152. On Arithmetic Properties of Symmetric Functions of Consecutive Integers

By Bunjiro Tsumura
Tsumura Research Institute, Tokyo

1. Main results. Let \( n \) be any integer \( \geq 2 \). We shall write:

\[
f_n(x) = \prod_{i=1}^{n} (x + i) = \sum_{k=0}^{\infty} a_k^{(n)} x^k,
\]

so that we have:

\[ a_0^{(n)} = n, \quad a_1^{(n)} = 1, \quad a_{k+2}^{(n)} = a_{k+1}^{(n)} = \cdots = 0 \]

and \( a_k^{(n)} \) \((1 \leq k \leq n-1)\) is the elementary symmetric function of degree \((n-k)\) of \( n \) consecutive integers \( \{1, 2, \ldots, n\} \). These numbers have interesting arithmetic properties as shown in the following theorems:

Theorem 1. Let \( p \) be any prime and suppose \( p-1 \leq n \). \( a_k^{(n)} \) being defined by \(1\), put

\[
b_k^{(n)} = \sum_{j=0}^{p-2} a_j^{(n)} a_j^{(p-1)}, \quad j = 0, 1, \ldots, p-2.
\]

(The right-hand side of \(2\) is a finite sum, because \( a_{n+1}^{(n)} = a_{n+2}^{(n)} = \cdots = 0 \).)

Then we have

\[
b_j^{(n)} \equiv 0 \pmod{p}
\]

for \( j = 0, 1, \ldots, p-2 \).

Remark. When \( p-1 = n \), \((3)\) means

\[
b_0^{(p-1)} = a_0^{(p-1)} a_1^{(p-1)} = (p-1)! + 1 \equiv 0 \pmod{p}
\]

and

\[
a_1^{(p-1)} a_2^{(p-1)} \equiv \cdots \equiv a_{p-2}^{(p-1)} \equiv 0 \pmod{p}.
\]

\((4)\) is nothing but the classical theorem of Wilson. Thus Theorem 1 can be regarded as a generalization of Wilson’s theorem.

From (5) follows, by the fundamental theorem on symmetric functions that any homogeneous symmetric function of \( \{1, 2, \ldots, p-1\} \) with integral coefficients of a positive degree \( \leq p-2 \) is always divisible by \( p \). The following theorem gives a more precise result:

Theorem 2. Let \( p \) be any prime \( \geq 3 \). Then any homogeneous symmetric function of \( \{1, 2, \ldots, p-1\} \) with integral coefficients of odd degree which is \( \geq 3 \) and \( \leq p-2 \), is always divisible by \( p^2 \).

Some special cases of this theorem are reported in Dickson [1], pp. 95–96.

The following theorem concerns again \( a_k^{(n)} \) for general \( n \) (not only for \( n=p-1 \)).

Theorem 3. \( a_k^{(n)} \) being defined by \(1\) as above, and \( p \) being any
prime \geq 2$, put $\left\lfloor \frac{n}{p} \right\rfloor = \nu_p(n)$. ([x], for $x \in \mathbb{R}$, denotes the largest integer \leq x.) For $\nu_p(n) \geq k$, $a_p(n)$ is divisible by $(\nu_p(n) - k)$-th power of $p$.

2. Sketch of proofs. Our Theorem 1 follows from the following Lemma. Let

$$F(x) = \sum_{k=0}^{n} A_k x^k$$

be a polynomial with integral coefficients of degree \leq n. Put $A_{n+1} = A_{n+2} = \cdots = 0$ and

$$B_j = \sum_{k=0}^{n} A_{j+(p-1)k}$$

for $j=0, 1, 2, \ldots, p-2$, where $p$ is any prime. If

$$F(1) \equiv F(2) \equiv \cdots \equiv F(p-1) \equiv 0 \pmod{p},$$

then we have

$$B_0 \equiv B_1 \equiv \cdots \equiv B_{p-2} \equiv 0 \pmod{p}.$$  

Proof. Put

$$G(x) = \sum_{j=0}^{p-2} B_j x^j, \quad F(x) - G(x) = H(x).$$

As we have, for $j = 0, 1, \ldots, p-2$,

$$i^j \equiv i^{j+(p-1)} \equiv i^{j+2(p-1)} \equiv \cdots \pmod{p}$$

for $i = 1, 2, \ldots, p-1$, we have

$$H(1) \equiv H(2) \equiv \cdots \equiv H(p-1) \equiv 0 \pmod{p}.$$  

From (6) follows now

$$G(1) \equiv G(2) \equiv \cdots \equiv G(p-1) \equiv 0 \pmod{p}.$$  

But $G(x)$ of a degree \leq p-2. Hence follows (7) by a well-known theorem of algebra.

It is obvious that for $F(x) = f_n(x)$, the condition (6) is satisfied. So we obtain Theorem 1.

To illustrate the proof of Theorem 2, consider the case of degree 3. Put generally:

$$s_k^{(n)} = \sum_{i=1}^{n} i^k.$$  

The values of $s_k^{(n)}$ are obtained by Bernoulli’s summation formula, and it is known that

$$s_k^{(p-1)} \equiv 0 \pmod{p} \quad \text{for } k = 1, 2, 3, 4, \ldots,$$

and

$$s_k^{(p-1)} = s_k^{(p-1)} = \cdots = 0 \pmod{p}.$$  

Now we have, by a well-known formula of Newton:

$$s_k^{(p-1)} - a_k^{(p-1)} s_k^{(p-1)} + a_k^{(p-1)} s_k^{(p-1)} - 3a_k^{(p-1)} = 0.$$  

In virtue of (8), (9), and (5), we obtain from (10)

$$3a_k^{(p-1)} \equiv 0 \pmod{p}.$$  

Now $a_k^{(p-1)}$ is the elementary symmetric function of $\{1, 2, \ldots, p-1\}$ of degree 3. As far as we are considering functions of degree 3
which is \( \leq p - 2 \), we should have \( p \geq 5 \). So (11) implies
\[
\alpha_{p-1}^{(p-1)} \equiv 0 \pmod{p^2}.
\]

Let \( s \) be any homogeneous symmetric function of degree 3 of \( \{1, 2, \ldots, p-1\} \) with integral coefficients. By the fundamental theorem on symmetric functions, \( s \) can be written in a form:
\[
s = c_1 a_{p-1}^{(p-1)} + c_2 a_{p-2}^{(p-1)} a_{p-3}^{(p-1)} + c_3 a_{p-3}^{(p-1)^3}
\]
where \( c_1, c_2, c_3 \) are integers. From (5), (12) follows then \( s \equiv 0 \pmod{p^2} \).

For higher degrees 5, 7, \ldots, \( p-2 \), the proof runs analogously. We have in particular:
\[
\alpha_{p-1}^{(p-1)} \equiv 0 \pmod{p^2}
\]
for \( p \geq 5 \).

The assertion of Theorem 3 for \( k = 0 \) is clear as \( a_0^{(n)} = n! \) and \( n! \) is, as is well-known, divisible by \( \left( \left\lceil \frac{n}{p} \right\rceil + \left\lceil \frac{n}{p^2} \right\rceil + \cdots \right) \)-th power of \( p \). We shall illustrate here the proof for \( k = 1 \), through induction based on the obvious recursion formula:
\[
a_{k+1}^{(n)} \cdot (n+1) + a_k^{(n)} = a_{k+1}^{(n+1)}
\]
which yields for \( k = 0 \)
\[
(14) \quad a_1^{(n)} \cdot (n+1) + a_0^{(n)} = a_1^{(n+1)}.
\]

Divide now two cases: (i) \( n+1 \not\equiv 0 \pmod{p} \) i.e. \( \left\lceil \frac{n+1}{p} \right\rceil = \left\lceil \frac{n}{p} \right\rceil \)
and (ii) \( n+1 \equiv 0 \pmod{p} \), i.e. \( \left\lceil \frac{n+1}{p} \right\rceil = \left\lceil \frac{n}{p} \right\rceil + 1 \).

Case (i): \( a_1^{(n)} \) is divisible by \( \left( \left\lceil \frac{n}{p} \right\rceil - 1 \right) \)-th power of \( p \) by the hypothesis of induction and \( a_0^{(n)} = n! \) is also divisible by the same power as noted above. Therefore so is also \( a_1^{(n+1)} \) by (14).

Case (ii): \( a_1^{(n)} (n+1) \) and \( a_0^{(n)} \) are both divisible by \( \left\lceil \frac{n}{p} \right\rceil \)-th power of \( p \), and so is also \( a_1^{(n+1)} \).

3. Some consequences and additional results. We have clearly
\[
\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a_{p-1}^{(p-1)}}{(p-1)!}.
\]

So if \( p \) is a prime \( \geq 5 \), we see by Theorems 2 and 3 (particularly by (13)), that this numerator is divisible by \( p^2 \) and \( \left( \left\lceil \frac{p-1}{2} \right\rceil - 1 \right) \)-th power of 2, \( \left( \left\lceil \frac{p-1}{3} \right\rceil - 1 \right) \)-th power of 3, \ldots. The author discovered and proved this as early as in 1907. \( a_1^{(p-1)} \equiv 0 \pmod{p^2} \) was first proved by Wolstenholme according to [1], p. 89.

From Theorem 1 follows in particular
\[
a_1^{(n)} \equiv 0 \pmod{p}
\]
if \( j + (p - 1) > n \). This occurs when \( p > \frac{n + 3}{2} \) so that \( p - 2 > n - p + 1 \) and \( p - 2 \geq j > n - p + 1 \). E.g. \( a_{102}^{(102)} \) is divisible by all 11 primes between 53 and 101 and moreover by 103² by virtue of Theorem 3.

If \( n \geq pt - 1 \), then the assertion (3) in Theorem 1 can be strengthened to

\[
b_j^{[a]} \equiv 0 \pmod{p^t}.
\]

All of the numbers \( a_k^{(p-2)}, k = 0, 1, 2, \ldots, p - 2 \) are \( -1 \pmod{p} \). The author observed still many other curious facts about \( a_k^{(p)} \), such as the following, but is not in a position to enunciate the precise rules:

(a) The numbers \( a_k^{(2p-2)}, k = 0, 1, 2, \ldots, p - 2 \) are \( \equiv 1 \pmod{p} \) if \( k = p - 1, p, p + 1, \ldots, 2p - 3 \) are \( \equiv -1 \pmod{p} \).

(b) Many of the numbers \( a_k^{(pt-1)}, k = 1, 2, \ldots, pt - 1 \) are \( \equiv 0 \pmod{p}, 0 \pmod{p^2}, \ldots, 0 \pmod{p^{t-1}} \).

If \( k = 0, p - 1, 2(p - 1), \ldots, t(p - 1) \), then \( a_k^{(pt-1)} \equiv \pm 1 \pmod{p} \) or \( \pm t \pmod{p} \).

The author wishes to express his thanks to Professor S. Iyanaga for his encouragement.

Reference