INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 6 (2006), #A24

THE CUBE OF THE FERMAT QUOTIENT

Karl Dilcher[1]
Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada
dilcher@mathstat.dal.ca

Ladislav Skula[2]
Department of Applied Mathematics, Faculty of Science, Masaryk University in Brno, Janáčkovo nám. 2a, 602 00 Brno, Czech Republic
skula@math.muni.cz

Received: 11/30/05, Revised: 6/14/06, Accepted: 7/24/06, Published: 10/06/06

Abstract

We prove a certain polynomial congruence modulo an odd prime $p \geq 5$, and as a consequence we obtain a congruence for the cube of the Fermat quotient to base 2 in terms of simple finite sums. This extends known results of a similar nature for the first and second powers of the Fermat quotient.

1. Introduction

For an odd prime p and an integer a with $p \nmid a$ the *Fermat quotient* of p to base a is defined by

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

Because of their close connection to the classical theory of Fermat's last theorem these quotients have been studied in great detail (see, e.g., [3]), and a large number of congruences for them are known. A particularly interesting one, due to Glaisher [1], is

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

[1]Supported by the Natural Sciences and Engineering Research Council of Canada.
[2]Supported by the Grant Agency of the Czech Republic (Methods of Theory of Numbers, 201/04/381).

Recently the second author discovered and conjectured

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

and subsequently Granville [2] proved this congruence. Granville also remarked that, based on calculations, an obvious extension of (2) and (3) probably does not exist. However, it turns out that a less obvious extension to $q_p(2)^3$, involving two sums of the expected type, does exist. It is the purpose of this paper to prove this congruence, namely

Theorem 1. *For any prime $p \geq 5$ we have*

$$q_p(2)^3 \equiv -3\sum_{j=1}^{p-1} \frac{2^j}{j^3} + \frac{7}{4}\sum_{j=1}^{p-1} \frac{(-1)^j}{j^3} \pmod{p}, \tag{4}$$

or equivalently

$$q_p(2)^3 \equiv -3\sum_{j=1}^{p-1} \frac{2^j}{j^3} + \frac{7}{16}\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j^3} \pmod{p}. \tag{5}$$

The proof of this result uses methods similar to those in [2]; this part is done in Section 2. The remainder of the proof is then presented in two versions. In Section 3 we present a short proof by the anonymous referee. Our own proof relies on some general results, proved in Section 4, concerning certain sums modulo p; we consider this of independent interest. Section 5 then concludes the second proof.

Congruences (2) – (4) give rise to the obvious question whether there exist similar formulas also for higher powers of $q_p(2)$. On the one hand, computer searches have been without success, while on the other hand the method of Section 2 below does not appear to extend to higher powers.

2. Proof of Theorem 1

As in [2], we define the following polynomials:

$$q(x) := \frac{x^p - (x-1)^p - 1}{p}, \tag{6}$$

$$G(x) := \sum_{j=1}^{p-1} \frac{x^j}{j^2}, \tag{7}$$

and the additional polynomial

$$G_3(x) := \sum_{j=1}^{p-1} \frac{x^j}{j^3}. \tag{8}$$

We also use the congruences (4) and (5) in [2], namely

$$G(x) \equiv G(1-x) + x^p G(1-\tfrac{1}{x}) \pmod{p}, \tag{9}$$
$$q(x)^2 \equiv -2x^p G(x) - 2(1-x^p)G(1-x) \pmod{p}. \tag{10}$$

We are now ready to state the following result which provides the main step towards the proof of Theorem 1. It can be seen as the cubic analogue of (10) and is of interest in its own right.

Theorem 2. *For any prime $p \geq 5$ we have*

$$\frac{1}{6}q(x)^3 \equiv -x^p G_3(x) - (1-x^p)G_3(1-x) - x^{2p}(1-x^p)G_3(1-\tfrac{1}{x}) - \frac{2}{3}G_3(-1)x^p(1-x^p) \pmod{p}. \tag{11}$$

Proof of Theorem 1. We specialize (11) by setting $x = 2$. Then it is obvious from (6) that

$$q(2) \equiv 2q_p(2) \pmod{p}. \tag{12}$$

Also, with (8) we have

$$x^p G_3(\tfrac{1}{x}) = \sum_{j=1}^{p-1} \frac{x^{p-j}}{j^3} = \sum_{j=1}^{p-1} \frac{x^j}{(p-j)^3} \equiv -G_3(x) \pmod{p}, \tag{13}$$

so that

$$2^p G_3(\tfrac{1}{2}) \equiv -G_3(2) \pmod{p}. \tag{14}$$

Finally, if we note that $2^p \equiv 2 \pmod{p}$, we get

$$q_p(2)^3 \equiv -3G_3(2) + \frac{3}{4}G_3(-1) - \frac{3}{2}\left(-\frac{2}{3}G_3(-1)\right) \pmod{p}. \tag{15}$$

This is obviously (4); the equivalence to (5) will be shown in Proposition 5 below. □

In the remainder of this section we will give the first half of the proof of Theorem 2. We begin by noting that from (6) it follows that

$$q'(x) \equiv -\sum_{j=1}^{p-1} x^{j-1} = x^{p-1} - \frac{1-x^p}{1-x} \pmod{p} \tag{16}$$

(see also [2, p. 2]). Also, from (7) and (8) it is obvious that

$$G_3'(x) = \frac{1}{x}G(x). \tag{17}$$

Adapting the main idea of proof in [2], we use (10) and (16) to obtain

$$\begin{aligned}\frac{d}{dx}q(x)^3 &= 3q(x)^2q'(x) \\ &\equiv 3\big(-2x^pG(x) - 2(1-x^p)G(1-x)\big)\left(x^{p-1} - \frac{1-x^p}{1-x}\right) \\ &= -6x^{2p}\frac{G(x)}{x} + 6(1-x^p)^2\frac{G(1-x)}{1-x} \\ &\quad + 6x^p(1-x^p)\left(\frac{G(x)}{1-x} - \frac{G(1-x)}{x}\right) \pmod p.\end{aligned} \tag{18}$$

With (9) we now get

$$\frac{G(x)}{1-x} \equiv \frac{G(1-x)+x^pG(1-\frac{1}{x})}{1-x} = \frac{G(1-x)}{1-x} - x^p\frac{1}{x}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}} \pmod p$$

and

$$\frac{G(1-x)}{x} \equiv \frac{G(x)-x^pG(1-\frac{1}{x})}{x} = \frac{G(x)}{x} - x^p\left(\frac{1}{x}-\frac{1}{x^2}\right)\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}} \pmod p,$$

so that

$$\frac{G(x)}{1-x} - \frac{G(1-x)}{x} \equiv \frac{G(1-x)}{1-x} - \frac{G(x)}{x} - x^p\frac{1}{x^2}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}} \pmod p. \tag{19}$$

Combining (18) and (19), we obtain after some simplification,

$$\frac{1}{6}\frac{d}{dx}q(x)^3 \equiv -x^p\frac{G(x)}{x} + (1-x^p)\frac{G(1-x)}{1-x} - x^{2p}(1-x^p)\frac{1}{x^2}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}} \pmod p. \tag{20}$$

Now the essential step consists of taking the antiderivative on both sides of (20), using (17):

$$\begin{aligned}\frac{1}{6}q(x)^3 \equiv -x^pG_3(x) - (1-x^p)G_3(1-x) - x^{2p}(1-x^p)G_3(1-\tfrac{1}{x}) \\ + c_0 + c_1x^p + c_2x^{2p} \pmod p.\end{aligned} \tag{21}$$

Here we have used the fact that the only powers of x occurring in (20) are powers of x^p, and the constants c_0, c_1, c_2 come from the fact that the polynomials on both sides of (21) have degree $< 3p$. To determine these constants we note that, as observed in [2], we have

$$q(0) \equiv q(1) \equiv 0 \pmod p, \tag{22}$$

but also

$$G_3(0) \equiv G_3(1) \equiv 0 \pmod{p}, \tag{23}$$

by a well-known congruence which is easy to prove. If we set $x = 0$ in (21) and note that $x^p G_3(1 - \frac{1}{x})$ is actually a polynomial in x, then we see that each term, with the exception of c_0, is congruent to 0 (mod p); hence $c_0 \equiv 0 \pmod{p}$. Similarly, if we set $x = 1$ in (21) then by (22) and (23) we have $c_1 + c_2 \equiv 0 \pmod{p}$, so that (21) becomes

$$\begin{aligned}\frac{1}{6}q(x)^3 \equiv -x^p G_3(x) - (1-x^p)G_3(1-x) - x^{2p}(1-x^p)G_3(1-\tfrac{1}{x}) \\ + c_1 x^p(1-x^p) \pmod{p}.\end{aligned} \tag{24}$$

It is important to note that c_1 is a constant that still depends on the prime p.

Thus it remains to evaluate the constant $c_1 \pmod{p}$. The main idea of both proofs rests on the fact that the function $q(x)$ has, in addition to $x = 0$ and $x = 1$, another zero in $\mathbb{Z}/p\mathbb{Z}$, or in an extension of this field.

3. First Proof of Theorem 2

The following determination of the constant c_1, which completes the proof of Theorem 2, is due to the referee.

The congruence (24) can be seen as an identity in $\mathbb{Q}[x]$ if we add a polynomial with rational coefficients whose numerators are all divisible by p. Now let a be a primitive sixth root of unity in $\mathbb{C}$, which means its minimal polynomial is $x^2 - x + 1$. Then $a - 1 = a^2$, and so $a^p - (a-1)^p - 1 = -((a^p)^2 - a^p + 1) = 0$ since a^p is also a primitive sixth root of unity, and thus $q(a) = 0$ by the definition (6). Since $a^p(1 - a^p) = 1$ and $1 - \frac{1}{a} = a$, as well as $1 - a = \overline{a}$ and $1 - a^p = \overline{a}^p$ with $\overline{a}$ the conjugate of a, (24) with $x = a$ gives

$$c_1 \equiv 2a^p G_3(a) + \overline{a}^p G_3(\overline{a}) \pmod{p}. \tag{25}$$

Replacing a by $\overline{a}$ and comparing with (25), we get $a^p G_3(a) \equiv \overline{a}^p G_3(\overline{a}) \pmod{p}$, and therefore

$$c_1 \equiv 3a^p G_3(a) \pmod{p}. \tag{26}$$

Now we define, for any integer r,

$$t(r) := \sum_{\substack{j=1 \\ j \equiv r \pmod 6}}^{p-1} \frac{1}{j^3}; \tag{27}$$

then $t(R) = t(r)$ if $R \equiv r \pmod 6$. Note that

$$G_3(-1) = \sum_{j=0}^{5} (-1)^j t(j) \equiv 2\big(t(0) + t(2) + t(4)\big), \tag{28}$$

and that

$$\begin{aligned} t(0)+t(2)+t(4) &= \sum_{\substack{j=1\\ j\equiv 0 \pmod 2}}^{p-1} \frac{1}{j^3} \equiv \sum_{\substack{j=1\\ j\equiv 0 \pmod 6}}^{3p-1} \frac{1}{j^3} \\ &= 3^3 \sum_{i=0}^{2} \sum_{\substack{j=ip+1\\ j\equiv 0 \pmod 6}}^{(i+1)p} \frac{1}{j^3} = 3^3 \sum_{i=0}^{2} \sum_{\substack{k=1\\ k\equiv -ip \pmod 6}}^{p} \frac{1}{j^3} \\ &= 27\big(t(0)+t(-p)+t(-2p)\big) \pmod p, \end{aligned}$$

where we have written $j = k + ip$. From the definition (27) we also have $t(j) \equiv -t(p-j) \pmod p$. We now consider two cases.

If $p \equiv 1 \pmod 6$, then $t(-p) \equiv -t(2p) = -t(2) \pmod p$ and $t(-2p) = t(4)$, so that

$$t(0)+t(2)+t(4) \equiv 27\big(t(0)-t(2)+t(4)\big) \pmod p. \tag{29}$$

Then

$$\begin{aligned} a^p G_3(a) &= \sum_{j=0}^{5} a^{p+j} t(j) \equiv t(0)(a-a^2)+t(2)(a^3-a^6)+t(4)(a^5-a^4) \\ &= t(0)-2t(2)+t(4) = \frac{3}{2}\big(t(0)-t(2)+t(4)\big) - \frac{1}{2}\big(t(0)+t(2)+t(4)\big), \end{aligned}$$

and with (29) and (28) we get

$$a^p G_3(a) \equiv -\frac{4}{9}\big(t(0)+t(2)+t(4)\big) \equiv -\frac{2}{9} G_3(-1) \pmod p. \tag{30}$$

Second, if $p \equiv -1 \pmod 6$, then $t(-p) \equiv -t(2p) = -t(-2) = -t(4) \pmod p$ and $t(-2p) = t(2)$, so that

$$t(0)+t(2)+t(4) \equiv 27\big(t(0)+t(2)-t(4)\big) \pmod p. \tag{31}$$

Then, as before,

$$\begin{aligned} a^p G_3(a) &= \sum_{j=0}^{5} a^{p+j} t(j) \equiv t(0)(a^5-a^4)+t(2)(a-a^2)+t(4)(a^3-a^0) \\ &= t(0)+t(2)-2t(4) = \frac{3}{2}\big(t(0)+t(2)-t(4)\big) - \frac{1}{2}\big(t(0)+t(2)+t(4)\big), \end{aligned}$$

and with (31) and (28) we get (30) again. Finally, (30) combined with (26) gives $c_1 \equiv -\frac{2}{3} G_3(-1) \pmod p$, as required. This completes the first proof of Theorem 2.

4. Sums of Certain Arithmetic Functions Modulo p

Let $f : \mathbb{Z} \to \mathbb{Z}$ and suppose that there are fixed integers c and d with $p \nmid d$ such that for all $x, y \in \mathbb{Z}$ we have

$$f(x) \equiv f(y) \pmod{p} \quad \text{whenever} \quad x \equiv y \pmod{p}, \tag{32}$$

$$f(-x) \equiv -f(x) \pmod{p}, \tag{33}$$

$$f(2x) \equiv cf(x) \pmod{p}, \qquad f(6x) \equiv df(x) \pmod{p}. \tag{34}$$

Then clearly

$$\sum_{j=1}^{p-1} f(j) \equiv 0 \pmod{p}. \tag{35}$$

Furthermore, for each $0 \le r \le 5$ we set

$$t(r) := \sum_{\substack{j=1 \\ j \equiv r \pmod 6}}^{p-1} f(j) \quad \text{and} \quad u(r) := \sum_{r\frac{p}{6} < j < (r+1)\frac{p}{6}} f(j). \tag{36}$$

For integers j and r as in the sum for $t(r)$ we have $1 \le p - j \le p - 1$ and $p - j \equiv 1 - r \pmod 6$ when $p \equiv 1 \pmod 6$, and $p - j \equiv 5 - r \pmod 6$ when $p \equiv 5 \pmod 6$. Therefore we get with (33),

$$t(r) \equiv \begin{cases} -t(1-r) \pmod{p} & \text{for} \quad 0 \le r \le 1 \quad \text{and} \quad p \equiv 1 \pmod 6, \\ -t(7-r) \pmod{p} & \text{for} \quad 2 \le r \le 5 \quad \text{and} \quad p \equiv 1 \pmod 6, \\ -t(5-r) \pmod{p} & \text{for} \quad 0 \le r \le 5 \quad \text{and} \quad p \equiv 5 \pmod 6. \end{cases} \tag{37}$$

We also need congruences connecting the sums $t(r)$, $u(r)$ with each other.

Proposition 1. *Let $p \ge 5$ be a prime. Then for $p \equiv 1 \pmod 6$ we have*

$$t(r) \equiv \begin{cases} -du(5) \pmod{p} & \text{for} \quad r = 0, \\ -du(r-1) \pmod{p} & \text{for} \quad 1 \le r \le 5, \end{cases} \tag{38}$$

while for $p \equiv 5 \pmod 6$ we have

$$t(r) \equiv du(r) \pmod{p}, \qquad 0 \le r \le 5 \quad (p \equiv 5 \pmod 6). \tag{39}$$

Proof. First, let $p \equiv 1 \pmod 6$. When $r = 0$ we get with (36), and using successively the congruences (34), (33), and (32),

$$\begin{aligned} t(0) &= \sum_{j=1}^{\frac{p-1}{6}} f(6j) \equiv d \sum_{j=1}^{\frac{p-1}{6}} f(j) \equiv -d \sum_{j=1}^{\frac{p-1}{6}} f(-j) \pmod{p} \\ &\equiv -d \sum_{j=1}^{\frac{p-1}{6}} f(p-j) = -d \sum_{\frac{5p}{6} < j < p} f(j) = -du(5) \pmod{p}. \end{aligned}$$

Now let $1 \leq r \leq 5$. Then we get, using the same congruences as above,

$$t(r) = \sum_{j=0}^{\frac{p-1}{6}-1} f(r+6j) \equiv -\sum_{j=0}^{\frac{p-1}{6}-1} f(rp-r-6j) \pmod{p}$$
$$\equiv -d \sum_{j=0}^{\frac{p-1}{6}-1} f(r\tfrac{p-1}{6} - j) = -d \sum_{(r-1)\frac{p}{6}<j<r\frac{p}{6}} f(j) = -du(r-1) \pmod{p}.$$

Now let $p \equiv 5 \pmod 6$ and $0 \leq r \leq 5$. Using (32) and (34), as well as the fact that $f(0) \equiv 0 \pmod p$ by (33), we get with (36),

$$t(r) = \sum_{j=0}^{\frac{p+1}{6}-1} f(r+6j) \equiv \sum_{j=0}^{\frac{p+1}{6}-1} f(r+6j+rp) \pmod{p}$$
$$\equiv d \sum_{j=0}^{\frac{p+1}{6}-1} f(j + r\tfrac{p+1}{6}) = d \sum_{r\frac{p}{6}<j<(r+1)\frac{p}{6}} f(j) = du(r) \pmod{p},$$

which completes the proof of the proposition. □

Combining (38) and (39) with (37), we obtain the following congruence for both cases $p \equiv 1, 5 \pmod 6$; it also follows directly from the definition of $u(r)$.

Corollary 1. *For $p \geq 5$ and $0 \leq r \leq 5$ we have*

$$u(r) \equiv -u(5-r) \pmod{p}. \tag{40}$$

Next we derive congruences for several other sums involving the function $f(j)$.

Proposition 2. *Let $p \geq 5$ be a prime and suppose that the function $f : \mathbb{Z} \to \mathbb{Z}$ satisfies (32) – (34). Then*

$$\sum_{j=1}^{p-1} (-1)^j f(j) \equiv 2c \sum_{j=1}^{\frac{p-1}{2}} f(j) \pmod{p}, \tag{41}$$

$$\sum_{\frac{p}{6}<j<\frac{p}{3}} f(j) \equiv \frac{d-c}{2d} \sum_{j=1}^{\frac{p-1}{2}} f(j) \pmod{p}. \tag{42}$$

Proof. To simplify notation, let γ be the left-hand sum in (41) and w the right-hand sum in both (41) and (42). Furthermore, set

$$S = \sum_{\substack{j=1 \\ j \text{ even}}}^{p-1} f(j), \qquad L = \sum_{\substack{j=1 \\ j \text{ odd}}}^{p-1} f(j).$$

Then

$$S = \sum_{j=1}^{\frac{p-1}{2}} f(2j) \equiv c \sum_{j=1}^{\frac{p-1}{2}} f(j) = cw \pmod{p}.$$

From (34) we get $L \equiv -S \pmod{p}$; therefore $\gamma = -L + S \equiv 2S \pmod{p}$, and

$$\gamma \equiv 2cw \pmod{p}, \tag{43}$$

which gives (41). On the other hand,

$$\gamma = t(0) + t(2) + t(4) - t(1) - t(3) - t(5),$$

and by (38) and (40) we get for $p \equiv 1 \pmod{6}$,

$$\begin{aligned} \gamma &\equiv -d\big(u(5) + u(1) + u(3) - u(0) - u(2) - u(4)\big) \pmod{p} \\ &\equiv -d\big(-2u(0) + 2u(1) - 2u(2)\big) = 2d\big(w - 2u(1)\big) \pmod{p}. \end{aligned}$$

Similarly, with (39) and (40) we get for $p \equiv 5 \pmod{6}$,

$$\begin{aligned} \gamma &\equiv d\big(u(0) + u(2) + u(4) - u(1) - u(3) - u(5)\big) \pmod{p} \\ &\equiv d\big(2u(0) - 2u(1) + 2u(2)\big) = 2d\big(w - 2u(1)\big) \pmod{p}. \end{aligned}$$

Combining this with (43), we get in both cases,

$$u(1) \equiv \frac{d-c}{2d} w \pmod{p}, \tag{44}$$

which is the same as (42). □

Finally we derive the following consequence which will be useful later.

Corollary 2. *Let $p \geq 5$ be a prime, and let $A := t(0) - t(2) - t(3) + t(5)$, $B := t(1) + t(2) - t(4) - t(5)$, and $w := \sum_{j=1}^{\frac{p-1}{2}} f(j)$. Then*

$$A \equiv -B \equiv \frac{3d-c}{2} w \pmod{p} \qquad \textit{for} \quad p \equiv 1 \pmod{6}, \tag{45}$$

$$A \equiv 0 \pmod{p}, \quad B \equiv \frac{3d-c}{2} w \pmod{p} \qquad \textit{for} \quad p \equiv 5 \pmod{6}. \tag{46}$$

Proof. With (37), (38), and (40) we get for $p \equiv 1 \pmod{6}$,

$$\begin{aligned} A \equiv t(0) - 2t(2) - t(3) &\equiv d\big(u(0) + 2u(1) + u(2)\big) \pmod{p}, \\ B \equiv -t(0) + 2t(2) + t(3) &\equiv -A \pmod{p}, \end{aligned}$$

while with (37) and (39) we get for $p \equiv 5 \pmod{6}$,

$$\begin{aligned} A &\equiv 0 \pmod{p}, \\ B \equiv t(0) + 2t(1) + t(2) &\equiv d\big(u(0) + 2u(1) + u(2)\big) \pmod{p}. \end{aligned}$$

In both cases (44) is valid, so that

$$d\big(u(0) + 2u(1) + u(2)\big) \equiv d\big(w + \frac{d-c}{2d} w\big) = \frac{3d-c}{2} w \pmod{p},$$

which completes the proof. □

5. Second Proof of Theorem 2

Let $p \geq 5$ be a prime, and let $\mathbb{F}$ be a field containing $\mathbb{Z}/p\mathbb{Z}$ such that the polynomial $x^2 - x + 1 = x(x-1) + 1$ has a root a in $\mathbb{F}$. Then a is a primitive 6th root of unity, and in $\mathbb{F}$ we have for each integer n,

$$a^n = \begin{cases} a & \text{if} \quad n \equiv 1 \pmod 6, \\ -a+1 & \text{if} \quad n \equiv 5 \pmod 6. \end{cases} \tag{47}$$

Also, in Section 3 we saw that $q(a) = 0$.

The following results deal with values of the sum $G_3(x)$ defined in (8). In analogy to the general sum w in Corollary 2 we denote

$$W := \sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j^3}.$$

Proposition 3. *For all primes $p \geq 5$ we have in the field $\mathbb{F}$*

$$G_3(a) = \begin{cases} \frac{a-1}{18} W & \textit{when} \quad p \equiv 1 \pmod 6, \\ -\frac{a}{18} W & \textit{when} \quad p \equiv 5 \pmod 6, \end{cases} \tag{48}$$

or equivalently,

$$aG_3(a) = \begin{cases} -\frac{1}{18} W & \textit{when} \quad p \equiv 1 \pmod 6, \\ -\frac{a-1}{18} W & \textit{when} \quad p \equiv 5 \pmod 6. \end{cases} \tag{49}$$

Proof. We set $f(x) = x^{p-4}$ for $x \in \mathbb{Z}$. Then $f(x) \equiv \frac{1}{x^3} \pmod p$ for $p \nmid x$, and f has all the properties required in Section 4, with $c \equiv \frac{1}{2^3} \pmod p$ and $d \equiv \frac{1}{6^3} \pmod p$. Using the sums $t(r)$ as defined in (36) we get the following identity in $\mathbb{F}$:

$$G_3(a) = \sum_{j=1}^{p-1} \frac{a^j}{j^3} = \big(t(0) - t(2) - t(3) + t(5)\big) + a\big(t(1) + t(2) - t(4) - t(5)\big).$$

The identities in (48) now follow from Corollary 2. Finally, (48) and (49) are equivalent since in $\mathbb{F}$ we have $a(a-1) = -1$. □

We are now ready to determine the constant c_1 in (24).

Proposition 4. *For primes $p \geq 5$ we have*

$$c_1 \equiv -\frac{1}{6} \sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j^3} \pmod p. \tag{50}$$

Proof. We consider (24) as a polynomial identity in $\mathbb{F}$ and evaluate the various members for $x = a$. Since $q(a) = 0$, the left-hand side is 0. Next, by (48) and (47) we get

$$a^p G_3(a) = \begin{cases} a\frac{a-1}{18}W = \frac{a-1-a}{18}W & \text{when} \quad p \equiv 1 \pmod 6, \\ -(-a+1)\frac{a}{18}W = \frac{a-1-a}{18}W & \text{when} \quad p \equiv 5 \pmod 6, \end{cases}$$

and thus

$$a^p G_3(a) = -\frac{1}{18}W. \tag{51}$$

Now we consider the congruence (13) as a polynomial identity in $\mathbb{F}$ and obtain, since $\frac{1}{a} = 1-a$,

$$G_3(1-a) = G_3(\tfrac{1}{a}) = -\frac{1}{a^p}G_3(a).$$

Using (49) and (47) we get

$$G_3(1-a) = \begin{cases} -\frac{a}{18}W & \text{when} \quad p \equiv 1 \pmod 6, \\ \frac{a-1}{18}W & \text{when} \quad p \equiv 5 \pmod 6. \end{cases} \tag{52}$$

Since $1 - \frac{1}{a} = \frac{a-1}{a} = a$ we have, again with (48),

$$G_3(1-\tfrac{1}{a}) = \begin{cases} \frac{a-1}{18}W & \text{when} \quad p \equiv 1 \pmod 6, \\ -\frac{a}{18}W & \text{when} \quad p \equiv 5 \pmod 6. \end{cases} \tag{53}$$

If we note that, by (47), $a^p(1-a^p) = 1$ for all primes $p \geq 5$, and

$$1 - a^p = \begin{cases} 1-a, \\ a, \end{cases} \qquad a^{2p}(1-a^p) = \begin{cases} a & \text{for} \quad p \equiv 1 \pmod 6, \\ -a+1 & \text{for} \quad p \equiv 5 \pmod 6, \end{cases}$$

then with (51) – (53) the right-hand side of (24) with $x = a$ becomes

$$\begin{cases} \frac{W}{18}\big(1-(1-a)(-a)-a(a-1)\big) + c_1 & \text{for} \quad p \equiv 1 \pmod 6, \\ \frac{W}{18}\big(1-a(a-1)-(-a+1)(-a)\big) + c_1 & \text{for} \quad p \equiv 5 \pmod 6. \end{cases}$$

Since $a(a-1) = -1$ and $q(a) = 0$, we get in both cases $c_1 = -\frac{1}{6}W$, which completes the proof of (50). □

Proposition 5. *For primes $p \geq 3$ we have*

$$4G_3(-1) \equiv \sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j^3} \pmod p. \tag{54}$$

Proof. For $p \geq 5$ let f be the function defined in the proof of Proposition 3. Then (41) gives

$$G_3(-1) = \sum_{j=1}^{p-1} \frac{(-1)^j}{j^3} \equiv \sum_{j=1}^{p-1} (-1)^j f(j) \equiv \frac{1}{4} \sum_{j=1}^{\frac{p-1}{2}} f(j) \pmod{p},$$

which is the same as (54). The case $p = 3$ can be verified directly. □

It is now obvious that (24) combined with (50) and (54) completes the proof of Theorem 2. The congruence (54) also shows that (4) and (5) are equivalent.

Acknowledgments

Research on this paper was begun while the first author visited Masaryk University in Brno, partly supported by the Grant Agency of the Czech Republic. He wishes to thank the Department of Mathematics and Professor Radan Kučera for their hospitality.

References

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

[2] A. Granville, *The square of the Fermat quotient*, Integers: Electronic J. of Combinatorial Number Theory **4** (2004), #A22 (electronic).

[3] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, New York, 1979.