ISSN 1066-369X, Russian Mathematics (Iz. VUZ), 2012, Vol. 56, No. 9, pp. 39–45. © Allerton Press, Inc., 2012.
Original Russian Text © S.A. Tyurin, 2012, published in Izvestiya Vysshikh Uchebnykh Zavedenii. Matematika, 2012, No. 9, pp. 47–53.

The Symbol of Type and the Wilson Theorem

S. A. Tyurin[1*]

[1] *Lobachevsky State University of Nizhni Novgorod, pr. Gagarina 23, Nizhni Novgorod, 603950 Russia*

Received July 20, 2011

Abstract—We introduce the notion of an element type for the field of residues modulo a prime number and study its role in factorial computation. We obtain an expression for its quantitative characteristic (the symbol of type) in terms of continued fractions and establish its connection with the Legendre symbol.

DOI: 10.3103/S1066369X12090058

Keywords and phrases: *number theory, finite fields, continued fractions.*

The development of cryptographic methods based on the number theory started at the end of the XXth century owing to the appearance of high-performance computers. An important role in these methods is played by the primality verification of natural numbers. Various primality tests are described in the literature on the cryptography (e.g., [1–3]). One of the most old tests is based on the application of the Wilson theorem. This theorem was first proved by Lagrange in 1771; at present there are several proofs of this theorem (e.g., [4]) and its generalizations [5].

In this paper, for a prime number p we consider the calculation of the number $\left(\frac{p-1}{2}\right)!$ molulo p in the case $p \equiv 3 \pmod 4$. This issue is connected with calculations in the algebra of truncated polynomials. Calculations of factorials in the field of residue classes modulo a prime number occur in studying properties of modular trigonometric functions [6]. The obtained formulas express a solution both with the help of the Legendre symbol and with the help of the introduced symbol of type of an element. We express the symbol of type in terms of continued fractions.

1. CALCULATION OF FACTORIALS IN A PRIME FIELD

According to the Wilson theorem ([4], P. 133), any prime number p allows the comparison $(p-1)! \equiv -1 \pmod p$. In what follows we assume that $p > 2$. Then for any number i $(1 < i < p-1)$ we obtain $i! \cdot (i+1) \cdot \ldots \cdot (p-1) \equiv -1 \pmod p$. Multiplying the comparisons

$$\begin{cases} p-1 \equiv -1 \pmod p, \\ p-2 \equiv -2 \pmod p, \\ \ldots\ldots\ldots\ldots\ldots \\ i+1 \equiv -(p-i-1) \pmod p, \end{cases}$$

taking into account the Wilson theorem, we obtain

$$i! \cdot (p-i-1)! \equiv (-1)^{i+1} \pmod p.$$

The latter comparison is used for calculations of modular trigonometric functions and exponentials in the algebra of truncated polynomials [6]. In a particular case with $i = \frac{(p-1)}{2}$ we obtain the comparison

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

[*] E-mail: saturin@list.ru.