Proof of a supercongruence conjectured by Sun through a $q$-microscope

VICTOR J W GUO

School of Mathematics and Statistics, Huaiyin Normal University, Huai’an 223300, Jiangsu, People’s Republic of China
E-mail: jwguo@hytc.edu.cn

MS received 18 December 2019; accepted 29 March 2020

Abstract. In 2011, Sun (Sci. China Math. 54 (2011) 2509–2535) made the following conjecture: for any odd prime $p$ and odd integer $m$,

$$
\frac{1}{m^2((m-1)/2)} \sum_{k=0}^{(m-1)/2} \left( \begin{array}{c} 2k \\ k \end{array} \right) 8^k - \left( \begin{array}{c} 2 \\ p \end{array} \right) \sum_{k=0}^{(m-1)/2} \left( \begin{array}{c} 2k \\ k \end{array} \right) 8^k \equiv 0 \pmod{p^2}.
$$


Keywords. Cyclotomic polynomial; $q$-binomial coefficient; $q$-congruence; super congruence; creative microscoping.

Mathematics Subject Classification. 11B65, 11A07, 33D15.

1. Introduction

During the past decade, congruences and supercongruences have been studied by quite a few authors. In 2011, Sun [14, Equation (1.6)] proved that, for any odd prime $p$,

$$
\sum_{k=0}^{(p-1)/2} \left( \begin{array}{c} 2k \\ k \end{array} \right) 8^k \equiv \left( \frac{2}{p} \right) + \left( \frac{-2}{p} \right) \frac{p^2}{4} E_{p-3} \pmod{p^3},
$$

where $\left( \frac{m}{n} \right)$ denotes the Jacobi symbol and $E_n$ is the $n$th Euler number. Later, Sun [15, Equation (1.7)] further proved that

$$
\sum_{k=0}^{(p'-1)/2} \left( \begin{array}{c} 2k \\ k \end{array} \right) 8^k \equiv \left( \frac{2}{p'} \right) \pmod{p^2}. \quad (1.1)
$$

© Indian Academy of Sciences
Published online: 20 October 2020
Recently, Sun [16, Conjecture 4(ii)] proposed the following conjecture: for any odd prime \( p \) and odd integer \( m \),

\[
\frac{1}{m^2} \left( \sum_{k=0}^{(m-1)/2} \frac{\binom{2k}{k}}{8^k} - \frac{2}{p} \sum_{k=0}^{(m-1)/2} \frac{\binom{2k}{k}}{8^k} \right) \equiv 0 \pmod{p^2}, \tag{1.2}
\]

which is clearly a generalization of (1.1).

In the past few years, \( q \)-analogues of congruences and supercongruences have caught the interest of a lot of people (see [3–13,17]). In particular, Guo and Liu [8] gave the following \( q \)-analogue of (1.1): for odd \( n > 1 \),

\[
\sum_{k=0}^{(n-1)/2} q^{k^2} \frac{(q; q^2)_k}{(q^4; q^4)_k} \equiv (-q)^{(1-n^2)/8} (\Phi_n(q))^2. \tag{1.3}
\]

Here and in what follows, \( (a; q)_n = (1-a)(1-aq) \cdots (1-aq^{n-1}) \), \( n = 0, 1, \ldots \), or \( n = \infty \), is the \( q \)-shifted factorial, and \( \Phi_n(q) \) is the \( n \)-th cyclotomic polynomial in \( q \) given by

\[
\Phi_n(q) = \prod_{1 \leq k \leq n \atop \gcd(n,k)=1} (q - \zeta^k),
\]

where \( \zeta \) is an \( n \)-th primitive root of unity. Moreover, Gu and Guo [4] gave some different \( q \)-analogues of (1.1), such as

\[
\sum_{k=0}^{(n-1)/2} \frac{(q; q^2)_k q^{2k}}{(-q^2; q^4)_k q^{2k}} \equiv \left( \frac{2}{n} \right) q^{2\lfloor (n+1)/4 \rfloor^2} (\Phi_n(q))^2, \tag{1.4}
\]

where \( \lfloor x \rfloor \) denotes the largest integer not exceeding \( x \). In order to prove Sun’s conjecture (1.2), we need the following new \( q \)-analogue of (1.1).

**Theorem 1.1.** Let \( n > 1 \) be an odd integer. Then

\[
\sum_{k=0}^{(n-1)/2} \frac{(q; q^2)_k (-1; q^4)_k q^{2k}}{(-q^2; q^4)_k (q^4; q^4)_k} \equiv \left( \frac{2}{n} \right) (\Phi_n(q))^2. \tag{1.5}
\]

Recall that the \( q \)-integer is defined by \( [n]_q = 1 + q + \cdots + q^{n-1} \) and the \( q \)-binomial coefficient \( \binom{m}{n}_q \) is defined as

\[
\binom{m}{n}_q = \begin{cases} 
\frac{(q; q)_m}{(q; q)_n (q; q)_{m-n}}, & \text{if } 0 \leq n \leq m, \\
0, & \text{otherwise}.
\end{cases}
\]

On the basis of (1.5), we are able to give the following \( q \)-analogue of (1.2).
Theorem 1.2. Let m and n be positive odd integers with n > 1. Then

\[
\frac{1}{[m]^2 [(m-1)/2]} q^{n^2} \left( \sum_{k=0}^{(m-1)/2} \frac{(q; q^2)^k(-1; q^4)^k}{(-q; q^2)^k(q^4; q^4)_k} q^{2k} \right)

\equiv 0 \pmod{\Phi_n(q)^2}.
\]

(1.6)

Moreover, the denominator of (the reduced form of) the left-hand side of (1.6) is relatively prime to \(\Phi_n(q)^2\) for any index \(j \geq 2\).

It is well known that \(\Phi_n(1) = p\) if \(n\) is a prime power \(p^r\) \((r \geq 1)\) and \(\Phi_n(1) = 1\) otherwise. Moreover, the denominator of (1.6) is no doubt a product of cyclotomic polynomials. This means that (1.2) immediately follows from (1.6) by letting \(n = p\) and taking the limits as \(q \to 1\).

We shall prove Theorem 1.1 in the next section. The proof of Theorem 1.2 will be given in Section 3 by using the method of “creative microscoping” recently introduced by Guo and Zudilin [10]. More precisely, we shall first give a generalization of Theorem 1.2 with an extra parameter \(a\), and Theorem 1.2 then follows from this generalization by taking \(a \to 1\). Finally, in Section 4, we give some hints on solving another similar conjecture of Sun.

2. Proof of Theorem 1.1

It is easy to check that

\[
(1 - q^{n-2j+1})(1 - q^{n+2j-1}) + (1 - q^{2j-1})^2 q^{n-2j+1} \equiv (1 - q^n)^2,
\]

and so

\[
(1 - q^{n-2j+1})(1 - q^{n+2j-1}) \equiv -(1 - q^{2j-1})^2 q^{n-2j+1} \pmod{\Phi_n(q)^2}
\]

since \(1 - q^n \equiv 0 \pmod{\Phi_n(q)}\). Thus, we have

\[
(q^{1-n}; q^2)_k(q^{1+n}; q^2)_k = (-1)^k q^{k^2-nk} \prod_{j=1}^{k} (1 - q^{n-2j+1})(1 - q^{n+2j-1})
\]

\[
\equiv q^{k^2-nk} \prod_{j=1}^{k} (1 - q^{2j-1}) q^{n-2j+1}
\]

\[
= (q; q^2)^2_k \pmod{\Phi_n(q)^2}.
\]

It follows that

\[
\sum_{k=0}^{(n-1)/2} \frac{(q; q^2)_k(-1; q^4)^k}{(-q; q^2)^k(q^4; q^4)_k} q^{2k} \equiv \sum_{k=0}^{(n-1)/2} \frac{(q^{1-n}; q^2)_k(q^{1+n}; q^2)_k(-1; q^4)^k}{(q; q^2)_k(-q; q^2)_k(q^4; q^4)_k} q^{2k}
\]

\[
= \left( \frac{2}{n} \right) \pmod{\Phi_n(q)^2}.
\]

(2.1)
Here the last step in (2.1) follows from a terminating $q$-analogue of Whipple’s $3F_2$ sum [2, Appendix (II.19)]:

\[
\sum_{k=0}^{n} \frac{(q^{-n}; q)_k(q^{n+1}; q)_k(c; q)_k(-c; q)_k}{(e; q)_k(c^2q/e; q)_k(q; q)_k(-q; q)_k} q^k
\]

\[
= \frac{(eq^{-n}; q^2)\infty(eq^{n+1}; q^2)\infty(c^2q^{1-n}/e; q^2)\infty(c^2q^{n+2}/e; q^2)\infty}{(e; q)\infty(c^2q/e; q)\infty} q^{n(n+1)/2}
\]

with $n \mapsto (n-1)/2$, $q \mapsto q^2$, $c^2 = -1$ and $e = q$.

3. Proof of Theorem 1.2

We first establish the following parametric generalization of Theorem 1.2.

**Theorem 3.1.** Let $m$ and $n$ be positive odd integers with $n > 1$. Then, modulo

\[
\prod_{j=0}^{(m-1)/2} (1 - a q^{(2j+1)n})(a - q^{(2j+1)n}),
\]

we have

\[
\sum_{k=0}^{(mn-1)/2} \frac{(aq^n; q^2)_k(q^n/a; q^2)_k(-1; q^4)_k}{(q^2)_k(-q^n; q^2)_k(q^4; q^4)_k} q^{2k} 
\equiv \left( \frac{2}{n} \right) \sum_{k=0}^{(m-1)/2} \frac{(aq^n; q^2)_k(q^{n/2}/a; q^{2n})_k(-1; q^{4n})_k}{(q^n; q^2)^n_k(-q^n; q^2)_k(q^{4n}; q^4)_k} q^{2nk}.
\]

**Proof.** It suffices to prove that both sides of (3.2) are identical for $a = q^{-(2j+1)n}$ and $a = q^{(2j+1)n}$ with $j = 0, 1, \ldots, (m-1)/2$, i.e.,

\[
\sum_{k=0}^{(mn-1)/2} \frac{(q^{1-(2j+1)n}; q^2)_k(q^{1+(2j+1)n}; q^2)_k(-1; q^4)_k}{(q^2)_k(-q^n; q^2)_k(q^4; q^4)_k} q^{2k} 
\equiv \left( \frac{2}{n} \right) \sum_{k=0}^{(m-1)/2} \frac{(q^{-2jn}; q^2)_k(q^{(2j+2)n}; q^2)_k(-1; q^{4n})_k}{(q^n; q^2)^n_k(-q^n; q^2)_k(q^{4n}; q^4)_k} q^{2nk}.
\]

Clearly, $(mn-1)/2 \geq ((2j+1)n-1)/2$ for $0 \leq j \leq (m-1)/2$, and $(q^{1-(2j+1)n}; q^2)_k = 0$ for $k > ((2j+1)n-1)/2$. By the identity in (2.1), the left-hand side of (3.3) is equal to $\left( \frac{2}{(2j+1)n} \right)$. Likewise, the right-hand side of (3.3) is equal to

\[
\left( \frac{2}{n} \right) \left( \frac{2}{2j+1} \right) = \left( \frac{2}{(2j+1)n} \right).
\]
where \((\frac{m}{2})\) is understood to be 1. This establishes the identity (3.3), and so the \(q\)-congruence (3.2) holds.

We can now prove Theorem 1.2.

**Proof of Theorem 1.2.** It is easy to see that

\[
q^N - 1 = \prod_{d|N} \Phi_d(q),
\]

and there are \(\lfloor m/n^j \rfloor - \lfloor (m - 1)/(2n^j - 1) \rfloor\) multiples of \(n^j - 1\) in the arithmetic progression 1, 3, ..., \(m\) for any positive integer \(j\). Thus, the limit of (3.1) as \(a \to 1\) has the factor

\[
\prod_{j=1}^{\infty} \Phi_{n^j}(q)^{2\lfloor m/n^j \rfloor - 2\lfloor (m - 1)/(2n^j - 1) \rfloor}.
\]

On the other hand, the denominator of the left-hand side of (3.2) is divisible by that of the right-hand side of (3.2). The former is equal to \((q^2; q^2)_{mn - 1}\) and its factor related to \(\Phi_n(q), \Phi_{n^2}(q), \ldots\) is just

\[
\prod_{j=1}^{\infty} \Phi_{n^j}(q)^{\lfloor mn - 1 \rfloor / n^j}.
\]

Moreover, writing \([m]_q = (q; q)_m/((1 - q)(q; q)_{m-1})\) as a product of cyclotomic polynomials (see, for example, [1]), and then using the fact \(\Phi_{n^j}(q^n) = \Phi_{n^{j+1}}(q)\), we know that the polynomial \([m]_q^{2\lfloor m/n^j \rfloor - \lfloor (m - 1)/(2n^j - 1) \rfloor - 2\lfloor (m - 1)/(2n^j - 1) \rfloor}\) only has the following factor:

\[
\prod_{j=2}^{\infty} \Phi_{n^j}(q)^{2\lfloor m/n^j \rfloor - \lfloor (m - 1)/(2n^j - 1) \rfloor - 2\lfloor (m - 1)/(2n^j - 1) \rfloor}
\]

related to \(\Phi_n(q), \Phi_{n^2}(q), \ldots\).

It is clear that

\[
2\lfloor m/n^j \rfloor - 2\lfloor (m - 1)/(2n^j - 1) \rfloor - \lfloor mn - 1 \rfloor / n^j = 2, \quad \text{for } j = 1
\]

and

\[
\lfloor mn - 1 \rfloor / n^j = \lfloor (m - 1)/(2n^j - 1) \rfloor, \quad \text{for } j \geq 2.
\]

Therefore, letting \(a \to 1\) in (3.2), we see that the \(q\)-congruence (1.6) holds, and the denominator on the left-hand side of (1.6) is relatively prime to \(\Phi_{n^j}(q)\) for \(j \geq 2\), as desired.
4. Concluding remarks

Sun [16, Conjecture 4(ii)] also made the following conjecture: for any odd prime $p$ and odd integer $m$,

$$\frac{1}{m^2 \binom{m-1}{(m-1)/2}} \left( \sum_{k=0}^{(mp-1)/2} \binom{2k}{k} \frac{16^k}{16^k} - \left( \frac{3}{p} \right) \sum_{k=0}^{(m-1)/2} \binom{2k}{k} \frac{16^k}{16^k} \right) \equiv 0 \pmod{p^2}, \quad (4.1)$$

of which the $m = 1$ case was already proved by Sun [15] himself. Gu and Guo [4] gave the following $q$-analogue of (4.1) for $m = 1$: for odd $n > 1$,

$$\sum_{k=0}^{(n-1)/2} \frac{(q^4; q^4)_k q^{2k}}{(q^4; q^4)_k (-q; q^2)_k} \equiv \left( \frac{3}{n} \right) q^{(n^2-1)/12} \pmod{\Phi_n(q)^2}. \quad (4.2)$$

However, we cannot utilize (4.2) to give a $q$-analogue of (4.1), similar to Theorem 1.2, because $(n^2 - 1)/12$ is not a linear function of $n$. Anyway, we believe that such a $q$-analogue of (4.1) should exist, which is left to the interested reader.

Acknowledgements

The author was partially supported by the National Natural Science Foundation of China (Grant No. 11771175).

References


**Communicating Editor: B Sury**