S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ
ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том xx, стр. xxx–xxx (202x) УДК 511.1
DOI 10.33048/semi.20xx.xx.xxx MSC 11A07

A REMARK ON SCHWINDT'S CONGRUENCE

F. Z. BENSACI, L. KHALDI

Abstract. In this paper, using some congruences involving the Bernoulli polynomials related to rational values, we present a generalized version of Schwindt's congruence.

Keywords: Congruence, Bernoulli polynomial, Fermat's little theorem, Fermat's last theorem.

1. Introduction

In 1637, Fermat affirmed in the margin of a book gathering the complete work of Diophantus, that it is not possible to find for an integer $n > 2$, nonzero integers $x,\ y$ and z such that $x^n + y^n = z^n$. This is also equivalent to say that it is not possible to find for an integer $n > 2$, nonzero integers $x,\ y$ and z such that $x^n + y^n + z^n = 0$. Over time this statement came to be known as Fermat's last theorem. Wieferich primes were first introduced in 1909 in relation to the first case of Fermat's last theorem. In the paper [5] Wieferich proved that, if p is an odd prime and $x^p + y^p + z^p = 0$ has a solution in integers x, y, z with $p \nmid xyz$, then $2^{p-1} \equiv 1 \pmod{p^2}$.

Bensaci, F. Z., Khaldi. L.,

Received .

In 1924, Vandiver [4] proved that if for an odd prime number p, the equation $x^n + y^n + z^n = 0$, admits a solution in integers x, y and z all of them coprime to p, then

$$\sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} \frac{1}{r^2} \equiv 0 \pmod{p},$$

where $\lfloor x \rfloor = \max\{k \in \mathbb{Z} \ / \ k \leq x\}$.

In 1933, Schwindt [3] proved for $p \geq 7$ the following congruence

$$5 \sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} \frac{1}{r^2} \equiv \sum_{r=1}^{\lfloor \frac{p}{6} \rfloor} \frac{1}{r^2} \pmod{p}. \tag{1}$$

Recall that a p-integer is a rational number whose denominator is coprime to p, and in the ring of p-integers denoted $\mathbb{Z}_{(p)}$ we write $\frac{a}{b} \equiv \frac{c}{d}$ (mod p) when $ad - bc \equiv 0 \pmod{p}$ in $\mathbb{Z}$.

The nth Bernoulli polynomial $B_n(x)$, is defined by means of the generating function [1, p. 804] as follows:

$$\sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!} = \frac{te^{xt}}{e^t - 1}, \quad (|t| < 2\pi). \tag{2}$$

The first Bernoulli polynomials are

$$B_0(x) = 1, \ B_1(x) = x - \frac{1}{2}, \ B_2(x) = x^2 - x + \frac{1}{6}, \ B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x,$$
$$B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30}, \ B_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x.$$

For another properties (see, [1, p. 804]), for example, we have the well-known symmetric formula

$$B_n(1-x) = (-1)^n B_n(x), \quad \text{for all } n \geq 0. \tag{3}$$

The next theorem presents a generalization of (1).

Theorem 1. *Let m be a positive integer and $p \geq 7$ be a prime number. If $p \neq m+1$ and $p \neq 2m+1$, then*

$$(1 + 2^{2m}) \sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} \frac{1}{r^{2m}} \equiv \sum_{r=1}^{\lfloor \frac{p}{6} \rfloor} \frac{1}{r^{2m}} \pmod{p}.$$

In particular, for $m = 1$ we obtain Schwindt's congruence

$$5 \sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} \frac{1}{r^2} \equiv \sum_{r=1}^{\lfloor \frac{p}{6} \rfloor} \frac{1}{r^2} \pmod{p}, \quad (p \geq 7).$$

The following result is a consequence of Theorem 1.

Theorem 2. *Let x, y and z be integers coprime to p, satisfying the equation*

$$x^{mp}+y^{mp}+z^{mp}=0, \quad \textit{for all } m\geq 1.$$

then, we have for every $m\geq 1$

$$\sum_{r=1}^{\lfloor \frac{p}{3}\rfloor}\frac{1}{r^{2m}}\equiv\sum_{r=1}^{\lfloor \frac{p}{6}\rfloor}\frac{1}{r^{2m}}\equiv 0 \pmod{p}.$$

In the following section, we present some congruences between Bernoulli polynomials and rational numbers in order to use them in the proof of Theorem 1.

2. Congruences involving $B_n\left(\frac{1}{3}\right)$ and $B_n\left(\frac{1}{6}\right)$

The following lemma can be found in Emma Lehmer's famous paper [2, Congruence (7)].

Lemma 1. *Let n be a non-negative integer and p be a prime number such that $p>n\geq 1$. For any integer $k\geq 2$ with $2k\not\equiv 2 \pmod{p-1}$, we have*

$$\sum_{r=1}^{\lfloor \frac{p}{n}\rfloor}(p-nr)^{2k}\equiv\frac{n^{2k}}{2k+1}\left(\frac{2k+1}{n}pB_{2k}-B_{2k+1}\left(\frac{s}{n}\right)\right) \pmod{p^3}.$$

where $s=p-n\lfloor\frac{p}{n}\rfloor$ is the remainder of the Euclidean division of p by n.

Lemma 2. *For any integer $n\geq 0$, we have*

$$B_n\left(\frac{1}{6}\right)=((-1)^{n-1}+2^{1-n})B_n\left(\frac{1}{3}\right).$$

Proof. Denoting by $[t^n]\left(P(t)\right)$ the coefficient of t^n in the polynomial $P(t)$. Using Relation (2), $B_n\left(\frac{1}{6}\right)$ can be written as follows:

$$B_n\left(\frac{1}{6}\right)=[t^n]\left(\sum B_n\left(\frac{1}{6}\right)\frac{t^n}{n!}\right)=[t^n]\left(\frac{te^{\frac{1}{6}t}}{e^t-1}\right). \tag{4}$$

Note that we have

$$\begin{aligned}\frac{te^{\frac{1}{6}t}}{e^t-1} &= \frac{te^{\frac{2}{3}t}}{e^{\frac{t}{2}}-1}\frac{e^{-\frac{1}{2}t}}{e^{\frac{t}{2}}+1} \\ &= \frac{te^{\frac{2}{3}t}}{e^{\frac{t}{2}}-1}\left(\frac{-1}{e^{\frac{t}{2}}+1}+e^{-\frac{1}{2}t}\right) \\ &= \frac{-te^{\frac{2}{3}t}}{e^t-1}+\frac{te^{\frac{1}{6}t}}{e^{\frac{t}{2}}-1} \\ &= \frac{-(-t)e^{-\frac{1}{3}t}}{e^{-t}-1}+2\frac{\frac{t}{2}e^{\frac{t}{2}\frac{1}{3}}}{e^{\frac{t}{2}}-1}. \qquad (5)\end{aligned}$$

From (4) and (5), we get

$$B_n\left(\frac{1}{6}\right) = ((-1)^{n-1}+2^{1-n})B_n\left(\frac{1}{3}\right).$$

Which is required. □

Theorem 3. *Let p be an odd prime and n, m two positive integers with $p > n$. Then we have*

$$\sum_{r=1}^{\lfloor \frac{p}{n} \rfloor} r^{p-2m-1} \equiv \frac{1}{2m}B_{p-2m}\left(\frac{s}{n}\right) \pmod{p}. \tag{6}$$

where $s = p - n\lfloor \frac{p}{n} \rfloor$.

Proof. Replacing $2k$ by $p-2m-1$ in Lemma 1 and writing the congruence modulo p, we obtain

$$\sum_{r=1}^{\lfloor \frac{p}{n} \rfloor} r^{p-2m-1} \equiv \frac{1}{p-2m}\left(\frac{p-2m}{n}pB_{p-2m-1} - B_{p-2m}\left(\frac{s}{n}\right)\right) \pmod{p}.$$

Here in $\mathbb{Z}_{(p)}$ we have $pB_{p-2m-1} \equiv 0 \pmod{p}$ because $p-1$ does not divide $p-2m-1$. Moreover, n is coprime to p, we conclude that we have

$$\sum_{r=1}^{\lfloor \frac{p}{n} \rfloor} r^{p-2m-1} \equiv \frac{1}{2m}B_{p-2m}\left(\frac{s}{n}\right) \pmod{p}.$$

Just notice that

$$\frac{1}{p-2m} \equiv -\frac{1}{2m} \pmod{p}.$$

This completes the proof. □

Corollary 1. *Let m be a positive integer and $p \geq 7$ be a prime number. If $p \neq m+1$ and $p \neq 2m+1$, then*

$$\sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} r^{p-2m-1} \equiv \begin{cases} \frac{1}{2m} B_{p-2m}\left(\frac{1}{3}\right) \pmod{p}, & \textit{if } p \equiv 1 \pmod{3}; \\ -\frac{1}{2m} B_{p-2m}\left(\frac{1}{3}\right) \pmod{p}, & \textit{if } p \equiv 2 \pmod{3}, \end{cases}$$

and

$$\sum_{r=1}^{\lfloor \frac{p}{6} \rfloor} r^{p-2m-1} \equiv \begin{cases} \frac{1}{2m} B_{p-2m}\left(\frac{1}{6}\right) \pmod{p}, & \textit{if } p \equiv 1 \pmod{6}; \\ -\frac{1}{2m} B_{p-2m}\left(\frac{1}{6}\right) \pmod{p}, & \textit{if } p \equiv 5 \pmod{6}. \end{cases}$$

Proof. Let us denote by s the remainder of the Euclidean division of p by 3, so

$$p = 3q + s,$$

with $q \in \mathbb{N}$ and $s = 1$ or 2. We then deduce from (6)

$$\sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} r^{p-2m-1} \equiv \frac{1}{2m} B_{p-2m}\left(\frac{s}{3}\right) \pmod{p}. \tag{7}$$

We denote by ℓ the remainder of the Euclidean division of p by 6. Then we have

$$p = 6q' + \ell,$$

with $q \in \mathbb{N}$ and $\ell = 1$ or 5 (because p is an odd prime, so we have $\ell \notin \{0, 2, 3, 4\}$). We then deduce from (6)

$$\sum_{r=1}^{\lfloor \frac{p}{6} \rfloor} r^{p-2m-1} \equiv \frac{1}{2m} B_{p-2m}\left(\frac{s}{6}\right) \pmod{p}. \tag{8}$$

Noting that when $\ell = 1$, then $p = 6q' + 1 = 3(2q') + 1 = 3q + s$, so $s = 1$ and when $\ell = 5$, then $p = 6q' + 5 = 3(2q' + 1) + 2$ hence $s = 2$. This allows us to say

- If $\ell = 1$, then $s = 1$, so, we get

$$\sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} r^{p-2m-1} \equiv \frac{1}{2m} B_{p-2m}\left(\frac{1}{3}\right) \pmod{p},$$

and

$$\sum_{r=1}^{\lfloor \frac{p}{6} \rfloor} r^{p-2m-1} \equiv \frac{1}{2m} B_{p-2m}\left(\frac{1}{6}\right) \pmod{p}.$$

- If $\ell = 5$, then $s = 2$ and with the help of (3), we have

$$\begin{aligned}\sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} r^{p-2m-1} &\equiv \frac{1}{2m} B_{p-2m}\left(\frac{2}{3}\right)\\ &\equiv -\frac{1}{2m} B_{p-2m}\left(\frac{1}{3}\right) \pmod{p},\end{aligned}$$

and

$$\begin{aligned}\sum_{r=1}^{\lfloor \frac{p}{6} \rfloor} r^{p-2m-1} &\equiv \frac{1}{2m} B_{p-2m}\left(\frac{5}{6}\right)\\ &\equiv -\frac{1}{2m} B_{p-2m}\left(\frac{1}{6}\right) \pmod{p}.\end{aligned}$$

Which is required. □

Lemma 3. *Let m be a positive integer and $p \geq 3$ be a prime number, we have*

$$B_{p-2m}\left(\frac{1}{6}\right) \equiv (1 + 2^{2m}) B_{p-2m}\left(\frac{1}{3}\right) \pmod{p}.$$

Proof. Applying Lemma 2 for $n = p - 2m$ and using Fermat's little theorem, we get

$$\begin{aligned}B_{p-2m}\left(\frac{1}{6}\right) &= (1 + 2^{1+2m-p}) B_{p-2m}\left(\frac{1}{3}\right)\\ &= \left(1 + \frac{2^{2m}}{2^{p-1}}\right) B_{p-2m}\left(\frac{1}{3}\right)\\ &\equiv (1 + 2^{2m}) B_{p-2m}\left(\frac{1}{3}\right) \pmod{p}. \qquad (9)\end{aligned}$$

Which is the desired result. □

3. Proof of Theorem 1

From (7), (8) and (9) we have

$$(1 + 2^{2m}) \sum_{r=1}^{\lfloor \frac{p}{3} \rfloor} r^{p-2m-1} \equiv \sum_{r=1}^{\lfloor \frac{p}{6} \rfloor} r^{p-2m-1} \pmod{p}. \qquad (10)$$

The proof of Theorem 1 is an immediate consequence of Relation (10), it suffices only to note that for $1 \leq r < p$, and use Fermat's little theorem to obtain

$$r^{p-2m-1} \equiv \frac{1}{r^{2m}} \pmod{p}.$$

Hence the proof is complete.

References

[1] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, National Bureau of Standards, 1964.

[2] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math.* **39** (1938), 350–360.

[3] H. Schwindt, Eine Bemerkung zu einem Kriterium von H. S. Vandiver, *Jahresbericht d. Deutschen Math. Verein* **43** (1933-34), 229–231.

[4] H. S. Vandiver, A new type of criteria for the first case of Fermat's last theorem, *Ann. of Math.* **26** (1924), 88–94.

[5] A. Wieferich, Zum letzten Fermat'schen Theorem, *J. Reine Angew. Math.* **136** (1909), 293–302.

Fatima Zohra Bensaci
Faculty of Mathematics,
LA3C, USTHB,
Algiers, Algeria
Email address: fbensacif@usthb.dz

Laala Khaldi
LIM Laboratory,
Department of Mathematics,
University of Bouira, 10000 Bouira,
Algeria
Email address: l.khaldi@univ-bouira.dz