J. Number Theory 130(2010), no. 4, 930–935.

SOME CURIOUS CONGRUENCES MODULO PRIMES

Li-Lu Zhao and Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zhaolilu@gmail.com, zwsun@nju.edu.cn

Abstract. Let n be a positive odd integer and let $p > n+1$ be a prime. We mainly derive the following congruence:

$$\sum_{0<i_1<\cdots<i_n<p} \left(\frac{i_1}{3}\right) \frac{(-1)^{i_1}}{i_1\cdots i_n} \equiv 0 \pmod p.$$

1. Introduction

Simple congruences modulo prime powers are of interest in number theory. Here are some examples of such congruences:

(a) (Wolstenholme) $\sum_{k=1}^{p-1} 1/k \equiv 0 \pmod{p^2}$ for any prime $p > 3$.

(b) (Z. W. Sun [S02, (1.13)]) For each prime $p > 3$ we have

$$\sum_{0<k<p/2} \frac{3^k}{k} \equiv \sum_{0<k<p/6} \frac{(-1)^k}{k} \pmod p.$$

(c) (Z. W. Sun [S07, Theorem 1.2]) If p is a prime and $a, n \in \mathbb{N} = \{0, 1, 2, \ldots\}$, then

$$\frac{1}{\lfloor n/p^a \rfloor !} \sum_{k\equiv 0 \pmod{p^a}} (-1)^k \binom{n}{k} \left(-\frac{k}{p^a}\right)^{\lfloor n/p^a \rfloor} \equiv 1 \pmod p.$$

(d) (Z. W. Sun and R. Tauraso [ST, Corollary 1.1]) For any prime p and $a \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ we have

$$\sum_{k=0}^{p^a-1} \binom{2k}{k} \equiv \left(\frac{p^a}{3}\right) \pmod{p^2},$$

Key words and phrases. Congruences modulo a prime, p-adic integers, polynomials.

2010 *Mathematics Subject Classification.* Primary 11A07; Secondary 11A41, 11T06.

The second author is responsible for communications, and supported by the National Natural Science Foundation (grant 10871087) of China.

where $(\frac{\cdot}{3})$ is the Legendre symbol.

Let $p > 3$ be a prime. In 2008, during his study of $\sum_{k=0}^{p-1}\binom{2k}{k}$ modulo powers of p with R. Tauraso, the second author conjectured that

$$\sum_{0<i<j<k<p}\left(\frac{i}{3}\right)\frac{(-1)^i}{ijk} \equiv 0 \pmod{p}, \tag{1.1}$$

i.e.,

$$\sum_{\substack{0<i<j<k<p \\ i\equiv 1,2 \pmod{6}}}\frac{1}{ijk} \equiv \sum_{\substack{0<i<j<k<p \\ i\equiv 4,5 \pmod{6}}}\frac{1}{ijk} \pmod{p}. \tag{1.2}$$

In this paper we confirm the above conjecture of Sun by establishing the following general theorem.

Theorem 1.1. *Let $n \in \mathbb{Z}^+$ and let $p > n+1$ be a prime.*

(i) *If n is odd, then*

$$\sum_{\substack{0<i_1<\cdots<i_n<p \\ i_1\equiv 1,2 \pmod{6}}}\frac{1}{i_1\cdots i_n} \equiv \sum_{\substack{0<i_1<\cdots<i_n<p \\ i_1\equiv 4,5 \pmod{6}}}\frac{1}{i_1\cdots i_n} \pmod{p}. \tag{1.3}$$

(i) *If n is even, then*

$$\sum_{\substack{0<i_1<\cdots<i_n<p \\ i_1\equiv 0 \pmod{3}}}\frac{(-1)^{i_1}}{i_1\cdots i_n} \equiv 2\sum_{\substack{0<i_1<\cdots<i_n<p \\ i_1\equiv 2,3,4 \pmod{6}}}\frac{1}{i_1\cdots i_n} \pmod{p}. \tag{1.4}$$

We deduce Theorem 1.1 from our following result.

Theorem 1.2. *Let $n \in \mathbb{Z}^+$ and let $p > n+1$ be a prime. Set*

$$F_n(x) = \sum_{0<i_1<\cdots<i_n<p}\frac{x^{i_1}}{i_1\cdots i_n} \in \mathbb{Z}_p[x], \tag{1.5}$$

where $\mathbb{Z}_p$ denotes the integral ring of the p-adic field $\mathbb{Q}_p$. Then we have

$$F_n(1-x) \equiv (-1)^{n-1}F_n(x) \pmod{p}, \tag{1.6}$$

i.e., all the coefficients of $F_n(1-x) - (-1)^{n-1}F_n(x)$ are congruent to 0 modulo p.

In the next section we use Theorem 1.2 to prove Theorem 1.1. Section 3 is devoted to our proof of Theorem 1.2.

2. Theorem 1.2 implies Theorem 1.1

Proof of Theorem 1.1 via Theorem 1.2. (1.3) holds trivially when $p = 3$ and $n = 1$. Below we assume that $p > 3$.

Let ω be a primitive cubic root of unity in an extension field over $\mathbb{Q}_p$. Then, in the ring $\mathbb{Z}_p[\omega]$ we have the congruence

$$F_n(-\omega^2) = F_n(1+\omega) \equiv (-1)^{n-1}F_n(-\omega) \pmod{p}. \tag{2.1}$$

For $r \in \mathbb{Z}$ we set

$$S_r = \sum_{\substack{0<i_1<\cdots<i_n<p \\ i_1 \equiv r \pmod{6}}} \frac{1}{i_1 \cdots i_n}.$$

Clearly

$$\begin{aligned} F_n(-\omega) =& S_0 - \omega S_1 + \omega^2 S_2 - S_3 + \omega S_4 - \omega^2 S_5 \\ =& S_0 - S_3 - \omega(S_1 - S_4) + (-1-\omega)(S_2 - S_5) \\ =& S_0 - S_3 - S_2 + S_5 - \omega(S_1 + S_2 - S_4 - S_5). \end{aligned}$$

Similarly,

$$F_n(-\omega^2) = S_0 - S_3 - S_2 + S_5 - \omega^2(S_1 + S_2 - S_4 - S_5).$$

Thus

$$\begin{aligned} F_n(-\omega) + F_n(-\omega^2) =& 2(S_0 - S_2 - S_3 + S_5) + S_1 + S_2 - S_4 - S_5 \\ =& 2S_0 + S_1 - S_2 - 2S_3 - S_4 + S_5 \end{aligned}$$

and

$$F_n(-\omega) - F_n(-\omega^2) = (\omega^2 - \omega)(S_1 + S_2 - S_4 - S_5).$$

Note that $(\omega - 1)(\omega^2 - 1) = 3$ is relatively prime to p. Therefore, by (2.1), if $2 \nmid n$ then

$$S_1 + S_2 - S_4 - S_5 \equiv 0 \pmod{p}; \tag{2.2}$$

if $2 \mid n$ then

$$2S_0 + S_1 - S_2 - 2S_3 - S_4 + S_5 \equiv 0 \pmod{p}. \tag{2.3}$$

To conclude the proof we only need to show that (2.3) is equivalent to

$$S_0 - S_3 \equiv 2(S_2 + S_3 + S_4) \pmod{p}. \tag{2.4}$$

Recall that

$$x^{p-1}-1\equiv\prod_{j=1}^{p-1}(x-j)\equiv\prod_{i=1}^{p-1}\left(x-\frac{1}{i}\right)\pmod p$$

(cf. Proposition 4.1.1 of [IR, p. 40]). Comparing the coefficients of x^{p-1-n} we get that

$$\sum_{0<i_1<\cdots<i_n<p}\frac{1}{i_1\cdots i_n}\equiv 0\pmod p. \tag{2.5}$$

So $\sum_{r=0}^{5}S_r\equiv 0\pmod p$, which implies the equivalence of (2.3) and (2.4). We are done. □

3. Proof of Theorem 1.2

Proof of Theorem 1.2. We use induction on n.

Observe that

$$\sum_{i=1}^{p-1}\binom{p}{i}(-1)^{i-1}x^i=1+(-x)^p-\sum_{i=0}^{p}\binom{p}{i}(-x)^i=1-x^p-(1-x)^p.$$

For $i=1,\ldots,p-1$ clearly

$$\frac{(-1)^{i-1}}{p}\binom{p}{i}=\frac{(-1)^{i-1}}{i}\binom{p-1}{i-1}\equiv\frac{1}{i}\pmod p.$$

Thus

$$F_1(x)\equiv\frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}(-1)^{i-1}x^i=\frac{1-x^p-(1-x)^p}{p}\pmod p$$

and hence $F_1(1-x)\equiv F_1(x)\pmod p$ as desired. This proves (1.6) for $n=1$.

For the induction step we need to do some preparation. For

$$P(x)=\sum_{i=0}^{m}a_ix^i\in\mathbb{Z}_p[x],$$

we define its *formal derivative* by

$$\frac{\mathrm{d}}{\mathrm{d}x}P(x)=\sum_{0<i\leqslant m}ia_ix^{i-1}.$$

If $1 \leqslant m \leqslant p-1$ and $\frac{\mathrm{d}}{\mathrm{d}x}P(x) \equiv 0 \pmod p$, then $a_i \equiv 0 \pmod p$ for all $i = 1, \ldots, m$, and hence $P(x) \equiv a_0 = P(0) \pmod p$.

Now assume that $1 < n < p-1$ and $F_{n-1}(1-x) \equiv (-1)^{n-2}F_{n-1}(x) \pmod p$. Then

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}F_n(x) &= \sum_{0<i_1<\cdots<i_n<p} \frac{x^{i_1-1}}{i_2\cdots i_n} = \sum_{1<i_2<\cdots<i_n<p} \frac{1}{i_2\cdots i_n}\sum_{i_1=1}^{i_2-1} x^{i_1-1} \\ &= \sum_{0<i_2<\cdots<i_n<p} \frac{1}{i_2\cdots i_n}\cdot\frac{x^{i_2-1}-1}{x-1} \\ &= \frac{F_{n-1}(x)}{x(x-1)} - \frac{1}{x-1}\sum_{0<i_2<\cdots<i_n<p}\frac{1}{i_2\cdots i_n}\end{aligned}$$

and hence

$$\begin{aligned}&\frac{\mathrm{d}}{\mathrm{d}x}\left(F_n(1-x) - (-1)^{n-1}F_n(x)\right) \\ =& -\left(\frac{F_{n-1}(1-x)}{(1-x)(1-x-1)} - \frac{1}{(1-x)-1}\sum_{0<i_2<\cdots<i_n<p}\frac{1}{i_2\cdots i_n}\right) \\ &+ (-1)^n\left(\frac{F_{n-1}(x)}{x(x-1)} - \frac{1}{x-1}\sum_{0<i_2<\cdots<i_n<p}\frac{1}{i_2\cdots i_n}\right) \\ =& \frac{(-1)^nF_{n-1}(x) - F_{n-1}(1-x)}{x(x-1)} - \left(\frac{1}{x} + \frac{(-1)^n}{x-1}\right)\sum_{0<i_2<\cdots<i_n<p}\frac{1}{i_2\cdots i_n}.\end{aligned}$$

Combining this with the induction hypothesis and (2.5), we obtain

$$x(x-1)\frac{\mathrm{d}}{\mathrm{d}x}(F_n(1-x) - (-1)^{n-1}F_n(x)) \equiv 0 \pmod p.$$

For the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, it is well known that $\mathbb{F}_p[x]$ is a principal ideal domain. So we have

$$\frac{\mathrm{d}}{\mathrm{d}x}(F_n(1-x) - (-1)^{n-1}F_n(x)) \equiv 0 \pmod p$$

and hence

$$\begin{aligned}&F_n(1-x) - (-1)^{n-1}F_n(x) \\ \equiv& F_n(1) + (-1)^nF_n(0) = \sum_{0<i_1<\cdots<i_n<p}\frac{1}{i_1\cdots i_n} \equiv 0 \pmod p\end{aligned}$$

with the help of (2.5). This concludes the induction step and we are done. □

References

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, New York, 1990.

[S02] Z. W. Sun, *On the sum* $\sum_{k\equiv r\,(\mathrm{mod}\ m)}\binom{n}{k}$ *and related congruences*, Israel J. Math. **128** (2002), 135–156.

[S07] Z. W. Sun, *Combinatorial congruences and Stirling numbers*, Acta Arith. **126** (2007), 387–398.

[ST] Z. W. Sun and R. Tauraso, *On some new congruences for binomial coefficients*, preprint, arXiv:0709.1665.