A CONGRUENCE FOR THE FERMAT QUOTIENT MODULO p^3

S. Khongsit
Department of Mathematics, Lady Keane College, Shillong, Meghalaya, India
shailanstar@gmail.com

P.K. Saikia
Department of Mathematics, North Eastern Hill University, Shillong, Meghalaya, India
promode4@gmail.com

Received: 4/3/15, Revised: 3/30/16, Accepted: 7/1/16, Published: 7/22/16

Abstract

For a prime $p > 3$ and the Fermat quotient $q_p(2) = (2^{p-1} - 1)/p$, Z.H. Sun proved that

$$\sum_{k=1}^{p-1} \frac{2^k}{k} + 2q_p(2) \equiv -\frac{7}{12}p^2 B_{p-3} \pmod{p^3},$$

where B_n is the n-th Bernoulli number. In this note, we give an elementary proof of this congruence.

1. Introduction

Fermat quotients, integers of the form $(a^{p-1} - 1)/p$ for integers a relatively prime to a prime p, have been of interest since the time of Eisenstein and Glaisher in the nineteenth century. Glaisher, in [1], proved that for a prime $p \geq 3$,

$$q_p(2) \equiv -\frac{1}{2}\sum_{k=1}^{p-1} \frac{2^k}{k} \pmod{p}.$$

Z.H. Sun, in [7] (See Theorem 4.1), used Mirimanoff polynomials to generalize Glaisher's congruence as follows:

$$\sum_{k=1}^{p-1} \frac{2^k}{k} + 2q_p(2) \equiv -\frac{7}{12}p^2 B_{p-3} \pmod{p^3}. \tag{1}$$

In this paper we give an elementary proof of the preceding congruence by using the following identity:

$$\sum_{k=1}^{n} \frac{(1-x)^k}{k} = \sum_{k=1}^{n} \binom{n}{k} \frac{(-1)^k}{k} (x^k - 1), \tag{2}$$

which holds for any positive integer n and any real number x. This identity appears as an exercise in [5] ; W. Kohnen [4] used it to derive a simple congruence modulo a prime p.

We shall also require some elementary properties of both Bernoulli numbers and harmonic numbers. Recall that Bernoulli numbers B_n, which are defined in terms of the relation

$$B_0 = 1, \qquad \sum_{i=0}^{m-1} \binom{m}{i} B_i = 0 \quad \text{for all} \quad m \geq 2,$$

satisfy the congruence

$$1^k + 2^k + ... + (p-1)^k \equiv pB_k \pmod{p^2} \tag{3}$$

for an odd prime p and positive even integer k such that $(p-1) \nmid k$; see Corollary to Proposition 15.2.2 in [3].

Harmonic numbers H_n, and more generally $H_{n,m}$, are defined respectively as

$$H_0 = 0, \qquad H_n = \sum_{i=1}^{n} \frac{1}{i} \ ,$$

and

$$H_{n,m} = \sum_{i=1}^{n} \frac{1}{i^m}$$

for any positive integers n and m. For a prime $p > 3$, one has the following well-known congruences:

$$H_{p-1} \equiv 0 \pmod{p^2} \quad \text{and} \quad H_{p-1,2} \equiv 0 \pmod{p}, \tag{4}$$

the first of which is known as Wolstenholme's congruence. In Lemma 2 of the following section, generalizations of these two congruences, modulo p^2 and p^3, are established.

2. Preliminary Results

In this section, we present preliminary results, mostly congruences involving harmonic numbers, which will be required for our proof of Sun's generalization of Glaisher's congruence.

Lemma 1. *For an odd prime p and for any integer $k = 1, 2, ..., p-1$, we have*

$$\binom{p-1}{k} \equiv (-1)^k\Big(1 - pH_k + p^2 \sum_{1\le i<j\le k} \frac{1}{ij}\Big) \pmod{p^3} \tag{5}$$

$$\equiv (-1)^k\big(1 - pH_k + (p^2/2)(H_k^2 - H_{k,2})\big) \pmod{p^3}. \tag{6}$$

Proof. See Lemma 2.9 in [7]. □

Congruences in the next lemma are special cases of certain general congruences obtained by Z.H. Sun in [6]. We provide direct proofs of these using elementary ideas.

Lemma 2. *For a prime $p > 3$,*

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^3} \equiv -2B_{p-3} \pmod{p}, \tag{7}$$

$$\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv \frac{2}{3}pB_{p-3} \pmod{p^2}, \tag{8}$$

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^2} \equiv \frac{7}{3}pB_{p-3} \pmod{p^2}, \tag{9}$$

$$\sum_{k=1}^{p-1} \frac{1}{k} \equiv -\frac{1}{3}p^2B_{p-3} \pmod{p^3}. \tag{10}$$

Proof. For any $j \in S = \{1, 2, ..., p-1\}$, one has $2j = pq_j + r_j$, where

$$q_j = \Big\lfloor \frac{2j}{p} \Big\rfloor = \begin{cases} 0 & \text{if } 1 \le j \le (p-1)/2 \\ 1 & \text{if } (p+1)/2 \le j \le p-1 \end{cases}.$$

Observe that, as $2j \equiv r_j \pmod{p}$, for any positive integer k,

$$(2j)^k \equiv r_j^k + kpq_j(2j)^{k-1} \pmod{p^2}.$$

It is also clear that r_j varies from 1 to $p-1$ in S as j does. Therefore, we see

that

$$\begin{aligned}\sum_{j=1}^{p-1} 2^k j^k &\equiv \sum_{j=1}^{p-1} j^k + kp\sum_{j=1}^{p-1} q_j (2j)^{k-1} \pmod{p^2} \\ &\equiv \sum_{j=1}^{p-1} j^k + pk2^{k-1} \sum_{j=(p+1)/2}^{p-1} j^{k-1} \pmod{p^2} \\ &\equiv \sum_{j=1}^{p-1} j^k + pk2^{k-1} \sum_{j=1}^{(p-1)/2} (p-j)^{k-1} \pmod{p^2} \\ &\equiv \sum_{j=1}^{p-1} j^k + pk2^{k-1}(-1)^{k-1} \sum_{j=1}^{(p-1)/2} j^{k-1} \pmod{p^2}.\end{aligned}$$

The last of the preceding congruences can be rewritten as

$$(2^k - 1)\sum_{j=1}^{p-1} j^k \equiv pk2^{k-1}(-1)^{k-1} \sum_{j=1}^{(p-1)/2} j^{k-1} \pmod{p^2}, \tag{11}$$

which we shall now simplify for $k = p-3$. Since $k = p-3$ is even and $(p-1) \nmid p-3$, congruence (3) for Bernoulli numbers implies that

$$\sum_{j=1}^{p-1} j^{p-3} \equiv pB_{p-3} \pmod{p^2}.$$

On the other hand, for an integer a prime to p, a^{p-1-k} can be considered an inverse of a^k modulo p. An easy calculation then shows that

$$2^{p-3} - 1 \equiv -\frac{3}{4} \pmod{p}.$$

Similarly, the right-hand side of congruence (11), for $k = p-3$, can be shown to equal

$$\frac{3}{8}p \sum_{j=1}^{(p-1)/2} \frac{1}{j^3} \pmod{p^2}.$$

Thus, congruence (11) reduces, for $k = p-3$, to

$$-2pB_{p-3} \equiv p \sum_{j=1}^{(p-1)/2} \frac{1}{j^3} \pmod{p^2},$$

which is the first congruence of the lemma.

Next, for any $j \in S$ with $2j = pq_j + r_j$, where q_j and r_j are as in the beginning of the proof, simple calculations show that

$$\begin{aligned}\frac{1}{(2j)^2} = \frac{1}{(pq_j + r_j)^2} &\equiv \frac{1}{r_j^2 + 2pq_jr_j} \pmod{p^2} \\ &\equiv \frac{1}{r_j^2}\big(1 - 2pq_j/r_j\big) \pmod{p^2}.\end{aligned}$$

Since r_j runs through the set S as j does, it follows, from the preceding relation and the definition of q_j, that

$$\frac{1}{4}\sum_{j=1}^{p-1}\frac{1}{j^2} \equiv \sum_{j=1}^{p-1}\frac{1}{j^2} - 2p\sum_{j=(p+1)/2}^{p-1}\frac{1}{(2j)^3} \pmod{p^2}.$$

This implies that

$$-\frac{3}{4}\sum_{j=1}^{p-1}\frac{1}{j^2} \equiv \frac{p}{4}\sum_{j=1}^{(p-1)/2}\frac{1}{j^3} \pmod{p^2}.$$

Therefore, by congruence (7), we obtain

$$\sum_{j=1}^{p-1}\frac{1}{j^2} \equiv \frac{2}{3}pB_{p-3} \pmod{p^2},$$

which is congruence (8) of the lemma.

Next, we observe that

$$\begin{aligned}\sum_{j=(p+1)/2}^{p-1}\frac{1}{j^2} = \sum_{j=1}^{(p-1)/2}\frac{1}{(p-j)^2} &\equiv \sum_{j=1}^{(p-1)/2}\frac{1}{j^2\big(1-2p/j\big)} \pmod{p^2} \\ &\equiv \sum_{j=1}^{(p-1)/2}\frac{1}{j^2}\big(1+2p/j\big) \pmod{p^2}. \quad (12)\end{aligned}$$

Since

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

whose left-hand side is congruent to $\frac{2}{3}pB_{p-3}$ modulo p^2 by congruence (8), it follows from (12) that

$$\begin{aligned}\frac{2}{3}pB_{p-3} &\equiv 2\sum_{j=1}^{(p-1)/2}\frac{1}{j^2} + 2p\sum_{j=1}^{(p-1)/2}\frac{1}{j^3} \pmod{p^2} \\ &\equiv 2\sum_{j=1}^{(p-1)/2}\frac{1}{j^2} - 4pB_{p-3} \pmod{p^2}.\end{aligned}$$

It is clear that the preceding congruence implies congruence (9) of the lemma. To prove the last congruence (10) of the lemma, we begin by noting that

$$\begin{aligned}\sum_{j=1}^{p-1}\frac{1}{p-j} &= -\sum_{j=1}^{p-1}\frac{1}{j\big(1-p/j\big)}\\ &\equiv -\sum_{j=1}^{p-1}\frac{1}{j}\big(1+p/j+p^2/j^2\big) \pmod{p^3}\\ &\equiv -\sum_{j=1}^{p-1}\frac{1}{j}-p\sum_{j=1}^{p-1}\frac{1}{j^2}-p^2\sum_{j=1}^{p-1}\frac{1}{j^3} \pmod{p^3}.\end{aligned}$$

Thus

$$\sum_{j=1}^{p-1}\frac{1}{j}\equiv -\sum_{j=1}^{p-1}\frac{1}{j}-p\sum_{j=1}^{p-1}\frac{1}{j^2}-p^2\sum_{j=1}^{p-1}\frac{1}{j^3} \pmod{p^3}. \tag{13}$$

Since

$$\sum_{j=1}^{p-1}\frac{1}{j^3}\equiv 0 \pmod{p},$$

we obtain the required congruence from (13) by using congruence (8). □

We shall also need the following result.

Lemma 3. *For any prime $p>3$, we have*

$$\sum_{k=1}^{p-1}\frac{H_{k-1}}{k^2}\equiv B_{p-3} \pmod{p} \tag{14}$$

and

$$\sum_{\substack{k=1\\ k\ odd}}^{p-1}\frac{H_{k-1}}{k^2}\equiv \frac{3}{8}B_{p-3} \pmod{p}. \tag{15}$$

Proof. Putting $x=0$ and $n=p$ in the identity

$$\sum_{k=1}^{n}\frac{(1-x)^k}{k}=\sum_{k=1}^{n}\binom{n}{k}\frac{(-1)^k}{k}(x^k-1),$$

one obtains

$$\sum_{k=1}^{p}\frac{1}{k}=\sum_{k=1}^{p}\binom{p}{k}(-1)^k\big(-\frac{1}{k}\big),$$

which readily yields the following:

$$\sum_{k=1}^{p-1}\frac{1}{k}=-\sum_{k=1}^{p-1}\frac{1}{k}\frac{p}{k}\binom{p-1}{k-1}(-1)^k.$$

It then follows, by Lemma 1, that

$$\sum_{k=1}^{p-1}\frac{1}{k}\equiv p\sum_{k=1}^{p-1}\frac{1}{k^2}\big(1-pH_{k-1}\big)\pmod{p^3}.$$

Therefore, by congruences (8) and (10) of Lemma 2, we obtain

$$-\frac{1}{3}p^2B_{p-3}\equiv\frac{2}{3}p^2B_{p-3}-p^2\sum_{k=1}^{p-1}\frac{H_{k-1}}{k^2}\pmod{p^3},$$

which implies the first congruence of this lemma.

Next, as

$$H_{p-(k+1)}=H_{p-1}-\sum_{j=1}^{k}\frac{1}{p-j}\equiv\sum_{j=1}^{k}\frac{1}{j}\equiv H_k\pmod{p},$$

one obtains easily the following congruence:

$$\sum_{\substack{k=1\\ k\,even}}^{p-1}\frac{H_{k-1}}{k^2}=\sum_{\substack{k=1\\ k\,odd}}^{p-1}\frac{H_{p-k-1}}{(p-k)^2}\equiv\sum_{\substack{k=1\\ k\,odd}}^{p-1}\frac{H_k}{k^2}=\sum_{\substack{k=1\\ k\,odd}}^{p-1}\frac{H_{k-1}}{k^2}+\sum_{\substack{k=1\\ k\,odd}}^{p-1}\frac{1}{k^3}\pmod{p}.$$

The preceding can be rewritten as

$$\sum_{k=1}^{p-1}\frac{H_{k-1}}{k^2}\equiv 2\sum_{\substack{k=1\\ k\,odd}}^{p-1}\frac{H_{k-1}}{k^2}+\sum_{\substack{k=1\\ k\,odd}}^{p-1}\frac{1}{k^3}\pmod{p}. \tag{16}$$

However

$$\begin{aligned}\sum_{\substack{k=1\\ k\,odd}}^{p-1}\frac{1}{k^3} &\equiv -\sum_{\substack{k=1\\ k\,even}}^{p-1}\frac{1}{k^3}\pmod{p}\\ &\equiv -\frac{1}{8}\sum_{k=1}^{(p-1)/2}\frac{1}{k^3}\pmod{p}\\ &\equiv \frac{1}{4}B_{p-3}\pmod{p}\end{aligned}$$

by congruence (7) of Lemma 2. It then follows from (16) that

$$\sum_{k=1}^{p-1}\frac{H_{k-1}}{k^2}\equiv 2\sum_{\substack{k=1\\ k\,odd}}^{p-1}\frac{H_{k-1}}{k^2}+\frac{1}{4}B_{p-3}\pmod{p},$$

which implies the second congruence of the lemma. □

3. Proof of the Main Result

We are now ready to prove the main result.

Theorem 1. *For a prime $p > 3$ and the Fermat quotient $q_p(2)$,*

$$\sum_{k=1}^{p-1} \frac{2^k}{k} + 2q_p(2) \equiv -\frac{7}{12}p^2 B_{p-3} \pmod{p^3}.$$

Proof. Putting $x = -1$ and $n = p$ in the identity

$$\sum_{k=1}^{n} \frac{(1-x)^k}{k} = \sum_{k=1}^{n} \binom{n}{k} \frac{(-1)^k}{k}(x^k - 1)$$

and then rearranging the terms, one obtains

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{2^k}{k} + 2q_p(2) &= \sum_{k=1}^{p-1} \binom{p}{k}(-1)^k \frac{(-1)^k - 1}{k} \\ &= p\sum_{k=1}^{p-1} \binom{p-1}{k-1}(-1)^k \frac{(-1)^k - 1}{k^2}. \end{aligned}$$

The preceding relation, with the help of Lemma 1, can be expressed as the following congruence:

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{2^k}{k} + 2q_p(2) &\equiv -p\sum_{k=1}^{p-1} \big(1 - pH_{k-1}\big) \frac{(-1)^k - 1}{k^2} \pmod{p^3} \\ &\equiv 2p \sum_{\substack{k=1 \\ k\,odd}}^{p-1} \frac{1}{k^2} - 2p^2 \sum_{\substack{k=1 \\ k\,odd}}^{p-1} \frac{H_{k-1}}{k^2} \pmod{p^3}. \end{aligned} \tag{17}$$

We next evaluate the sum in the first term on the right-hand side of (17).

$$\begin{aligned} \sum_{\substack{k=1 \\ k\,odd}}^{p-1} \frac{1}{k^2} = \sum_{\substack{k=1 \\ k\,even}}^{p-1} \frac{1}{(p-k)^2} &\equiv \sum_{\substack{k=1 \\ k\,even}}^{p-1} \frac{1}{k^2}\big(1 + 2p/k\big) \pmod{p^2} \\ &\equiv \sum_{\substack{k=1 \\ k\,even}}^{p-1} \frac{1}{k^2} + 2p \sum_{\substack{k=1 \\ k\,even}}^{p-1} \frac{1}{k^3} \pmod{p^2} \\ &\equiv \frac{1}{4}\sum_{k=1}^{(p-1)/2} \frac{1}{k^2} + \frac{p}{4}\sum_{k=1}^{(p-1)/2} \frac{1}{k^3} \pmod{p^2}, \end{aligned}$$

which, because of congruences (7) and (9) of Lemma 2, implies that

$$\begin{aligned}\sum_{\substack{k=1\\ k\ odd}}^{p-1}\frac{1}{k^2} &\equiv \frac{7}{12}pB_{p-3}-\frac{1}{2}pB_{p-3} \pmod{p^2}\\ &\equiv \frac{1}{12}pB_{p-3} \pmod{p^2}.\end{aligned}$$

Therefore congruence (17) simplifies to

$$\sum_{k=1}^{p-1}\frac{2^k}{k}+2q_p(2)\equiv\frac{1}{6}p^2B_{p-3}-2p^2\sum_{\substack{k=1\\ k\ odd}}^{p-1}\frac{H_{k-1}}{k^2} \pmod{p^3}.$$

It then follows, by the congruence in (15), that

$$\begin{aligned}\sum_{k=1}^{p-1}\frac{2^k}{k}+2q_p(2) &\equiv \frac{1}{6}p^2B_{p-3}-\frac{3}{4}p^2B_{p-3} \pmod{p^3}\\ &\equiv -\frac{7}{12}p^2B_{p-3} \pmod{p^3}.\end{aligned}$$

The proof of the theorem is complete. □

It is worth noting that Glaisher's century-old congruence modulo p for the Fermat quotient $q_p(2)$ actually holds modulo p^2.

References

[1] J.W.L. Glaisher, On the residues of the sums of the products of the first p-1 numbers and their powers to modulo p^2 or p^3 *Q.J. Math.* **31** (1900), 321-353.

[2] A. Granville, The square of the Fermat quotient, *Integers* **4** (2004), A22.

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, GTM 84, Springer-Verlag, New York Heidelberg Berlin, 1982.

[4] W. Kohnen, A simple congruence modulo p, *Amer. Math. Monthly* **104** (1997), 444-445.

[5] J. Riordan, *Combinatorial Identities*, John Wiley and Sons Inc., New York Sydney, 1968.

[6] Z.H. Sun, Congruences concerning Bernoulli numbers and Bernoulli polynomials, *Discrete Appl. Math.* **105** (2000), 193-223.

[7] Z.H. Sun, Congruences involving Bernoulli and Euler numbers, *J. Number Theory* **128** (2008), 280-312.