets indexed by the positive integers and let $P_n(k)$ denote the number of k-orderings of A_n that are an arithmetic progression. Suppose that*

i) for any fixed $k \in \mathbf{N}$, $P_n(k+1)/P_n(k) \to 1$ as $n \to \infty$; and

ii) there exists a function $f : \mathbf{N} \to \mathbf{R}$ such that for all n, $P_n(k) < k!$ for all $k > f(n)$ and for any $O\big(f(n)\big)$ function $g(n)$, $P_n\big(g(n)\big) \to \infty$ as $n \to \infty$.

Let $P_n^*(x)$ be the analytic continuation of P_n to all of $\mathbf{R}$ and let L_n denote the length of the longest arithmetic subsequence in an ordering of A_n chosen uniformly at random. There exists a function $\psi : \mathbf{N} \to \mathbf{R}$ that is $O\big(f(n)\big)$ and $\omega(1)$ such that for all positive integers n,

$$\frac{P_n^*(\psi(n))}{\Gamma(\psi(n) + 1)} = 1 \tag{6}$$

and $\mathbf{P}\{\psi(n) - 6 \leq L_n < \psi(n) + 1\} \to 1$ as $n \to \infty$.

Proof. We first prove the existence of the function ψ. Let $n \in \mathbf{N}$ and note first that $P_n^*(1) = |A_n|$, since this is the number of distinct base points. If $|A_n| = 1$,

we set $\psi(n) = 1$. Otherwise, we may consider the function $h_n(x) = P_n^*(x) - \Gamma(x+1)$, which is analytic on the real interval $[1, \infty)$ and positive at $x = 1$, since in this case $h_n(1) = |A_n| > 1$. By hypothesis (ii), whenever $k > f(n)$ is an integer we must have $P_n^*(k) < \Gamma(k+1)$. Note that $h_n(f(n)+1) < 0$, so by the intermediate value theorem, there exists a point $1 < x^* < f(n) + 1$ for which $h_n(x^*) = 0$ and we can set $\psi(n) = x^*$ (if there is more than one choice for x^*, we pick the smallest one). It is clear from this construction that $\psi(n)$ must be $O(f(n))$, and $\psi(n)$ must also be $\omega(1)$; otherwise setting $g = \psi$ violates hypothesis (ii) by continuity of the function $\Gamma(x+1)$.

In the random ordering of A_n, there are $\binom{|A_n|}{k}$ subsequences of length k. Each of the $k!\binom{|A_n|}{k} = |A_n|!/(|A_n| - k)!$ orderings of length k has an equal chance of appearing as a subsequence of the random ordering, so the probability of a given subsequence of length k being an arithmetic progression is $P_n(k)(|A_n| - k)!/|A_n|!$. Let $\mathcal{C}(k)$ be the set of all subsequences of length k in the original random sequence; we have $|\mathcal{C}(k)| = \binom{|A_n|}{k}$. For a subsequence $S \in \mathcal{C}(k)$, let B_S be the event that S is a k-term arithmetic progression. Letting $N(n, k)$ denote the number of k-term arithmetic progressions in the ordering of A_n, we have, by linearity of expectation,

$$\mathbf{E}\{N(n,k)\} = \mathbf{E}\left\{\sum_{S \in \mathcal{C}(k)} \mathbf{1}_{B_S}\right\} = \sum_{S \in \mathcal{C}(k)} \mathbf{P}\{B_S\}$$
$$= \binom{|A_n|}{k} \frac{P_n(k)(|A_n| - k)!}{|A_n|!} = \frac{P_n(k)}{k!}. \tag{7}$$

By hypothesis (i), we see that

$$\frac{\mathbf{E}\{N(n, k+1)\}}{\mathbf{E}\{N(n, k)\}} = \frac{P_n(k+1)}{(k+1)!} \cdot \frac{k!}{P_n(k)} \sim_n \frac{1}{k+1} \tag{8}$$

and hence the expected value of $N(n, k)$ decreases with k. We constructed $\psi(n)$ so that $\mathbf{E}\{N(n, \psi(n))\} = 1$, so a union bound now gives

$$\mathbf{P}\{L_n \geq \psi(n) + 1\} \leq \mathbf{E}\{N(n, \psi(n) + 1)\}$$
$$= \frac{\mathbf{E}\{N(n, \psi(n) + 1)\}}{\mathbf{E}\{N(n, \psi(n))\}} \tag{9}$$
$$\sim_n \frac{1}{\psi(n) + 1},$$

which goes to zero as $n \to \infty$ since $\psi(n) \to \infty$.

On the other hand, we have

$$\frac{\mathbf{E}\{N(n,\psi(n))\}}{\mathbf{E}\{N(n,\psi(n)-1\}} \sim_n \frac{1}{\psi(n)}, \tag{10}$$

which implies that $\mathbf{E}\{N(n,\psi(n)-1)\} \sim_n \psi(n)$. Continuing in this manner, we see that $\mathbf{E}\{N(n,\psi(n)-s)\} \sim_n \psi(n)^s$ and $\lim_{n\to\infty} \mathbf{E}\{N(n,\psi(n)-s)\} = \infty$ for all integers $1 \le s < \psi(n)$. To turn this into a lower bound on L_n, one must also analyse the behaviour of the second moment

$$\mathbf{E}\{N(n,k)^2\} = \mathbf{E}\Big\{\Big(\sum_{S\in\mathcal{C}(k)} \mathbf{1}_{B_S}\Big)\Big(\sum_{T\in\mathcal{C}(k)} \mathbf{1}_{B_T}\Big)\Big\}. \tag{11}$$

For any S in $\mathcal{C}(k)$ and $0 \le m \le k$, let $\mathcal{C}_{Sm}(k) \subseteq \mathcal{C}(k)$ denote the set of all subsequences T of length k that have exactly m elements in common with S and that are themselves progressions (i.e., such that B_T holds). Then, expanding the second moment to

$$\mathbf{E}\{N(n,k)^2\} = \mathbf{E}\Big\{\sum_{S\in\mathcal{C}(k)} \mathbf{1}_{B_S} \sum_{m=0}^{k} |\mathcal{C}_{S_m}(k)|\Big\}, \tag{12}$$

we approach the inner summation by considering each set $\mathcal{C}_{Sm}(k)$ separately. Assuming both S and T are k-term arithmetic progressions, for $1 \le m \le k$, we note that if T and S both contain m elements, then those m elements must form a subprogression of both T and S. There are no more than k^2 ways to form a subprogression of length m in S, since there are k choices for the first element of the subprogression and $\le k$ choices for the second element; these two choices determine the subprogression entirely. Now, given a specific subprogression R of length m, we count the number of possibilities for T. The first element of R is the jth element of T for some $1 \le j \le k$, so there are no more than k possibilities for its position in T. There are also $\le k$ choices for the second element of R, and after this, T is completely defined. Thus $|\mathcal{C}_{Sm}(k)| \le k^4$ for all $1 \le m \le k$. (This is a substantial overcount for $m > 1$; when $m = k$ there is in fact only one possibility for T.) Next, we consider the set $\mathcal{C}_{S0}(k)$ of all sequences that have no elements in common with S, which has size $\binom{|A_n|-k}{k}$. Each of these subsequences is a progression with probability no more than

$$\frac{P_n(k)}{\binom{|A_n|-k}{k}k!} = \frac{P_n(k)(|A_n|-2k)!}{(|A_n|-k)!}, \tag{13}$$

so the expected number of progressions among these subsequences is at most $P_n(k)/k!$. Putting these facts together, we find that

$$\mathbf{E}\big\{N(n,k)^2\big\} \leq \frac{P_n(k)}{k!}\left(\frac{P_n(k)}{k!} + \sum_{m=1}^{k} k^4\right) = \frac{P_n(k)}{k!}\left(\frac{P_n(k)}{k!} + k^5\right), \quad (14)$$

meaning that $\mathbf{V}\big\{N(n,k)\big\} \leq P_n(k)k^5/k!$. We have, by the Chung-Erdős inequality [4],

$$\mathbf{P}\{L_n < k\} = \mathbf{P}\big\{N(n,k) = 0\big\} \leq \frac{\mathbf{V}\big\{N(n,k)\big\}}{\mathbf{E}\big\{N(n,k)\big\}^2} = \frac{k^5}{P_n(k)/k!}.$$

Plugging in $k = \psi(n) - 6$, we have

$$\mathbf{P}\{L_n < \psi(n) - 6\} \leq \frac{\mathbf{V}\big\{N(n,\psi(n)-6)\big\}}{\mathbf{E}\big\{N(n,\psi(n)-6)\big\}^2} \sim_n \frac{\big(\psi(n)-6\big)^5}{\psi(n)^6} \to 0.$$

We have shown that $\mathbf{P}\big\{\psi(n)-6 \leq L_n < \psi(n)+1\big\} \to 1$, completing the proof. $\square$

Note that this lemma does not use the commutativity of the groups Z_n; in the final section of this paper we briefly discuss possible noncommutative generalizations. Our first main theorem is a direct consequence of the previous lemma.

Theorem 4. *For positive integers n and d, let L_n denote the longest arithmetic subsequence in an ordering of $[1,n]^d$, chosen uniformly at random. There exists a function $\psi(n,d)$ with $\psi(n,d) \sim_n 2d\log n/\log\log n$ such that the probability that $\psi(n,d)-6 \leq L_n < \psi(n,d)+1$ tends to 1 as n approaches infinity.*

Proof. Set $Z_n = \mathbf{Z}^d$ for all n, let $A_n = [1,n]^d$, and let $P_n^*(k)$ be the analytic continuation of P_{nkd} as defined in Lemma 2. A simple computation shows that for fixed k and d, $P_{(n+1)kd}/P_{nkd} \to 1$ as $n \to \infty$, and setting $f(n) = n$, we have $P_{nkd} = 0 < k!$ for all $k > f(n)$. By our earlier observation that $P_{nkd} \sim_n n^{2d}/(k-1)^d$, substituting any $O(n)$ function for k we have $\lim_{n\to\infty} P_{nkd} = \infty$. Thus we may apply Lemma 3 to obtain a function $\psi(n,d)$ satisfying

$$\frac{P_{n(\psi(n,d))d}}{\psi(n,d)!} = 1,$$

for all $n \in \mathbf{N}$. The fact that $P_{nkd} \sim_n n^{2d}/(k-1)^d$ implies that $\psi(n,d)! \sim_n n^{2d}/(\psi(n,d)-1)^d$, and applying Stirling's formula, we obtain $\psi(n,d) \sim_n 2d \log n / \log \log n$. The rest of the theorem follows from the previous lemma, and *a fortiori* we have $L_n \sim_n 2d \log n / \log \log n$. $\qquad\square$

Because the set of arithmetic progressions is invariant under translation and dilation, as a corollary in the integer case we can replace $[1,n]$ with the entries of any arithmetic progression of length n.

Corollary 5. *Let S be an arithmetic progression of length n in $\mathbf{Z}$, i.e., S is of the form*

$$S = \big(a, a+r, a+2r, \ldots, a+(n-1)r\big)$$

for some $a, r \in \mathbf{Z}$, $r \neq 0$. Randomly permute the entries of S and let L_n be the length of the longest arithmetic progression in the shuffled sequence. If ψ is the function given by Theorem 4, then $\psi(n) - 6 \leq L_n < \psi(n) + 1$ with probability that tends to 1 as the length n of the arithmetic progression tends to infinity. $\qquad\square$

For $d = 1$ and small values of n, one can easily generate the exact distribution of L_n using a computer. Let $f_n(k)$ denote the number of permutations of $[1,n]$ whose longest embedded arithmetic progression has length k; so $\mathbf{P}\{L_n = k\} = f_n(k)/n!$. Table 1 contains the values of $f_n(k)$ for $n \leq 10$. No general formula for $f_n(k)$ has been found, but the case $k = 2$ (these are known as 3-*free permutations*) has received a fair amount of attention in the literature. A. Sharma found the explicit upper bound $f_n(2) \leq (2.7)^n/21$, valid for $n \geq 11$, as well as the asymptotic result $f_n(2) = \omega_n(2^n n^k)$, which holds for any choice of k [12]. The lower bound was improved to $(1/2)c^n$ for $n \geq 8$, where $c = 2132^{1/10} \approx 2.152$, by T. D. LeSaulnier and S. Vijay [11]. More recently, B. Correll, Jr. and R. W. Ho presented an efficient dynamic programming algorithm to count 3-free permutations and used these results to inductively refine previously-known bounds [3].

n	$f_n(1)$	$f_n(2)$	$f_n(3)$	$f_n(4)$	$f_n(5)$	$f_n(6)$	$f_n(7)$	$f_n(8)$	$f_n(9)$	$f_n(10)$
1	1									
2	0	2								
3	0	4	2							
4	0	10	12	2						
5	0	20	82	16	2					
6	0	48	516	134	20	2				
7	0	104	3232	1480	198	24	2			
8	0	282	21984	15702	2048	274	28	2		
9	0	496	168368	162368	28048	3204	362	32	2	
10	0	1066	1306404	1902496	374194	39420	4720	462	36	2

Table 1: Permutations of $[1, n]$ with longest arithmetic subsequence of length k

3. Finite Additive Groups

The aim of this section is to extend our result for torsion-free groups to finite abelian groups. Thus, for a finite abelian group Z, we are now studying the case $A = Z$. The extension proceeds smoothly in the case of cyclic groups, which in turn provides some information for arbitrary finite additive groups via the structure theorem.

We shall prove that the case in which $Z = \mathbf{Z}/n\mathbf{Z}$ and $A = Z$ has the same asymptotics as the case $A = [1, n] \subseteq \mathbf{Z}$. Before we proceed, we recall that Euler's *totient function* $\varphi(n)$ counts the numbers coprime to and less than a given n, that is,

$$\varphi(n) = \big|\{m \in [1, n] : \gcd(m, n) = 1\}\big|.$$

A basic result of group theory states that for $1 \leq d < n$, the number of elements of order d in $\mathbf{Z}/n\mathbf{Z}$ is $\varphi(d)$. We will write $d\backslash n$ to indicate that d divides n. As before, we count progressions in k-orderings of A, starting first with the case that $Z = \mathbf{Z}/n\mathbf{Z}$, the cyclic group of order n.

Lemma 6. *Let Q_{nk} denote the number of k-orderings of $\mathbf{Z}/n\mathbf{Z}$ that form an arithmetic progression. For every n, $Q_{n1} = n$ and $Q_{nk} = 0$ for all $k > n$; for $2 \leq k \leq n$, we have*

$$Q_{nk} = n\Big(n - \sum_{j=1}^{k-1} \mathbf{1}_{[j\backslash n]}\varphi(j)\Big). \tag{15}$$

In particular, $Q_{nn} = n\varphi(n)$ and we also have the bounds

$$n^2 - \frac{3}{\pi^2}n(k-1)^2 - o_k(nk^2) \le Q_{nk} \le n(n-1). \tag{16}$$

If n is prime, then $Q_{nk} = n(n-1)$ for all k.

Proof. The cases $k = 1$ and $k > n$ are obvious, so let $2 \le k \le n$. By the n-fold symmetry of $\mathbf{Z}/n\mathbf{Z}$, it suffices to count the number of k-term arithmetic progressions with base point 0, and then multiply the result by n. For any $r \in \mathbf{Z}/n\mathbf{Z} \setminus \{0\}$, the sequence

$$\big(0, r, 2r, \ldots, (k-1)r\big)$$

is a valid k-ordering if and only if the element 0 does not appear twice. This is equivalent to the condition that the order of r be at least k. Since the order of a group element must divide n, to calculate the number of possible steps r we start with n and subtract the number of elements of order j for $1 \le j \le k$ where $j \backslash n$; this equals $\varphi(j)$ for all $j < n$. Multiplying this by the n possible base points yields the formula Equation (15).

The fact that $Q_{nn} = n\varphi(n)$ follows from the observation that the summation equals $n - \varphi(n)$ when $k = n$. The upper bound in Equation (16) is clear because the summation is at least 1 (for $j = 1$); if n is prime, then this bound is met with equality. To prove the lower bound, we use the asymptotic formula

$$\sum_{j=1}^{k} \varphi(k) = \frac{3}{\pi^2}k^2 + O_k\big(k(\log k)^{2/3}(\log\log k)^{2/3}\big), \tag{17}$$

whose proof can be found in [14]. It yields

$$\begin{aligned} Q_{nk} &= n\Big(n - \sum_{j=1}^{k-1} \mathbf{1}_{[j\backslash n]}\varphi(j)\Big) \\ &\ge n\Big(n - \sum_{j=1}^{k-1} \varphi(j)\Big) \\ &= n^2 - \frac{3}{\pi^2}n(k-1)^2 - o_k(nk^2). \end{aligned} \tag{18}$$

Now we can compute the length of the longest arithmetic subsequence in an ordering of a cyclic group, which is similar to the case $d = 1$ in Theorem 4.

Theorem 7. *For a positive integer n, let L_n denote the length of the longest arithmetic subsequence of an ordering of $\mathbf{Z}/n\mathbf{Z}$, chosen uniformly at random. There exists a function $\chi(n)$ with $\chi(n) \sim_n 2 \log n / \log \log n$ such that $\chi(n) - 6 \leq L_n < \chi(n) + 1$ with probability tending to 1 as n tends to infinity.*

Proof. Let Q_{nk} be as in Lemma 6 and let $Q_n^*(x)$ be an analytic function on all of $\mathbf{R}$ such that $Q_n^*(k) = Q_{nk}$ for all positive integers k. For a fixed k, we have

$$\frac{(n+1)^2 - O_k\big((n+1)k^2\big)}{n(n-1)} \leq \frac{Q_{(n+1)k}}{Q_{nk}} \leq \frac{(n+1)n}{n^2 - O_k(nk^2)}. \qquad (19)$$

Taking n to infinity in both bounds tells us that $Q_{(n+1)k}/Q_{nk} \to 1$. Let $f(n) = n^{1/3} + C$, where C is chosen such that $f(n)! > n(n-1)$ for all $n \in \mathbf{N}$. So $Q_{nk} \leq n(n-1) < f(n)! < k!$ for any $k > f(n)$ and letting $g(n)$ be any $O(n^{1/3})$ function, we have, by the previous lemma, $Q_{ng(n)} \geq n^2 - O(ng(n)^2) = n^2 - o(n^2) \to \infty$, so we can apply Lemma 3 with $A_n = Z_n = \mathbf{Z}/n\mathbf{Z}$ for all n to obtain a function χ satisfying

$$\frac{Q_n^*(\chi(n))}{\Gamma(\chi(n) + 1)} = 1.$$

Since $\chi(n)! = Q_{n\chi(n)} = n^2 - o(n^2)$ for all $n \in \mathbf{N}$, we obtain $\chi(n) \sim_n 2 \log n / \log \log n$, from a simple application of Stirling's approximation, and we have $\chi(n) - 6 \leq L_n < \chi(n) + 1$ with probability tending to 1. $\qquad \square$

Note that although the function $\psi(n, 1)$ obtained by applying Theorem 4 to $d = 1$ has the same asymptotics as $\chi(n)$ from Theorem 7, we have $\psi(n, 1) < \chi(n)$. This follows from the functional equations defining ψ and χ and also makes sense intuitively, since it is easier, in some sense, to form a progression if one is allowed to loop around the edge of the interval, which is possible in the cyclic case. As a concrete example, $(0, 2, 6, 1, 3, 5, 4)$ has the 4-term arithmetic subsequence $(0, 6, 5, 4)$ when the sequence is regarded as an ordering of the group $\mathbf{Z}/7\mathbf{Z}$ (the base point is 0 and the step size is 6), but it has no arithmetic subsequence of length 4 when regarded simply as an ordering of the discrete interval $[0, 6]$.

Table 2 contains exact values of $g_n(k) = n!\mathbf{P}\{L_n = k\}$ for small n, and comparing Tables 1 and 2, it is clear that L_n is expected to be longer when $A_n = \mathbf{Z}/n\mathbf{Z}$ than when $A_n = [1, n]$. A closer look at Table 2 reveals certain curiosities not present in the torsion-free case. Firstly, the sequence $\mathbf{E}\{L_n\}$ is not strictly increasing; for instance, we have $\mathbf{E}\{L_7\} = 4.25$ and $\mathbf{E}\{L_8\} \approx 4.136$.

n	$g_n(1)$	$g_n(2)$	$g_n(3)$	$g_n(4)$	$g_n(5)$	$g_n(6)$	$g_n(7)$	$g_n(8)$	$g_n(9)$	$g_n(10)$
1	1									
2	0	2								
3	0	0	6							
4	0	8	8	8						
5	0	0	40	60	20					
6	0	0	468	192	48	12				
7	0	0	462	3150	1176	210	42			
8	0	128	4192	27872	6592	1312	192	32		
9	0	0	57402	182790	99630	19656	2970	378	54	
10	0	0	67440	1795320	1594640	146200	22000	2840	320	40

Table 2: Orderings of $\mathbf{Z}/n\mathbf{Z}$ whose longest arithmetic subsequence has length k

The same can be said for L_{11} and L_{12}, and this phenomenon can be attributed to the fact that Q_{nk} is greater, in proportion to n, when n is prime. Next, we see that $\mathbf{P}\{L_n = n\} = n\varphi(n)$, which follows directly from Lemma 6. Lastly, we note that an ordering of $\mathbf{Z}/n\mathbf{Z}$ can be 3-free only if n is a power of 2. In fact, we can derive a simple explicit formula for the number of 3-free orderings of $\mathbf{Z}/n\mathbf{Z}$.

Theorem 8. *Let $n \geq 1$ be an integer. The number $g_n(2)$ of orderings of $\mathbf{Z}/n\mathbf{Z}$ that do not contain any arithmetic subsequence of length 3 equals 2^{n-1} if $n = 2^m$ for some $m \geq 1$, and is zero otherwise. An ordering of $\mathbf{Z}/2^m\mathbf{Z}$ that contains no progression of length 3 consists of 2^{m-1} elements of the same parity, followed by the 2^{m-1} elements of the opposite parity.*

Proof. In this proof all arithmetic operations are taken modulo n. Obviously $g_1(2) = 0$, so we begin by supposing that $n = p$ is an odd prime and fixing an arbitrary ordering of $\mathbf{Z}/p\mathbf{Z}$. Let z_1 and z_2 denote the first two elements of the sequence and consider $r = z_2 - z_1$. Since p is odd, $z_2 + r \neq z_1$ and must therefore come later in the sequence. So there is an embedded progression of length 3. More generally, suppose that $n \geq 3$ is not a power of 2 and let p be an odd prime that divides n. Note that the elements $0, n/p, 2n/p, \ldots, (p-1)n/p$ must appear in some order in the sequence, and this sequence contains a 3-term progression if and only if the same ordering, with each element divided by n/p, is a 3-term progression. But this is an ordering of $0, 1, 2, \ldots, p-1$, and we already showed that every ordering of $\mathbf{Z}/p\mathbf{Z}$ contains a 3-term arithmetic progression when p is an odd prime.

Now we handle the case in which $n = 2^m$, by induction on m. For the case

$m = 1$, both orderings of $\mathbf{Z}/2\mathbf{Z}$ are 3-free, and both can be split into an odd half and an even half. Now suppose that there are $2^{n/2-1}$ orderings of $\mathbf{Z}/(n/2)\mathbf{Z}$ that are 3-free. For any pair (S, T) of such orderings, with $S = (s_1, s_2, \ldots, s_{n/2})$ and $T = (t_1, t_2, \ldots, t_{n/2})$, note that

$$(2s_1, 2s_2, \ldots, 2s_{n/2}, 2t_1 + 1, 2t_2 + 1, \ldots, 2t_1 + 1)$$

and

$$(2t_1 + 1, 2t_2 + 1, \ldots, 2t_{n/2} + 1, 2s_1, 2s_2, \ldots, 2s_{n/2})$$

are two orderings of $\mathbf{Z}/n\mathbf{Z}$ that are 3-free and uniquely determined by the pair (S, T). This means there are at least $2 \cdot (2^{n/2-1})^2 = 2^{n-1}$ orderings of $\mathbf{Z}/n\mathbf{Z}$ with no 3-term arithmetic progressions. To see that we have, in fact, counted all of them, let an ordering of $\mathbf{Z}/n\mathbf{Z}$ be given that is 3-free; we aim to show that it is of one of the two forms prescribed above. Let S be the subsequence of all even elements, and let T be the subsequence of all odd elements. Note that neither of these two subsequences can contain a progression of length 3, so these sequences S and T were included in the count above. The last thing to show is that all the even elements are on one side of the ordering and all of the odd elements are on the other side. To do this, fix an odd element z and consider $z + 1$ and $z - 1$. These elements are distinct (since n is a power of 2) and both even, but if one is to the left of z and one is to the right, then a 3-term progression appears. So both $z + 1$ and $z - 1$ are on the same side of z (without loss of generality, assume it is the left side). Next, consider $z + 3$ and $z - 3$. For the same reason as before, they must both be on the same side of z, but if they are to the right of z, then we would have one of the arithmetic subsequences $(z - 1, z + 1, z + 3)$ or $(z + 1, z - 1, z - 3)$, depending on the order of $z + 1$ and $z - 1$. An analogous argument applies if $z + 1$ and $z - 1$ had been to the right of z. So $z + 3$ and $z - 3$ are on the same side of z as $z + 1$ and $z - 1$. Continuing in this manner for $z \pm 5, z \pm 7, \ldots$, we find that all of the even elements are on the same side of all of the odd elements, meaning that the sequences of the form given in the theorem statement are the only 3-free orderings. The induction is complete and the theorem is proved. □

Because the groups of order n may have wildly different structures, we cannot hope to give a sensible asymptotic result that is valid for all finite additive groups. For example, both $\mathbf{Z}/2^d\mathbf{Z}$ and $(\mathbf{Z}/2\mathbf{Z})^d$ have order 2^d, but Theorem 7 tells us that a random ordering of the first group will have an arithmetic subsequence of length asymptotic to $2\log(2^d)/\log\log(2^d)$ with probability tending to 1, while

an ordering of the second group cannot have a 3-term arithmetic subsequence. Every finite abelian group Z admits a unique *invariant factor decomposition*

$$Z = \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_d\mathbf{Z}$$

where $n_1 \backslash n_2$, $n_2 \backslash n_3$, and so on (the factors increase in size from left to right). In other words, $\mathbf{Z}/n_d\mathbf{Z}$ is the largest cyclic subgroup of Z and Z cannot be written as a product of fewer than d cyclic groups. Of course, we have $n = n_1 n_2 \cdots n_d$. With this decomposition, we can generalize the bounds obtained in Lemma 6 to all finite additive groups.

Lemma 9. *Let Z be a group of order n whose invariant factor decomposition is*

$$Z = \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_d\mathbf{Z}.$$

Let Q_{nk} be as in Lemma 6 and for $2 \le k \le n_d$, let $Q_k(Z)$ be the number of k-orderings of Z that are an arithmetic progression; so $Q_{nk} = Q_k(\mathbf{Z}/n\mathbf{Z})$. Let j be the smallest index for which $k \le n_j$. Then

$$n \prod_{i=j}^{d} n_i - O_k(nk^{2d}) \le Q_k(Z) \le n \prod_{i=j}^{d} n_i - n. \tag{20}$$

Proof. For the upper bound, we cannot simply take a product over the $Q_{n_i k}$, because this does not count progressions whose projection onto some factor is not a valid k-ordering. For example, $\big((0,4),(2,6),(0,0)\big)$ is a valid progression in $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$, but its projection onto $\mathbf{Z}/4\mathbf{Z}$ is $(0,2,0)$, which is not a valid 3-ordering. Instead, we form the product of trivial progressions in the first $j-1$ factors with the number $n_i{}^2$ of starting pairs in the last $d-j+1$ factors, and then subtract the n progressions that are trivial in Z, obtaining

$$Q_{nk} \le \Big(\prod_{i=1}^{j-1} n_i\Big)\Big(\prod_{i=j}^{d} n_i{}^2\Big) - n = n \prod_{i=j}^{d} n_i - n. \tag{21}$$

As for the lower bound, we can undercount the number of progressions in Z by counting the product of trivial progressions in the first $j-1$ factors and valid

nontrivial progressions in the remaining $d - j + 1$ factors. This gives us

$$
\begin{aligned}
Q_k(Z) &\geq \Big(\prod_{i=1}^{j-1} n_i \Big) \Big(\prod_{i=j}^{d} Q_{n_i k} \Big) \\
&\geq \Big(\prod_{i=1}^{j-1} n_i \Big) \Big(\prod_{i=j}^{d} \big(n_i{}^2 - 3n_i(k-1)^2/\pi^2 - o_k(n_i k^2) \big) \Big) \qquad (22) \\
&\geq n \prod_{i=j}^{d} n_i - O_k(nk^{2d}). \quad \blacksquare
\end{aligned}
$$

Thus for a finite abelian group Z and a given k, one can compute the decomposition of Z into d invariant factors $\mathbf{Z}/n_1\mathbf{Z}, \ldots, \mathbf{Z}/n_d\mathbf{Z}$ and determine the smallest index j for which $k \leq n_j$. Then if N_k denotes the number of k-term arithmetic progressions that appear as subsequences in a random ordering of Z, we have

$$
\frac{nn_j n_{j+1} \cdots n_d - n}{k!} - O_k(nk^{2d}) \leq \mathbf{E}\{N_k\} \leq \frac{nn_j n_{j+1} \cdots n_d - n}{k!}. \qquad (23)
$$

This fact can be used to construct sequences of abelian groups Z_n that can be fed into Lemma 3 to obtain asymptotic information about the length of the maximal arithmetic subsequence.

We end this section by outlining an an explicit example in which $n_1 = n_2 = \cdots = n_d = p$, a prime number. An *elementary p-group* is an abelian group isomorphic to $(\mathbf{Z}/p\mathbf{Z})^d$ for some prime p and integer d. Thus we have a sequence of additive groups $Z_p = (\mathbf{Z}/p\mathbf{Z})^d$ indexed by the primes. Since $Q_{pk} = p(p-1)$ for every $2 \leq k \leq p$, by a calculation similar to that used in the proof of Lemma 2, the number of k-orderings of $(\mathbf{Z}/p\mathbf{Z})^d$ that are an arithmetic progression is $(Q_{pk} + p)^d - p^d = p^{2d} - p^d$. Letting $\tau(p, d)$ be the function from $\mathbf{R}$ to $\mathbf{R}$ satisfying

$$
\frac{p^{2d} - p^d}{\Gamma(\tau(p, d) + 1)} = 1, \qquad (24)
$$

we have $\tau(p, d) \sim_p 2d \log p / \log \log p$ and Lemma 3 tells us that $\tau(p, d) - 6 \leq L_n \tau(p, d) + 1$ with probability tending to one as p marches towards infinity along the primes. (Strictly speaking, one would actually have to modify the statement and hypotheses of Lemma 3 to allow for sequences of groups A_n indexed by any monotone increasing sequence of positive integers.) The same asymptotic result holds if the primes p are replaced by arbitrary integers n, but in this

case the function $\tau(n,d)$ is not monotone with respect to n. So although we still have $\tau(n,d) \sim_n 2d \log n / \log \log n$, the values of $\tau(n,d)$ will fluctuate as n approaches infinity, attaining local maxima at prime values of n.

4. Further Work

We will now discuss some related problems that have yet to be resolved, as well as possible noncommutative generalizations. As mentioned in the introduction, it is still unknown whether permutations of the positive integers must necessarily contain arithmetic progressions of length 4. Furthermore, the functions $f_n(k)$ and $g_n(k)$ remain largely unstudied, except in the case $k = 2$. One might study the number of $(k+1)$-free orderings of $[1,n]$ or $\mathbf{Z}/n\mathbf{Z}$, which corresponds to the partial sums

$$\sum_{j=1}^{k} f_n(j) \quad \text{and} \quad \sum_{j=1}^{k} g_n(j),$$

respectively.

We end off by briefly considering what happens when we remove the condition that the underlying group be abelian. We will denote a non-abelian group by G and use multiplicative notation; thus for $r \in G$ we have, for instance, $r^2 = rr$ and $r^{-3} = r^{-1}r^{-1}r^{-1}$. A *left progression* is a sequence $(a, ra, r^2a, \dots, r^{k-1}a)$, where $a, r \in G$ and $k \in \mathbf{Z}$. With the same definitions for a, r, and k, a *right progression* is a sequence $(a, ar, ar^2, \dots, ar^{k-1})$. Note that the length of the longest left progression in a sequence is not the same, in general, as the length of the longest right progression. For example, in the free group F_2, with generators a and b, the sequence (a, ba, b^2a) contains a left progression of length 3 but no right progression of length 3.

However, in the case that $A \subseteq G$ is closed under inverses, the number of k-orderings of A that are left progressions is the same as the number of k-orderings of A that are right progressions, because if $S(A,k)$ is the set of all k-orderings of A, there is a bijection $f : S(A,k) \to S(A,k)$ that maps $(s_1, s_2, \dots, s_k)$ to $(s_1{}^{-1}, s_2{}^{-1}, \dots, s_k{}^{-1})$, and a sequence $T \in S(A,k)$ is a left progression if and only if $f(T)$ is a right progression. In particular, if every k-ordering of A is just as likely to arise as a subsequence of some ordering of A, then the expected number of left progressions of length k in a random ordering is the same as the expected number of right progressions.

It would be interesting to compute asymptotic formulas for L_n, akin to the

ones we found for $\mathbf{Z}^d$, $\mathbf{Z}/n\mathbf{Z}$, and $(\mathbf{Z}/p\mathbf{Z})^d$, for families of non-abelian groups, such as the free groups F_d, the symmetric groups $\mathfrak{S}_n$, or the dihedral groups D_n. In an infinite group such as F_d, one must select a finite subset A. A somewhat natural choice for the free group is the set of all reduced words with length at most n, but perhaps a more faithful analogue of $[1, n]^d \subseteq \mathbf{Z}^d$ is the set of all words $w \in F_d$ such that $f(w) \in [-n, n]^d$ where f is the canonical homomorphism from F_d to $F_d/[F_d, F_d] \cong \mathbf{Z}^d$. In any case, both of these subsets of F_d are closed under inverses, so it suffices to study, say, the longest right progression. The second moment method we used in Lemma 3 did not rely on the group being abelian, but we anticipate that more sophisticated counting methods will be required to count the expected number of progressions in subsequences of orderings when dealing with nonabelian groups.

References

[1] Lars Valerian Ahlfors, *Complex Analysis*, McGraw-Hill, New York, 1953.

[2] Itai Benjamini, Ariel Yadin, and Ofer Zeitouni, Maximal arithmetic progressions in random subsets, *Electron. Commun. Probab.* **12** (2007), 365–376.

[3] Bill Correll, Jr. and Randy Wesley Ho, A note on 3-free permutations, *Integers* **17** (2017), A55, 10 pp..

[4] Kai Lai Chung and Paul Erdős, On the application of the Borel-Cantelli lemma, *Trans. Amer. Math. Soc.* **72** (1952), 179–186.

[5] James Avery Davis, Roger Charles Entringer, Ronald Lewis Graham, and Gustavus James Simmons, On permutations containing no long arithmetic progressions, *Acta Arith.* **34** (1977), 81–90.

[6] Noam David Elkies and Ashvin Anand Swaminathan, Permutations that destroy arithmetic progressions in elementary p-groups, *Electron. J. Combin.* **24** (2017), P1.20.

[7] Roger Charles Entringer and Douglas Elmer Jackson, Elementary Problem 2440, *Amer. Math. Monthly* **80** (1973), 1058.

[8] Alan Frieze, On the length of the longest monotone subsequence in a random permutation, *Ann. Appl. Probab.* **1** (1991), 301–305.

[9] Jesse Geneson, Forbidden arithmetic progressions in permutations of subsets of the integers, *Discrete Math.* **342** (2019), 1489–1491.

[10] Peter Hegarty, Permutations avoiding arithmetic patterns, *Electron. J. Combin.* **11** (2004), R39.

[11] Timothy Dale LeSaulnier and Sujith Vijay, On permutations avoiding arithmetic progressions, *Discrete Math.* **311** (2011), 205–207.

[12] Arun Sharma, Enumerating permutations that avoid three-term arithmetic progressions, *Electron. J. Combin.* **16** (2009), R63.

[13] Endre Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27** (1975), 199–245.

[14] Arnold Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1963.

[15] Edmund Taylor Whittaker and George Neville Watson, *A Course of Modern Analysis, 4th ed.*, Cambridge University Press, Cambridge, 1996.