Математички Билтен
Vol.39 (LXV) No.2
2015 (13–18)
Скопје, Македонија

ISSN 0351-336X

UDC: 511.17:519.212.2

A CONGRUENCE FOR FERMAT QUOTIENT

MIOMIR ANDJIĆ AND ROMEO MEŠTROVIĆ

Abstract. Let p be a prime, and let $q_p(2) = (2^{p-1}-1)/p$ be the Fermat quotient of p to base 2. In this paper we prove that for any prime $p > 3$

$$q_p(2) \equiv \frac{(-1)^{\lfloor p/3\rfloor - \lfloor p/6\rfloor} 3^{(p-1)/2} - 1}{p} - \frac{(-1)^{\lfloor p/3\rfloor - \lfloor p/6\rfloor} 3^{(p-3)/2}}{2} \sum_{k=(p+1)/2}^{p-1} \frac{(-3)^k}{k} \pmod p,$$

where $\lfloor a\rfloor$ denotes the greatest integer not exceeding a.

1. Introduction and the main result

If p is a prime and a is an integer not divisible by p, then by Fermat little theorem $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. 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 according to Fermat little theorem. This quotient has been extensively studied because of its links to numerous question in Number Theory. In particular, Fermat quotients appear and play a major role in various questions of computational and algebraic number theory (see the survey [5] of classical result). Among other properties, the p-divisibility of Fermat quotient $q_p(a)$ by p has numerous applications which include the Fermat Last Theorem and squarefreeness testing (see [1], [2], [8], [11], [18] and [20]).

Here, as usually in the sequel, we consider the congruence relation modulo a prime power p^e extended to the ring of rational numbers with denominators not divisible by p. For such fractions we put $m/n \equiv r/s \,(\mathrm{mod}\, p^e)$ if and only if $ms \equiv nr \,(\mathrm{mod}\, p^e)$, and the residue class of m/n is the residue class of mn' where n' is the inverse of n modulo p^e.

2010 *Mathematics Subject Classification.* 11A07; 05A10, 05A19, 11B65.

Key words and phrases. Fermat quotient, congruence modulo a prime (prime power), de Moivre's formula.

A classical congruence, due to F. G. Eisenstein [4] in 1850, asserts that for a prime $p \geq 3$,

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

which was extended in 1861 by J. J. Sylvester [22] and in 1901 by J. W. L. Glaisher [7, pp. 21–22] as

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

The above congruence was generalized in 1905 by M. Lerch in the first paper of substance on Fermat quotients [12] (see also [1, pp. 32–35]). Lerch developed equivalent results entailing fewer terms.

As noticed in [16], the connection of Fermat quotients with the first case of Fermat Last Theorem retains its historical interest despite the complete proof of this theorem by A. Wiles in 1995, and Skula's demonstration in 1992 [20] that the failure of the first case of Fermat Last Theorem would imply the vanishing of many similar sums but with much smaller ranges (sums of Lerch's type which cannot be evaluated in terms of Fermat quotients). Some criteria concerning the first case of Fermat Last Theorem on Lerch's type sums were established in Ribenboim's book [18], in 1995 by Dilcher and Skula [2] (cf. [3, Section 8]) and in 2012 by J. B. Dobson [3].

In 1900 J. W. L. Glaisher [6] proved that for a prime $p \geq 3$ it holds a curious congruence

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

Another variation of Eisenstein's congruence (1.1) and Glaisher's congruence (1.2) was obtained in 1997 by W. Kohnen [10] (also see [13]).

In 2004 L. Skula [9] conjectured that

$$q_p(2)^2 \equiv -\sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p}. \tag{1.3}$$

Applying a certain polynomial congruence, A. Granville [9] proved the congruence (1.3). In [15] the second author of this paper established a simple and elementary proof of the congruence (1.3).

In [21, Theorem 4.1] Z.-H. Sun extended the congruences (1.2) and (1.3) modulo p^3 and p^2, respectively. Furthermore, these Sun's congruences are extended in [14, Theorem 1.5] and [16, Theorem 1.2]. Notice also that some curious combinatorial congruences modulo p^2 involving the Fermat quotient $q_p(2)$ are recently established in [17].

Here we prove the following result.

Theorem 1. *Let $p > 3$ be a prime. Then*

$$\begin{aligned} q_p(2) \equiv & \frac{(-1)^{\lfloor p/3 \rfloor - \lfloor p/6 \rfloor} 3^{(p-1)/2} - 1}{p} \\ & - \frac{(-1)^{\lfloor p/3 \rfloor - \lfloor p/6 \rfloor} 3^{(p-3)/2}}{2} \sum_{k=(p+1)/2}^{p-1} \frac{(-3)^k}{k} \pmod{p}, \end{aligned} \tag{1.4}$$

where $\lfloor a \rfloor$ denotes the greatest integer not exceeding a.

As an immediate consequence of Theorem 1, we obtain the known result concerning the Legendre symbol $\left(\frac{3}{p}\right)$ for a prime $p > 3$ (see, e.g., [19, §7.3, p. 257, Exercise 2]).

Corollary 1.1. *Let $p > 3$ be a prime. Then*

$$3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) \equiv (-1)^{\lfloor p/3 \rfloor - \lfloor p/6 \rfloor} \pmod{p}.$$

Proof of Theorem 1 is elementary and it is based on de Moivre's formula and some congruences modulo a prime.

2. Proof of Theorem 1 and Corollary 1.1

Lemma 1. *Let $p > 3$ be a prime, and let n be a positive integer such that $p = 6n-1$ or $p = 6n+1$. Then*

$$q_p(2) = \frac{(-1)^n 3^{(p-1)/2} - 1}{p} + (-1)^n \sum_{j=1}^{(p-1)/2} \frac{1}{2j} \binom{p-1}{2j-1} (-1)^j 3^{(p-1-2j)/2}. \tag{2.1}$$

Proof. By using the binomial expansion and the identity $\binom{m}{k} = \frac{m}{k}\binom{m-1}{k-1}$ with $1 \le k \le m$, we have

$$\begin{aligned} (\sqrt{3}+i)^p + (\sqrt{3}-i)^p &= \sum_{k=0}^{p} \binom{p}{k} \sqrt{3}^{p-k} i^k + \sum_{k=0}^{p} (-1)^k \binom{p}{k} \sqrt{3}^{p-k} i^k \\ &= 2 \sum_{j=0}^{(p-1)/2} (-1)^j \binom{p}{2j} \sqrt{3}^{p-2j} \\ &= 2\sqrt{3} \sum_{j=0}^{(p-1)/2} (-1)^j \binom{p}{2j} 3^{(p-1-2j)/2} \\ &= 2 \cdot 3^{p/2} + 2\sqrt{3} \sum_{j=1}^{(p-1)/2} (-1)^j \frac{p}{2j} \binom{p-1}{2j-1} 3^{(p-1-2j)/2}. \end{aligned} \tag{2.2}$$

On the other hand, by de Moivre's formula, we have

$$\begin{aligned}(\sqrt{3}+i)^p+(\sqrt{3}-i)^p =& 2^p\left(\left(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}\right)^p+\left(\cos\frac{\pi}{6}-i\sin\frac{\pi}{6}\right)\right)^p\\ =& 2^{p+1}\cos\frac{p\pi}{6}.\end{aligned} \tag{2.3}$$

If $p=6n\pm1$ with a positive integer n, then

$$\cos\frac{p\pi}{6}=\cos\frac{(6n\pm1)\pi}{6}=\cos\left(n\pi\pm\frac{\pi}{6}\right)=(-1)^n\frac{\sqrt{3}}{2}. \tag{2.4}$$

Comparing (2.2), (2.3) and (2.4), we obtain

$$(-1)^n2^{p-1}=3^{(p-1)/2}+\sum_{j=1}^{(p-1)/2}\frac{p}{2j}\binom{p-1}{2j-1}(-1)^j3^{(p-1-2j)/2}. \tag{2.5}$$

Since $2^{p-1}=pq_p(2)+1$, substituting this into (2.5) immediately gives (2.1). □

Proof of Theorem 1. Let n be a positive integer defined as in Lemma 1, that is, $p=6n\pm1$.

Notice that for each $j=1,2,\dots,(p-1)/2$ there holds

$$\begin{aligned}\binom{p-1}{2j-1}&=\frac{(p-1)(p-2)\cdots(p-(2j-1))}{(2j-1)!}\\ &\equiv\frac{(0-1)(0-2)\cdots(0-(2j-1))}{(2j-1)!}\\ &=\frac{(-1)^{2j-1}(2j-1)!}{(2j-1)!}=-1\pmod p.\end{aligned} \tag{2.6}$$

Substituting (2.6) into (2.1) of Lemma 1 and using the fact that $3^{p-1}\equiv1(\bmod p)$, we get

$$\begin{aligned}q_p(2)&\equiv\frac{(-1)^n3^{(p-1)/2}-1}{p}+(-1)^n\sum_{j=1}^{(p-1)/2}\frac{(-1)^{j-1}}{2j}3^{(p-1-2j)/2}\pmod p\\ &=\frac{(-1)^n3^{(p-1)/2}-1}{p}-\frac{(-1)^n3^{(p-1)/2}}{2}\sum_{j=1}^{(p-1)/2}\frac{(-1)^j}{j}3^{-j}\\ &\equiv\frac{(-1)^n3^{(p-1)/2}-1}{p}+\frac{(-1)^n3^{(p-1)/2}}{2}\sum_{j=1}^{(p-1)/2}\frac{(-1)^{p-1-j}}{p-j}3^{p-1-j}\pmod p\\ &=\frac{(-1)^n3^{(p-1)/2}-1}{p}+\frac{(-1)^n3^{(p-1)/2}}{2}\sum_{k=(p+1)/2}^{p-1}\frac{(-3)^{k-1}}{k}\\ &=\frac{(-1)^n3^{(p-1)/2}-1}{p}-\frac{(-1)^n3^{(p-3)/2}}{2}\sum_{k=(p+1)/2}^{p-1}\frac{(-3)^k}{k}\pmod p.\end{aligned} \tag{2.7}$$

Since $p = 6n \pm 1$ implies that $n = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor$, substituting this into (2.7) yields the congruence (1.4) of Theorem 1. □

Proof of Corollary 1.1. From the congruence (1.4) of Theorem 1 we see that that

$$(-1)^{\lfloor p/3 \rfloor - \lfloor p/6 \rfloor} 3^{(p-1)/2} - 1 \equiv 0 \pmod{p},$$

or equivalently,

$$3^{(p-1)/2} \equiv (-1)^{\lfloor p/3 \rfloor - \lfloor p/6 \rfloor} \pmod{p}.$$

This together with the fact that by the well known Euler's criterion, for any prime $p > 3$ we have

$$3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) \pmod{p}$$

concludes the proof. □

References

[1] T. Agoh, K. Dilcher and L. Skula, *Fermat quotients for composite moduli*, J. Number Theory, 66 (1997) 29–50. MR 1467188.

[2] K. Dilcher, L. Skula, *A new criterion for the first case of Fermat's last theorem*, Math. Comp., 64 (1995) 363–392.

[3] J. B. Dobson, *On Lerch's formula for the Fermat quotient*, preprint `arXiv:1103.3907v3 [math.NT]` (2012).

[4] F. G. Eisenstein, *Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definirt werden*, Bericht. K. Preuss. Akad. Wiss. Berlin, 15 (1850) 36–42 (Reprinted in *Mathematische Werke*, Chelsea, New York, 1975, Vol. 2, 705–711).

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

[6] 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*, Q. J. Math., 31 (1900) 321–353.

[7] J. W. L. Glaisher, *On the residues of r^{p-1} to modulus p^2, p^3, etc.*, Q. J. Math., 32 (1901) 1–27.

[8] A. Granville, *Some conjectures related to Fermat's Last Theorem*, In Number Theory, R. A. Mollin (ed.), W. de Gruyter, Berlin, New York, 1990, 177–192.

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

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

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

[12] M. Lerch, *Zur Theorie des Fermatschen Quotienten $(a^{p-1}-1)/p = q(a)$*, Math. Ann., 60 (1905) 471–490.

[13] R. Meštrović, *An extension of a congruence by Kohnen*, preprint `arXiv:1109.2340v3 [math.NT]` (2011).

[14] R. Meštrović, *An extension of Sury's identity and related congruences*, Bull. Austral. Math. Soc., 85 (2012) 482–496.

[15] R. Meštrović, *An elementary proof of a congruence by Skula and Granville*, Arch. Math. (Brno) 48 (2012) 113–120.

[16] R. Meštrović, *Congruences involving the Fermat quotient*, Czechoslovak Math. J., 63 (2013) 949–968.

[17] R. Meštrović, *Five curious congruences modulo p^2*, Math. Slovaca 65 (2015), 451–462.

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

[19] H. N. Shapiro, *Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 1983.

[20] L. Skula, *Fermat's last theorem and the Fermat quotients*, Comment. Math. Univ. St. Pauli, 41 (1) (1992) 35–54.
[21] Z.-H. Sun, *Congruences involving Bernoulli and Euler numbers*, J. Number Theory 128 (2008) 280–312.
[22] J. J. Sylvester, *Sur une propriété des nombres premiers qui se ratache au théorème de Fermat*, C. R. Acad. Sci. Paris 52 (1861) 161–163 (Reprinted in Sylvester's Collected Math. Papers, Vol. 2, 229–231, Cambridge Univ. Press, 1908).

Faculty for Information Technology,
University "Mediterranean", Podgorica, Montenegro
Email address: miomir.andjic@unimediteran.net

Maritime Faculty, University of Montenegro, Kotor, Montenegro
Email address: romeo@ac.me