THE NUMBER OF PERMUTATIONS WHICH FORM ARITHMETIC PROGRESSIONS MODULO \( m \)

BY

FLORIAN LUCA and AUGUSTINE O. MUNAGI

Abstract. We find a formula for the number of permutations of \( \{1, 2, \ldots, n\} \) which form arithmetic progressions modulo \( m \).

Mathematics Subject Classification 2010: 05A05, 05A15.

Key words: permutations, arithmetic progressions.

1. Introduction

Let \( \sigma = (\sigma(1), \ldots, \sigma(n)) \) be a permutation of \( [n] = \{1, 2, \ldots, n\} \). We say that \( \sigma \) is an arithmetic progression (AP) modulo \( m \) if \( \sigma(i + 1) - \sigma(i) \equiv r \pmod{m} \) for all \( i = 1, \ldots, n - 1 \). Let \( a(n, m) \) denote the number of AP permutations modulo \( m \) of \( [n] \), that is, with \( S_n \) the symmetric group on \( n \) symbols,

\[
a(n, m) = \#\{\sigma \in S_n : \sigma \mod{m} \text{ is an AP}\}.
\]

From our search of the literature, it seems that only the special case \( m = n \) has been considered. In Sloane’s On-Line Encyclopedia of Integer Sequences [6, A002618] one finds the assertion:

\[
a(n, n) = n\phi(n),
\]

where \( \phi(n) \) denotes Euler’s totient function.

In this note we consider the more general function \( a(n, m) \). The motivation arose partly from similar investigations in integer partitions dealing with the enumeration of standard AP’s [1, 3, 5]. However, the latter problem is trivial for permutations since the number of standard AP’s in \( S_n \) is
easily seen to be 1 when \( n = 1 \), and when \( n \geq 2 \) there are just two AP’s namely:

\[ (1, 2, \ldots, n), (n, n-1, \ldots, 1). \]

Clearly, \( a(n, 1) = n! \), and since the two permutations in (2) are always counted by \( a(n, m) \) for every \( m > 0 \), it follows that

\[
\lim_{m \to \infty} a(n, m) = 2, \quad n \geq 2.
\]

Indeed the following specific result, which is apparent from Table 1, may be deduced from our main theorem (Theorem 2), proved in section 2.

**Proposition 1.** We have

i. \( a(n, n + 1) = \phi(n + 1) \).

ii. \( a(n, M) = 2, \ M \geq n + 2 \).

<table>
<thead>
<tr>
<th>( n \backslash m )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>24</td>
<td>8</td>
<td>4</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>120</td>
<td>12</td>
<td>8</td>
<td>4</td>
<td>20</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>720</td>
<td>72</td>
<td>48</td>
<td>8</td>
<td>8</td>
<td>12</td>
<td>6</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>5040</td>
<td>144</td>
<td>48</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>42</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>40320</td>
<td>1152</td>
<td>144</td>
<td>128</td>
<td>16</td>
<td>8</td>
<td>12</td>
<td>23</td>
<td>6</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>362880</td>
<td>2880</td>
<td>1296</td>
<td>96</td>
<td>64</td>
<td>16</td>
<td>8</td>
<td>54</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Number \( a(n, m) \) of AP permutations modulo \( m \) of \( \mathbb{Z}_n \).

Lastly, we note that the sequence \( a(n, 2), n > 0 \): 1, 2, 2, 8, 12, 72, \ldots, may be obtained by direct reasoning: \( a(2k - 1, 2) = (k - 1)!k! \) or \( a(2k, 2) = 2k!^2 \), \( k > 0 \), that is,

\[
a(n, 2) = 2 \left( \frac{n}{2} \right)!^2 \quad \text{if } n \text{ is even},
\]

\[
a(n, 2) = \left( \frac{n + 1}{2} \right)! \left( \frac{n - 1}{2} \right)! \quad \text{if } n \text{ is odd}.
\]
These numbers have previously appeared in [4, 7] in connection with parity-alternating permutations which are the permutation analogues of alternating subsets (see also [2]). It is easy to see that a permutation counted by \(a(n, 2)\) consists of parity-alternating entries: each gap distance is either 1 or \(-1\) which implies a parity change.

2. Main theorem
The result is the following.

**Theorem 2.** Write \(n = mq + t\), where \(q \geq 0\) and \(1 \leq t \leq m\). Then the following formula holds

\[
a(n, m) = (q + 1)!q!^{m-t}A(t, m),
\]

where

\[
A(t, m) = \begin{cases} 
  m\phi(m), & \text{if} \quad t = m, \\
  \phi(m), & \text{if} \quad t \in \{1, m-1\}, \\
  2, & \text{if} \quad t \in [2, m-2].
\end{cases}
\]

**Proof.** We assume that \(m > 1\) and \(n > 1\). We let \(\sigma\) be a permutation which is an AP modulo \(m\). Then \(\sigma(i) = a_1 + ir\) for \(i = 1, \ldots, n\). We note first that \(r\) and \(m\) are coprime, for if not, then putting \(d = \gcd(m, r)\), we get that all numbers \(\sigma(i)\) are congruent to \(a_1\) \((\mod d)\). Since these numbers are in fact the numbers \(1, \ldots, n\) modulo \(m\) in some order, we get that \(1 \equiv 2 \mod d\), so \(d = 1\). Now we write \(n = qm + t\) where \(q \geq 0\) and \(1 \leq t \leq m\) as in the statement of the theorem. Then the numbers \(1, \ldots, n\) run through all residue classes modulo \(m\) \(q\) times and one extra time they run only through the residue classes \(1, \ldots, t\) modulo \(m\). Thus, the numbers \(a_1 + ir\) for \(i = 1, \ldots, n\) must do the same. Since \(\gcd(r, m) = 1\), as \(i\) runs through a complete residue system \(\{1, \ldots, m\}\) modulo \(m\), so do the numbers \(a_1 + ir\) for \(i \in \{1, \ldots, m\}\). In particular, as \(i\) ranges from 1 to \(mq\), the numbers \(a_1 + ir\) go through all residue classes modulo \(m\) \(q\) times. So, we conclude that for \(i \in \{mq + 1, \ldots, mq + t\}\) the residues of \(a_1 + ir\) must be exactly the residues \(\{1, \ldots, t\}\) in some order. Since we are working modulo \(m\) anyway, we may assume that \(i \in \{1, \ldots, t\}\), so that the image of the map \(\tau(i) = a_1 + ir\) modulo \(m\) for \(i \in \{1, \ldots, t\}\) is exactly the set of residues \(\{1, \ldots, t\}\).

If \(t = m\), there is no restriction, so we can take any of the \(\phi(m)\) values for \(r\) and any of the \(m\) values for \(a_1\).
If \( t = 1 \), then we must take \( a_1 \equiv 1 - r \pmod{m} \). So, for \( t = 1 \) and any \( r \) there is exactly one possibility for \( a_1 \).

If \( t = m - 1 \), then \( \{a_1 + r, a_1 + 2r, \ldots, a_1 + (m - 1)r\} \) are \( \{1, 2, \ldots, m - 1\} \). Thus, \( a_1 \equiv 0 \pmod{m} \) in this case.

Assume now that \( t \not\in \{1, m - 1, m\} \). Then \( \{r, 2r, \ldots, tr\} \pmod{m} \) modulo \( m \) is the same as \( \{-a_1 + 1, -a_1 + 2, \ldots, -a_1 + t\} \pmod{m} \). In particular, the second set of residues modulo \( m \) does not contain the residue 0 and it is an interval, that is of the form \( [a,b] = \{k : a \leq k \leq b\} \). We show that one of the end points of the interval is either 1 or \( m - 1 \). Assume this is not so. Then \( [-a_1 + 1, -a_1 + t] \subseteq [2, m - 2] \). Now changing \( i \) to \(-i\), we get that multiplication by \( r \) maps \([-t, -1]\) into \([a_1 - t, a_1 - 1]\), which is also an interval in \([2, m - 2]\). However, the set of nonzero differences of elements in \([1, t]\) is \((-t - 1), -1 \cup [1, (t - 1)]\) which is in \([-t, -1] \cup [1, t]\) so via the multiplication by \( r \) map, is taken into \([a_1 - t, a_1 - 1] \cup [-a_1 + 1, -a_1 + t] \) which, as we said earlier, is either an interval or a union of two intervals in \([2, m - 2]\). However, of course the set of nonzero differences in \([-a_1 + 1, -a_1 + t]\) contains the residue 1. This contradiction shows that it is not possible for \([-a_1 + 1, -a_1 + t]\) to be an interval in \([2, m - 2]\). Assume that \(-a_1 + t = m - 1\). Then \( a_1 \) is uniquely defined and multiplication by \( r \) maps \([1, t]\) into \([-t, -1]\). By changing the sign of \( r \) if necessary, we may assume that multiplication by \( r \) maps \([1, t]\) to \([1, t]\). It then also maps \([t + 1, m - 1]\) which takes \([1, m - (t + 1)]\) into itself and so by changing the signs, if needed, it takes \([1, m - (t + 1)]\) into itself. Since the sum of \( t \) and \( m - (t + 1) \) is \( m - 1 \), we may assume, up to replacing \( t \) by \((m - (t + 1))\) and changing \( r \) to \(-r\), that \( t \leq (m - 1)/2 \). We now show that \( r = 1 \). Assume that this is not so. Clearly, \( r \in [1, t] \). Suppose that \( r \geq 2 \). The largest multiple of \( r \) which is at most \( t \) is \( r \lfloor t/r \rfloor \). Clearly, \( \lfloor t/r \rfloor \leq t/r < t \) because \( r \geq 2 \). Then \[
\left\lfloor \frac{t}{r} \right\rfloor + 1 \leq t \quad \text{therefore} \quad r \left( \left\lfloor \frac{t}{r} \right\rfloor + 1 \right) \in \{1, 2, \ldots, t\} \pmod{m}.
\]
However, \( r(\lfloor t/r \rfloor + 1) > t \) and \( r(\lfloor t/r \rfloor + 1) = r\lfloor t/r \rfloor + r \leq t + r \leq 2t \leq m - 1 \). Thus, the residue of \[
r \left( \left\lfloor \frac{t}{r} \right\rfloor + 1 \right)
\]
is not in the interval \([1, t]\) modulo \( m \), a contradiction.

So, we showed that if \( t \not\in \{1, m - 1, m\} \), then \( r = \pm 1 \). In this case, if \( r = 1 \), then the set \( \{a_1 + 1, \ldots, a_1 + t\} \pmod{m} \) has to be the same set of
residues as \( \{1, 2, \ldots, t\} \) modulo \( m \) so that \( a_1 \equiv 0 \pmod{m} \). In case when \( r = -1 \), then the set of residues \( \{a_1 - 1, \ldots, a_1 - t\} \) modulo \( m \) has to be the same as the set of residues of \( \{1, \ldots, t\} \) modulo \( m \), so we get that \( a_1 = t + 1 \pmod{m} \). So, for \( r \in \{1, \ldots, m\} \) and coprime to \( m \), we define

\[
B(r) = \begin{cases}  
    r, & \text{if } t = m, \\
    1, & \text{if } t \in \{1, m - 1\}, \\
    0, & \text{if } t \in \{2, m - 2\} \
\end{cases}
\]

For a fixed \( r \) coprime to \( m \), the number \( B(r) \) defined above counts the number of choices for \( a_1 \in \mathbb{Z}/m\mathbb{Z} \) such that modulo \( m \), the function \( \tau(i) = a_1 + ir \pmod{m} \) is a permutation of \( \{1, 2, \ldots, t\} \). Since otherwise the values of \( \{1, \ldots, n\} \) which are all in a fixed residue class modulo \( m \) and which appear either \( q \) or \( q + 1 \) times, according to whether the residue class is in \( \{1, \ldots, t\} \) or in \( \{t + 1, \ldots, m\} \), respectively, can be permuted freely among themselves, we get that

\[
a(n, m) = (q + 1)! q^{m-t} \sum_{1 \leq r \leq m \atop \gcd(r, m) = 1} B(r) = (q + 1)! q^{m-t} A(t, m),
\]

which completes the proof of the theorem.

**Acknowledgements.** A. M. was partially supported by National Research Foundation of South Africa under grant number 80860.

**REFERENCES**


Received: 5.III.2013
Accepted: 19.IV.2013

The John Knopfmacher Centre
for Applicable Analysis and Number Theory,
University of the Witwatersrand,
P.O. Box Wits 2050,
SOUTH AFRICA
florian.luca@wits.ac.za

Augustine.Munagi@wits.ac.za