

Congruences for the cycle indicator of the symmetric group

Abdelaziz Bellagh and Assia Oulebsir

Abstract. Let n be a positive integer and let C_n be the cycle indicator of the symmetric group S_n . Carlitz proved that if p is a prime, and if r is a non negative integer, then we have the congruence

$$C_{r+np} \equiv (X_1^p - X_p)^n C_r \pmod{p\mathbb{Z}_p[X_1, \dots, X_{r+np}]},$$

where \mathbb{Z}_p is the ring of p -adic integers. We prove that for $p \neq 2$, the preceding congruence holds modulo $np\mathbb{Z}_p[X_1, \dots, X_{r+np}]$. This allows us to prove a Junod's conjecture for Meixner polynomials.

1 Introduction and results

Let n be a positive integer. The cycle indicator of the symmetric group S_n , is the polynomial C_n defined by

$$C_n = \sum c_n(m_1, \dots, m_n) \prod_{i=1}^n X_i^{m_i},$$

where the sum is over all non negative integers m_i such that $\sum_{i=1}^n im_i = n$, and

$$c_n(m_1, \dots, m_n) = \frac{n!}{\prod_{i=1}^n i^{m_i} (m_i!)}$$

MSC 2020: 11B65, 11A07, 11S05

Keywords: Congruences, cycle indicator, Meixner polynomials.

Affiliation:

Abdelaziz Bellagh (Corresponding author) – Faculté de Mathématiques, U.S.T.H.B,
 Laboratoire LATN, B.P 32, El ALIA, Bab Ezzouar, 16111, Alger, ALGÉRIE.

E-mail: abellagh@yahoo.fr

Assia Oulebsir – Faculté de Mathématiques, U.S.T.H.B, Laboratoire LATN, B.P 32, El
 ALIA, Bab Ezzouar, 16111, Alger, ALGÉRIE.

E-mail: oulebsir.assia@hotmail.com

If we set $C_0 = 1$, then the exponential generating function for C_n is

$$\exp\left(\sum_{i=1}^{\infty} X_i \frac{t^i}{i}\right) = \sum_{n=0}^{\infty} C_n(X_1, \dots, X_n) \frac{t^n}{n!}; \tag{1}$$

furthermore, the coefficients $c_n(m_1, \dots, m_n)$ of the polynomial C_n are integers; see Riordan [5, p. 67–68].

Carlitz [1, p 1222] proved, that for any prime p , and any positive integer n , and $m_1, \dots, m_{np} \in \{0, \dots, np\}$, such that $np = \sum_{i=1}^{np} im_i$, and for any non negative integer r , we have

$$c_{np}(m_1, \dots, m_{np}) \equiv \begin{cases} (-1)^{m_p} \binom{n}{m_p} \pmod{p\mathbb{Z}_p}, & \text{if } \sum_{i \notin \{1,p\}} m_i = 0, \\ 0 \pmod{p\mathbb{Z}_p}, & \text{if } \sum_{i \notin \{1,p\}} m_i \neq 0; \end{cases} \tag{2}$$

$$\text{and } C_{r+np} \equiv (X_1^p - X_p)^n C_r \pmod{p\mathbb{Z}_p[X_1, \dots, X_{r+np}]}, \tag{3}$$

where \mathbb{Z}_p is the ring of p -adic integers. We give the following generalization:

Proposition 1.1. *Let $r, n, p, m_1, \dots, m_{np}$ be as above, and let*

$$n^* = \begin{cases} n/2, & \text{if } n \in 2\mathbb{Z} \\ n, & \text{otherwise.} \end{cases}$$

1) *If $\sum_{i \notin \{1,p\}} m_i = 0$, then*

$$c_{np}(m_1, \dots, m_{np}) \equiv (-1)^{pm_p} \binom{n}{m_p} \pmod{n^*p\mathbb{Z}_p}. \tag{4}$$

2) *If $\sum_{i \notin \{1,p\}} m_i \neq 0$, then*

$$c_{np}(m_1, \dots, m_{np}) \equiv 0 \pmod{n^*p\mathbb{Z}_p}. \tag{5}$$

3) *The cycle indicator polynomials satisfy the congruence*

$$C_{r+np} \equiv (X_1^p - X_p)^n C_r \pmod{n^*p\mathbb{Z}_p[X_1, \dots, X_{r+np}]}. \tag{6}$$

Corollary 1.2. *Let p be a prime, and let n, r be positive integers such that $1 \leq r \leq p - 1$ and $r + np = \sum_{i=1}^{r+np} im_i$, where the m_i are non negative integers. We define n^* as in the proposition.*

a) *If $m_1 \geq p(n - m_p) \geq 0$, then we have the following congruence modulo $n^*p\mathbb{Z}_p$,*

$$c_{r+np}(m_1, \dots, m_{r+np}) \equiv (-1)^{pm_p} \binom{n}{m_p} c_r(m_1 + pm_p - np, m_2, \dots, m_r). \tag{7}$$

b) Otherwise, we have $c_{r+np}(m_1, \dots, m_{r+np}) \equiv 0 \pmod{n^*p\mathbb{Z}_p}$.

Remark 1.3. Under the hypotheses of Corollary 1.2, if $r + pn = m_1 + pm_p$ and if $n \geq m_p$, then we deduce from the congruences (4) and (7), that

$$c_{r+np}(m_1, 0, \dots, 0, m_p, 0, \dots, 0) \equiv c_{np}(m_1 - r, 0, \dots, 0, m_p, 0, \dots, 0) \pmod{n^*p\mathbb{Z}_p}$$

We will need the following lemma in the next corollary.

Lemma 1.4 (Junod [3]). *Let m, n be two positive integers, and let α, β be two elements of a commutative ring \mathcal{A} containing \mathbb{Z}_p .*

If $m \in p\mathbb{Z}$ and $\alpha \equiv \beta \pmod{m\mathcal{A}}$, then $\alpha^n \equiv \beta^n \pmod{mn\mathcal{A}}$.

Meixner polynomials are defined by their exponential generating function

$$\frac{1}{\sqrt{1+t^2}} \exp(X \arctan t) = \sum_{n=0}^{\infty} Q_n(X) \frac{t^n}{n!}.$$

Let Q_n^* be the polynomials defined by the exponential generating function

$$\exp(X \arctan t) = \sum_{n=0}^{\infty} Q_n^*(X) \frac{t^n}{n!}.$$

Junod [2, p 73], proved that, if $p \neq 2$, then

$$Q_{np}^*(X) \equiv Q_{np}(X) \pmod{np\mathbb{Z}_p[X]}, \text{ and} \tag{8}$$

$$Q_p(X) \equiv (X^p - (-1)^{(p-1)/2} X) \pmod{p\mathbb{Z}_p[X]}. \tag{9}$$

Since $X \arctan t = \sum_{i=1}^{\infty} x_i \frac{t^i}{i}$, where $x_i = 0$, when i is even, and $x_i = (-1)^{(i-1)/2} X$, when i is odd, it follows from equality (1), that $Q_n^*(X) = C_n(x_1, \dots, x_n)$, for any positive integer n . Using (6), (8), (9) and the lemma, we deduce that:

Corollary 1.5. *If $p \neq 2$, then*

$$Q_{np}(X) \equiv Q_p^n(X) \equiv (X^p - (-1)^{(p-1)/2} X)^n \pmod{np\mathbb{Z}_p[X]}.$$

This gives us a positive answer to a conjecture of Junod [2, p 74].

2 Proof of the proposition

For $n \notin p\mathbb{Z}$, the congruences (4) and (5) follow from (2), or from Macdonald [4, p 30]. Hence, we prove these congruences for $n \in p\mathbb{Z}$.

1) Let m be a non negative integer, then we have

$$\binom{np}{pm} \equiv \binom{n}{m} \pmod{np\mathbb{Z}_p}, \text{ and } pm \binom{n}{m} \equiv 0 \pmod{np\mathbb{Z}_p} \tag{10}$$

$$(mp)! = (-1)^{pm+1}\Gamma(pm + 1)(m!)p^m, \text{ and} \tag{11}$$

$$\Gamma(pm + 1) + 1 \in (pm/2)\mathbb{Z}_p, \tag{12}$$

where Γ denotes the Morita p -adic Gamma function; see Robert [4, p 369].

If $\sum_{i \notin \{1,p\}} m_i = 0$, then we have

$$c_{np}(m_1, \dots, m_{np}) = \frac{(np)!}{m_1!m_p!p^{m_p}} = \binom{np}{pm_p} \frac{(pm_p)!}{m_p!p^{m_p}}.$$

Hence the congruence (4) follows from (10), (11) and (12). Furthermore, in this case, $c_{np}(m_1, \dots, m_{np})$ and $\binom{n}{m_p}$ have the same p -adic valuation, since

$$c_{np}(m_1, \dots, m_{np}) = (-1)^{pm_p} \binom{n}{m_p} \frac{\Gamma(np + 1)}{\Gamma(m_1 + 1)}. \tag{13}$$

2) Now we prove by induction on the p -adic valuation ν of n , that if $np = \sum_{i=1}^{np} im_i$ and if there exists $i \in \{2, \dots, np\} - \{p\}$ such that $m_i \neq 0$, then the congruence (5) is satisfied. For $\nu = 0$, the congruence (5) is true. We assume the congruence (5) holds for $\nu - 1 \geq 0$.

First, we consider the case where p does not divide m_i . Then we have

$$np - i = i(m_i - 1) + \sum_{\substack{j=1 \\ j \neq i}}^{np-i} jm_j, \text{ and}$$

$$c_{np}(m_1, \dots, m_{np}) = \left(\frac{np(np-1) \cdots (np-i+1)}{im_i} \right) c', \text{ where}$$

$$c' = \begin{cases} c_{np-i}(m_1, \dots, m_{i-1}, m_i - 1, m_{i+1}, \dots, m_{np-i}), & \text{if } np \geq 2i, \\ c_{np-i}(m_1, \dots, m_{np-i}), & \text{if } np < 2i \text{ and } m_i = 1. \end{cases}$$

Then, we note that $(np - 1) \cdots (np - i + 1) \in (i/2)\mathbb{Z}_p$.

Indeed, if μ is the p -adic valuation of i , and if $\mu \geq 2$ with $i \neq 4$, we have

$$(np - 1) \cdots (np - i + 1) \in (np - p^{\mu-1} - p) \prod_{j=1}^{\mu-1} (np - p^j)\mathbb{Z}_p.$$

Hence the congruence (5) follows (in this case, we do not need the induction hypothesis).

On the other hand, if for all $j \notin \{1, p\}$, we have that p divides m_j , then p divides m_1 . Hence, if we set $m_j = pm'_j$ for any $j \neq p$, we obtain that

$$n = (m'_1 + m_p) + \sum_{\substack{j=2 \\ j \neq p}}^n jm'_j.$$

By (11), we get

$$c_{np}(m_1, \dots, m_{np}) = uz \binom{m_p + m'_1}{m_p} c', \text{ where}$$

$$u = (-1)^{np+1} \Gamma(pn + 1) \prod_{\substack{j=1 \\ j \neq p}}^n \Gamma(m'_j p + 1)^{-1} (-1)^{pm'_j+1},$$

$$z = \prod_{\substack{j=2 \\ j \neq p}}^n p^{(j-1)m'_j} j^{-m'_j(p-1)}, \text{ and}$$

$$c' = c_n(m'_1 + m_p, m'_2, \dots, m'_{p-1}, 0, m'_{p+1}, \dots, m'_n).$$

Since the p -adic Gamma function takes its values in the set of invertible elements in the ring \mathbb{Z}_p , we deduce that the p -adic valuation of u is zero. Then we remark that if μ denotes the p -adic valuation of a positive integer i such that $i \notin \{1, p\}$, we have $i - 1 > (p - 1)\mu$. Hence $z \in p\mathbb{Z}_p$. By the induction hypothesis (on the p -adic valuation ν of n), we have $c' \in (n/p)^* p\mathbb{Z}_p$. Since $(n/p)^* p \in n^* \mathbb{Z}_p$, we conclude that the congruence (5) holds for ν .

3) Using the congruences (4) and (5), we get

$$C_{np} \equiv \sum_{m_1 + pm_p = np} (-1)^{pm_p} \binom{n}{m_p} X_1^{m_1} X_p^{m_p} \pmod{n^* p\mathbb{Z}_p[X_1, \dots, X_{np}]},$$

$$\equiv (X_1^p + (-1)^p X_p)^n \pmod{n^* p\mathbb{Z}_p[X_1, \dots, X_{np}]}.$$
(14)

In particular, if ν is the p -adic valuation of n , we have

$$C_{p^{\nu+1}} \equiv (X_1^p + (-1)^p X_p)^{p^\nu} \pmod{n^* p\mathbb{Z}_p[X_1, \dots, X_{np}]}.$$
(15)

Deriving equality (1) with respect to t , we obtain that for any positive integer m , we have

$$C_m = \sum_{j=0}^{m-1} \frac{(m-1)!}{j!} X_{m-j} C_j = \begin{vmatrix} X_1 & -1 & 0 & 0 \\ X_2 & X_1 & -2 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ X_{m-1} & X_{m-2} & X_{m-3} & -(m-1) \\ X_m & X_{m-1} & X_{m-2} & X_1 \end{vmatrix}$$
(16)

(by expanding the determinant by the last row).

Taking $k = n/p^\nu$, $m = r + np$, and reducing the identity (16) modulo $p^{\nu+1}$, we get

$$C_{r+kp^{\nu+1}} \equiv C_r (C_{p^{\nu+1}})^k \pmod{p^{\nu+1} \mathbb{Z}_p[X_1, \dots, X_m]}.$$

Using (15), we deduce the congruence (6). □

Remark 2.1. If $p \neq 2$, $(p - 1)! \not\equiv -1 \pmod{p^2 \mathbb{Z}}$ (i.e., if p is not a Wilson's prime), and if $n \in p\mathbb{Z}$, the congruence (4), does not hold modulo $n p^2 \mathbb{Z}_p$. Indeed, by (13), we have for $m_p = 1$,

$$c_{np}(m_1, \dots, m_{np}) - (-1)^{pm_p} \binom{n}{m_p} = n(1 - q).$$

where $q = \frac{\Gamma(np + 1)}{\Gamma(m_1 + 1)} = -\prod_{j=1}^{p-1} (np - j) \equiv -\prod_{j=1}^{p-1} j \pmod{p^2\mathbb{Z}}$.

References

- [1] Carlitz. L: Some congruences for the Bell polynomials. *Pacific Math. J* Vol. 11 (No. 4) (1961) 1215–1222.
- [2] Junod.A: Congruences par l'analyse p -adique et le calcul symbolique. Thèse de Doctorat Université de Neuchâtel. (2003).
- [3] Junod.A: Congruences pour les polynômes et nombres de Bell. *Bulletin de la Société Mathématique de Belgique* (No. 9) (2002) 503–509.
- [4] Macdonald.I.G: *Symmetric function and Hall polynomials*. Oxford science publications mathematical monographs (1995).
- [5] Riordan.J: *An introduction to combinatorial analysis*. John Wiley and Sons, Inc, New York, London, Sydney (1967).
- [6] Robert.A: *A course in p -adic analysis*. Springer-Verlag, New York-Heidelberg (1999).

Received: June 19, 2021

Accepted for publication: October 08, 2021

Communicated by: Pasha Zusmanovich