International Journal of Number Theory

A q-congruence involving the Jacobi symbol

Victor J. W. Guo

School of Mathematical Sciences, Huaiyin Normal University
Huai'an 223300, Jiangsu, People's Republic of China
jwguo@hytc.edu.cn

He-Xia Ni*

Department of Applied Mathematics, Nanjing Audit University
Nanjing 211815, People's Republic of China
nihexia@yeah.net

Received (Day Month Year)
Accepted (Day Month Year)

Let n be a positive odd integer and m a positive integer with $\gcd(m,n)=1$. We prove that

$$\frac{(q^m;q^m)_{(n-1)/2}}{(q;q)_{(n-1)/2}} \equiv \begin{cases} (\frac{m}{n})q^{\frac{(m-1)(n^2-1)}{16}} \pmod{\Phi_n(q)}, & \text{if } 16|(m-1)(n^2-1), \\ (\frac{m}{n})q^{\frac{(m-1)(n^2-1)+8n}{16}} \pmod{\Phi_n(q)}, & \text{otherwise.} \end{cases}$$

Here $(x;q)_n = (1-x)(1-xq)\cdots(1-xq^{n-1})$, $(\frac{m}{n})$ denotes the Jacobi symbol, and $\Phi_n(q)$ is the n-th cyclotomic polynomial in q. This confirms a recent conjecture of the first author.

Keywords: congruence; cyclotomic polynomial; Fermat's little theorem.

Mathematics Subject Classification 2010: 05A30, 11A07

1. Introduction

Let p be an odd prime. For any positive integer a with $p \nmid a$, the well-known Fermat's little theorem asserts that

$$a^{p-1} \equiv 1 \pmod{p}.$$

Cao and Pan [1] noted that a q-analogue of Fermat's little theorem is as follows:

$$\frac{(q^a;q^a)_{p-1}}{(q;q)_{p-1}} \equiv 1 \pmod{[p]},$$

*Corresponding author.

where $(x;q)_n=(1-x)(1-xq)\cdots(1-xq^{n-1})$ and $[p]=1+q+\cdots+q^{p-1}$. Let $\left(\frac{a}{p}\right)$ be the Legendre symbol modulo p. They also showed that, for any odd prime p and positive integer a with $p\nmid a$,

$$q^{a-1}\frac{(q^{16a};q^{16a})_{(p-1)/2}}{(q^{16};q^{16})_{(p-1)/2}}\equiv\left(\frac{a}{p}\right)\pmod{[p]}, \tag{1.1}$$

which is clearly a q-analogue of the congruence $a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\pmod p$.

Let $\Phi_n(q)$ be the n-th cyclotomic polynomial in q. It is easy to see that $\Phi_p(q)=[p]$ for any prime p. The aim of this note is to give the following result, which was originally conjectured by the first author [3, Conjecture 4.2].

Theorem 1.1. *Let $m,n>1$ be positive integers with n odd and $\gcd(m,n)=1$. Then*

$$\frac{(q^m;q^m)_{(n-1)/2}}{(q;q)_{(n-1)/2}}\equiv\begin{cases}(\frac{m}{n})q^{\frac{(m-1)(n^2-1)}{16}}\pmod{\Phi_n(q)}, & \text{if } 16|(m-1)(n^2-1),\\ (\frac{m}{n})q^{\frac{(m-1)(n^2-1)+8n}{16}}\pmod{\Phi_n(q)}, & \text{otherwise.}\end{cases} \tag{1.2}$$

Here, $\left(\frac{m}{n}\right)$ is the Jacobi symbol.

Note that the congruence (1.2) is trivial for $\gcd(m,n)>1$. In this case we have $\left(\frac{m}{n}\right)=0$, and there exists some $k\in\{1,2,\ldots,(n-1)/2\}$ such that n divides mk, which leads to $(q^m;q^m)_{(n-1)/2}\equiv 0\pmod{\Phi_n(q)}$.

It is easy to see that $\Phi_n(q)$ divides $\Phi_n(q^2)$ and so $\Phi_n(q)$ divides $\Phi_n(q^{16})$ too. Hence, replacing q by q^{16} in (1.2) and noticing that $q^n\equiv 1\pmod{\Phi_n(q)}$, we obtain

$$\frac{(q^{16m};q^{16m})_{(n-1)/2}}{(q^{16};q^{16})_{(n-1)/2}}\equiv\left(\frac{m}{n}\right)q^{1-m}\pmod{\Phi_n(q)},$$

which reduces to (1.1) when $n=p$ is an odd prime. Namely, the congruence (1.2) is a generalization of (1.1).

2. Proof of Theorem 1.1

For any integer t, let $\langle t\rangle_n$ stand for the least non-negative residue of t modulo n. Let

$$R_n(m)=\{1\leqslant r<n/2\,|\,\langle mr\rangle_n>n/2\}.$$

The well-known Gauss' lemma (see, for example, [6] or [7, Theorem 4.5]) states that

$$\left(\frac{m}{n}\right)=(-1)^{|R_n(m)|}.$$

Moreover, we need the following result due to Cao and Pan [1, Lemma 2]. In order to make the paper more self-contained, we include their proof here.

Lemma 2.1. *Let $m, n > 1$ be positive integers with n odd and* $\gcd(m, n) = 1$. *Then*

$$\sum_{j\in R_n(m)} j \equiv \frac{1-m}{16m} \pmod{n}.$$

Proof. It is easy to see that

$$\sum_{j\in R_n(-m)} j = \sum_{\substack{1\leqslant j<n/2\\ \langle -jm\rangle_n > n/2}} j = \sum_{\substack{1\leqslant j<n/2\\ \langle jm\rangle_n < n/2}} j,$$

and so

$$\sum_{j\in R_n(m)} j + \sum_{j\in R_n(-m)} j = \sum_{j=1}^{(n-1)/2} j = \frac{(n^2-1)}{8} \equiv -\frac{1}{8} \pmod{n}. \tag{2.1}$$

Moreover, for every integer j with $1 \leqslant j < n/2$, the inequality $\langle jm\rangle_n > n/2$ holds if and only if there exists an integer $s \in \{1, 2, \ldots, (n-1)/2\}$ such that

$$jm \equiv -s \pmod{n},$$

namely,

$$sm^{-1} \equiv -j \pmod{n}.$$

It follows that

$$\sum_{j\in R_n(m)} j = \sum_{\substack{1\leqslant j<n/2\\ \langle jm\rangle_n > n/2}} j \equiv m^{-1} \sum_{\substack{1\leqslant s<n/2\\ \langle sm^{-1}\rangle_n > n/2}} (-s) = -m^{-1} \sum_{s\in R_n(m^{-1})} s \pmod{n},$$

and so

$$\sum_{j\in R_n(m)} j - \sum_{j\in R_n(-m)} j \equiv -m^{-1} \sum_{s\in R_n(m^{-1})} s - m^{-1} \sum_{s\in R_n(-m^{-1})} s \equiv \frac{1}{8}m^{-1} \pmod{n}, \tag{2.2}$$

where the second congruence follows from (2.1). Combining (2.1) and (2.2), we complete the proof of Lemma 2.1. □

Proof of Theorem 1.1. For any integer r, let $\pm t_r \in \{(1-n)/2, \ldots, -1, 0, 1, \ldots, (n-1)/2\}$ be the residue of mr modulo n, where t_r is non-negative. By definition, the cardinality $|R_n(m)|$ is clearly the number of negative signs in $\{\pm t_r \,|\, 1 \leqslant r < n/2\}$. We claim that $t_i \neq t_j$ for $1 \leqslant i < j \leqslant (n-1)/2$. In fact, if $t_i = t_j$ for some i and j with $1 \leqslant i < j \leqslant (n-1)/2$, then $mi \equiv \pm mj \pmod{n}$. Since $\gcd(m, n) = 1$, we must have $i \pm j \equiv 0 \pmod{n}$. But this is impossible because $1 \leqslant |i \pm j| \leqslant |i| + |j| \leqslant n-1$. It follows that the set $\{t_1, t_2, \ldots, t_{(n-1)/2}\}$ coincides with the set $\{1, 2, \ldots, (n-1)/2\}$,

and so

$$\frac{(q^m;q^m)_{(n-1)/2}}{(q;q)_{(n-1)/2}} = \frac{(1-q^m)(1-q^{2m})\dots(1-q^{\frac{(n-1)m}{2}})}{(1-q)(1-q^2)\dots(1-q^{\frac{n-1}{2}})}$$
$$\equiv (-1)^{|R_n(m)|}q^{\sum_{j\in R_n(m)} jm}$$
$$= \Big(\frac{m}{n}\Big)\, q^{\sum_{j\in R_n(m)} jm} \pmod{\Phi_n(q)}.$$

By Lemma 2.1, we have

$$\sum_{j\in R_n(m)} jm \equiv \frac{1-m}{16} \equiv \begin{cases} \frac{(m-1)(n^2-1)}{16} \pmod n, & \text{if } 16|(m-1)(n^2-1), \\ \frac{(m-1)(n^2-1)+8n}{16} \pmod n, & \text{otherwise.} \end{cases}$$

The proof of (1.2) then follows from the fact that $q^r \equiv q^s \pmod{\Phi_n(q)}$ if $r \equiv s \pmod n$. □

3. Concluding remarks

Cao and Pan [1] proved (1.1) by using Gauss' lemma and Lemma 2.1. On the other hand, the congruence (1.2) for n being an odd prime power was proved by the first author [3, Theorem 4.3] without using Gauss' lemma. Since the congruence (1.1) can be deduced from the congruence (1.2) for $n = p$, a simple proof of (1.1) independent of Gauss' lemma can be easily given. However, Gauss' lemma plays an important role in our proof of (1.2) for general n. We do not know any other proof of (1.2) without using Gauss' lemma.

As already pointed by the first author [3], replacing q by q^2 in (1.2) and noticing that $q^n \equiv 1 \pmod{\Phi_n(q)}$, we obtain the following conclusion: for any positive odd n,

$$\frac{(q^{2m};q^{2m})_{(n-1)/2}}{(q^2;q^2)_{(n-1)/2}} \equiv \Big(\frac{m}{n}\Big)\, q^{\frac{(m-1)(n^2-1)}{8}} \pmod{\Phi_n(q)},$$

which in the $m = 2$ case gives

$$(-q^2;q^2)_{(n-1)/2} \equiv (-1)^{\frac{n^2-1}{8}} q^{\frac{n^2-1}{8}} \pmod{\Phi_n(q)}. \tag{3.1}$$

Moreover, using the q-WZ (Wilf–Zeilberger) method [8], the first author [3, (2.17)] proved that

$$\sum_{k=0}^{n-1}(-1)^k[6k+1]\frac{(q;q^2)_k^3}{(q^4;q^4)_k^3} \equiv \frac{(-1)^{\frac{n-1}{2}}[n]q^{\frac{1-n^2}{2}}}{(-q^2;q^2)_{(n-1)/2}} \pmod{[n]\Phi_n(q)} \tag{3.2}$$

(for more q-congruences proved by this method, we refer the reader to [2,4]). From (3.1) and (3.2) we immediately deduce that

$$\sum_{k=0}^{n-1}(-1)^k[6k+1]\frac{(q;q^2)_k^3}{(q^4;q^4)_k^3} \equiv [n](-q)^{-\frac{(n-1)(n+5)}{8}} \pmod{[n]\Phi_n(q)}.$$

It was conjectured in [3, Conjecture 1.1] that the above congruence still holds modulo $[n]\Phi_n(q)^2$, which was later confirmed by the first author and Zudilin [5] using the creative microscoping method.

Acknowledgments. We thank the anonymous referee for a careful reading of this paper. The first author was partially supported by the National Natural Science Foundation of China (grant 11771175). The second author was partially supported by Nanjing University Innovation and Creative Program for PhD candidate (grant CXCY17-10) and the National Natural Science Foundation of China (grant 11571162).

References

[1] H. Cao and H. Pan, On the q-analogue of quadratic residues, *Nanjing Daxue Xuebao Shuxue Bannian Kan* **23** (2006), 136–139.

[2] V. J. W. Guo, A q-analogue of a Ramanujan-type supercongruence involving central binomial coefficients, *J. Math. Anal. Appl.* **458** (2018), 590–600.

[3] V. J. W. Guo, A q-analogue of the (L.2) supercongruence of Van Hamme, *J. Math. Anal. Appl.* **466** (2018), 749–761.

[4] V. J. W. Guo, q-Analogues of two "divergent" Ramanujan-type supercongruences, *Ramanujan J.*, in press; https://doi.org/10.1007/s11139-019-00161-0

[5] V. J. W. Guo and W. Zudilin, A q-microscope for supercongruences, *Adv. Math.* **346** (2019), 329–358.

[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd Edition, Spring-Verlag, New York, 1990.

[7] F. Lemmermeyer, *Reciprocity Laws from Euler to Eisenstein*, Springer-Verlag, Berlin Heidelberg, 2000.

[8] H. S. Wilf and D. Zeilberger, An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities, *Invent. Math.* **108** (1992), 575–633.