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], [5] and [9]). Ribenboim [10] and Granville [5], besides proving new results, provide a review of known facts and open problems.

By a classical Glaisher’s result (see [4] or [7]) for a prime $p \geq 3$,

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

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

(1.2) \[ q_p(2)^2 \equiv -\sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p}. \]
Applying certain polynomial congruences, Granville [7] 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.

**Remark 1.1.** Recently, given a prime \( p \) and a positive integer \( r < p - 1 \), R. Tauraso [14, Theorem 2.3] established the congruence

\[
\sum_{k=1}^{p-1} \frac{2^k}{k^r} \equiv \frac{p-1}{2^r} \pmod{p},
\]

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

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

### 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

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

**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

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

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

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

The last three sums will be called \( S_1 \), \( S_2 \) and \( S_3 \), respectively. We will determine them modulo \( p \) as follows.

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

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

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

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

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

\[(2.4)\]

\[
= \sum_{k=1}^{p-1} \frac{2^kH_k}{k+1} \pmod{p}.
\]

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

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

\[(2.5)\]

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

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

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
\[
\sum_{k=1}^{p-1} \frac{2^k H_k}{k+1} \equiv \sum_{k=1}^{p-2} \frac{2^k H_k}{k+1} = \sum_{k=1}^{p-2} \frac{2^{p-k-1} H_{p-k-1}}{p-k} = - \sum_{k=1}^{p-2} \frac{H_k}{k \cdot 2^k} \equiv - \sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \pmod{p}.
\]
(2.8)

Further, using Wolstenholme’s theorem, we have
\[
\sum_{k=1}^{p-1} \frac{H_k}{(k+1)2^k} = 2 \sum_{k=0}^{p-2} \frac{H_{k+1} - \frac{1}{k+1}}{(k+1)2^{k+1}} + \frac{H_{p-1}}{p \cdot 2^{p-1}} = 2 \sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} - 2 \sum_{k=1}^{p-1} \frac{1}{k^2 \cdot 2^k} + \frac{H_{p-1}}{p \cdot 2^{p-1}} \equiv 2 \sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} - 2 \sum_{k=1}^{p-1} \frac{1}{k^2 \cdot 2^k} \pmod{p}.
\]
(2.9)

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

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

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

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

Lemma 2.4. 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
\[
\left(\sum_{k=1}^{p-1} \frac{1}{k}\right) \left(\sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k}\right) = \sum_{1 \leq j < i \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{1 \leq j < i \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2 \cdot 2^k},
\]
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
\[
\sum_{1 \leq i < j \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{1 \leq j < i \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2 \cdot 2^k} \equiv 0 \pmod{p}.
\]
Since \( 2^p \equiv 2 \pmod{p} \), we have
\[
\sum_{1 \leq j < i \leq p-1} \frac{1}{ij \cdot 2^j} = \sum_{1 \leq j < i \leq p-1} \frac{2^{p-j}}{(p-i)(p-j)} = \frac{1}{2} \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} \pmod{p},
\]
which substituting into (2.13) gives
\[
\sum_{1 \leq i < j \leq p-1} \frac{1}{ij \cdot 2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2 \cdot 2^k} \equiv -\frac{1}{2} \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} \pmod{p}.
\]
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
\[
\sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} = -\frac{1}{2} \sum_{1 \leq i < j \leq p-1} \frac{2^j}{ij} \pmod{p}.
\]
Since
\[
0 \equiv \left(\sum_{k=1}^{p-1} \frac{1}{k}\right) \left(\sum_{k=1}^{p-1} \frac{1}{2^k}\right) = \sum_{1 \leq j \leq p-1} \frac{2^j}{ij} + \sum_{1 \leq i \leq j \leq p-1} \frac{2^j}{ij} \pmod{p},
\]
comparing this with (2.15), we immediately obtain
\[
\sum_{k=1}^{p-1} \frac{H_k}{k \cdot 2^k} \equiv \frac{1}{2} \sum_{1 \leq i \leq j \leq p-1} \frac{2^i}{ij} \pmod{p}.
\]
From a well known fact that (see e.g., [9, p. 353])
\[
\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \pmod{p},
\]
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).

Lemma 2.5. For any positive integer \( n \) we have

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

**Proof.** Using the well known identities \( \sum_{i=k}^{j} \binom{i-1}{k-1} = \binom{j}{k} \) and \( \frac{1}{j} \binom{j-1}{k} = \frac{1}{k} \binom{j-1}{k-1} \) with \( k \leq j \), and the fact that \( \binom{i}{k} = 0 \) when \( i < k \), we have

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

as desired. \( \square \)

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

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

**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

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

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

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

\[
= \frac{1}{4} \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} - \frac{1}{2} \sum_{k=1}^{p-1} \frac{1}{k^2} \equiv \frac{1}{4} \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} \pmod{p}
\]

Finally, the above congruence together with the fact that from (2.17) (see e.g., [12, Corollary 5.2 (a) with \(k = 2\)])

\[
2 \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} \equiv \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} + \sum_{k=1}^{(p-1)/2} \frac{1}{(p-k)^2} = \sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \pmod{p}
\]

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**


Maritime Faculty, University of Montenegro,
Dobrota 36, 85330 Kotor, Montenegro
E-mail: romeo@ac.me