2-adic properties for the numbers of involutions in the alternating groups

著者	KODA Tatsuhiko, SATO Masaki, TAKEGAHARA Yugen
journal or publication title	Journal of Algebra and Its Applications
volume	14
number	4
page range	1550052
year	2015-05
URL	http://hdl.handle.net/10258/00008883

doi: info:doi/10.1142/S0219498815500528

2-adic properties for the numbers of involutions in the alternating groups

著者	KODA Tatsuhiko, SATO Masaki, TAKEGAHARA Yugen
journal or publication title	Journal of Algebra and Its Applications
volume	14
number	4
page range	1550052
year	2015-05
URL	http://hdl.handle.net/10258/00008883

doi: info:doi/10.1142/S0219498815500528

2-adic properties for the numbers of involutions in the alternating groups.

Tatsuhiko Koda, Masaki Sato, and Yugen Takegahara*

Muroran Institute of Technology, 27-1 Mizumoto, Muroran 050-8585, Japan

September 23, 2014

Abstract

We study the 2-adic properties for the numbers of involutions in the alternative groups, and give an affirmative answer to a conjecture of D. Kim and J. S. Kim [14]. Some analogous and general results are also presented.

1 Introduction

Let S_n be the symmetric group of degree n, and let A_n be the alternating group of degree n. Let ϵ be the identity of a group. Given a positive integer m, we denote by $a_n(m)$ the number of permutations $\sigma \in S_n$ such that $\sigma^m = \epsilon$. Let p be a prime. By definition and Wilson's theorem, $a_p(p) = 1 + (p-1)! \equiv 0 \pmod{p}$. Moreover, $a_n(m) \equiv 0 \pmod{\gcd(m, n!)}$ by a theorem of Frobenius (see, *e.g.*, [10]).

Let u be a positive integer. There exist remarkable p-adic properties of $a_n(p^u)$ (cf. Theorems 4.2–4.4). The beginning of them is due to H. Ochiai [16] and K. Conrad [4]. For each integer a, $\mathrm{ord}_p(a)$ denotes the exponent of p in the decomposition of a into prime factors. As a pioneer work, the formula

$$\mathrm{ord}_p(a_n(p)) \geq \left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]$$

(cf. Corollary 4.5) was given in [6, 7, 9], which was also shown by various methods (cf. [4, 11, 13, 14]); moreover, the equality holds for all n such that $n - [n/p^2]p^2 \leq p - 1$ (see, *e.g.*, [6, 11, 13]). When $p = 2$, this formula was found by S. Chowla, I. N.

*This work was supported by JSPS KAKENHI Grant number 22540004
*E-mail: yugen@mmm.muroran-it.ac.jp
2000 *Mathematics Subject Classification.* Primary 05A15; Secondary 11S80, 20B30, 20E22.
Keyword. symmetric group, alternating group, Artin-Hasse exponential, p-adic analytic function, wreath product.

Herstein, and W. K. Moore [2]. The precise formula for $\mathrm{ord}_2(a_n(2))$ is known as

$$\mathrm{ord}_2(a_n(2)) = \begin{cases} \left[\dfrac{n}{2}\right] - \left[\dfrac{n}{4}\right] + 1 & \text{if } n \equiv 3 \pmod 4, \\ \left[\dfrac{n}{2}\right] - \left[\dfrac{n}{4}\right] & \text{otherwise} \end{cases}$$

(cf. Example 4.6). The value of $\mathrm{ord}_2(a_n(4))$ is also determined (cf. Proposition 4.7).

We denote by $t_n(m)$ the number of even permutations $\sigma \in A_n$ such that $\sigma^m = \epsilon$. Recently, D. Kim and J. S. Kim [14] proved that for any nonnegative integer y,

$$\mathrm{ord}_2(t_{4y}(2)) = y + \chi_o(y),\ \mathrm{ord}_2(t_{4y+2}(2)) = \mathrm{ord}_2(t_{4y+3}(2)) = y,$$

where $\chi_o(y) = 1$ if y is odd, and $\chi_o(y) = 0$ if y is even. They also conjectured that for any nonnegative integer y, there exists a 2-adic integer α satisfying

$$\mathrm{ord}_2(t_{4y+1}(2)) = y + \chi_o(y) \cdot (\mathrm{ord}_2(y + \alpha) + 1)$$

(see [14, Conjecture 5.6]). According to [14], $\alpha = 1 + 2 + 2^3 + 2^8 + 2^{10} + \cdots$ satisfies the condition for all $y \leq 1000$. In this paper, we solve affirmatively their conjecture (cf. Theorem 5.1), and present some analogous and general results, including the result for $\mathrm{ord}_2(t_n(4))$ (cf. Theorems 5.4). We adapt K. Conrad's methods presented in [4] to the case of $t_n(2^u)$.

Sections 2–5 are devoted to the study of $\mathrm{ord}_p(a_n(p^u))$ and $\mathrm{ord}_2(t_n(2^u))$. In addition to the above results, we also show that, if $r = 0$ or $r = 1$, then there exists a 2-adic integer α_r such that

$$\mathrm{ord}_2(t_{2^{u+1}y+r}(2^u)) = (2^{u+1} - u - 2)y + \chi_o(y) \cdot (\mathrm{ord}_2(y + \alpha_r) + u)$$

for any nonnegative integer y (cf. Theorem 5.6).

Let $C_p \wr S_n$ be the wreath product of C_p by S_n, where C_p is a cyclic group of order p, and let $C_2 \wr A_n$ be the wreath product of C_2 by A_n. We are also interested in the number of elements x of these wreath products such that $x^m = \epsilon$. Let $b_n(p^u)$ be the number of elements x of $C_p \wr S_n$ such that $x^{p^u} = \epsilon$, and let $q_n(2^u)$ be the number of elements x of $C_2 \wr A_n$ such that $x^{2^u} = \epsilon$. In Sections 6–8, we focus on the p-adic properties of $b_n(p^u)$ and the 2-adic properties of $q_n(2^u)$. When $u = 1$, we are successful in finding the fact that

$$\mathrm{ord}_p(b_n(p)) = n - \left[\frac{n}{p}\right] \quad \text{and} \quad \mathrm{ord}_2(q_n(2)) = \left[\frac{n+1}{2}\right] + \chi_o\left(\left[\frac{n}{2}\right]\right)$$

(cf. Examples 7.4 and 8.2). The former fact with $p = 2$ is due to T. Yoshida [20]. The results for $\mathrm{ord}_p(b_n(p^u))$ and $\mathrm{ord}_2(q_n(2^u))$ with $u \geq 2$ are similar to those for $\mathrm{ord}_p(a_n(p^{u-1}))$ and $\mathrm{ord}_2(t_n(2^{u-1}))$, while there are slight differences between the proofs (cf. Example 7.5, Proposition 7.6, Theorems 8.3, 8.5, and 8.7).

2 Generating functions

For each $\sigma \in S_n$, $\sigma^{p^u} = \epsilon$ if and only if the cycle type of σ is of the form

$$(1^{j_0}, p^{j_1}, \ldots, (p^u)^{j_u}),$$

where $j_0, j_1, \ldots, j_u$ are nonnegative integers satisfying $\sum_k j_k p^k = n$. Since the number of such a permutations is $n!/\prod_{k=0}^{u} p^{kj_k} j_k!$ (see, *e.g.*, [12, Lemma 1.2.15] or [18, Chap. 4 §2]), it follows that

$$a_n(p^u) = \sum_{j_0+j_1p+\cdots+j_up^u=n} \frac{n!}{\prod_{k=0}^{u} p^{kj_k} j_k!}. \tag{1}$$

Set $a_n^0(p^u) = a_n(p^u)$, and define

$$a_n^1(p^u) = \sum_{j_0+j_1p+\cdots+j_up^u=n} \frac{(-1)^{j_0+j_1+\cdots+j_u} n!}{\prod_{k=0}^{u} p^{kj_k} j_k!}. \tag{2}$$

Then we have

$$t_n(p^u) = \frac{a_n^0(p^u) + (-1)^n a_n^1(p^u)}{2}. \tag{3}$$

(Obviously, $a_n(p^u) = t_n(p^u)$ if $p \neq 2$.) Let $\natural$ denotes both 0 and 1. We always assume that $a_0^\natural(p^u) = 1$. By Eqs. (1)–(3), we have

$$\sum_{n=0}^{\infty} \frac{a_n^\natural(p^u)}{n!} X^n = \exp\left((-1)^\natural \sum_{k=0}^{u} \frac{1}{p^k} X^{p^k}\right) \tag{4}$$

and

$$\sum_{n=0}^{\infty} \frac{t_n(2^u)}{n!} X^n = \frac{1}{2} \exp\left(\sum_{k=0}^{u} \frac{1}{2^k} X^{2^k}\right) + \frac{1}{2} \exp\left(X - \sum_{k=1}^{u} \frac{1}{2^k} X^{2^k}\right)$$

(see also [3] and [18, Chap. 4, Problem 22]). Let $\{c_n^\natural\}_{n=0}^{\infty}$ be a sequence given by

$$\sum_{n=0}^{\infty} c_n^\natural X^n = \exp\left((-1)^\natural \sum_{k=0}^{\infty} \frac{1}{p^k} X^{p^k}\right). \tag{5}$$

Then by [5, Proposition 1] (see also [15, p. 97, Exercise 18]), $c_n^\natural \in \mathbb{Z}_p \cap \mathbb{Q}$, where $\mathbb{Z}_p$ is the ring of p-adic integers. When $\natural = 0$, this formal power series is called the Artin-Hasse exponential (cf. [5], [15, Chap. IV §2], [19, §48]). We write $c_n = c_n^0$ for the sake of simplicity. By definition, $c_r = a_r(p^u)/r!$ for any nonnegative integer r less than p^{u+1}. According to Mathematica, we have the following lemma.

Lemma 2.1 *If $p = 2$, then the values of $c_r^\natural$ for integers r with $0 \le r \le 17$ are as follows :*

r	0	1	2	3	4	5	6	7	8	9	10	11
c_r^0	1	1	1	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{7}{15}$	$\frac{16}{45}$	$\frac{67}{315}$	$\frac{88}{315}$	$\frac{617}{2835}$	$\frac{2626}{14175}$	$\frac{18176}{155925}$
c_r^1	1	-1	0	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{5}$	$\frac{1}{45}$	$-\frac{5}{63}$	$-\frac{8}{105}$	$\frac{43}{405}$	$-\frac{74}{14175}$	$-\frac{559}{17325}$

r	12	13	14	15	16	17
c_r^0	$\frac{6949}{66825}$	$\frac{423271}{6081075}$	$\frac{2172172}{42567525}$	$\frac{19151162}{638512875}$	$\frac{58438907}{638512875}$	$\frac{899510224}{10854718875}$
c_r^1	$\frac{697}{18711}$	$-\frac{13232}{552825}$	$-\frac{30727}{14189175}$	$\frac{450991}{49116375}$	$-\frac{5519014}{91216125}$	$\frac{8250311}{144729585}$

For any nonnegative integer r less than p^{u+1}, we set

$$H_{u,r}^\natural(X) = \sum_{y=0}^{\infty} \frac{a_{p^{u+1}y+r}^\natural(p^u)}{(p^{u+1}y+r)!}(-(-1)^\natural p^{u+1})^y X^y,$$

and define a sequence $\{d_{n,r}^\natural\}_{n=0}^{\infty}$ by

$$\sum_{n=0}^{\infty} d_{n,r}^\natural X^n = \left(\sum_{j=0}^{\infty} c_{p^{u+1}j+r}^\natural(-(-1)^\natural p^{u+1})^j X^j\right) \exp\left(\sum_{i=1}^{\infty} \frac{\varepsilon^\natural p^{p^i(u+1)}}{p^{u+i+1}} X^{p^i}\right),$$

where $\varepsilon^\natural = -1$ if $p = 2$ and $\natural = 0$, and $\varepsilon^\natural = +1$ otherwise.

Lemma 2.2 *Let r be a nonnegative integer less than p^{u+1}. Then*

$$H_{u,r}^\natural(X) = \exp(X) \sum_{n=0}^{\infty} d_{n,r}^\natural X^n.$$

Proof. Using Eqs. (4) and (5), we have

$$\sum_{n=0}^{\infty} \frac{a_n^\natural(p^u)}{n!} X^n = \left(\sum_{n=0}^{\infty} c_n^\natural X^n\right) \exp\left(-(-1)^\natural \sum_{k=u+1}^{\infty} \frac{1}{p^k} X^{p^k}\right).$$

This formula yields

$$\sum_{y=0}^{\infty} \frac{a_{p^{u+1}y+r}^\natural(p^u)}{(p^{u+1}y+r)!} X^{p^{u+1}y+r} = \left(\sum_{j=0}^{\infty} c_{p^{u+1}j+r}^\natural X^{p^{u+1}j+r}\right)$$
$$\times \exp\left(-(-1)^\natural \sum_{i=0}^{\infty} \frac{1}{p^{u+i+1}} X^{p^{u+i+1}}\right).$$

Omit X^r and substitute $(-(-1)^\natural p^{u+1})X$ for $X^{p^{u+1}}$. Then we have

$$\sum_{y=0}^{\infty} \frac{a^\natural_{p^{u+1}y+r}(p^u)}{(p^{u+1}y+r)!}(-(-1)^\natural p^{u+1})^y X^y = \left(\sum_{j=0}^{\infty} c^\natural_{p^{u+1}j+r}(-(-1)^\natural p^{u+1})^j X^j\right) \times \exp\left(-(-1)^\natural \sum_{i=0}^{\infty} \frac{(-(-1)^\natural p^{u+1})^{p^i}}{p^{u+i+1}} X^{p^i}\right).$$

This completes the proof. □

Remark 2.3 In [4], Conrad has given the equation in Lemma 2.2 with $\natural = 0$.

3 Fundamental facts

In this section, we provide four fundamental facts for the study of $\mathrm{ord}_p(a^\natural_n(p^u))$ and $\mathrm{ord}_p(t_n(p^u))$. The next lemma is well-known (cf. [8, Problems 164 and 165], [15, p. 7, Exercise 14], [19, Lemma 25.5]).

Lemma 3.1 *Suppose that $n = n_0 + n_1p + n_2p^2 + \cdots \neq 0$, where n_i, $i = 0, 1, \ldots$, are nonnegative integers less than p. Then*

$$\mathrm{ord}_p(n!) = \sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right] = \frac{n - n_0 - n_1 - n_2 - \cdots}{p-1} \leq \frac{n-1}{p-1}.$$

For each non-zero p-adic integer $x = \sum_{i=0}^{\infty} x_i p^i$ with $0 \leq x_i \leq p-1$, we denote by $\mathrm{ord}_p(x)$ the first index i such that $x_i \neq 0$. The p-adic absolute vale of a p-adic integer x is given by

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p(x)} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

We define a subring $\mathbb{Z}_p\langle X\rangle$ of $\mathbb{Z}_p[[X]]$ by

$$\mathbb{Z}_p\langle X\rangle = \left\{ \sum_{n=0}^{\infty} m_n X^n \in \mathbb{Z}_p[[X]] \;\middle|\; \lim_{n\to\infty} |m_n|_p = 0 \right\}.$$

For each $g(X) = \sum_{n=0}^{\infty} g_n X^n \in \mathbb{Z}_p[[X]]$, $g(X) + p^{k_1}X^{k_2}\mathbb{Z}_p\langle X\rangle$ denotes the set of all formal power series $f(X) = \sum_{n=0}^{\infty} f_n X^n$ such that $f(X) - g(X) \in p^{k_1}X^{k_2}\mathbb{Z}_p\langle X\rangle$, where k_1 and k_2 are nonnegative integers.

Lemma 3.2 *Let k be a positive integer, and let a be a p-adic integer such that $\mathrm{ord}_p(a) = k$. Excepting the case where $p = 2$ and $k = 1$,*

$$\exp(aX) \in 1 + aX + \frac{a^2}{2}X^2 + \frac{a^3}{6}X^3 + p^{2k+1}X^4\mathbb{Z}_p\langle X\rangle.$$

Proof. Observe that

$$\exp(aX) - 1 - aX - \frac{a^2}{2} X^2 - \frac{a^3}{6} X^3 = p^{2k} X^3 \sum_{n=1}^{\infty} p^{-2k} \frac{a^{n+3}}{(n+3)!} X^n.$$

Then it follows from Lemma 3.1 that

$$\mathrm{ord}_p \left(p^{-2k} \frac{a^{n+3}}{(n+3)!} \right) \geq k(n+1) - \frac{n+2}{p-1} = \left(k - \frac{1}{p-1} \right) n + \left(k - \frac{2}{p-1} \right).$$

This completes the proof. □

The next lemma is essentially due to K. Conrad [4] (see also [19, Theorem 54.4]).

Lemma 3.3 *Let $\sum_{n=0}^{\ell} m_n X^n$ be a polynomial of degree ℓ with coefficients in $\mathbb{Z}_p$, and let $\sum_{n=1}^{\infty} w_n X^n \in p^k X \mathbb{Z}_p\langle X \rangle$, k a nonnegative integer. Define a sequence $\{d_n\}_{n=0}^{\infty}$ by $d_0 = m_0$ and $d_n = m_n + w_n$ for $n = 1, 2, \ldots$. Then there exists a p-adic analytic function $g(X) \in \mathbb{Z}_p\langle X \rangle$ such that*

$$\sum_{n=0}^{\infty} \frac{g(n)}{n!} X^n = \exp(X) \sum_{n=0}^{\infty} d_n X^n \quad \textit{and} \quad g(X) \in \sum_{i=0}^{\ell} m_i i! \binom{X}{i} + p^k X \mathbb{Z}_p\langle X \rangle,$$

where

$$\binom{X}{i} = \frac{X(X-1)\cdots(X-i+1)}{i!}, \quad i = 1, 2, \ldots, \quad \textit{and} \quad \binom{X}{0} = 1.$$

Proof. Define a formal series

$$f(X) = \sum_{i=0}^{\infty} d_i i! \binom{X}{i}.$$

For any nonnegative integer i, we have

$$\sum_{n=0}^{\infty} \frac{i! \binom{n}{i}}{n!} X^n = \exp(X) \cdot X^i,$$

which is extended to the formula

$$\sum_{n=0}^{\infty} \frac{f(n)}{n!} X^n = \exp(X) \sum_{n=0}^{\infty} d_n X^n$$

by $\mathbb{Z}_p$-linearly. For each positive integer i, let $\{k_{in}\}_{n=1}^{\infty}$ be a sequence given by

$$\sum_{n=1}^{\infty} k_{in} X^n = i! \binom{X}{i}.$$

Then $k_{in} \in \mathbb{Z}$, and $k_{in} = 0$ if $n \geq i+1$. Since $\lim_{n\to\infty} |w_n|_p = 0$, it follows that

$$f(x) - \sum_{i=0}^{\ell} m_i i! \binom{x}{i} = \sum_{i=1}^{\infty} w_i i! \binom{x}{i} = \sum_{i=1}^{\infty} \sum_{n=1}^{i} w_i k_{in} x^n = \sum_{n=1}^{\infty} \left(\sum_{i=n}^{\infty} w_i k_{in} \right) x^n$$

for any $x \in \mathbb{Z}_p$. In particular, $\sum_{i=n}^{\infty} w_i k_{in} \in p^k \mathbb{Z}_p$ for any positive integer n. Moreover, $\lim_{n\to\infty} |\sum_{i=n}^{\infty} w_i k_{in}|_p = 0$. Now define a formal power series

$$g(X) = \sum_{i=0}^{\ell} m_i i! \binom{X}{i} + \sum_{n=1}^{\infty} \left(\sum_{i=n}^{\infty} w_i k_{in} \right) X^n.$$

Then $f(n) = g(n)$ for $n = 0, 1, 2, \ldots$. This completes the proof. $\square$

The following theorem is part of [8, Theorem 6.2.6] (see also [15, Chap. IV Theorem 14]).

Theorem 3.4 (p-adic Weierstrass Preparation Theorem) *Let*

$$f(X) = \sum f_n X^n$$

be a power series with coefficients in the field $\mathbb{Q}_p$ of p-adic numbers such that $\lim_{n\to\infty} |f_n|_p = 0$. Let N be the number defined by

$$|f_N|_p = \max |f_n|_p \quad \text{and} \quad |f_n|_p < |f_N|_p \text{ for all } n > N.$$

Then there exists a polynomial

$$k_0 + k_1 X + k_2 X^2 + \cdots + k_N X^N$$

of degree N with coefficients in $\mathbb{Q}_p$, and a formal power series

$$1 + m_1 X + m_2 X^2 + \cdots$$

with coefficients in $\mathbb{Q}_p$, satisfying

(i) $f(X) = (k_0 + k_1 X + k_2 X^2 + \cdots + k_N X^N)(1 + m_1 X + m_2 X^2 + \cdots)$,

(ii) $|k_N|_p = \max |k_n|_p$,

(iii) $\lim_{n\to\infty} |m_n|_p = 0$,

(iv) $|m_n|_p < 1$ *for all* $n \geq 1$.

4 p-adic properties of $a_n(p^u)$

We define a sequence $\{e_n^\natural\}_{n=0}^\infty$ by

$$\sum_{n=0}^{\infty} e_n^\natural X^n = \exp\left(\sum_{i=2}^{\infty} \frac{\varepsilon^\natural p^{p^i(u+1)}}{p^{u+i+1}} X^{p^i}\right),$$

so that for any nonnegative integer r less than p^{u+1},

$$\sum_{n=0}^{\infty} d_{n,r}^\natural X^n = \left(\sum_{j=0}^{\infty} c_{p^{u+1}j+r}^\natural (-(-1)^\natural p^{u+1})^j X^j\right) \exp\left(\frac{\varepsilon^\natural p^{p(u+1)}}{p^{u+2}} X^p\right) \sum_{n=0}^{\infty} e_n^\natural X^n.$$

To give p-adic properties of $a_n(p^u)$, we need the following.

Lemma 4.1 $\sum_{n=0}^{\infty} e_n^\natural X^n \in 1 + p^{3u+1} X \mathbb{Z}_p\langle X\rangle$.

Proof. If $i \geq 2$, then $p^i = (1+p-1)^i \geq i(p-1)+p \geq i+2 \geq 4$, and thereby,

$$\begin{aligned}\mathrm{ord}_p\left(\frac{p^{p^i(u+1)}}{p^{u+i+1}}\right) &= p^i(u+1) - (u+i+1)\\ &= p^i u + p^i - (u+i+1)\\ &\geq 4u + (i+2) - (u+i+1)\\ &= 3u+1.\end{aligned}$$

Hence the assertion follows from Lemma 3.2. This completes the proof. □

The results are divided into three theorems, which generalize part of the results proved by K. Conrad [4] (see also [11, 16]).

Theorem 4.2 *Suppose that $p \geq 3$. Let r be a nonnegative integer less than p^{u+1}. Then there exists a p-adic analytic function $g_r(X) \in \mathbb{Z}_p\langle X\rangle$ such that*

$$g_r(y) = \frac{a_{p^{u+1}y+r}(p^u)}{(p^{u+1}y+r)!}(-p^{u+1})^y y!$$

for any nonnegative integer y and

$$g_r(X) \in c_r - c_{p^{u+1}+r} p^{u+1} X + p^{2u+1} X \mathbb{Z}_p\langle X\rangle.$$

Proof. Using Lemmas 3.2 and 4.1, we have

$$\begin{aligned}\sum_{n=0}^{\infty} d_{n,r}^0 X^n &= \left(\sum_{j=0}^{\infty} c_{p^{u+1}j+r}(-p^{u+1})^j X^j\right) \exp\left(\frac{p^{p(u+1)}}{p^{u+2}} X^p\right) \sum_{n=0}^{\infty} e_n^0 X^n\\ &\in c_r - c_{p^{u+1}+r} p^{u+1} X + p^{2u+1} X \mathbb{Z}_p\langle X\rangle.\end{aligned}$$

Hence the assertion follows from Lemmas 2.2 and 3.3. This completes the proof. □

Theorem 4.3 *Suppose that $p = 2$ and $u \geq 2$. Let r be a nonnegative integer less than 2^{u+1}. Then there exists a 2-adic analytic function $g_r^\natural(X) \in \mathbb{Z}_2\langle X\rangle$ such that*

$$g_r^\natural(y) = \frac{a^\natural_{2^{u+1}y+r}(2^u)}{(2^{u+1}y+r)!}(-(-1)^\natural 2^{u+1})^y y!$$

for any nonnegative integer y and

$$g_r^\natural(X) \in c_r^\natural(1-(-1)^\natural 2^u X(X-1) + 2^{2u-1}X(X-1)(X-2)(X-3)) \\ -(-1)^\natural c^\natural_{2^{u+1}+r}2^{u+1}X + 2^{2u+1}X\mathbb{Z}_2\langle X\rangle.$$

Proof. By definition,

$$\sum_{n=0}^{\infty} d^\natural_{n,r}X^n = \left(\sum_{j=0}^{\infty} c^\natural_{2^{u+1}j+r}(-(-1)^\natural 2^{u+1})^j X^j\right)\exp(-(-1)^\natural 2^u X^2)\sum_{n=0}^{\infty} e_n^\natural X^n.$$

(Note that $\varepsilon^\natural = -(-1)^\natural$ if $p = 2$.) Using Lemma 3.2, we have

$$\exp(-(-1)^\natural 2^u X^2) \in 1-(-1)^\natural 2^u X^2 + 2^{2u-1}X^4 + 2^{2u+1}X^6\mathbb{Z}_2\langle X\rangle.$$

Moreover, it follows from Lemma 4.1 that

$$\sum_{i=0}^{\infty} d^\natural_{n,r}X^n \in c_r^\natural(1-(-1)^\natural 2^u X^2 + 2^{2u-1}X^4) \\ -(-1)^\natural c^\natural_{2^{u+1}+r}2^{u+1}X + 2^{2u+1}X\mathbb{Z}_2\langle X\rangle.$$

Hence the assertion follows from Lemmas 2.2 and 3.3. This completes the proof. □

Theorem 4.4 *Suppose that $p = 2$ and $u = 1$. Let r be a nonnegative integer less than 4. Then there exists a 2-adic analytic function $g_r^\natural(X) \in \mathbb{Z}_2\langle X\rangle$ such that*

$$g_r^\natural(y) = \frac{a^\natural_{4y+r}(2)}{(4y+r)!}((-1)^\natural 4)^y y!$$

for any nonnegative integer y and

$$g_r^\natural(X) \in c_r^\natural(1-2X+4\delta_{\natural 1}X(X-1) - 4X(X-1)(X-2)(X-3)) \\ +(-1)^\natural 4c^\natural_{4+r}X + 8X\mathbb{Z}_2\langle X\rangle,$$

where δ is the Kronecker delta.

Proof. Substituting $-X$ for X in Lemma 2.2, we have

$$\begin{aligned}\sum_{y=0}^{\infty} \frac{a^{\natural}_{4y+r}(2)}{(4y+r)!}((-1)^{\natural}4)^y X^y &= \exp(X)\exp(-2X-(-1)^{\natural}2X^2) \\ &\quad\times \left(\sum_{j=0}^{\infty} c^{\natural}_{4j+r}((-1)^{\natural}4)^j X^j\right)\sum_{n=0}^{\infty} e^{\natural}_n(-1)^n X^n. \end{aligned} \tag{6}$$

Moreover, it follows from Eq. (4) with $p=2$ and $u=2$ that

$$\begin{aligned}\exp(-2X-(-1)^{\natural}2X^2) &= \exp(-2X+2X^2+4X^4)\exp(-4\delta_{\natural 0}X^2-4X^4) \\ &= \left(\sum_{n=0}^{\infty} \frac{a_n(4)}{n!}(-2X)^n\right)\exp(-4\delta_{\natural 0}X^2-4X^4).\end{aligned}$$

By Lemma 3.1 and Theorem 4.3,

$$\operatorname{ord}_2\left(\frac{a_n(4)}{n!}(-2)^n\right) = \operatorname{ord}_2(a_n(4)) + \operatorname{ord}_2\left(\frac{(-2)^n}{n!}\right) \geq \left[\frac{n}{2}\right] + \left[\frac{n}{4}\right] - 2\left[\frac{n}{8}\right] + 1$$

if $n \geq 1$ (see also Proposition 4.7). Observe that

$$\operatorname{ord}_2\left(\frac{a_n(4)}{n!}(-2)^n\right) \geq 4$$

if $n \geq 4$. Then, since $a_0(4) = a_1(4) = 1$, $a_2(4) = 2$, and $a_3(4) = 4$, we have

$$\sum_{n=0}^{\infty} \frac{a_n(4)}{n!}(-2X)^n \in 1 - 2X + 4X^2 + 16X\mathbb{Z}_2\langle X\rangle.$$

This, combined with Lemma 3.2, yields

$$\exp(-2X-(-1)^{\natural}2X^2) \in (1-2X+4X^2)(1-4\delta_{\natural 0}X^2-4X^4) + 8X\mathbb{Z}_2\langle X\rangle.$$

Hence it follows from Lemma 4.1 that

$$\begin{aligned}&\exp(-2X-(-1)^{\natural}2X^2)\left(\sum_{j=0}^{\infty} c^{\natural}_{4j+r}((-1)^{\natural}4)^j X^j\right)\sum_{n=0}^{\infty} e^{\natural}_n(-1)^n X^n \\ &\qquad \in c^{\natural}_r(1-2X+4\delta_{\natural 1}X^2-4X^4) + (-1)^{\natural}4c^{\natural}_{4+r}X + 8X\mathbb{Z}_2\langle X\rangle.\end{aligned}$$

The assertion now follows from Lemma 3.3 and Eq. (6). □

Let r be a nonnegative integer less than p^{u+1}. By Lemma 3.1,

$$\operatorname{ord}_p\left(\frac{(p^{u+1}y+r)!}{p^{(u+1)y}y!}\right) = \sum_{j=1}^{u}\left[\frac{p^{u+1}y+r}{p^j}\right] - uy = \left\{\frac{p^{u+1}-1}{p-1} - (u+1)\right\}y + \operatorname{ord}_p(r!)$$

for any nonnegative integer y. Combining this fact with Theorems 4.2, 4.3, and 4.4, we obtain the following.

Corollary 4.5 ([13]) *Let r be a nonnegative integer less than p^{u+1}. Then*

$$\begin{aligned}\mathrm{ord}_p\left(a_{p^{u+1}y+r}(p^u)\right) &\geq \sum_{j=1}^{u}\left[\frac{p^{u+1}y+r}{p^j}\right]-uy\\ &=\left\{\frac{p^{u+1}-1}{p-1}-(u+1)\right\}y+\mathrm{ord}_p(r!)\end{aligned}$$

for any nonnegative integer y. Moreover, if $\mathrm{ord}_p(c_r)\leq u$, then

$$\begin{aligned}\mathrm{ord}_p(a_{p^{u+1}y+r}(p^u)) &= \sum_{j=1}^{u}\left[\frac{p^{u+1}y+r}{p^j}\right]-uy+\mathrm{ord}_p(c_r)\\ &=\left\{\frac{p^{u+1}-1}{p-1}-(u+1)\right\}y+\mathrm{ord}_p(r!)+\mathrm{ord}_p(c_r)\end{aligned}$$

for any nonnegative integer y.

Example 4.6 ([6, 13, 14, 16]) Suppose that $p=2$ and $u=1$. By Lemma 2.1 and Corollary 4.5,

$$\mathrm{ord}_2(a_n(2))=\begin{cases}\left[\dfrac{n}{2}\right]-\left[\dfrac{n}{4}\right]+1 & \text{if } n\equiv 3 \pmod 4,\\ \left[\dfrac{n}{2}\right]-\left[\dfrac{n}{4}\right] & \text{otherwise.}\end{cases}$$

Proposition 4.7 *Suppose that $p=2$ and $u=2$, and let r be a nonnegative integer less than 8. For any nonnegative integer y,*

$$\begin{aligned}\mathrm{ord}_2(a_{8y+r}(4)) &= \left[\frac{8y+r}{2}\right]+\left[\frac{8y+r}{4}\right]-2y+\mathrm{ord}_2(c_r)\\ &=4y+\mathrm{ord}_2(r!)+\mathrm{ord}_2(c_r),\end{aligned}$$

that is, the values of $\mathrm{ord}_2(a_{8y+r}(4))-4y$, $0\leq r\leq 7$, are as follows :

r	0	1	2	3	4	5	6	7
$\mathrm{ord}_2(a_{8y+r}(4))-4y$	0	0	1	2	4	3	8	4

Proof. If $r\neq 6$, then the proposition follows from Lemma 2.1 and Corollary 4.5. By Theorem 4.3, there exists a 2-adic analytic function $g_6^0(X)\in\mathbb{Z}_2\langle X\rangle$ such that

$$g_6^0(y)=\frac{a_{8y+6}(4)}{(8y+6)!}(-8)^y y!$$

for any nonnegative integer y and

$$g_6^0(X)\in c_6(1-4X(X-1)+8X(X-1)(X-2)(X-3))-8c_{14}X+2^5X\mathbb{Z}_2\langle X\rangle.$$

Let y be a nonnegative integer. We have $\mathrm{ord}_2(a_{8y+6}(4))=4y+4+\mathrm{ord}_2(g_6^0(y))$. Since $c_6=16/45$ and $c_{14}=2172172/42567525$, it follows that $\mathrm{ord}_2(g_6^0(y))=4$. Hence $\mathrm{ord}_2(a_{8y+6}(4))=4y+8$. This completes the proof. □

5 2-adic properties of $t_n(2^u)$

The first statement of the following theorem is due to D. Kim and J. S. Kim [14], and the second one is an affirmative answer to a conjecture of them.

Theorem 5.1 *Suppose that $p = 2$ and $u = 1$. Then the following statements hold for any nonnegative integer y.*

(a) $\mathrm{ord}_2(t_{4y}(2)) = y + \chi_o(y)$, $\mathrm{ord}_2(t_{4y+2}(2)) = \mathrm{ord}_2(t_{4y+3}(2)) = y$.

(b) *There exists a 2-adic integer α such that*

$$\mathrm{ord}_2(t_{4y+1}(2)) = y + \chi_o(y) \cdot (\mathrm{ord}_2(y + \alpha) + 1).$$

Proof. Keep the notation of Theorem 4.4, and let y be a nonnegative integer. Then by Eq. (3), we have

$$t_{4y+r}(2) = \frac{(4y + r)!}{4^y \cdot y!} \cdot \frac{g_r^0(y) + (-1)^{r+y} g_r^1(y)}{2}.$$

Now set $L_{r,y}(X) = (g_r^0(X) + (-1)^{r+y} g_r^1(X))/2$. Then there exists a 2-adic analytic function $M_{r,y}(X) \in \mathbb{Z}_2\langle X\rangle$ such that

$$\begin{aligned} L_{r,y}(X) = c_r^0 & \frac{1 - 2X - 4X(X-1)(X-2)(X-3)}{2} \\ & +(-1)^{r+y} c_r^1 \frac{1 - 2X + 4X(X-1) - 4X(X-1)(X-2)(X-3)}{2} \\ & +2(c_{4+r}^0 - (-1)^{r+y} c_{4+r}^1)X + 4XM_{r,y}(X). \end{aligned}$$

Moreover, it follows from Lemma 2.1 that

$$\begin{aligned} & L_{0,y}(y) \equiv L_{1,y}(y) \equiv 1 \pmod 4, \\ & L_{2,y}(y) \equiv \frac{1}{2} \pmod 2, \quad L_{3,y}(y) \equiv \frac{1}{6} \pmod 2 \end{aligned}$$

if y is even, and

$$\begin{aligned} & L_{0,y}(y) \equiv -2y^2 \pmod 4, \quad L_{1,y}(y) \equiv \frac{38}{15} y - 2y^2 \pmod 4, \\ & L_{2,y}(y) \equiv \frac{1}{2} - y \pmod 2, \quad L_{3,y}(y) \equiv \frac{1}{2} - y \pmod 4 \end{aligned}$$

if y is odd. Since $\mathrm{ord}_2((4y + r)!/4^y \cdot y!) = y + \mathrm{ord}_2(r!)$, it follows that

$$\mathrm{ord}_2(t_{4y+r}(2)) = \begin{cases} y + \chi_o(y) & \text{if } r = 0, \\ y & \text{if } r = 1 \text{ and } y \text{ is even}, \\ y & \text{if } r = 2 \text{ or } r = 3. \end{cases}$$

Assume that y is odd. Then by Lemma 2.1,

$$L_{1,y}(X) = -2X(X-1) + \frac{8}{15}X + 4XM_{1,y}(X) = \frac{38}{15}X - 2X^2 + 4XM_{1,y}(X).$$

Hence it follows from Theorem 3.4 that there exists a polynomial

$$k_0 + k_1X + k_2X^2$$

of degree 2 with coefficients in $\mathbb{Q}_2$, and a power series

$$1 + m_1X + m_2X^2 + \cdots$$

with coefficients in $\mathbb{Q}_2$, satisfying the conditions (i)–(iv) with $f(X) = L_{1,y}(X)$, $N = 2$, and $p = 2$. We have $k_0 = 0$, $k_1 \equiv 38/15 \pmod 4$, and $k_2 \equiv -2 - k_1m_1 \pmod 4$. Now set $\lambda = 2^{-1}k_2$. Then $\mathrm{ord}_2(\lambda) = 0$, because $\mathrm{ord}_2(m_1) > 0$. Observe that $\alpha := 2^{-1}k_1\lambda^{-1} \in \mathbb{Z}_2$ and

$$L_{1,y}(X) = 2\lambda X(X+\alpha)(1 + m_1X + m_2X^2 + \cdots).$$

Then we have

$$\mathrm{ord}_2(t_{4y+1}) = y + 1 + \mathrm{ord}_2(y+\alpha).$$

This completes the proof. □

Remark 5.2 According to Mathematica,

$$\alpha \equiv 1 + 2 + 2^3 + 2^8 + 2^{10} + 2^{12} \pmod{2^{14}}.$$

The following lemma is an immediate consequence of Eq. (3) and Theorem 4.3.

Lemma 5.3 *Suppose that $p = 2$ and $u \geq 2$. Let r be a nonnegative integer less than 2^{u+1}, and let y be a nonnegative integer. Then there exists a 2-adic analytic function $M_{r,y}(X) \in \mathbb{Z}_2\langle X\rangle$ such that*

$$t_{2^{u+1}y+r}(2^u) = \frac{(2^{u+1}y+r)!}{2^{(u+1)y}\cdot y!}\cdot L_{r,y}(y)$$

with

$$\begin{aligned} L_{r,y}(X) = \quad & (-1)^y c_r^0 \frac{1 - 2^uX(X-1) + 2^{2u-1}X(X-1)(X-2)(X-3)}{2} \\ & +(-1)^r c_r^1 \frac{1 + 2^uX(X-1) + 2^{2u-1}X(X-1)(X-2)(X-3)}{2} \\ & +2^u(-(-1)^y c^0_{2^{u+1}+r} + (-1)^r c^1_{2^{u+1}+r})X + 2^{2u}XM_{r,y}(X). \end{aligned}$$

Moreover, $\mathrm{ord}_2(t_{2^{u+1}y+r}(2^u)) = (2^{u+1} - u - 2)y + \mathrm{ord}_2(r!) + \mathrm{ord}_2(L_{r,y}(y))$.

We set $\chi_e(y) = 1 - \chi_o(y)$ for any nonnegative integer y.

Theorem 5.4 *Suppose that $p = 2$ and $u = 2$. Then the following statements hold for any nonnegative integer y.*

(a) $\mathrm{ord}_2(t_{8y+2}(4)) = \mathrm{ord}_2(t_{8y+3}(4)) = 4y$, $\mathrm{ord}_2(t_{8y+4}(4)) = 4y+2$, $\mathrm{ord}_2(t_{8y+5}(4)) = 4y+3+\chi_e(y)$, $\mathrm{ord}_2(t_{8y+6}(4)) = 4y+3$, $\mathrm{ord}_2(t_{8y+7}(4)) = 4y+4+\chi_e(y)$.

(b) *If $r = 0$ or $r = 1$, then there exists a 2-adic integer α_r such that*

$$\mathrm{ord}_2(t_{8y+r}(4)) = 4y + \chi_o(y) \cdot (\mathrm{ord}_2(y+\alpha_r) + 2).$$

Proof. Keep the notation of Lemma 5.3 with $u = 2$. Then by Lemma 2.1,

$$\begin{aligned} &L_{0,y}(y) \equiv L_{1,y}(y) \equiv 1 \pmod 8, \quad L_{2,y}(y) \equiv \frac{1}{2} \pmod 4,\\ &L_{3,y}(y) \equiv L_{4,y}(y) \equiv \frac{1}{6} \pmod 4, \quad L_{5,y}(y) \equiv \frac{2}{15} \pmod 8,\\ &L_{6,y}(y) \equiv \frac{17}{90} \pmod 4, \quad L_{7,y}(y) \equiv \frac{46}{315} \pmod 8 \end{aligned}$$

if y is even, and

$$\begin{aligned} &L_{0,y}(y) \equiv 4y\left(y - \frac{251}{315}\right) \pmod{16}, \quad L_{1,y} \equiv 4y\left(y - \frac{2519}{2835}\right) \pmod{16},\\ &L_{2,y}(y) \equiv L_{3,y}(y) \equiv L_{4,y}(y) \equiv -\frac{1}{2} \pmod 4, \quad L_{5,y}(y) \equiv -\frac{1}{3} \pmod 4,\\ &L_{6,y}(y) \equiv -\frac{1}{6} \pmod 4, \quad L_{7,y}(y) \equiv -\frac{1}{15} \pmod 4 \end{aligned}$$

if y is odd. This, combined with Lemma 5.3, yields the statement (a). The proof of the statement (b) is analogous to that of Theorem 5.1, while the assertion is a special case of Theorem 5.6. This completes the proof. □

Remark 5.5 According to Mathematica,

$$\alpha_0 \equiv 1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^7 + 2^9 + 2^{10} + 2^{12} + 2^{13} + 2^{14} + 2^{15} \pmod{2^{17}}$$

and

$$\alpha_1 \equiv 1 + 2 + 2^4 + 2^7 + 2^8 \pmod{2^{12}}.$$

The statement (b) of Theorem 5.4 is extended to a result for $\mathrm{ord}_2(t_{2^{u+1}y+r}(2^u))$ with $u \geq 3$ and $r = 0$ or $r = 1$.

Theorem 5.6 *Suppose that* $p = 2$ *and* $u \geq 2$. *Let* y *be a nonnegative integer. If* $r = 0$ *or* $r = 1$, *then there exists a* 2*-adic integer* α_r *such that*

$$\mathrm{ord}_2(t_{2^{u+1}y+r}(2^u)) = (2^{u+1} - u - 2)y + \chi_o(y) \cdot (\mathrm{ord}_2(y + \alpha_r) + u).$$

Moreover, if $\mathrm{ord}_2(c^0_{2^{u+1}+r} + (-1)^r c^1_{2^{u+1}+r}) = 0$ *with* $r = 0$ *or* $r = 1$, *then*

$$\mathrm{ord}_2(t_{2^{u+1}y+r}(2^u)) = (2^{u+1} - u - 2)y + \chi_o(y) \cdot u.$$

Proof. Keep the notation of Lemma 5.3. Since $c^0_0 = c^1_0 = c^0_1 = 1$ and $c^1_1 = -1$ by Lemma 2.1, it follows from Lemma 5.3 that the assertion holds if y is even. Assume that y is odd. Then

$$L_{r,y}(X) = 2^u(-1 + \hat{c}_{2^{u+1}+r})X + 2^u X^2 + 2^{2u} X M_{r,y}(X),$$

where $\hat{c}_{2^{u+1}+r} = c^0_{2^{u+1}+r} + (-1)^r c^1_{2^{u+1}+r}$. In each of the cases where $r = 0$ and $r = 1$, it follows from Theorem 3.4 that there exists a polynomial

$$k_0 + k_1 X + k_2 X^2$$

of degree 2 with coefficients in $\mathbb{Q}_2$, and a power series

$$1 + m_1 X + m_2 X^2 + \cdots$$

with coefficients in $\mathbb{Q}_2$, satisfying the conditions (i)–(iv) with $f(X) = L_{r,y}(X)$, $N = 2$, and $p = 2$. We have $k_0 = 0$, $k_1 \equiv 2^u(-1 + \hat{c}_{2^{u+1}+r}) \pmod{2^{2u}}$, and $k_2 \equiv 2^u - k_1 m_1 \pmod{2^{2u}}$. Now set $\lambda_r = 2^{-u} k_2$. Then $\mathrm{ord}_2(\lambda_r) = 0$, because $\mathrm{ord}_2(m_1) > 0$. Observe that $\alpha_r := 2^{-u} k_1 \lambda_r^{-1} \in \mathbb{Z}_2$ and

$$L_{r,y}(X) = 2^u \lambda_r X(X + \alpha_r)(1 + m_1 X + m_2 X^2 + \cdots).$$

Combining this fact with Lemma 5.3, we conclude that

$$\mathrm{ord}_2(t_{2^{u+1}y+r}(2^u)) = (2^{u+1} - u - 2)y + \mathrm{ord}_2(y + \alpha_r) + u$$

Moreover, if $\mathrm{ord}_2(\hat{c}_{2^{u+1}+r}) = 0$, then $\mathrm{ord}_2(\alpha_r) > 0$, and thereby, $\mathrm{ord}_2(y + \alpha_r) = 0$. This completes the proof. □

6 Wreath products

Let G be a finite group, and let K be a subgroup of S_n. The wreath product $G \wr K$ of G by K is defined to be the set

$$G \wr K = \{(g_1, \ldots, g_n)\sigma \mid (g_1, \ldots, g_n) \in G^{(n)} \quad \text{and} \quad \sigma \in K\},$$

where $G^{(n)}$ is the direct product of n copies of G, with multiplication given by

$$(g_1, \ldots, g_n)\sigma(h_1, \ldots, h_n)\tau = (g_1 h_{\sigma^{-1}(1)}, \ldots, g_n h_{\sigma^{-1}(n)})\sigma\tau.$$

Let m be a positive integer. We set

$$a(G \wr K, m) = \sharp\{(g_1, \ldots, g_n)\sigma \in G \wr K \mid ((g_1, \ldots, g_n)\sigma)^m = \epsilon\}.$$

Lemma 6.1 *Let $\tau \in S_n$ be a cycle of length ℓ. Then $((g_1, \ldots, g_n)\tau)^m = \epsilon$ if and only if ℓ divides m and $(g_i g_{\tau^{-1}(i)} \cdots g_{\tau^{-\ell+1}(i)})^{m/\ell} = \epsilon$ for all $i = 1, 2, \ldots, n$.*

Proof. The proof is straightforward. □

Let $\{\ell_0, \ell_1, \ldots, \ell_s\}$ be the set of divisors of a positive integer m. We quote the following (cf. [12, Lemma 4.2.10]).

Lemma 6.2 *The number of elements $(g_1, \ldots, g_n)\sigma$ of $G \wr S_n$ such that the cycle type of σ is $(\ell_0^{j_0}, \ell_1^{j_1}, \ldots, \ell_s^{j_s})$ and $((g_1, \ldots, g_n)\sigma)^m = \epsilon$ is*

$$n! \prod_{k=0}^{s} \frac{|G|^{(\ell_k - 1)j_k} a(G, m/\ell_k)^{j_k}}{\ell_k{}^{j_k} j_k!},$$

where $a(G, m/\ell_k) = \sharp\{g \in G \mid g^{m/\ell_k} = \epsilon\}$.

Proof. Let k be a nonnegative integer less than or equal to s, and let $\tau = (i_1 \ \cdots \ i_{\ell_k})$ be a cycle of length ℓ_k. Then it follows from Lemma 6.1 that the number of elements $(g_1, \ldots, g_n)$ of $G^{(n)}$ such that $((g_1, \ldots, g_n)\tau)^m = \epsilon$ and $g_i = \epsilon$ for all $i \neq i_1, \ldots, i_{\ell_k}$ is $|G|^{\ell_k - 1} a(G, m/\ell_k)$. Thus the lemma holds. □

By Lemma 6.2, we have

$$b_n(p^u) = a(C_p \wr S_n, p^u) = \sum_{j_0 + j_1 p + \cdots + j_u p^u = n} n! \left(\prod_{k=0}^{u} \frac{p^{p^k j_k}}{p^{k j_k} j_k!} \right) \frac{1}{p^{j_u}}. \tag{7}$$

Set $b_n^0(p^u) = b_n(p^u)$, and define

$$b_n^1(p^u) = \sum_{j_0 + j_1 p + \cdots + j_u p^u = n} (-1)^{j_0 + j_1 + \cdots + j_u} n! \left(\prod_{k=0}^{u} \frac{p^{p^k j_k}}{p^{k j_k} j_k!} \right) \frac{1}{p^{j_u}}. \tag{8}$$

Then by Lemma 6.2, we have

$$q_n(p^u) = a(C_p \wr A_n, p^u) = \frac{b_n^0(p^u) + (-1)^n b_n^1(p^u)}{2}. \tag{9}$$

(Obviously, $b_n(p^u) = q_n(p^u)$ if $p \neq 2$.) Let $\natural$ denotes both 0 and 1. We always assume that $b_0^\natural(p^u) = 1$. By Eqs. (7)–(9), we have

$$\sum_{n=0}^{\infty} \frac{b_n^\natural(p^u)}{n!} X^n = \exp\left((-1)^\natural \sum_{k=0}^{u-1} \frac{p^{p^k}}{p^k} X^{p^k} + (-1)^\natural \frac{p^{p^u}}{p^{u+1}} X^{p^u} \right), \tag{10}$$

$$\sum_{n=0}^{\infty} \frac{q_n(2^u)}{n!} X^n = \frac{1}{2} \exp\left(\sum_{k=0}^{u-1} \frac{2^{2^k}}{2^k} X^{2^k} + \frac{2^{2^u}}{2^{u+1}} X^{2^u} \right)$$
$$+ \frac{1}{2} \exp\left(2X - \sum_{k=1}^{u-1} \frac{2^{2^k}}{2^k} X^{2^k} - \frac{2^{2^u}}{2^{u+1}} X^{2^u} \right)$$

(cf. [1], [17, Proposition 3.4]). Moreover, by Eq. (5), we have

$$\sum_{n=0}^{\infty} c_n^{\natural}(pX)^n = \exp\left((-1)^{\natural}\sum_{k=0}^{\infty}\frac{p^{p^k}}{p^k}X^{p^k}\right). \tag{11}$$

Recall that $\varepsilon^{\natural} = -1$ if $p = 2$ and $\natural = 0$, and $\varepsilon^{\natural} = +1$ otherwise. For any nonnegative integer r less than p^u, we set

$$\widetilde{H}_{u,r}^{\natural}(X) = \sum_{y=0}^{\infty}\frac{b_{p^u y+r}^{\natural}(p^u)}{(p^u y+r)!}\left(-(-1)^{\natural}\frac{p^{u+1}}{p^{p^u}(p-1)}X\right)^y,$$

and define a sequence $\{\widetilde{d}_{n,r}^{\natural}\}_{n=0}^{\infty}$ by

$$\sum_{n=0}^{\infty}\widetilde{d}_{n,r}^{\natural}X^n = \left(\sum_{j=0}^{\infty}c_{p^u j+r}^{\natural}p^r\left(-(-1)^{\natural}\frac{p^{u+1}}{p-1}X\right)^j\right)\exp\left(\sum_{i=1}^{\infty}\frac{\varepsilon^{\natural}p^{p^i(u+1)}}{p^{u+i}(p-1)^{p^i}}X^{p^i}\right).$$

Lemma 6.3 *Let r be a nonnegative integer less than p^u. Then*

$$\widetilde{H}_{u,r}^{\natural}(X) = \exp(X)\sum_{n=0}^{\infty}\widetilde{d}_{n,r}^{\natural}X^n.$$

Proof. Using Eqs. (10) and (11), we have

$$\sum_{n=0}^{\infty}\frac{b_n^{\natural}(p^u)}{n!}X^n = \left(\sum_{n=0}^{\infty}c_n^{\natural}(pX)^n\right)\exp\left(-(-1)^{\natural}\frac{p^{p^u}}{p^u}X^{p^u}\right)$$
$$\times\exp\left((-1)^{\natural}\frac{p^{p^u}}{p^{u+1}}X^{p^u}\right)\exp\left(-(-1)^{\natural}\sum_{k=u+1}^{\infty}\frac{p^{p^k}}{p^k}X^{p^k}\right).$$

This formula yields

$$\sum_{y=0}^{\infty}\frac{b_{p^u y+r}^{\natural}(p^u)}{(p^u y+r)!}X^{p^u y+r} = \left(\sum_{j=0}^{\infty}c_{p^u j+r}^{\natural}p^{p^u j+r}X^{p^u j+r}\right)\exp\left(-(-1)^{\natural}\frac{p^{p^u}}{p^u}X^{p^u}\right)$$
$$\times\exp\left((-1)^{\natural}\frac{p^{p^u}}{p^{u+1}}X^{p^u}\right)\exp\left(-(-1)^{\natural}\sum_{i=1}^{\infty}\frac{p^{p^{u+i}}}{p^{u+i}}X^{p^{u+i}}\right).$$

Omit X^r and substitute $(-(-1)^{\natural}p^{u+1}X/p^{p^u}(p-1))^{1/p^u}$ for X. Then we have

$$\sum_{y=0}^{\infty}\frac{b_{p^u y+r}^{\natural}(p^u)}{(p^u y+r)!}\left(-(-1)^{\natural}\frac{p^{u+1}}{p^{p^u}(p-1)}X\right)^y = \left(\sum_{j=0}^{\infty}c_{p^u j+r}^{\natural}p^r\left(-(-1)^{\natural}\frac{p^{u+1}}{p-1}X\right)^j\right)$$
$$\times\exp(X)\exp\left(\sum_{i=1}^{\infty}\frac{-(-1)^{\natural}\cdot(-(-1)^{\natural})^{p^i}p^{p^i(u+1)}}{p^{u+i}(p-1)^{p^i}}X^{p^i}\right).$$

This completes the proof. □

7 p-adic properties of $b_n(p^u)$

In order to analyze $\sum_{n=0}^{\infty} \tilde{d}_{n,r}^{\natural} X^n$, we define a sequence $\{\tilde{e}_n^{\natural}\}_{n=0}^{\infty}$ by

$$\sum_{n=0}^{\infty} \tilde{e}_n^{\natural} X^n = \exp\left(\sum_{i=2}^{\infty} \frac{\varepsilon^{\natural} p^{p^i(u+1)}}{p^{u+i}(p-1)^{p^i}} X^{p^i}\right).$$

The proof of the following lemma is analogous to that of Lemma 4.1.

Lemma 7.1 $\sum_{n=0}^{\infty} \tilde{e}_n^{\natural} X^n \in 1 + p^{3u+2} X\mathbb{Z}_p\langle X\rangle.$

We are now in position to state a p-adic property of $b_n(p^u)$.

Theorem 7.2 *Let r be a nonnegative integer less than p^u. Then there exists a p-adic analytic function $g_r^{\natural}(X) \in \mathbb{Z}_p\langle X\rangle$ such that*

$$g_r^{\natural}(y) = \frac{b_{p^u y+r}^{\natural}(p^u)}{(p^u y + r)!}\left(-(-1)^{\natural}\frac{p^{u+1}}{p^{p^u}(p-1)}\right)^y y!$$

for any nonnegative integer y and

$$g_r^{\natural}(X) \in c_r^{\natural} p^r \left\{1 + \varepsilon^{\natural}\frac{p^{(u+1)(p-1)}}{(p-1)^p} X(X-1)(X-2)\cdots(X-p+1)\right\} - (-1)^{\natural} c_{p^u+r}^{\natural}\frac{p^{u+1+r}}{p-1} X + p^{2u+1+r} X\mathbb{Z}_p\langle X\rangle.$$

Proof. Using Lemmas 3.2 and 7.1, we have

$$\begin{aligned}\sum_{n=0}^{\infty} \tilde{d}_{n,r}^{\natural} X^n &= \left(\sum_{j=0}^{\infty} c_{p^u j+r}^{\natural} p^r \left(-(-1)^{\natural}\frac{p^{u+1}}{p-1} X\right)^j\right) \\ &\qquad \times \exp\left(\frac{\varepsilon^{\natural} p^{p(u+1)}}{p^{u+1}(p-1)^p} X^p\right)\sum_{n=0}^{\infty} \tilde{e}_n^{\natural} X^n \\ &\in c_r^{\natural} p^r \left\{1 + \varepsilon^{\natural}\frac{p^{(u+1)(p-1)}}{(p-1)^p} X^p\right\} \\ &\qquad - (-1)^{\natural} c_{p^u+r}^{\natural}\frac{p^{u+1+r}}{p-1} X + p^{2u+1+r} X\mathbb{Z}_p\langle X\rangle.\end{aligned}$$

Hence the assertion follows from Lemmas 3.3 and 6.3. This completes the proof. □

This theorem, together with Lemma 3.1, yields the following.

Corollary 7.3 *Let r be a nonnegative integer less than p^u. Then*

$$\begin{aligned}\mathrm{ord}_p\left(b_{p^u y+r}(p^u)\right) &\geq \sum_{j=0}^{u-1}\left[\frac{p^u y+r}{p^j}\right]-uy\\ &=\left\{\frac{p^u-1}{p-1}+p^u-(u+1)\right\}y+r+\mathrm{ord}_p(r!)\end{aligned}$$

for any nonnegative integer y. If $\mathrm{ord}_p(c_r)\leq u$, then

$$\begin{aligned}\mathrm{ord}_p(b_{p^u y+r}(p^u)) &= \sum_{j=0}^{u-1}\left[\frac{p^u y+r}{p^j}\right]-uy+\mathrm{ord}_p(c_r)\\ &=\left\{\frac{p^u-1}{p-1}+p^u-(u+1)\right\}y+r+\mathrm{ord}_p(r!)+\mathrm{ord}_p(c_r)\end{aligned}$$

for any nonnegative integer y.

Example 7.4 Suppose that $u=1$. Then for any nonnegative integer r less than p, we have $\mathrm{ord}_p(c_r)=0$. Hence

$$\mathrm{ord}_p(b_n(p))=n-\left[\frac{n}{p}\right]\quad\text{and}\quad \mathrm{ord}_2(b_n(2))=\left[\frac{n+1}{2}\right].$$

Example 7.5 Suppose that $p=2$ and $u=2$. By Lemma 2.1 and Corollary 7.3,

$$\mathrm{ord}_2(b_n(4))=\begin{cases} n+\left[\frac{n}{2}\right]-2\left[\frac{n}{4}\right]+1 & \text{if } n\equiv 3 \pmod 4,\\ n+\left[\frac{n}{2}\right]-2\left[\frac{n}{4}\right] & \text{otherwise.}\end{cases}$$

Proposition 7.6 *Suppose that $p=2$ and $u=3$, and let r be a nonnegative integer less than 8. For any nonnegative integer y,*

$$\begin{aligned}\mathrm{ord}_2(b_{8y+r}(8)) &= 8y+r+\left[\frac{8y+r}{2}\right]+\left[\frac{8y+r}{4}\right]-3y+\mathrm{ord}_2(c_r)\\ &= 11y+r+\mathrm{ord}_2(r!)+\mathrm{ord}_2(c_r),\end{aligned}$$

that is, the values of $\mathrm{ord}_2(b_{8y+r}(8))-11y-r$, $0\leq r\leq 7$, are the following :

r	0	1	2	3	4	5	6	7
$\mathrm{ord}_2(b_{8y+r}(8))-11y-r$	0	0	1	2	4	3	8	4

Proof. If $r\neq 6$, then the theorem follows from Lemma 2.1 and Corollary 7.3. By Lemma 2.1 and Theorem 7.2, there exists a 2-adic analytic function $g_6^0(X)\in\mathbb{Z}_2\langle X\rangle$ such that

$$g_6^0(y)=\frac{b_{8y+6}(8)}{(8y+6)!}\left(-\frac{1}{16}\right)^y y!$$

for any nonnegative integer y and

$$g_6^0(X) \in 2^6 \cdot \frac{16}{45}(1 - 16X(X-1)) - 2^{10} \cdot \frac{2172172}{42567525} X + 2^{13} X \mathbb{Z}_2\langle X \rangle.$$

Hence Lemma 3.1 implies that $\mathrm{ord}_2(b_{8y+6}(8)) = 11y + 4 + \mathrm{ord}_2(g_6^0(y)) = 11y + 14$ for any nonnegative integer y. This completes the proof. □

8 2-adic properties of $q_n(2^u)$

The following lemma is an immediate consequence of Eq. (9) and Theorem 7.2.

Lemma 8.1 *Suppose that $p = 2$. Let r be a nonnegative integer less than 2^u, and let y be a nonnegative integer. Then there exists a 2-adic analytic function $M_{r,y}(X) \in \mathbb{Z}_2\langle X \rangle$ such that*

$$q_{2^u y + r}(2^u) = \frac{(2^u y + r)!}{2^{uy} \cdot y!} \cdot 2^{(2^u - 1)y} \cdot L_{r,y}(y)$$

with

$$\begin{aligned} L_{r,y}(X) = (-1)^y 2^r c_r^0 \frac{1 - 2^{u+1}X(X-1)}{2} &+ (-2)^r c_r^1 \frac{1 + 2^{u+1}X(X-1)}{2} \\ &+ 2^{u+r}(-(-1)^y c_{2^u+r}^0 + (-1)^r c_{2^u+r}^1)X + 2^{2u+r} X M_{r,y}(X). \end{aligned}$$

Moreover, $\mathrm{ord}_2(q_{2^u y + r}(2^u)) = (2^{u+1} - u - 2)y + \mathrm{ord}_2(r!) + \mathrm{ord}_2(L_{r,y}(y))$.

Example 8.2 Suppose that $p = 2$ and $u = 1$. Let r be a nonnegative integer less than 2, and let y be a nonnegative integer. By Lemma 2.1 and Lemma 8.1, we have

$$\mathrm{ord}_2(q_{2y+r}(2)) = y + \left[\frac{r+1}{2}\right] + \chi_o(y) = \begin{cases} y & \text{if } y \text{ is even and if } r = 0, \\ y+1 & \text{if } y \text{ is even and if } r = 1, \\ y+1 & \text{if } y \text{ is odd and if } r = 0, \\ y+2 & \text{if } y \text{ is odd and if } r = 1. \end{cases}$$

We conclude this paper with the following three results for $\mathrm{ord}_2(q_n(2^u))$.

Theorem 8.3 *Suppose that $p = 2$ and $u = 2$. Then the following statements hold for any nonnegative integer y.*

(a) $\mathrm{ord}_2(q_{4y}(4)) = 4y + 2\chi_o(y)$, $\mathrm{ord}_2(q_{4y+2}(4)) = 4y + 2$, $\mathrm{ord}_2(q_{4y+3}(4)) = 4y + 3$.

(b) *There exists a 2-adic integer β such that*

$$\mathrm{ord}_2(q_{4y+1}(4)) = 4y + 1 + \chi_o(y) \cdot (\mathrm{ord}_2(y + \beta) + 3).$$

Proof. Keep the notation of Lemma 8.1 with $u = 2$. Set $h_{r,y} = \mathrm{ord}_2(L_{r,y}(y))$. Then by Lemma 2.1,

$$h_{0,y}(y) = 0, \quad h_{1,y} = h_{2,y} = 1, \quad h_{3,y} = 2$$

if y is even, and

$$h_{0,y} = 2, \quad L_{1,y}(y) \equiv 16y\left(y - \frac{13}{15}\right) \pmod{32}, \quad h_{2,y} = 1, \quad h_{3,y} = 2$$

if y is odd. Thus the statement (a) follows from Lemma 8.1. The proof of the statement (b) is analogous to that of Theorem 5.1(b), while the assertion is a special case of Theorem 8.7. This completes the proof. □

Remark 8.4 According to Mathematica,

$$\beta \equiv 1 + 2^2 + 2^3 + 2^4 + 2^6 + 2^7 + 2^8 \pmod{2^{13}}.$$

Theorem 8.5 *Suppose that $p = 2$ and $u = 3$. Then the following statements hold for any nonnegative integer y.*

(a) $\mathrm{ord}_2(q_{8y+2}(8)) = 11y + 2$, $\mathrm{ord}_2(q_{8y+3}(8)) = 11y + 3$, $\mathrm{ord}_2(q_{8y+4}(8)) = 11y + 6$, $\mathrm{ord}_2(q_{8y+5}(8)) = 11y + 8 + \chi_e(y)$, $\mathrm{ord}_2(q_{8y+6}(8)) = 11y + 9$, $\mathrm{ord}_2(q_{8y+7}(8)) = 11y + 11 + \chi_e(y)$.

(b) *If $r = 0$ or $r = 1$, then there exists a 2-adic integer β_r such that*

$$\mathrm{ord}_2(q_{8y+r}(8)) = 11y + r + \chi_o(y) \cdot (\mathrm{ord}_2(y + \beta_r) + 4).$$

Proof. Keep the notation of Lemma 8.1 with $u = 3$. Set $h_{r,y} = \mathrm{ord}_2(L_{r,y}(y))$. Then by Lemma 2.1,

$$h_{0,y} = 0, \quad h_{1,y} = h_{2,y} = 1, \quad h_{3,y} = 2, \quad h_{4,y} = 3, \quad h_{5,y} = 6, \quad h_{6,y} = 5, \quad h_{7,y} = 8$$

if y is even, and

$$L_{0,y}(y) \equiv 16y\left(y - \frac{283}{315}\right) \pmod{64}, \quad L_{1,y}(y) \equiv 32y\left(y - \frac{2677}{2835}\right) \pmod{128},$$
$$h_{2,y} = 1, \quad h_{3,y} = 2, \quad h_{4,y} = 3, \quad h_{5,y} = h_{6,y} = 5, \quad h_{7,y} = 7$$

if y is odd. Thus the statement (a) follows from Lemma 8.1. The proof of the statement (b) is analogous to that of Theorem 5.1(b), while the assertion is a special case of Theorem 8.7. This completes the proof. □

Remark 8.6 According to Mathematica,

$$\beta_0 \equiv 1 + 2 + 2^2 + 2^3 + 2^4 + 2^6 + 2^8 + 2^9 \pmod{2^{12}}$$

and

$$\beta_1 \equiv 1 + 2^3 + 2^4 + 2^5 + 2^6 + 2^8 + 2^{10} + 2^{11} + 2^{12} \pmod{2^{14}}.$$

The statement (b) both of Theorems 8.3 and 8.5 is extended to a result for $\mathrm{ord}_2(q_{2^u y+r}(2^u))$ with $u \geq 4$ and $r = 0$ or $r = 1$.

Theorem 8.7 *Suppose that $p = 2$ and $u \geq 2$. Let y be a nonnegative integer. If $r = 0$ or $r = 1$, then there exists a 2-adic integer β_r such that*

$$\mathrm{ord}_2(q_{2^u y+r}(2^u)) = (2^{u+1} - u - 2)y + r + \chi_o(y) \cdot (\mathrm{ord}_2(y + \beta_r) + u + 1).$$

Moreover, if $\mathrm{ord}_2(c^0_{2^u+r} + (-1)^r c^1_{2^u+r}) = 0$ *with $r = 0$ or $r = 1$, then*

$$\mathrm{ord}_2(q_{2^u y+r}(2^u)) = (2^{u+1} - u - 2)y + r + \chi_o(y) \cdot u.$$

Proof. Keep the notation of Lemma 8.1. Since $c^0_0 = c^1_0 = c^0_1 = 1$ and $c^1_1 = -1$ by Lemma 2.1, it follows from Lemma 8.1 that the assertion holds if y is even. Assume that y is odd. Then

$$L_{0,y}(X) = 2^{u+1}X(X-1) + 2^u(c^0_{2^u} + c^1_{2^u})X + 2^{2u}XM_{0,y}(X),$$
$$L_{1,y}(X) = 2^{u+2}X(X-1) + 2^{u+1}(c^0_{2^u+1} - c^1_{2^u+1})X + 2^{2u+1}XM_{1,y}(X).$$

Hence, if $\mathrm{ord}_2(c^0_{2^u+r} + (-1)^r c^1_{2^u+r}) = 0$, then the assertion follows from Lemma 8.1. Suppose that $\mathrm{ord}_2(c^0_{2^u+r} + (-1)^r c^1_{2^u+r}) > 0$. Then by an argument analogous to that in the proof of Theorem 5.6, we have

$$\mathrm{ord}_2(L_{r,y}(y)) = r + \mathrm{ord}_2(y + \beta_r) + u + 1$$

for some $\beta_r \in \mathbb{Z}_2$. Hence the assertion follows from Lemma 8.1. This completes the proof. □

ACKNOWLEDGMENT

The authors would like to thank a referee for helpful suggestions.

REFERENCES

1. N. Chigira, The solutions of $x^d = 1$ in finite groups, J. Algebra **180** (1996), 653–661.

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

3. S. Chowla, I. N. Herstein, and W. R. Scott, The solutions of $x^d = 1$ in symmetric groups, Norske Vid. Selsk. Forh. (Trondheim) **25** (1952), 29–31.

4. K. Conrad, p-adic properties of truncated Artin-Hasse coefficients, 1998, preprint.

5. J. Dieudonné, On the Artin-Hasse exponential series, Proc. Amer. Math. Soc. **8** (1957), 210–214.

6. A. Dress and T. Yoshida, On p-divisibility of the Frobenius numbers of symmetric groups, 1991, unpublished note.

7. B. Dwork, A note on the p-adic gamma function, Groupe d'étude d'Analyse ultramétrique, 9e année, 1981/82, fasc. 3, n° J5, 10 pp., Inst. Henri Poincaré, Paris, 1983.

8. F. Q. Gouvêa, p-adic Numbers, 2nd ed., Universitext, Springer-Verlag, New York, 1997.

9. M. Grady and M. Newman, Residue periodicity in subgroup counting functions; in :"The Rademacher Legacy to Mathematics," Contemp. Math. **166** (1994), 265–273.

10. M. Hall Jr., The Theory of Groups, 2nd edition, Chelsea, New York, 1976.

11. H. Ishihara, H. Ochiai, Y. Takegahara, and T. Yoshida, p-divisibility of the number of solutions of $x^p = 1$ in a symmetric group, Ann. Comb. **5** (2001), 197–210.

12. G. D. James and A. Kerber, The Representation Theory of the Symmetric Group, Encyclopedia of mathematics and its applications, Vol. 16, Addison-Wesley, Reading, MA, 1981.

13. H. Katsurada, Y. Takegahara, and T. Yoshida, The number of homomorphisms from a finite abelian group to a symmetric group, Comm. Algebra **28** (2000), 2271–2290.

14. D. Kim and J. S. Kim, A combinatorial approach to the power of 2 in the number of involutions, J. Combin. Theory Ser. A **117** (2010), 1082–1094.

15. N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, 2nd ed., Springer-Verlag, New York, 1984.

16. H. Ochiai, A p-adic property of the Taylor series of $\exp(x + x^p/p)$, Hokkaido Math. J. **28** (1999), 71–85.

17. S. Okada, Wreath products by the symmetric groups and product posets of Young's lattices, J. Combin. Theory Ser. A **55** (1990), 14–32.

18. J. Riordan, An Introduction to Combinatorial Analysis, Wiley, New York, 1958.

19. W. H. Schikhof, Ultrametric Calculus, Cambridge University Press, Cambridge, 1984.

20. T. Yoshida, Private discussions.