Advances in Applied Mathematics 130 (2021) 102228

Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama

A q-analogue of Wilson's congruence

Hao Pan [a,1], Yu-Chen Sun [b,*]

[a] School of Applied Mathematics, Nanjing University of Finance and Economics, Nanjing 210023, People's Republic of China
[b] Department of Mathematics and Statistics, University of Turku, 20014 Turku, Finland

ARTICLE INFO

Article history:
Received 8 February 2021
Received in revised form 1 May 2021
Accepted 14 May 2021
Available online xxxx

MSC:
primary 05A30
secondary 05A05, 05A10, 11A07

Keywords:
Wilson's congruence
Permutation cycle
Major index

ABSTRACT

Let $\mathcal{C}_n$ be the set of all permutation cycles of length n over $\{1, 2, \ldots, n\}$. Let

$$\mathfrak{f}_n(q) := \sum_{\sigma \in \mathcal{C}_{n+1}} q^{\operatorname{maj} \sigma}$$

be a q-analogue of the factorial $n!$, where maj denotes the major index. We prove a q-analogue of Wilson's congruence

$$\mathfrak{f}_{n-1}(q) \equiv \mu(n) \pmod{\Phi_n(q)},$$

where μ denotes the Möbius function and $\Phi_n(q)$ is the n-th cyclotomic polynomial.

* Corresponding author.
E-mail addresses: haopan79@zoho.com (H. Pan), yuchensun93@163.com (Y.-C. Sun).
1 The first author is supported by the National Natural Science Foundation of China (Grant No. 12071208).

https://doi.org/10.1016/j.aam.2021.102228

1. Introduction

For each $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$, define the q-integer

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

The q-integer evidently is a q-analogue of the original integer, since $\lim_{q\to 1}[n]_q = n$. Suppose that p is a prime. Correspondingly, q-congruences are the q-analogues of those congruences of integers. For example, for a prime p and a positive integer a with $(a, p) = 1$, it is not difficult to show that (cf. [6, (1.4)])

$$\prod_{k=1}^{p-1} [a]_{q^k} \equiv 1 \pmod{[p]_q}, \tag{1.1}$$

where the above congruence is considered over the polynomial ring $\mathbb{Z}[q]$. Clearly (1.1) is the q-analogue of Fermat's congruence

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.2}$$

Using the same discussion, (1.1) can be extended to

$$\prod_{k=1}^{n-1} [a]_{q^k} \equiv 1 \pmod{\Phi_n(q)}, \tag{1.3}$$

where $(a, n) = 1$ and

$$\Phi_n(q) := \prod_{\substack{1\le k\le n\\(k,n)=1}} (q - e^{2\pi i\cdot\frac{k}{n}})$$

denotes the n-th cyclotomic polynomial.

Another important congruence in number theory is the Wilson congruence

$$(p-1)! \equiv -1 \pmod{p} \tag{1.4}$$

for each prime p. The classical q-analogue of the factorial $n!$ is given by

$$[n]_q! := [1]_q[2]_q \cdots [n]_q.$$

Unfortunately, seemingly there exists no suitable q-analogue of Wilson's congruence for the q-factorial $[p-1]_q!$. For examples, we have

$$[6]_q! \equiv 3 + 3q - 4q^3 - 6q^4 - 4q^5 \pmod{[7]_q}.$$

Alternatively, in [1], Chapman and Pan gave a partial q-analogue of Wilson's congruence for those prime $p > 3$ with $p \equiv 3 \pmod 4$:

$$\prod_{k=1}^{p-1} [k]_{q^k} \equiv -1 \pmod{[p]_q}. \tag{1.5}$$

However, (1.5) is invalid if the prime $p \equiv 1 \pmod 4$, though Chapman and Pan also determined $\prod_{k=1}^{p-1}[k]_{q^k}$ modulo $[p]_q$ for those prime $p \equiv 1 \pmod 4$, with help of the fundamental unit and the class number of the quadratic field $\mathbb{Q}(\sqrt{p})$.

In this short note, we shall try to obtain a unified q-analogue of Wilson's congruence for all primes, from the viewpoint of combinatorics. Our motivation arises from Peterson's combinatorial proof of Wilson's congruence [8]. Let $\mathcal{S}_n$ denote the permutation group of order n, i.e., the set of all permutations over $\{1, 2, \dots, n\}$. Clearly $|\mathcal{S}_n| = n!$. For each $\sigma \in \mathcal{S}_n$, define the major index of σ

$$\operatorname{maj} \sigma := \sum_{\substack{1 \le i \le n-1 \\ \sigma(i) > \sigma(i+1)}} i.$$

It is known (cf. [3, Theorem 1.1]) that

$$[n]_q! = \sum_{\sigma \in \mathcal{S}_n} q^{\operatorname{maj} \sigma}. \tag{1.6}$$

Let

$$\mathcal{C}_n := \{\sigma \in \mathcal{S}_n : \sigma \text{ is a cycle of length } n\}.$$

We also have $|\mathcal{C}_n| = (n-1)!$. Define

$$\mathfrak{f}_n(q) := \sum_{\sigma \in \mathcal{C}_{n+1}} q^{\operatorname{maj} \sigma}. \tag{1.7}$$

Clearly $\mathfrak{f}_n(q)$ is another q-analogue of the factorial $n!$. In this note, we shall prove a q-analogue of Wilson's congruence for $\mathfrak{f}_n(q)$. Recall the Möbius function

$$\mu(n) := \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n = p_1 \cdots p_k \text{ where } p_1, \dots, p_k \text{ are distinct primes}, \\ 0 & \text{if } n > 1 \text{ is not square-free.} \end{cases}$$

Theorem 1.1. *Suppose that $n \ge 2$. Then*

$$\mathfrak{f}_{n-1}(q) \equiv \mu(n) \pmod{\Phi_n(q)}. \tag{1.8}$$

In particular, if p is prime, then

$$\mathfrak{f}_{p-1}(q) \equiv -1 \pmod{[p]_q}. \tag{1.9}$$

The group acting method to derive congruences was systematically developed by Rota and Sagan [10,11]. Subsequently, Sagan [12] extended this method to q-congruences. For more arithmetical applications of group actions, the readers may refer to [2,4,5,7,9]. In the next section, we shall follow the way of Sagan in [12] and use a group action on $\mathcal{C}_n$ to prove Theorem 1.1. Let us briefly describe Sagan's way to prove q-congruences. For a finite set A, in order to determine the polynomial $\sum_{a\in A} q^{m_a}$ modulo $\Phi_n(q)$, we may construct a group action T on A, and show that $\sum_{a\in U} q^{m_a}$ is divisible by $\Phi_n(q)$ for each orbit U under T with $|U| \geq 2$. Thus we only need to find out all fixed points under T.

Let us introduce some notions, which will be used in the next section. For each integer $n \geq 2$, let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n. We always identify $\mathbb{Z}_n$ with $\{1, 2, \ldots, n\}$, and view $\mathcal{S}_n$ as the permutation group over $\mathbb{Z}_n$. In particular, for each $1 \leq a, b \leq n$, we say $a < b$ over $\mathbb{Z}_n$ if and only if $a < b$ over $\mathbb{Z}$. Furthermore, for each $\sigma \in \mathcal{S}_n$, define

$$\overline{\mathrm{maj}}\,\sigma := \sum_{\substack{1\leq i\leq n\\ \sigma(i)>\sigma(i+1)}} i$$

and

$$\overline{\mathrm{des}}\,\sigma := \sum_{\substack{1\leq i\leq n\\ \sigma(i)>\sigma(i+1)}} 1.$$

2. Proof of Theorem 1.1

For a cycle $\sigma \in \mathcal{C}_n$, write $\sigma = (a_1, a_2, \ldots, a_n)$ provided that

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \quad \ldots, \quad \sigma(a_n) = a_1.$$

Let $\tau \in \mathcal{S}_n$ be defined by

$$\tau(a) = a + 1$$

for each $a \in \{1, 2, \ldots, n\}$, i.e., $\tau = (1, 2, \ldots, n)$. The following result is well-known.

Lemma 2.1. *For each $1 \leq r \leq n-1$, $\tau^r \in \mathcal{C}_n$ if and only if r is prime to n, where τ^k denotes the k-th iteration of τ.*

For each $\sigma \in \mathcal{S}_n$, let

$$T\sigma := \tau \circ \sigma \circ \tau^{-1}.$$

Then we have $T\mathcal{C}_n = \mathcal{C}_n$. In fact, for each cycle $\sigma = (a_1, a_2, \ldots, a_n) \in \mathcal{C}_n$,

$$T\sigma = (a_1 + 1, a_2 + 1, \ldots, a_n + 1) \in \mathcal{C}_n.$$

Clearly $T^n\sigma = \sigma$ for each $\sigma \in \mathcal{C}_n$, where T^k denotes the k-th iteration of T. Hence T can be viewed as a group action on $\mathcal{C}_n$.

For each $\sigma \in \mathcal{C}_n$, let

$$U_\sigma := \{T^k\sigma : 1 \le k \le n\}$$

denote the orbit of σ. We may partition $\mathcal{C}_n$ into union of disjoint orbits

$$\mathcal{C}_n = \bigcup_{\sigma \in X} U_\sigma.$$

Since T is a group action, we must have $|U_\sigma|$ divides n for each $\sigma \in X$.

Lemma 2.2. *Suppose that $\sigma \in \mathcal{C}_n$. Then $T\sigma = \sigma$ if and only if*

$$\sigma = \tau^r$$

for some $1 \le r \le n-1$ with $(r, n) = 1$.

Proof. It is easy to check that $T\tau^r = \tau^r$ for each $1 \le r \le n-1$. Conversely, according to the definition of T, we have

$$T\sigma(a+1) = \sigma(a) + 1$$

for each $a \in \mathbb{Z}_n$. Since $T\sigma = \sigma$,

$$\sigma(a) - a = T\sigma(a+1) - (a+1) = \sigma(a+1) - (a+1)$$

for each $a \in \mathbb{Z}_n$. Let $r = \sigma(a) - a$. Then $\sigma = \tau^r$. Since σ is a cycle, we have $(r, n) = 1$ by Lemma 2.1. □

According to Lemma 2.2, for each $\sigma \in X$, $|U_\sigma| = 1$ if and only if $\sigma = \tau^r$ for some r prime to n. That is,

$$\mathcal{C}_n = \{\tau^r : 1 \le r < n,\ (r, n) = 1\} \cup \bigcup_{\substack{\sigma \in X \\ |U_\sigma| > 1}} U_\sigma. \tag{2.1}$$

It follows from the definitions of maj and $\overline{\mathrm{maj}}$ that

$$\overline{\mathrm{maj}}\,\sigma = \begin{cases} \mathrm{maj}\,\sigma + n, & \text{if } \sigma(n) > \sigma(1), \\ \mathrm{maj}\,\sigma, & \text{otherwise.} \end{cases}$$

So we always have

$$\overline{\operatorname{maj}}\,\sigma \equiv \operatorname{maj}\sigma \pmod{n}. \tag{2.2}$$

Lemma 2.3. *Suppose that $\sigma \in \mathcal{C}_n$. Then*

$$\overline{\operatorname{maj}}\,T\sigma \equiv \overline{\operatorname{maj}}\,\sigma + \overline{\operatorname{des}}\,\sigma - 1 \pmod{n}. \tag{2.3}$$

Furthermore,

$$\overline{\operatorname{des}}\,T\sigma = \overline{\operatorname{des}}\,\sigma. \tag{2.4}$$

Proof. If $\sigma(i-1), \sigma(i) \neq n$, then

$$T\sigma(i) > T\sigma(i+1) \Longleftrightarrow \sigma(i-1)+1 > \sigma(i)+1 \Longleftrightarrow \sigma(i-1) > \sigma(i).$$

Assume that $\sigma(i_0) = n$. Clearly

$$T\sigma(i_0+1) = n+1 = 1 < T\sigma(i_0+2),$$

as well as $T\sigma(i_0) > T\sigma(i_0+1)$. Hence

$$\overline{\operatorname{maj}}\,T\sigma = i_0 + \sum_{\substack{1\le i\le n\\ i\neq i_0, i_0+1\\ T\sigma(i)>T\sigma(i+1)}} i = i_0 + \sum_{\substack{1\le i\le n\\ i\neq i_0, i_0+1\\ \sigma(i-1)>\sigma(i)}} i,$$

where we identify $\sigma(0)$ with $\sigma(n)$. Apparently

$$\sum_{\substack{1\le i\le n\\ i\neq i_0, i_0+1\\ \sigma(i-1)>\sigma(i)}} i = \sum_{\substack{0\le i\le n-1\\ i\neq i_0-1, i_0\\ \sigma(i)>\sigma(i+1)}} (i+1) \equiv \sum_{\substack{1\le i\le n\\ i\neq i_0-1, i_0\\ \sigma(i)>\sigma(i+1)}} (i+1) \pmod{n}.$$

It follows that

$$\overline{\operatorname{maj}}\,T\sigma \equiv i_0 + \sum_{\substack{1\le i\le n\\ i\neq i_0-1, i_0\\ \sigma(i)>\sigma(i+1)}} i + \sum_{\substack{1\le i\le n\\ i\neq i_0-1\\ \sigma(i)>\sigma(i+1)}} 1 \pmod{n}.$$

Finally, since $\sigma(i_0) = n$ is greater than $\sigma(i_0-1)$ and $\sigma(i_0+1)$, we have

$$i_0 + \sum_{\substack{1\le i\le n\\ i\neq i_0-1, i_0\\ \sigma(i)>\sigma(i+1)}} i = \overline{\operatorname{maj}}\,\sigma$$

and

$$\sum_{\substack{1\le i\le n\\ i\ne i_0-1,i_0\\ \sigma(i)>\sigma(i+1)}} 1 = \overline{\operatorname{des}}\,\sigma - 1.$$

(2.3) is concluded.

Similarly, we also have

$$\overline{\operatorname{des}}\,T\sigma = 1 + \sum_{\substack{1\le i\le n\\ i\ne i_0,i_0+1\\ T\sigma(i)>T\sigma(i+1)}} 1 = 1 + \sum_{\substack{1\le i\le n\\ i\ne i_0-1,i_0\\ \sigma(i)>\sigma(i+1)}} = \overline{\operatorname{des}}\,\sigma. \quad \square$$

Lemma 2.4. *For each $\sigma \in \mathcal{C}_n$, $\overline{\operatorname{des}}\,\sigma = 1$ if and only if $\sigma = \tau^r$ for some r prime to n.*

Proof. By Lemma 2.2 and (2.4), we only need to show that $\sigma = \tau^r$ with $(r, n) = 1$ when $\overline{\operatorname{des}}\,\sigma = 1$. Since n must contribute 1 to $\operatorname{des}(\sigma)$, $\overline{\operatorname{des}}\,\sigma = 1$ means $1, \dots, n-1$ contribute 0, i.e., σ is a cyclic shift of the identity $12\cdots n$. Hence $\sigma = \tau^r$ for some $1 \le r \le n$. Of course, r must be prime to n since $\sigma \in \mathcal{C}_n$. $\square$

Now we are ready to prove Theorem 1.1. In view of (2.1),

$$\mathfrak{f}_{n-1}(q) = \sum_{\substack{1\le r\le n\\ (r,n)=1}} q^{\operatorname{maj}\tau^r} + \sum_{\substack{\sigma\in X\\ |U_\sigma|>1}} \sum_{\upsilon\in U_\sigma} q^{\operatorname{maj}\upsilon}.$$

Suppose that $\sigma \in X$ and $|U_\sigma| \ge 2$. By Lemma 2.4, we have $\overline{\operatorname{des}}\,\sigma \ge 2$. Let $h = |U_\sigma|$. According to Lemma 2.3,

$$\begin{aligned}\sum_{\upsilon\in U_\sigma} q^{\operatorname{maj}\upsilon} \equiv \sum_{k=0}^{h-1} q^{\overline{\operatorname{maj}}\,T^k\sigma} &\equiv q^{\overline{\operatorname{maj}}\,\sigma} \sum_{k=0}^{h-1} q^{k(\overline{\operatorname{des}}\,\sigma-1)} \\ &= q^{\overline{\operatorname{maj}}\,\sigma} \cdot \frac{1-q^{h(\overline{\operatorname{des}}\,\sigma-1)}}{1-q^{\overline{\operatorname{des}}\,\sigma-1}} \pmod{\Phi_n(q)}.\end{aligned}$$

Since $1 \le \overline{\operatorname{des}}\,\sigma - 1 \le n-1$, $1 - q^{\overline{\operatorname{des}}\,\sigma-1}$ is not divisible by $\Phi_n(q)$. On the other hand, $T^h\sigma = \sigma$ since $|U_\sigma| = h$. So, by (2.3), we must have

$$h(\overline{\operatorname{des}}\,\sigma - 1) \equiv 0 \pmod{n},$$

i.e.,

$$1 - q^{h(\overline{\operatorname{des}}\,\sigma-1)} \equiv 0 \pmod{\Phi_n(q)}.$$

Thus for each $\sigma \in X$ with $|U_\sigma| > 1$, we have

$$\sum_{\upsilon \in U_\sigma} q^{\mathrm{maj}\,\upsilon} \equiv 0 \pmod{\Phi_n(q)}.$$

It follows that

$$\mathfrak{f}_{n-1}(q) \equiv \sum_{\substack{1\le r\le n\\(r,n)=1}} q^{\mathrm{maj}\,\tau^r} = \sum_{\substack{1\le r\le n\\(r,n)=1}} q^{n-r} = \sum_{\substack{1\le r\le n\\(r,n)=1}} q^r \pmod{\Phi_n(q)}.$$

Finally, it suffices to show that

$$\sum_{\substack{1\le r\le n\\(r,n)=1}} q^r \equiv \mu(n) \pmod{\Phi_n(q)}.$$

Let ζ be a n-th primitive root of unity. Then

$$\Phi_n(q) = \prod_{\substack{1\le k\le n\\(k,n)=1}} (q-\zeta^k).$$

So we only need to prove that for each $1 \le k \le n$ with $(k,n)=1$,

$$\lim_{q\to\zeta^k} \sum_{\substack{1\le r\le n\\(r,n)=1}} q^r = \mu(n). \tag{2.5}$$

(2.5) is a classical result on Ramanujan's sum

$$\sum_{\substack{1\le r\le n\\(r,n)=1}} \zeta^{kr}.$$

However, for the sake of completeness, here we give the proof of (2.5) as follows:

$$\sum_{\substack{1\le r\le n\\(r,n)=1}} \zeta^{kr} = \sum_{r=1}^{n} \zeta^{kr} \sum_{d\mid(r,n)} \mu(d) = \sum_{d\mid n} \mu(d) \sum_{j=1}^{n/d} \zeta^{kdj}$$
$$= \mu(n) + \sum_{\substack{d\mid n\\d<n}} \mu(d) \cdot \frac{1-\zeta^{kn}}{1-\zeta^{kd}} = \mu(n).$$

All are done. □

Remark. For each $\sigma \in \mathcal{S}_n$, define the inversion number of σ

$$\mathrm{inv}\,\sigma := \big|\{(i,j) : 1 \le i < j \le n,\ \sigma(i) > \sigma(j)\}\big|.$$

According to [3, Theorem 1.1], we also have

$$[n]_q! = \sum_{\sigma\in\mathcal{S}_n} q^{\operatorname{inv}\sigma}.$$

It is natural to ask what

$$\sum_{\sigma\in\mathcal{C}_n} q^{\operatorname{inv}\sigma} \pmod{\Phi_n(q)}$$

is. Unfortunately, the situation seems complicated. For example, we have

$$\sum_{\sigma\in\mathcal{C}_7} q^{\operatorname{inv}\sigma} \equiv 102+56q+38q^2+144q^3-14q^4+170q^5 \pmod{[7]_q}$$

and

$$\sum_{\sigma\in\mathcal{C}_9} q^{\operatorname{inv}\sigma} \equiv 2692-3980q+4690q^2-2386q^3+776q^4+1004q^5 \pmod{\Phi_9(q)}.$$

So, we may ask whether for each $n \geq 2$, there exists a subset $X_n \subset \mathcal{S}_n$ with $|X_n| = (n-1)!$ such that

$$\sum_{\sigma\in X_n} q^{\operatorname{inv}\sigma} \pmod{\Phi_n(q)}$$

could give another q-analogue of Wilson's congruence.

Acknowledgment

We are grateful to the anonymous referee for his/her very helpful comments on this paper.

References

[1] R. Chapman, H. Pan, q-analogues of Wilson's theorem, Int. J. Number Theory 4 (2008) 539–547.
[2] E. Deutsch, B.E. Sagan, Congruences for Catalan and Motzkin numbers and related sequences, J. Number Theory 117 (2006) 191–215.
[3] J. Haglund, The q, t-Catalan Numbers and the Space of Diagonal Harmonics, With an appendix on the combinatorics of Macdonald polynomials, University Lecture Series, vol. 41, American Mathematical Society, Providence, RI, 2008.
[4] D. Kim, J.S. Kim, A combinatorial approach to the power of 2 in the number of involutions, J. Comb. Theory, Ser. A 117 (2010) 1082–1094.
[5] M. Konvalinka, Divisibility of generalized Catalan numbers, J. Comb. Theory, Ser. A 114 (2007) 1089–1100.
[6] H. Pan, A q-analogue of Lehmer's congruence, Acta Arith. 128 (2007) 303–318.
[7] H. Pan, Congruences for q-Lucas numbers, Electron. J. Comb. 20 (2013) 29.
[8] J. Peterson, Beviser for Wilsons og Fermats Theoremer, Tidsskr. Math. 2 (1872) 64–65.

[9] A. Postnikov, B.E. Sagan, What power of two divides a weighted Catalan number?, J. Comb. Theory, Ser. A 114 (2007) 970–977.
[10] G.-C. Rota, B.E. Sagan, Congruences derived from group action, Eur. J. Comb. 1 (1980) 67–76.
[11] B.E. Sagan, Congruences via Abelian groups, J. Number Theory 20 (1985) 210–237.
[12] B.E. Sagan, Congruence properties of q-analogs, Adv. Math. 95 (1992) 127–143.