q-ANALOGUE OF WILSON'S THEOREM

ROBIN CHAPMAN AND HAO PAN

Abstract. We give q-analogues of Wilson's theorem for the primes congruent 1 and 3 modulo 4 respectively. And q-analogues of two congruences due to Mordell and Chowla are also established.

1. Introduction

For arbitrary positive integer n, let

$$[n]_q = \frac{1-q^n}{1-q} = 1 + q + \cdots + q^{n-1}.$$

Clearly $\lim_{q\to 1}[n]_q = 1$, so we say that $[n]_q$ is a q-analogue of the integer n. Supposing that $a \equiv b \pmod{n}$, we have

$$[a]_q = \frac{1-q^a}{1-q} = \frac{1-q^b+q^b(1-q^{a-b})}{1-q} \equiv \frac{1-q^b}{1-q} = [b]_q \pmod{[n]_q}.$$

Here the above congruence is considered over the polynomial ring in the variable q with integral coefficients. And q-analogues of some arithmetical congruences have been studied in [9, 1, 7, 8].

Let p be a prime. The well-known Wilson theorem states that

$$(p-1)! \equiv 1 \pmod{p}.$$

Unfortunately, in general,

$$\prod_{j=1}^{p-1}[j]_q \not\equiv -q^n \pmod{[p]_q}$$

for any integer n. However, we have the following q-analogue of Wilson's theorem for a prime $p \equiv 3 \pmod 4$.

Theorem 1.1. *Suppose that $p > 3$ is a prime and $p \equiv 3 \pmod 4$. Then we have*

$$\prod_{j=1}^{p-1}[j]_{q^j} \equiv -1 \pmod{[p]_q}. \tag{1.1}$$

2000 *Mathematics Subject Classification.* Primary 11A07; Secondary 05A30, 11R29.

In [6] (or see [10, Theorem 8]), Mordell proved that if $p > 3$ is a prime and $p \equiv 3 \pmod 4$ then

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{h(-p)+1}{2}} \pmod p, \tag{1.2}$$

where $h(-p)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-p})$. Now we can give a q-analogue of (1.2).

Theorem 1.2. *Let $p > 3$ be a prime with $p \equiv 3 \pmod 4$. Then we have*

$$\prod_{j=1}^{(p-1)/2} [j]_{q^{16j}} \equiv (-1)^{\frac{h(-p)+1}{2}} q \pmod{[p]_q}. \tag{1.3}$$

The case $p \equiv 1 \pmod 4$ is a little complicated. Let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol modulo p. It is well-known that for any a prime to p, $\left(\frac{a}{p}\right) = 1$ or -1 according to whether a is a quadratic residue modulo p. Let ε_p and $h(p)$ be the fundamental unit and the class number of $\mathbb{Q}(\sqrt{p})$ respectively.

Theorem 1.3. *Suppose that p is a prime and $p \equiv 1 \pmod 4$. Then we have*

$$\prod_{j=1}^{p-1} [j]_{q^j} \equiv A + B \sum_{j=1,\left(\frac{j}{p}\right)=-1}^{p-1} q^j \pmod{[p]_q}, \tag{1.4}$$

where

$$A = \frac{\varepsilon_p^{2h(p)} + \varepsilon_p^{-2h(p)}}{2} + \frac{\varepsilon_p^{2h(p)} - \varepsilon_p^{-2h(p)}}{2\sqrt{p}} \quad \textit{and} \quad B = \frac{\varepsilon_p^{2h(p)} - \varepsilon_p^{-2h(p)}}{\sqrt{p}}.$$

Write $\varepsilon_p = (u_p + v_p\sqrt{p})/2$ where u_p, v_p are positive integers with the same parity. Clearly $u_p^2 - pv_p^2 = \pm 4$ since ε_p is an unit. Letting $q \to 1$ in (1.4), we obtain that

$$-1 \equiv (p-1)! \equiv A + \frac{B(p-1)}{2} \equiv \frac{\varepsilon_p^{2h(p)} + \varepsilon_p^{-2h(p)}}{2} \equiv \frac{u_p^{2h(p)}}{2^{2h(p)}} \pmod p.$$

It follows that $h(p)$ is odd and the norm of ε_p is always -1, i.e., $u_p^2 - pv_p^2 = -4$.

In [4] (or see [10, Theorem 9]), Chowla extended Mordell's result (1.2) for $p \equiv 1 \pmod 4$. Let $h(p)$ and $\varepsilon_p = (u_p + v_p\sqrt{p})/2$ be defined as above. Then Chowla proved that

$$\left(\frac{p-1}{2}\right)! \equiv \frac{(-1)^{\frac{h(p)+1}{2}} u_p}{2} \pmod p. \tag{1.5}$$

Now we have the following q-analogue of Chowla's congruence:

Theorem 1.4. *Suppose that p is a prime and $p \equiv 1 \pmod 4$. Then*

$$\prod_{j=1}^{(p-1)/2} [j]_{q^j} \equiv -Cq - D \sum_{j=1,\left(\frac{j}{p}\right)=-1}^{p-1} q^{j+1} \pmod{[p]_q}, \tag{1.6}$$

where

$$C=\frac{\varepsilon_p^{h(p)}-\varepsilon_p^{-h(p)}}{2}+\frac{\varepsilon_p^{h(p)}+\varepsilon_p^{-h(p)}}{2\sqrt{p}}\quad\text{and}\quad D=\frac{\varepsilon_p^{h(p)}+\varepsilon_p^{-h(p)}}{\sqrt{p}}.$$

Let us explain why (1.6) implies (1.5). Letting $q\to 1$ in (1.6), it is derived that

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv -\left(\frac{\varepsilon_p^{h(p)}-\varepsilon_p^{-h(p)}}{2}+\frac{\varepsilon_p^{h(p)}+\varepsilon_p^{-h(p)}}{2\sqrt{p}}+\frac{p-1}{2}\cdot\frac{\varepsilon_p^{h(p)}+\varepsilon_p^{-h(p)}}{\sqrt{p}}\right)\\ &\equiv -\frac{((u_p+v_p\sqrt{p})/2)^{h(p)}-((-u_p+v_p\sqrt{p})/2)^{h(p)}}{2}\\ &\equiv -\frac{u_p^{h(p)}}{2^{h(p)}}=-(u_p^2/4)^{\frac{h(p-1)}{2}}\frac{u_p}{2}\equiv-\frac{(-1)^{\frac{h(p)-1}{2}}u_p}{2}\pmod p.\end{aligned}$$

The proofs of Theorems 1.1-1.4 will be given in the next sections.

2. Proofs of Theorems 1.1 and 1.2

In this section we assume that $p>3$ is a prime and $p\equiv 3\pmod 4$. Write

$$\prod_{j=1}^{p-1}[j]_{q^j}=\prod_{j=1}^{p-1}\frac{1-q^{j^2}}{1-q^j}\ \text{and}\ \prod_{j=1}^{(p-1)/2}[j]_{q^j}=\prod_{j=1}^{(p-1)/2}\frac{1-q^{j^2}}{1-q^j}.$$

Observe that

$$[p]_q=\frac{1-q^p}{1-q}=\prod_{j=1}^{p-1}(q-\zeta^j)$$

where $\zeta=e^{2\pi i/p}$. Also we know that $\sigma_s:\zeta\longmapsto\zeta^s$ is an automorphism over $\mathbb{Q}(\zeta)$ provided that $p\nmid s$. Hence it suffices to show that

$$\prod_{j=1}^{p-1}\frac{1-\zeta^{j^2}}{1-\zeta^j}=-1\qquad\text{and}\qquad\prod_{j=1}^{(p-1)/2}\frac{1-\zeta^{j^2}}{1-\zeta^j}=(-1)^{\frac{h(-p)+1}{2}}\zeta.$$

Let Q and N denote respectively the sets of quadratic residues and quadratic non-residues of p in the interval $[1,p-1]$. Then

$$\prod_{j=1}^{p-1}\frac{1-\zeta^{j^2}}{1-\zeta^j}=\frac{\prod_{j=1}^{\frac{p-1}{2}}(1-\zeta^{j^2})^2}{\prod_{j=1}^{p-1}(1-\zeta^j)}=\frac{U^2}{UV}=\frac{U}{V},$$

where

$$U=\prod_{k\in Q}(1-\zeta^k),\qquad\text{and}\qquad V=\prod_{k\in N}(1-\zeta^k).$$

But since -1 is a quadratic non-residue modulo p,

$$V=\prod_{k\in Q}(1-\zeta^{p-k})=\prod_{k\in Q}(1-\zeta^{-k})=U\prod_{k\in Q}(-\zeta^k).$$

Now

$$\sum_{k\in Q} k \equiv \sum_{j=1}^{(p-1)/2} j^2 = \frac{p(p^2-1)}{24} \equiv 0 \pmod p$$

as p is prime to 6 and so $p^2 \equiv 1 \pmod{24}$. We conclude that

$$U/V = (-1)^{\frac{p-1}{2}} \zeta^{-\sum_{k\in Q} k} = -1$$

as desired.

Now let us begin to prove

$$\prod_{j=1}^{(p-1)/2} \frac{1-\zeta^{16j^2}}{1-\zeta^{16j}} = \frac{\prod_{j=1}^{(p-1)/2}(1-\zeta^{16j^2})}{\prod_{j=1}^{(p-1)/2}(1-\zeta^{16j})} = (-1)^{\frac{h(-p)+1}{2}} \zeta. \tag{2.1}$$

Clearly the numerator of the left side of (2.1) is U. Let

$$W = \prod_{j=1}^{(p-1)/2} (1-\zeta^{16j})$$

denote its denominator. Let $M = \{1, 2, \ldots, (p-1)/2\}$. Then $W = W_+ W_-$ where

$$W_+ = \prod_{j\in M\cap Q} (1-\zeta^{16j}), \qquad \text{and} \qquad W_- = \prod_{j\in M\cap N} (1-\zeta^{16j}).$$

Now

$$W_- = \sum_{M'\cap Q} (1-\zeta^{-16k}) = \frac{U}{W_+} \prod_{k\in M'\cap Q} (-\zeta^{-16k})$$

where $M' = \{(p+1)/2, \ldots, p-1\}$. We know (see [10, Section 1.3]) that

$$\begin{aligned} h(-p) =& \frac{1}{2-\left(\frac{2}{p}\right)} \sum_{k=1}^{(p-1)/2} \left(\frac{k}{p}\right) = \frac{1}{2-\left(\frac{2}{p}\right)} \left(\frac{p-1}{2} - 2\sum_{k\in M\cap N} 1\right) \\ \equiv& -1 - 2|M\cap N| = -1 - 2|M'\cap Q| \pmod 4. \end{aligned}$$

Also, we have

$$\begin{aligned} \frac{p^2-1}{8} =& \sum_{k=1}^{(p-1)/2} k = \sum_{k\in M\cap Q} k + \sum_{k\in M\cap N} k = \sum_{k\in M\cap Q} k + \sum_{k\in M'\cap Q} (p-k) \\ \equiv& \sum_{k\in Q} k - 2\sum_{k\in M'\cap Q} k \equiv -2\sum_{k\in M'\cap Q} k \pmod p, \end{aligned}$$

whence $\sum_{k\in M'\cap Q} 16k \equiv 1 \pmod p$. Thus

$$\frac{U}{W} = \frac{U}{W_+W_-} = (-1)^{|M'\cap Q|} \prod_{k\in M'\cap Q} \zeta^{16k} = (-1)^{(1+h(-p))/2}\zeta,$$

which confirms (2.1). □

3. When $p \equiv 1 \pmod 4$

Below suppose that p is a prime congruent 1 modulo 4 and $\zeta = e^{2\pi i/p}$. Let $Q,\ N \subseteq [1, p-1]$ be the sets of quadratic residues and quadratic non-residues of p respectively. Let

$$U = \prod_{k\in Q}(1-\zeta^k) \quad \text{and} \quad V = \prod_{k\in N}(1-\zeta^k).$$

In order to prove Theorem 1.3, we only need to show prove that

$$A + B\sum_{j\in N}\zeta^j = \prod_{j=1}^{p-1}\frac{1-\zeta^{j^2}}{1-\zeta^j} = \frac{\prod_{j\in Q}(1-\zeta^j)^2}{\prod_{j\in Q}(1-\zeta^j)\prod_{j\in N}(1-\zeta^j)} = \frac{U}{V}. \tag{3.1}$$

By the analytic class number formula [2, Chapter 1, Section 4, Theorem 2]

$$U = \varepsilon_p^{-h(p)}\sqrt{p} \qquad \text{and} \qquad V = \varepsilon_p^{h(p)}\sqrt{p}.$$

Thus $U/V = \varepsilon_p^{-2h(p)} = a - b\sqrt{p}$ where

$$2a = \varepsilon_p^{2h(p)} + \varepsilon_p^{-2h(p)} \in \mathbb{Z} \quad \text{and} \quad 2b = (\varepsilon_p^{2h(p)} - \varepsilon_p^{-2h(p)})/\sqrt{p} \in \mathbb{Z}.$$

Also, by Gauss's formula for the quadratic Gauss sum

$$\sqrt{p} = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\zeta^j = \sum_{j=1}^{p-1}\zeta^j - 2\sum_{j\in N}\zeta^j = -1 - 2\sum_{j\in N}\zeta^j.$$

Hence

$$\frac{U}{V} = a + b\left(1 + 2\sum_{j\in N}\zeta^j\right),$$

which is clearly equivalent to (3.1).

Remark. The first author used products like $\prod_{j\in N}(1-\zeta^j)$ extensively in [3].

Let us now consider the product

$$\prod_{j=1}^{(p-1)/2}\frac{1-\zeta^{16j^2}}{1-\zeta^{16j}} = \frac{U}{\Pi_{16}}$$

where

$$\Pi_r = \prod_{j=1}^{(p-1)/2}(1-\zeta^{rj}).$$

When r and s are prime to p, we have $\Pi_{rs} = \sigma_s(\Pi_r)$ where σ_s is the automorphism over $\mathbb{Q}(\zeta)$ mapping ζ to ζ^s. It turns out to be convenient to compute Π_{16} as $\sigma_4(\Pi_4)$.

As $p \equiv 1 \pmod 4$ we know that $U = \varepsilon_p^{-h(p)}\sqrt{p}$. For each r prime to p,

$$|\Pi_r|^2 = \Pi_r \Pi_{-r} = \prod_{j=1}^{p-1}(1-\zeta^j) = p,$$

so $|\Pi_r| = \sqrt{p}$. Now

$$\begin{aligned}\frac{\Pi_4}{|\Pi_4|} = \prod_{j=1}^{(p-1)/2}\frac{1-\zeta^{4j}}{|1-\zeta^{4j}|} = \prod_{j=1}^{(p-1)/2}(-\zeta^{2j})\frac{2i\sin(4\pi j/p)}{|2i\sin(4\pi j/p)|} \\ =(-1)^M\prod_{j=1}^{(p-1)/2}(-i\zeta^{2j}) = (-1)^M(-i)^{(p-1)/2}\zeta^{(p^2-1)/4} \\ =(-1)^{(p-1)/4+M}\zeta^{(p^2-1)/4}\end{aligned}$$

where

$$M = |\{1 \leqslant j \leqslant (p-1)/2 : \sin(4\pi j/p) < 0\}|.$$

Note that when $0 < j < p/2$, $\sin(4\pi j/p) < 0$ if and only if $p/4 < j < p/2$. So $M = (p-1)/4$, and

$$\Pi_4 = \zeta^{(p^2-1)/4}\sqrt{p}.$$

Also,

$$\sigma_4(\sqrt{p}) = \sigma_4\left(\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\zeta^j\right) = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\zeta^{4j} = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\zeta^j = \sqrt{p}$$

Thus

$$\Pi_{16} = \sigma_4(\zeta^{(p^2-1)/4}\sqrt{p}) = \zeta^{p^2-1}\sqrt{p} = \zeta^{-1}\sqrt{p}.$$

Assume that $\varepsilon_p^{h(p)} = (c + d\sqrt{p})/2$ where c, d are integers with the same parity. Recall that the norm of ε_p is -1 and $h(p)$ is odd. Hence $\varepsilon_p^{-h(p)} = (-c + d\sqrt{p})/2$. So

$$c = \varepsilon_p^{h(p)} - \varepsilon_p^{-h(p)} \qquad \text{and} \qquad d\sqrt{p} = \varepsilon_p^{h(p)} + \varepsilon_p^{-h(p)}.$$

As $\sqrt{p} = -1 - 2\sum_{j\in N}\zeta^j$, we have

$$\varepsilon_p^{-h(p)} = \frac{-c + d\sqrt{p}}{2} = -\frac{c+d}{2} - d\sum_{j\in N}\zeta^j.$$

Therefore

$$\prod_{j=1}^{(p-1)/2}\frac{1-\zeta^{16j^2}}{1-\zeta^{16j}} = \frac{U}{\Pi_{16}} = \frac{\varepsilon_p^{-h(p)}\sqrt{p}}{\zeta^{-1}\sqrt{p}} = -\frac{(c+d)\zeta}{2} - d\sum_{j\in N}\zeta^{j+1}.$$

This concludes that

$$\prod_{j=1}^{(p-1)/2}[j]_{q^{16j}} \equiv -\frac{c+d}{2}q - d\sum_{j\in N} q^{j+1} \pmod{[p]_q}.$$

We are done. □

Acknowledgment. The second author thanks Professor Zhi-Wei Sun for his helpful suggestions on this paper.

References

[1] G. E. Andrews, *q-Analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher*, Discrete Math., **204**(1999), 15-25.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Presss, New York and London, 1966.

[3] R. Chapman, *Determinants of Legendre symbol matrices*, Acta Arithmetica, **115**(2004), 231-244.

[4] S. Chowla, *On the class number of real quadratic field*, Proc. Natl. Acad. Sci. USA, **47**(1961), 878.

[5] K. Ireland and M. Rosen, *A classical introduction to modern number theory, 2nd ed.*, Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.

[6] L. J. Mordell, *The congruence* $((p-1)/2)! \equiv \pm 1 \pmod p$, Amer. Math. Monthly, **68**(1961), 145-146.

[7] H. Pan, *Arithmetic properties of q-Fibonacci numbers and q-Pell numbers*, Discrete Math., to appear, arXiv:math.CO/0508546.

[8] H. Pan and Z.-W. Sun, *On q-Euler numbers, q-Salie numbers and q-Carlitz numbers*, Acta Arith., to appear, arXiv:math.CO/0505548.

[9] B. E. Sagan, *Congruence properties of q-analogs*, Adv. Math., **95**(1992), 127-143.

[10] J. Urbanowicz and K. S. Williams, *Congruences for L-functions,* Mathematics and its Applications 511, Kluwer Academic Publishers, Dordrecht, 2000.

Department of Mathematics, University of Exeter, Exeter, EX4 4QE, UK, 01392 263971

E-mail address: `rjc@maths.ex.ac.uk`

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: `haopan79@yahoo.com.cn`