Séminaire Lotharingien de Combinatoire **86B** (2022)
Article #81, 10 pp.

Proceedings of the 34th Conference on Formal Power Series and Algebraic Combinatorics (Bangalore)

Derangements and the p-Adic Incomplete Gamma Function

Andrew O'Desky[1] and David Harry Richman[*2]

[1] *Department of Mathematics, Princeton University, Princeton NJ, USA*
[2] *Department of Mathematics, University of Washington, Seattle WA, USA*

Abstract. The derangement-counting sequence satisfies strong p-adic regularity properties. We prove that these p-adic properties generalize to various other derangement-like sequences. To fit these observations into a unified framework, we show the existence of a p-adic analogue of the incomplete gamma function.

Keywords: derangement, incomplete gamma function, p-adic numbers

1 Introduction

A *derangement* on a finite set is a permutation with no fixed points. The number of derangements on n elements is

$$d(n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!, \tag{1.1}$$

which follows from inclusion-exclusion. The first few values of the derangement-counting sequence $d(n)$ are given in Table 1.

n	0	1	2	3	4	5	6	7	8	9
d(n)	1	0	1	2	9	44	265	1854	14833	133496

Table 1: Number of derangements.

Can we use the values of $d(n)$ on nonnegative integers $n \in \mathbb{N}$ to extrapolate a function $d(x)$ on some larger domain of inputs? For example, what value can be reasonably assigned to $d(1/3)$ or to $d(-1)$?

One route to answering this question is via the following observation.

Observation 1. *The function $f(n) = (-1)^n d(n)$ is* congruence preserving *in the sense that*

$$a \equiv b \pmod{m} \qquad \textit{implies} \qquad f(a) \equiv f(b) \pmod{m} \tag{1.2}$$

for any nonnegative integers a, b, m.

*hrichman@uw.edu

This observation was noted by Wright [15, Theorem 1] and Barsky [2, Proposition 5]. In the language of p-adic analysis, Observaton 1 implies that $(-1)^n d(n)$ is p-adically continuous for every prime p. (Moreover, it is Lipschitz continuous with Lipschitz constant 1.) Since $\mathbb{N}$ is dense in $\mathbb{Z}_p$, it follows that there is a unique continuous extension $f(x) = (-1)^x d(x)$ defined on $\mathbb{Z}_p$, interpolating values of f on $\mathbb{N}$. This p-adic extension can be used to define $d(-1) \in \mathbb{Z}_p$ for any p, and $(-1)^{1/3} d(1/3) \in \mathbb{Z}_p$ for any $p \neq 3$.

We now describe another "classical" example of looking at a combinatorial sequence under a p-adic lens. An *arrangement* on a finite set $[n]$ is a choice of subset $A \subset [n]$ and a choice of permutation on A. The number of arrangements on $[n]$ is

$$a(n) = \sum_{k=0}^{n} \binom{n}{k} k!. \tag{1.3}$$

n	0	1	2	3	4	5	6	7	8	9
$a(n)$	1	2	5	16	65	326	1957	13700	109601	986410

Table 2: Number of arrangements.

Observation 2. *The function $a(n)$ is congruence preserving in the sense of* (1.2).

This observation was noted by Hall [7, Corollary 2], who also made note of the floor function identity $a(n) = \lfloor e\, n! \rfloor$ when $n \geq 1$. In [7] Hall investigates general properties of the set of all congruence preserving functions $\mathbb{N} \to \mathbb{Z}$, and calls such functions *pseudo-polynomials*; it contains the polynomials $\mathbb{Z}[x]$ as a strict subset.

In this article, which is an extended abstract for [12], we describe several new extensions of this phenomenon, where a combinatorially-defined sequence satisfies strong p-adic regularity. These extensions are described in Sections 1.1 and 1.2. In Section 1.3, we describe how to construct a continuous, two-variable p-adic function which is a natural analogue to the incomplete gamma function.

1.1 r-cyclic derangements and arrangements

Let C_r denote the cyclic group of order r. The wreath product $C_r \wr S_n$ can be realized as the subgroup of $GL_n(\mathbb{C})$ generated by the permutation matrices and the diagonal matrices of (multiplicative) order r; it is a finite group of order $r^n n!$.

The action of the symmetric group S_n on the finite set $[n]$ generalizes to a natural action of $C_r \wr S_n$ on the set $[r] \times [n]$. In the matrix representation described above, the set $[r] \times [n]$ can be identified with the orbit of the unit coordinate vectors in $\mathbb{C}^n$. We say an element of $C_r \wr S_n$ is an *r-cyclic derangement* if its action on $[r] \times [n]$ has no fixed points. For example, the 2-cyclic derangements for $n = 2$ correspond to the matrices

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

The study of such generalized derangements was initiated by Faliharimalala–Zeng [4, Equation (2.7)] and Assaf [1, Theorem 2.1], who gave the following expression for the number of r-cyclic derangements:

$$d(n,r) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} r^{n-k} (n-k)!. \tag{1.4}$$

(For an interesting q-analogue extension of (1.4), see [5, Equation (2.5)].)

We similarly define an *r-cyclic arrangement* on $[r] \times [n]$ as a choice of subset $A \subset [n]$ and an element of $C_r \wr S_{|A|}$. The number of r-cyclic arrangements on $[r] \times [n]$ is

$$a(n,r) = \sum_{k=0}^{n} \binom{n}{k} r^k k!. \tag{1.5}$$

The p-adic regularity of derangements and arrangements extend to $d(n,r)$ and $a(n,r)$, for each choice of r.

Theorem 3. *Let p be a prime.*

1. *For any positive integer r, the function $n \mapsto (-1)^n d(n,r)$ is p-adically continuous.*
2. *For any positive integer r, the function $n \mapsto a(n,r)$ is p-adically continuous.*

For convenience, the two cases of Theorem 3 may be combined into a single one: when r is replaced with a negative integer $-r$ in the expression (1.5), we obtain

$$a(n,-r) := \sum_{k=0}^{n} \binom{n}{k} (-r)^k k! = (-1)^n d(n,r).$$

We also note that the upper limit in the sum (1.5) may be extended to infinity without changing the value $a(n,r) = \sum_{k=0}^{\infty} \binom{n}{k} r^k k!$, since the terms with $k > n$ all vanish. We will return to the expression $a(n,r)$ in Section 1.3.

1.2 Cycle restricted permutations

A derangement is a permutation whose cycle type has no length-1 cycles. More generally, we may be interested in the class of permutations whose cycle type is restricted to having lengths in a given set. For any set of positive integers L, let

$$d^L(n) = \#(\text{permutations in } S_n \text{ with cycle lengths in } L). \tag{1.6}$$

We call such permutations counted by $d^L(n)$ the *cycle restricted permutations* of L. Thus the usual derangement numbers satisfy $d(n) = d^L(n)$ for $L = \{2, 3, 4, \ldots\}$, and counting all permutations we have $n! = d^L(n)$ for $L = \mathbb{N}^+$.

Theorem 4. *Let L be a set of positive integers, and let $d^L(n)$ be defined by (1.6). Let p denote a prime. For $p \geq 3$:*

1. *$d^L(n)$ is p-adically continuous if and only if $1 \in L$ and $p \notin L$.*
2. *$(-1)^n d^L(n)$ is p-adically continuous if and only if $1 \notin L$ and $p \in L$.*

   In the case $p = 2$: $(-1)^n$ is 2-adically continuous, and

3. *$d^L(n)$ is 2-adically continuous if and only if $1 \in L$ and $2 \notin L$, or $1 \notin L$ and $2 \in L$.*

For example, let $\{3^i\} := \{1, 3, 9, 27, \ldots\}$ denote the set of powers of 3; the initial values of $d^{\{3^i\}}(n)$ are shown in Table 3. The function $n \mapsto d^{\{3^i\}}(n)$ can be p-adically interpolated by a continuous function on $\mathbb{Z}_p$ if and only if $p \neq 3$.

n	0	1	2	3	4	5	6	7	8	9
$d^{\{3^i\}}(n)$	1	1	1	3	9	21	81	351	1233	46089

Table 3: Number of $\{3^i\}$-cycle restricted permutations.

An essential step to proving Theorem 4 is the following formal power series identity.

Proposition 5. *Let $d^L(n)$ be defined by (1.6). Then the exponential generating function of $d^L(n)$ factors as*

$$\sum_{n \geq 0} d^L(n) \frac{X^n}{n!} = \prod_{r \in L} \exp\left(\frac{X^r}{r}\right).$$

The proof is a convenient application of combinatorial species (see [11, §1] for a quick introduction or [3] for a comprehensive treatment). To connect Proposition 5 to Theorem 4, we apply Mahler's criterion for p-adic continuity as described in Section 2.

1.3 A p-adic incomplete gamma function

Just as the values of the gamma function at positive integers count permutations, the values of the incomplete gamma function essentially count r-cyclic arrangements and derangements on $[r] \times [n]$ (see Section 1.1). The p-adic regularity of Theorem 3 can be strengthened to p-adic continuity in both variables of $a(n, r)$ jointly, and this leads to a construction for a p-adic incomplete gamma function.

Recall that the (upper) incomplete gamma function $\Gamma(s,z)$ is defined for $s,z \in \mathbb{R}$, $z > 0$, by the integral

$$\Gamma(s,z) = \int_z^\infty t^s \exp(-t)\frac{dt}{t}. \tag{1.7}$$

(The function $\Gamma(s,z)$ may be extended to $s,z \in \mathbb{C}$ by analytic continuation.) In analogy with the classical formula $\Gamma(n+1) = n!$ we may verify that

$$\Gamma(n+1, 1/r) = a(n,r)r^{-n}e^{-1/r} \tag{1.8}$$

for $(n,r) \in \mathbb{N} \times \mathbb{Z} \setminus \{0\}$, where $a(n,r)$ is given by (1.5). Recall that $a(n,r)$ counts r-cyclic arrangements if $r > 0$, resp. $(-r)$-cyclic derangements if $r < 0$.

Equation (1.8) shows that the p-adic continuity of the incomplete gamma function essentially reduces to the p-adic continuity of $a(n,r)$. Theorem 3 may be strengthened to observe that $a(n,r)$ is jointly continuous in both arguments p-adically. As a technicality to deal with the transcendental factor $e^{-1/r}$ in (1.8), we need to choose a field homomorphism $\tau_p\colon \mathbb{Q}(e) \to \mathbb{Q}_p$. For this choice we let $\tau_p(1/e) = \sum_{k\geq 0} p^k/k!$.

Theorem 6. *There exists a unique continuous function $\Gamma_p\colon \mathbb{Z}_p \times (1 + p\mathbb{Z}_p) \to \mathbb{Z}_p$ satisfying*

$$\Gamma_p(n, 1/r) = \tau_p\Gamma(n, 1/r)$$

for any positive integers n and r satisfying $r \equiv 1 \pmod p$. Explicitly, for any $s \in \mathbb{Z}_p$ and $z \in 1 + p\mathbb{Z}_p$ we have

$$\Gamma_p(s,z) = \exp_p(pz)z^{s-1}\sum_{k=0}^{\infty}\binom{s-1}{k}z^{-k}k!, \tag{1.9}$$

where $\exp_p(x) = \sum_{k\geq 0} x^k/k!$ is the p-adic exponential function on $\mathbb{Z}_p$.

We hope that the p-adic incomplete gamma function constructed in Theorem 6 may have interesting applications in number theory. See Section 3 for related discussion.

2 p-adic continuity

In this section we briefly recall some results from p-adic analysis. For more background we refer to [13, 14]. For an introduction to p-adic numbers, see [8].

Given a function $f\colon \mathbb{N} \to \mathbb{Q}$, the basic question of p-adic interpolation is whether f extends to a continuous function $\widetilde{f}\colon \mathbb{Z}_p \to \mathbb{Q}_p$. This question is generally approached using Mahler expansions and finite differences.

2.1 Mahler expansion

For a nonnegative integer k, let $\binom{x}{k} \in \mathbb{Q}[x]$ denote the polynomial

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}.$$

The polynomials $\{\binom{x}{k} : k = 0, 1, 2, \ldots\}$ form a basis of $\mathbb{Q}[x]$ as a $\mathbb{Q}$-vector space.

Definition 7. A *Mahler series* is an expression of the form $\sum_{k\geq 0} c_k \binom{x}{k}$ where $c_k \in \mathbb{Q}$. A function f admits a *Mahler expansion* if there are constants c_k such that

$$f(x) = \sum_{k\geq 0} c_k \binom{x}{k} = c_0 + c_1 \binom{x}{1} + c_2 \binom{x}{2} + \cdots$$

for all x in the domain of f. The constants c_k are the *Mahler coefficients* of f.

It is helpful to think of Mahler expansions as a "discrete analogue" to Taylor expansions in calculus. A function on the domain $\mathbb{Z}$ or $\mathbb{Z}_p$ may fail to admit a Mahler expansion, but a function on $\mathbb{N}$ always has a Mahler expansion. Finding a Mahler expansion for a function $f : \mathbb{N} \to \mathbb{Q}$ means to solve for c_k in the system of equations

$$f(n) = \sum_{k=0}^{n} \binom{n}{k} c_k \qquad \text{for } n = 0, 1, 2, \ldots. \tag{2.1}$$

The constant coefficient is simply $c_0 = f(0)$, and the other coefficients can be found using finite differences. The *finite difference operator* Δ is defined by

$$\Delta f(x) = f(x+1) - f(x).$$

Applied to the polynomial $\binom{x}{k}$, we have the familiar combinatorial identity $\Delta\binom{x}{k} = \binom{x+1}{k} - \binom{x}{k} = \binom{x}{k-1}$. Taking iterated finite differences, we have $\Delta^i\binom{n}{k} = \binom{n}{k-i}$ if $i \leq k$ and 0 otherwise. Assuming that $f(x) = \sum_{k\geq 0} c_k \binom{x}{k}$, we have

$$\Delta^i f(x) = \sum_{k\geq i} c_k \binom{x}{k-i} = c_i + c_{i+1}\binom{x}{1} + c_{i+2}\binom{x}{2} + \cdots$$

hence

$$c_n = \Delta^n f(0) = \sum_k (-1)^k \binom{n}{k} f(n-k) \qquad \text{for } n = 0, 1, 2, \ldots \tag{2.2}$$

yields a solution to (2.1). To summarize, we have shown that an arbitrary function $f : \mathbb{N} \to \mathbb{Q}$ has Mahler coefficients given by (2.2)

The question of which $f : \mathbb{N} \to \mathbb{Q}$ admit a continuous extension to $\mathbb{Z}_p \to \mathbb{Q}_p$ was conveniently answered by Mahler, using Mahler coefficients. Let $|\cdot|_p : \mathbb{Z}_p \to \mathbb{R}$ denote the p-adic absolute value.

Theorem 8 (Mahler [9, Lemma 1, Theorem 1]). *Suppose $f : \mathbb{N} \to \mathbb{Q}$ is a function with Mahler coefficients c_k. Then f extends to a continuous function $\widetilde{f} : \mathbb{Z}_p \to \mathbb{Q}_p$ if and only if $|c_k|_p \to 0$ as $k \to \infty$.*

For example, the function $f(n) = 3^n$ has Mahler coefficients

$$c_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} 3^{n-k} = (3-1)^n = 2^n.$$

By Mahler's theorem, 3^x extends continuously to $x \in \mathbb{Z}_p$ if and only if $|2^n|_p \to 0$ as $n \to \infty$, which occurs if and only if $p = 2$. A similar argument shows that $(-1)^x$ extends continuously to $x \in \mathbb{Z}_p$ if and only if $p = 2$.

2.2 Exponential generating functions

The relation between a function's values $f(n) =: a_n$ and its Mahler coefficients c_n has a convenient expression using exponential generating functions (EGFs). The exponential generating function of a sequence (a_n) is the formal power series

$$\sum_{n=0}^{\infty} a_n \frac{X^n}{n!} \in \mathbb{Q}[[X]].$$

Proposition 9. *Consider two sequences (a_n) and (c_n) of rational numbers, with associated EGFs*

$$A(X) = \sum_{n \geq 0} a_n \frac{X^n}{n!}, \qquad C(X) = \sum_{n \geq 0} c_n \frac{X^n}{n!}.$$

Then the following are equivalent:

1. *(c_n) are the Mahler coefficients of the function $f(n) = a_n$;*
2. *$a_n = \sum_{k=0}^{n} \binom{n}{k} c_k$;*
3. *$c_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} a_k$;*
4. *$A(X) = \exp(X) C(X)$, where $\exp(X) = \sum_{n \geq 0} \frac{X^n}{n!}$.*

2.3 Analyzing cycle restricted permutations

To deduce Theorem 4 from Proposition 5, we need to combine the following statements. Recall that for a set L of cycle lengths, the counts of cycle restricted permutations $d^L(n)$ satisfy the generating function identity

$$\sum_{n \geq 0} d^L(n) \frac{X^n}{n!} = \prod_{r \in L} \exp\left(\frac{X^r}{r}\right).$$

Thus we focus our attention on individual factors $\exp\left(\frac{X^r}{r}\right)$ for $r \in \mathbb{N}^+$, or for slightly more generality their integer powers $\exp\left(\frac{mX^r}{r}\right)$ for $m \in \mathbb{Z}$.

Proposition 10. *Let r be a positive integer and $m \in \mathbb{Z}$. Consider the formal power series*

$$\sum_{n\geq 0} c_n \frac{X^n}{n!} := \exp\left(\frac{mX^r}{r}\right).$$

1. *If $r = 1$ or p, then $|c_n|_p \to 0$ as $n \to \infty$ if and only if p divides m.*
2. *If $r \neq 1$ or p, then $|c_n|_p \to 0$ as $n \to \infty$.*

We then address the case of an infinite product of factors of this type.

Proposition 11. *Let $m_1, m_2, \ldots \in \mathbb{Z}$, and consider the formal power series in $\mathbb{Q}_p[[X]]$ defined by the infinite product*

$$\sum_{n\geq 0} c_n \frac{X^n}{n!} := \prod_{r=1}^{\infty} \exp\left(\frac{m_r X^r}{r}\right). \tag{2.3}$$

Then the EGF coefficients c_n satisfy $|c_n|_p \to 0$ as $n \to \infty$ if and only if $m_1 \equiv m_p \pmod{p}$.

We leave the details of the proof in [12] for the interested reader.

3 Parallel story: factorials and the gamma function

The factorial $n!$ counts the number of permutations on a finite set of n elements. The first few values are shown in Table 4.

n	0	1	2	3	4	5	6	7	8	9
$n!$	1	1	2	6	24	120	720	5040	40320	362880

Table 4: Number of permutations.

The question of whether the values $n!$ can be interpolated over $\mathbb{R}$ (or $\mathbb{C}$) is classical, going back to Euler and Gauss. The gamma function $\Gamma(s)$ is defined for positive real s by the integral

$$\Gamma(s) = \int_0^{\infty} t^s \exp(-t) \frac{dt}{t}, \tag{3.1}$$

and satisfies $\Gamma(n+1) = n!$. (Compare to (1.7) earlier.) The function $\Gamma(s)$ can be extended by analytic continuation to a meromorphic function on $s \in \mathbb{C}$.

The question of whether $n!$ can be interpolated p-adically is more recent. It is straightforward to compute the Mahler coefficients of the factorial function

$$n! = 1 + 1\binom{n}{2} + 2\binom{n}{3} + 9\binom{n}{4} + 44\binom{n}{5} + \cdots ; \tag{3.2}$$

these coefficients in fact coincide with the derangement numbers $d(n)$ (cf. Table 1). The p-adic absolute value $|d(n)|_p$ does not decay as $n \to \infty$ for any prime p, so the function $n \mapsto n!$ is not p-adically continuous by Mahler's theorem.

Morita [10] discovered that it is possible to p-adically interpolate a "factorial-like" function, after making the following tweaks:

$$\Gamma_p^{Mor}(n+1) = (-1)^{n+1} \prod_{\substack{1 \le k \le n \\ p \nmid k}} k. \tag{3.3}$$

Namely, an alternating sign is introduced, and integer multiples of p are left out of the product. The formula (3.3) defines a p-adic continuous function $\Gamma_p^{Mor} \colon \mathbb{Z}_p \to \mathbb{Z}_p$. Morita's p-adic analogue of the gamma function was found to satisfy various nice arithmetic formulas, see, *e.g.*, Gross–Koblitz [6].

Since the gamma function in the classical (Archimedean) case is reached by taking a limit in one argument of the incomplete gamma function, namely $\Gamma(s) = \lim_{z \to 0} \Gamma(s, z)$, it is natural to expect a nice relation between Morita's p-adic gamma function (or perhaps another p-adic gamma function analogue) and the p-adic incomplete gamma function constructed in Section 1.3. Such a relation is currently beyond our understanding. We hope to explore this in future work.

Acknowledgements

We thank Sami Assaf, Daniel Barsky, A. Suki Dasher, Jeffrey Lagarias, and Julian Rosen for helpful comments, corrections, and inspiration for this work.

References

[1] S. H. Assaf. "Cyclic derangements". *Electron. J. Combin.* **17**.1 (2010), Research Paper 163, 14. Link.

[2] D. Barsky. "Analyse p-adique et suites classiques de nombres". *Sém. Lothar. Combin.* (1981).

[3] F. Bergeron, G. Labelle, and P. Leroux. *Combinatorial species and tree-like structures*. Vol. 67. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1998, pp. xx+457.

[4] H. L. M. Faliharimalala and J. Zeng. "Derangements and Euler's difference table for $C_l \wr S_n$". *Electron. J. Combin.* **15**.1 (2008), Research paper 65, 22. Link.

[5] H. L. M. Faliharimalala and J. Zeng. "Fix-Euler–Mahonian statistics on wreath products". *Adv. in Appl. Math.* **46**.1-4 (2011), pp. 275–295. DOI.

[6] B. H. Gross and N. Koblitz. "Gauss sums and the p-adic Γ-function". *Ann. of Math. (2)* **109**.3 (1979), pp. 569–581. DOI.

[7] R. R. Hall. "On pseudo-polynomials". *Mathematika* **18** (1971), pp. 71–77. DOI.

[8] N. Koblitz. *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*. Second. Vol. 58. Graduate Texts in Mathematics. Springer-Verlag, New York, 1984, pp. xii+150. DOI.

[9] K. Mahler. "An interpolation series for continuous functions of a p-adic variable". *J. Reine Angew. Math.* **199** (1958), pp. 23–34. DOI.

[10] Y. Morita. "A p-adic analogue of the Γ-function". *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **22**.2 (1975), pp. 255–266.

[11] A. M. Nelson. "A generalized cyclotomic identity". *Adv. Math.* **83**.1 (1990), pp. 1–29. DOI.

[12] A. O'Desky and D. H. Richman. "Derangements and the p-adic incomplete gamma function". *Trans. Amer. Math. Soc.* (2020). To appear. arXiv:2012.04615.

[13] A. M. Robert. *A Course in p-Adic Analysis*. Vol. 198. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. xvi+437. DOI.

[14] W. H. Schikhof. *Ultrametric calculus*. Vol. 4. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2006, pp. xii+306.

[15] E. M. Wright. "Arithmetical properties of Euler's rencontre number". *J. London Math. Soc. (2)* **4** (1971/72), pp. 437–442. DOI.