

Rainbow arithmetic progressions

STEVE BUTLER, CRAIG ERICKSON, LESLIE HOGBEN,
KIRSTEN HOGENSON, LUCAS KRAMER, RICHARD L. KRAMER,
JEPHIAN CHIN-HUNG LIN, RYAN R. MARTIN*, DERRICK STOLEE,
NATHAN WARNBERG, AND MICHAEL YOUNG†

In this paper, we investigate the anti-Ramsey (more precisely, anti-van der Waerden) properties of arithmetic progressions. For positive integers n and k , the expression $\text{aw}([n], k)$ denotes the smallest number of colors with which the integers $\{1, \dots, n\}$ can be colored and still guarantee there is a rainbow arithmetic progression of length k . We establish that $\text{aw}([n], 3) = \Theta(\log n)$ and $\text{aw}([n], k) = n^{1-o(1)}$ for $k \geq 4$.

For positive integers n and k , the expression $\text{aw}(\mathbb{Z}_n, k)$ denotes the smallest number of colors with which elements of the cyclic group of order n can be colored and still guarantee there is a rainbow arithmetic progression of length k . In this setting, arithmetic progressions can “wrap around,” and $\text{aw}(\mathbb{Z}_n, 3)$ behaves quite differently from $\text{aw}([n], 3)$, depending on the divisibility of n . As shown in [Jungić et al., *Combin. Prob. Comput.*, 2003], $\text{aw}(\mathbb{Z}_{2^m}, 3) = 3$ for any positive integer m . We establish that $\text{aw}(\mathbb{Z}_n, 3)$ can be computed from knowledge of $\text{aw}(\mathbb{Z}_p, 3)$ for all of the prime factors p of n . However, for $k \geq 4$, the behavior is similar to the previous case, that is, $\text{aw}(\mathbb{Z}_n, k) = n^{1-o(1)}$.

KEYWORDS AND PHRASES: Arithmetic progression, rainbow coloring, anti-Ramsey, Behrend construction.

1. Introduction

Let G be an additive (abelian) group such as the integers or the integers modulo n , and let S be a finite nonempty subset of G . A k -term arithmetic progression (k -AP) in S is a set of distinct elements of the form

$$a, a + d, a + 2d, \dots, a + (k - 1)d$$

arXiv: [1404.7232](https://arxiv.org/abs/1404.7232)

*Research supported in part by National Security Agency grant H98230-13-1-0226.

†Research supported in part by NSF DMS 0946431.

where $d \geq 1$ and $k \geq 2$. An r -coloring of S is a function $c : S \rightarrow [r]$, where $[r] := \{1, \dots, r\}$. We say such a coloring is *exact* if c is surjective. Given an r -coloring c of S , the i^{th} color class is $C_i := \{x \in S : c(x) = i\}$. An arithmetic progression is called *rainbow* if the image of the progression under the r -coloring is injective. Formally, given $c : S \rightarrow [r]$ we say a k -term arithmetic progression is rainbow if $\{c(a + id) : i = 0, 1, \dots, k - 1\}$ has k distinct values.

The *anti-van der Waerden number* $\text{aw}(S, k)$ is the smallest r such that every exact r -coloring of S contains a rainbow k -term arithmetic progression. Note that this tautologically defines $\text{aw}(S, k) = |S| + 1$ whenever $|S| < k$, and this definition retains the property that there is a coloring with $\text{aw}(S, k) - 1$ colors that has no rainbow k -AP. Since $\text{aw}(S, 2) = 2$ for all S , we assume henceforth that $k \geq 3$.

Several important results on the existence of rainbow 3-APs implying information about $\text{aw}([n], 3)$ and $\text{aw}(\mathbb{Z}_n, 3)$ (in our notation) have been established by Jungić, et al. [8]. A preliminary study of the anti-van der Waerden number was done by Uherka in [13]; it should be noted the notation there is slightly different, with $AW(k, n)$ used to denote our $\text{aw}([n], k)$. Other results on balanced colorings of the integers with no rainbow 3-AP have been obtained by Axenovich and Fon-Der-Flaass [1] and Axenovich and Martin [2].

First, we consider the set $S = [n]$. The value of $\text{aw}([n], 3)$ is logarithmic in n :

Theorem 1.1. *For every integer $n \geq 9$,*

$$\lceil \log_3 n \rceil + 2 \leq \text{aw}([n], 3) \leq \lceil \log_2 n \rceil + 1.$$

Moreover, $\text{aw}([n], 3) = \lceil \log_3 n \rceil + 2$ for $n \in \{3, 4, 5, 6, 7\}$ and $\text{aw}([8], 3) = 5$.

Theorem 1.1 is proven by Lemmas 2.3 and 2.6 (for $n \geq 9$), and Remark 2.1 gives exact values of $\text{aw}([n], 3)$ that justify the second statement. We conjecture that the lower bound is, essentially, correct:

Conjecture 1.2. *There exists a constant C such that $\text{aw}([n], 3) \leq \lceil \log_3 n \rceil + C$ for all $n \geq 3$.*

The behavior of $\text{aw}([n], k)$ is, however, different for $k \geq 4$. Instead of logarithmic, it is almost linear:

Theorem 1.3. *For $k \geq 4$,*

$$ne^{-O(\sqrt{\log n})} < \text{aw}([n], k) \leq ne^{-\log \log \log n - \omega(1)}.$$

Theorem 1.3 is established by Lemma 2.8 and Corollary 2.14.

Finally, we consider arithmetic progressions in the cyclic group \mathbb{Z}_n .

Remark 1.4. For positive integers n and k , $\text{aw}(\mathbb{Z}_n, k) \leq \text{aw}([n], k)$, because every AP in $[n]$ corresponds to an AP in \mathbb{Z}_n .

However, because progressions in \mathbb{Z}_n may “wrap around,” there are additional APs in \mathbb{Z}_n , some of which may be rainbow. Thus it is possible that every coloring of \mathbb{Z}_n with $\text{aw}([n], k) - 1$ colors guarantees a rainbow k -AP, so strict inequality is possible. As was shown in [8, Theorem 3.5] (and follows from Theorem 1.6 below), there are infinitely many values of n for which $\text{aw}(\mathbb{Z}_n, 3) = 3$, for example, when n is a power of two.

Definition 1.5. Let $n \geq 3$ be an integer. Define $f_2(n)$ to be 0 if n is odd and 1 if n is even. Define $f_3(n)$ to be the number of odd prime factors p of n that have $\text{aw}(\mathbb{Z}_p, 3) = 3$ and $f_4(n)$ to be the number of odd prime factors p of n that have $\text{aw}(\mathbb{Z}_p, 3) = 4$, both counted according to multiplicity.

Theorem 1.6. *For every prime number p , $3 \leq \text{aw}(\mathbb{Z}_p, 3) \leq 4$. For an integer $n \geq 2$, the value of $\text{aw}(\mathbb{Z}_n, 3)$ is determined by the values of $\text{aw}(\mathbb{Z}_p, 3)$ for the prime factors p :*

$$\text{aw}(\mathbb{Z}_n, 3) = 2 + f_2(n) + f_3(n) + 2f_4(n).$$

For an integer $n \geq 2$ having every prime factor less than 100, $f_4(n)$ is the number of odd prime factors of n in the set $Q_4 := \{17, 31, 41, 43, 73, 89, 97\}$ and $f_3(n)$ is the number of odd prime factors of n in Q_3 , where Q_3 is the set of all odd primes less than 100 and not in Q_4 .

Theorem 1.6 is established by Proposition 3.5, Corollary 3.15 and Proposition 3.17.

For $k \geq 4$, the bounds we obtain for $\text{aw}(\mathbb{Z}_n, k)$ are the same as those for $\text{aw}([n], k)$:

Theorem 1.7. *For $k \geq 4$,*

$$ne^{-O(\sqrt{\log n})} < \text{aw}(\mathbb{Z}_n, k) \leq ne^{-\log \log \log n - \omega(1)}.$$

Theorem 1.7 is established by Remark 1.4 and Lemma 3.20.

The structure of the paper is as follows: Section 2 presents results pertaining to $\text{aw}([n], k)$, with Theorem 1.1 proved in Section 2.1 and Theorem 1.3 proved in Section 2.2. Results pertaining to $\text{aw}(\mathbb{Z}_n, k)$ appear in Section 3, with Theorem 1.6 proved in Section 3.1 and Theorem 1.7 proved in Section 3.2. Section 4 describes the methods and algorithms used to compute

values of $\text{aw}([n], k)$ and $\text{aw}(\mathbb{Z}_n, k)$, while Section 5 contains conjectures and open questions for future research.

In the remainder of this section we establish a basic but necessary observation that $\text{aw}(S, \cdot)$ is monotone in k .

Observation 1.8. *Let G be an additive (abelian) group such as the integers or the integers modulo n , let S be a finite nonempty subset of G , and let $k \geq 3$ be an integer. Then $\text{aw}(S, k) \leq \text{aw}(S, k + 1)$.*

Observation 1.8 follows immediately from Proposition 1.9 below and was noted by Uherka in [13] for the function $\text{aw}([n], \cdot)$.

Proposition 1.9. *Let G be an additive (abelian) group such as the integers or the integers modulo n , let S be a finite nonempty subset of G , and let $k \geq 3$ be an integer. If there is an exact r -coloring of S that has no rainbow k -AP, then $\text{aw}(S, k) \geq r + 1$.*

Proof. Let c be an exact r -coloring of S with color set $\{1, \dots, r\}$ that has no rainbow k -AP. We proceed by constructing an exact $(r - 1)$ -coloring of S with no rainbow k -AP. For $x \in S$, define

$$\hat{c}(x) = \begin{cases} c(x) & \text{if } c(x) \in \{1, \dots, r - 2\}, \\ r - 1 & \text{if } c(x) \in \{r - 1, r\}. \end{cases}$$

Note that \hat{c} is an exact $(r - 1)$ -coloring of S . Let K be a k -AP in S . Since there is no rainbow k -AP under c there exists $j, \ell \in K$ such that $c(j) = c(\ell)$. It then follows that $\hat{c}(j) = \hat{c}(\ell)$. Hence K is not rainbow under the coloring \hat{c} . By the generality of K , \hat{c} is an exact $(r - 1)$ -coloring of S that has no rainbow k -AP. Repeating this construction we obtain an exact $(r - i)$ -coloring of S with no rainbow k -AP for $i \in \{1, 2, \dots, r - 1\}$. Therefore $\text{aw}(S, k) \geq r + 1$. \square

2. $\text{aw}([n], k)$

In this section we establish properties of $\text{aw}([n], k)$. Sections 2.1 and 2.2 establish our main results for $\text{aw}([n], 3)$ and $\text{aw}([n], k), k \geq 4$, respectively. Sections 2.3 and 2.4 contain additional results valid for all k and specific to $k = 3$, respectively.

In Table 1 we give our calculated values of $\text{aw}([n], k)$ for $k \geq 3$. We have a larger list of known values in the case of $k = 3$ that is included in Remark 2.1 below; in Table 1 we include only the values $\text{aw}([n], 3)$ for which we have a value for $\text{aw}([n], 4)$ so that we may compare them. We also restrict $n, k \geq 3$, and have stopped with $k = \lceil \frac{n}{2} \rceil + 1$, because $\text{aw}([n], k) = n$ if and only if $k \geq \lceil \frac{n}{2} \rceil + 1$ (Proposition 2.16 below).

The growth rates when $k = 3$ and when $k \geq 4$ appear to be different based on data given in Table 1. The upper bound of $\lceil \log_2 n \rceil + 1$ given in Proposition 2.6 for $k = 3$ and the lower bound of $n^{1-o(1)}$ in Lemma 2.8 for $k \geq 4$ confirm that the growth rates are indeed radically different.

Table 1: Values of $\text{aw}([n], k)$ for $3 \leq k \leq \frac{n+3}{2}$

$n \setminus k$	3	4	5	6	7	8	9	10	11	12	13	14
3	3											
4	4											
5	4	5										
6	4	6										
7	4	6	7									
8	5	6	8									
9	4	7	8	9								
10	5	8	9	10								
11	5	8	9	10	11							
12	5	8	10	11	12							
13	5	8	11	11	12	13						
14	5	8	11	12	13	14						
15	5	9	11	13	14	14	15					
16	5	9	12	13	15	15	16					
17	5	9	13	13	15	16	16	17				
18	5	10	14	14	16	17	17	18				
19	5	10	14	15	17	17	18	18	19			
20	5	10	14	16	17	18	19	19	20			
21	5	11	14	16	17	19	20	20	20	21		
22	6	12	14	17	18	20	21	21	21	22		
23	6	12	14	17	19	20	21	22	22	22	23	
24	6	12	15	18	20	20	22	23	23	23	24	
25	6	12	15	19	21	21	23	23	24	24	24	25

2.1. Main results for $\text{aw}([n], 3)$

Before we address Theorem 1.1, we show a summary of the computed data for this case in Remark 2.1 below.

Remark 2.1. The exact values of $\text{aw}([n], 3)$ are known from computer computations (described in Section 4) for $n \leq 58$, and are recorded here.

1. $\text{aw}([n], 3) = 2$ for $n \in \{1\}$.
2. $\text{aw}([n], 3) = 3$ for $n \in \{2, 3\}$.
3. $\text{aw}([n], 3) = 4$ for $n \in \{4, \dots, 7\} \cup \{9\}$.

- 4. $\text{aw}([n], 3) = 5$ for $n \in \{8\} \cup \{10, \dots, 21\} \cup \{27\}$.
- 5. $\text{aw}([n], 3) = 6$ for $n \in \{22, \dots, 26\} \cup \{28, \dots, 58\}$.

Now we turn to the proof of Theorem 1.1, beginning with the lower bound.

Proposition 2.2. *Let n be a positive integer and let $s \in \{-2, -1, 0, 1, 2\}$. Then $\text{aw}([3n - s], 3) \geq \text{aw}([n], 3) + 1$ provided $n \geq s$.*

Proof. Let $r = \text{aw}([n], 3)$ and $s \in \{0, 1, 2\}$. We construct an exact r -coloring of $[3n - s]$ that does not contain a rainbow 3-AP. By definition there exists an exact $(r - 1)$ -coloring, denoted c , of $[n]$ such that there is no rainbow 3-AP in $[n]$. Color $[3n - s]$ in the following manner: If $i + s$ is divisible by 3, then $\hat{c}(i) = c((i + s)/3)$, otherwise $\hat{c}(i) = r$. Consider a 3-AP, K , in $[3n - s]$. Then either the three terms in $K + s$ are all divisible by 3 or at least two of the terms in $K + s$ are not divisible by 3. If all terms in $K + s$ are divisible by 3, then K is not rainbow under \hat{c} , since there is no rainbow 3-AP under c . If two terms of $K + s$ are not divisible by 3 then those two terms are both colored r and K is not rainbow. Hence $\text{aw}([3n - s], 3) \geq r + 1$ for $s \in \{0, 1, 2\}$.

For $s \in \{-2, -1\}$, use the same coloring as for $s = 0$. □

Using Proposition 2.2, we establish the lower bound in Theorem 1.1.

Lemma 2.3. *Let n be a positive integer. Then $\text{aw}([n], 3) \geq \lceil \log_3 n \rceil + 2$.*

Proof. The proof is by induction. The cases $n = 1, 2, 3$ are true by inspection. Suppose $n > 3$ and that $\text{aw}([m], 3) \geq \lceil \log_3 m \rceil + 2$ for all m satisfying $1 \leq m < n$. We show that $\text{aw}([n], 3) \geq \lceil \log_3 n \rceil + 2$. First, we write $n = 3m - s$, where $s \in \{0, 1, 2\}$ and $2 \leq m < n$. Then by Proposition 2.2,

$$\begin{aligned} \text{aw}([n], 3) &= \text{aw}([3m - s], 3) \geq \text{aw}([m], 3) + 1 \geq \lceil \log_3 m \rceil + 2 + 1 \\ &= \lceil \log_3(3m) \rceil + 2 \geq \lceil \log_3 n \rceil + 2. \end{aligned} \quad \square$$

Example 2.4. Induction and the proof of Proposition 2.2 produce the following exact $(m + 1)$ -coloring of $[3^m]$ that does not have a rainbow 3-AP: For $x \in [3^m]$ with the prime factorization $x = 2^{e_2} 3^{e_3} 5^{e_5} \dots p^{e_p}$, $c(x) = m + 1 - e_3$. This attains the value in Lemma 2.3.

To complete the proof of Theorem 1.1, we establish the upper bound.

Lemma 2.5. *Let c be an exact r -coloring of $[n]$ that does not have a rainbow 3-AP. For $i \in [r]$, define $b_i \in [n]$ to be the least x such that the induced coloring on $[x]$ has exactly i colors. Then for all $i \in [r - 1]$, $b_{i+1} \geq 2b_i$. Furthermore, for any $1 \leq i \leq j \leq r$, we have $b_j \geq 2^{j-i} b_i$.*

Proof. Observe that $b_1 = 1$. Suppose that $b_{i+1} < 2b_i$ for some $i \in [r - 1]$. Then $\{2b_i - b_{i+1}, b_i, b_{i+1}\}$ is a rainbow 3-AP. The last statement follows by induction, since $b_i \leq 2^{-1}b_{i+1} \leq 2^{-2}b_{i+2} \leq \dots \leq 2^{-(j-i)}b_j$. \square

Lemma 2.6. For $n \geq 9$, $\text{aw}([n], 3) \leq \lceil \log_2 n \rceil + 1$.

Proof. Suppose $r = \text{aw}([n], 3) - 1$, so there is an r -coloring with no rainbow 3-AP. Lemma 2.5 implies that $n \geq b_r \geq 2^{r-1}$. Thus $\text{aw}([n], 3) \leq \lfloor \log_2 n \rfloor + 2$, which establishes the result for n not a power of 2. The case $\text{aw}([2^m], 3) \leq m + 1$ follows similarly by using the fact that $\text{aw}([2^m], 3) = m + 1$ for $m = 4$ and $m = 5$ (see Remark 2.1); $\text{aw}([16], 3) = 5$ implies $b_5 > 16 = 2^4$ for any rainbow-free coloring with $r \geq 5$. Then for $m > 5$, Lemma 2.5 implies an r -coloring of 2^m has $2^m \geq b_r \geq 2^{r-5}b_5 > 2^{r-1}$, so $m \geq r$ and $m + 1 \geq \text{aw}(2^m, 3)$. \square

This completes the proof of Theorem 1.1.

2.2. Main results for $\text{aw}([n], k), k \geq 4$

In this section we specialize to the case $k \geq 4$, focusing on lower and upper bounds that give $\text{aw}([n], k) = n^{1-o(1)}$. Lemma 2.8 gives the lower bound and Corollary 2.14 gives the upper bound.

Let $\text{sz}(n, k)$ denote the largest size of a set $S \subseteq [n]$ such that S contains no k -AP (similar notation was introduced in [5] in honor of Szemerédi [12]). Determining bounds on $\text{sz}(n, k)$ is a fundamental problem in the study of arithmetic progressions. Behrend [3], Gowers [6], and others [9, 10] have established various bounds on $\text{sz}(n, k)$. Proposition 2.7 provides a strong link between $\text{sz}(n, k)$ and our anti-van der Waerden numbers, allowing us to use known results on $\text{sz}(n, k)$ to bound $\text{aw}(n, k)$.

Proposition 2.7. For all $n > k \geq 3$,

$$\text{sz}(n, \lfloor k/2 \rfloor) + 1 \leq \text{aw}([n], k) - 1 \leq \text{sz}(n, k).$$

Proof. If c is an exact r -coloring of $[n]$ that contains no rainbow k -AP, then selecting one element of each color class creates a set S that contains no k -AP; therefore $\text{aw}([n], k) - 1 \leq \text{sz}(n, k)$. If S is a set in $[n]$ that contains no $\lfloor k/2 \rfloor$ -AP, then color $[n]$ by giving each element in S a distinct color and the elements of $[n] \setminus S$ a new color. If a k -AP $\{a_1, a_2, \dots, a_k\}$ is rainbow in this coloring, then exactly one such a_i is in $[n] \setminus S$. But this implies that the entries a_j where $j \not\equiv i \pmod{2}$ form an AP in S with at least $\lfloor k/2 \rfloor$ terms, a contradiction. \square

2.2.1. Theorem 1.3: proof of lower bound Lemma 2.6 and Behrend’s results (stated in Theorem 2.10 and Proposition 2.11 below) show that the upper bound in Proposition 2.7 is not useful for $k = 3$. Observe that when $k \in \{4, 5\}$, the lower bound in Proposition 2.7 is trivial but is in fact useful in the case of $k \geq 6$. We provide a similar lower bound for $k \in \{4, 5\}$ in Lemma 2.8 by carefully studying Behrend’s original construction [3] of a relatively large set $S \subset [n]$ that contains no 3-AP, thus giving a lower bound on $\text{sz}(n, 3)$.

Let $\{a_1, a_2, a_3, a_4\}$ be a 4-AP with $a_1 \leq a_2 \leq a_3 \leq a_4$. A set $A \subset \{a_1, a_2, a_3, a_4\}$ of size $|A| = 3$ is called a *punctured 4-AP*. If such a punctured 4-AP A is not a 3-AP, then it is of the form $A = \{a_1, a_2, a_4\}$ or $A = \{a_1, a_3, a_4\}$. We prove that Behrend’s construction in fact contains no punctured 4-AP (Proposition 2.9 below). This leads to Lemma 2.8 below.

Lemma 2.8. *There exists an absolute constant $b > 0$ such that for all $n, k \geq 4$,*

$$\text{aw}([n], k) > ne^{-b\sqrt{\log n}} = n^{1-o(1)}.$$

The proof of Lemma 2.8 follows from Proposition 2.9, Theorem 2.10, Proposition 2.11 and Proposition 2.12, which follow.

Proposition 2.9. *Suppose $S \subseteq [n]$ does not contain any punctured 4-APs. Then $\text{aw}([n], k) > |S| + 1$ for all $n \geq k \geq 4$.*

Proof. Color each member of S a distinct color, and color each integer in $[n] \setminus S$ with a new color called *zero*. If there is a rainbow 4-AP in this coloring, then at most one of the elements in this 4-AP is colored zero. Thus there must be a punctured 4-AP in the other colors, but S contains no punctured 4-AP. \square

There is a bijection between vectors $\mathbf{x} = (x_1, \dots, x_m)^\top \in \mathbb{Z}^m$ where $x_i \in \{0, 1, \dots, 2d - 2\}$ for all $i \in [m]$ and elements of $\{0, 1, \dots, (2d - 1)^m - 1\}$, by viewing \mathbf{x} as a $(2d - 1)$ -ary representation of an integer:

$$\mathbf{x} = (x_1, \dots, x_m)^\top \longleftrightarrow a_{\mathbf{x}} = \sum_{i=1}^m x_i(2d - 1)^{i-1}.$$

Moreover, observe that if $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^m$ with $x_i, y_i \in \{0, \dots, d - 1\}, i = 1, \dots, m$, are associated with $a_{\mathbf{x}}, a_{\mathbf{y}} \in \{0, 1, \dots, (2d - 1)^m - 1\}$ by this bijection, then $\mathbf{x} + \mathbf{y}$ has $x_i + y_i \in \{0, \dots, 2d - 1\}$ and $\mathbf{x} + \mathbf{y}$ is associated with $a_{\mathbf{x}+\mathbf{y}} = a_{\mathbf{x}} + a_{\mathbf{y}} \in \{0, 1, \dots, (2d - 1)^m - 1\}$.

Recall that for a vector $\mathbf{x} \in \mathbb{R}^m, \|\mathbf{x}\|^2 = \sum_{i=1}^m x_i^2$. Let m, ℓ, d be positive integers and define $X_\ell(m, d)$ to be the set of vectors $\mathbf{x} = (x_1, \dots, x_m)^\top$ such that

1. $x_i \in \{0, \dots, d - 1\}$ for all $i \in \{1, \dots, m\}$, and
2. $\|\mathbf{x}\|^2 = \ell$.

The set $S_\ell(m, d)$ of integers associated with the vectors in $X_\ell(m, d)$ via the map $\mathbf{x} \rightarrow a_{\mathbf{x}}$ forms a subset of integers in $\{0, 1, \dots, (2d-1)^m - 1\}$. Behrend [3] used the pigeonhole principle to prove the following lemma; here we state the version from [4].

Theorem 2.10. [3, 4] *There exist absolute constants $b, b' > 0$ such that for all n and positive integers $m = m(n)$, $\ell = \ell(n)$, and $d = d(n)$ such that $S_\ell(m, d) \subseteq [n]$ the following inequality holds:*

$$|S_\ell(m, d)| \geq \frac{b'n}{2\sqrt{8 \log_2 n} (\log n)^{1/4}} \geq ne^{-b\sqrt{\log n}}.$$

The important property of $S_\ell(m, d)$ is that it avoids non-trivial arithmetic progressions. We include Behrend’s simple proof of this fact for completeness.

Proposition 2.11. [3] *The set $S_\ell(m, d)$ contains no 3-AP.*

Proof. Suppose $\{a_{\mathbf{x}_1}, a_{\mathbf{x}_2}, a_{\mathbf{x}_3}\}$ is a 3-AP in $S_\ell(m, d)$. Let $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ be the associated vectors in $X_\ell(m, d)$. Since $a_{\mathbf{x}_1} + a_{\mathbf{x}_3} = 2a_{\mathbf{x}_2}$, we also have that $\mathbf{x}_1 + \mathbf{x}_3 = 2\mathbf{x}_2$. See Figure 1. However, by the triangle inequality, we have that

$$2\sqrt{\ell} = 2\|\mathbf{x}_2\| = \|\mathbf{x}_1 + \mathbf{x}_3\| \leq \|\mathbf{x}_1\| + \|\mathbf{x}_3\| = 2\sqrt{\ell},$$

and equality can only hold if $\mathbf{0}, \mathbf{x}_1, \mathbf{x}_3$ and $2\mathbf{x}_2$ are collinear. However, since $\|\mathbf{x}_1\| = \|\mathbf{x}_3\|$, this would imply $\mathbf{x}_1 = \mathbf{x}_3$ and thus $a_{\mathbf{x}_1} = a_{\mathbf{x}_3}$, a contradiction. \square

Proposition 2.12. *The set $S_\ell(m, d)$ contains no punctured 4-AP.*

Proof. Let $\{a_{\mathbf{x}_1}, a_{\mathbf{x}_2}, a_{\mathbf{x}_3}, a_{\mathbf{x}_4}\}$ be a 4-AP. Since $S_\ell(m, d)$ contains no 3-AP, it must be that one of $a_{\mathbf{x}_2}$ or $a_{\mathbf{x}_3}$ is not in $S_\ell(m, d)$. Assume by symmetry that $a_{\mathbf{x}_2} \notin S_\ell(m, d)$ and $a_{\mathbf{x}_1}, a_{\mathbf{x}_3}, a_{\mathbf{x}_4} \in S_\ell(m, d)$. Let $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4$ be the associated vectors where $\mathbf{x}_1, \mathbf{x}_3, \mathbf{x}_4 \in X_\ell(m, d)$.

Since $a_{\mathbf{x}_1} + a_{\mathbf{x}_3} = 2a_{\mathbf{x}_2}$, we have $\mathbf{x}_1 + \mathbf{x}_3 = 2\mathbf{x}_2$. See Figure 1. However, as in the proof of Proposition 2.11, this implies that $\|\mathbf{x}_2\| < \sqrt{\ell}$. Since $a_{\mathbf{x}_2} + a_{\mathbf{x}_4} = 2a_{\mathbf{x}_3}$, we have $\mathbf{x}_2 + \mathbf{x}_4 = 2\mathbf{x}_3$. However, this implies that

$$2\sqrt{\ell} = 2\|\mathbf{x}_3\| = \|\mathbf{x}_2 + \mathbf{x}_4\| \leq \|\mathbf{x}_2\| + \|\mathbf{x}_4\| < 2\sqrt{\ell},$$

a contradiction. \square

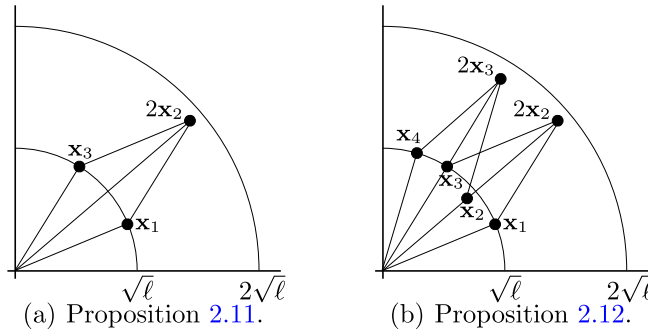


Figure 1: Proofs of Propositions 2.11 and 2.12.

Lemma 2.8 now follows by combining Propositions 2.9 and 2.12. It may be possible that the bound in Lemma 2.8 could be improved by using the construction of Elkin [4, 7] that avoids 3-APs using $\frac{bn(\log n)^{1/4}}{2^{\sqrt{8 \log_2 n}}}$ elements for some constant $b > 0$. Since this construction avoids a 3-AP, we can use Proposition 2.7 directly in order to obtain a coloring with no 6-AP, giving $\text{aw}([n], k) > \frac{bn(\log n)^{1/4}}{2^{\sqrt{8 \log_2 n}}}$ for all $k \geq 6$. Further use of constructions of Rankin [10] or Laba and Lacey [9] of large sets that avoid k -APs could slightly improve the asymptotics of $\text{aw}([n], k)$, but these bounds are all of the form $n^{1-o(1)}$.

2.2.2. Theorem 1.3: proof of upper bound A theorem of Gowers, stated here as Theorem 2.13, provides an upper bound for $\text{aw}([n], k)$. However, n must be very large compared to k for this upper bound to be significantly different than the naïve upper bound of n itself.

Theorem 2.13. [6, Theorem 1.3] *For every positive integer k there is a constant $b = b(k) > 0$ such that every subset of $[n]$ of size at least $n(\log_2 \log_2 n)^{-b}$ contains a k -AP. Moreover, b can be taken to be $2^{-2^{k+9}}$.*

Corollary 2.14. *Let n and k be positive integers. Then there exists a constant b such that $\text{aw}([n], k) \leq \lceil n(\log_2 \log_2 n)^{-b} \rceil$. That is, for a fixed positive integer k , the function $\text{aw}([n], k)$ of n is $o(\frac{n}{\log \log n})$.*

Proof. Consider an exact t -coloring of $[n]$, where $t := \lceil n(\log_2 \log_2 n)^{-b} \rceil$ and $b = 2^{-2^{k+9}}$. Since the coloring is exact, there exists a set $A \subseteq [n]$ of t differently colored integers. By Theorem 2.13, A contains a k -AP. Therefore $\text{aw}([n], k) \leq t$. □

Note that the upper bound in Corollary 2.14 can be expressed as $ne^{-\log \log \log n - \omega(1)}$. Then combining this upper bound on $\text{aw}([n], k)$ and the lower bound from Lemma 2.8, we have that for $k \geq 4$

$$ne^{-b\sqrt{\log n}} < \text{aw}([n], k) \leq ne^{-\log \log \log n - \omega(1)}.$$

This completes the proof of Theorem 1.3.

2.3. Additional results for $\text{aw}([n], k)$ valid for all k

In this section we present some additional elementary results for $\text{aw}([n], k)$. The next proposition describes a relationship between $\text{aw}([n], k)$ and $\text{aw}([n - 1], k)$.

Proposition 2.15. *Let n and k be positive integers. Then $\text{aw}([n], k) \leq \text{aw}([n - 1], k) + 1$.*

Proof. Let $r = \text{aw}([n], k)$. Note that if $n < k$ our result follows from the definition. Suppose $n \geq k$. Then there is some exact $(r - 1)$ -coloring of $[n]$ that has no rainbow k -AP, and without loss of generality n is colored $r - 1$. Consider this coloring restricted to $[n - 1]$. Then we have two cases:

1. This is an exact $(r - 1)$ -coloring of $[n - 1]$.
2. The only integer in $[n]$ with the color $r - 1$ is n , so this is an exact $(r - 2)$ -coloring of $[n - 1]$.

Note that since $[n]$ had no rainbow k -AP in both of our cases we still do not have a rainbow k -AP. So by Proposition 1.9 we have $\text{aw}([n - 1], k) \geq r - 1 = \text{aw}([n], k) - 1$ and the result follows. \square

In the next proposition we characterize the values of k for which $\text{aw}([n], k) = n$.

Proposition 2.16. *Let n and k be positive integers with $k \leq n$. Then $\text{aw}([n], k) = n$ if and only if $k \geq \lceil \frac{n}{2} \rceil + 1$.*

Proof. Suppose $k \geq \lceil \frac{n}{2} \rceil + 1$. We show that $\text{aw}([n], k) > n - 1$. Color $\lceil \frac{n}{2} \rceil$ and $\lceil \frac{n}{2} \rceil + 1$ with the same color and all the remaining integers with unique colors. This is an exact $(n - 1)$ -coloring. Since $k \geq \lceil \frac{n}{2} \rceil + 1$, the integers in any k -AP must be consecutive integers, and the values $\lceil \frac{n}{2} \rceil$ and $\lceil \frac{n}{2} \rceil + 1$ must be contained in any k -AP. Hence no k -AP is rainbow.

For the converse, suppose $\text{aw}([n], k) = n$. Color $[n]$ with $n - 1$ colors such that there is no rainbow k -AP. Therefore exactly one color class has size two and the rest have size one. Denote the color class of size two as $C = \{n_1, n_2\}$,

$n_1 < n_2$. Then every k -AP contains both n_1 and n_2 , or else we would have a rainbow k -AP. Suppose that $k \leq \lceil \frac{n}{2} \rceil$. Then $\{1, 2, \dots, k\}$ and $\{n - k + 1, n - k + 2, \dots, n\}$ are k -APs. Note that $\{1, 2, \dots, k\} \subseteq \{1, 2, \dots, \lceil \frac{n}{2} \rceil\}$ and $\{n - k + 1, n - k + 2, \dots, n\} \subseteq \{\lfloor \frac{n}{2} \rfloor + 1, \dots, n\}$. Then $n_1, n_2 \in \{1, 2, \dots, \lceil \frac{n}{2} \rceil\} \cap \{\lfloor \frac{n}{2} \rfloor + 1, \dots, n\}$. This intersection is empty or contains one element depending on whether n is even or odd. In both cases, this contradicts the fact that $n_1 \neq n_2$ and $n_1, n_2 \in \{1, 2, \dots, \lceil \frac{n}{2} \rceil\} \cap \{\lfloor \frac{n}{2} \rfloor + 1, \dots, n\}$. Therefore $k \geq \lceil \frac{n}{2} \rceil + 1$. \square

The following upper bound was proved by Uherka [13]; we include the brief proof for completeness.

Proposition 2.17. [13] *Let $n, k, n_1,$ and n_2 be positive integers such that $k \leq n_1 \leq n_2 \leq n$ and $n_1 + n_2 = n$. Then $\text{aw}([n], k) \leq \text{aw}([n_1], k) + \text{aw}([n_2], k) - 1$.*

Proof. Let $r = \text{aw}([n_1], k) + \text{aw}([n_2], k) - 1$, and consider an arbitrary exact r -coloring c of $[n]$. Let $r_1 = |c([n_1])|$ and $r_2 = |c(\{n_1 + 1, \dots, n_1 + n_2\})|$. Since $n_1 + n_2 = n$, $r \leq r_1 + r_2$. This implies that $r_1 \geq \text{aw}([n_1], k)$ or $r_2 \geq \text{aw}([n_2], k)$. Clearly $r_1 \geq \text{aw}([n_1], k)$ implies c has a rainbow k -AP. By translating $c(\{n_1 + 1, \dots, n_1 + n_2\})$ to a coloring on $[n_2]$, we also see that c has a rainbow k -AP if $r_2 \geq \text{aw}([n_2], k)$. Thus $\text{aw}([n], k) \leq r = \text{aw}([n_1], k) + \text{aw}([n_2], k) - 1$. \square

2.4. Additional results for $\text{aw}([n], 3)$

In this section we establish additional bounds on $\text{aw}([n], 3)$ in Propositions 2.18 and 2.19, and use Proposition 2.19 together with Remark 2.1, Proposition 2.2, and Lemma 2.3 to compute (at least) 93 additional exact values for $\text{aw}([n], 3)$.

Proposition 2.18. *For $n \geq 2$, there exists $m \leq \lfloor \frac{n}{2} \rfloor$ such that $\text{aw}([n], 3) \leq \text{aw}([m], 3) + 1$.*

Proof. We may assume that $n \geq 3$, since the case $n = 2$ follows by inspection. Let $r = \text{aw}([n], 3)$. Then there exists an $(r - 1)$ -coloring, namely c , of $[n]$ that has no rainbow 3-AP. Let t be the length of a shortest consecutive integer sequence in $[n]$ that contains all $r - 1$ colors, say the interval is $\{s + 1, s + 2, \dots, s + t\}$ for some s . Define \hat{c} to be an $(r - 1)$ -coloring of $[t] = \{1, 2, \dots, t\}$ so that $\hat{c}(j) := c(s + j)$ for $1 \leq j \leq t$. Notice that $\hat{c}(1)$ and $\hat{c}(t)$ cannot be the same color and each must be the only element of its color class, or else we could find a smaller t . Let $\hat{c}(1) = a$ and define b_i to be the smallest element of $[t]$ such that $[b_i]$ has $i + 1$ colors for $1 \leq i \leq r - 2$. Note that if b_i is odd, i.e., $b_i = 2x + 1$, then $\{1, x + 1, 2x + 1\}$

is a rainbow 3-AP. So the set of even numbers of $[t]$ are colored with exactly $r - 2$ colors with no rainbow 3-AP. Define $m = \lfloor \frac{t}{2} \rfloor \leq \lfloor \frac{n}{2} \rfloor$ and consider the coloring \tilde{c} of $[m]$ induced by the coloring \hat{c} of the even integers in $[t]$. The coloring \tilde{c} uses at least $r - 2$ colors and has with no rainbow 3-AP, so $\text{aw}([m], 3) - 1 = (r - 2) + 1 \leq \text{aw}([m], 3)$. \square

Proposition 2.19. *Let m, n , and ℓ be positive integers. If $m < n < 2^\ell(m + 1)$, then $\text{aw}([n], 3) \leq \text{aw}([m], 3) + \ell$.*

Proof. Suppose not. Then there exists $m, \ell \geq 1$ and n with $m < n < 2^\ell(m + 1)$ such that there is a coloring c on $[n]$ using exactly $r = \text{aw}([m], 3) + \ell$ colors that does not have a rainbow 3-AP. For $i \in [r]$, let $b_i \in [n]$ be the least x such that the induced coloring on $[x]$ has exactly i colors. Since $r - \ell = \text{aw}([m], 3)$, we must have $b_{r-\ell} \geq m + 1$, since otherwise the induced coloring on $[m]$ contains at least $\text{aw}([m], 3)$ colors, which is impossible. Thus by Lemma 2.5, $n \geq b_r \geq 2^\ell b_{r-\ell} \geq 2^\ell(m + 1)$, which contradicts our assumption on n . \square

Corollary 2.20. $\text{aw}([n], 3) = 7$ for $64 \leq n \leq 80$.

Proof. Since $\text{aw}([m], 3) = 6$ for $22 \leq m \leq 26$, and $3 \cdot 22 - 2 = 64$ and $3 \cdot 26 + 2 = 80$, we see that $\text{aw}([n], 3) \geq 7$, by Proposition 2.2. Since $27 < 64 \leq n \leq 80 < 112 = 4 \cdot 28$, we have $\text{aw}([n], 3) \leq \text{aw}([27], 3) + 2 = 5 + 2 = 7$ by Proposition 2.19 and Remark 2.1. \square

Corollary 2.21. $\text{aw}([n], 3) = 7$ for $82 \leq n \leq 111$.

Proof. Since $27 < 82 \leq n \leq 111 < 112 = 4 \cdot 28$, we have $\text{aw}([n], 3) \leq \text{aw}([27], 3) + 2 = 5 + 2 = 7$ by Proposition 2.19 and Remark 2.1. Also, since $3^4 = 81 < n \leq 111 < 243 = 3^5$, we have $4 < \log_3 n \leq 5$, so that $\text{aw}([n], 3) \geq \lceil \log_3 n \rceil + 2 = 5 + 2 = 7$ by Lemma 2.3. \square

Corollary 2.22. $\text{aw}([n], 3) = 8$ for $190 \leq n \leq 235$.

Proof. Since $\text{aw}([m], 3) = 7$ for $64 \leq m \leq 80$, and $3 \cdot 64 - 2 = 190$ and $3 \cdot 80 + 2 = 242$, we see that $\text{aw}([n], 3) \geq 8$ for $190 \leq n \leq 242$, by Proposition 2.2. For $58 < n < 236 = 2^2 \cdot (58 + 1)$, we see that $\text{aw}([n], 3) \leq \text{aw}([58], 3) + 2 = 6 + 2 = 8$, by Proposition 2.19 and Remark 2.1. \square

Finally we combine the upper and lower bounds.

Proposition 2.23. *If $3^u < n < 2 \cdot 3^u + 2$, then $u + 3 \leq \text{aw}([n], 3) \leq \text{aw}([3^u], 3) + 1$. If $2 \cdot 3^u + 1 < n < 4 \cdot 3^u + 4$, then $u + 3 \leq \text{aw}([n], 3) \leq \text{aw}([3^u], 3) + 2$.*

Proof. The lower bounds follow immediately from Lemma 2.3, and the first upper bound follows immediately from Proposition 2.19. For the second, apply Proposition 2.19 with $m = 2 \cdot 3^u + 1$ and $\ell = 1$ to obtain $\text{aw}([n], 3) \leq \text{aw}([m], 3) + 1$ and since $3^u < m < 2 \cdot 3^u + 2$, $\text{aw}([m], 3) \leq \text{aw}([3^u], 3) + 1$. \square

3. $\text{aw}(\mathbb{Z}_n, k)$

In this section we establish properties of $\text{aw}(\mathbb{Z}_n, k)$. Sections 3.1 and 3.2 establish our main results for $\text{aw}(\mathbb{Z}_n, 3)$ and $\text{aw}(\mathbb{Z}_n, k), k \geq 4$, respectively. Section 3.3 contains additional results.

Please note that for $x \in \mathbb{Z}$, we will also use x to denote the equivalence class $\{x + in : i \in \mathbb{Z}\}$ in \mathbb{Z}_n . Because arithmetic progressions may “wrap around” in the group \mathbb{Z}_n , we call attention to the fact that we consider only k -APs that include k distinct members of \mathbb{Z}_n . Naturally, one of our first questions about $\text{aw}(\mathbb{Z}_n, k)$ concerns its relationship with $\text{aw}([n], k)$. Theorem 3.3(a) below and Lemma 2.3 show that $\text{aw}(\mathbb{Z}_n, k)$ need not be asymptotic to $\text{aw}([n], k)$ for $k = 3$ and $n = 2^m$. However, we do have the simple bound $\text{aw}(\mathbb{Z}_n, k) \leq \text{aw}([n], k)$ (already stated in Remark 1.4).

3.1. Main results for $\text{aw}(\mathbb{Z}_n, 3)$

When we turn to the special case $k = 3$, many values of $\text{aw}(\mathbb{Z}_n, 3)$ can be computed, and new phenomena appear. Our main results in this case are described by Theorem 1.6, which we establish in this section.

Currently available computational data is given in Table 2; the row label displays the range of n for which the values of $\text{aw}(\mathbb{Z}_n, 3)$ are reported in that row, and the column heading is the ones digit within this range. This data led to the discovery of several results established in this section and is used to establish the second statement in Theorem 1.6 that concerns integers having all prime factors less than one hundred.

Many odd primes p have $\text{aw}(\mathbb{Z}_p, 3) = 3$ (see Table 2 below). However, there are several examples of odd primes p for which $\text{aw}(\mathbb{Z}_p, 3) = 4$. In Example 3.1 below we exhibit an explicit exact coloring that establishes $\text{aw}(\mathbb{Z}_{17}, 3) \geq 4$.

Example 3.1. Coloring the elements of \mathbb{Z}_{17} in order as

$$3 \ 1 \ 1 \ 2 \ 1 \ 2 \ 2 \ 2 \ 1 \ 1 \ 2 \ 2 \ 2 \ 1 \ 2 \ 1 \ 1$$

is an exact 3-coloring that does not contain a rainbow 3-AP. Computations establish that equality holds and so $\text{aw}(\mathbb{Z}_{17}, 3) = 4$.

Table 2: Computed values of $\text{aw}(\mathbb{Z}_n, 3)$ for $n = 3, \dots, 99$ (the row label gives the range of n and the column heading is the ones digit within this range)

	0	1	2	3	4	5	6	7	8	9
0–9				3	3	3	4	3	3	4
10–19	4	3	4	3	4	4	3	4	5	3
20–29	4	4	4	3	4	4	4	5	4	3
30–39	5	4	3	4	5	4	5	3	4	4
40–49	4	4	5	4	4	5	4	3	4	4
50–59	5	5	4	3	6	4	4	4	4	3
60–69	5	3	5	5	3	4	5	3	5	4
70–79	5	3	5	4	4	5	4	4	5	3
80–89	4	6	5	3	5	5	5	4	4	4
90–99	6	4	4	5	4	4	4	4	5	5

Definition 3.2. When dealing with a coloring c of \mathbb{Z}_{st} , the i^{th} residue class modulo s is $R_i := \{j \in \mathbb{Z}_{st} : j \equiv i \pmod{s}\}$ and the i^{th} residue palette modulo s is $P_i := \{c(\ell) : \ell \in R_i\}$. For a positive integer t , we call the elements of the two residue classes, R_0 and R_1 , modulo 2 in \mathbb{Z}_{2t} the *even numbers* and the *odd numbers*, respectively.

3.1.1. Consequences of results in Jungić et al. In this section we state two important results of Jungić et al. [8] and derive implications. These are used in the proof of Theorem 1.6. The next result is an equivalent form of Theorem 3.5 in that paper.

Theorem 3.3. [8, Theorem 3.5] *Let n be a positive integer. Then $\text{aw}(\mathbb{Z}_n, 3) = 3$ if and only if one of the following conditions is satisfied:*

- a) n is a power of 2,
- b) n is prime and 2 is a generator of the multiplicative group \mathbb{Z}_n^\times ,
- c) n is prime, $\frac{n-1}{2}$ is odd, and the order of 2 in \mathbb{Z}_n^\times is $\frac{n-1}{2}$.

Theorem 3.4. [8, Theorem 3.2] *Let n be an odd positive integer and q be the smallest prime factor of n . Then every 3-coloring of \mathbb{Z}_n in which every color class has at least $\frac{n}{q} + 1$ elements contains a rainbow 3-AP.*

A coloring c of \mathbb{Z}_n is an *extremal coloring* if c is an exact $(\text{aw}(\mathbb{Z}_n, 3) - 1)$ -coloring of \mathbb{Z}_n with no rainbow 3-AP. A coloring c of \mathbb{Z}_n is a *singleton coloring* if some color is used exactly once.

Proposition 3.5. *Let p be a prime positive integer. Then $3 \leq \text{aw}(\mathbb{Z}_p, 3) \leq 4$, and $\text{aw}(\mathbb{Z}_p, 3) = 4$ implies every extremal coloring of \mathbb{Z}_p is a singleton coloring.*

Proof. First we suppose $\text{aw}(\mathbb{Z}_p, 3) \geq 5$ and let c be an extremal coloring with $r = \text{aw}(\mathbb{Z}_p, 3) - 1 \geq 4$ colors. That is, c does not have a rainbow 3-AP. Hence, there is at least one color class with more than one element. We can define a 3-coloring \hat{c} by partitioning the color classes of c into three sets and defining the color classes of \hat{c} to be the unions of the color classes in the sets. Clearly \hat{c} is a 3-coloring of \mathbb{Z}_p that does not have a rainbow 3-AP. By Theorem 3.4, there exists a color class of \hat{c} with $< \frac{p}{3} + 1 = 2$ elements. This means that all but one of the color classes has a single element (and $r = 4$). Without loss of generality, let the singleton colors be in positions $0, x$, and y , with $0 < x < y < p$ (when viewed as integers rather than elements of \mathbb{Z}_p). In order to avoid the rainbow 3-AP in c consisting of $0, \frac{x}{2}, x$, x must be odd, and similarly y must be odd as well. But then $x, \frac{y-x}{2}, y$ is a rainbow 3-AP in c , contradicting $\text{aw}(\mathbb{Z}_p, 3) \geq 5$.

Next, suppose that $\text{aw}(\mathbb{Z}_p, 3) = 4$ and let c be an extremal coloring of $r = 3$ colors. Since c has no rainbow 3-AP, Theorem 3.4 gives that there is a color class with one element. That is, c must be a singleton coloring. \square

Since $\text{aw}(\mathbb{Z}_p, 3) = 3$ implies \mathbb{Z}_p has the singleton extremal coloring $c(0) = 1$ and $c(i) = 2$ for every $i \not\equiv 0 \pmod{p}$, the next corollary is immediate.

Corollary 3.6. *Every prime p has a singleton extremal coloring of \mathbb{Z}_p .*

Since $\text{aw}(\mathbb{Z}_{2^m}, 3) = 3$, there are infinitely many values of n for which $\text{aw}(\mathbb{Z}_n, 3) = 3$. As stated in Theorem 1.6, $\text{aw}(\mathbb{Z}_n, 3)$ can be made arbitrarily large and computed from the values of $\text{aw}(\mathbb{Z}_p, 3)$ for the prime factors p of n . For primes p , $\text{aw}(\mathbb{Z}_p, 3) > 3$ seems rare from the data in Table 2. However, it follows from Theorem 3.3 that there are infinitely many primes p such that $\text{aw}(\mathbb{Z}_p, 3) = 4$:

Corollary 3.7. *If p is a prime and $p \equiv 1 \pmod{8}$, then $\text{aw}(\mathbb{Z}_p, 3) = 4$. There are infinitely many such primes.*

Proof. Since $p \equiv 1 \pmod{8}$, $\frac{p-1}{2}$ is even. Also, 2 must be a square in \mathbb{Z}_p^\times , which implies it is not a generator of \mathbb{Z}_p^\times . So by Theorem 3.3, $\text{aw}(\mathbb{Z}_p, 3) \neq 3$. Then by Proposition 3.5, $\text{aw}(\mathbb{Z}_p, 3) = 4$. By Dirichlet's Theorem there are infinitely many primes $p \equiv 1 \pmod{8}$. \square

3.1.2. Proof of Theorem 1.6 In this section we present a series of results that lead to equivalent lower and upper bounds on $\text{aw}(\mathbb{Z}_n, 3)$ in terms of the prime factorization of n , establishing Theorem 1.6.

The next result gives our main recursive upper bound for $\text{aw}(\mathbb{Z}_n, 3)$.

Proposition 3.8. *Suppose s is odd, and either t is odd or $t = 2^m$. Then*

$$\text{aw}(\mathbb{Z}_{st}, 3) \leq \text{aw}(\mathbb{Z}_t, 3) + \text{aw}(\mathbb{Z}_s, 3) - 2.$$

Proposition 3.8 is established by Propositions 3.10 (t odd) and 3.13 ($t = 2^m$) below, after the proofs of necessary preliminaries.

Proposition 3.9. *Let s be an odd positive integer. Suppose c is a coloring of \mathbb{Z}_{st} that does not have a rainbow 3-AP. Let R_0, R_1, \dots, R_{s-1} be the residue classes modulo s in \mathbb{Z}_{st} with associated residue palettes P_i . Let m be an index such that $|P_m| \geq |P_i|$ for all i . Then $|P_i \setminus P_m| \leq 1$ for all i .*

Proof. For arbitrary nonnegative integers h and j , we show that $|P_{h+j} \setminus P_h| \geq 2$ implies $P_h = P_{h+2j}$. Assume $|P_{h+j} \setminus P_h| \geq 2$. Suppose first that $P_{h+2j} \setminus P_h$ is not empty and $z \in P_{h+2j} \setminus P_h$. Since $|P_{h+j} \setminus P_h| \geq 2$, we can pick some $y \in P_{h+j} \setminus P_h$ other than z . Let $\ell_y, \ell_z \in \mathbb{Z}_{st}$ with $\ell_y \in R_{h+j}, \ell_z \in R_{h+2j}$ and $c(\ell_y) = y, c(\ell_z) = z$. Define $\ell_x := 2\ell_y - \ell_z \in R_h$, so $x := c(\ell_x)$ is a color in P_h . By the choice of $y, y \neq z; z \neq x$ since $z \in P_{h+2j} \setminus P_h$ and $x \in P_h; x \neq y$ since $y \in P_{h+j} \setminus P_h$ and $x \in P_h$. Thus ℓ_x, ℓ_y, ℓ_z is a rainbow 3-AP, a contradiction. Therefore we conclude that $P_{h+2j} \subseteq P_h$. With this condition, we consider the case $P_h \setminus P_{h+2j}$ is not empty. Let $x \in P_h \setminus P_{h+2j}$. Similarly, it is possible to pick $y \in P_{h+j} \setminus P_h$. Let $\ell_x, \ell_y \in \mathbb{Z}_{st}$ with $\ell_x \in R_h, \ell_y \in R_{h+j}$, and $c(\ell_x) = x, c(\ell_y) = y$. Thus $\ell_z := 2\ell_y - \ell_x \in R_{h+2j}$ and so $z := c(\ell_z)$ is a color in P_{h+2j} . Again, $x \neq y$ by the choice of $y; x \neq z$ since $x \in P_h \setminus P_{h+2j}$ and $z \in P_{h+2j}; y \neq z$ since $y \in P_{h+j} \setminus P_h$ and $z \in P_{h+2j} \subseteq P_h$. Since we again have a contradiction, $P_h = P_{h+2j}$.

Next we show that $|P_{h+j} \setminus P_h| \geq 2$ implies $|P_h \setminus P_{h+j}| \leq 1$. Suppose $|P_{h+j} \setminus P_h| \geq 2$ and $|P_h \setminus P_{h+j}| \geq 2$, and then show this leads to a contradiction. By the result just established, $P_h = P_{h+2j}$. Since $|P_{h+2j} \setminus P_{h+j}| = |P_h \setminus P_{h+j}| \geq 2$, $P_{h+j} = P_{h+3j}$. Therefore $P_h = P_{h+qj}$ whenever q is even and $P_{h+j} = P_{h+qj}$ whenever q is odd. Since s is odd, the order d of j in \mathbb{Z}_s is also an odd number. That means $P_h = P_{h+dj} = P_{h+j}$, which is a contradiction.

Finally, since $|P_m|$ is chosen to be maximum, $|P_m \setminus P_j| \geq 2$ whenever $|P_j \setminus P_m| \geq 2$, which is impossible. Hence $|P_j \setminus P_m| \leq 1$. \square

Proposition 3.10. *Suppose s and t are both odd. Then $\text{aw}(\mathbb{Z}_{st}, 3) \leq \text{aw}(\mathbb{Z}_s, 3) + \text{aw}(\mathbb{Z}_t, 3) - 2$.*

Proof. Let c be a coloring of \mathbb{Z}_{st} that does not have a rainbow 3-AP. Consider the residue classes and residue palettes modulo s and without loss of generality assume $|P_0| \geq |P_i|$ for all i . We claim that

$$(1) \quad \left| \bigcup_{i=0}^{s-1} P_i \right| \leq (\text{aw}(\mathbb{Z}_s, 3) - 1) + (\text{aw}(\mathbb{Z}_t, 3) - 1) - 1.$$

The proof is by contradiction. Assume that (1) is false, i.e., assume

$$(2) \quad \left| \bigcup_{i=0}^{s-1} P_i \right| \geq (\text{aw}(\mathbb{Z}_s, 3) - 1) + (\text{aw}(\mathbb{Z}_t, 3) - 1)$$

and define a coloring \hat{c} of $\mathbb{Z}_s = \{0, 1, \dots, s - 1\}$ in the following way: Let α be a color not in $\bigcup_{i=1}^{s-1} (P_i \setminus P_0)$ and define

$$\hat{c}(i) = \begin{cases} \alpha & \text{if } P_i \subseteq P_0, \\ \text{the element of } P_i \setminus P_0 & \text{if } P_i \not\subseteq P_0. \end{cases}$$

Note that Proposition 3.9 implies that the required element in $P_i \setminus P_0$ is unique, so this coloring is well-defined. Since c does not have a rainbow 3-AP, we know $|P_0| \leq \text{aw}(\mathbb{Z}_t, 3) - 1$ so

$$\begin{aligned} \left| \bigcup_{i=1}^{s-1} (P_i \setminus P_0) \right| &\geq \left| \bigcup_{i=0}^{s-1} P_i \right| - (\text{aw}(\mathbb{Z}_t, 3) - 1) \\ &\geq (\text{aw}(\mathbb{Z}_s, 3) - 1) + (\text{aw}(\mathbb{Z}_t, 3) - 1) - (\text{aw}(\mathbb{Z}_t, 3) - 1) \\ &= \text{aw}(\mathbb{Z}_s, 3) - 1. \end{aligned}$$

Note that every color that is not in P_0 , together with α , is used in \hat{c} , so \hat{c} uses at least $\text{aw}(\mathbb{Z}_s, 3)$ colors. Thus a rainbow 3-AP exists in \hat{c} .

We show that a rainbow 3-AP in \hat{c} implies a rainbow 3-AP in c , providing a contradiction and establishing that (1) is true. Let x, y, z be a rainbow 3-AP in \mathbb{Z}_s using coloring \hat{c} , with $y = x + d \pmod s$ and $z = x + 2d \pmod s$. Since x, y, z are rainbow, $\hat{c}(u) \neq \hat{c}(v)$ for all distinct $u, v \in \{x, y, z\}$, and so at most one $u \in \{x, y, z\}$ has $\hat{c}(u) = \alpha$. Note that by definition $\hat{c}(u) \in P_u$ or $\hat{c}(u) = \alpha$ for $u \in \{x, y, z\}$.

Case 1: $\hat{c}(z) \neq \alpha$ and $\hat{c}(y) \neq \alpha$. Then we can find g_2 and g_3 such that $c(g_2s + y) = \hat{c}(y)$ and $c(g_3s + z) = \hat{c}(z)$. Define $d' := (g_3s + z) - (g_2s + y)$. Then

$$\begin{aligned} (g_3s + z) - d' &= (g_2s + y) \equiv y \pmod s \\ (g_3s + z) - 2d' &= 2g_2s + 2y - g_3s - z \equiv 2y - z \\ &\equiv 2(x + d) - (x + 2d) \equiv x \pmod s. \end{aligned}$$

With $\ell := (g_3s + z) - 2d'$, consider the 3-AP $\{\ell, (g_3s + z) - d', (g_3s + z)\}$. We show that this 3-AP is rainbow: Note that $\hat{c}(y) \notin P_0$ and $\hat{c}(z) \notin P_0$.

If $\hat{c}(x) = \alpha$, then $P_x \subseteq P_0$, so $\ell \in R_x$ implies $c(\ell) \neq \hat{c}(y) = c(g_2s + y)$ and $c(\ell) \neq \hat{c}(z) = c(g_3s + z)$. If $\hat{c}(x) \neq \alpha$, then $\hat{c}(x)$ is the unique element of $P_x \setminus P_0$ and $\hat{c}(x) \neq \hat{c}(y), \hat{c}(z)$, so $\ell \in R_x$ implies $c(\ell) \neq \hat{c}(y)$ and $c(\ell) \neq \hat{c}(z)$. Thus c has a rainbow 3-AP, contradicting our assumption (2). The case where both $\hat{c}(x) \neq \alpha$ and $\hat{c}(y) \neq \alpha$ is symmetric to Case 1. So only Case 2 remains.

Case 2: $\hat{c}(y) = \alpha$. Then $\hat{c}(x) \in P_x \setminus P_0$ and $\hat{c}(z) \in P_z \setminus P_0$, so we can find g_1 and g_3 such that $c(g_1s + x) = \hat{c}(x)$ and $c(g_3s + z) = \hat{c}(z)$, and define $e := (g_3s + z) - (g_1s + x)$. Since st is odd, 2 is invertible in \mathbb{Z}_{st} and there exists d' such that $2d' \equiv e \pmod{st}$, and hence $2d' \equiv e \pmod{s}$. Also, $e \equiv z - x \equiv 2d \pmod{s}$. Thus $2d \equiv 2d' \pmod{s}$ and so $d \equiv d' \pmod{s}$ since s is odd. Then

$$\begin{aligned} (g_1s + x) + 2d' &\equiv (g_1s + x) + ((g_3s + z) - (g_1s + x)) \\ &\equiv g_3s + z \equiv z \pmod{s} \\ (g_1s + x) + d' &\equiv x + d \equiv y \pmod{s}. \end{aligned}$$

With $\ell := (g_1s + x) + d'$, the 3-AP $\{(g_1s + x), \ell, (g_1s + x) + 2d'\}$ is rainbow, because $\ell \in R_y$ and $P_y \subseteq P_0$, so $c(\ell) \neq \hat{c}(x) = c(g_1s + x)$ and $c(\ell) \neq \hat{c}(z) = c(g_3s + z)$.

In all cases, c has a rainbow 3-AP, contradicting our assumption (2). □

Next we prove two technical propositions used in the proof of Proposition 3.13, Propositions 3.11 and 3.12.

Proposition 3.11. *Let m and s be positive integers with s odd. Suppose c is a coloring of $\mathbb{Z}_{2^m s}$ using at least $r := \text{aw}(\mathbb{Z}_s, 3) + 1$ colors that does not have a rainbow 3-AP. Let R_0, R_1, \dots, R_{s-1} be the residue classes modulo s in $\mathbb{Z}_{2^m s}$ with associated residue palettes P_i . Then $1 \leq |P_i| \leq 2$ for $i = 0, \dots, s - 1$, and all palettes P_i of size two share a common color.*

Proof. Since P_i is nonempty, $1 \leq |P_i|$. Observe that the coloring c of R_i induces a coloring on \mathbb{Z}_{2^m} that uses only the colors in P_i and cannot contain a rainbow 3-AP. Thus $|P_i| \leq 2$ by Theorem 3.3, establishing the first statement.

By Proposition 3.9, each pair of residue palettes of size two must intersect. Suppose the palettes of size two do not all intersect in a common color. Then there are exactly three colors α, β, γ that are used by all the palettes of size two, and there are exactly three distinct palettes of size two, each consisting of two of these three colors. We show this configuration leads to a contradiction.

Create a coloring \hat{c} of \mathbb{Z}_s by the following method:

$$\hat{c}(i) = \begin{cases} c(i) & \text{if } |P_i| = 1, \\ \beta & \text{if } P_i = \{\alpha, \beta\}, \\ \text{the unique element of } P_i \setminus \{\gamma\} & \text{if } |P_i| = 2 \text{ and } \gamma \in P_i. \end{cases}$$

Observe that \hat{c} uses r colors if there exists i such that $P_i = \{\gamma\}$ and $r - 1 = \text{aw}(\mathbb{Z}_s, 3)$ colors otherwise, so in either case \hat{c} must have a rainbow 3-AP. Suppose that $\{x, y, z\}$ is a rainbow 3-AP for the coloring \hat{c} of \mathbb{Z}_s . Since $\hat{c}(x)$, $\hat{c}(y)$, and $\hat{c}(z)$ are distinct colors, at least one of the palettes P_x, P_y, P_z contains only one color. Consider the sizes of P_x, P_y , and P_z .

Case 1: $|P_z| = 1$. Observe that $\hat{c}(i)$ is always an element in P_i by our definition of $\hat{c}(i)$. Pick $n_1 \in R_x$ and $n_2 \in R_y$ such that $c(n_1) = \hat{c}(x)$ and $c(n_2) = \hat{c}(y)$. Thus $n_3 := 2n_2 - n_1$ is an element in R_z and so $c(n_3) = \hat{c}(z)$. Since $\hat{c}(x), \hat{c}(y), \hat{c}(z)$ are all distinct, $\{n_1, n_2, n_3\}$ is a rainbow 3-AP. The case $|P_x| = 1$ is symmetric.

Case 2: $|P_x| = |P_z| = 2$ and $|P_y| = 1$. Since $\hat{c}(x) \neq \hat{c}(z)$, it must be that $\{\hat{c}(x), \hat{c}(z)\} = \{\alpha, \beta\}$. Without loss of generality, we assume that $\hat{c}(x) = \beta$ and $\hat{c}(z) = \alpha$. By the definition of \hat{c} , $P_z = \{\alpha, \gamma\}$. Then P_x is one of $\{\alpha, \beta\}$ or $\{\beta, \gamma\}$. If $\hat{c}(y) \notin P_x \cup P_z$, then any 3-AP $\{n_1, n_2, n_3\}$ where $n_1 \in R_x$ and $c(n_1) = \beta$, $n_2 \in R_y$, and $n_3 \in R_z$ is a rainbow 3-AP in the original coloring. Thus, $\hat{c}(y) \in P_x \cup P_z \subseteq \{\alpha, \beta, \gamma\}$, but $\hat{c}(y) \notin \{\alpha, \beta\} = \{\hat{c}(x), \hat{c}(z)\}$, so $\hat{c}(y) = \gamma$. Note that this implies \hat{c} uses all r colors.

Since this is the final case, and all previous cases led to contradictions, every rainbow 3-AP in \mathbb{Z}_s given by the coloring \hat{c} must be of the form $\{x, y, z\}$ where $\{\hat{c}(x), \hat{c}(z)\} = \{\alpha, \beta\}$ and $\hat{c}(y) = \gamma$. Create a new coloring

$$c' \text{ of } \mathbb{Z}_s \text{ where } c'(i) = \begin{cases} c(i) & \text{if } \hat{c}(i) \neq \gamma, \\ \beta & \text{if } \hat{c}(i) = \gamma. \end{cases}$$

Now, every 3-AP that was previously non-rainbow in \hat{c} remains non-rainbow in c' and the rainbow 3-APs (which necessarily used the colors α, β , and γ) are no longer rainbow. Thus, this coloring c' does not have a rainbow 3-AP, but c' uses $r - 1 = \text{aw}(\mathbb{Z}_s, 3)$ colors, a contradiction.

The above cases show that having no common color among the palettes of size two leads to a contradiction. Therefore, all of the residue palettes of size two share a common color. \square

Proposition 3.12. *Suppose c is a coloring of \mathbb{Z}_{2t} ($t \geq 1$) that does not have a rainbow 3-AP. Let A and B denote the residue palettes modulo 2 in \mathbb{Z}_{2t}*

associated with the even and odd numbers, respectively. Then $|A \setminus B| \leq 1$ and $|B \setminus A| \leq 1$.

Proof. It suffices to show that $|A \setminus B| \leq 1$ for every such coloring c because if $|B \setminus A| \geq 2$, then the coloring defined by the rotation $c'(x) := c(x + 1)$ has the roles of A and B reversed. Suppose not, so there exist two colors α, γ that appear only in A . Let $n_1 = 2m_1$ and $n_3 = 2m_3$ be even elements such that $c(n_1) = \alpha$ and $c(n_3) = \gamma$. We can select m_1 and m_3 such that $0 \leq m_1 < m_3 < t$. Performing arithmetic in the integers, we can choose $m_3 - m_1$ to be minimum with respect to the fact that the set of colors $\{c(2m_1), c(2m_3)\}$ is $\{\alpha, \gamma\}$. Let $n_2 = m_1 + m_3$ and observe that $\{n_1, n_2, n_3\}$ is a 3-AP and hence is not rainbow. Therefore, n_2 must have the color α or γ and thus is even. However, this implies that $n_2 = 2m_2$ and $m_1 < m_2 < m_3$, while one of the sets of colors $\{c(2m_1), c(2m_2)\}$ or $\{c(2m_2), c(2m_3)\}$ is $\{\alpha, \gamma\}$, so one of the pairs (m_1, m_2) , (m_2, m_3) violates our extremal choice. \square

Proposition 3.13. *Let m and s be positive integers with s odd. Then*

$$\text{aw}(\mathbb{Z}_{2^m s}, 3) \leq \text{aw}(\mathbb{Z}_s, 3) + 1.$$

Proof. The result is immediate for $s = 1$ because Theorem 3.3 gives that $\text{aw}(\mathbb{Z}_{2^m}, 3) = 3$ and because $\text{aw}(\mathbb{Z}_s, 3) = s + 1$ for $s < 3$, so assume $s \geq 3$. We proceed by induction on m . Suppose c is an exact r -coloring of $\mathbb{Z}_{2^m s}$ with $r = \text{aw}(\mathbb{Z}_s, 3) + 1$ that does not have a rainbow 3-AP. Let A and B denote the residue palettes of the even and odd numbers, respectively. By Proposition 3.12, $|A \setminus B| \leq 1$ and $|B \setminus A| \leq 1$, so $|B| \geq r - 1$ and $|A| \geq r - 1$. The base case $m = 1$ is then immediate, because the coloring of the even numbers of \mathbb{Z}_{2s} induces a coloring of \mathbb{Z}_s , so a rainbow 3-AP necessarily exists, producing a contradiction.

Now consider $m > 1$. As usual $R_i, i = 0, \dots, s - 1$, are the residue classes modulo s of $\mathbb{Z}_{2^m s}$ and $P_i, i = 0, \dots, s - 1$, are the residue palettes. Recall that by Proposition 3.11, $1 \leq |P_i| \leq 2$ for all i . For $0 \leq i \leq s - 1$, let $A_i = P_i \cap A$ be the colors appearing on the even numbers in R_i , and let $B_i = P_i \cap B$ be the colors appearing on the odd numbers in R_i . Thus, $P_i = A_i \cup B_i$, $A = \bigcup_{i=0}^{s-1} A_i$, and $B = \bigcup_{i=0}^{s-1} B_i$. We claim that $|A| = |B| = r - 1$. To see this, observe that the even elements induce a coloring of $\mathbb{Z}_{2^{m-1}s}$, so if $|A| = r$, then a rainbow 3-AP necessarily exists, since $r \geq \text{aw}(\mathbb{Z}_{2^{m-1}s}, 3)$ by the induction hypothesis. Thus $|A| \leq r - 1$, and so $|A| = r - 1$. The proof that $|B| = r - 1$ is analogous.

Since $|A| = |B| = r - 1$, there exist colors α, β such that $A \setminus B = \{\alpha\}$ and $B \setminus A = \{\beta\}$. Assume $\alpha \in A_u$ and $\beta \in B_v$. Let $j = v - u$, hence

$\beta \in B_{u+j} = B_v$. Since there is no rainbow 3-AP, $u + 2j$ must have a color in palette A , $\alpha \in A_{u+2j}$, which then implies $\beta \in B_{u+3j} = B_{v+2j}$. Iterating this process gives that $\alpha \in A_{u+2\ell j}$ and $\beta \in B_{v+2\ell j}$ for all $\ell \geq 0$. Since s is odd, we have that for all $q \geq 0$, A_{u+qj} is of the form $A_{u+2\ell j}$ for some ℓ and similarly, every $B_{u+qj} = B_{v+(q-1)j}$ is of the form $B_{v+2\ell j}$ for some ℓ . Therefore, $P_{u+qj} = \{\alpha, \beta\}$ for all $q \geq 0$. By Proposition 3.11, there is a common color for palettes of size two, and thus one of α or β is this common color. Without loss of generality, assume that α is the common color for all palettes of size 2. This implies that $|B_i| = 1$ for all $0 \leq i \leq s-1$. Hence, defining $\hat{c}(i)$ to be the unique color in B_i defines an exact $(r-1)$ -coloring of \mathbb{Z}_s that avoids rainbow 3-APs. However, $r-1 = \text{aw}(\mathbb{Z}_s, 3)$, a contradiction. \square

Proposition 3.8 is now established from Proposition 3.10 and Proposition 3.13. We now turn our attention to establishing the lower bound.

Proposition 3.14. *Suppose s is odd and \mathbb{Z}_s has a singleton extremal coloring. Then for $t \geq 2$,*

$$\text{aw}(\mathbb{Z}_{st}, 3) \geq \text{aw}(\mathbb{Z}_t, 3) + \text{aw}(\mathbb{Z}_s, 3) - 2.$$

Proof. Let c_s be a singleton extremal coloring of \mathbb{Z}_s . Note that we can shift c_s so that $c_s(0)$ is the color that is used exactly once. Choose a coloring c_t of \mathbb{Z}_t using $\text{aw}(\mathbb{Z}_t, 3) - 1$ colors not used by c_s that does not have a rainbow 3-AP. Let R_0, R_1, \dots, R_{s-1} be the residue classes modulo s in \mathbb{Z}_{st} . Define a coloring \hat{c} of \mathbb{Z}_{st} as follows: For $i = 1, \dots, s-1$ and $\ell \in R_i$, $\hat{c}(\ell) := c_s(i)$, and for $0 \leq j \leq t-1$, $\hat{c}(js) := c_t(j)$. Notice that we now have an exact $\text{aw}(\mathbb{Z}_s, 3) - 2 + \text{aw}(\mathbb{Z}_t, 3) - 1$ coloring of \mathbb{Z}_{st} because we have removed color $c_s(0)$. Clearly, if a 3-AP is within some residue class it is not rainbow. Because s is odd, $d \not\equiv 0 \pmod{s}$ implies $2d \not\equiv 0 \pmod{s}$ and $2d \not\equiv d \pmod{s}$, so a 3-AP that is not entirely within one residue class has elements in three different residue classes. But a rainbow 3-AP with elements in three different residue classes would imply a rainbow 3-AP in c_s , which does not exist. So we have found a coloring of \mathbb{Z}_{st} using $\text{aw}(\mathbb{Z}_t, 3) + \text{aw}(\mathbb{Z}_s, 3) - 3$ colors that does not have a rainbow 3-AP. Thus $\text{aw}(\mathbb{Z}_{st}, 3) \geq \text{aw}(\mathbb{Z}_t, 3) + \text{aw}(\mathbb{Z}_s, 3) - 2$. \square

Corollary 3.15. *For an integer $n \geq 2$,*

$$\text{aw}(\mathbb{Z}_n, 3) = 2 + f_2(n) + f_3(n) + 2f_4(n).$$

Proof. By Proposition 3.5, every odd prime factor p has $3 \leq \text{aw}(\mathbb{Z}_p, 3) \leq 4$. Apply Proposition 3.8, removing one odd prime s at a time and observing

that for $\text{aw}(\mathbb{Z}_s, 3) = 3$, $\text{aw}(\mathbb{Z}_s, 3) - 2$ adds one to the total, whereas for $\text{aw}(\mathbb{Z}_s, 3) = 4$, $\text{aw}(\mathbb{Z}_s, 3) - 2$ adds two to the total. Thus $\text{aw}(\mathbb{Z}_n, 3) \leq 2 + f_2(n) + f_3(n) + 2f_4(n)$. For the reverse inequality, suppose p is an odd prime. Then every extremal coloring of \mathbb{Z}_p is a singleton coloring by Proposition 3.5. So we can apply Proposition 3.14 to remove one odd prime at a time to show that $\text{aw}(\mathbb{Z}_n, 3) = 2 + f_2(n) + f_3(n) + 2f_4(n)$. \square

Remark 3.16. The constructive proof of Proposition 3.14 gives a singleton extremal coloring of \mathbb{Z}_n from the singleton extremal colorings of the prime factors of n . Since \mathbb{Z}_{2^m} has the singleton extremal coloring $c(0) = 1$ and $c(i) = 2$ for every $i \not\equiv 0 \pmod{2^m}$, every positive integer has a singleton extremal coloring.

Proposition 3.17. *For all primes $p < 100$, $\text{aw}(\mathbb{Z}_p, 3) = 3$ if $p \notin Q_4 := \{17, 31, 41, 43, 73, 89, 97\}$ and $\text{aw}(\mathbb{Z}_p, 3) = 4$ if $p \in Q_4$.*

Proof. The statement that for any prime $p < 100$, $\text{aw}(\mathbb{Z}_p, 3) = 3$ if $p \notin Q_4$ and $\text{aw}(\mathbb{Z}_p, 3) = 4$ if $p \in Q_4$ has been verified computationally (see Table 2). \square

The next example illustrates the use of Corollary 3.15 to compute $\text{aw}(\mathbb{Z}_n, 3)$ in the case that every prime factor of n is less than 100.

Example 3.18. Let $n = 14, 582, 937, 583, 067, 568$. Since $n = 2^4 \cdot 3 \cdot 11^2 \cdot 13 \cdot 17^2 \cdot 53^3 \cdot 67^2$, $\text{aw}(\mathbb{Z}_n, 3) = 3 + 9 + 2 \cdot 2 = 16$.

3.2. Main results for $\text{aw}(\mathbb{Z}_n, k)$, $k \geq 4$

In this section, we specialize to the case where $k \geq 4$ and prove Theorem 1.7. Corollary 3.19 below, which follows from Corollary 2.14 and Remark 1.4, gives us $ne^{-\log \log \log n - \omega(1)}$ as an upper bound for $\text{aw}(\mathbb{Z}_n, k)$.

Corollary 3.19. *For every fixed positive integer k , $\text{aw}(\mathbb{Z}_n, k) = o\left(\frac{n}{\log \log n}\right)$.*

Our lower bound for $\text{aw}(\mathbb{Z}_n, k)$ when $n > 12$ is presented in Lemma 3.20.

Lemma 3.20. *There exists an absolute constant $b > 0$ such that for all $c > 3$, $\frac{n}{c} \geq 4$ and $k \geq 4$,*

$$\text{aw}(\mathbb{Z}_n, k) > \left(\frac{n}{c}\right) e^{-b\sqrt{\log(n/c)}} = ne^{-b\sqrt{\log(n/c)} - \log c} = n^{1-o(1)}.$$

Lemma 3.20 is proven using the Behrend construction from Section 2.2 and using Proposition 3.21 below. The Behrend construction in the integers $\{1, \dots, m\}$ has no punctured 4-AP and size $me^{-b\sqrt{\log m}}$ for some absolute constant b .

Proposition 3.21. *Let $c > 3$ be a real number, and let $\lfloor \frac{n}{c} \rfloor$ denote the first $\lfloor \frac{n}{c} \rfloor$ consecutive residues in \mathbb{Z}_n . Suppose $S \subseteq \lfloor \frac{n}{c} \rfloor$ does not contain any punctured 4-APs. Then $\text{aw}(\mathbb{Z}_n, k) > |S| + 1$ for all $k \geq 4$.*

Proof. Color each member of S a distinct color, and color each member of $\mathbb{Z}_n \setminus S$ with a new color called zero. Each $i \in \mathbb{Z}_n$ with $\frac{n}{c} < i < n$ will be colored zero. If $K = \{a_1, a_2, a_3, a_4\}$ is a rainbow 4-AP in \mathbb{Z}_n , then at most one element of K is not in S . Without a loss of generality, assume K is ordered as a_1, a_2, a_3, a_4 and $a_3, a_4 \in S$. Then there exists $d \in \mathbb{Z}$ such that $d \equiv a_4 - a_3 \pmod{n}$ and $|d| \leq \frac{n}{c}$.

Suppose $a_2 \in S$. Because $|d| \leq \frac{n}{c} < \frac{n}{2}$, we must have that a_2, a_3, a_4 is a 3-AP in $\lfloor \frac{n}{c} \rfloor$. This contradicts the fact that S contains no punctured 4-APs, so we must have $a_2 \notin S$ and $a_1 \in S$. However, since $2|d| \leq \frac{2n}{c} < \frac{(c-1)n}{c}$, we must have that a_1, a_3, a_4 is a punctured 4-AP in $\lfloor \frac{n}{c} \rfloor$. This is a contradiction, so $a_1 \notin S$.

This means that K could not have been rainbow, so we have a $(|S| + 1)$ -coloring of \mathbb{Z}_n with no rainbow 4-APs. □

We use the bound for the Behrend construction in Lemma 2.8 to obtain the bounds for $\text{aw}(\mathbb{Z}_n, k)$, $k \geq 4$:

$$ne^{-b\sqrt{\log(n/c)} - \log c} < \text{aw}(\mathbb{Z}_n, k) \leq ne^{-\log \log \log n - \omega(1)}.$$

This completes the proof of Theorem 1.7.

3.3. Additional results for $\text{aw}(\mathbb{Z}_n, k)$

In this section, we present computed data for $\text{aw}(\mathbb{Z}_n, k)$, $k \geq 4$, establish the value of $\text{aw}(\mathbb{Z}_n, k)$ for $k = n, n - 1$, and $n - 2$, and present some examples that show some additional results fail to extend from $[n]$ to \mathbb{Z}_n . Table 3 below lists the computed values of $\text{aw}(\mathbb{Z}_n, k)$ for $k = 4, \dots, n$ in the row labeled n .

Next we examine $\text{aw}(\mathbb{Z}_n, k)$ for k close to n .

Proposition 3.22. *For positive n and k we have $\text{aw}(\mathbb{Z}_n, k) = n$ if and only if $k = n$.*

Proof. If $k = n$ the result is obvious. Now suppose that $k < n$ and consider an exact $(n - 1)$ -coloring of \mathbb{Z}_n . Then there are two numbers with the same color and all other numbers are colored distinctly. Suppose x and y are the the two numbers with the same color. Then $\{x + 1, \dots, x + k\}$ is a k -AP that does not contain x , and so is rainbow. Therefore $\text{aw}(\mathbb{Z}_n, k) \leq n - 1$. □

Table 3: Computed values of $\text{aw}(\mathbb{Z}_n, k)$ for $k \geq 4$

$n \setminus k$	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
4	4															
5	4	5														
6	5	5	6													
7	4	5	6	7												
8	6	6	7	7	8											
9	5	6	8	8	8	9										
10	6	8	8	8	9	9	10									
11	5	6	7	8	9	9	10	11								
12	8	9	10	10	11	11	11	11	12							
13	5	7	8	9	10	10	11	11	12	13						
14	6	8	10	12	12	12	12	12	13	13	14					
15	8	11	12	12	12	13	14	14	14	14	14	15				
16	8	10	10	11	14	14	14	14	15	15	15	15	16			
17	6	8	10	11	12	12	13	14	14	15	15	15	16	17		
18	8	10	13	14	14	16	16	16	17	17	17	17	17	17	18	
19	6	9	10	12	12	14	14	15	16	16	16	17	17	17	18	19

Corollary 3.23. For positive n , $\text{aw}(\mathbb{Z}_n, n - 1) = n - 1$.

A pattern can be observed in the values of $\text{aw}(\mathbb{Z}_n, n - 2)$, and this is established in Proposition 3.24.

Proposition 3.24. For positive $n \geq 5$, if n is prime then $\text{aw}(\mathbb{Z}_n, n - 2) = n - 2$; otherwise $\text{aw}(\mathbb{Z}_n, n - 2) = n - 1$.

Proof. We trivially have a lower bound of $n - 2$ for $\text{aw}(\mathbb{Z}_n, n - 2)$. First we assume n is prime. We claim that for any two distinct elements x and y there is an $(n - 2)$ -AP that misses x and y . To see this, simply form the n -AP with $a = x$ and $d = (y - x)$, this will cover all of \mathbb{Z}_n and now removing the first two terms leaves us with an $(n - 2)$ -AP that does not contain x or y . So suppose we have an exact $(n - 2)$ -coloring. Then either there is one color that occurs three times or two colors that each occur twice, and in either case all other colors occur exactly once. In either case we can choose two numbers to avoid and then the remaining $n - 2$ numbers are rainbow, but as just noted above the remaining $n - 2$ numbers are an arithmetic progression. Therefore every $(n - 2)$ -coloring contains a rainbow progression.

When n is not a prime, let p be the smallest prime divisor of n and consider the $(n - 2)$ -coloring formed by coloring $0, p$ and $2p$ monochromatically, with the remaining numbers all given distinct colors. This is an $(n - 2)$ -coloring (since $2p < n$ by assumption that $n \geq 5$). We claim this coloring has no rainbow $(n - 2)$ -AP (along with the upper bound of $n - 1$, this claim

establishes the result). Suppose that $K = \{a, a + d, \dots, a + (n - 3)d\}$ is a rainbow $(n - 2)$ -AP, so all the elements of K are distinct and K necessarily misses two of $0, p, 2p$. Since \mathbb{Z}_n cannot have a proper subgroup of order $n - 2$, extending K to a n -AP necessarily produces all elements of \mathbb{Z}_n and thus $\{a + (n - 2)d, a + (n - 1)d\} \subseteq \{0, p, 2p\}$. But then we have that p divides $d = ((a + (n - 1)d) - (a + (n - 2)d))$, showing that this arithmetic progression can have at most $\frac{n}{p} < n - 2$ terms, which is a contradiction. \square

Proposition 3.22 shows that the “if” direction of Theorem 2.16 ($k \geq \lceil \frac{n}{2} \rceil + 1$ implies $\text{aw}([n], k) = n$) does not extend to \mathbb{Z}_n . Example 3.25 below shows that the extension of Proposition 2.15 to \mathbb{Z}_n , which would assert that $\text{aw}(\mathbb{Z}_n, k) \leq \text{aw}(\mathbb{Z}_{n-1}, k) + 1$, is not true in general. There are counterexamples in both the cases $k = 3$ and $k \geq 4$.

Example 3.25. By Corollary 3.15, $\text{aw}(\mathbb{Z}_{30}, 3) = 5$, and $\text{aw}(\mathbb{Z}_{29}, 3) = 3$ (see Table 2 in Section 3.1). Furthermore, $\text{aw}(\mathbb{Z}_8, 4) = 6$ and $\text{aw}(\mathbb{Z}_7, 4) = 4$ (see Table 3).

Example 3.26 below shows that Theorem 2.17, which bounds the anti-van der Waerden number of a sum in terms of the anti-van der Waerden numbers of the summands, does not extend to \mathbb{Z}_n .

Example 3.26. According to our computed data (see Table 3),

$$\text{aw}(\mathbb{Z}_{12}, 4) = 8 > 4 + 4 - 1 = \text{aw}(\mathbb{Z}_5, 4) + \text{aw}(\mathbb{Z}_7, 4) - 1.$$

There are also examples for $k = 3$, such as $\text{aw}(\mathbb{Z}_{54}, 3) = 6 > 3 + 3 - 1 = \text{aw}(\mathbb{Z}_{47}, 3) + \text{aw}(\mathbb{Z}_7, 3) - 1$.

4. Computation

Many of the results we have proved in this paper were first conjectured from examination of data. In this section, we briefly discuss an efficient algorithm to find an exact r -coloring of $[n]$ or \mathbb{Z}_n that avoids a rainbow k -AP, if such a coloring exists. For the sake of brevity, we will focus on the case of coloring $[n]$ since this case has a few extra properties that the \mathbb{Z}_n case does not. Specifically, we have $[m] \subseteq [n]$ for all $m \leq n$ while \mathbb{Z}_n contains a copy of \mathbb{Z}_m if and only if m divides n .

Fix k, n , and r and assume that all values of $\text{aw}([m], k)$ have been computed for $k \leq m < n$. Let $c : [n] \rightarrow [r] \cup \{*\}$ be a function called a *partial r -coloring*, where every position i has color $c(i) \in [r]$ or $c(i) = *$ and i is *uncolored*. By starting with all positions uncolored, we recursively attempt

to extend a partial r -coloring c where the positions in $[i]$ are colored to an exact r -coloring c' that avoids rainbow k -APs. We branch at each recursive call for all possible choices of color for $c(i+1)$ such that no k -AP within $[i+1]$ is colored with k distinct colors. To guarantee that no chosen color creates a rainbow k -AP, we maintain a list of sets $D(j) \subseteq [r]$ that contain all of the possible colors for the position j . Specifically, assigning $c(j)$ to be any color in $[r] \setminus D(j)$ will immediately create a rainbow k -AP. Whenever a color is assigned to a position i , we consider a k -AP, X , whose second-to-last element is i . If the set $c(X) = \{c(i') : i' \in X - \max X\}$ contains $k-1$ distinct colors, we say that X is an *almost-rainbow k -AP* and the color for $\max X$ must be one of these $k-1$ colors. Therefore, we can update $D(\max X)$ to be $D(\max X) \cap c(X)$. For simplicity, we update $D(i)$ to be $\{c(i)\}$ when i is assigned the color $c(i)$.

We can also make a few small adjustments to greatly reduce the search space. First, we assume that the coloring c is lexicographically-minimum: for two colors $a, b \in [r]$ with $a < b$, we assume that the first position with color a appears before the first position with color b . Second, the domains $D(j)$ contain the possible colors for the positions that remain uncolored. If $\bigcup_{j \in [n]} D(j) \neq [r]$, then c cannot extend to an exact r -coloring. Finally, if the first i positions are all colored with the color 1, then for any extension of c to an exact r -coloring of $[n]$, the last $n-i+1$ positions form an exact r -coloring. Thus, if $\text{aw}([n-i+1], k) \leq r$, then it is impossible to extend c to an exact r -coloring of $[n]$ without creating a rainbow k -AP.

Our recursive algorithm is given as Algorithm 1 and is initialized by Algorithm 2. Similar algorithms are implemented for the case of r -coloring \mathbb{Z}_n . All source code and data are available online¹ including computed values of $\text{aw}([n], k)$ and $\text{aw}(\mathbb{Z}_n, k)$, extremal colorings, and reports of computation time.

5. Conjectures and open questions

We conclude by summarizing some open questions and conjectures, beginning with those related to $[n]$.

Uherka [13] observed that $\text{aw}([n], 3)$ is not a monotone function in n , as there are values of n where $\text{aw}([n], 3) = \text{aw}([n-1], 3) - 1$. Does this happen infinitely often? Are larger drops possible?

Conjecture 5.1. *For positive integers n and k , $\text{aw}([n], k) \geq \text{aw}([n-1], k) - 1$.*

¹All source code and data can be found at <https://github.com/derrickstolee/RainbowAPs>

Algorithm 1 FindColorings($k, r, n, \text{aw}, c, D, i$) – Find exact D -colorings on $[n]$ that avoid rainbow k -APs and extend the coloring c on $[i - 1]$. Assume $\text{aw}([m], k)$ is known for all $m < n$.

```

if  $i \equiv n$  then
  output  $c$ 
  return
else if  $\cup_{j \in [n]} D(j) \neq [r]$  then
  return // This coloring cannot extend to an exact  $r$ -coloring!
else if  $i > 2$  and  $\forall j < i, c(j) \equiv 1$  and  $\text{aw}([n - i + 2], k) \leq r$  then
  return // An exact  $r$ -coloring extending  $c$  induces an exact  $r$ -coloring on
   $\{i - 1, \dots, n\}$ .
end if
 $M \leftarrow \max\{c(j) : j < i\} \cup \{0\}$ 
// Attempt all colors in the domain  $D(i)$  that are at most  $M + 1$ .
for all  $a \in D(i) \cap [M + 1]$  do
   $c(i) \leftarrow a, \quad D(i) \leftarrow \{a\}$ 
  // Update all domains  $D'(t)$  when almost-rainbow  $k$ -APs exist.
   $D' \leftarrow D$ 
  for all  $d \in \{1, \dots, \lceil i/(k - 2) \rceil - 1\}$  do
     $A \leftarrow \emptyset$ 
    for all  $\ell \in \{0, \dots, k - 2\}$  do
       $t \leftarrow i - \ell \cdot d$ 
       $A \leftarrow A \cup \{c(t)\}$ 
    end for
    if  $|A| \equiv k - 1$  then
       $t \leftarrow i + d$ 
       $D'(t) \leftarrow D'(t) \cap A$ 
    end if
  end for
  call FindColorings( $k, r, n, \text{aw}, c, D', i + 1$ )
end for

```

Algorithm 2 FindColoring(k, r, n, aw) – Find exact r -colorings on $[n]$ that avoid rainbow k -APs.

```

for all  $i \in [n]$  do
   $c(i) \leftarrow *$ 
   $D(i) \leftarrow [r]$ 
end for
call FindColorings( $k, r, n, \text{aw}, c, D, 1$ )

```

Conjecture 1.2 states that the lower bound $\text{aw}([n], 3) \geq \lceil \log_3 n \rceil + 2$ is correct to within an additive constant. We further conjecture that the lower

bound in Lemma 2.3 is in fact the exact value when n is a power of three. It is true for the computed data available (see Remark 2.1).

Conjecture 5.2. *Let m be a nonnegative integer. Then $\text{aw}([3^m], 3) = m + 2$.*

Question 5.3. *Is it true that $\text{aw}([3n], 3) = \text{aw}([n], 3) + 1$ for all positive integers n ?*

We now turn our attention to \mathbb{Z}_n .

Question 5.4. *Are there infinitely many primes p such that $\text{aw}(\mathbb{Z}_p, 3) = 3$?*

Based on [8, Theorem 3.5] (see also Theorem 3.3), one approach to finding primes p for which $\text{aw}(\mathbb{Z}_p, 3) = 3$ is to search for primes p such that the multiplicative group \mathbb{Z}_p^\times is generated by 2. However, the existence of an infinite family of such primes is still open.

Conjecture 5.5 (Artin's Conjecture). [11, p. 217] *There are infinitely many primes p such that 2 is a generator of the multiplicative group \mathbb{Z}_p^\times .*

If Artin's Conjecture holds, it would give us an infinite family of \mathbb{Z}_p such that $\text{aw}(\mathbb{Z}_p, 3) = 3$. Jungić et al. also established another family of primes p with $\text{aw}(\mathbb{Z}_p, 3) = 3$ (see Theorem 3.3), namely those primes p such that $\frac{p-1}{2}$ is odd and the order of 2 in \mathbb{Z}_p^\times is $\frac{p-1}{2}$.

Acknowledgements

We thank the referee for a very helpful report, including pointing out some of the consequences [8, Theorem 3.5] and suggesting the current proof of Lemma 2.6, which we had proved another way using Proposition 2.18. The majority of this research was done during the 2013–2014 academic year at Iowa State University.

References

- [1] M. Axenovich and D. Fon-Der-Flaass, On rainbow arithmetic progressions. *Electron. J. Combin.* **11** (2004), no. 1, Research Paper 1, 7pp. [MR2034415](#)
- [2] M. Axenovich and R.R. Martin, Sub-Ramsey numbers for arithmetic progressions. *Graphs Combin.* **22** (2006), no. 1, 297–309. [MR2264853](#)
- [3] F.A. Behrend, On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci. USA* **32** (1946), 331–332. [MR0018694](#)

- [4] M. Elkin, An improved construction of progression-free sets. *Israel J. Math.* **184** (2011), 93–128. [MR2823971](#)
- [5] W. Gasarch, J. Glenn, and C.P. Kruskal, Finding large 3-free sets I: The small n case. *J. Comput. System Sci.* **74** (2008), no. 4, 628–655. [MR2417032](#)
- [6] W.T. Gowers, A new proof of Szemerédi’s theorem. *Geom. Funct. Anal.* **11** (2001), no. 3, 465–588. [MR1844079](#)
- [7] B. Green and J. Wolf, A note on Elkin’s improvement of Behrend’s construction. In *Additive Number Theory*, D. Chudnovsky and G. Chudnovsky, Eds., pp. 141–144, Springer, New York, 2010. [MR2744752](#)
- [8] V. Jungić, J. Licht (Fox), M. Mahdian, J. Nešetřil, and R. Radoičić, Rainbow arithmetic progressions and anti-Ramsey results. *Combin. Probab. Comput.* **12** (2003), no. 5–6, 599–620. [MR2037073](#)
- [9] I. Laba and M.T. Lacey, On sets of integers not containing long arithmetic progressions. Manuscript available at [arXiv:math/0108155](#) [[math.CO](#)].
- [10] R.A. Rankin, Sets of integers containing not more than a given number of terms in arithmetical progression. *Proc. Roy. Soc. Edinburgh Sect. A* **65** (1960/1961), 332–344 (1960/61). [MR0142526](#)
- [11] J.H. Silverman, *A friendly introduction to number theory*, 4th ed. Pearson, Upper Saddle River, NJ, 2013.
- [12] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression. Collection of articles in memory of Juriĭ Vladimirovič Linnik. *Acta Arith.* **27** (1975), 199–245. [MR0369312](#)
- [13] K. Uherka, An introduction to Ramsey theory and anti-Ramsey theory on the integers. Master’s Creative Component (2013), Iowa State University.

STEVE BUTLER

DEPARTMENT OF MATHEMATICS

IOWA STATE UNIVERSITY

AMES, IA

USA

E-mail address: butler@iastate.edu

CRAIG ERICKSON
DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
GRAND VIEW UNIVERSITY
DES MOINES, IA
USA
E-mail address: cerickson@grandview.edu

LESLIE HOGBEN
DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IA
USA
AMERICAN INSTITUTE OF MATHEMATICS
600 E. BROKAW ROAD
SAN JOSE, CA
USA
E-mail address: hogben@aimath.org

KIRSTEN HOGENSON
DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IA
USA
E-mail address: kahogens@iastate.edu

LUCAS KRAMER
MATHEMATICS DEPARTMENT
BETHEL COLLEGE
NORTH NEWTON, KS
USA
E-mail address: lkramer@bethelks.edu

RICHARD L. KRAMER
DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IA
USA
E-mail address: ricardo@iastate.edu

JEPHIAN CHIN-HUNG LIN
DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IA
USA
E-mail address: chlin@iastate.edu

RYAN R. MARTIN
DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IA
USA
E-mail address: rymartin@iastate.edu

DERRICK STOLEE
DEPARTMENT OF MATHEMATICS
DEPARTMENT OF COMPUTER SCIENCE
IOWA STATE UNIVERSITY
AMES, IA
USA
E-mail address: dstolee@iastate.edu

NATHAN WARNBERG
DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF WISCONSIN-LA CROSSE
LA CROSSE, WI
USA
E-mail address: nwarnberg@uwlax.edu

MICHAEL YOUNG
DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IA
USA
E-mail address: myoung@iastate.edu

RECEIVED 29 APRIL 2014