Europ. J. Combinatorics (1980) **1**, 283–287

Congruences for the q-secant Numbers

George E. Andrews and Dominique Foata

The q-secant number $E_{2n}(q)$ is shown to be congruent to $q^{2n(n-1)}$ (its term of highest degree) $\bmod(q+1)^2$ by using the combinatorial set-up of alternating permutations.

1. Introduction

Following Jackson [5] the q-secant numbers $E_{2n}(q)$ are polynomials that may be defined by

$$\sum_{n\geqslant 0} E_{2n}(q)u^{2n}/(q;q)_{2n} = 1\Big/\sum_{n\geqslant 0}(-1)^n u^{2n}/(q;q)_{2n} \tag{1.1}$$

where $(a;q)_n=(1-a)(1-aq)\cdots(1-aq^{n-1})$ for $n\geqslant 1$ and $(a;q)_0=1$. When q equals 1, the q-secant numbers become the ordinary secant (or Euler) numbers E_{2n} that occur in the Taylor expansion of $1/\cos x$. The recurrence

$$E_{2n}\equiv 1 \bmod 4 \tag{1.2}$$

goes back to Sylvester (see e.g. [6, p. 260]). As the polynomial $E_{2n}(q)$ is monic of degree $2n(n-1)$ (see Proposition 4.2 below), a good candidate for a q-analog of (1.2) is

$$E_{2n}(q)\equiv q^{2n(n-1)} \bmod (q+1)^2. \tag{1.3}$$

It is the purpose of this paper to derive (1.3) first by analytical methods, then combinatorially, that is, by making use of the classical interpretations of Euler and tangent numbers in terms of alternating permutations [1]. The latter numbers are the coefficients of the Taylor expansion of tan u. They also have q-analogs (further used in the paper) defined by

$$\sum_{n\geqslant 0} T_{2n+1}(q)u^{2n+1}/(q;q)_{2n+1} = \Big(\sum_{n\geqslant 0}(-1)^n u^{2n+1}\Big/(q;q)_{2n+1}\Big)\Big/\Big(\sum_{n\geqslant 0}(-1)^n u^{2n}/(q;q)_{2n}\Big). \tag{1.4}$$

2. Recurrence Formulae

Let $E(u)$ (resp. $T(u)$) be the generating function for the q-secant (resp. q-tangent) numbers as written in (1.1) (resp. (1.4)). Recurrence relations for the q-secant and q-tangent numbers can be derived by transforming the infinite series (1.1) and (1.4) into rational functions of $(\mathrm{i}u;q)_\infty$ and $(-\mathrm{i}u;q)_\infty$ (of course, $\mathrm{i}=(-1)^{1/2}$ and $(a;q)_\infty=\lim_n(a;q)_n$). The calculations were made by Andrews and Gessel [3, Equation (2.7) and the next one] who obtained

$$E(u)=2(-\mathrm{i}u;q)_\infty(\mathrm{i}u;q)_\infty/((-\mathrm{i}u;q)_\infty+(\mathrm{i}u;q)_\infty)$$

$$T(u)=(-\mathrm{i})((-\mathrm{i}u;q)_\infty-(\mathrm{i}u;q)_\infty)/((-\mathrm{i}u;q)_\infty+(\mathrm{i}u;q)_\infty).$$

From these expressions it is straightforward to get

$$E(u)-E(qu)=uE(qu)T(u)$$

$$T(u)-T(qu)=u+uT(qu)T(u).$$

AMS (MOS) subject classifications (1970), Primary 05A14, 05A19; secondary 33A30.

0195-6698/80/040283+05 $01.00/0

Equating coefficients of u^{2n-1} (resp. u^{2n}) in the expansions of both numbers of the first (resp. the second) one yields

$$E_{2n}(q)=\sum_{0\leqslant k\leqslant n-1}\begin{bmatrix}2n-1\\2k\end{bmatrix}q^{2k}E_{2k}(q)T_{2n-2k-1}(q)\quad(n\geqslant 1)\tag{2.1}$$

$$T_{2n+1}(q)=\sum_{0\leqslant k\leqslant n-1}\begin{bmatrix}2n\\2k+1\end{bmatrix}q^{2k+1}T_{2k+1}(q)T_{2n-2k-1}(q)\quad(n\geqslant 1),\tag{2.2}$$

where, of course, $\left[{N \atop M}\right]$ denotes the Gaussian polynomial

$$\begin{aligned}\begin{bmatrix}N\\M\end{bmatrix}&=(q;q)_N/((q;q)_M(q;q)_{N-M})\quad\text{for } 0\leqslant M\leqslant N\\&=0 \text{ otherwise.}\end{aligned}$$

Note that (2.1) and (2.2) provide the first values:

$$\begin{gathered}E_0(q)=E_2(q)=1;\qquad E_4(q)=q(q+1)^2+q^4;\\E_6(q)=q^2(q+1)^2(1+q^2+q^4)(1+q+q^2+2q^3)+q^{12};\\T_1(q)=1;\qquad T_3(q)=q(1+q);\qquad T_5(q)=q^2(1+q)^2(1+q^2)^2.\end{gathered}$$

3. An Inductive Proof

Formula (1.3) is trivial for $n=0,1$. Proceed by induction on $n\geqslant 2$, assuming that

$$q^{2k}E_{2k}(q)\equiv q^{2k^2}\bmod(q+1)^2$$

holds for every $k\leqslant n-1$. As $(1+q)^n$ divides $T_{2n+1}(q)$, as it was shown in [3], it follows from (2.1) that $\bmod(q+1)^2$ we have

$$\begin{aligned}E_{2n}(q)&\equiv\begin{bmatrix}2n-1\\2n-4\end{bmatrix}q^{2n-4}E_{2n-4}(q)T_3(q)+\begin{bmatrix}2n-1\\2n-2\end{bmatrix}q^{2n-2}E_{2n-2}(q)T_1(q)\\&\equiv\begin{bmatrix}2n-1\\3\end{bmatrix}q^{2(n-2)^2}q(1+q)+\begin{bmatrix}2n-1\\1\end{bmatrix}q^{2(n-1)^2}\\&\equiv(1+q)\left\{\begin{bmatrix}2n-1\\3\end{bmatrix}q^{2(n-2)^2}q+\frac{1-q^{2n-2}}{1-q^2}q^{2(n-1)^2}\right\}+q^{2n(n-1)}.\end{aligned}$$

As q tends to -1, the polynomial expression inside the curly parenthesis tends to zero. Therefore, the first term in the right-hand side member of the last equation vanishes $\bmod(q+1)^2$. This proves (1.3) for every $n\geqslant 0$.

The combinatorial proof is derived in the following paragraphs.

4. Alternating Permutations

A permutation $x=x_1x_2\cdots x_n$ of $1,2,\ldots,n(n\geqslant 1)$ is said to be *alternating* if $x_1<x_2$, $x_2>x_3$, $x_3<x_4,\cdots$ and so on, alternatively. The letters x_{2i-1} (resp. x_{2i}) are the troughs (resp. peaks) of x. The notion was introduced by Désiré André [1] that showed that the Euler number E_{2n} (resp. the tangent number T_{2n+1}) was equal to the number of alternating permutations of length $2n$(resp. $2n+1$).

By convention, there is one alternating permutation of length 0 and one of length 1. As usual, the *number of inversions* of a permutation $x=x_1x_2\cdots x_n$ is the number of pairs (i,j) with $1\leqslant i<j\leqslant n$ and $x_i>x_j$. It will be denoted by INV x.

Proposition 4.1. *For every $n \geq 0$ the polynomial $E_{2n}(q)$ (resp. $T_{2n+1}(q)$) is the generating function for alternating permutations of length $2n$ (resp. $2n+1$) by number of inversions.*

As the proposition has been proved in various contexts [4, 7, 8, 9], we only sketch a proof based on recurrence relations (2.1) and (2.2). As the Gaussian polynomial $\left[{2n-1 \atop 2k}\right]$ is the generating function for the permutations of $1^{2k}2^{2n-2k-1}$ by number of inversions (see e.g. [2, p. 41]), it is easy to derive by induction on n that the running term on the right-hand side of (2.1) is the generating function for the alternating permutations of length $2n$ with $(2k+1)$th letter equal to 1 by number of inversions. Hence, $E_{2n}(q)$ is the sum of all those generating polynomials. The result for $T_{2n+1}(q)$ is proved in an analogous manner by using (2.2).

5. Balanced Permutations

We next show that $E_{2n}(q)$ is monic by proving that there is a unique alternating permutation with maximal number of inversions.

Let $1 \leq i \leq 2n-1$. An alternating permutation $x = x_1x_2 \cdots x_{2n}$ is said to be *i-balanced,* if either i and $(i+1)$ are adjacent letters in x, in this order, or i and $(i+1)$ are not adjacent but $(i+1)$ occurs to the left of i.

For instance $x = 263\,415$ is i-balanced only for $i = 1, 3, 5$.

When x is i-balanced for every $i = 1, 2, \ldots, 2n-1$, we simply say that x is *balanced.*

Lemma 5.1. *The permutation $(2n-1) . 2n . (2n-3) . (2n-2) . \ldots . 3 . 4 . 1 . 2$ is the only balanced alternating permutation of length $2n$.*

Proof. The lemma holds for $n = 1$, since $1 . 2$ is the only alternating permutation of length 2. Assume $n \geq 2$ and let $x = x_1x_2 \cdots x_{2n}$ be a balanced alternating permutation. As $2n$ is necessarily a peak of x, it must be the leftmost one, i.e. $x_2 = 2n$. Now if the first letter x_1 was equal to i with $i \leq 2n-2$, then $(i+1)$ would occur to the right of i and x would not be balanced. Thus

$$x = (2n-1) . 2n . x_3 . x_4 . \ldots . x_{2n}.$$

Therefore x is balanced if and only if the factor $x_3x_4 \ldots x_{2n}$ is i-balanced for every $i = 1, 2, \ldots, 2n-3$. As, by induction, $(2n-3) . (2n-2) . \ldots . 3 . 4 . 1 . 2$ is the only balanced alternating permutation of length $(2n-2)$, we obtain the unique balanced alternating permutation of length $2n$ by placing $(2n . 1) . 2n$ at the beginning of it.

Let $x = x_1x_2 \cdots x_{2n}$ by a non-balanced alternating permutation and denote by i the greatest integer for which x is not i-balanced. If $(i+1)$ and i were adjacent letters in x in this order, all the letters greater than $(i+1)$ would be to the left of $(i+1)$. On the other hand, as x is alternating of even length, i would be a trough, that is, $x_j = i+1 > i = x_{j+1}$ and $i = x_{j+1} < x_{j+2}$ with $j+2 \leq n$. But this would contradict the fact that all letters greater than i are to the left of $x_j = i+1$. Therefore x is of the form

$$x = wiw'(i+1)w''$$

with w' a non-empty factor. Define

$$\Phi(x) = w(i+1)w'iw''.$$

Clearly, $\Phi(x)$ is also alternating and

$$\mathrm{INV}\ \Phi(x) = \mathrm{INV}\ x + 1. \tag{5.1}$$

PROPOSITION 5.2. *The polynomial $E_{2n}(q)$ is monic of degree $2n(n-1)$.*

PROOF. From (5.1) it follows that an alternating permutation with a maximal number of inversions is necessarily balanced. As there is only one such a permutation, the polynomial $E_{2n}(q)$ is monic. Finally, the balanced alternating permutation $(2n-1).2n.(2n-3).(2n-2).....3.4.1.2$ has an inversion number equal to $2n(n-1)$.

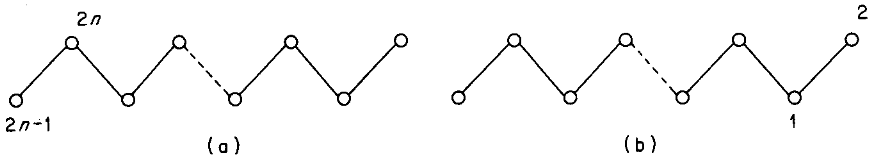
6. THE CONGRUENCE

We are then left to prove:

THEOREM 6.1. *Let $n \geqslant 0$; then*

$$E_{2n}(q) \equiv {}^{2n(n-1)} \bmod (q+1)^2.$$

PROOF. The theorem holds for $n=0$ and 1. Let $n \geqslant 2$ and denote by A_{2n} (resp. B_{2n}) the set of all alternating permutations of length $2n$ having $(2n-1)$ among their troughs (resp. having 2 among their peaks). If x belongs to A_{1n} (resp. B_{2n}) its graph has the (a)-form (resp. (b)-form).



(a) (b)

Therefore

$$\sum \{q^{\mathrm{INV}\,x} : x \in A_{2n}\} = \sum \{q^{\mathrm{INV}\,x} : x \in B_{2n}\} = q^{4(n-1)} E_{2n-2}(q)$$

and

$$\sum \{q^{\mathrm{INV}\,x} : x \in A_{2n} \cap B_{2n}\} = q^{4(n-2)+4(n-1)} E_{2n-4}(q).$$

By induction

$$\sum \{q^{\mathrm{INV}\,x} : x \in A_{2n} \cup B_{2n}\} \equiv 2q^{4(n-1)} q^{2(n-1)(n-2)} - q^{4(n-2)+4(n-1)} q^{2(n-2)(n-3)} \bmod (q+1)^2$$
$$\equiv q^{2n(n-1)} \bmod (q+1)^2.$$

Let C_{2n} be the complement of $A_{2n} \cup B_{2n}$, that is, the set of alternating permutations of length $2n$ having $(2n-1)$ and $2n$ among their peaks and 1 and 2 among their troughs. There remains to prove

$$\sum \{q^{\mathrm{INV}\,x} : x \in C_{2n}\} \equiv 0 \bmod (q+1)^2.$$

Let σ and τ be the transpositions $(2n-1, 2n)$ and $(1, 2)$, respectively, and G be the group of order 4 generated by $\{\sigma, \tau\}$. Clearly G acts on C_{2n}, and the generating polynomial for the four elements of each orbit by number of inversions is divisible by $(q+1)^2$. Therefore the generating polynomial for all elements of C_{2n} is also divisible by $(q+1)^2$.

REFERENCES

1. D. André, Sur les permutations alternées, *J. Math. Pures Appl.* **7** (1881), 167–184.
2. G. E. Andrews, The theory of partitions, *Encyclopedia of Mathematics and its Applications*, Vol. 2, Addison-Wesley, Reading, Mass., 1976.

3. G. E. Andrews and I. Gessel, Divisibility properties of the q-tangent numbers, *Proc. Amer. Math. Soc.* **68** (1978), 380–384.
4. I. Gessel, Generating functions and enumeration of sequences, Ph.D. Thesis, Massachusetts Institute of Technology, 1977.
5. F. H. Jackson, A basic-sine and cosine with symbolical solutions of certain differential equations, *Proc. Edinburgh Math. Soc.* **22** (1904), 28–39.
6. N. Nielsen, *Traité Élémentaire des Nombres de Bernoulli*, Gauthier-Villars, Paris, 1923.
7. D. Rawlings, Generalized Worpitzky identities, with applications to permutation enumeration, *European J. Combin.*, to appear.
8. M. P. Schützenberger, Oral communication, Combinatorics Conference, Oberwolfach, 1975.
9. R. P. Stanley, Binomial posets, Möbius inversion and permutation enumeration, *J. Combin. Theory Ser. A* **20** (1976), 336–356.

Received 23 June 1980

G. E. Andrews

Department of Mathematics, Pennsylvania State University,
University Park, Pennsylvania 16802, U.S.A.

D. Foata

Département de Mathématique, Université de Strasbourg,
7, rue René Descartes, F67084, Strasbourg, France