On a theorem of G. Baron and A. Schinzel

ALEKSANDER GRYTCZUK

Abstract. G. Baron and A. Schinzel [1] generalized the wellknown Wilson's theorem. In this paper—under Theorem B—an extension of their theorem can be found.

1. Introduction

In 1979 an extension of Wilson's theorem was given by G. Baron and A. Schinzel [1]. Namely they proved the following:

Theorem A. For any prime p and any residues $x_i \bmod p$ we have

$$\sum_{\sigma\in S_{p-1}} x_{\sigma(1)}\left(x_{\sigma(1)}+x_{\sigma(2)}\right)\cdots\left(x_{\sigma(1)}+\cdots+x_{\sigma(p-1)}\right)\equiv \equiv (x_1+\cdots+x_{p-1})^{p-1} \pmod p \tag{1}$$

where summation is taken over all permutation σ of $\{1,2,\cdots,p-1\}$.

In the present Note we prove the following extension of Theorem A:

Theorem B. For any prime p and any residues $x_i \bmod p$ and for fixed natural number k such that $p-1\nmid k$ we have

$$\sum_{\sigma\in S_{p-1}} x_{\sigma(1)}^k\left(x_{\sigma(1)}^k+x_{\sigma(2)}^k\right)\cdots\left(x_{\sigma(1)}^k+\cdots+x_{\sigma(p-1)}^k\right)\equiv \equiv \left(x_1^k+\cdots+x_{p-1}^k\right)^{p-1} \pmod p \tag{2}$$

and if $x_i\neq 0$ are residues mod p, p is an odd prime such that $p-1\mid k$ then

$$\sum_{\sigma\in S_{p-1}} x_{\sigma(1)}^k\left(x_{\sigma(1)}^k+x_{\sigma(2)}^k\right)\cdots\left(x_{\sigma(1)}^k+\cdots+ +x_{\sigma(p-1)}^k\right)\equiv 1 \pmod p \tag{3}$$

where summation is taken over all permutation σ of $\{1,2,\cdots,p-1\}$.

We note that Ch. Snyder [3] gave interesting applications of (1) to differentials in rings of characteristic p.

2. PROOF of the Theorem B. Let

$$S_{1,\sigma} = \sum_{\sigma \in S_{p-1}} x_{\sigma(1)} \left(x_{\sigma(1)} + x_{\sigma(2)}\right) \cdots \left(x_{\sigma(1)} + \cdots + x_{\sigma(p-1)}\right) \tag{4}$$

and

$$S_{k,\sigma} = \sum_{\sigma \in S_{p-1}} x^k_{\sigma(1)} \left(x^k_{\sigma(1)} + x^k_{\sigma(2)}\right) \cdots \left(x^k_{\sigma(1)} + \cdots + x^k_{\sigma(p-1)}\right) \tag{5}$$

First we note that if $p-1 \nmid k$ and $k > p-1$ then $k = (p-1)t + r$, $1 \leq r < p-1$ and by Fermat's theorem we obtain $S_{k,\sigma} \equiv S_{r,\sigma} \pmod{p}$. Thus it suffices to prove (2) in the case $k < p-1$. It is easy to see that for such k we have

$$x^k_i \equiv x_{\sigma(i)} \pmod{p} \tag{6}$$

for some σ and $i = 1, 2, \cdots, p-1$.
From (6) we obtain

$$S_{k,\sigma} \equiv \sum_{\sigma \in S_{p-1}} x_{\sigma(\sigma(1))} \left(x_{\sigma(\sigma(1))} + x_{\sigma(\sigma(2))}\right) \cdots \left(x_{\sigma(\sigma(1))} + \cdots + x_{\sigma(\sigma(p-1))}\right) \pmod{p} \tag{7}$$

By (7) and (1) it follows that

$$S_{k,\sigma} \equiv \left(x_{\sigma(1)} + \cdots + x_{\sigma(p-1)}\right)^{p-1} \pmod{p}. \tag{8}$$

Now by (8) and (6) we obtain

$$s_{k,\sigma} \equiv \left(x^k_1 + \cdots + x^k_{p-1}\right)^{p-1} \pmod{p}$$

and (2) is proved.

For the proof (3) we remark that $k = (p-1)t$ and by Fermat's theorem we obtain

$$S_{k,\sigma} \equiv \sum_{\sigma \in S_{p-1}} 1 \cdot 2 \cdots (p-1) = (p-1)!(p-1)! \pmod{p} \tag{9}$$

From (9) and Wilson's theorem we obtain

$$S_{k,\sigma} \equiv 1 \pmod{p} \quad \text{and the proof is finished.}$$

Corollary. Let x_i be residues mod p from reduced system such that for $i \neq j, x_i \neq x_j$, then

$$S_{k,\sigma} \equiv 0 \pmod{p} \quad \text{if} \quad p-1 \nmid k. \tag{10}$$

PROOF. Let $\sigma_k = x_1^k + x_2^k + \cdots + x_{p-1}^k$ then by Eisenstein's result (Cf.[2],p.95) we have $\sigma_k \equiv 0 \pmod{p}$ if $p-1 \nmid k$.
From this fact and (2) we obtain (10) and the proof is complete.

Reference

[1] G. BARON and A. SCHINZEL, An extension of Wilson's theorem, *C. R. Math. Rep. Acad. Sci. Canad*, Vol. 1, No 2 (1979), 115–118.

[2] L. E. DICKSON, History of the Theory of Numbers, Vol. I. repr. by Chelsea. (1952).

[3] Ch. SNYDER, Kummer congruences for the coefficients of Hurwitz series, *Acta Arith.*, XL (1982), 175–191.