ACTA ARITHMETICA
128.4 (2007)

A q-analogue of Lehmer's congruence

by

Hao Pan (Shanghai)

1. Introduction. In 1938, Lehmer [Leh] established an interesting congruence:

$$\sum_{j=1}^{(p-1)/2} \frac{1}{j} \equiv -2\mathrm{Q}_p(2) + \mathrm{Q}_p(2)^2 p \pmod{p^2}, \tag{1.1}$$

where $p \geq 3$ is a prime and $\mathrm{Q}_p(2) = (2^{p-1}-1)/p$. Lehmer's congruence can be considered as an extension of Wolstenholme's [W] harmonic series congruence

$$\sum_{j=1}^{p-1} \frac{1}{j} \equiv 0 \pmod{p^2} \tag{1.2}$$

for any prime $p > 3$. On the other hand, the q-analogues of some arithmetic congruences have been investigated by several authors (e.g., see [A], [F], [C], [GZ] and [PS]). Recently, Shi and Pan [SP] proved the following q-analogue of (1.2):

$$\sum_{j=1}^{p-1} \frac{1}{[j]_q} \equiv \frac{p-1}{2}(1-q) + \frac{p^2-1}{24}(1-q)^2[p]_q \pmod{[p]_q^2}, \tag{1.3}$$

where $[n]_q = (1-q^n)/(1-q) = 1 + q + \cdots + q^{n-1}$. Here congruence (1.3) is considered over the ring of the polynomials in q with integral coefficients. Obviously (1.2) is deduced from (1.3) when $q \to 1$.

The main purpose of the present paper is to establish a q-analogue of Lehmer's congruence. Set

$$(a;q)_n = \begin{cases} (1-a)(1-aq)\cdots(1-aq^{n-1}) & \text{if } n \geq 1, \\ 1 & \text{if } n = 0. \end{cases}$$

2000 *Mathematics Subject Classification*: Primary 11B65; Secondary 05A10, 05A30, 11A07.

It is easy to see that for any $m \geq 0$ with $p \nmid m$ we have a q-analogue of Fermat's little theorem:

$$\frac{(q^m;q^m)_{p-1}}{(q;q)_{p-1}} \equiv 1 \pmod{[p]_q}. \tag{1.4}$$

Indeed, since

$$[m]_q = \frac{1-q^m}{1-q} \equiv \frac{1-q^n}{1-q} = [n]_q \pmod{[p]_q}$$

whenever $m \equiv n \pmod{p}$,

$$\frac{(q^m;q^m)_{p-1}}{(q;q)_{p-1}} = \prod_{j=1}^{p-1} \frac{1-q^{jm}}{1-q^j} = \prod_{j=1}^{p-1} \frac{[jm]_q}{[j]_q} \equiv 1 \pmod{[p]_q}.$$

So we can define the q-Fermat quotient by

$$\mathrm{Q}_p(m,q) = \frac{(q^m;q^m)_{p-1}/(q;q)_{p-1} - 1}{[p]_q}.$$

THEOREM 1.1. *Let p be an odd prime. We have*

$$\begin{aligned} 2\sum_{j=1}^{(p-1)/2} \frac{1}{[2j]_q} + 2\mathrm{Q}_p(2,q) - \mathrm{Q}_p(2,q)^2[p]_q \\ \equiv \left(\mathrm{Q}_p(2,q)(1-q) + \frac{p^2-1}{8}(1-q)^2\right)[p]_q \pmod{[p]_q^2}. \end{aligned} \tag{1.5}$$

In 1895, with the help of De Moivre's theorem, Morley [M] proved that

$$(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2} \equiv 4^{p-1} \pmod{p^3} \tag{1.6}$$

for any prime $p \geq 5$. In [G1], Granville generalized the congruence of Morley and showed that

$$(-1)^{(p-1)(m-1)/2} \prod_{k=1}^{m-1} \binom{p-1}{\lfloor kp/m \rfloor} \equiv m^p - m + 1 \pmod{p^2} \tag{1.7}$$

for any $m \geq 2$ and prime $p \geq 3$, where $\lfloor x \rfloor$ denotes the greatest integer not exceeding x. Now we can give the q-analogues of (1.6) and (1.7). For any $m, n \in \mathbb{N}$, define the q-binomial coefficients by

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{(q;q)_n}{(q;q)_m(q;q)_{n-m}}$$

if $n \geq m$, and if $n < m$, then let $\begin{bmatrix} n \\ m \end{bmatrix}_q = 0$. It is easy to see that $\begin{bmatrix} n \\ m \end{bmatrix}_q$ is a polynomial in q with integral coefficients, since the q-binomial coefficients

satisfy the recurrence relation

$$\begin{bmatrix} n+1 \\ m \end{bmatrix}_q = q^m \begin{bmatrix} n \\ m \end{bmatrix}_q + \begin{bmatrix} n \\ m-1 \end{bmatrix}_q.$$

THEOREM 1.2.

$$(-1)^{(p-1)/2} q^{(p^2-1)/4} \begin{bmatrix} p-1 \\ (p-1)/2 \end{bmatrix}_{q^2} \equiv (-q;q)_{p-1}^2 - \frac{p^2-1}{24}(1-q)^2[p]_q^2 \pmod{[p]_q^3} \tag{1.8}$$

for any prime $p \geq 5$.

THEOREM 1.3. *Let* $p \geq 3$ *be a prime and* $m \geq 2$ *be an integer with* $p \nmid m$. *Then*

$$(-1)^{(p-1)(m-1)/2} q^M \prod_{k=1}^{m-1} \begin{bmatrix} p-1 \\ \lfloor kp/m \rfloor \end{bmatrix}_{q^m} \equiv \frac{m(q^m;q^m)_{p-1}}{(q;q)_{p-1}} - m + 1 \pmod{[p]_q^2}, \tag{1.9}$$

where

$$M = m \sum_{k=1}^{m-1} \binom{\lfloor kp/m \rfloor + 1}{2}.$$

The proofs of Theorems 1.1–1.3 will be given in the next sections.

REMARK. Motivated by the brilliant discovery of Agrawal, Kayal and Saxena [AKS] on primality testing, the referee posed the interesting problem whether any of these q-congruences could identify primes. Recently the author and Chapman established some q-analogues of Wilson's theorem [CP]. Hence at least for $p \equiv 3 \pmod 4$, we have $\prod_{j=1}^{p-1}[j]_{q^j} \equiv -1 \pmod{[p]_q}$ if and only if p is a prime.

2. Some lemmas. In this section we assume that p is a prime greater than 3. The following lemmas will be used in the proofs of Theorems 1.1 and 1.2.

LEMMA 2.1.

$$\sum_{j=1}^{p-1} \frac{1}{[j]_q} \equiv \frac{p-1}{2}(1-q) \pmod{[p]_q}, \tag{2.1}$$

$$\sum_{j=1}^{p-1} \frac{q^j}{[j]_q^2} \equiv -\frac{p^2-1}{12}(1-q)^2 \pmod{[p]_q}, \tag{2.2}$$

$$\sum_{j=1}^{p-1}\frac{1}{[j]_q^2}\equiv -\frac{(p-1)(p-5)}{12}(1-q)^2 \pmod{[p]_q}. \tag{2.3}$$

Proof. See Theorem 4 in [A] and Lemma 2 in [SP]. ∎

Lemma 2.2.

$$q^{kp}=\sum_{j=0}^{k}(-1)^j\binom{k}{j}(1-q)^j[p]_q^j.$$

Proof.

$$\sum_{j=0}^{k}(-1)^j\binom{k}{j}(1-q)^j[p]_q^j=(1-(1-q)[p]_q)^k=(1-(1-q^p))^k=q^{kp}.$$ ∎

From Lemma 2.2, we deduce that

$$q^{kp}\equiv 1-k(1-q)[p]_q+\frac{k(k-1)}{2}(1-q)^2[p]_q^2 \pmod{[p]_q^3}. \tag{2.4}$$

Lemma 2.3.

$$4\sum_{1\le j<k\le p-1}\frac{(-1)^k}{[j]_q[k]_q}\equiv\left(\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\right)^2+(p-3)(1-q)\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q}+\frac{(p-1)(p+7)}{12}(1-q)^2 \pmod{[p]_q}. \tag{2.5}$$

Proof. Since p is odd,

$$\begin{aligned}\left(\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\right)^2&=\left(\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\right)\left(\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}-(1-q)\sum_{j=1}^{p-1}(-1)^j\right)\\&=\left(\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\right)\left(\sum_{j=1}^{p-1}\frac{(-q)^j}{[j]_q}\right)\\&=\sum_{k=2}^{2p-2}(-1)^k\sum_{j=\max\{1,k-p+1\}}^{\min\{k-1,p-1\}}\frac{q^j}{[j]_q[k-j]_q}.\end{aligned}$$

Then we have

$$\begin{aligned}&\left(\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\right)\left(\sum_{j=1}^{p-1}\frac{(-q)^j}{[j]_q}\right)-(-1)^p\sum_{j=1}^{p-1}\frac{q^j}{[j]_q[p-j]_q}\\&\quad=\sum_{k=2}^{p-1}(-1)^k\sum_{j=1}^{k-1}\frac{q^j}{[j]_q[k-j]_q}+\sum_{k=p+1}^{2p-2}(-1)^k\sum_{j=k-p+1}^{p-1}\frac{q^j}{[j]_q[k-j]_q}\end{aligned}$$

$$= \sum_{k=2}^{p-1}(-1)^k \sum_{j=1}^{k-1} \frac{q^j}{[j]_q[k-j]_q} + \sum_{l=2}^{p-1}(-1)^{2p-l} \sum_{j=p-l+1}^{p-1} \frac{q^j}{[j]_q[2p-l-j]_q}$$

(here $l = 2p-k$)

$$= \sum_{k=2}^{p-1}(-1)^k \sum_{j=1}^{k-1} \frac{q^j}{[j]_q[k-j]_q} + \sum_{l=2}^{p-1}(-1)^l \sum_{i=1}^{l-1} \frac{q^{p+i-l}}{[p+i-l]_q[p-i]_q}$$

(here $i = l+j-p$).

Note that

$$\frac{q^{p+i-l}}{[p+i-l]_q[p-i]_q} = \frac{q^{p+i-l}(1-q)^2}{(1-q^{p+i-l})(1-q^{p-i})}$$
$$\equiv \frac{q^i(1-q)^2}{(1-q^{l-i})(1-q^i)} \pmod{[p]_q}.$$

It follows that

$$\Big(\sum_{j=1}^{p-1} \frac{(-1)^j}{[j]_q}\Big)\Big(\sum_{j=1}^{p-1} \frac{(-q)^j}{[j]_q}\Big) + \sum_{j=1}^{p-1} \frac{q^j}{[j]_q[p-j]_q}$$
$$\equiv \sum_{k=2}^{p-1}(-1)^k \sum_{j=1}^{k-1} \frac{q^j}{[j]_q[k-j]_q} + \sum_{l=2}^{p-1}(-1)^l \sum_{i=1}^{l-1} \frac{q^i}{[i]_q[l-i]_q}$$
$$= 2\sum_{k=2}^{p-1}(-1)^k \sum_{j=1}^{k-1} \frac{q^j(1-q)^2}{(1-q^j)(1-q^{k-j})}$$
$$= 2\sum_{k=2}^{p-1} \frac{(-1)^k q^k(1-q)^2}{1-q^k} \sum_{j=1}^{k-1} \Big(\frac{1}{q^{k-j}-q^k} + \frac{1}{1-q^{k-j}}\Big)$$
$$= 2 \sum_{1\le j<k\le p-1} \frac{(-1)^k(q^k+q^j)}{[j]_q[k]_q} \pmod{[p]_q}.$$

We can write

$$\sum_{1\le j<k\le p-1} \frac{(-1)^k(q^k+q^j)}{[j]_q[k]_q}$$
$$= \sum_{1\le j<k\le p-1} \frac{(-1)^k(2-(1-q^k)-(1-q^j))}{[j]_q[k]_q}$$
$$= 2 \sum_{1\le j<k\le p-1} \frac{(-1)^k}{[j]_q[k]_q} - (1-q)\Big(\sum_{k=2}^{p-1} \frac{(-1)^k(k-1)}{[k]_q} + \sum_{j=1}^{p-2} \frac{1}{[j]_q} \sum_{k=j+1}^{p-1} (-1)^k\Big).$$

Now

$$\sum_{k=2}^{p-1}\frac{(-1)^k(k-1)}{[k]_q}=\frac{1}{2}\sum_{k=1}^{p-1}\left(\frac{(-1)^k(k-1)}{[k]_q}+\frac{(-1)^{p-k}(p-k-1)}{[p-k]_q}\right)$$
$$=\frac{1}{2}\sum_{k=1}^{p-1}(-1)^k(k-1)\left(\frac{1}{[k]_q}+\frac{1}{[p-k]_q}\right)+\frac{p-2}{2}\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q}$$
$$=\frac{1}{2}\sum_{k=1}^{p-1}(-1)^k(k-1)\left(\frac{[p]_q}{[k][p-k]_q}+(1-q)\right)+\frac{p-2}{2}\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q}$$
$$\equiv\frac{p-1}{4}(1-q)+\frac{p-2}{2}\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q}\pmod{[p]_q}.$$

And from (2.1) we have

$$\sum_{j=1}^{p-2}\frac{1}{[j]_q}\sum_{k=j+1}^{p-1}(-1)^k=\frac{1}{2}\sum_{j=1}^{p-1}\frac{1-(-1)^j}{[j]_q}$$
$$\equiv\frac{p-1}{4}(1-q)-\frac{1}{2}\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\pmod{[p]_q}.$$

Finally, by (2.3),

$$\sum_{j=1}^{p-1}\frac{q^j}{[j]_q[p-j]_q}=\sum_{j=1}^{p-1}\frac{q^{p-j}}{[j]_q[p-j]_q}=\sum_{j=1}^{p-1}\frac{q^p}{[j]_q([p]_q-[j]_q)}$$
$$\equiv\frac{(p-1)(p-5)}{12}(1-q)^2\pmod{[p]_q}.$$

Thus combining the equations and congruences above, we obtain

$$4\sum_{1\le j<k\le p-1}(-1)^k\frac{1}{[j]_q[k]_q}-\left(\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\right)\left(\sum_{j=1}^{p-1}\frac{(-q)^j}{[j]_q}\right)$$
$$\equiv(p-3)(1-q)\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q}+\frac{(p-1)(p+7)}{12}(1-q)^2\pmod{[p]_q}.\ \blacksquare$$

Lemma 2.4.

$$\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\equiv 2\sum_{j=1}^{(p-1)/2}\frac{1}{[2j]_q}-\frac{p-1}{2}(1-q)$$
$$-\frac{p^2-1}{24}(1-q)^2[p]_q\pmod{[p]_q^2}. \tag{2.6}$$

Proof. Clearly

$$\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}=\sum_{j=1}^{(p-1)/2}\frac{1}{[2j]_q}-\sum_{j=1}^{(p-1)/2}\frac{1}{[2j-1]_q}$$
$$=\sum_{j=1}^{(p-1)/2}\frac{1}{[2j]_q}-\sum_{j=1}^{(p-1)/2}\frac{1}{[p-2j]_q}.$$

Observe that

$$\frac{1}{[p-2j]_q}=\frac{q^{2j}}{[p]_q-[2j]_q}=\frac{q^{2j}([p]_q+[2j]_q)}{[p]_q^2-[2j]_q^2}$$
$$\equiv -\frac{q^{2j}([p]_q+[2j]_q)}{[2j]_q^2}\ (\mathrm{mod}\,[p]_q^2).$$

By (2.2), we have

$$-\frac{p^2-1}{12}(1-q)^2\equiv\sum_{j=1}^{p-1}\frac{q^j}{[j]_q^2}=\sum_{j=1}^{(p-1)/2}\frac{q^{2j}}{[2j]_q^2}+\sum_{j=1}^{(p-1)/2}\frac{q^{p-2j}}{[p-2j]_q^2}\tag{2.7}$$
$$=\sum_{j=1}^{(p-1)/2}\frac{q^{2j}}{[2j]_q^2}+\sum_{j=1}^{(p-1)/2}\frac{q^{p+2j}}{([p]_q-[2j]_q)^2}$$
$$\equiv 2\sum_{j=1}^{(p-1)/2}\frac{q^{2j}}{[2j]_q^2}\ (\mathrm{mod}\,[p]_q).$$

Hence

$$\sum_{j=1}^{p-1}\frac{(-1)^j}{[j]_q}\equiv\sum_{j=1}^{(p-1)/2}\frac{1}{[2j]_q}+\sum_{j=1}^{(p-1)/2}\frac{q^{2j}([p]_q+[2j]_q)}{[2j]_q^2}$$
$$\equiv\sum_{j=1}^{(p-1)/2}\frac{1+q^{2j}}{[2j]_q}-\frac{p^2-1}{24}(1-q)^2[p]_q$$
$$=2\sum_{j=1}^{(p-1)/2}\frac{1}{[2j]_q}-\frac{p-1}{2}(1-q)-\frac{p^2-1}{24}(1-q)^2[p]_q\ (\mathrm{mod}\,[p]_q^2).\ \blacksquare$$

3. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. One can directly verify (1.5) when $p=3$. So below we assume that $p\ge 5$. It is well-known (cf. Corollary 10.2.2 of [AAR]) that

$$(x;q)_n=\sum_{j=0}^{n}\begin{bmatrix}n\\ j\end{bmatrix}_q q^{\binom{j}{2}}(-x)^j.$$

Then we have

$$\frac{(-1;q)_p - q^{\binom{p}{2}} - 1}{[p]_q} \tag{3.1}$$
$$= \frac{1}{[p]_q}\sum_{k=1}^{p-1}\begin{bmatrix}p\\k\end{bmatrix}_q q^{\binom{k}{2}} = \sum_{k=1}^{p-1}\frac{1}{[k]_q}\prod_{j=1}^{k-1}\frac{q^j(1-q^{p-j})}{1-q^j}$$
$$= \sum_{k=1}^{p-1}\frac{1}{[k]_q}\prod_{j=1}^{k-1}\left(\frac{[p]_q}{[j]_q}-1\right) \equiv [p]_q \sum_{1\le j<k\le p-1}\frac{(-1)^k}{[j]_q[k]_q} - \sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q} \pmod{[p]_q^2}.$$

Consequently,

$$\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q} \equiv -\frac{(-1;q)_p - q^{\binom{p}{2}} - 1}{[p]_q}$$
$$\equiv -\frac{2(-q;q)_{p-1}-2}{[p]_q} - \frac{p-1}{2}(1-q) \pmod{[p]_q}.$$

Thus, applying Lemma 2.3, we have

$$\sum_{1\le j<k\le p-1}\frac{(-1)^k}{[j]_q[k]_q} - \frac{(p-1)(p+7)}{48}(1-q)^2 \tag{3.2}$$
$$\equiv \frac{1}{4}\left(\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q}\right)\left(\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q} + (p-3)(1-q)\right)$$
$$\equiv \frac{1}{4}\left(-2\mathrm{Q}_p(2,q) - \frac{p-1}{2}(1-q)\right)\left(-2\mathrm{Q}_p(2,q) + \frac{p-5}{2}(1-q)\right)$$
$$= \mathrm{Q}_p(2,q)^2 + \mathrm{Q}_p(2,q)(1-q) - \frac{(p-1)(p-5)}{16}(1-q)^2 \pmod{[p]_q}.$$

On the other hand, it follows from (2.4) that

$$\frac{(-1;q)_p - q^{\binom{p}{2}} - 1}{[p]_q}$$
$$\equiv \frac{2(-q;q)_{p-1}-2}{[p]_q} + \frac{p-1}{2}(1-q) - \frac{(p-1)(p-3)}{8}(1-q)^2[p]_q \pmod{[p]_q^2}.$$

Then by Lemma 2.4,

$$\sum_{k=1}^{p-1}\frac{(-1)^k}{[k]_q} + \frac{(-1;q)_p - q^{\binom{p}{2}} - 1}{[p]_q} \tag{3.3}$$
$$\equiv 2\sum_{j=1}^{(p-1)/2}\frac{1}{[2j]_q} + 2\mathrm{Q}_p(2,q) - \frac{(p-1)(p-2)}{6}(1-q)^2[p]_q \pmod{[p]_q^2}.$$

Combining (3.1), (3.2) and (3.3), the desired (1.5) is obtained. ∎

Proof of Theorem 1.2. Since

$$\begin{bmatrix} p-1 \\ (p-1)/2 \end{bmatrix}_{q^2} = \prod_{j=1}^{(p-1)/2} \frac{[p-j]_{q^2}}{[j]_{q^2}} = \prod_{j=1}^{(p-1)/2} \frac{[p]_{q^2} - [j]_{q^2}}{q^{2j}[j]_{q^2}},$$

we have

$$(3.4)\quad (-1)^{(p-1)/2} q^{(p^2-1)/4} \begin{bmatrix} p-1 \\ (p-1)/2 \end{bmatrix}_{q^2} = \prod_{j=1}^{(p-1)/2} \left(1 - \frac{[p]_{q^2}}{[j]_{q^2}}\right)$$

$$\equiv 1 - \frac{1+q^p}{1+q} \sum_{j=1}^{(p-1)/2} \frac{[p]_q}{[j]_{q^2}} + \frac{(1+q^p)^2}{(1+q)^2} \sum_{1\le j<k\le (p-1)/2} \frac{[p]_q^2}{[j]_{q^2}[k]_{q^2}} \pmod{[p]_{q^2}^3}.$$

From Theorem 1.1, we deduce that

$$(3.5)\quad \frac{1+q^p}{1+q} \sum_{j=1}^{(p-1)/2} \frac{1}{[j]_{q^2}} = (1+q^p) \sum_{j=1}^{(p-1)/2} \frac{1}{[2j]_q}$$

$$\equiv -(1+q^p)\mathrm{Q}_p(2,q)$$

$$+ \frac{1+q^p}{2}\left(\mathrm{Q}_p(2,q)^2 + \mathrm{Q}_p(2,q)(1-q) + \frac{p^2-1}{8}(1-q)^2\right)[p]_q$$

$$\equiv -(1+q^p)\mathrm{Q}_p(2,q) + \mathrm{Q}_p(2,q)^2[p]_q + \mathrm{Q}_p(2,q)(1-q)[p]_q$$

$$+ \frac{p^2-1}{8}(1-q)^2[p]_q \pmod{[p]_q^2}.$$

Notice that

$$\sum_{1\le j<k\le (p-1)/2} \frac{1}{[j]_{q^2}[k]_{q^2}} = \frac{1}{2}\left(\left(\sum_{j=1}^{(p-1)/2} \frac{1}{[j]_{q^2}}\right)^2 - \sum_{j=1}^{(p-1)/2} \frac{1}{[j]_{q^2}^2}\right)$$

$$= \frac{(1+q)^2}{2}\left(\left(\sum_{j=1}^{(p-1)/2} \frac{1}{[2j]_q}\right)^2 - \sum_{j=1}^{(p-1)/2} \frac{1}{[2j]_q^2}\right).$$

Theorem 1.1 implies that

$$\sum_{j=1}^{(p-1)/2} \frac{1}{[2j]_q} \equiv -\mathrm{Q}_p(2,q) \pmod{[p]_q}.$$

Then using (2.7), we get

$$\sum_{j=1}^{(p-1)/2} \frac{1}{[2j]_q^2} = \sum_{j=1}^{(p-1)/2} \frac{q^{2j}}{[2j]_q^2} + (1-q) \sum_{j=1}^{(p-1)/2} \frac{1}{[2j]_q}$$

$$\equiv -\frac{p^2-1}{24}(1-q)^2 - \mathrm{Q}_p(2,q)(1-q) \pmod{[p]_q}.$$

Consequently,

$$\frac{2}{(1+q)^2}\sum_{1\le j<k\le (p-1)/2}\frac{1}{[j]_{q^2}[k]_{q^2}} \equiv \mathrm{Q}_p(2,q)^2+\mathrm{Q}_p(2,q)(1-q)+\frac{p^2-1}{24}(1-q)^2 \pmod{[p]_q}. \tag{3.6}$$

Thus it follows from (3.4), (3.5) and (3.6) that

$$\begin{aligned}
&(-1)^{(p-1)/2}q^{(p^2-1)/4}\begin{bmatrix} p-1\\ (p-1)/2\end{bmatrix}_{q^2}-1\\
&\equiv [p]_q^2\frac{4}{(1+q)^2}\sum_{1\le j<k\le (p-1)/2}\frac{1}{[j]_{q^2}[k]_{q^2}}-[p]_q\frac{1+q^p}{1+q}\sum_{j=1}^{(p-1)/2}\frac{1}{[j]_{q^2}}\\
&\equiv \mathrm{Q}_p(2,q)^2[p]_q^2+(1+q^p)\mathrm{Q}_p(2,q)[p]_q+\mathrm{Q}_p(2,q)(1-q)[p]_q^2-\frac{p^2-1}{24}(1-q)^2[p]_q^2\\
&=((-q;q)_{p-1}-1)((-q;q)_{p-1}+1)-\frac{p^2-1}{24}(1-q)^2[p]_q^2 \pmod{[p]_q^3}. \ \blacksquare
\end{aligned}$$

4. Fermat quotient

LEMMA 4.1. *Let p be an odd prime. Suppose that m is a positive integer with $(m,p)=1$. Then*

$$\mathrm{Q}_p(m,q)\equiv\sum_{j=1}^{p-1}\frac{\lfloor jm/p\rfloor}{[jm]_q}-\frac{(p-1)(m-1)}{2}(1-q) \pmod{[p]_q}. \tag{4.1}$$

Proof. For each $j\in\{1,\dots,p-1\}$, let $r_j=jm-\lfloor jm/p\rfloor\, p$. Then

$$\begin{aligned}
\frac{(q^m;q^m)_{p-1}}{(q;q)_{p-1}}&=\prod_{j=1}^{p-1}\frac{1-q^{jm}}{1-q^j}=\prod_{j=1}^{p-1}\left(\frac{1-q^{r_j}}{1-q^j}+\frac{q^{r_j}(1-q^{\lfloor jm/p\rfloor p})}{1-q^j}\right)\\
&=\prod_{j=1}^{p-1}\frac{1-q^{r_j}}{1-q^j}\left(1+\frac{q^{r_j}(1-q^{\lfloor jm/p\rfloor p})}{1-q^{r_j}}\right).
\end{aligned}$$

Since r_j runs through $1,\dots,p-1$ together with j, we have

$$\begin{aligned}
&\frac{(q^m;q^m)_{p-1}}{(q;q)_{p-1}}\\
&=\prod_{j=1}^{p-1}\left(1+\frac{q^{r_j}(1-q^{\lfloor jm/p\rfloor p})}{1-q^{r_j}}\right)\equiv 1+(1-q^p)\sum_{j=1}^{p-1}\frac{q^{r_j}}{1-q^{r_j}}\cdot\frac{1-q^{\lfloor jm/p\rfloor p}}{1-q^p}\\
&\equiv 1+(1-q^p)\sum_{j=1}^{p-1}\left\lfloor\frac{jm}{p}\right\rfloor\frac{q^{r_j}}{1-q^{r_j}}\equiv 1+[p]_q\sum_{j=1}^{p-1}\left\lfloor\frac{jm}{p}\right\rfloor\frac{q^{jm}}{[jm]_q} \pmod{[p]_q^2}.
\end{aligned}$$

Finally,

$$\sum_{j=1}^{p-1}\left\lfloor\frac{jm}{p}\right\rfloor\frac{q^{jm}}{[jm]_q}=\sum_{j=1}^{p-1}\frac{\lfloor jm/p\rfloor}{[jm]_q}-(1-q)\sum_{j=1}^{p-1}\left\lfloor\frac{jm}{p}\right\rfloor$$
$$=\sum_{j=1}^{p-1}\frac{\lfloor jm/p\rfloor}{[jm]_q}-\frac{(p-1)(m-1)}{2}(1-q).\ \blacksquare$$

REMARK. Letting $q\to 1$ in (4.1), we obtain

$$\frac{m^p-m}{p}\equiv\sum_{j=1}^{p-1}\frac{\lfloor jm/p\rfloor}{j}\pmod p,$$

which was first discovered by Lerch [Ler].

Proof of Theorem 1.3. We write

$$\begin{bmatrix}p-1\\ \lfloor kp/m\rfloor\end{bmatrix}_{q^m}=\prod_{j=1}^{\lfloor kp/m\rfloor}\frac{[p]_{q^m}-[j]_{q^m}}{q^{jm}[j]_{q^m}}=q^{-m\binom{\lfloor kp/m\rfloor+1}{2}}\prod_{j=1}^{\lfloor kp/m\rfloor}\left(\frac{[p]_{q^m}}{[j]_{q^m}}-1\right).$$

As $p\nmid m$, $[p]_q$ divides $[p]_{q^m}=(1-q^{mp})/(1-q^m)$. Thus

$$(-1)^{(p-1)(m-1)/2}q^{\sum_{k=1}^{m-1}m\binom{\lfloor kp/m\rfloor+1}{2}}\prod_{k=1}^{m-1}\begin{bmatrix}p-1\\ \lfloor kp/m\rfloor\end{bmatrix}_{q^m}$$
$$=\prod_{k=1}^{m-1}\prod_{j=1}^{\lfloor kp/m\rfloor}\left(1-\frac{[p]_{q^m}}{[j]_{q^m}}\right)$$
$$\equiv 1-[p]_{q^m}\sum_{k=1}^{m-1}\sum_{1\le j<kp/m}\frac{1}{[j]_{q^m}}\quad(\text{here } kp/m\notin\mathbb{Z},\ \text{so } j\le\lfloor kp/m\rfloor<kp/m)$$
$$=1-[p]_{q^m}\sum_{j=1}^{p-1}\frac{m-1-\lfloor jm/p\rfloor}{[j]_{q^m}}\pmod{[p]_q^2}.$$

In view of (2.1) and Lemma 4.1, we have

$$[p]_{q^m}\sum_{j=1}^{p-1}\frac{m-1-\lfloor jm/p\rfloor}{[j]_{q^m}}$$
$$=(m-1)[mp]_q\sum_{j=1}^{p-1}\frac{1}{[jm]_q}-[mp]_q\sum_{j=1}^{p-1}\frac{\lfloor jm/p\rfloor}{[jm]_q}$$
$$\equiv(m-1)[mp]_q\frac{p-1}{2}(1-q)-[mp]_q\mathrm{Q}_p(m,q)-\frac{(p-1)(m-1)}{2}(1-q)[mp]_q$$
$$\equiv\ -m[p]_q\mathrm{Q}_p(m,q)\pmod{[p]_q^2}.\ \blacksquare$$

REMARK. For further developments of Granville's congruence (1.7), the reader is referred to [S].

5. A conjecture of Skula. Recently, with the help of polynomials over finite fields, Granville [G2] confirmed a conjecture of Skula:

$$\left(\frac{2^{p-1}-1}{p}\right)^2 \equiv -\sum_{j=1}^{p-1}\frac{2^j}{j^2} \pmod p \tag{5.1}$$

for any prime $p \geq 5$. Using our q-analogue of Lehmer's congruence, we have the following q-analogue of (5.1):

THEOREM 5.1. *Let $p \geq 5$ be a prime. Then*

$$\begin{aligned}\sum_{j=1}^{p-1}\frac{q^j(-q;q)_j}{[j]_q^2} &+ \mathrm{Q}_p(2,q)^2 \\ &\equiv -(p-1)\mathrm{Q}_p(2,q)(1-q) - \frac{(7p-5)(p-1)}{24}(1-q)^2 \pmod{[p]_q}.\end{aligned} \tag{5.2}$$

LEMMA 5.2.

$$\sum_{k=0}^{n}(-1)^k\begin{bmatrix}n\\k\end{bmatrix}_q q^{\binom{n-k}{2}}(-q;q)_k = (-1)^n q^{\binom{n+1}{2}}. \tag{5.3}$$

Proof. From the well-known q-binomial theorem (cf. Theorem 10.2.1 of [AAR]), we have

$$\sum_{k=0}^{\infty}\frac{(-1)^k q^{\binom{k}{2}}}{(q;q)_k}x^k = (x;q)_\infty \quad \text{and} \quad \sum_{k=0}^{\infty}\frac{(-q;q)_k}{(q;q)_k}x^k = \frac{(-qx;q)_\infty}{(x;q)_\infty}.$$

Then by comparing the coefficient of x^n on both sides of

$$(x;q)_\infty\frac{(-qx;q)_\infty}{(x;q)_\infty} = (-qx;q)_\infty,$$

we obtain

$$\sum_{k=0}^{n}\frac{(-1)^{n-k}q^{\binom{n-k}{2}}(-q;q)_k}{(q;q)_{n-k}(q;q)_k} = \frac{q^{\binom{n}{2}+n}}{(q;q)_n},$$

which is an equivalent form of (5.3). ∎

COROLLARY 5.3. *For any odd prime p, we have*

$$\sum_{j=1}^{p-1}\frac{q^j(-q;q)_j}{[j]_q} \equiv -2\mathrm{Q}_p(2,q) - (p-1)(1-q) \pmod{[p]_q}. \tag{5.4}$$

Proof. From Lemma 5.2, we deduce that

$$\begin{aligned}\sum_{j=1}^{p-1}\frac{q^j(-q;q)_j}{[j]_q} &\equiv \sum_{j=1}^{p-1}\frac{q^{p(p-1)/2-jp+j}(-q;q)_j}{[j]_q}\\ &\equiv -\frac{1}{[p]_q}\sum_{j=1}^{p-1}(-1)^j q^{\binom{p}{2}+\binom{j}{2}-jp+j}\begin{bmatrix}p\\ j\end{bmatrix}_q(-q;q)_j\\ &= -\frac{1}{[p]_q}\sum_{j=1}^{p-1}(-1)^j q^{\binom{p-j}{2}}\begin{bmatrix}p\\ j\end{bmatrix}_q(-q;q)_j\\ &= -\frac{1}{[p]_q}\left((-1)^p q^{\binom{p+1}{2}}-q^{\binom{p}{2}}-(-1)^p(-q;q)_p\right)\pmod{[p]_q}.\end{aligned}$$

Notice that

$$\frac{2-q^{\binom{p+1}{2}}-q^{\binom{p}{2}}}{[p]_q}\equiv\frac{p+1}{2}(1-q)+\frac{p-1}{2}(1-q)=p(1-q)\pmod{[p]_q},$$

and that

$$\begin{aligned}&\frac{(-q;q)_p-2}{[p]_q}\\ &\quad=\frac{(-q;q)_{p-1}(1+q^p)-2}{[p]_q}=\frac{2(-q;q)_{p-1}-2}{[p]_q}-(1-q)(-q;q)_{p-1}\\ &\quad\equiv 2\mathrm{Q}_p(2,q)-(1-q)\pmod{[p]_q}.\end{aligned}$$

Hence

$$\begin{aligned}\sum_{j=1}^{p-1}\frac{q^j(-q;q)_j}{[j]_q}&\equiv-\frac{(-q;q)_p-q^{\binom{p+1}{2}}-q^{\binom{p}{2}}}{[p]_q}\\ &\equiv -2\mathrm{Q}_p(2,q)-(p-1)(1-q)\pmod{[p]_q}.\ \blacksquare\end{aligned}$$

Remark. Corollary 5.3 is the q-analogue of an observation of Glaisher:

$$\frac{2^{p-1}-1}{p}\equiv-\sum_{j=1}^{p-1}\frac{2^{j-1}}{j}\pmod p. \tag{5.5}$$

Lemma 5.4.

$$\sum_{k=1}^{n}(-1)^k\begin{bmatrix}n\\ k\end{bmatrix}_q q^{\binom{n-k}{2}}\frac{(-q;q)_k}{[k]_q}=q^{\binom{n}{2}}\sum_{k=1}^{n}\frac{(-q)^k-1}{[k]_q}. \tag{5.6}$$

Proof. We make an induction on n. The case $n=1$ is trivial. Assume that $n>1$ and that (5.6) holds for the smaller values of n. Then we conclude

that

$$\sum_{k=1}^{n}(-1)^k\begin{bmatrix}n\\k\end{bmatrix}_q q^{\binom{n-k}{2}}\frac{(-q;q)_k}{[k]_q}$$
$$=\sum_{k=1}^{n}(-1)^k\left(q^k\begin{bmatrix}n-1\\k\end{bmatrix}_q+\begin{bmatrix}n-1\\k-1\end{bmatrix}_q\right)q^{\binom{n-k}{2}}\frac{(-q;q)_k}{[k]_q}$$
$$=q^{n-1}\sum_{k=1}^{n-1}(-1)^k\begin{bmatrix}n-1\\k\end{bmatrix}_q q^{\binom{n-k-1}{2}}\frac{(-q;q)_k}{[k]_q}$$
$$+\frac{1}{[n]_q}\sum_{k=1}^{n}(-1)^k\begin{bmatrix}n\\k\end{bmatrix}_q q^{\binom{n-k}{2}}(-q;q)_k$$
$$=q^{\binom{n}{2}}\sum_{k=1}^{n-1}\frac{(-q)^k-1}{[k]_q}+\frac{1}{[n]_q}((-1)^n q^{\binom{n+1}{2}}-q^{\binom{n}{2}}),$$

where in the last step we apply the induction hypothesis and Lemma 5.2. ∎

Proof of Theorem 5.1. Using Lemma 5.4, we have

$$\sum_{j=1}^{p-1}\frac{q^j(-q;q)_j}{[j]_q^2}\equiv\sum_{j=1}^{p-1}\frac{q^{p(p-1)/2-jp+j}(-q;q)_j}{[j]_q^2}$$
$$\equiv-\frac{1}{[p]_q}\sum_{j=1}^{p-1}(-1)^j q^{\binom{p-j}{2}}\begin{bmatrix}p\\j\end{bmatrix}_q\frac{(-q;q)_j}{[j]_q}$$
$$=-\frac{q^{\binom{p}{2}}}{[p]_q}\sum_{j=1}^{p}\frac{(-q)^j-1}{[j]_q}+(-1)^p\frac{(-q;q)_p}{[p]_q^2}$$
$$=-\frac{q^{\binom{p}{2}}}{[p]_q}\sum_{j=1}^{p-1}\frac{(-q)^j-1}{[j]_q}-\frac{(-q;q)_p-q^{\binom{p+1}{2}}-q^{\binom{p}{2}}}{[p]_q^2}\pmod{[p]_q}.$$

With help of (1.3) and Theorem 1.1, we get

$$\sum_{k=1}^{p-1}\frac{(-q)^j-1}{[j]_q}=-\sum_{k=1}^{p-1}\frac{(-1)^j(1-q^j)}{[j]_q}+\sum_{k=1}^{p-1}\frac{(-1)^j-1}{[j]_q}$$
$$=-\sum_{j=1}^{(p-1)/2}\frac{2}{[2j-1]_q}=\sum_{j=1}^{(p-1)/2}\frac{2}{[2j]_q}-\sum_{k=1}^{p-1}\frac{2}{[j]_q}$$
$$\equiv-2\mathrm{Q}_p(2,q)+\mathrm{Q}_p(2,q)^2[p]_q+\mathrm{Q}_p(2,q)(1-q)[p]_q+\frac{p^2-1}{8}(1-q)^2[p]_q$$
$$-\left((p-1)(1-q)+\frac{p^2-1}{12}(1-q)^2[p]_q\right)\pmod{[p]_q^2}.$$

By (2.4) we have

$$\begin{aligned}
&\frac{(-q;q)_p - q^{\binom{p+1}{2}} - q^{\binom{p}{2}}}{[p]_q^2} \\
&\quad = \frac{2(-q;q)_{p-1} - q^{\binom{p+1}{2}} - q^{\binom{p}{2}}}{[p]_q^2} - \frac{(-q;q)_{p-1}}{[p]_q}(1-q) \\
&\quad \equiv \frac{2(-q;q)_{p-1} - 2}{[p]_q^2} + \frac{p}{[p]_q}(1-q) - \frac{(p-1)^2}{4}(1-q)^2 - \frac{(-q;q)_{p-1}}{[p]_q}(1-q) \\
&\quad = \frac{2\mathrm{Q}_p(2,q)}{[p]_q} + \frac{(p-1)(1-q)}{[p]_q} - \frac{(p-1)^2}{4}(1-q)^2 \\
&\qquad - \mathrm{Q}_p(2,q)(1-q) \pmod{[p]_q}.
\end{aligned}$$

Therefore

$$\begin{aligned}
&\sum_{j=1}^{p-1} \frac{q^j(-q;q)_j}{[j]_q^2} \\
&\quad \equiv \left(\frac{(p-1)(1-q)}{2} - \frac{1}{[p]_q}\right) \sum_{j=1}^{p-1} \frac{(-q)^j - 1}{[j]_q} - \frac{(-q;q)_p - q^{\binom{p+1}{2}} - q^{\binom{p}{2}}}{[p]_q^2} \\
&\quad \equiv -(p-1)\mathrm{Q}_p(2,q)(1-q) - \mathrm{Q}_p(2,q)^2 \\
&\qquad - \frac{(7p-5)(p-1)}{24}(1-q)^2 \pmod{[p]_q}. \ \blacksquare
\end{aligned}$$

Acknowledgements. I am grateful to the anonymous referee for his/her helpful suggestions. I also thank my advisor, Prof. Zhi-Wei Sun, for his useful comments.

References

[AKS] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, Ann. of Math. 160 (2004), 781–793.

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

[AAR] G. E. Andrews, R. Askey and R. Roy, *Special Functions*, Cambridge Univ. Press, Cambridge, 1999.

[CP] R. Chapman and H. Pan, *q-Analogues of Wilson's theorem*, Int. J. Number Theory, accepted.

[C] W. E. Clark, *q-Analogue of a binomial coefficient congruence*, Int. J. Math. Math. Sci. 18 (1995), 197–200.

[F] R. D. Fray, *Congruence properties of ordinary and q-binomial coefficients*, Duke Math. J. 34 (1967), 467–480.

[G1] A. Granville, *Arithmetic properties of binomial coefficients I*: *Binomial coefficients modulo prime powers*, in: Organic Mathematics (Burnaby, BC, 1995), CMS Conf. Proc. 20, Amer. Math. Soc., Providence, RI, 1997, 253–276.

[G2] —, *The square of the Fermat quotient*, Integers 4 (2004), A22.

[GZ] V. J. W. Guo and J. Zeng, *Some arithmetic properties of the q-Euler numbers and q-Salié numbers*, European J. Combin. 27 (2006), 884–895.

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

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

[M] F. Morley, *Note on the congruence* $2^{4n} \equiv (-1)^n (2n)!/(n!)^2$, *where* $2n+1$ *is a prime*, Ann. of Math. 9 (1895), 168–170.

[PS] H. Pan and Z. W. Sun, *On q-Euler numbers*, *q-Salié numbers and q-Carlitz numbers*, Acta Arith. 124 (2006), 41–57.

[S] Z. W. Sun, *Products of binomial coefficients modulo* p^2, ibid. 97 (2001), 87–98.

[SP] L.-L. Shi and H. Pan, *A q-analogue of Wolstenholme's harmonic series congruence*, Amer. Math. Monthly 114 (2007), 529–531.

[W] J. Wolstenholme, *On certain properties of prime numbers*, Quart. J. Math. 5 (1862), 35–39.

Department of Mathematics
Shanghai Jiaotong University
Shanghai 200240, People's Republic of China
E-mail: haopan79@yahoo.com.cn

Received on 20.6.2006
and in revised form on 28.3.2007 (5223)