AN ACTION ON PERMUTATIONS WITH APPLICATION TO EULERIAN NUMBERS

SHINJI TANIMOTO

Received October 19, 2000

ABSTRACT. An action on permutations is introduced, which preserves the numbers of their ascents and descents. Periodicity of permutations under the action is investigated and its application is given to proofs of some congruence relations modulo a prime for Eulerian numbers.

1. Introduction. For a positive integer n, an *ascent* (or an *up*) in a permutation $a_1a_2\cdots a_n$ of $\{1,2,\ldots,n\}$ means an adjacent pair such that $a_i < a_{i+1}$ for some i $(1 \leq i \leq n-1)$. For k $(0 \leq k \leq n-1)$ let us denote by $E(n,k)$ the set of all permutations with exactly k ascents and by $e(n,k)$ its cardinal number, namely, an *Eulerian number*. A *descent* (or a *down*) in a permutation $a_1a_2\cdots a_n$ is an adjacent pair such that $a_i > a_{i+1}$ for some i $(1 \leq i \leq n-1)$. In this paper we call a consecutive sequence $a_i\cdots a_j$ in a permutation $a_1a_2\cdots a_n$ an *ascending chain* (or "run up" due to [3]) if $a_{i-1} > a_i < a_{i+1} < \cdots < a_j > a_{j+1}$. For a permutation $A = a_1a_2\cdots a_n$ we define its *reflection* by $A^* = a_na_{n-1}\cdots a_1$. It is easy to see that $A^* \in E(n,k)$ if and only if $A \in E(n,n-k-1)$, because the number of descents in A is equal to $n-k-1$. Since two adjacent ascending chains of permutations in $E(n,k)$ are separated by a descent, we see that the number of ascending chains is equal to $(n-k-1)+1 = n-k$.

We introduce an action on permutations which preserves the numbers of ascents and descents of permutations. Our main objective is to deduce properties of periodicity under the action and to apply them for studying properties of Eulerian numbers. Our result includes a generalization of a congruence relation modulo a prime, which was given in [5]. As for other properties and identities of Eulerian numbers we refer to [1, 2, 4], for example.

2. Periods of permutations under an action. We introduce an action denoted by σ on the set of all permutations of $\{1,2,\ldots,n\}$. This is defined by adding one to all entries of a permutation $A = a_1a_2\cdots a_n$ and by changing $n+1$ into one. But when $a_1 = n$, all entries a_i are cyclically shifted to the left by one place and one is added so that we obtain $\sigma A = b_2b_3\cdots b_n1$, where $b_i = a_i + 1$ for $2 \leq i \leq n$. Moreover, when $a_n = n$, all entries a_i are cyclically shifted to the right by one place and one is added so that we obtain $\sigma A = 1b_1b_2\cdots b_{n-1}$, where $b_i = a_i + 1$ for $1 \leq i \leq n-1$. Thus, for example, we have $\sigma(426315) = 531426$, $\sigma(531426) = 164253$ and $\sigma(624135) = 352461$.

By the definition of ascents it is easy to see that if $A = a_1a_2\cdots a_n$ is in $E(n,k)$, then σA is also in $E(n,k)$. We denote successive applications of the action σ by $\sigma^2A = \sigma(\sigma A)$ and inductively by $\sigma^\ell A = \sigma(\sigma^{\ell-1}A)$ for a positive integer ℓ. For convenience sake we take $\sigma^0 A = A$ for all permutations A. In order to consider periodicity of the action it is effective to adopt terminology from finite group actions as in [2]. For $A = a_1a_2\cdots a_n$ it is

2000 *Mathematics Subject Classification.* 11B68.
Key words and phrases. Eulerian numbers, permutations.

shown that there exists a positive integer ℓ such that $\sigma^\ell A = A$. We call the smallest such positive integer the *period* of A and the set $\{A, \sigma A, \ldots, \sigma^{\ell-1}A\}$ of distinct permutations the *orbit* of A. We sometimes denote the period of a permutation A by $\pi(A)$. Permutations with period one, or those satisfying $\sigma A = A$ are called *fixed points* of the action σ. It is easily seen that fixed points are only two permutations; $12\cdots n \in E(n, n-1)$ and $n\cdots 21 \in E(n, 0)$. We divide $E(n,k)$ into two parts. $E^-(n,k)$ is the set of permutations $A = a_1 a_2 \cdots a_n$ with $a_1 < a_n$ and $E^+(n,k)$ is the set of those with $a_1 > a_n$. Observe that $\sigma A \in E^-(n,k)$ for $A \in E^-(n,k)$ and $\sigma A \in E^+(n,k)$ for $A \in E^+(n,k)$ hold, as is easily seen.

Lemma 1. *For any permutation A,*

(i) $A^{**} = A$;

(ii) $(\sigma A)^* = \sigma A^*$;

(iii) $\pi(A^*) = \pi(A)$.

Proof. The proofs of (i) and (ii) are obvious. Applying induction to (ii) yields $(\sigma^\ell A)^* = \sigma^\ell A^*$ for a positive integer ℓ. Putting $\ell = \pi(A)$ we have $A^* = \sigma^{\pi(A)} A^*$. Hence we see that $\pi(A^*) \le \pi(A)$. Since the reverse inequality also holds, the proof of (iii) is complete.

Lemma 2. *For a permutation $A = a_1 a_2 \cdots a_n$ in $E(n,k)$, where $0 \le k \le n-1$, the following relations hold.*

(i) *For $A \in E^-(n,k)$, $\sigma^{n(n-k)} A = A$.*

(ii) *For $A \in E^+(n,k)$, $\sigma^{n(k+1)} A = A$.*

Proof. First we prove (i). Applying σ^n remains each entry unchanged. But in case of $E^-(n,k)$ some entries at the right-hand end of permutation change their positions and move to the left-hand end. Those entries constitutes an ascending chain of A. Thus the last ascending chain of permutation is collectively moved to the left end. Since A is in $E(n,k)$, it contains $n-k$ ascending chains. Therefore, $n-k$ applications of σ^n yields A, i.e., $\sigma^{n(n-k)} A = A$. In order to prove (ii) let us consider the reflection of $A \in E^+(n,k)$. Since A^* belongs to $E^-(n, n-k-1)$, applying Lemma 1 and the result (i), we see that $\sigma^{n(k+1)} A^* = A^*$ and hence $\sigma^{n(k+1)} A = A$.

A relation proved in Lemma 2 is frequently used in the sequel. Let a permutation $A \in E^-(n,k)$ be written as $A_1 A_2 \cdots A_{n-k}$ by arranging all $n-k$ ascending chains. Then it holds that

$$\sigma^n A = A_{n-k} A_1 A_2 \cdots A_{n-k-1}.$$

Taking $A = 2671453 \in E^-(7,4)$, for example, three ascending chains are $A_1 = (267)$, $A_2 = (145)$, $A_3 = (3)$. Then $\sigma^7 A = 3267145$, $\sigma^{14} A = 1453267$ and $\sigma^{21} A = 2671453$.

Lemma 2 also implies that the period of a permutation in $E(n,k)$ is a divisor of $n(n-k)$ or $n(k+1)$. The following theorem says in turn that it is a multiple of $n-k$ or $k+1$.

Theorem 3. *For a permutation $A \in E(n,k)$, where $0 \le k \le n-1$, the period $\pi(A)$ is equal to $d(n-k)$ or $d(k+1)$ for a divisor d of n, according to $A \in E^-(n,k)$ or $A \in E^+(n,k)$.*

Proof. Suppose $A \in E^-(n,k)$. By the relation following Lemma 2, if the period $\pi(A)$ is a multiple of n, then $\pi(A) = n(n-k)$ holds, since A is composed of $n-k$ ascending chains. So let us suppose the contrary and let $\pi(A) = qn + r$, where q is a nonnegative

integer and the residue r satisfies $1 \le r \le n-1$. Since $A \in E^-(n,k)$ is composed of $n-k$ ascending chains, we write it by $A = A_1 A_2 \cdots A_{n-k}$. Then

$$\sigma^r A = A_{q+1} \cdots A_{n-k} A_1 \cdots A_q.$$

This follows from the fact that $\sigma^{\pi(A)} A = \sigma^{qn}(\sigma^r A) = A$ and each σ^n moves an ascending chain at the right end into the left end. Similarly, from $\sigma^{2(qn+r)} A = \sigma^{2qn}(\sigma^{2r} A) = A$, we obtain

$$\sigma^{2r} A = A_{2q+1} \cdots A_{n-k} A_1 \cdots A_{2q}.$$

In a similar way, for an integer $s = n/\gcd(n,r)$ for which sr becomes the smallest positive multiple of n, we have

$$\sigma^{sr} A = A_{sq+1} \cdots A_{n-k} A_1 \cdots A_{sq}.$$

On the other hand, from $sr = nr/\gcd(n,r)$, we also have

$$\sigma^{sr} A = A_{(n-k)-r/\gcd(n,r)+1} \cdots A_{n-k} A_1 \cdots A_{(n-k)-r/\gcd(n,r)}.$$

Here the indices of A in both expressions should be considered as modulo $n-k$. Observing the indices of both the last ascending chains, we have

$$sq = \frac{qn}{\gcd(n,r)} \equiv n-k-\frac{r}{\gcd(n,r)} \pmod{n-k}.$$

Therefore, for some integer d,

$$\pi(A) = qn + r = d(n-k).$$

Lemma 2 says that $\pi(A)$ divides $n(n-k)$. Therefore, d is a divisor of n. In case of $A \in E^+(n,k)$, A^* belongs to $E^-(n, n-k-1)$ and hence we see that the period of A is equal to $d(k+1)$ for some divisor d of n.

This theorem tells us that possible minimal periods of permutations in $E(n,k)$ is either $n-k$ or $k+1$. The following theorem answers the question whether such permutations exist.

Theorem 4. *There exists a unique orbit of the period $n-k$ in $E^-(n,k)$ if and only if $\gcd(n,k) = 1$. Similarly, there exists a unique orbit of the period $k+1$ in $E^+(n,k)$ if and only if $\gcd(n,k+1) = 1$.*

Proof. Let $\ell = n-k$ be the period of $A \in E^-(n,k)$. Then its orbit $\{\sigma A, \ldots, \sigma^\ell A = A\}$ appears n times repeatedly in the set $\{\sigma A, \ldots, \sigma^{n(n-k)} A = A\}$. As is seen from the proof of Lemma 2, each entry in A is only once changed to 1 at the left end of permutation in the course of $n(n-k)$ applications of σ. Therefore, a unique $\sigma^i A$ in $\{\sigma A, \ldots, \sigma^\ell A = A\}$ has the form $B = 1 a_2 a_3 \cdots a_n$. Since A and B generate the same orbit of period $n-k$, it suffices to consider the orbit of B. Let $s = n+1-a_n$. Then $\sigma^s B$ also has the form $1 b_2 b_3 \cdots b_n$. This implies $\sigma^s B = B$ and hence $s \ge \ell$. But, in order to obtain B again, we must apply σ to B at least s times. Consequently, we get $s \le \ell$ and the equality $n+1-a_n = \ell$ or $a_n = n+1-\ell$ holds. Thus, under σ^ℓ, a_n changes to 1 and a_{n-1} to a_n, and so on. Therefore we see that all entries are determined as follows; $a_{n-j} = n+1-(j+1)\ell \pmod{n}$ for j $(0 \le j \le n-2)$. The condition for such a permutation to exist is $\gcd(n,\ell) = \gcd(n,k) = 1$. Conversely, it is easy to show that such a permutation A (or B) has a period of $\ell = n-k$. Next to verify that it indeed belongs to $E^-(n,k)$, note that $\sigma^{g\ell} A = A$ for $g = n/\gcd(n,\ell) = n$. Then $g\ell$ is the minimal multiple of n. Assume that $A \in E^-(n,h)$. Lemma 2 says that the minimal

m such that $\sigma^{mn}A = A$ is $m = n-h$. Hence $g\ell = n(n-h)$ holds, from which we get $h = k$. The latter half follows from the former.

3. Application to Eulerian numbers. When n is a prime, the set $E(n,k)$ is easily partitioned into a few classes in terms of periods. The aim of this section is to derive some congruence relations for Eulerian numbers $e(n,k)$ from the partition. Let $e^-(n,k)$ or $e^+(n,k)$ be the cardinality of $E^-(n,k)$ or $E^+(n,k)$, respectively. Ordinary Eulerian numbers are given by $e(n,k) = e^-(n,k) + e^+(n,k)$.

Theorem 5. *Let p be a prime and m, k positive integers such that $1 \le k \le p^m - 1$.*

(i) *If* $\gcd(p,k) = 1$, *then* $e^-(p^m,k) \equiv p^m - k \pmod{p(p^m-k)}$,
otherwise $e^-(p^m,k) \equiv 0 \pmod{p(p^m-k)}$.

(ii) *If* $\gcd(p,k+1) = 1$, *then* $e^+(p^m,k) \equiv k+1 \pmod{p(k+1)}$,
otherwise $e^+(p^m,k) \equiv 0 \pmod{p(k+1)}$.

Proof. We will prove these relations by classifying permutations of $E(p^m,k)$ in terms of periods. Since p is a prime, it follows from Theorem 3 that periods of permutations in $E^-(p^m,k)$ or $E^+(p^m,k)$ are of the form $p^i(p^m-k)$ or $p^i(k+1)$, respectively, for some i $(0 \le i \le m)$. Let α be the number of orbits of period p^m-k in $E^-(p^m,k)$ and let β be that of period $k+1$ in $E^+(p^m,k)$. Then $e^-(p^m,k)$ equal the sum of $\alpha(p^m-k)$ and a multiple of $p(p^m-k)$, and $e^+(p^m,k)$ is the sum of $\beta(k+1)$ and a multiple of $p(k+1)$. Due to Theorem 4, if $\gcd(p^m,k) = \gcd(p,k) = 1$ then $\alpha = 1$ and otherwise $\alpha = 0$. Moreover, if $\gcd(p^m,k+1) = \gcd(p,k+1) = 1$ then $\beta = 1$ and otherwise $\beta = 0$. From this observation the congruence relations in (i) and (ii) follow immediately.

In [5] a special case (m =1) of the next corollary is proved by means of relationships between Stirling numbers and Eulerian numbers. However, our proof needs no analytic calculation involving identities of Eulerian numbers, and it is simple and straightforward.

Corollary 6. *Let p be a prime and m a positive integer. The congruence relation $e(p^m,k) \equiv 1 \pmod{p}$ holds for k $(0 \le k \le p^m - 1)$.*

Proof. Since $e(p^m,0) = 1$, it is evident for $k = 0$. Let $k \ge 1$. Suppose first that both the conditions $\gcd(p^m,k) = \gcd(p,k) = 1$ and $\gcd(p^m,k+1) = \gcd(p,k+1) = 1$ are fulfilled. Then, by the preceding theorem, we have $e^-(p^m,k) \equiv -k \pmod{p}$ and $e^+(p^m,k) \equiv k+1 \pmod{p}$. Since $e(n,k) = e^-(n,k) + e^+(n,k)$, in this case the congruence relation follows. Next suppose that $\gcd(p,k) = 1$ and $\gcd(p,k+1) \ne 1$. Then $k+1$ is a multiple of p. Theorem 5 implies $e^-(p^m,k) \equiv -k \equiv 1 \pmod{p}$ and $e^+(p^m,k) \equiv 0 \pmod{p}$. Finally suppose that $\gcd(p,k) \ne 1$ and $\gcd(p,k+1) = 1$. Then k is a multiple of p and by Theorem 5 we have $e^-(p^m,k) \equiv 0 \pmod{p}$ and $e^+(p^m,k) \equiv k+1 \equiv 1 \pmod{p}$. In both cases the congruence relation also holds.

References

[1] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics,* Addison-Wesley, Reading, 1989.

[2] A. Kerber, *Algebraic Combinatorics Via Finite Group Actions,* BI-Wissenschaftsverlag, Mannheim, 1991.

[3] D.E. Knuth, *The Art of Computer Programming,* Vol. 2 (2nd Edition), Addison-Wesley, Reading, 1981.

[4] D.E. Knuth, *The Art of Computer Programming,* Vol. 3, Addison-Wesley, Reading, 1973.

[5] J. E. Nymann and R. A. Sáenz, *Eulerian Numbers: Inversion Formulas and Congruences Modulo a Prime,* Fibonacci Quart. **37** (1999), 154-161.

Department of Applied Mathematics, Kochi Women's University, Kochi 780-8515, Japan.

E-mail: tanimoto@cc.kochi-wu.ac.jp