Записки научных
семинаров ПОМИ
Том 440, 2015 г.

A. N. Andrianov

FRACTIONAL FACTORIALS AND PRIME NUMBERS (A REMARK ON THE PAPER "ON PRIME VALUES OF SOME QUADRATIC POLYNOMIALS")

Abstract. Congruences mod p for a prime p and partial products of numbers $1, \dots, p-1$ are obtained.

§1. Full factorials

According the Wilson theorem, for a positive rational prime number p, factorial of $p-1$ satisfies the congrusnce

$$(p-1)! = 1 \cdot 2 \dots (p-1) \equiv -1 \pmod{p}.$$

If p is odd, then one can write

$$\begin{aligned}(p-1)! &= 1 \cdots (p-1)/2 \cdot ((p-1)/2+1) \cdots ((p-1)/2+(p-1)/2)\\ &= ((p-1)/2)! \cdot (p-(p-1)/2) \cdots (p-1)\\ &\equiv (-1)^{(p-1)/2}(((p-1)/2)!)^2 \pmod{p}.\end{aligned}$$

and so the Wilson congruence can be written in the form

$$(((p-1)/2)!)^2 \equiv (-1)^{(p+1)/2} \pmod{p}. \tag{1}$$

On the other hand, since

$$((p-1)!)^2 = (((p-1)/2)!)^2 \prod_{i=1}^{(p-1)/2} ((p-1)/2+i)^2 \equiv 1 \pmod{p},$$

we have got the congruence

$$\prod_{i=1}^{(p-1)/2} ((p-1)/2+i)^2 \equiv (-1)^{(p+1)/2} \pmod{p}. \tag{2}$$

Key words and phrases: congruences mod p for a prime p, partial products of integers $1, \dots, p-1$.

§2. Primes $p \equiv 1 \pmod 4$

If a prime p satisfies $p \equiv 1 \pmod 4$, then congruences (1) and (2) can be written as

$$(((p-1)/4)!)^2 \prod_{i=1}^{(p-1)/4} ((p-1)/4+i)^2 \equiv -1 \pmod p, \tag{3}$$

and

$$\prod_{i=1}^{(p-1)/4} ((p-1)/2+i)^2 \prod_{i=1}^{(p-1)/4} (3(p-1)/4+i)^2 \equiv -1 \pmod p, \tag{4}$$

correspondingly.

The following theorem makes more precise Theorem 1 of A. N. Andrianov [1] (compere with [2], problem 9c to Chapter 5).

Theorem. *Let p be a prime number, $p \equiv 1 \pmod 4$, and let $p = A^2 + B^2$ be a representation of p as sum of two integral squares with even A. Then the following congruences are valid*

$$(((p-1)/4!)^4 \equiv 1/4A^2 \pmod p, \tag{5}$$

$$\prod_{i=1}^{(p-1)/4} ((p-1)/4+i)^4 \equiv 4A^2 \pmod p, \tag{6}$$

$$\prod_{i=1}^{(p-1)/4} ((p-1)/2+i)^4 \equiv 1/4A^2 \pmod p, \tag{7}$$

$$\prod_{i=1}^{(p-1)/4} (3(p-1)/4+i)^4 \equiv 4A^2 \pmod p. \tag{8}$$

Proof. The congruence (5) was proved in Andrianov [1]. The congruence (6) follows from (5) and (3). The congruence (7) and (8) similarly follows from (4). Proofs are based on consideration of sums of Legendre symbols of the form

$$S(K) = \sum_{t=0}^{p-1} \left(\frac{t(t^2+K)}{p} \right). \qquad \square$$

References

1. A. N. Andrianov, *On prime values of some quadratic polynomials.* — Zap. Nauchn. Semin. POMI (2014), 5–10.
2. I. M. Vinogradov, *Basic Number Theory.* M., (1981).

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
наб. р. Фонтанки, д. 27,
191023 С.-Петербург, Россия
E-mail: anandr@pdmi.ras.ru,
anatoli.andrianov@gmail.com

Поступило 19 октября 2015 г.