Journal of Combinatorial Theory, Series A 117 (2010) 1082–1094

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

A combinatorial approach to the power of 2 in the number of involutions

Dongsu Kim [1], Jang Soo Kim [2]

Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology, Daejeon 305-701, Republic of Korea

ARTICLE INFO

Article history:
Received 25 February 2009
Available online 21 August 2009

Keywords:
Power of a prime
Divisibility
Involutions

ABSTRACT

We provide a combinatorial approach to the largest power of p in the number of permutations π with $\pi^p = 1$, for a fixed prime number p. With this approach, we find the largest power of 2 in the number of involutions, in the signed sum of involutions and in the numbers of even or odd involutions.

1. Introduction

The largest power of a prime in some well-known numbers has been studied in many papers, for instance, see [1–3,5–11]. In this paper we are interested in the largest power of a prime in the numbers of permutations with some conditions.

Let $\mathfrak{S}_n$ denote the set of permutations of $[n] = \{1, 2, \dots, n\}$. Let p be a prime number and n a positive integer. Let $\tau_p(n)$ denote the number of permutations $\pi \in \mathfrak{S}_n$ such that $\pi^p = 1$, and let $\mathrm{ord}_p(n)$ denote the largest integer k such that p^k divides n.

In 1951, using recurrence relation with induction, Chowla, Herstein and Moore [2] proved that

$$\mathrm{ord}_2\big(\tau_2(n)\big) \geqslant \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor.$$

Using generating function, Grady and Newman [6] obtained, for any prime p,

$$\mathrm{ord}_p\big(\tau_p(n)\big) \geqslant \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor. \tag{1}$$

E-mail addresses: dongsu.kim@kaist.ac.kr (D. Kim), jskim@kaist.ac.kr (J.S. Kim).

[1] The author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2009-0063183).

[2] The author was supported by the second stage of the Brain Korea 21 Project, The Development Project of Human Resources in Mathematics, KAIST in 2009.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2009.08.002

Using p-adic analysis, Ochiai [10] found the exact value of $\mathrm{ord}_p(\tau_p(n))$ for prime numbers $p \leqslant 23$. Let t_n denote $\tau_2(n)$, the number of involutions in $\mathfrak{S}_n$. Ochiai's result gives

$$\mathrm{ord}_2(t_n) = \left\lfloor \frac{n}{2} \right\rfloor - 2\left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n+1}{4} \right\rfloor. \tag{2}$$

In addition, Chowla et al. [2] considered the sequence $\{t_n \bmod m\}_{n\geqslant 0}$ for a fixed integer m and proved that m is a period of the sequence if m is odd. We will prove that in fact, it is the smallest period. If m is even, then the sequence is not periodic because $t_0 = 1$ but t_n is even for all $n \geqslant 2$. However there is an integer N such that $\{t_n \bmod m\}_{n\geqslant N}$ is periodic.

Our main results are in Sections 2 and 3, where we prove (1) and (2) using combinatorial arguments. The weighted sum of involutions is considered in Section 4. In Section 5 we find ord_2 of the signed sum of involutions, the number of odd involutions, and the number of even involutions. In Section 6 we find the smallest N such that $\{t_n \bmod m\}_{n\geqslant N}$ is periodic and find the smallest period of the sequence when m is even. We also consider the odd factor of the number of involutions and prove that the smallest period of the sequence $\{t_n/2^{\mathrm{ord}_2(t_n)} \bmod 2^s\}_{n\geqslant 0}$ is 2^{s+1} if $s \geqslant 3$.

2. A combinatorial proof

Let $\mathfrak{S}_{n,p}$ denote the set of permutations $\pi \in \mathfrak{S}_n$ with $\pi^p = 1$. For instance, for $p = 2$ it is the set of all involutions in $\mathfrak{S}_n$. Each permutation in $\mathfrak{S}_{n,p}$ is a product of disjoint p-cycles and 1-cycles. For example, for $\pi = 38725614 \in \mathfrak{S}_{8,3}$, the disjoint product is $(1,3,7)(2,8,4)(5)(6)$. A cycle usually consists of distinct integers, but we allow cycles to have repeated entries for convenience.

We define a *label map* $f_p : \{1,2,\ldots,n\} \to \{1,2,\ldots,\lfloor (n-1)/p\rfloor + 1\}$ by $f_p(i) = \lfloor (i-1)/p\rfloor + 1$, extend it to cycles $\sigma = (s_1,\ldots,s_j)$ by $f_p(\sigma) = (f_p(s_1),\ldots,f_p(s_j))$ which is regarded as a cycle with repeated entries, and to $\mathfrak{S}_{n,p}$ by

$$f_p(\pi) = \{f_p(\sigma_1),\ldots,f_p(\sigma_k)\}$$

for $\pi = \sigma_1\sigma_2\cdots\sigma_k$ in the disjoint cycle notation. Note that $f_p(\pi)$ is regarded as a multiset.

As a map defined on $\mathfrak{S}_{n,p}$, f_p induces an equivalence relation $\sim$ on $\mathfrak{S}_{n,p}$, namely $\pi \sim \tau$ if and only if $f_p(\pi) = f_p(\tau)$.

Fix a prime p, and let $n = pt + r$ with $0 \leqslant r < p$. A p-cycle $\sigma = (s_1, s_2, \ldots, s_p)$ in some $f_p(\pi)$ is said to be of *type A* if $s_1 = s_2 = \cdots = s_p$; of *type B* otherwise. We are interested in the size of each equivalence class of $\sim$ on $\mathfrak{S}_{n,p}$. As a matter of fact, we need the size of some collections of equivalence classes. An equivalence class may be represented as a multiset of cycles with repeated entries from $\{1,2,\ldots,t+1\}$. In fact there are three kinds of cycles in the representation of equivalence classes: p-cycles of type A, p-cycles of type B, and 1-cycles. A typical equivalence class is of the form $\{A_1,\ldots,A_i; B_1^{d_1},\ldots,B_j^{d_j}; C_1^{e_1},\ldots,C_k^{e_k}\}$, as a multiset, where A's denote p-cycles of type A, B's denote those of type B and C's are 1-cycles. Since the multiplicities $e_1,\ldots,e_k$ play a critical role, we refine the form to $\{A_1,\ldots,A_i; B_1^{d_1},\ldots,B_j^{d_j}; C_1^{e_1},\ldots,C_k^{e_k}; D_1^p,\ldots,D_\ell^p\}$ with $e_1,\ldots,e_k < p$, where A's, B's, C's are the same as before, while D's are 1-cycles. We collect all equivalence classes $\{A_1,\ldots,A_i; B_1^{d_1},\ldots,B_j^{d_j}; C_1^{e_1},\ldots,C_k^{e_k}; D_1^p,\ldots,D_\ell^p\}$ with fixed B's, C's, and a fixed set of integers appearing in either A's or D's. Let

$$\{s_1,s_2,\ldots,s_h; B_1^{d_1},\ldots,B_j^{d_j}; C_1^{e_1},\ldots,C_k^{e_k}\}$$

denote such a collection. The collection may be represented as

$$\{s_1,s_2,\ldots,s_h; E_1^{m_1},\ldots,E_\ell^{m_\ell}\},$$

where E's denote either a p-cycle of type B of multiplicity at most p or a 1-cycle with multiplicity less than p. Note that $\{s_1,\ldots,s_h\} \subset [t]$ and each $i \in [t] \setminus \{s_1,\ldots,s_h\}$ appears exactly p times in the collection and $t+1$ appears exactly r times. The distinct collections produce a partition of $\mathfrak{S}_{n,p}$, which in turn defines an equivalence relation, denoted by $\sim'$. Let $\tilde{f}_p$ denote the quotient map corresponding to this equivalence relation.

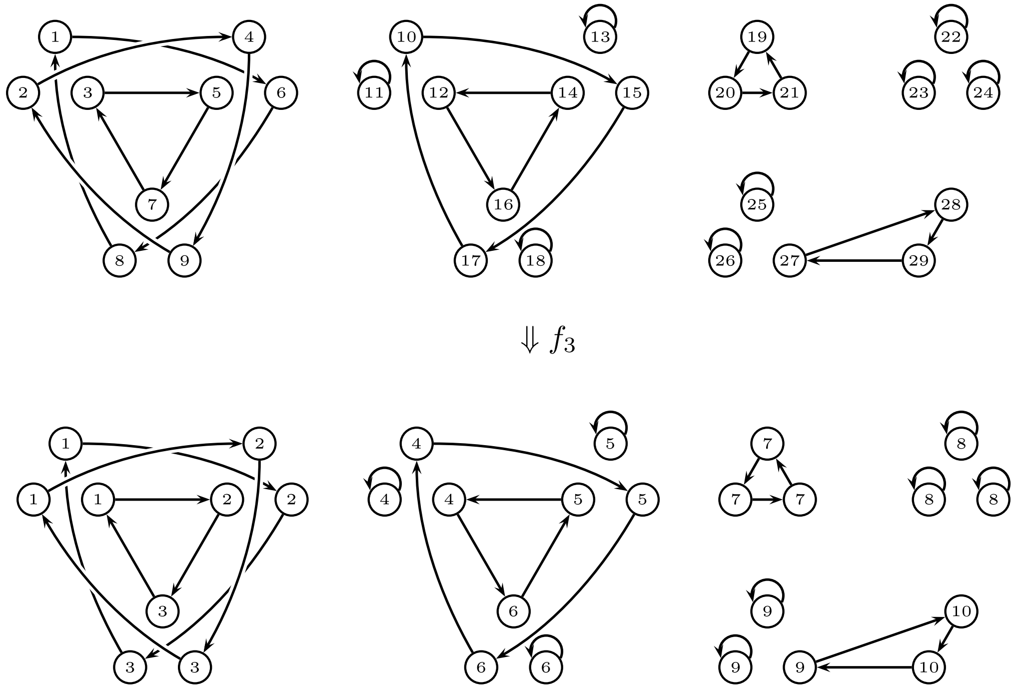

Fig. 1. Visualization of π and $f_3(\pi)$ in Example 2.1.

Example 2.1. Let $\pi \in \mathfrak{S}_{29,3}$ be the following permutation in cycle notation:

$$\pi = (1,6,8)(2,4,9)(3,5,7)(10,15,17)(11)(12,16,14)(13)(18)$$
$$(19,20,21)(22)(23)(24)(25)(26)(27,28,29).$$

Then $f_3(\pi) = \{(1,2,3)^3, (4,5,6), (4), (4,6,5), (5), (6), (7,7,7), (8)^3, (9)^2, (9,10,10)\}$. The permutation π belongs to an equivalence class

$$\{(7,7,7); (1,2,3)^3, (4,5,6), (4,6,5), (9,10,10); (4), (5), (6), (9)^2; (8)^3\}$$

of the form $\{A_1, \ldots, A_i; B_1^{d_1}, \ldots, B_j^{d_j}; C_1^{e_1}, \ldots, C_k^{e_k}; D_1^p, \ldots, D_\ell^p\}$, which is a member of the collection

$$\tilde{f}_3(\pi) = \{7, 8; (1,2,3)^3, (4,5,6), (4,6,5), (9,10,10), (4), (5), (6), (9)^2\}.$$

We visualize this example in Fig. 1, where 7 and 8 are the integers in A's or D's.

Lemma 2.2. *Let p be a prime and $n = pt + r$ with $0 \leqslant r < p$. Let $H = \{s_1, s_2, \ldots, s_h; E_1^{m_1}, \ldots, E_\ell^{m_\ell}\}$ be an equivalence class of $\mathfrak{S}_{n,p}/\sim'$ described above. Then the number of all permutations in the collection is*

$$\left|\tilde{f}_p^{-1}(H)\right| = \frac{(1+(p-1)!)^h (p!)^{t-h} r!}{m_1! m_2! \cdots m_\ell!}. \tag{3}$$

Proof. We need to enumerate the set $\tilde{f}_p^{-1}(H)$. Each permutation in the set has the special disjoint cycle decomposition prescribed by H. Recall that each s_i can represent either a p-cycle or a 1-cycle of multicity p. If s_i represents a p-cycle, it contributes a factor $(p-1)!$ to the total number of permutations to be counted; if it represents a 1-cycle with multicity p, it contributes a factor 1. So in total each s_i contributes a factor $(p-1)!+1$, which explains the factor $(1+(p-1)!)^h$ in (3).

Now recall that p is prime and E's are a p-cycle or 1-cycle. Each $j \in [t] \setminus \{s_1, \dots, s_h\}$ appears exactly p times in $E_1^{m_1}, \dots, E_\ell^{m_\ell}$, which will be replaced by p integers $p(j-1)+1, p(j-1)+2, \dots, pj$, contributing the factor $(p!)^{t-h}$ in (3); and $t+1$ appears exactly r times, which correspond to r integers $pt+1, pt+2, \dots, pt+r$, contributing a factor $r!$. This argument overcounts the set $\tilde{f}_p^{-1}(H)$, since E_i appears m_i times and the argument respects ordering of the cycles, while we are interested in unordered cycle decompositions. Moreover, since each E_i is a 1-cycle or a p-cycle of type B, there is no other repetition arising from a cyclic rotation inside a cycle in E_i's. So we need exactly the factor $\frac{1}{m_1!m_2!\cdots m_\ell!}$ in (3) to count the unordered structures. □

Now we can prove (1) combinatorially.

Theorem 2.3. *Let p be a prime and n a positive integer. Then*

$$\operatorname{ord}_p\bigl(\tau_p(n)\bigr) \geqslant \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor.$$

Proof. Note that

$$\tau_p(n) = |\mathfrak{S}_{n,p}| = \sum_H \bigl|\tilde{f}_p^{-1}(H)\bigr|,$$

where H runs through all distinct equivalence classes of $\mathfrak{S}_{n,p}/\sim'$, i.e., distinct images of $\tilde{f}_p$. Thus it suffices to show that for any equivalence class of $\mathfrak{S}_{n,p}/\sim'$, we have $\operatorname{ord}_p(|\tilde{f}_p^{-1}(H)|) \geqslant \lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor$.

Let $H = \{s_1, s_2, \dots, s_h; E_1^{m_1}, \dots, E_\ell^{m_\ell}\}$ be an equivalence class of $\mathfrak{S}_{n,p}/\sim'$. By Lemma 2.2, we have

$$\bigl|\tilde{f}_p^{-1}(H)\bigr| = \frac{(1+(p-1)!)^h (p!)^{t-h} r!}{m_1!m_2!\cdots m_\ell!}.$$

Since $(p-1)! \equiv -1 \mod p$, ord_p of the numerator is at least t. Moreover, $m_i \leqslant p$ for all i, and if $m_i = p$ then E_i is a p-cycle, which implies that there are at most $\lfloor \frac{n}{p^2} \rfloor$ m_i's with $m_i = p$. Thus we get $\operatorname{ord}_p(|\tilde{f}_p^{-1}(H)|) \geqslant \lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor$. □

3. The power of 2 in the number of involutions

For $p = 2$, $\mathfrak{S}_{n,p}$ is in fact the set of involutions in $\mathfrak{S}_n$, which will be denoted by $\mathfrak{I}_n$. Recall that t_n stands for the number of involutions in $\mathfrak{S}_n$, i.e., $|\mathfrak{I}_n|$. We will compute $\operatorname{ord}_2(t_n)$ exactly and look at β_n the odd factor of t_n, i.e.,

$$\beta_n = \frac{t_n}{2^{\operatorname{ord}_2(t_n)}}.$$

Let $n = 2t + r$ with $0 \leqslant r < 2$. Recall the equivalence relation $\sim'$ on $\mathfrak{S}_{n,2}$ in Section 2. Each equivalence class of $\mathfrak{S}_{n,2}/\sim'$ is represented by

$$H = \bigl\{s_1, s_2, \dots, s_h; E_1^{m_1}, \dots, E_\ell^{m_\ell}\bigr\},$$

where E's denote either a 2-cycle, consisting of two distinct integers, of multiplicity at most two or a 1-cycle with multiplicity one. The equivalence class may be represented by a graph $G = (\mathcal{V}, \mathcal{E})$ with vertex set

$$\mathcal{V} = \{v_1, v_2, \dots, v_t\}, \quad \text{if } n = 2t; \qquad \{v_1, v_2, \dots, v_{t+1}\}, \quad \text{if } n = 2t+1,$$

and edge set $\mathcal{E} = \{\{a, b\}\colon (a, b) = E_j, \text{ for some } j \text{ and } a \neq b\}$, regarded as a multiset, where the multiplicity of the edge corresponding to E_j is m_j. We can construct H from G if we know n.

Let $\mathfrak{G}_n$ be the set of all graphs with vertex set

$$\{v_1, v_2, \dots, v_t\}, \quad \text{if } n = 2t; \qquad \{v_1, v_2, \dots, v_{t+1}\}, \quad \text{if } n = 2t+1,$$

satisfying the following conditions:

- there is no loop,
- the degree of each vertex is at most two, and that of v_{t+1} is at most one,
- the multiplicity of each edge is at most two.

Then there is a one-to-one correspondence between the set of equivalence classes of $\mathfrak{S}_{n,2}/\sim'$ and the set $\mathfrak{G}_n$. Thus we have the induced surjection $\tilde{f}_2 : \mathfrak{I}_n \to \mathfrak{G}_n$.

Each connected component of a graph in $\mathfrak{G}_n$ is either a cycle of length at least two or a path.

The corollary below follows immediately from Lemma 2.2, since a 2-cycle is an edge with multiplicity 2 in this case.

Corollary 3.1. *Let $G \in \mathfrak{G}_n$ have s 2-cycles. Then*

$$\left|\tilde{f}_2^{-1}(G)\right| = 2^{\lfloor \frac{n}{2} \rfloor - s}.$$

The maximum number of 2-cycles in a graph $G \in \mathfrak{G}_n$ is $\lfloor \frac{n}{4} \rfloor$, which gives $\operatorname{ord}_2(t_n) \geqslant \lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{4} \rfloor$. Since there may be many such G's, we need to do more to determine $\operatorname{ord}_2(t_n)$ exactly. Let g_n denote the number of $G \in \mathfrak{G}_n$ without 2-cycles. It is easy to see that

$$g_{2n+1} = g_{2n} + n g_{2n-1}.$$

For $n \leqslant 3$, g_{2n} is just the number of simple (labeled) graphs with n vertices. Thus $g_0 = g_2 = 1$, $g_4 = 2$ and $g_6 = 8$. Using the above recurrence, we get $g_1 = 1$, $g_3 = 2$, $g_5 = 6$ and $g_7 = 26$. For more values of g_n, see Table 1.

Let $(a; b)_n$ denote the following product:

$$(a; b)_n = \prod_{i=0}^{n-1} (a + ib).$$

Note that $(1; 2)_n$ is always odd, in fact, it is the product of the first n odd integers.

Theorem 3.2. *Let $n = 4k + r$ with $0 \leqslant r < 4$. Then*

$$t_n = 2^{k + \lfloor r/2 \rfloor} \sum_{i=0}^{k} 2^i \binom{k}{i} \frac{(1; 2)_{k + \lfloor r/2 \rfloor}}{(1; 2)_{i + \lfloor r/2 \rfloor}} g_{4i+r}.$$

Proof. Since $\tilde{f}_2 : \mathfrak{I}_n \to \mathfrak{G}_n$ is a surjection, we have

$$t_n = \sum_{G \in \mathfrak{G}_n} \left|\tilde{f}_2^{-1}(G)\right|.$$

If $G \in \mathfrak{G}_n$ has i 2-cycles, then by Corollary 3.1, $|\tilde{f}_2^{-1}(G)| = 2^{\lfloor n/2 \rfloor - i}$. Since the number of such G is $\binom{\lfloor n/2 \rfloor}{2i}(1; 2)_i g_{n-4i}$, we get

$$\begin{aligned} t_n &= \sum_{i=0}^{k} 2^{\lfloor n/2 \rfloor - i} \binom{\lfloor n/2 \rfloor}{2i} (1; 2)_i g_{n-4i} \\ &= \sum_{i=0}^{k} 2^{\lfloor n/2 \rfloor - k + i} \binom{\lfloor n/2 \rfloor}{2k - 2i} (1; 2)_{k-i} g_{n-4k+4i} \end{aligned}$$

$$= \sum_{i=0}^{k} 2^{k+\lfloor r/2\rfloor+i} \binom{2k+\lfloor r/2\rfloor}{2i+\lfloor r/2\rfloor} (1;2)_{k-i} g_{4i+r}$$

$$= 2^{k+\lfloor r/2\rfloor} \sum_{i=0}^{k} 2^{i} \binom{k}{i} \frac{(1;2)_{k+\lfloor r/2\rfloor}}{(1;2)_{i+\lfloor r/2\rfloor}} g_{4i+r}. \qquad \square$$

Since $g_0 = g_1 = g_2 = 1$, $g_3 = 2$ and $g_7 = 26$, we have the following theorem, where $\delta_{r,3}$ is 1, if $r = 3$; 0, otherwise.

Theorem 3.3. *Let $n = 4k + r$ with $0 \leqslant r < 4$. Then the largest power of 2 and the odd factor β_n of t_n are the following*:

$$\mathrm{ord}_2(t_n) = k + \left\lfloor \frac{r}{2} \right\rfloor + \delta_{r,3} = \left\lfloor \frac{n}{2} \right\rfloor - 2\left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n+1}{4} \right\rfloor,$$

$$\beta_n = \sum_{i=0}^{k} 2^{i-\delta_{r,3}} \binom{k}{i} \frac{(1;2)_{k+\lfloor r/2\rfloor}}{(1;2)_{i+\lfloor r/2\rfloor}} g_{4i+r}.$$

4. Weighted sum of involutions

For $\pi \in \mathfrak{I}_n$, let $\sigma_i(\pi)$ denote the number of i-cycles in π. We define the weight of an involution π to be

$$\mathrm{wt}(\pi) = x^{\sigma_1(\pi)} y^{\sigma_2(\pi)}.$$

Consider the weight generating function

$$t_n(x, y) = \sum_{\pi \in \mathfrak{I}_n} \mathrm{wt}(\pi). \tag{4}$$

We can easily verify

$$t_n(x, y) = x \cdot t_{n-1}(x, y) + (n-1) y \cdot t_{n-2}(x, y).$$

Note that $t_n(x, -1)$ is the matchings polynomial of the complete graph with n vertices, which is equivalent to a Hermite polynomial, see [4].

We will find a formula for $t_n(x, y)$. Recall that $n = 2t + r$ with $0 \leqslant r < 2$ and the vertex set of a graph in $\mathfrak{G}_n$ is either $[t]$ or $[t + 1]$ depending on the parity of n. For $G \in \mathfrak{G}_n$, we put the weight on each edge and vertex as follows:

- For every edge e, $\mathrm{wt}(e) = y$.
- For $i \neq t + 1$,

$$\mathrm{wt}(v_i) = \begin{cases} 1, & \text{if } \deg(v_i) = 2, \\ x, & \text{if } \deg(v_i) = 1, \\ \frac{x^2+y}{2}, & \text{if } \deg(v_i) = 0. \end{cases}$$

- $$\mathrm{wt}(v_{t+1}) = \begin{cases} 1, & \text{if } \deg(v_{t+1}) = 1, \\ x, & \text{if } \deg(v_{t+1}) = 0. \end{cases}$$

The weight $\mathrm{wt}(G)$ of G is defined to be the product of weights of all vertices and edges. It is not difficult to see that $\mathrm{wt}(G)$ is the average of the weights of π with $\tilde{f}_2(\pi) = G$, i.e.,

$$\sum_{\pi \in \tilde{f}_2^{-1}(G)} \mathrm{wt}(\pi) = \left|\tilde{f}_2^{-1}(G)\right| \mathrm{wt}(G).$$

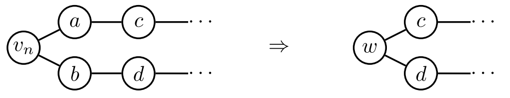

Fig. 2. Collapsing v_n, a and b to w.

Let

$$g_n(x,y)=\sum_G \mathrm{wt}(G),$$

where the sum is over all $G\in\mathfrak{G}_n$ without 2-cycles.

Using the same argument in the proof of Theorem 3.2, we have the following theorem, since a 2-cycle has two edges of weight y.

Theorem 4.1. *Let $n=4k+r$ with $0\leqslant r<4$. Then*

$$t_n(x,y)=2^{k+\lfloor r/2\rfloor}\sum_{i=0}^{k}2^i\binom{k}{i}\frac{(1;2)_{k+\lfloor r/2\rfloor}}{(1;2)_{i+\lfloor r/2\rfloor}}y^{2k-2i}g_{4i+r}(x,y).$$

We now find a recursion for $g_n(x,y)$.

Proposition 4.2. *Let $g_k(x,y)=0$ for negative integers k and $g_0(x,y)=1$. Then for each positive integer n, the following hold*:

$$g_{2n+1}(x,y)=x\cdot g_{2n}(x,y)+ny\cdot g_{2n-1}(x,y), \tag{5}$$

$$\begin{aligned}g_{2n}(x,y)={}&\frac{x^2+y}{2}g_{2n-2}(x,y)+(n-1)xy\cdot g_{2n-3}(x,y)\\&+2\binom{n-1}{2}y^2\cdot g_{2n-4}(x,y)+3\binom{n-1}{3}y^4\cdot g_{2n-8}(x,y).\end{aligned}\tag{6}$$

Proof. The first recurrence, (5), is easy. For (6), let $\mathfrak{H}_{2n}$ be the set of $G\in\mathfrak{G}_{2n}$ without 2-cycles.

We divide $\mathfrak{H}_{2n}$ into four sets as follows:

$$\mathfrak{H}_{2n}^{(0)}=\{G\in\mathfrak{H}_{2n}\colon \deg(v_n)=0\},$$
$$\mathfrak{H}_{2n}^{(1)}=\{G\in\mathfrak{H}_{2n}\colon \deg(v_n)=1\},$$
$$\mathfrak{H}_{2n}^{(2)}=\{G\in\mathfrak{H}_{2n}\colon v_n \text{ is contained in a 4-cycle}\},$$
$$\mathfrak{H}_{2n}^{(*)}=\{G\in\mathfrak{H}_{2n}\colon \deg(v_n)=2 \text{ and } v_n \text{ is not contained in a 4-cycle}\}.$$

Then it is easy to see that the weighted sums of G in $\mathfrak{H}_{2n}^{(0)}$, $\mathfrak{H}_{2n}^{(1)}$ and $\mathfrak{H}_{2n}^{(2)}$ are, respectively, the first, second and fourth terms in the right-hand side of (6).

Let G be a graph in $\mathfrak{H}_{2n}^{(*)}$ and a, b be the vertices adjacent to v_n in G. Let G' denote the graph obtained from G by collapsing the three vertices v_n, a and b to a new vertex w as shown in Fig. 2. Since v_n is not contained in a 4-cycle, there is no 2-cycle in G' and we can consider G' as a graph in $\mathfrak{H}_{2n-4}$ by relabeling vertices. Once a,b and w are fixed, for each $G'\in\mathfrak{H}_{2n-4}$, there are two graphs G_1 and G_2 in $\mathfrak{H}_{2n}^{(*)}$ which collapse to G'. For instance, if w is an isolated vertex in G', then a and b are connected to each other in G_1, and disconnected in G_2. In this case, $\mathrm{wt}(G_1)=\mathrm{wt}(G')\frac{y^3}{(x^2+y)/2}$ and $\mathrm{wt}(G_2)=\mathrm{wt}(G')\frac{y^2x^2}{(x^2+y)/2}$. If w is connected to c and d (one of them may be vacant), then a and b are connected to c and d in G_1; d and c in G_2 respectively. In this case, $\mathrm{wt}(G_1)=\mathrm{wt}(G_2)=y^2\,\mathrm{wt}(G')$.

Table 1
The values of $g_n = g_n(1,1)$ for $0 \leqslant n \leqslant 21$.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
g_n	1	1	1	2	2	6	8	26	41	145	253	978	1858	7726	15 796	69 878	152 219	711 243	1 638 323	8 039 510	99 862 594	252 998 224

Table 2
The values of $g_n(1,-1)$ for $0 \leqslant n \leqslant 21$.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$g_n(1,-1)$	1	1	0	−1	−1	1	2	−1	−6	−2	28	38	−140	−368	732	3308	−3934	−30 398	19 232	292 814	−44 946	−2 973 086

In both cases, we have $\mathrm{wt}(G_1) + \mathrm{wt}(G_2) = 2y^2\,\mathrm{wt}(G')$. Thus the sum of $\mathrm{wt}(G)$ for $G \in \mathfrak{H}_{2n}^{(*)}$ is equal to the third term in the right-hand side of (6). $\Box$

Using Proposition 4.2, we can compute $g_n(1,1)$ and $g_n(1,-1)$; see Tables 1 and 2. We will use these tables in the next section.

5. Odd and even involutions

Recall that $\sigma_2(\pi)$ is the number of 2-cycles of π. The *sign* of an involution $\pi \in \mathfrak{I}_n$ is defined as usual, i.e.,

$$\mathrm{sign}(\pi) = (-1)^{\sigma_2(\pi)}.$$

An involution is called *even* (resp. *odd*), if the sign is 1 (resp. -1). Let $\mathfrak{I}_n^e$ (resp. $\mathfrak{I}_n^o$) be the set of even (resp. odd) involutions in $\mathfrak{I}_n$, and let $t_n^e = |\mathfrak{I}_n^e|$ and $t_n^o = |\mathfrak{I}_n^o|$.

By definition of $t_n(x,y)$, we have

$$t_n(1,1) = t_n^e + t_n^o, \qquad t_n(1,-1) = t_n^e - t_n^o.$$

Using the above equations, we will find $\mathrm{ord}_2(t_n^e)$ and $\mathrm{ord}_2(t_n^o)$. To do this we need the following lemma.

Lemma 5.1. *Let k and i be positive integers. Then*

$$\mathrm{ord}_2\left(2^i\binom{k}{i}\right) \geqslant \mathrm{ord}_2(k) + i - \mathrm{ord}_2(i).$$

Especially, we have

$$\mathrm{ord}_2\left(2^i\binom{k}{i}\right) \geqslant \mathrm{ord}_2(k) + 1,$$

and if $i \geqslant 5$, then

$$\mathrm{ord}_2\left(2^i\binom{k}{i}\right) \geqslant \mathrm{ord}_2(k) + 3.$$

Proof. It follows from the identity $2^i\binom{k}{i} = 2^i \cdot \frac{k}{i}\binom{k-1}{i-1}$. $\Box$

According to Theorem 4.1, for $n = 4k + r$ with $0 \leqslant r < 4$, we have

$$t_n(1,-1) = 2^{k+\lfloor r/2\rfloor}\sum_{i=0}^{k} 2^i\binom{k}{i}\frac{(1;2)_{k+\lfloor r/2\rfloor}}{(1;2)_{i+\lfloor r/2\rfloor}}\,g_{4i+r}(1,-1).$$

Table 3
The largest power of 2 in the number of involutions, in the signed sum of involutions and in the numbers of even or odd involutions.

n	$\mathrm{ord}_2(t_n(1,1))$	$\mathrm{ord}_2(t_n(1,-1))$	$\mathrm{ord}_2(t_n^e)$	$\mathrm{ord}_2(t_n^o)$
$4k$	k	k	$k+\chi_o(k)$	unknown
$4k+1$	k	k	unknown	$k+\mathrm{ord}_2(k)+\chi_e(k)$
$4k+2$	$k+1$	$k+3+\mathrm{ord}_2(k)$	k	k
$4k+3$	$k+2$	$k+1$	k	k

Theorem 5.2. *Let $n=4k+r$ with $0\leqslant r<4$. Then*

$$\mathrm{ord}_2\big(t_n(1,-1)\big)=\begin{cases} k+\lfloor \frac{r}{2}\rfloor, & \text{if } r\neq 2,\\ k+3+\mathrm{ord}_2(k), & \text{if } r=2.\end{cases}$$

Proof. By Table 2, we have $g_0(1,-1)=g_1(1,-1)=1, g_2(1,-1)=0$ and $g_3(1,-1)=-1$. Thus, if $r\neq 2$ then $\mathrm{ord}_2(t_n(1,-1))=\lfloor\frac{n}{2}\rfloor-\lfloor\frac{n}{4}\rfloor$.

If $r=2$, then $t_n(1,-1)=2^{k+1}\sum_{i=0}^k a_i$ where $a_i=2^i\binom{k}{i}\frac{(1;2)_{k+1}}{(1;2)_{i+1}}g_{4i+2}(1,-1)$. Since $g_2(1,-1)=0$ and $g_6(1,-1)=2$, we have $a_0=0$ and $\mathrm{ord}_2(a_1)=\mathrm{ord}_2(k)+2$. For $i\geqslant 2$, using Table 2 and Lemma 5.1 we get $\mathrm{ord}_2(a_i)\geqslant \mathrm{ord}_2(k)+3$. Thus $\mathrm{ord}_2(t_{4k+2}(1,-1))=k+3+\mathrm{ord}_2(k)$. $\square$

Now we can make a table of $\mathrm{ord}_2(t_n(1,1))$ and $\mathrm{ord}_2(t_n(1,-1))$; see Table 3.

Since $t_n^e=\frac{1}{2}(t_n(1,1)+t_n(1,-1))$ and $t_n^o=\frac{1}{2}(t_n(1,1)-t_n(1,-1))$, we get the following corollary.

Corollary 5.3. *Let k be a nonnegative integer. Then*

$$\mathrm{ord}_2\big(t_{4k+2}^e\big)=\mathrm{ord}_2\big(t_{4k+2}^o\big)=\mathrm{ord}_2\big(t_{4k+3}^e\big)=\mathrm{ord}_2\big(t_{4k+3}^o\big)=k.$$

We find $\mathrm{ord}_2(t_{4k}^e)$ and $\mathrm{ord}_2(t_{4k+1}^o)$ in the following two theorems separately. Let $\chi_o(n)$ (resp. $\chi_e(n)$) denote 1 if n is odd (resp. even), and 0 otherwise.

Theorem 5.4. *Let k be a nonnegative integer. Then*

$$\mathrm{ord}_2\big(t_{4k}^e\big)=2\left\lfloor\frac{k+1}{2}\right\rfloor=k+\chi_o(k).$$

Proof. We have $t_{4k}^e=2^k\sum_{i=0}^k a_i$, where

$$a_i=2^{i-1}\binom{k}{i}\frac{(1;2)_k}{(1;2)_i}\big(g_{4i}(1,1)+g_{4i}(1,-1)\big).$$

Using Tables 1 and 2, we have

$$g_0(1,1)+g_0(1,-1)=1+1=2,$$
$$g_4(1,1)+g_4(1,-1)=2-1=1,$$
$$g_8(1,1)+g_8(1,-1)=41-6\equiv 3 \mod 4.$$

Thus

$$a_0=(1;2)_k,\qquad a_1=k(1;2)_k,\qquad a_2=k(k-1)\frac{(1;2)_k}{3}\cdot(4q+3),$$

and

$$3(a_0+a_1+a_2) = (1;2)_k\big(3+3k+(4q+3)\big(k^2-k\big)\big)$$
$$\equiv (1;2)_k \cdot 3\big(k^2+1\big) \mod 4.$$

Thus $\operatorname{ord}_2(a_0+a_1+a_2) = \chi_o(k)$. Since $\operatorname{ord}_2(a_i) \geqslant 2$ for $i \geqslant 3$, we finish the proof. $\square$

Theorem 5.5. *Let k be a nonnegative integer. Then*

$$\operatorname{ord}_2\big(t^o_{4k+1}\big) = k + \operatorname{ord}_2(k) + \chi_e(k).$$

Proof. We have $t^o_{4k+1} = 2^k \sum_{i=0}^k a_i$, where

$$a_i = 2^{i-1}\binom{k}{i}\frac{(1;2)_k}{(1;2)_i}\big(g_{4i+1}(1,1) - g_{4i+1}(1,-1)\big).$$

Using Tables 1 and 2, we have

$$g_1(1,1) - g_1(1,-1) = 1-1 = 0,$$
$$g_5(1,1) - g_5(1,-1) = 6-1 = 5,$$
$$g_9(1,1) - g_9(1,-1) = 145+2 \equiv 3 \mod 4,$$
$$g_{17}(1,1) - g_{17}(1,-1) = 711\,243 + 30\,398 \equiv 1 \mod 2.$$

Thus we can write $a_0 = 0$, $a_1 = (1;2)_k \cdot 5k$, $a_2 = (1;2)_k\binom{k}{2}\frac{2\cdot(4q_1+3)}{3}$, $a_3 = (1;2)_k\binom{k}{3}\frac{2^2\cdot q_2}{5\cdot 3}$ and $a_4 = (1;2)_k\binom{k}{4}\frac{2^3\cdot(2q_3+1)}{7\cdot 5\cdot 3}$ for some integers q_1, q_2 and q_3.

Note that by Lemma 5.1 we have $\operatorname{ord}_2(a_i) \geqslant \operatorname{ord}_2(k)+3$ for $i \geqslant 5$. Thus, if k is odd, then we have $\operatorname{ord}_2(t^o_{4k+1}) = k$.

Now assume that k is even. Then

$$\operatorname{ord}_2(a_0+a_1+a_2) = \operatorname{ord}_2\big(k\big(15+(k-1)(4q_1+3)\big)\big),$$
$$\operatorname{ord}_2(a_3) \geqslant \operatorname{ord}_2(k) + \operatorname{ord}_2(k-2) + 1 \geqslant \operatorname{ord}_2(k)+2,$$
$$\operatorname{ord}_2(a_4) = \operatorname{ord}_2(k) + \operatorname{ord}_2(k-2).$$

If $k=4m$, then $\operatorname{ord}_2(a_4) = \operatorname{ord}_2(k)+1$ and, $\operatorname{ord}_2(a_0+a_1+a_2) \geqslant \operatorname{ord}_2(k)+2$. If $k = 4m+2$, then $\operatorname{ord}_2(a_4) \geqslant \operatorname{ord}_2(k)+2$, and $\operatorname{ord}_2(a_0+a_1+a_2) = \operatorname{ord}_2(k)+1$. Thus, if k is even, then we always have $\operatorname{ord}_2(a_0+\cdots+a_4) = \operatorname{ord}_2(k)+1$.

In all cases we have $\operatorname{ord}_2(t^o_{4k+1}) = k + \chi_e(k)(\operatorname{ord}_2(k)+1) = k + \operatorname{ord}_2(k) + \chi_e(k)$. $\square$

Now we can fill all the entries in Table 3 except $\operatorname{ord}_2(t^e_{4k+1})$ and $\operatorname{ord}_2(t^o_{4k})$. Based on Maple experiments, we conjecture the following.

Conjecture 5.6. *There is a 2-adic integer $\rho = \sum_{i\geqslant 0}\rho_i 2^i$, with $0 \leqslant \rho_i \leqslant 1$, satisfying*

$$\operatorname{ord}_2\big(t^e_{4k+1}\big) = k + \chi_o(k)\cdot\big(\operatorname{ord}_2(k+\rho)+1\big).$$

For example, $\rho = 1+2+2^3+2^8+2^{10}+\cdots$ satisfies the condition for all $k \leqslant 1000$.

6. The smallest period of β_n mod 2^s

Chowla et al. [2] proved that, if m is odd, then $t_{n+m} \equiv t_n \mod m$. We give their proof here for self containment.

Theorem 6.1. *(See [2].) If m is odd, then*

$$t_{n+m} \equiv t_n \mod m.$$

Proof. Induction on $n \geqslant 0$. We have

$$t_m = \sum_{2i+j=m} \frac{m!}{2^i i! j!} = \sum_{2i+j=m} \frac{m!}{2^i (i+j)!} \binom{i+j}{j} \equiv 1 \mod m,$$

because $\frac{m!}{2^i(i+j)!}\binom{i+j}{j}$ is divisible by m if $i > 0$; and 1 if $i = 0$. Thus $t_{m+1} = t_m + mt_{m-1} \equiv 1 \bmod m$. We get $t_{n+m} \equiv t_n \bmod m$ for $n = 0, 1$. Suppose it holds for $n = 0, 1, \ldots, k$. Then it is true for $n = k+1$ because

$$\begin{aligned} t_{k+1+m} &= t_{k+m} + (k+m)t_{k+m-1} \\ &\equiv t_k + kt_{k-1} \bmod m \\ &= t_{k+1}. \qquad \square \end{aligned}$$

The above theorem means that the sequence $\{t_n \bmod m\}_{n\geqslant 0}$ has a period m. In fact, m is the smallest period.

Theorem 6.2. *Let m be an odd integer. Then m is the smallest period of the sequence $\{t_n \bmod m\}_{n\geqslant 0}$.*

Proof. Let d be the smallest period. Then $t_d \equiv t_0 \equiv 1 \bmod m$, $t_{d+1} \equiv t_1 \equiv 1 \bmod m$, and $t_{d+2} \equiv t_2 \equiv 2 \bmod m$. On the other hand, we have $t_{d+2} = t_{d+1} + (d+1)t_d \equiv d+2 \bmod m$. Thus m divides d, and we get $m = d$. $\square$

If m is even, then $\{t_n \bmod m\}_{n\geqslant 0}$ does not have a period because $t_0 = 1$ but t_n is even for all $n \geqslant 2$. However, there exists an integer N such that $\{t_n \bmod m\}_{n\geqslant N}$ has a period.

Theorem 6.3. *Let ℓ be an odd integer and k be a positive integer. Let $m = 2^k\ell$ and let N be the smallest integer such that $\{t_n \bmod m\}_{n\geqslant N}$ has a period. Then $N = 4k-2$ and ℓ is the smallest period of $\{t_n \bmod m\}_{n\geqslant N}$.*

Proof. By Theorem 3.3, we have $\mathrm{ord}_2(t_{4k-3}) = k-1$ and $\mathrm{ord}_2(t_n) \geqslant k$ for $n \geqslant 4k-2$. Thus $t_{4k-3+y} \not\equiv t_{4k-3} \bmod 2^k$ for any positive integer y, which implies $N \geqslant 4k-2$. On the other hand, we have $t_{n+\ell} \equiv t_n \bmod 2^k$ for $n \geqslant 4k-2$. Since $t_{n+\ell} \equiv t_n \bmod \ell$ by Theorem 6.1, we get $t_{n+\ell} \equiv t_n \bmod m$ for $n \geqslant 4k-2$. Thus $\{t_n \bmod m\}_{n\geqslant 4k-2}$ has a period ℓ and we get $N = 4k-2$.

It remains to show that ℓ is the smallest period. It is easy to see that any period of $\{t_n \bmod m\}_{n\geqslant N}$ is divisible by the smallest period of $\{t_n \bmod \ell\}_{n\geqslant 0}$, which is ℓ. Thus we get the theorem. $\square$

Recall that β_n is the odd factor of t_n. Similarly we can find the smallest period of $\{\beta_n \bmod 2^s\}_{n\geqslant 0}$. Let $h(n) = \mathrm{ord}_2(t_n) = \lfloor \frac{n}{2} \rfloor - 2\lfloor \frac{n}{4} \rfloor + \lfloor \frac{n+1}{4} \rfloor$. Then $t_n = 2^{h(n)}\beta_n$. Thus we have

$$\beta_{n+1} = 2^{h(n)-h(n+1)}\beta_n + 2^{h(n-1)-h(n+1)}n\beta_{n-1},$$

which is equivalent to the following: if $n = 4k+r$ with $0 \leqslant r \leqslant 3$ then

$$\beta_{n+1} = 2^{h(r)-h(r+1)}\beta_n + 2^{h(r-1)-h(r+1)}n\beta_{n-1}. \tag{7}$$

To find the smallest period of $\{\beta_n \bmod 2^s\}_{n\geqslant 0}$, we need the following two lemmas.

Lemma 6.4. *Let $s \geqslant 3$ be an integer. Then*

$$(1;2)_{2^{s-1}} \equiv 1 \mod 2^s.$$

Proof. Induction on s. It is true for $s=3$. Assume it is true for $s \geqslant 3$. Then $(1;2)_{2^{s-1}} = 2^s k + 1$ for some integer k. Then it holds for $s+1$ because

$$\begin{aligned}(1;2)_{2^s} &= 1\cdot 3\cdot 5\cdots\left(2^{s+1}-1\right)\\ &= \left(1\cdot 3\cdot 5\cdots\left(2^s-1\right)\right)\cdot\left(\left(2^{s+1}-1\right)\left(2^{s+1}-3\right)\cdots\left(2^{s+1}-\left(2^s-1\right)\right)\right)\\ &\equiv (1;2)_{2^{s-1}}\cdot(-1)^{2^{s-1}}(1;2)_{2^{s-1}} \bmod 2^{s+1}\\ &= 2^{2s}k^2+2^{s+1}k+1\\ &\equiv 1 \mod 2^{s+1}. \qquad \square\end{aligned}$$

Lemma 6.5. *If $s \geqslant 3$ then*

$$\beta_{n+2^{s+1}} \equiv \beta_n \mod 2^s.$$

Proof. We use induction on n. First we will show that $\beta_{2^{s+1}+n} \equiv 1 \bmod 2^s$ for $n = 0, 1$. By Theorem 3.3,

$$\beta_{2^{s+1}+n} = \sum_{i=0}^{2^{s-1}} 2^i \binom{2^{s-1}}{i} \frac{(1;2)_{2^{s-1}+\lfloor n/2\rfloor}}{(1;2)_{i+\lfloor n/2\rfloor}} \cdot \frac{g_{4i+n}}{2^{\delta_{n,3}}} = \sum_{i=0}^{2^{s-1}} 2^i \binom{2^{s-1}}{i} \frac{(1;2)_{2^{s-1}}}{(1;2)_i} g_{4i+n}.$$

By Lemmas 5.1 and 6.4, we get $\beta_{2^{s+1}+n} \equiv (1;2)_{2^{s-1}} \equiv 1 \bmod 2^s$.

We have shown that the theorem is true for $n = 0, 1$. Assume $n \geqslant 1$ and the theorem is true for all nonnegative integers less than $n+1$. Then it is also true for $n+1$ because if $n = 4k + r$ for $0 \leqslant r \leqslant 3$ then by (7) we get

$$\begin{aligned}\beta_{n+1+2^{s+1}} &= 2^{h(r)-h(r+1)}\beta_{n+2^{s+1}} + 2^{h(r-1)-h(r+1)}\left(n+2^{s+1}\right)\beta_{n-1+2^{s+1}}\\ &\equiv 2^{h(r)-h(r+1)}\beta_n + 2^{h(r-1)-h(r+1)} n\beta_{n-1} \bmod 2^s\\ &= \beta_{n+1}. \qquad \square\end{aligned}$$

Now we have the following theorem.

Theorem 6.6. *If $s \geqslant 3$ then 2^{s+1} is the smallest period of the sequence $\{\beta_n \bmod 2^s\}_{n\geqslant 0}$.*

Proof. By Lemma 6.5, 2^{s+1} is a period. Since the smallest period divides every period, it has to be 2^k for some k. It is sufficient to show that 2^s is not a period.

Assume that 2^s is a period. By the recurrence relation (7), we have

$$\beta_{2^s+2} = \frac{1}{2}\beta_{2^s+1} + \frac{2^s+1}{2}\beta_{2^s}, \qquad \beta_{2^s+1} = \beta_{2^s} + 2^s \cdot 2\beta_{2^s-1}.$$

Thus

$$\beta_{2^s+2} = \left(1+2^{s-1}\right)\beta_{2^s} + 2^s\beta_{2^s-1}.$$

Since 2^s is a period, $\beta_{2^s} \equiv \beta_0 = 1 \bmod 2^s$. Then we have $\beta_{2^s+2} \equiv 1 + 2^{s-1} \bmod 2^s$, which is a contradiction to $\beta_{2^s+2} \equiv \beta_2 = 1 \bmod 2^s$. $\square$

Acknowledgments

We would like to thank Professor Christian Krattenthaler for informing us of the Ochiai's paper. We also thank the anonymous referees for their careful reading and helpful comments.

References

[1] Ronald Alter, K.K. Kubota, Prime and prime power divisibility of Catalan numbers, J. Combin. Theory Ser. A 15 (1973) 243–256.

[2] S. Chowla, I.N. Herstein, W.K. Moore, On recursions connected with symmetric groups, I, Canad. J. Math. 3 (1951) 328–334.

[3] Emeric Deutsch, Bruce E. Sagan, Congruences for Catalan and Motzkin numbers and related sequences, J. Number Theory 117 (1) (2006) 191–215.

[4] C.D. Godsil, Algebraic Combinatorics, Chapman and Hall Math. Ser., Chapman & Hall, New York, 1993.

[5] P. Goetgheluck, Notes: Computing binomial coefficients, Amer. Math. Monthly 94 (4) (1987) 360–365.

[6] Michael Grady, Morris Newman, Residue periodicity in subgroup counting functions, in: Contemp. Math., vol. 166, Amer. Math. Soc., Providence, RI, 1994, pp. 265–273.

[7] Hideki Ishihara, Hiroyuki Ochiai, Yugen Takegahara, Tomoyuki Yoshida, p-Divisibility of the number of solutions of $x^p = 1$ in a symmetric group, Ann. Comb. 5 (2) (2001) 197–210.

[8] Donald E. Knuth, Herbert S. Wilf, The power of a prime that divides a generalized binomial coefficient, J. Reine Angew. Math. 396 (1989) 212–219.

[9] Matjaž Konvalinka, Divisibility of generalized Catalan numbers, J. Combin. Theory Ser. A 114 (6) (2007) 1089–1100.

[10] Hiroyuki Ochiai, A p-adic property of the Taylor series of $\exp(x + x^p/p)$, Hokkaido Math. J. 28 (1) (1999) 71–85.

[11] Alexander Postnikov, Bruce E. Sagan, What power of two divides a weighted Catalan number? J. Combin. Theory Ser. A 114 (5) (2007) 970–977.