CONGRUENCES WITH FACTORIALS MODULO P

Yong-Gao Chen[1]
Department of Mathematics, Nanjing Normal University, Nanjing 210097, P. R. China

Li-Xia Dai[2]
Department of Mathematics, Nanjing Normal University, Nanjing 210097, P. R. China
lilidainjnu@163.com

Received: 3/20/06, Revised: 7/18/06, Accepted: 8/7/06, Published: 8/28/06

Abstract

It is proved that the number of $a \in \{1, \cdots, p-1\}$ which can be represented as a product of two factorials is at least $\frac{3}{4}p + O(p^{1/2}(\log p)^2)$. This improves the result given by Garaev et.al. [Trans. Amer. Math. Soc., 356 (2004)5089-5102]. Beyond this, we pose several conjectures.

1. Introduction

Throughout this paper, p is an odd prime. In [6,F11], it is conjectured that about p/e of the residue classes $a \pmod p$ are missed by the sequence $n!$. If this were so, the sequence $n!$ modulo p should assume about $(1-1/e)p$ distinct values. Some results of this spirit have appeared in [1]. The above conjecture immediately implies that if p is large enough, then every residue class a modulo p can be represented as a product of two factorials. Unfortunately, this conjecture appears to be very hard. Various additive and multiplicative congruences with factorials have been considered in [2, 3, 4, 5, 7, 8].

We denote by $F_l(a, p-1)$ the number of solutions to the congruence

$$\prod_{i=1}^{l} n_i! \equiv a \pmod p, \ 1 \le n_1, \cdots, n_l \le p-1,$$

where $a \in \{1, \ 2, \ldots, p-1\}$. Let $V_l(p-1)$ be the number of $a \in \{1, \ 2, \ldots, p-1\}$ for which $F_l(a, p-1) > 0$, that is,

$$V_l(p-1) = \sharp \left\{ \prod_{i=1}^{l} n_i! \pmod p \ \middle| \ 1 \le n_1, \cdots, n_l \le p-1 \right\}.$$

[1]Both authors supported by the National Natural Science Foundation of China, Grant No. 10471064.
[2]Corresponding author

Garaev et.al. [3] proved that

$$V_2(p-1) \geq \frac{5}{8}p + O\big(p^{1/2}(\log p)^2\big).$$

In this paper we prove the following result.

Theorem.

$$V_2(p-1) \geq \frac{3}{4}p + O\big(p^{1/2}(\log p)^2\big).$$

We pose the following conjectures.

Conjecture 1. *For any odd prime p, any integer $a \in \{1, 2, \cdots, p-1\}$ can be represented as a product of two factorials except for $p = 11$ and $a = 7$.*

Conjecture 2. *If a is a factorial, $a \neq 0$, then there are infinitely many primes p for which there are no integers n with $a \equiv n! \pmod p$.*

Conjecture 3. *Let a be an integer. If for any prime p there is an integer n with $a \equiv n! \pmod p$, then $a = -1$, $a = 0$, or a is a factorial.*

2. Proof of the Theorem

Lemma(Zhang [9, 10]). Let $N(p)$ denote the number of all pairs $(a,\ b)$ with $a,\ b \in \{1, 2, \cdots, p-1\}$ for which a and b are of opposite parity and $ab \equiv 1 \pmod p$. Then

$$N(p) = \frac{1}{2}p + O\big(p^{1/2}(\log p)^2\big).$$

Proof of Theorem. Define

$$\begin{aligned}
I_1 &= \{\ (a,\ b) \mid ab \equiv 1 \pmod p,\ 2 \mid a,\ 2 \nmid b,\ a,\ b = 1, 2, \cdots, p-1\},\\
I_2 &= \{\ (a,\ b) \mid ab \equiv 1 \pmod p,\ 2 \nmid a,\ 2 \mid b,\ a,\ b = 1, 2, \cdots, p-1\},\\
I_3 &= \{\ (a,\ b) \mid ab \equiv 1 \pmod p,\ 2 \mid a,\ 2 \mid b,\ a,\ b = 1, 2, \cdots, p-1\},\\
I_4 &= \{\ (a,\ b) \mid ab \equiv 1 \pmod p,\ 2 \nmid a,\ 2 \nmid b,\ a,\ b = 1, 2, \cdots, p-1\}.
\end{aligned}$$

It is obvious that

$$|I_2| + |I_4| = |I_1| + |I_4| = \frac{p-1}{2}, \tag{1}$$

$$|I_1| + |I_3| = |I_1| + |I_4| = \frac{p-1}{2}. \tag{2}$$

Hence $|I_1| = |I_2|,\ |I_3| = |I_4|$. Thus, by the lemma we have

$$|I_1| = |I_2| = \frac{1}{2}N(p) = \frac{1}{4}p + O\big(p^{1/2}(\log p)^2\big). \tag{3}$$

By (1), (2), and (3) we obtain

$$|I_3| = |I_4| = \frac{1}{4}p + O\big(p^{1/2}(\log p)^2\big). \tag{4}$$

Let $a,\ b \in \{1, 2, \cdots, p-1\}$ with $ab \equiv 1 \pmod p$. Wilson's Theorem implies that (the similar arguments appear in [1, 2, 3])

$$-1 \equiv (p-1)! \equiv (-1)^{a-1}(a-1)!(p-a)! \pmod p$$

and

$$-1 \equiv (p-1)! \equiv (-1)^b b!(p-b-1)! \pmod p.$$

Hence,

$$a \equiv (-1)^a a!(p-a)! \pmod p, \text{ and}$$

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

Thus, if a is even or if b is odd, then a can be represented as a product of two factorials. This implies that if $(a,\ b) \in I_1 \cup I_3 \cup I_4$, then $a \in V_2(p-1)$.

Therefore, by (3) and (4) we have

$$V_2(p-1) \geq |I_1| + |I_3| + |I_4| \geq \frac{3p}{4} + O\big(p^{1/2}(\log p)^2\big).$$

This completes the proof of the theorem.

References

[1] C. Cobeli, M. Vâjâitu and A. Zaharescu, *The sequence* $n!$ (mod p). J. Ramanujan Math. Soc. 15(2000), 135-154.

[2] P. Erdős and C. Stewart, *On the greatest and least prime factors of* $n! + 1$. J. London Math. Soc. 13(1976), 513-519.

[3] M. Z. Garaev, F. Luca, I. E. Shparlinski, *Character sums and congruences with* $n!$. Trans. Amer. Math. Soc. 356 (2004), 5089-5102.

[4] M. Z. Garaev, F. Luca, I. E. Shparlinski, *Waring problem with factorials.* Bull. Austral. Math. Soc. 71 (2005), 259-264.

[5] M. Z. Garaev, F. Luca, I. E. Shparlinski, *Sums and congruences with factorials.* J. Reine Angew. Math. 584 (2005), 29-44.

[6] R. K. Guy, *Unsolved Problems in Number Theory.* 2nd ed. Springer, New York, 1994.

[7] F. Luca and P. Stănică, *Products of factorials modulo p.* Colloq. Math. 96 (2003), 191-205.

[8] C. Stewart, *On the greatest and least prime factors of* $n! + 1$ *II.* Publ. Math. Debrecen 65 (2004), 461-480.

[9] W. P. Zhang, *On a problem of D. H. Lehmer and its generalization.* Composito Math. 86 (1993), 307-316.

[10] W. P. Zhang, *On a problem of D. H. Lehmer and its generalization II.* Composito Math. 91 (1994), 47-56.