Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2025, 12(2):1-7**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Congruences Concerning Quadratic Product Modulo Primes

Chen Ao, Shen Zhongyan*

Department of Mathematics, Zhejiang International Studies University, China
*Corresponding author: Email: huanchenszyan@163.com

Abstract: In this paper we use the properties of Bernoulli numbers, Bernoulli polynomials and mathematical induction to study and obtain the congruences of harmonic sums and quadratic product modulo primes.

Keywords: Congruences, Quadratic product, Legendre symbol

1. Introduction

The Bernoulli numbers $\{B_n\}$ and Bernoulli polynomials $\{B_n(x)\}$ are defined by the relations

$$B_0 = 1, \sum_{k=0}^{n-1} \binom{n}{k} B_k = 0 \ (n \geq 2) \text{ and } B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k} \ (n \geq 0).$$

It is well known that $B_{2k+1}=0$ for $k \geq 1$ and , $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, etc. Several researchers studied the congruences of Bernoulli numbers，see for example in [1-9].

Wilson's theorem [10] is expressed as follows, if p is a prime, then

$$\prod_{i=1}^{p-1} i \equiv (p-1)! \equiv -1 \pmod p.$$

Gauss[11] generalized Wilson's theorem from prime number modulus to composite number modulus. Let $m > 1$ be an arbitrary integer, then

$$\prod_{\substack{i=1 \\ (i,m)=1}}^{m} i = \begin{cases} -1 \pmod m, \text{if } m = 2,4, p^{\alpha}, 2p^{\alpha}; \\ 1 \pmod m, \ \textit{otherwise}, \end{cases}$$

where p is an odd prime.

By Wilson's theorem, we have

$$\prod_{i=1}^{\frac{p-1}{2}} i^2 = 1^2 \cdot 2^2 \cdots \left(\frac{p-1}{2}\right)^2 = \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

The congruence of $(\frac{p-1}{2})!$ modulo p , readers may refer to [12,13].

$$\prod_{i=1}^{\frac{p-1}{2}}(i+1)=2\times 3\times\cdots\times\frac{p+1}{2}\equiv\left(\frac{p+1}{2}\right)!\equiv\frac{1}{2}\left(\frac{p-1}{2}\right)!\,(\bmod p),$$

$$\prod_{i=2}^{\frac{p-1}{2}}(i-1)=1\times 2\times\cdots\times\left(\frac{p-3}{2}\right)\equiv\left(\frac{p-3}{2}\right)!\equiv -2\left(\frac{p-1}{2}\right)!\ \ (\bmod p),$$

$$\prod_{i=2}^{\frac{p-1}{2}}(i^2-1)=\prod_{i=2}^{\frac{p-1}{2}}(i-1)(i+1)\equiv\frac{p+1}{2p-2}\left[\left(\frac{p-1}{2}\right)!\right]^2\equiv\frac{1}{2}(-1)^{\frac{p-1}{2}}\ \ (\bmod p).$$

Similarly, for any given integer j, it is easy to obtain the congruences about

$$\prod_{i=1}^{\frac{p-1}{2}}(i-j),\ \prod_{i=1}^{\frac{p-1}{2}}(i+j),\ \prod_{i=1}^{\frac{p-1}{2}}(i^2-j^2)$$

modulo prime p. For any positive integers j,k, we will study the congruence about $\prod_{i=1}^{(p-1)/2}\left(i^{2j}\pm k\right)$ modulo prime p. Due to similar proofs, we will provide the congruence about $\prod_{i=1}^{(p-1)/2}\left(i^2+k\right)$ modulo prime p.

Theorem 1 Let prime $p>3$ and k be a positive integer we have

$$\prod_{i=1}^{\frac{p-1}{2}}(i^2+k)\equiv k^{\frac{p-1}{2}}+\left[\left(\frac{p-1}{2}\right)!\right]^2+\sum_{n=1}^{\frac{p-3}{2}}(-1)^{\frac{p-1}{2}-n-1}k^{\frac{p-1}{2}-n}\frac{\left(1-2^{1+2n}\right)B_{p-2-2n}}{2n+1}p\,(\bmod p^2).$$

Corollary 1 Let prime $p>3$, we have

$$\prod_{i=1}^{\frac{p-1}{2}}(i^2+k)\equiv\left(\frac{k}{p}\right)-\left(\frac{-1}{p}\right)(\bmod p),$$

where $\left(\frac{\bullet}{p}\right)$ denotes the Legendre symbol, see [10, 19, 20],

Corollary 2 Let prime $p>3$, we have

$$\prod_{i=1}^{\frac{p-1}{2}}(i^2+1)\equiv\begin{cases}0\ (\bmod p),\ p\equiv 1\ (\bmod 4),\\ 2\ (\bmod p),\ p\equiv 3\ (\bmod 4).\end{cases}$$

$$\prod_{i=1}^{\frac{p-1}{2}}(i^2+2)\equiv\begin{cases}0\ (\bmod p),\ p\equiv 1,3\ (\bmod 8),\\ -2\ (\bmod p),\ p\equiv 5\ (\bmod 8),\\ 2\ (\bmod p),\ p\equiv 7\ (\bmod 8).\end{cases}$$

2. Lemmas

Lemma 1[14] For any odd prime p, we have

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

Lemma 2[15,16] For positive integer m, we have

$$\sum_{r=0}^{n-1} r^m = \frac{B_{m+1}(n) - B_{m+1}}{m+1}.$$

Lemma 3[16,17] For positive integer m, we have

$$B_m(x+y) = \sum_{r=0}^{m} \binom{m}{r} B_{m-r}(x)\, y^r.$$

Lemma 4[16,18] For positive integer m, we have

$$B_m\left(\frac{1}{2}\right) = \left(2^{1-m} - 1\right) B_m.$$

Lemma 5 For any odd prime p, we have

$$\sum_{x=1}^{\frac{p-1}{2}} x^k \equiv \begin{cases} -\frac{1}{8}\left(\bmod p^2\right), & \text{if } k=1, \\ \frac{1-2^{k+1}}{2^k(k+1)} B_{k+1} \left(\bmod p^2\right), & \text{if } 1<k<p-1 \text{ and } k \text{ is odd}, \\ \frac{\left(1-2^{k-1}\right)B_k}{2^k} p \left(\bmod p^2\right), & \text{if } 1<k<p-1 \text{ and } k \text{ is even}. \end{cases}$$

Proof By Lemma 2, we have

$$\sum_{x=1}^{\frac{p-1}{2}} x^k = \sum_{x=1}^{\frac{p+1}{2}-1} x^k = \frac{B_{k+1}\left(\frac{p+1}{2}\right) - B_{k+1}}{k+1} = \frac{B_{k+1}\left(\frac{p}{2}+\frac{1}{2}\right) - B_{k+1}\left(\frac{1}{2}\right) + B_{k+1}\left(\frac{1}{2}\right) - B_{k+1}}{k+1}.$$

By Lemma 3 and Lemma 4, we obtain

$$\begin{aligned} \sum_{x=1}^{\frac{p-1}{2}} x^k &= \frac{\sum_{r=0}^{k+1}\binom{k+1}{r} B_{k+1-r}\left(\frac{1}{2}\right)\left(\frac{p}{2}\right)^r - B_{k+1}\left(\frac{1}{2}\right)}{k+1} + \frac{\left(2^{-k}-2\right)B_{k+1}}{k+1} \\ &\equiv B_k\left(\frac{1}{2}\right)\frac{p}{2} + \frac{\left(2^{-k}-2\right)B_{k+1}}{k+1} \\ &\equiv \frac{\left(1-2^{k-1}\right)B_k}{2^k} p + \frac{1-2^{k+1}}{2^k(k+1)} B_{k+1} \left(\bmod p^2\right). \end{aligned}$$

If $k=1$, then

$$\sum_{x=1}^{\frac{p-1}{2}} x = \frac{1-4}{2\times 2} B_2 \equiv -\frac{1}{8}\left(\bmod p^2\right).$$

If $1<k<p-1$ and k is odd, then $B_k = 0$, we have

$$\sum_{x=1}^{\frac{p-1}{2}} x^k \equiv \frac{1-2^{k+1}}{2^k(k+1)} B_{k+1} \left(\bmod p^2\right).$$

If $1<k<p-1$ and k is even, then $B_{k+1} = 0$, we have

$$\sum_{x=1}^{\frac{p-1}{2}} x^k \equiv \frac{\left(1-2^{k-1}\right)B_k}{2^k} p \ \left(\bmod p^2\right).$$

In conclusion, Lemma 5 is proved.

Lemma 6 Let prime $p>3$, $\alpha_1,\alpha_2,\cdots,\alpha_n \in Z^+$, $r=2(\alpha_1+\alpha_2+\cdots+\alpha_n)\le p-3$, we have

$$\sum_{\substack{1\le t_1,\cdots,t_n\le \frac{p-1}{2} \\ t_i\ne t_j}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_n^{2\alpha_n} \equiv (-1)^{n-1}(n-1)!\frac{\left(1-2^{r-1}\right)B_r}{2^r} p \left(\bmod p^2\right) \tag{1}$$

and

$$\sum_{1\le t_1<t_2\cdots<t_n\le \frac{p-1}{2}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_n^{2\alpha_n} \equiv (-1)^{n-1}\frac{\left(1-2^{r-1}\right)B_r}{n2^r} p \left(\bmod p^2\right). \tag{2}$$

Proof When $n=1$ and $r=2\alpha_1$, by Lemma 5, we obtain

$$\sum_{1\le t_1\le \frac{p-1}{2}} t_1^{2\alpha_1} = \frac{\left(1-2^{r-1}\right)B_r}{2^r} p \ (\bmod p^2).$$

(1) holds. Suppose that (1) holds when $n=k-1$, then we get

$$\sum_{\substack{1\le t_1,\cdots,t_{k-1}\le \frac{p-1}{2} \\ t_i\ne t_j}} t_1^{2\beta_1}t_2^{2\beta_2}\cdots t_{k-1}^{2\beta_{k-1}} \equiv (-1)^{k-2}(k-2)!\frac{\left(1-2^{r-1}\right)B_r}{2^r} p \left(\bmod p^2\right), \tag{3}$$

where $\beta_1,\beta_2,\cdots,\beta_{k-1}\in Z^+$, $r=2\left(\beta_1+\beta_2+\cdots+\beta_{k-1}\right)$. When $n=k$,

$$\sum_{\substack{1\le t_1,\cdots t_k\le \frac{p-1}{2} \\ t_i\ne t_j}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_k^{2\alpha_k} = \sum_{\substack{1\le t_1,\cdots t_{k-1}\le \frac{p-1}{2} \\ t_i\ne t_j}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_{k-1}^{2\alpha_{k-1}}\left(\sum_{t_k=1}^{\frac{p-1}{2}} t_k^{2\alpha_k} - t_1^{2\alpha_k} - \cdots - t_{k-1}^{2\alpha_k}\right)$$

$$= \sum_{\substack{1\le t_1,\cdots t_{k-1}\le \frac{p-1}{2} \\ t_i\ne t_j}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_{k-1}^{2\alpha_{k-1}}\sum_{t_k=1}^{\frac{p-1}{2}} t_k^{2\alpha_k} - \sum_{\substack{1\le t_1,\cdots t_{k-1}\le \frac{p-1}{2} \\ t_i\ne t_j}} t_1^{2\alpha_1+2\alpha_k}t_2^{2\alpha_2}\cdots t_{k-1}^{2\alpha_{k-1}} - \cdots$$

$$- \sum_{\substack{1\le t_1,\cdots t_{k-1}\le \frac{p-1}{2} \\ t_i\ne t_j}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_{k-1}^{2\alpha_{k-1}+2\alpha_k}. \tag{4}$$

By equation (3) and Lemma 5, we have

$$\sum_{\substack{1\le t_1,\cdots t_{k-1}\le \frac{p-1}{2} \\ t_i\ne t_j}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_{k-1}^{2\alpha_{k-1}}\sum_{t_k=1}^{\frac{p-1}{2}} t_k^{2\alpha_k} \equiv 0\left(\bmod p^2\right).$$

Where equations (3) and (4) can be simplified as

$$\sum_{\substack{1\le t_1,\cdots t_k\le\frac{p-1}{2}\\ t_i\ne t_j}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_k^{2\alpha_k} \equiv -(k-1)\sum_{\substack{1\le t_1,\cdots t_{k-1}\le\frac{p-1}{2}\\ t_i\ne t_j}} t_1^{2\alpha_1+2\alpha_k}t_2^{2\alpha_2}\cdots t_{k-1}^{2\alpha_{k-1}}$$

$$\equiv -(k-1)(-1)^{k-2}(k-2)!\frac{\left(1-2^{r-1}\right)B_r}{2^r}p$$

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

In summary, equation (1) is proven.

Due to

$$\sum_{\substack{1\le t_1,\cdots,t_n\le\frac{p-1}{2}\\ t_i\ne t_j}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_n^{2\alpha_n} \equiv n!\sum_{1\le t_1<t_2\cdots<t_n\le\frac{p-1}{2}} t_1^{2\alpha_1}t_2^{2\alpha_2}\cdots t_n^{2\alpha_n} \left(\bmod p^2\right),$$

By (1)， we obtain that (2) holds.

3. Proof of the Theorems

Proof of Theorem 1

Expand the continuous product we obtain

$$\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+k\right)=k^{\frac{p-1}{2}}+\prod_{i=1}^{\frac{p-1}{2}}i^2+k^{\frac{p-3}{2}}\sum_{1\le i_1\le\frac{p-1}{2}}i_1^2+k^{\frac{p-5}{2}}\sum_{1\le i_1<i_2\le\frac{p-1}{2}}i_1^2i_2^2+\cdots$$
$$+k^{\frac{p-1-2n}{2}}\sum_{1\le i_1<\cdots<i_n\le\frac{p-1}{2}}i_1^2i_2^2\cdots i_n^2+\cdots. \tag{5}$$

Let $\alpha_1=\alpha_2=\cdots=\alpha_n=1$ in Lemma 6, we can get

$$\sum_{1\le t_1<\cdots<t_{\frac{p-1}{2}-n}\le\frac{p-1}{2}}\frac{1}{t_1^2t_2^2\cdots t_{\frac{p-1}{2}-n}^2}\equiv(-1)^{\frac{p-1}{2}-n-1}\frac{\left(1-2^{p-2-2n}\right)B_{p-2-2n}}{(\frac{p-1}{2}-n)2^{p-1-2n}}p\left(\bmod p^2\right). \tag{6}$$

Substitute（6）into（5）， and by Euler's Theorem, we have

$$\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+k\right)\equiv k^{\frac{p-1}{2}}+\left[\left(\frac{p-1}{2}\right)!\right]^2+\sum_{n=1}^{\frac{p-3}{2}}k^{\frac{p-1}{2}-n}(-1)^{\frac{p-1}{2}-n-1}\frac{\left(1-2^{p-2-2n}\right)B_{p-2-2n}}{(\frac{p-1}{2}-n)2^{p-1-2n}}p$$

$$\equiv k^{\frac{p-1}{2}}+\left[\left(\frac{p-1}{2}\right)!\right]^2+\sum_{n=1}^{\frac{p-3}{2}}(-1)^{\frac{p-1}{2}-n-1}k^{\frac{p-1}{2}-n}\frac{\left(1-2^{1+2n}\right)B_{p-2-2n}}{2n+1}p \pmod{p^2}.$$

We completed the proof of Theorem 1.

Proof of Corollary 1

By lemma 1 and $k^{\frac{p-1}{2}}\equiv\left(\frac{k}{p}\right)(\bmod p)$ in Theorem 1, we get

$$\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+k\right)\equiv k^{\frac{p-1}{2}}+\left[\left(\frac{p-1}{2}\right)!\right]^2$$
$$\equiv k^{\frac{p-1}{2}}+(-1)^{\frac{p+1}{2}}$$
$$\equiv k^{\frac{p-1}{2}}-(-1)^{\frac{p-1}{2}}$$
$$\equiv\left(\frac{k}{p}\right)-\left(\frac{-1}{p}\right)(\bmod p).$$

We completed the proof of Corollary 1.

Proof of Corollary 2

When $k=1$ in Corollary 1, we have

$$\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+1\right)\equiv 1-\left(\frac{-1}{p}\right)\quad(\bmod p).$$

When $p\equiv 1\,(\bmod 4)$, we have $\left(\frac{-1}{p}\right)=1$, $\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+1\right)\equiv 0\quad(\bmod p)$.

When $p\equiv 3\,(\bmod 4)$, we have $\left(\frac{-1}{p}\right)=-1$, $\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+1\right)\equiv 2\quad(\bmod p)$.

When $k=2$ in Corollary 1, we have

$$\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+2\right)\equiv\left(\frac{2}{p}\right)-\left(\frac{-1}{p}\right)\quad(\bmod p).$$

When $p\equiv 1\,(\bmod 8)$, we have $\left(\frac{2}{p}\right)=1$, $\left(\frac{-1}{p}\right)=1$ and $\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+2\right)\equiv 0\quad(\bmod p)$.

When $p\equiv 3\,(\bmod 8)$, we have $\left(\frac{2}{p}\right)=-1$, $\left(\frac{-1}{p}\right)=-1$ and $\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+2\right)\equiv 0\quad(\bmod p)$.

When $p\equiv 5\,(\bmod 8)$, we have $\left(\frac{2}{p}\right)=-1$ and $\left(\frac{-1}{p}\right)=1$, then $\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+2\right)\equiv -2\quad(\bmod p)$.

When $p\equiv 7\,(\bmod 8)$, we have $\left(\frac{2}{p}\right)=1$ and $\left(\frac{-1}{p}\right)=-1$, then

$$\prod_{i=1}^{\frac{p-1}{2}}\left(i^2+2\right)\equiv 2\quad(\bmod p).$$

We completed the proof of Corollary 2.

4. Conclusion

In this work we use the properties of Bernoulli numbers, Bernoulli polynomials and mathematical induction to prove Lemma 5 and Lemma 6. In the existing congruences, the variables of multiple harmonic sums are all between 1 and $p-1$, but the variables of multiple harmonic sums we proved are between 1 and $(p-1)/2$, which is an innovation. Then we use Lemma 6 and Legendre symbols to prove Theorem 1 and corollaries, the results of congruences are also quite beautiful.

References

[1]. T. Cai, Z. Shen, L. Jia (2017). A congruence involving harmonic sums modulo pαq β, Int. J. Number Theory, 13(5): 1083–1094.

[2]. C.-G. Ji (2005). A simple proof of a curious congruence by Zhao, Proc. Amer. Math. Soc., 133(12): 3469–3472.

[3]. M. McCoy, K. Thielen, L. Wang, J. Zhao (2017). A family of super congruences involving multiple harmonic sums, Int. J. Number Theory, 13 (1): 109–128.

[4]. Z. Shen, T. Cai (2018). Congruences involving alternating harmonic sums modulo p αq β, Math. Slovaca, 68 (5): 975–980.

[5]. L. Wang (2015). A new curious congruence involving multiple harmonic sums, J. Number Theory, 154:16–31.

[6]. L. Wang, T. Cai (2014). A curious congruence modulo prime powers, J. Number Theory, 144: 15–24.

[7]. B. Xia,T. Cai(2010). Bernoulli numbers and congruences for harmonic sums, Int. J. Number Theory, 6(4): 849–855.

[8]. J. Zhao (2007). Bernoulli numbers, Wolstenholme's theorem, and p 5 variations of Lucas' theorem, J. Number Theory, 123(1): 18–26.

[9]. X. Zhou, T. Cai (2007). A generalization of a curious congruence on harmonic sums, Proc. Amer. Math. Soc., 135(5): 1329–1333.

[10]. T. X. Cai2021. A Modern Introduction to Classical Number Theory. World Scientific, Singapore.

[11]. C. F. Gauss1986. Disquisitiones Arithmeticae, Springer-Verlag.

[12]. S. Chowla (1961). On the class number of real quadratic field, Proc. Natl. Acad. Sci. USA, 47:878.

[13]. Z. W. Sun (2019). On some determinants with Legendre symbol entries, Finite Fields Appl., 56:285–307.

[14]. L. J. Mordell (1961). The congruence [J]. The American Mathematical Monthly, 68(2): 145-146.

[15]. T. X. Cai, X. D. Fu, X. Zhou (2007). A congruence involving the quotients of Euler and its applications (II). Acta Arith., 130: 203-214.

[16]. K. Ireland, M. Rosen (1982). A Classical Introduction to Modern Number Theory, Springer, New York,239-248.

[17]. W. Magnus, F. Oberhettinger, R. P. Soni (1966). Formulas and Theorems for the Special Functions of Mathematical Physics, 3rd ed., Springer-Verlag, New York, 25-32.

[18]. A. Granville, Z. W. Sun (1996). Values of Bernoulli polynomials, Pacific J. Math. ,172:117-137.

[19]. George E. Andrews (1994). Number Theory. Dover Publications, Inc. New York.

[20]. Kenneth Ireland, Michael Rosen (1990). A Classical Introduction to Modern Number Theory, (2nd edition), Springer, New York, 64.