A CONGRUENCE FOR THE SQUARE OF THE FERMAT QUOTIENT

S. KHONGSIT, A. M. BUHPHANG*, and P. K. SAIKIA

Communicated by Alexandru Zaharescu

For a prime $p > 3$, it has been known for the last hundred years that the Fermat quotient $q_p(2) = \frac{2^{p-1}-1}{p}$ satisfies the congruence

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

In 2004, A. Granville proved the following extension

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

of the congruence. We shall present an elementary proof of Granville's congruence.

AMS 2010 Subject Classification: Primary 11A07, Secondary 11A41.

Key words: prime, Fermat quotient, congruence.

1. INTRODUCTION

For an odd prime p and an integer a such that $p \nmid a$, the Fermat quotient $q_p(a)$ is defined as $q_p(a) = (a^{p-1} - 1)/p$, which is an integer, by Fermat's little theorem.

For a prime $p > 3$, Glaisher [2], in 1901, proved that ,

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

Remarkably, after a hundred years the following striking extension

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

* Corresponding author

of Glaisher's congruence was conjectured by L. Skula and later proved by A. Granville [3] in 2004.

In this paper we present an elementary proof of Granville's congruence. While Granville employed anti-derivatives involving Mirimanoff polynomials, our proof is based on the identity

$$\sum_{k=1}^{n} \frac{(1-x)^k}{k} = \sum_{k=1}^{n} \binom{n}{k} \frac{(-1)^k}{k}(x^k - 1), \tag{3}$$

which holds for any positive integer n and any real number x. The identity was also used in [5] to prove the following generalization of Glaisher's congruence modulo p^3:

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

which was earlier proved by Z. H. Sun in [8]. Note that the above congruence modulo p^2 yields

$$q_p(2) \equiv -\frac{1}{2}\sum_{k=1}^{p-1} \frac{2^k}{k} \pmod{p^2}. \tag{4}$$

We begin with few preliminary results which we shall need for our proof of the main result.

2. PRELIMINARY RESULTS

Lemma 2.1. *For a prime $p > 3$ and for any integer $k = 1, 2, ..., p-1$,*

$$\binom{2p}{k} \equiv (-1)^{k-1}\frac{2p}{k} \pmod{p^2} \tag{5}$$

and

$$\binom{2p}{p+k} \equiv (-1)^{k-1}\frac{2p}{k} \pmod{p^2}. \tag{6}$$

Proof. Since $2p - j \equiv -j \pmod{p}$, it follows that

$$\begin{aligned} \binom{2p}{k} &= \frac{2p}{k}\frac{\prod_{j=1}^{k-1}(2p-j)}{(k-1)!} \\ &\equiv (-1)^{k-1}\frac{2p}{k} \pmod{p^2}. \end{aligned}$$

As the binomial coefficient $\binom{2p}{p+k} = \binom{2p}{p-k}$, a similar calculation establishes the next congruence. □

We shall also need the following version of the well-known Wolstenholme's theorem (see Theorem 2 in [1]):

$$\binom{2p}{p} \equiv 2 \pmod{p^3}. \tag{7}$$

We now provide a short proof of this congruence. Note that

$$\begin{aligned} \prod_{j=1}^{p-1}(1-2p/j) &= 1-2p\sum_{j=1}^{p-1}\frac{1}{j}+(2p)^2\sum_{1\le j<l\le p-1}\frac{1}{jl}-\dots \\ &\equiv 1 \pmod{p^3} \end{aligned} \tag{8}$$

since

$$\begin{aligned} \sum_{k=1}^{p-1}\frac{1}{k} &\equiv -\frac{1}{3}p^2B_{p-3} \pmod{p^3} \\ &\equiv 0 \pmod{p^3} \end{aligned}$$

and

$$\begin{aligned} 2\sum_{1\le j<k\le p-1}\frac{1}{jk} &= \left(\sum_{j=1}^{p-1}\frac{1}{j}\right)\left(\sum_{j=1}^{p-1}\frac{1}{k}\right)-\sum_{j=1}^{p-1}\frac{1}{j^2} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

See Lemma 2 in [5] for the proof of the two previous congruences.

It then follows that

$$\begin{aligned} \prod_{j=1}^{p-1}(2p-j)=\prod_{j=1}^{p-1}-j(1-2p/j) &\equiv (-1)^{p-1}(p-1)!\prod_{j=1}^{p-1}(1-2p/j) \\ &\equiv (p-1)! \pmod{p^3}. \end{aligned}$$

Therefore

$$\begin{aligned} \binom{2p}{p} &= \frac{2p}{p}\frac{\prod_{j=1}^{p-1}(2p-j)}{(p-1)!} \\ &\equiv 2\frac{(-1)^{p-1}(p-1)!}{(p-1)!} \pmod{p^3} \\ &\equiv 2 \pmod{p^3}, \end{aligned}$$

which establishes (7).

We begin our proof of the main result by first expressing $pq_p(2)^2$ in terms of certain sums.

Lemma 2.2. *For a prime $p > 3$,*

$$\sum_{k=1}^{p-1} \frac{2^k}{k} + \sum_{k=1}^{p-1} \frac{2^{p+k}}{p+k} \equiv -4pq_p(2)^2 - 6q_p(2) - 2p \sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p^2}. \tag{9}$$

Proof. Since $(1 + p/k)(1 - p/k) \equiv 1 \pmod{p^2}$, it follows that

$$\frac{2^{p+k}}{p+k} = 2^p \frac{2^k}{k(1+p/k)} \equiv 2^p \frac{2^k}{k}(1 - p/k) \pmod{p^2}$$

Now, as by definition, $2pq_p(2) = 2^p - 2$ and $2^p \equiv 2 \pmod{p}$ by Fermat's little theorem, we see that

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{2^{p+k}}{p+k} &\equiv 2^p \sum_{k=1}^{p-1} \frac{2^k}{k} - 2p \sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p^2} \\ &\equiv (2pq_p(2) + 2) \sum_{k=1}^{p-1} \frac{2^k}{k} - 2p \sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p^2} \end{aligned}$$

Using Glaisher's congruence (4) and the preceeding congruence, one then has

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

This completes the proof. □

We now come to the proof of our main result.

3. MAIN RESULT

Theorem 3.1. *For a prime $p > 3$,*

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

Proof. Putting $x = -1$ and $n = 2p$ 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

$$\sum_{k=1}^{2p}\frac{2^k}{k}=\sum_{k=1}^{2p}\binom{2p}{k}\frac{(-1)^k}{k}((-1)^k-1)=2\sum_{\substack{k=1\\2\nmid k}}^{2p}\binom{2p}{k}\frac{1}{k}$$

Splitting up the sums on both sides of the equation, we then have

$$\sum_{k=1}^{p}\frac{2^k}{k}+\sum_{k=1}^{p}\frac{2^{p+k}}{p+k}=2\sum_{\substack{k=1\\2\nmid k}}^{p}\binom{2p}{k}\frac{1}{k}+2\sum_{\substack{k=1\\2\mid k}}^{p-1}\binom{2p}{p+k}\frac{1}{p+k}$$

which we rewrite by grouping together the terms containing p in the denominators as follows:

$$\sum_{k=1}^{p-1}\frac{2^k}{k}+\sum_{k=1}^{p-1}\frac{2^{p+k}}{p+k}+\frac{2^p}{p}+\frac{2^{2p}}{2p}-2\binom{2p}{p}\frac{1}{p}$$

$$=2\sum_{\substack{k=1\\2\nmid k}}^{p-1}\binom{2p}{k}\frac{1}{k}+2\sum_{\substack{k=1\\2\mid k}}^{p-1}\binom{2p}{p+k}\frac{1}{p+k}\,. \tag{10}$$

Note that

$$\begin{aligned}\frac{2^p}{p}+\frac{2^{2p}}{2p} &= \frac{2^p-2}{p}+\frac{2}{p}+\frac{(2^p-2)^2}{2p}+4\frac{2^p-2}{2p}+\frac{4}{2p}\\ &= 2q_p(2)+2pq_p(2)^2+4q_p(2)+\frac{4}{p}\end{aligned}$$

and

$$\frac{2}{p}\left(2-\binom{2p}{p}\right)\equiv 0 \pmod{p^2}$$

by the congruence in (7). Thus equation (10), by using Lemma 2.2, as well as the congruences (5) and (6), can be simplified as follows

$$\begin{aligned}-2pq_p(2)^2-2p\sum_{k=1}^{p-1}\frac{2^k}{k^2} &\equiv 2\sum_{\substack{k=1\\2\nmid k}}^{p-1}\frac{2p}{k^2}(-1)^{k-1}+\\ &\quad 2\sum_{\substack{k=1\\2\mid k}}^{p-1}\frac{2p}{k(p+k)}(-1)^{k-1}\pmod{p^2}.\end{aligned} \tag{11}$$

However, since the right hand side of (11) is congruent modulo p^2 to

$$4p\sum_{\substack{k=1\\2\nmid k}}^{p-1}\frac{1}{k^2}-4p\sum_{\substack{k=1\\2\mid k}}^{p-1}\frac{1}{k^2},$$

it vanishes mod p^2 (see Theorem 1 in [5]).

Therefore the congruence in (11) reduces to

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

which is Granville's congruence. $\square$

REFERENCES

[1] D. F. Bailey, *Some Binomial Coefficient Congruences.* Appl. Math. Lett. **4** (1991), *4*, 1–5.

[2] 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.

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

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

[5] S. Khongsit and P. K. Saikia, *A Congruence for the Fermat quotient modulo p^3.* Integers **16** (2016), A52.

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

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

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

Received February 22, 2018

Lady Keane College
Department of Mathematics
793001 Shillong, Meghalaya, India
shailanstar@gmail.com

North Eastern Hill University
Department of Mathematics
Permanent Campus
Shillong-793022, Meghalaya, India
ardeline17@gmail.com, promode4@gmail.com