

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 ≥ 2 . We shall write:

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

so that we have:

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

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

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

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

Then we have

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

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

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

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

and

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

(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 $\{1, 2, \dots, p-1\}$ 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 ≥ 3 . Then any homogeneous symmetric function of $\{1, 2, \dots, p-1\}$ with integral coefficients of odd degree which is ≥ 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