152. *On Arithmetic Properties of Symmetric Functions of Consecutive Integers*

By Bunjiro TSUMURA

Tsumura Research Institute, Tokyo

(Comm. by Zyoiti SUETUNA, M.J.A., Oct. 12, 1967)

1. **Main results.** Let n be any integer $\geqslant 2$. We shall write:

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

so that we have:

$$a_0^{(n)}=n!, \quad a_n^{(n)}=1, \quad a_{n+1}^{(n)}=a_{n+2}^{(n)}=\cdots=0$$

and $a_k^{(n)}$ $(1\leq k\leq n-1)$ is the elementary symmetric function of degree $(n-k)$ of n consecutive integers $\{1, 2, \cdots, n\}$. 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*

$$(2) \qquad b_j^{(n)}=\sum_{\nu=0}^{\infty}a_{j+(p-1)\nu}^{(n)}, \quad j=0, 1, \cdots, p-2.$$

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

Then we have

$$(3) \qquad b_j^{(n)}\equiv 0 \pmod p$$

for $j=0, 1, \cdots, p-2$.

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

$$(4) \qquad b_0^{(p-1)}=a_0^{(p-1)}+a_{p-1}^{(p-1)}=(p-1)!+1\equiv 0 \pmod p$$

and

$$(5) \qquad a_1^{(p-1)}\equiv a_2^{(p-1)}\equiv \cdots \equiv a_{p-2}^{(p-1)}\equiv 0 \pmod p.$$

(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 $\{1, 2, \cdots, p-1\}$ 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 $\geqslant 3$. Then any homogeneous symmetric function of $\{1, 2, \cdots, p-1\}$ with integral coefficients of odd degree which is $\geqslant 3$ 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* $\geqslant 2$, *put* $\left[\frac{n}{p}\right]=\nu_p^{(n)}$. ($[x]$, *for* $x \in \mathbf{R}$, *denotes the largest integer* $\leq x$.) *For* $\nu_p^{(n)} \geqslant k$, $a_k^{(n)}$ *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*

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

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

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

then we have

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

Proof. Put

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

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

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

for $i=1, 2, \cdots, p-1$, 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. q.e.d.

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

(8) $$s_k^{(p-1)}\equiv 0 \pmod p$$

for $k=1, 2, 3, 4, \cdots$, and

(9) $$s_3^{(p-1)}\equiv s_5^{(p-1)}\equiv \cdots \equiv 0 \pmod{p^2}.$$

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

(10) $$s_3^{(p-1)}-a_{p-2}^{(p-1)}s_2^{(p-1)}+a_{p-3}^{(p-1)}s_1^{(p-1)}-3a_{p-4}^{(p-1)}=0.$$

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

(11) $$3a_{p-4}^{(p-1)}\equiv 0 \pmod{p^2}.$$

Now $a_{p-4}^{(p-1)}$ is the elementary symmetric function of $\{1, 2, \cdots, p-1\}$ of degree 3. As far as we are considering functions of degree 3 which is $\leq p-2$, we should have $p \geqslant 5$. So (11) implies

(12) $$a_{p-4}^{(p-1)} \equiv 0 \pmod{p^2}.$$

Let s be any homogeneous symmetric function of degree 3 of $\{1, 2, \cdots, p-1\}$ with integral coefficients. By the fundamental theorem on symmetric functions, s can be written in a form:

$$s = c_1 a_{p-4}^{(p-1)} + c_2 a_{p-2}^{(p-1)} a_{p-3}^{(p-1)} + c_3 (a_{p-2}^{(p-1)})^3$$

where c_1, c_2, c_3 are integers. From (5), (12) follows then $s \equiv 0 \pmod{p^2}$.

For higher degrees $5, 7, \cdots, p-2$, the proof runs analogously. We have in particular:

(13) $$a_1^{(p-1)} \equiv 0 \pmod{p^2}$$

for $p \geqslant 5$.

The assertion of Theorem 3 for $k=0$ is clear as $a_0^{(n)} = n!$ and $n!$ is, as is well-known, divisible by $\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots\right)$-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) $$a_1^{(n)} \cdot (n+1) + a_0^{(n)} = a_1^{(n+1)}.$$

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

Case (i): $a_1^{(n)}$ is divisible by $\left(\left[\frac{n}{p}\right] - 1\right)$-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 $\left[\frac{n}{p}\right]$-th power of p, and so is also $a_1^{(n+1)}$.

3. Some consequences and additional results. We have clearly

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a_1^{(p-1)}}{(p-1)!}.$$

So if p is a prime $\geqslant 5$, we see by Theorems 2 and 3 (particularly by (13)), that this numerator is divisible by p^2 and $\left(\left[\frac{p-1}{2}\right] - 1\right)$-th power of 2, $\left(\left[\frac{p-1}{3}\right] - 1\right)$-th power of 3, $\cdots$. 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

$$a_j^{(n)} \equiv 0 \pmod{p}$$

if $j+(p-1)>n$. This occurs when $p>\frac{n+3}{2}$ so that $p-2>n-p+1$ and $p-2\geqslant j>n-p+1$. E.g. $a_{51}^{(102)}$ is divisible by all 11 primes between 53 and 101 and moreover by 103^2 by virtue of Theorem 3.

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

$$b_j^{(n)}\equiv 0 \qquad (\mathrm{mod}\ p^t).$$

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

(a) The numbers $a_k^{(2p-2)}$, $k=0, 1, 2, \cdots, p-2$ are $\equiv 1$ (mod p)
$k=p-1, p, p+1, \cdots, 2p-3$ are $\equiv -1$ (mod p).

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

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

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

Reference

[1] L. E. Dickson: History of the Theory of Numbers (Chap. III). Washington (1919).