Congruences With Factorials Modulo p II

Dai Lixia

(School of Mathematics and Computer Science, Nanjing Normal University, Nanjing 210097, China)

Abstract Let p be an odd prime and k be an integer with $1\leqslant k\leqslant p^{(1-1/\log\log p)}$. Let $l_k(p)$ be the smallest integer $l\geqslant 1$ such that for every integer λ the congruence $(n_1!)^k+\cdots+(n_l!)^k\equiv\lambda\pmod p$ has a solution in positive integers n_1, $\cdots$, n_l. It is proved that $l_k(p)=O((\log p)^3\log\log p\cdot k^{(1+1/\log\log p)})$.

Key words factorials; exponential sums; congruences

CLC number O156.1 **Document code** A **Article ID** 1001-4616(2008)04-0033-04

关于阶乘模 p 的序列 II

戴丽霞

(南京师范大学数学与计算机科学学院, 江苏 南京 210097)

[摘要] 研究了模 p 的序列 $(n_1!)^k+\cdots+(n_l!)^k\equiv\lambda\pmod p$, 其中 p 是奇素数, k 是正整数且 $1\leqslant k\leqslant p^{(1-1/\log\log p)}$. $l_k(p)$表示最小的正整数使得对任意的整数 λ 上述序列均有正整数解. 证明了 $l_k(p)=O((\log p)^3\log\log p\cdot k^{(1+1/\log\log p)})$.

[关键词] 阶乘, 指数和, 序列

Throughout this paper, p is an odd prime. In [1], 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 [2]. The above conjecture immediately implies that every residue class a modulo p can be represented as a product of at most two factorials. Unfortunately this conjecture appears to be very hard.

Studying the congruences with factorials is very interesting but also very complex. Various additive and multiplicative congruences with factorials have been considered in [3-6] and [7-10].

In particular, it has been shown in [10] that any residue class λ modulo p can be represented in the form $n_1!+\cdots+n_l!\equiv\lambda\pmod p$ with $l(p)=O((\log p)^3\log\log p)$. This result is extended in this paper, that is,

Theorem 1 Let k be an integer with $1\leqslant k\leqslant p^{(1-1/\log\log p)}$. Let $l_k(p)$ be the smallest integer $l\geqslant 1$ such that for every integer λ the congruence

$$(n_1!)^k+\cdots+(n_l!)^k\equiv\lambda\pmod p$$

has a solution in positive integers n_1, $\cdots$, n_l. Then we have

$$l_k(p)=O((\log p)^3\log\log p\cdot k^{(1+1/\log\log p)}).$$

1 Two Lemmas

We denote by $J_l(N,k)$ the number of solutions to the congruence

Received date 2008-01-12.

Foundation item Supported by the National Natural Science Foundation of China (10801075), Natural Science Foundation of Jiangsu Higher Education Institutions of China (08KJB11007) and Science Foundation of Nanjing Normal University (2006101XGQ0128).

Corresponding author Dai Lixia, doctor, lecturer, majored in number theory. E-mail: lilidainju@163.com

$$\sum_{i=1}^{l}(n_i!)^k \equiv \sum_{i=l+1}^{2l}(n_i!)^k \pmod p, \tag{1}$$

where

$$1 \leqslant n_1, \cdots, n_{2l} \leqslant N, \ k < N.$$

Let $\boldsymbol{F}_p$ be a finite field of p elements. We always assume that $\boldsymbol{F}_p$ is represented by the elements of the set $\{0, 1, \cdots, p-1\}$. We also define

$$e_p(z) = \exp(2\pi iz/p),$$

which is an additive character of $\boldsymbol{F}_p$.

It is very useful to recall the identities

$$\sum_{a=0}^{p-1} e_p(au) \equiv \begin{cases} 0, & \text{if } u \not\equiv 0 \pmod p, \\ p, & \text{if } u \equiv 0 \pmod p, \end{cases} \tag{2}$$

which we will repeatedly use, in particular to relate the number of solutions of various congruences and exponential sums.

Firstly we give several lemmas.

Lemma 1 For any positive integers l, k, N with $1 \leqslant k \leqslant p^{(1-1/\log\log p)}$, $l < N < p$ and $k < N$, we have

$$J_l(N, k) \ll l^2 N^{2l-1+1/(l+1)} k^{l/(l+1)}.$$

Proof Let us define exponential sum

$$S_a(N, k) = \sum_{n=1}^{N} e_p(a(n!)^k).$$

The identity (2) implies that

$$J_l(N, k) = \frac{1}{p}\sum_{a=0}^{p-1} |S_a(N, k)|^{2l}.$$

Set

$$K = \left[\left(\frac{kN^l}{l}\right)^{1/(l+1)}\right].$$

Applying the Hölder inequality, we derive

$$|S_a(N, k)|^{2l} = \Big|\sum_{t=1}^{K}\sum_{(t-1)NK^{-1} < m \leqslant tNK^{-1}} e_p(a(m!)^k)\Big|^{2l} \leqslant K^{2l-1}\sum_{t=1}^{K}\Big|\sum_{(t-1)NK^{-1} < m \leqslant tNK^{-1}} e_p(a(m!)^k)\Big|^{2l}.$$

Hence

$$J_l(N, k) \leqslant K^{2l-1} G_l(K, N, k),$$

where $G_l(K, N, k)$ is the number of solutions of the congruence

$$\sum_{i=1}^{l}(m_i!)^k \equiv \sum_{i=l+1}^{2l}(m_i!)^k \pmod p, \quad 1 \leqslant m_1, \cdots, m_{2l} \leqslant N, \tag{3}$$

subject to the conditions $|m_i - m_j| < NK^{-1}$ for $1 \leqslant i, j \leqslant 2l$.

Without loss of generality, we may assume that

$$m = \min\{m_i \mid 1 \leqslant i \leqslant 2l\}.$$

Denote $m_1 = m$ and put

$$m_i = m + s_i, \ 1 \leqslant i \leqslant 2l,$$

where $s_1 = 0$ and $0 \leqslant s_i < NK^{-1}$ $(2 \leqslant i \leqslant 2l)$. Obviously, $G_l(K, N, k) \leqslant 2lG_l^*(K, N, k)$, where $G_l^*(K, N, k)$ is the number of solutions of (3) with the additional restriction that

$$m_1 = m.$$

Then after dividing by $m_1! \not\equiv 0 \pmod p$, the above congruence (3) takes the form

$$\Phi_{s_1, \cdots, s_{2l}}(m) \equiv 0 \pmod p, \tag{4}$$

where

$$\Phi_{s_1, \cdots, s_{2l}}(X) = \sum_{i=1}^{l}\prod_{v=1}^{s_i}(X+v)^k - \sum_{i=l+1}^{2l}\prod_{v=1}^{s_i}(X+v)^k.$$

The number of solutions of the congruence (4) is collected from two sets of variables m and s_i, $1 \leqslant i \leqslant 2l$:

(i) the first set is such that $\Phi_{s_1, \cdots, s_{2l}}(X)$ is a polynomial of m of degree greater than zero (but less than kNK^{-1});

(ii) the second set consists of those for which $\Phi_{s_1, \cdots, s_{2l}}(X)$ vanishes modulo p as a polynomial of m.

The number of solutions $G^*_{l1}(K, N, k)$ of (4) corresponding to the first set is at most

$$G^*_{l1}(K, N, k) \leqslant kNK^{-1}(NK^{-1} + 1)^{2l-1} \leqslant k(NK^{-1} + 1)^{2l}. \tag{5}$$

For the second set of variables, we have that as a polynomial, $\Phi_{s_1, \cdots, s_{2l}}(X)$ vanishes modulo p if and only if the sequence $s_{l+1}, \cdots, s_{2l}$ is a permutation of the sequence $s_1 = 0, s_2, \cdots, s_l$. Therefore, this happens for at most $l!(NK^{-1} + 1)^{l-1}$ values of $s_1 = 0, s_2, \cdots, s_{2l}$. For these values, the congruence (4) is satisfied for all values of $m = 1, \cdots, N$. Thus

$$G^*_{l2}(K, N, k) \leqslant l!(NK^{-1} + 1)^{l-1}N. \tag{6}$$

It follows from (5) and (6) that

$$G^*_l(K, N, k) = G^*_{l1}(K, N, k) + G^*_{l2}(K, N, k) \leqslant l!(NK^{-1} + 1)^{l-1}N + k(NK^{-1} + 1)^{2l} \leqslant$$
$$l!N^lK^{-l+1}(KN^{-1} + 1)^{l-1} + kN^{2l}K^{-2l}(KN^{-1} + 1)^{2l}.$$

By our choice of K and the stirling formula we have

$$1 + KN^{-1} \leqslant 1 + \left(\frac{k}{l!N}\right)^{1/(l+1)} = 1 + O(1/l).$$

Therefore,

$$G^*_l(K, N, k) \ll l!N^lK^{-l+1} + kN^{2l}K^{-2l},$$

and hence,

$$J_l(N, k) \ll K^{2l-1}(l!N^lK^{-l+1} + kN^{2l}K^{-2l}) \ll l(l!N^lK^l + kN^{2l}K^{-1}).$$

By our choice of K, we see that

$$l!N^lK^l \leqslant kN^{2l}K^{-1}$$

and also that for sufficiently large N,

$$K \geqslant \left(\frac{kN^l}{l!}\right)^{1/(l+1)} - 1 \geqslant \frac{N^{l/(l+1)}k^{1/(l+1)}}{2(l!)^{1/(l+1)}}.$$

Hence

$$J_l(N, k) \ll l(l!)^{1/(l+1)}N^{2l-1+1/(l+1)}k^{l/(l+1)} \ll l^2N^{2l-1+1/(l+1)}k^{l/(l+1)}.$$

This completes the proof of Lemma 1.

For positive integers $k, d, H, N < p$, we now consider double exponential sums of the form

$$W_a(d; H, N) = \sum_{h=1}^{H}\left|\sum_{n=1}^{N} e_p(ah(n!)^k)\right|^d.$$

Lemma 2 For any positive integer $l \geqslant 1$, we have

$$|W_a(d; H, N)| \leqslant (pHJ_d(N, k))^{1/2}.$$

Proof Applying the Hölder inequality we obtain

$$|W_a(d; H, N)|^2 \leqslant H\sum_{h=1}^{H}\left|\sum_{n=1}^{N} e_p(ah(n!)^k)\right|^{2l} \leqslant H\sum_{h=1}^{p}\left|\sum_{n=1}^{N} e_p(ah(n!)^k)\right|^{2d} = pHJ_d(N, k).$$

This completes the proof of Lemma 2.

2 Proof of Theorem 1

For some positive integers $k, s, l, H < p$, we denote by T the number of solutions of the congruence

$$\sum_{i=1}^{2s} h_i(n_{i1}!)^k + \cdots + (n_{il}!)^k + \sum_{i=1}^{2l}(m_i!)^k \equiv \lambda \pmod p,$$

where

$$1 \leqslant n_{1_1}, \cdots, n_{2s_l}, m_1, \cdots, m_{2l} \leqslant p - 1, \quad 1 \leqslant h_1, \cdots, h_{2s} \leqslant H.$$

By the identity (2), we have

$$T=\frac{1}{p}\sum_{a=0}^{p-1}\left(\sum_{h=1}^{H}\left(\sum_{n=1}^{p}e_p(ah(n!)^k)\right)^l\right)^{2s}\left(\sum_{m=1}^{p}e_p(a(m!)^k)\right)^{2l}\cdot e_p(-a\lambda).$$

Separating the term $H^{2s}p^{2sl+2l-1}$ corresponding to $a=0$, we derive

$$|T-H^{2s}p^{2sl+2l-1}|\leqslant\frac{1}{p}\sum_{a=1}^{p-1}\left(\sum_{h=1}^{H}\left|\sum_{n=1}^{p}e_p(ah(n!)^k)\right|^l\right)^{2s}\left|\sum_{m=1}^{p}e_p(a(m!)^k)\right|^{2l}.$$

Hence by Lemma 2 and Lemma 1, we have the following inequalities

$$|T-H^{2s}p^{2sl+2l-1}|\leqslant\frac{1}{p}(pHJ_l(p,k))^s\sum_{a=1}^{p-1}\left|\sum_{m=1}^{p}e_p(a(m!)^k)\right|^{2l}\leqslant p^sH^s(J_l(p,k))^{s+1}\ll H^sl^{2s+2}p^{2ls+2l-1+(s+1)/(l+1)}k^{l(s+1)/(l+1)}.$$

Therefore, the inequality

$$T\geqslant H^{2s}p^{2sl+2l-1}-CH^sl^{2s+2}p^{2ls+2l-1+(s+1)/(l+1)}k^{l(s+1)/(l+1)}$$

holds with some absolute constant $C>0$. Setting $l=[\log p]$, $s=[\log\log p]$ and $H=\left[e^6l^2k^{\frac{l(s+1)}{s(l+1)}}\right]$, we obtain that $T>0$. Thus every residue class λ modulo p can be represented by a sum of the same number $l_k(p)$ of factorials, where

$$l_k(p)\leqslant 2sH+2l\ll(\log p)^3\log\log p\cdot k^{(1+1/\log\log p)}.$$

This completes the proof of Theorem 1.

[References]

[1] Guy R K. Unsolved Problems in Number Theory[M]. 2nd ed. New York: Springer, 1994.

[2] Cobeli C, Vâjâitu M, Zaharescu A. The sequence $n!\pmod p$[J]. J Ramanujan Math Soc, 2000, 15(3): 135-154.

[3] Chen Yonggao, Dai Lixia. Congruences with factorials modulo p[J/OL]. Integers: Electronic J Comb Number Theory, 2006, 6: A21. http://www.integers-ejcnt.org/.

[4] Erdős P, Stewart C. On the greatest and least prime factors of $n!+1$[J]. J London Math Soc, 1976, 13(3): 513-519.

[5] Garaev M Z, Luca F, Shparlinski I E. Character sums and congruences with $n!$[J]. Trans Amer Math Soc, 2004, 356(12): 5089-5102.

[6] Garaev M Z, Luca F, Shparlinski I E. Sums and congruences with factorials[J]. J Reine Angew Math, 2005, 584(3): 29-44.

[7] Luca F, Stănică P. Products of factorials modulo p[J]. Colloq Math, 2003, 96(2): 191-205.

[8] Stewart C. On the greatest and least prime factors of $n!+1$ II[J]. Publ Math Debrecen, 2004, 65(3): 461-480.

[9] Vinogradov I M. Elements of Number Theory[M]. New York: Dover Publications, 1945.

[10] Garaev M Z, Luca F, Shparlinski I E. Waring problem with factorials[J]. Bull Austral Math Soc, 2005, 71(2): 259-264.

[责任编辑: 丁 蓉]