AN ELEMENTARY PROOF OF A CONGRUENCE BY SKULA AND GRANVILLE

ROMEO MEŠTROVIĆ

Abstract. Let $p \geq 5$ be a prime, and let $q_p(2) := (2^{p-1} - 1)/p$ be the Fermat quotient of $p$ to base 2. The following curious congruence was conjectured by L. Skula and proved by A. Granville

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

In this note we establish the above congruence by entirely elementary number theory arguments.

1. Introduction and Statement of the Main Result

The Fermat Little Theorem states that if $p$ is a prime and $a$ is an integer not divisible by $p$, then $a^{p-1} \equiv 1 \pmod{p}$. This gives rise to the definition of the Fermat quotient of $p$ to base $a$

$$q_p(a) := \frac{a^{p-1} - 1}{p},$$

which is an integer. Fermat quotients played an important role in the study of cyclotomic fields and Fermat Last Theorem. More precisely, divisibility of Fermat quotient $q_p(a)$ by $p$ has numerous applications which include the Fermat Last Theorem and squarefreeness testing (see [1], [2], [3], [7] and [9]). Ribenboim [10] and Granville [7], besides proving new results, provide a review of known facts and open problems.

By a classical Glaisher’s result (see [4] or [5]) for a prime $p \geq 3$,

$$q_p(2) \equiv -\frac{1}{2} \sum_{k=1}^{p-1} \frac{2^k}{k} \pmod{p}. \quad (1.1)$$

Recently Skula conjectured that for any prime $p \geq 5$,

$$q_p(2)^2 \equiv -\sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p}. \quad (1.2)$$

Applying certain polynomial congruences, Granville [5] proved the congruence (1.2). In this note, we give an elementary proof of this congruence which is based on congruences for some harmonic type sums.

\begin{flushleft}
2010 Mathematics Subject Classification. Primary 11B75; Secondary 11A07, 11B65, 05A19, 05A19.

Keywords and phrases. Congruence, Fermat quotient, harmonic numbers.
\end{flushleft}
Remark 1.1. Recently, given a prime p and a positive integer \( r < p - 1 \), R. Tauraso [13] Theorem 2.3] established the congruence \( \sum_{k=1}^{p-1} 2^k / k^r \pmod{p} \) in terms of an alternating \( r \)-tuple harmonic sum. For example, combining this result when \( r = 2 \) with the congruence (1.2) [14] Corollary 2.4], it follows that

\[
\sum_{1 \leq i < j \leq p-1} \frac{(-1)^j}{ij} \equiv q_p(2)^2 \equiv -\sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p}.
\]

2. Proof of the congruence (1.2)

The harmonic numbers \( H_n \) are defined by

\[
H_n := \sum_{j=1}^{n} \frac{1}{j}, \quad n = 1, 2, \ldots,
\]

where by convention \( H_0 = 0 \).

Lemma 2.1. For any prime \( p \geq 5 \) we have

(2.1) \[
q_p(2)^2 \equiv \sum_{k=1}^{p-1} \left( 2^k + \frac{1}{2^k} \right) \frac{H_k}{k + 1} \pmod{p}.
\]

Proof. In the present proof we will always suppose that \( i \) and \( j \) are positive integers such that \( i \leq p - 1 \) and \( j \leq p - 1 \), and that all the summations including \( i \) and \( j \) range over the set of such pairs \((i, j)\).

Using the congruence (1.1) and the fact that by Fermat Little Theorem, \( 2^{p-1} \equiv 1 \pmod{p} \), we get

\[
q_p(2)^2 = \left( \frac{2^{p-1} - 1}{p} \right)^2 \equiv \frac{1}{4} \left( \sum_{k=1}^{p-1} \frac{2^k}{k} \right)^2 = \frac{1}{4} \left( \sum_{k=1}^{p-1} \frac{2^{p-k}}{p-k} \right)^2.
\]

(2.2)

\[
= \frac{1}{4} \left( 2 \sum_{k=1}^{p-1} \frac{2^{(p-1)-k}}{-k} \right)^2 = \left( \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \right)^2
\]

\[
= \sum_{i+j \leq p} \frac{1}{ij \cdot 2^{i+j}} + \sum_{i+j \geq p} \frac{1}{ij \cdot 2^{i+j}} - \sum_{i+j=p} \frac{1}{ij \cdot 2^{i+j}}
\]

\[
:= S_1 + S_2 - S_3 \pmod{p}.
\]

We will determine \( S_1, S_2 \) and \( S_3 \) modulo \( p \) as follows.

\[
S_1 = \sum_{i+j \leq p} \frac{1}{ij \cdot 2^{i+j}} = \sum_{k=2}^{p} \frac{1}{k \cdot 2^{i+j}} = \sum_{k=2}^{p} \frac{1}{k \cdot 2^{i+j}}
\]

(2.3)

\[
= \sum_{k=2}^{p} \frac{1}{2^k} \sum_{i=1}^{k-1} \left( \frac{1}{i} + \frac{1}{k-i} \right) = \sum_{k=2}^{p} \frac{2H_{k-1}}{k \cdot 2^k} = \sum_{k=1}^{p-1} \frac{H_k}{(k+1)2^k}.
\]

Observe that the pair \((i, j)\) satisfies \( i + j = k \) for some \( k \in \{p, p+1, \ldots, 2p-2\} \) if and only if for such a \( k \) holds \((p-i) + (p-j) = l \) with \( l := 2p - k \leq p \).
Accordingly, using the fact that by Fermat Little Theorem, $2^{2p} \equiv 2^2 \pmod p$, we have

$$S_2 = \sum_{i+j \geq p} \frac{1}{ij \cdot 2^{i+j}} = \sum_{(p-i)+(p-j) \geq p} \frac{1}{(p-i)(p-j) \cdot 2^{(p-i)+(p-j)}}$$

$$= \sum_{i+j \leq p} \frac{1}{ij \cdot 2^{p-i-j}} \equiv \frac{1}{4} \sum_{i+j \leq p} \frac{2^{i+j}}{ij} \equiv \frac{1}{4} \sum_{k=2}^{p} \sum_{i+j=k} \frac{2^{k}}{ij}$$

(2.4)

$$= \frac{1}{4} \sum_{k=2}^{p} \frac{2^k}{k} \sum_{i=1}^{k-1} \left( \frac{1}{i} + \frac{1}{k-i} \right) = \sum_{k=2}^{p} \frac{2^{k-1}H_{k-1}}{k}$$

$$= \sum_{k=1}^{p-1} \frac{2^k H_k}{k+1} \pmod p.$$  

By Wolstenholme’s theorem (see, e.g., [15], [6]; for its generalizations see [11, Theorems 1 and 2]) if $p$ is a prime greater than 3, then the numerator of the fraction $H_{p-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ is divisible by $p^2$. Hence, we find that

$$S_3 = \sum_{i+j=p} \frac{2^{i+j}}{ij} = 2^p \sum_{i=1}^{p-1} \frac{1}{i(p-i)}$$

(2.5)

$$= \frac{2^p}{p} \sum_{i=1}^{p-1} \left( \frac{1}{i} + \frac{1}{p-i} \right) = \frac{2^{p-1}}{p} H_{p-1} \equiv 0 \pmod p.$$  

Finally, substituting (2.3), (2.4) and (2.5) into (2.2), we immediately obtain (2.1). \qed

Proof of the following result easily follows from the congruence $H_{p-1} \equiv 0 \pmod p$.

**Lemma 2.2.** [13, Lemma 2.1] Let $p$ be an odd prime. Then

(2.6)

$H_{p-k-1} \equiv H_k \pmod p$

for every $k = 1, 2, \ldots, p-2$.

**Lemma 2.3.** For any prime $p \geq 5$ we have

(2.7)

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

**Proof.** Since by Wolstenholme’s theorem, $H_{p-1}/p \equiv 0 \pmod p$, using this and the congruences $2^{p-1} \equiv 1 \pmod p$ and (2.6) of Lemma 2.2, we immediately obtain

$$\sum_{k=1}^{p-1} \frac{2^k H_k}{k+1} \equiv \sum_{k=1}^{p-2} \frac{2^k H_k}{k+1} = \sum_{k=1}^{p-2} \frac{2^{p-k-1} H_{p-k-1}}{p-k}$$

(2.8)

$$= -\sum_{k=1}^{p-2} \frac{H_k}{k \cdot 2^k} \equiv -\sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \pmod p.$$
Further, we have
\[
\sum_{k=1}^{p-2} \frac{H_k}{(k+1)2^k} = 2 \sum_{k=1}^{p-2} \frac{H_k}{(k+1)2^{k+1}} - \frac{1}{k+1}.
\]
(2.9)

Moreover, from \(2^p \equiv 2 \pmod{p}\) we have
\[
\sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} = \sum_{k=1}^{p-1} \frac{1}{(p-k)2^{p-k}} 
\]
(2.10)

The congruences (2.8), (2.9) and (2.10) immediately yield
\[
\sum_{k=1}^{p-1} \left(2^k + \frac{1}{2^k}\right) \frac{H_k}{k+1} = \sum_{k=1}^{p-1} \frac{2^k H_k}{k+1} + \sum_{k=1}^{p-1} \frac{H_k}{(k+1)2^k} 
\]
(2.11)
\[
\equiv \sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} - \sum_{k=1}^{p-1} \frac{2^k}{k^2} \quad \pmod{p}.
\]

Finally, comparing (2.1) of Lemma 2.1 with (2.11), we obtain the desired congruence (2.7).

Notice that the congruence \(\sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \equiv 0 \pmod{p}\) for any prime \(p \geq 5\) is recently established by Z.W. Sun \([13, \text{Theorem 1.1 (1.1)}]\) and it is based on the identity from \([13, \text{Lemma 2.4}]\). Here we give another simple proof of this congruence (Lemma 2.6).

**Lemma 2.6.** For any prime \(p \geq 5\) we have
\[
\sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \equiv \frac{1}{2} \sum_{1 \leq i \leq j \leq p-1} \frac{2^i - 1}{ij} \pmod{p}.
\]
(2.12)

**Proof.** From the identity
\[
\left(\sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k}\right) \left(\sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k}\right) = \sum_{1 \leq i < j \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{1 \leq j < i \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2 \cdot 2^k},
\]
and the congruence \(H_{p-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p}\) it follows that
\[
\sum_{1 \leq i < j \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{1 \leq j < i \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2 \cdot 2^k} \equiv 0 \pmod{p}.
\]
(2.13)
Since \( 2^p \equiv 2 \pmod{p} \), we have
\[
\sum_{1 \leq j < i \leq p-1} \frac{1}{ij} \cdot 2^j \equiv \sum_{1 \leq j < i \leq p-1} \frac{1}{2} \frac{2^{p-j}}{(p-i)(p-j)} \equiv \frac{1}{2} \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} \pmod{p},
\]
which substituting into (2.13) gives
\[
(2.14) \quad \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} \cdot 2^j + \sum_{k=1}^{p-1} \frac{1}{k} \cdot 2^k \equiv -\frac{1}{2} \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} \pmod{p}.
\]
Further, if we observe that
\[
\sum_{k=1}^{p-1} \frac{H_k}{k} \cdot 2^k = \sum_{k=1}^{p-1} \frac{H_{k-1} + 1}{k} \cdot 2^k = \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} \cdot 2^j + \sum_{k=1}^{p-1} \frac{1}{k^2} \cdot 2^k,
\]
then substituting (2.14) into the previous identity, we obtain
\[
(2.15) \quad \sum_{k=1}^{p-1} \frac{H_k}{k} \cdot 2^k \equiv -\frac{1}{2} \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} \pmod{p}.
\]
Since
\[
0 \equiv \left( \sum_{k=1}^{p-1} \frac{1}{k} \right) \left( \sum_{k=1}^{p-1} \frac{2^k}{k} \right) = \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} + \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} \pmod{p},
\]
comparing this with (2.15), we immediately obtain
\[
(2.16) \quad \sum_{k=1}^{p-1} \frac{H_k}{k} \cdot 2^k \equiv -\frac{1}{2} \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} \pmod{p}.
\]
From a well known fact that (see e.g., [9, p. 353])
\[
(2.17) \quad \sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \pmod{p}
\]
we find that
\[
\sum_{1 \leq i \leq j \leq p-1} \frac{1}{ij} = \frac{1}{2} \left( \left( \sum_{k=1}^{p-1} \frac{1}{k} \right)^2 + \sum_{k=1}^{p-1} \frac{1}{k^2} \right) \equiv 0 \pmod{p}.
\]
Finally, the above congruence and (2.16) immediately yield the desired congruence (2.12).

\[\Box\]

**Lemma 2.5.** For any positive integer \( n \) holds
\[
(2.18) \quad \sum_{1 \leq i < j \leq n} \frac{2^i - 1}{ij} = \sum_{k=1}^{n} \frac{1}{k^2} \binom{n}{k}.
\]
Proof. Using the well known identities
\[ \sum_{i=k}^{j} \binom{i-1}{k-1} = \binom{j}{k} \quad \text{and} \quad \frac{1}{k} \binom{i}{k} = \frac{1}{k} \binom{i-1}{k-1} \]
with \( k \leq j \), and the fact that \( \binom{i}{k} = 0 \) when \( i < k \), we have

\[
\sum_{1 \leq i \leq j \leq n} \frac{2^i - 1}{ij} = \sum_{1 \leq i \leq j \leq n} \frac{(1 + 1)^i - 1}{ij} = \sum_{1 \leq i \leq j \leq n} \frac{i}{j} \sum_{k=1}^{i} \frac{1}{k} \binom{i}{k}
\]

\[
= \sum_{1 \leq i \leq j \leq n} \frac{1}{j} \sum_{k=1}^{n} \frac{1}{k} \binom{i-1}{k-1} = \sum_{k=1}^{n} \frac{1}{k} \sum_{1 \leq i \leq j \leq n} \frac{1}{j} \binom{i-1}{k-1}
\]

\[
= \sum_{k=1}^{n} \frac{1}{k} \sum_{j=i}^{n} \frac{1}{j} \binom{j}{k} = \sum_{k=1}^{n} \frac{1}{k} \sum_{j=k}^{n} \frac{1}{j} \binom{j-1}{k-1}
\]

\[
= \sum_{k=1}^{n} \frac{1}{k^2} \sum_{j=k}^{n} \frac{1}{j} \binom{j-1}{k-1} = \sum_{k=1}^{n} \frac{1}{k^2} \binom{n}{k},
\]
as desired. \( \square \)

Lemma 2.6. [13, Theorem 1.1 (1.1)] For any prime \( p \geq 5 \) holds

\[
(2.19) \quad \sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \equiv 0 \pmod{p}.
\]

Proof. Using the congruence (2.12) from Lemma 2.4 and the identity (2.18) with \( n = p - 1 \) in Lemma 2.5, we find that

\[
(2.20) \quad \sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \equiv \sum_{k=1}^{p-1} \frac{1}{k^2} \binom{p-1}{k} \pmod{p}.
\]

It is well known (see e.g., [8]) that for \( k = 1, 2, \ldots, p - 1 \),

\[
(2.21) \quad \binom{p-1}{k} \equiv (-1)^k \pmod{p}.
\]

Then from (2.20), (2.21) and (2.17) we get

\[
\sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \equiv \sum_{k=1}^{p-1} \frac{(-1)^k}{k^2} = \sum_{k=1}^{p-1} \frac{1}{k^2} - 2 \sum_{1 \leq j \leq p-1 \atop 2 \mid j} \frac{1}{j^2}
\]

\[
\equiv -2 \sum_{1 \leq j \leq p-1 \atop 2 \mid j} \frac{1}{j^2} = -\frac{1}{2} \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} \pmod{p}.
\]
Finally, the above congruence together with a well known fact that (see e.g., [12] Corollary 5.2 (a) with \( k = 2 \))

\[
\frac{1}{k^2} \equiv 0 \pmod{p}
\]

yields

\[
\sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \equiv 0 \pmod{p}.
\]

This concludes the proof. \( \square \)

**Proof of the congruence** (1.2). The congruence (1.2) immediately follows from (2.7) of Lemma 2.3 and (2.19) of Lemma 2.6. \( \square \)

**References**

[1] Agoh, T., Skula, L., *Fermat quotients for composite moduli*, J. Number Theory 66 (1997) 29–50.

[2] Cao, H. Q., Pan, H., *A congruence involving product of \( q \)-binomial coefficients*, J. Number Theory 121 (2006), 224–233.

[3] Ernvall, R., Metsänkylä, T., *On the \( p \)-divisibility of Fermat quotients*, Math. Comp. 66 (1997), 1353–1365.

[4] Glaisher, J. W. L., *On the residues of the sums of the inverse powers of numbers in arithmetical progression*, Q. J. Math. 32 (1900), 271-288.

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

[6] Granville, A., *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, in Organic Mathematics–Burnaby, BC 1995, CMS Conf. Proc., vol. 20, American Mathematical Society, Providence, RI, 1997, 253-276.

[7] Granville, A., *Some conjectures related to Fermat’s Last Theorem*, Number Theory (Banff, AB, 1988), de Gruyter, Berlin, 1990, 177–192.

[8] Hardy, G. H., Wright, E. M., *An Introduction to the Theory of Numbers*, Fourth Edition, Clarendon Press, Oxford, 1960.

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

[10] Ribenboim, P., *13 Lectures on Fermat’s Last Theorem*, Springer-Verlag, New York, Heidelberg, Berlin, 1979.

[11] Slavutsky, I. Sh., *Leudesdorf’s theorem and Bernoulli numbers*, Arch. Math. 35 (1999), 299–303.

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

[13] Sun, Z. W., *Arithmetic theory of harmonic numbers*, Proc. Amer. Math. Soc., article in press; preprint arXiv:0911.4433v3 [math.NT] (2009).

[14] Tauraso, R., *Congruences involving alternating multiple harmonic sums*, Electron. J. Comb. 17 (2010), \# R16.

[15] Wolstenholme, J., *On certain properties of prime numbers*, Quart. J. Pure Appl. Math. 5 (1862), 35-39.

Maritime Faculty, University of Montenegro, Dobrota 36, 85330 Kotor, Montenegro

*E-mail address: romeo@ac.me*