Doubling modulo odd integers, generalizations, and unexpected occurrences

Jean-Paul Allouche[1], Manon Stipulanti[‡2], and Jia-Yan Yao[§3]

[1]CNRS, IMJ-PRG, Sorbonne Université, Paris, France,
jean-paul.allouche@imj-prg.fr
[2]Department of Mathematics, University of Liège, Belgium,
m.stipulanti@uliege.be
[3]Department of Mathematics, Tsinghua University, Beijing 100084, People's Republic of China, jyyao@mail.tsinghua.edu.cn

May 22, 2025

A tribute to the memory of Jacques Roubaud 1932–2024

Abstract

The starting point of this work is an equality between two quantities A and B found in the literature, which involve the *doubling-modulo-an-odd-integer* map, i.e., $x \in \mathbb{N} \mapsto 2x \bmod (2n+1)$ for some positive integer n. More precisely, this doubling map defines a permutation $\sigma_{2,n}$ and each of A and B counts the number $C_2(n)$ of cycles of $\sigma_{2,n}$, hence $A = B$. In the first part of this note, we give a direct proof of this last equality. To do so, we consider and study a generalized (k,n)-perfect shuffle permutation $\sigma_{k,n}$, where we multiply by an integer $k \geq 2$ instead of 2, and its number $C_k(n)$ of cycles. The second part of this note lists some of the many occurrences and applications of the doubling map and its generalizations in the literature: in mathematics (combinatorics of words, dynamical systems, number theory, correcting algorithms), but also in card-shuffling, juggling, bell-ringing, poetry, and music composition.

Keywords: Modular arithmetic, multiplicative order, permutations, cycles, perfect shuffle, combinatorics of words, card-shuffling, juggling, bell-ringing, poetry, music composition

2020 Mathematics Subject Classification: 11B50, 11B83, (primary); 05A05, 05A19, 11A25, 20B30, 20B99, 00A65 (secondary)

1 Introduction

The starting point of this note was the observation that the permutation τ_m (for some odd integer $m \geq 3$) occurring in the 2021 paper [28] by Guo, Han, and Wu, and defined on $[0, m-2]$ by

$$\tau_m := \begin{pmatrix} 0 & 1 & \cdots & \frac{m-3}{2} & \frac{m-1}{2} & \frac{m+1}{2} & \cdots & m-2 \\ 1 & 3 & \cdots & m-2 & 0 & 2 & \cdots & m-3 \end{pmatrix}, \tag{1}$$

[‡]Manon Stipulanti is an FNRS Research Associate supported by the FNRS research grant 1.C.104.24F.
[§]Jia-Yan Yao is partially supported by the National Natural Science Foundation of China (Grant No. 12231013).

is the same (up to notation) as the permutation σ_n (for some integer $n \geq 1$) occurring in the 1983-1984 paper [4] by Allouche, and defined on $[1, 2n]$ by

$$\sigma_n := \begin{pmatrix} 1 & 2 & \cdots & n & n+1 & n+2 & \cdots & 2n \\ 2 & 4 & \cdots & 2n & 1 & 3 & \cdots & 2n-1 \end{pmatrix}. \tag{2}$$

(For slightly more on these two papers, see Section 5.1 below.) The fact that these permutations are the same up to notation can be seen, e.g., from the fact that the first one can be defined by $i \to 2i+1 \bmod m$ (for each $i \in [0, m-2]$), while the second one can be defined by $j \to 2j \bmod (2n+1)$ (for each $j \in [1, 2n]$). In particular, the number of cycles in the decomposition into a product of disjoint cycles of τ_m is given in [28] by

$$-1 + \frac{1}{\mathsf{ord}(2,m)} \sum_{j=0}^{\mathsf{ord}(2,m)-1} \gcd(2^j - 1, m), \tag{3}$$

while it is given in [4] by

$$\sum_{\substack{d \mid m \\ d \neq 1}} \frac{\varphi(d)}{\mathsf{ord}(2,d)}, \tag{4}$$

where φ is the Euler totient function and, for each odd integer ℓ, $\mathsf{ord}(2, \ell)$ is the multiplicative order of 2 modulo ℓ. (See precise definitions in the next section.)

The quantities in (3) and (4) are equal since they count the same objects. While wanting to give a direct proof of their equality, i.e., without associating them with counting some objects, we came across many occurrences of the innocent-looking map

$$x \in \mathbb{N} \mapsto 2x \bmod (2n+1), \tag{5}$$

where n is a fixed positive integer, as accounted below in Section 5. The previous map is naturally called *doubling modulo an odd integer*. The purpose of this note is twofold. First, we propose direct proofs of the equality between the quantities in (3) and (4), as a particular case of our Proposition 3.2 with Corollary 3.4. Before doing so, we consider in Section 2 a permutation, noted $\sigma_{k,n}$, that generalizes σ_n from (2), and describe the number $C_k(n)$ of cycles in the decomposition of $\sigma_{k,n}$ into a product of disjoint cycles. Proposition 3.2 is then showed in Section 3, for which we give two proofs with different flavors. In Section 4, we study the asymptotics of the related sequence $(C_k(n))_{n \geq 1}$ for each value of k. Finally, in Section 5, we review some of many manifestations and applications of the doubling-modulo-odd-integers map of (5) and its generalizations, as well as some numerous occurrences of the quantity defined in (4) that we have found in the literature.

1.1 Notation

For all integers $k \geq 2$ and $n \geq 1$, we define the (k, n)-*perfect shuffle permutation* to be the permutation $\sigma_{k,n} \colon x \mapsto kx \bmod (kn+1)$ for $x \in [1, kn]$ (we take its name after [23]). The case $k = 2$ corresponds to the permutation σ_n from (2), which is also called the *perfect shuffle permutation of order* $2n$ in [24].

Example 1.1. For $k = 2$ and $n = 3$, we have $\sigma_{2,3} \colon 1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 6, 4 \mapsto 1, 5 \mapsto 3, 6 \mapsto 5$.

In particular, we are interested in the decomposition of $\sigma_{k,n}$ into a product of disjoint cycles. For all integers $k \geq 2$ and $n \geq 1$, we let $C_k(n)$ be the number of cycles in the decomposition of the permutation $\sigma_{k,n}$ into a product of disjoint cycles. By *cycles*, we mean cycles of all lengths, even singletons that correspond to elements fixed by the permutation.

Example 1.2. The decomposition of $\sigma_{2,3}$ into cycles gives $\sigma_{2,3} = (124)(365)$, so $C_2(3) = 2$. The cycles in the decomposition of $\sigma_{3,5}$ are (1 3 9 11), (2 6), (4 12), (5 15 13 7), (8), and (10 14) with respective length $4, 2, 2, 4, 1, 2$, so $C_3(5) = 6$.

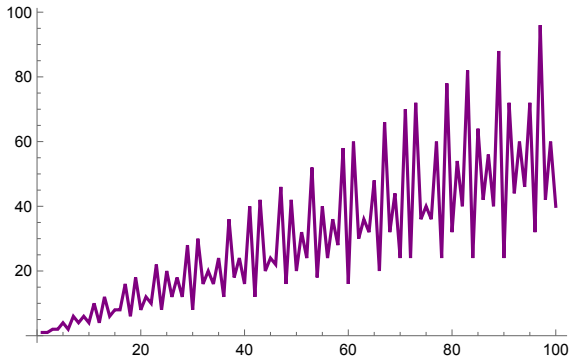

Figure 1: The first few values of Euler's totient function φ.

For various values of k, we have computed in Table 1 the first few terms of the sequence $(C_k(n))_{n\geq 1}$. The sequence corresponding to $k=2$ is [63, A006694], while the others do not seem to be indexed in Sloane's OEIS [63].

k	$(C_k(n))_{n\geq 1}$
2	$1,1,2,2,1,1,4,2,1,5,2,2,3,1,6,4,5,1,4,2,\ldots$
3	$2,1,3,4,6,1,5,2,6,1,3,2,12,1,5,2,14,5,3,6,\ldots$
4	$2,4,2,4,8,4,2,8,2,4,14,4,2,8,2,12,8,8,8,8,\ldots$
5	$3,2,7,4,7,10,11,2,3,4,13,2,11,14,11,4,3,10,25,4,\ldots$
6	$3,1,2,8,5,9,14,6,9,1,2,2,1,9,10,8,1,1,14,2,\ldots$
7	$4,5,3,4,14,7,13,20,16,1,11,6,6,9,5,8,38,1,3,8,\ldots$

Table 1: For $k\in[2,7]$, the first few terms of the sequence $(C_k(n))_{n\geq 1}$, where $C_k(n)$ gives the number of cycles in the decomposition of the permutation $\sigma_{k,n}$ into a product of disjoint cycles.

To obtain several descriptions of the quantity $C_k(n)$, we introduce some notation. For two integers $a,b\geq 1$, we let $\gcd(a,b)$ denote their greatest common divisor. We also set $\gcd(0,b)=b$ if $b\neq 0$. For a finite set A, we let $\#A$ denote the number of elements of A, i.e.,

$$\#A=\sum_{k\in A}1. \tag{6}$$

We let φ denote the Euler totient function defined, for an integer $n\geq 1$, by the number of integers in the interval $[1,n]$ that are coprime with n, i.e., $\varphi(n)=\#\{k\in[1,n]\mid \gcd(k,n)=1\}$. See Fig. 1 for the first few values of the Euler totient function, which is also sequence A000010 in Sloane's OEIS [63]. We recall (and reprove) the next well-known formula (e.g., see [66, Relation (33), page 32]) that will be useful later on.

Lemma 1.3. *For each integer $n\geq 1$, we have $\sum_{d|n}\varphi(d)=n$.*

Proof. Let us quickly recall how to prove this equality. We may proceed as follows

$$n=\sum_{1\leq k\leq n}1=\sum_{d|n}\sum_{\substack{1\leq k\leq n\\ \gcd(k,n)=d}}1=\sum_{d|n}\sum_{\substack{1\leq k'\leq n/d\\ \gcd(k',n/d)=1}}1=\sum_{d|n}\varphi(n/d)=\sum_{d'|n}\varphi(d'),$$

where the last equality is obtained via the classical change of summation index $d'=n/d$. □

Given a positive integer n and an integer a coprime to n, we let $\mathsf{ord}(a,n)$ be the *multiplicative order of a modulo n*, which is the smallest positive integer ℓ such that $a^\ell\equiv 1 \bmod n$. Note

that $\mathsf{ord}(a,1) = 1$ for each integer $a \geq 2$. For example, the sequence $(\mathsf{ord}(2, 2n+1))_{n\geq 0}$ starts with $1, 2, 4, 3, 6, 10, 12$; it is sequence A002326 in Sloane's OEIS [63]. We let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the multiplicative group of invertible elements of $\mathbb{Z}/n\mathbb{Z}$. Recall that an integer k is a *primitive root modulo* n if k is a generator of the multiplicative group of integers modulo n, i.e., if for every integer a coprime to n, there is some integer ℓ for which $k^\ell \equiv a \bmod n$. In particular, for k to be a primitive root modulo n, a necessary and sufficient condition is that $\mathsf{ord}(k,n) = \varphi(n)$.

2 A first interpretation and an incursion into permutation group theory

One way of interpreting the quantity $C_k(n)$ is the following one. Also see [4, 24] for the particular case $k = 2$.

Proposition 2.1. *For all integers $k \geq 2$ and $n \geq 1$, the number $C_k(n)$ of cycles in the decomposition of the permutation $\sigma_{k,n}$ into a product of disjoint cycles is equal to*

$$\sum_{\substack{d \mid kn+1 \\ d \neq 1}} \frac{\varphi(d)}{\mathsf{ord}(k,d)}.$$

Example 2.2. With $k = 3$ and $n = 5$, recall from Example 1.2 that the cycles of $\sigma_{k,n}$ are (1 3 9 11), (2 6), (4 12), (5 15 13 7), (8), and (10 14). Their number is given by

$$C_k(n) = \sum_{\substack{d \mid kn+1 \\ d \neq 1}} \frac{\varphi(d)}{\mathsf{ord}(k,d)} = \frac{1}{1} + \frac{2}{2} + \frac{4}{2} + \frac{8}{4} = 6.$$

Proof of Proposition 2.1. The cardinality of the orbit of $j \in [1, kn]$ under $\sigma_{k,n}$ is

$$\mathsf{ord}\left(k, \frac{kn+1}{\gcd(j, kn+1)}\right),$$

which is the smallest integer $s \geq 1$ such that $k^s j \equiv j \bmod (kn+1)$. (We note that if two elements i, j are in the same orbit, then $\gcd(i, kn+1) = \gcd(j, kn+1)$, since k and $kn+1$ are coprime; this follows from an adaptation of [24, Proposition 1] to the general case.) So, letting $d = \gcd(j, kn+1)$, the cycles in the decomposition of $\sigma_{k,n}$ have length

$$\mathsf{ord}\left(k, \frac{kn+1}{d}\right), \tag{7}$$

where d divides $(kn+1)$ and $d \neq kn+1$ (since $d = \gcd(j, kn+1)$ and $1 \leq j \leq kn$). Furthermore, the number of cycles with that particular length is

$$\frac{\varphi\left(\frac{kn+1}{d}\right)}{\mathsf{ord}\left(k, \frac{kn+1}{d}\right)}. \tag{8}$$

So, the number of cycles in the decomposition of the permutation $\sigma_{k,n}$ into a product of disjoint cycles is equal to

$$C_k(n) = \sum_{\substack{d \mid kn+1 \\ d \neq kn+1}} \frac{\varphi\left(\frac{kn+1}{d}\right)}{\mathsf{ord}\left(k, \frac{kn+1}{d}\right)},$$

which, after the change of the summation index $d' = (kn+1)/d$, yields the expected equality. □

d	a	cycles
3	1	(5 10)
	2	(10 5)
5	1	(3 6 12 9)
	2	(6 12 9 3)
	3	(9 3 6 12)
	4	(12 9 3 6)

d	a	cycles
15	1	(1 2 4 8)
	2	(2 4 8 1)
	4	(4 8 1 2)
	7	(7 14 13 11)
	8	(8 1 2 4)
	11	(11 7 14 13)
	13	(13 11 7 14)
	14	(14 13 11 7)

Table 2: For $k = 2$ and $n = 7$, we use Theorem 2.4 to obtain the cycles of the permutation $\sigma_{k,n}$.

Due to the proof of the previous result (in particular (7) and (8)), we obtain the following information on the cycles of the permutation $\sigma_{k,n}$.

Corollary 2.3. *Let $k \geq 2$ and $n \geq 1$ be integers. For each divisor d of $kn+1$ with $d \neq 1$, the permutation $\sigma_{k,n}$ possesses $\varphi(d)/\mathsf{ord}(k,d)$ cycles of length $\mathsf{ord}(k,d)$ in its decomposition into a product of disjoint cycles.*

In fact, the structure of the cycles in the (n,k)-perfect shuffle permutation is precisely described in [23, Theorem 1] restated below. Furthermore, the authors provide a linear-time algorithm to compute representatives of the cycles, which they call *seeds* (the *seed set* contains integers in $[1, kn]$ such that no two seeds are in the same cycle and every cycle contains a seed).

Theorem 2.4 ([23, Theorem 1])**.** *Let $k \geq 2$ and $n \geq 1$ be integers. The r-tuple $(a_0, a_1, \ldots, a_{r-1})$ with $r \geq 1$ is a cycle of the (n,k)-perfect shuffle permutation if and only if there exist a divisor d of $kn+1$ with $d \neq 1$ and an element $a \in [1, d-1]$ (coprime with d) such that $r = \mathsf{ord}(k,d)$ and $a_i = \frac{a(kn+1)}{d} k^i \bmod (kn+1)$ for $i \in [0, r-1]$.*

Proof. We repeat the proof of Proposition 2.1, but with more precision. Let $(a_0, a_1, \ldots, a_{r-1})$ be a cycle of the (n,k)-perfect shuffle permutation with $r \geq 1$. By definition, this is equivalent to saying that there exists an integer $j \in [1, kn]$ such that $a_i \equiv jk^i \mod (kn+1)$ $(0 \leq i < r)$, where r is the smallest integer $s \geq 1$ such that $jk^s \equiv j \bmod (kn+1)$. Put $d = \frac{kn+1}{\gcd(j, kn+1)}$, and write $j = a \gcd(j, kn+1)$ for some integer a. Then $d \neq 1$, since $j < kn+1$. Also note here that $1 \leq a < d$, $\gcd(a,d) = 1$, and r is the smallest integer $s \geq 1$ such that $(k^s - 1)a \equiv 0 \bmod d$. Hence $r = \mathsf{ord}(k,d)$, for a and d are coprime. The above argument can be reversed, so the desired result holds. □

Example 2.5. Let $k = 2$ and $n = 7$. The lengths of the cycles in the decomposition of the permutation $\sigma_{k,n}$ as a product of disjoint cycles belong to $\{\mathsf{ord}(k,d) \mid d \text{ divides } (kn+1) \text{ and } d \neq 1\} = \{2, 4\}$ due to Corollary 2.3. They are (1 2 4 8), (3 6 12 9), (5 10), and (7 14 13 11). The divisors of $kn + 1 = 15$ are $1, 3, 5, 15$. According to Theorem 2.4, we show in Table 2 all possible values of d and a to build the cycles of $\sigma_{k,n}$. Observe that the same cycle is rotated to obtain another cycle. Seed sets are, e.g., $\{1, 3, 5, 7\}$ and $\{2, 3, 10, 7\}$.

The *order* of a permutation σ is the smallest number of times the permutation must be applied to return to the identity permutation, i.e., the smallest integer ℓ such that $\sigma^\ell = \mathrm{id}$. In fact, the order of σ is equal to the least common multiple of the lengths of cycles in its decomposition into a product of disjoint cycles.

Proposition 2.6. *For all integers $k \geq 2$ and $n \geq 1$, the order of the permutation $\sigma_{k,n}$ is $\mathsf{ord}(k, kn+1)$.*

Proof. Using Corollary 2.3, we obtain that the order of the permutation $\sigma_{k,n}$ is given by

$$L = \mathrm{lcm}\{\mathsf{ord}(k,d) \mid d \text{ is a divisor of } kn+1 \text{ and } d \neq 1\}. \tag{9}$$

To prove the statement, we show that $L = \mathsf{ord}(k, kn+1)$. For the sake of conciseness, let us write $\theta(d) = \mathsf{ord}(k,d)$ for a divisor d of $kn+1$. By minimality of $\theta(d)$, we have that $\theta(d)$ divides $\theta(kn+1)$ when d divides $kn+1$ (indeed, in this case, since $k^{\theta(kn+1)} - 1$ is a multiple of $kn+1$, then $k^{\theta(kn+1)} - 1$ is also a multiple of d), hence $L = \theta(kn+1)$ by the formula (9). □

Example 2.7. Resuming Example 2.5, we find that the order of the permutation $\sigma_{k,n}$ is given by $\mathrm{lcm}\{2,4\} = 4$.

Given a permutation σ on $[0,n]$, an *inversion* is a pair $\{i,j\}$ of elements in $[0,n]$ such that $i < j$ implies $\sigma(i) > \sigma(j)$. The permutation σ is *even* (resp., *odd*) if its number of inversions is even (resp., odd). The *signature* $\mathrm{sign}(\sigma)$ of σ is equal to 1 (resp., -1) if σ is even (resp., odd). Looking again at Table 1, we may compute the signature of the first few permutations $\sigma_{k,n}$: for $k \in \{2,3,6,7\}$, we obtain the sequence of signatures $-1,-1,1,1$ and for $k \in \{4,5\}$, the signature is always 1. We propose two ways to compute the signature of $\sigma_{k,n}$, one direct and the other using Corollary 2.3.

Proposition 2.8. *For all integers $k \geq 2$ and $n \geq 1$, the number of inversions of the permutation $\sigma_{k,n}$ is given by $\frac{(k-1)k}{2} \cdot \frac{n(n+1)}{2}$. In particular, for each $k \geq 2$, the sequence $(\mathrm{sign}(\sigma_{k,n}))_{n\geq 1}$ of signatures of the permutation $\sigma_{k,n}$ is periodic with periods given by*

$$\begin{cases} (-1,-1,1,1), & \text{if } k \equiv 2 \bmod 4; \\ (-1,-1,1,1), & \text{if } k \equiv 3 \bmod 4; \\ (1), & \text{if } k \equiv 0 \bmod 4; \\ (1), & \text{if } k \equiv 1 \bmod 4. \end{cases}$$

Proof. For each $\ell \in [1,k]$, define I_ℓ to be the interval of integers $[(\ell-1)n+1, \ell n]$. We note that we have $\sigma_{k,n}(x) = kx - (\ell-1)(kn+1)$ for $x \in I_\ell$ and $\ell \in [1,k]$. (For example, $\sigma_{3,n}$ maps x to $3x$ if $x \in [1,n]$, to $3x-(3n+1)$ if $x \in [n+1,2n]$, and to $3x-2(3n+1)$ if $x \in [2n+1,3n]$.) The pair $\{i,j\}$ cannot be an inversion unless $i \in I_\ell$ and $j \in I_{\ell'}$ with $\ell, \ell' \in [1,k]$ and $\ell < \ell'$. Couting these pairs of ℓ, ℓ' gives

$$\sum_{\ell=1}^{k-1} (k-\ell) = \sum_{\ell=1}^{k-1} \ell = \frac{(k-1)k}{2}.$$

After analyzing the behavior of the map $\sigma_{k,n}$, the number of inversions $\{i,j\}$ with $i \in I_\ell$, $j \in I_{\ell'}$, $\ell, \ell' \in [1,k]$, and $\ell < \ell'$ is

$$\sum_{m=1}^{n} m = \frac{n(n+1)}{2}.$$

Indeed if we write $i = (\ell-1)n+m$ and $j = (\ell'-1)n+m'$ with $1 \leq m, m' \leq n$, then $\sigma_{k,n}(i) > \sigma_{k,n}(j)$ if and only if $k(m'-m) < \ell' - \ell < k$, which means $1 \leq m' \leq m$. Putting together these two quantities gives the first part of the statement.

To get the second part of the statement, it is enough to carefully analyze, for all integers $k \geq 2$ and $n \geq 1$, the parity of $\frac{(k-1)k}{2} \cdot \frac{n(n+1)}{2}$. □

Corollary 2.9. *For all integers $k \geq 2$ and $n \geq 1$, the signature of the permutation $\sigma_{k,n}$ is determined by the parity of $kn - C_k(n)$.*

k	2	3	4	5	6	7
Queneau-like numbers w.r.t k in $[1,20]$	$1,2,5,6,9,14,18$	$2,6,10,14$	$\emptyset$	$\emptyset$	$2,10,13,17,18$	$10,18$

Table 3: For $k \in [2,7]$, the first few Queneau-like numbers with respect to k.

Proof. Recall that a length-ℓ cycle is an even (resp., odd) permutation if ℓ is odd (resp., even). Thus, using Corollary 2.3, we know that the signature of $\sigma_{k,n}$ is determined by the parity of

$$\sum_{\substack{d|kn+1\\ d\neq 1}} \frac{\varphi(d)}{\mathsf{ord}(k,d)}(\mathsf{ord}(k,d)-1) = \sum_{\substack{d|kn+1\\ d\neq 1}} \varphi(d) - \sum_{\substack{d|kn+1\\ d\neq 1}} \frac{\varphi(d)}{\mathsf{ord}(k,d)} = kn - C_k(n),$$

where, for the last equality, we used Lemma 1.3 and Proposition 2.1. □

We note that combining the previous two results allows us to determine the parity of the number $C_k(n)$ for all integers $k \geq 2$ and $n \geq 1$.

Given an integer $n \geq 1$, let us consider the permutation μ_n over $[1,n]$ that maps x to $\frac{x}{2}$ if x is even, and $n - \frac{x-1}{2}$ otherwise, and referred to as the *Queneau-Daniel permutation* [15]. An integer n is a *Queneau number* if the corresponding permutation μ_n is a cycle of length n. The first few Queneau numbers are $1,2,3,5,6,9,11,14,18$ (also see [63, A054639]). They were first analyzed by Queneau, then Bringer proposed a first systematic mathematical study of these numbers and their generalizations [15]; then they were fully characterized by Dumas [22], also see [69], the history in [61], and the survey [8]. In the case of the permutation $\sigma_{k,n}$ one could ask a similar question, i.e., for which integers n do we have $C_k(n) = 1$? We call these integers *Queneau-like numbers with respect to k*. In view of Table 1, we are able to compute the first few Queneau-like numbers with respect to the first few values of $k \in [2,7]$ in Table 3. Queneau-like numbers with respect to $k = 2$ are related to the sequence [63, A163782] (see Corollary 2.12 below); the other sequences of Queneau-like numbers do not seem to appear in the OEIS [63]. We obtain the following characterization of Queneau-like numbers.

Proposition 2.10. *Let $k \geq 2$ and $n \geq 1$ be integers. The following are equivalent.*

(1) The integer n is a Queneau-like number with respect to k.

(2) The permutation $\sigma_{k,n}$ is a cycle of length kn.

(3) The integer $kn+1$ is a prime number and k is a primitive root modulo $(kn+1)$.

(4) The multiplicative order of k modulo $(kn+1)$ is kn, i.e., $\mathsf{ord}(k, kn+1) = kn$.

Proof. The equivalence (1) ⇔ (2) follows from the definition of Queneau-like numbers.

We show (2) ⇔ (3). We first note that the permutation $\sigma_{k,n}$ is a cycle of length kn if and only if $C_k(n) = 1$. Using Proposition 2.1, we obtain that this condition is equivalent to ask that

$$\sum_{\substack{d|kn+1\\ d\neq 1}} \frac{\varphi(d)}{\mathsf{ord}(k,d)} = 1.$$

As each term in the sum is a positive number, $C_k(n) = 1$ if and only if $kn+1$ is a prime and $\frac{\varphi(kn+1)}{\mathsf{ord}(k,kn+1)} = 1$. As the multiplicative group $(\mathbb{Z}/(kn+1)\mathbb{Z})^*$ is of cardinality $\varphi(kn+1)$, we obtain that the last part of the condition is equivalent to asking that k is a primitive root modulo $kn+1$, as desired.

We finally show that (2) ⇔ (4). Due to the previous paragraph, Item (2) rewrites: $kn+1$ is a prime and $\mathsf{ord}(k, kn+1) = kn$, by definition of the Euler totient function. Now we show that the

n	1	2	3	4	5
μ_{2n}	(1 2)	(1 4 2), (3)	(1 6 3 5 4 2)	(1 8 4 2), (3 7 5 6)	(1 10 5 8 4 2), (3 9 6), (7)
$\sigma_{2,n}$	(1 2)	(1 2 4 3)	(1 2 4), (3 6 5)	(1 2 4 8 7 5), (3 6)	(1 2 4 8 5 10 9 7 3 6)

Table 4: For $n \in [1, 5]$, we compare the cycle decomposition of the Queneau-Daniel permutation μ_{2n} and our $(2, n)$-perfect shuffle permutation $\sigma_{2,n}$.

first part of the latter condition is superfluous. Suppose that $\mathsf{ord}(k, kn + 1) = kn$. We always have that $\gcd(k, kn+1) = 1$, thus k and its powers are invertible modulo $kn+1$. If $\mathsf{ord}(k, kn + 1) = kn$, this means that the multiplicative group generated by k has cardinality kn, thus is equal to the set of all non-zero elements of $\mathbb{Z}/(kn + 1)\mathbb{Z}$. In particular, all non-zero elements of $\mathbb{Z}/(kn + 1)\mathbb{Z}$ are invertible, so $kn + 1$ is a prime number, as desired. □

Remark 2.11. An alternative proof of the equivalence between Items (2) and (4) of Proposition 2.10 is to use Theorem 2.4. Indeed, we notably want to find a divisor d of $kn + 1$ with $d \neq 1$ such that $kn = \mathsf{ord}(k, d)$. If $d \neq kn + 1$, then $d < kn$ and the condition cannot be fulfilled; so $d = kn + 1$, as expected.

We note that Item (3) reminds us of the result from [4, Corollaires page 8] for the case $k = 2$.

While we are able to eliminate the condition that $kn + 1$ is a prime number when assuming Item (4) of Proposition 2.10, we note that it may happen that k is a primitive root modulo $kn+1$ but $kn + 1$ is not a prime number. For example, for $k = 2$ and $n = 4$, we have that $2n + 1 = 9$ is composite but 2 generates $(\mathbb{Z}/9\mathbb{Z})^\times$.

We also note the following question: let us fix some integer $k \geq 2$; then, is the set of Queneau-like numbers with respect to k infinite? Due to Item (4), we ask whether k is a primitive root modulo infinitely many primes of the form $kn + 1$. This is a difficult question to answer since it is related to Artin's primitive root conjecture of 1927 (see the survey [44]).

We end this remark by mentioning *conjugate permutations*. Recall that two permutations σ and τ are *conjugates* if there exists a permutation π such that $\tau = \pi\sigma\pi^{-1}$, where we let π^{-1} denote the *inverse (permutation)* of π. It is clear that conjugate permutations share the same number of cycles in their decomposition into disjoint cycles and their cycles have the same lengths, although the actual elements in the cycles may differ (actually the converse is also true). In our case, the Queneau-Daniel permutation μ_{2n} and the $(2, n)$-perfect shuffle permutation $\sigma_{2,n}$ are not necessarily conjugate, e.g., see Table 4.

It turns out that Queneau-like numbers with respect to $k = 2$ are related to the famous Josephus problem (e.g., see [26, Section 1.3]). Let $n \geq 2$ be an integer and put the numbers from the interval $[1, n]$ on a circle. In a cyclic way, mark the second unmarked number until all n numbers are marked. For example, with $n = 6$, we mark 2, then 4, 6, 3, 1, and finally 5. Considering the permutation defined by the order in which the numbers are marked, we say that n is a *J_2-prime number* if this permutation consists of a single cycle of length n. For every $k \geq 2$, *J_k-prime numbers* are defined analogously by marking every kth number instead. The sequences of J_k-primes for $k \in [2, 20]$ are indexed by [63, A163782-A163800]. We next show that J_2-primes are Queneau-like numbers with respect to $k = 2$, and vice versa. For larger values k, we note that our Queneau-like numbers with respect to k differ from J_k-primes.

Corollary 2.12. *Let $n \geq 2$ be integer. Then n is a J_2-prime number if and only if n is a Queneau-like number with respect to $k = 2$.*

Proof. By the equivalence (1) ⇔ (3) of Proposition 2.10, it suffices to show that an integer $n \geq 2$ is a J_2-prime number if and only if $2n + 1$ is a prime number and 2 generates $(\mathbb{Z}/(2n + 1)\mathbb{Z})^\times$. Recall that by [7, Theorem 5.12], an integer $n \geq 2$ is a J_2-prime number if and only if $2n + 1$ is a prime number and exactly one of the following two conditions holds:

(1) $n \equiv 1 \bmod 4$, and 2 generates $(\mathbb{Z}/(2n + 1)\mathbb{Z})^\times$, but -2 does not;

(2) $n \equiv 2 \bmod 4$, and both 2 and -2 generate $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$.

Hence if n is a J_2-prime number, then $2n+1$ is a prime number and 2 generates $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$, as desired.

Conversely, assume that $2n+1$ is prime and 2 generates $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$. We distinguish two cases below to show that n satisfies the sufficient condition of [7, Theorem 5.12], so that n is a J_2-prime number.

Case 1: First assume that $n \equiv 1, 2 \bmod 4$. Since $\mathsf{ord}(2, 2n+1) = 2n$ and $(2^n)^2 \equiv 1 \bmod (2n+1)$, we have $2^n \equiv -1 \bmod (2n+1)$, for $\mathbb{Z}/(2n+1)\mathbb{Z}$ is a field. If $n \equiv 1 \bmod 4$, then n is odd, and thus $(-2)^n \equiv 1 \bmod (2n+1)$, so -2 cannot generate $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$. If $n \equiv 2 \bmod 4$, then n is even, and we have $(-2)^n = 2^n \equiv -1 \bmod (2n+1)$, so $\mathsf{ord}(-2, 2n+1) = 2n$, and -2 generates $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$.

Case 2: Now assume that $n \equiv 0, 3 \bmod 4$. Then we can write $2n+1 = 8m \pm 1$ for some integer m. By [7, Proposition 3.9], there exists an integer $x \in \mathbb{Z}/(2n+1)\mathbb{Z}$ such that $x^2 \equiv 2 \bmod (2n+1)$. Since $2n+1$ is prime, the cardinality of $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$ is $2n$, so we have $2^n \equiv x^{2n} \equiv 1 \bmod (2n+1)$. This implies $2n = \mathsf{ord}(2, 2n+1) \leq n$, which is absurd and Case 2 cannot occur. □

Using the reasoning in the proof of Proposition 2.1 or Corollary 2.3, we obtain the following result. In particular, $C_k(n)$ gives the multiplicity of 1 as a zero of some polynomial (also see [4, Corollaires page 8] for the case $k = 2$).

Corollary 2.13. *Let $k \geq 2$ and $n \geq 1$ be integers and let $(e_1, e_2, \ldots, e_{kn})$ denote the canonical basis of $\mathbb{R}^{kn}$. Let $f_{k,n}$ be the endomorphism of $\mathbb{R}^{kn}$ defined by $f_{k,n}(e_j) := e_{\sigma_{k,n}(j)}$ for every integer $j \in [1, kn]$, where $\sigma_{k,n}$ is the (n,k)-perfect shuffle permutation defined above. Then the characteristic polynomial of $f_{k,n}$ is*

$$\chi_{f_{k,n}}(X) = \prod_{\substack{d \mid kn+1 \\ d \neq 1}} (X^{\mathsf{ord}(k,d)} - 1)^{\frac{\varphi(d)}{\mathsf{ord}(k,d)}}.$$

Proof. Let $M_{k,n}$ denote the matrix associated with $f_{k,n}$ in the canonical basis of $\mathbb{R}^{kn}$. From a classical result on the characteristic polynomial of a permutation matrix (e.g., see [3, Section 1]), we obtain

$$\chi_{f_{k,n}}(X) = \det(XI - M_{k,n}) = \prod_{\ell} (X^\ell - 1)^{c_\ell}, \tag{10}$$

where c_ℓ is the number of length-ℓ cycles in the decomposition of $\sigma_{k,n}$ in a product of cycles. (To prove (10), it is enough to reorder the elements $e_1, \ldots, e_{kn}$ following the cycles of the decomposition of $\sigma_{k,n}$: first, we start with the vectors $e_1, e_{\sigma_{k,n}(1)}, e_{\sigma^2_{k,n}(1)}, \ldots, e_{\sigma^{t-1}_{k,n}(1)}$, where t is the length of the cycle containing 1, then we choose a non-already-visited vector e_m, and so on and so forth.)

Using the reasoning in the proof of Proposition 2.1 leading to computing the possible lengths of cycles and numbers of fixed length cycles in $\sigma_{k,n}$ or Corollary 2.3, Equality (10) becomes

$$\chi_{f_{k,n}}(X) = \prod_{\substack{d \mid kn+1 \\ d \neq kn+1}} \left(X^{\mathsf{ord}\left(k, \frac{kn+1}{d}\right)} - 1\right)^{\varphi\left(\frac{kn+1}{d}\right)/\mathsf{ord}\left(k, \frac{kn+1}{d}\right)} = \prod_{\substack{d \mid kn+1 \\ d \neq 1}} \left(X^{\mathsf{ord}(k,d)} - 1\right)^{\frac{\varphi(d)}{\mathsf{ord}(k,d)}},$$

where the second equality is obtained after the change of index $d' = (kn+1)/d$. □

Example 2.14. We resume Example 2.2 for which $k = 3$ and $n = 5$. If we look at Equality (10), we have 1 length-1, 3 length-2 and 2 length-4 cycles in $\sigma_{k,n}$, so in the case the characteristic polynomial of $f_{k,n}$ is $(X-1)(X^2-1)^3(X^4-1)^2$. This coincides with the formula in Corollary 2.13 since we obtain

$$\left\{ \left(\mathsf{ord}(k,d), \frac{\varphi(d)}{\mathsf{ord}(k,d)} \right) \middle| \, d \text{ divides } kn+1 \text{ and } d \neq 1 \right\} = \{(1,1), (2,1), (2,2), (4,2)\}.$$

3 A second interpretation through arithmetic and algebra

For all integers $k \geq 2$ and $n \geq 1$, we define the quantity

$$i_k(n) := \sum_{d|n} \frac{\varphi(d)}{\mathsf{ord}(k,d)}. \tag{11}$$

Note that our definition is the same as the definition given in [19, 44, 45, 49], but slightly different from the one given in [57, 70]. For $k \in [2,7]$, the first few terms of the sequence $(i_k(kn+1))_{n\geq 1}$ are given in Table 5. The sequence corresponding to $k = 2$ is [63, A081844] (also see the related sequence [63, A000374]), while the others do not seem to be indexed in Sloane's OEIS [63]. Also note that $i_k(kn+1)$ and $C_k(n)$ only differ by 1.

k	$(i_k(kn+1))_{n\geq 1}$
2	$2, 2, 3, 3, 2, 2, 5, 3, 2, 6, 3, 3, 4, 2, 7, 5, 6, 2, 5, 3, \ldots$
3	$3, 2, 4, 5, 7, 2, 6, 3, 7, 2, 4, 3, 13, 2, 6, 3, 15, 6, 4, 7, \ldots$
4	$3, 5, 3, 5, 9, 5, 3, 9, 3, 5, 15, 5, 3, 9, 3, 13, 9, 9, 9, 9, \ldots$
5	$4, 3, 8, 5, 8, 11, 12, 3, 4, 5, 14, 3, 12, 15, 12, 5, 4, 11, 26, 5, \ldots$
6	$4, 2, 3, 9, 6, 10, 15, 7, 10, 2, 3, 3, 2, 10, 11, 9, 2, 2, 15, 3, \ldots$
7	$5, 6, 4, 5, 15, 8, 14, 21, 17, 2, 12, 7, 7, 10, 6, 9, 39, 2, 4, 9, \ldots$

Table 5: For $k \in [2,7]$, the first few terms of the sequence $(i_k(kn+1))_{n\geq 1}$.

Remark 3.1. If q is the order of a finite field, then, applying [45, Lemma 5] to the particular case where we look at divisors of $qn+1$ shows that $i_q(qn+1)$ gives the number of distinct irreducible factors of the polynomial $X^{qn+1}-1$ in $\mathbb{F}_q[X]$. For example, the sequence [63, A081844] corresponds to $q = 2$.

Another way to write $i_k(kn+1)$ (or $C_k(n)$) is the following one, to which we propose two independent proofs: one with an arithmetical flavor, the other on the algebraic side.

Proposition 3.2. *For all integers $k \geq 2$ and $n \geq 1$, we have*

$$i_k(kn+1) = \frac{1}{\mathsf{ord}(k,kn+1)} \sum_{j=0}^{\mathsf{ord}(k,kn+1)-1} \gcd(k^j - 1, kn+1).$$

Remark 3.3. Here we have used the usual convention that $\gcd(0,r) = r$ for every integer $r \geq 1$. Note that, for all integers $k \geq 2$ and $n \geq 1$, we also have

$$\sum_{j=0}^{\mathsf{ord}(k,kn+1)-1} \gcd(k^j - 1, kn+1) = \sum_{j=1}^{\mathsf{ord}(k,kn+1)} \gcd(k^j - 1, kn+1). \tag{12}$$

"Arithmetical" proof of Proposition 3.2. For every integer $n \geq 1$, we let $U(n)$ be the quantity

$$U(n) := \sum_{x=1}^{kn} A(x),$$

where $A(x) := \#\{j \in [0, \mathsf{ord}(k,kn+1)-1] \mid (k^j-1)x \equiv 0 \bmod (kn+1)\}$.

Fix some $j \in [0, \mathsf{ord}(k,kn+1)-1]$ and take $x \in [1,kn]$. We have

$$(k^j-1)x \equiv 0 \bmod (kn+1) \Leftrightarrow (k^j-1)x' \equiv 0 \bmod \left(\frac{kn+1}{\gcd(x,kn+1)}\right),$$

where $x' := \frac{x}{\gcd(x,kn+1)}$. Since $\gcd\Big(x', \frac{(kn+1)}{\gcd(x,kn+1)}\Big) = 1$, we get

$$(k^j-1)x' \equiv 0 \bmod \left(\frac{kn+1}{\gcd(x,kn+1)}\right) \Leftrightarrow (k^j-1) \equiv 0 \bmod \left(\frac{kn+1}{\gcd(x,kn+1)}\right).$$

Thus, we find

$$\begin{aligned} A(x) &= \#\left\{ j \in [0, \mathsf{ord}(k,kn+1)-1] \mid j \text{ is a multiple of } \mathsf{ord}\left(k, \frac{(kn+1)}{\gcd(x,kn+1)}\right)\right\} \\ &= \frac{\mathsf{ord}(k,kn+1)}{\mathsf{ord}\Big(k, \frac{kn+1}{\gcd(x,kn+1)}\Big)}. \end{aligned}$$

(We may even verify that $\mathsf{ord}\Big(k, \frac{kn+1}{\gcd(x,kn+1)}\Big)$ divides $\mathsf{ord}(k,kn+1)$.) Observing that $x \in [1,kn]$ implies that $\gcd(x,kn+1) < kn+1$, we obtain that

$$\begin{aligned} \frac{U(n)}{\mathsf{ord}(k,kn+1)} &= \sum_{x=1}^{kn} \frac{1}{\mathsf{ord}\Big(k, \frac{kn+1}{\gcd(x,kn+1)}\Big)} \\ &= \sum_{\substack{d \mid kn+1 \\ d \neq kn+1}} \sum_{\substack{1 \le x \le kn \\ \gcd(x,kn+1)=d}} \frac{1}{\mathsf{ord}\big(k, \frac{kn+1}{d}\big)} \\ &= \sum_{\substack{d \mid kn+1 \\ d \neq kn+1}} \frac{1}{\mathsf{ord}\big(k, \frac{kn+1}{d}\big)} \sum_{\substack{1 \le x < kn+1 \\ \gcd(x,kn+1)=d}} 1. \end{aligned}$$

We apply the change of index $x' = x/d$ to obtain

$$\frac{U(n)}{\mathsf{ord}(k,kn+1)} = \sum_{\substack{d \mid kn+1 \\ d \neq kn+1}} \frac{1}{\mathsf{ord}\big(k, \frac{kn+1}{d}\big)} \sum_{\substack{1 \le x' < (kn+1)/d \\ \gcd(x',(kn+1)/d)=1}} 1 = \sum_{\substack{d \mid kn+1 \\ d \neq kn+1}} \frac{\varphi\big(\frac{kn+1}{d}\big)}{\mathsf{ord}\big(k, \frac{kn+1}{d}\big)}$$

by definition of φ. Using the change of index $d' = (kn+1)/d$, we obtain

$$\frac{U(n)}{\mathsf{ord}(k,kn+1)} = \sum_{\substack{d \mid kn+1 \\ d \neq 1}} \frac{\varphi(d)}{\mathsf{ord}(k,d)}. \tag{13}$$

On the other hand, we can write

$$\begin{aligned} U(n) &= \#\{(j,x) \in [0, \mathsf{ord}(k,kn+1)-1] \times [1,kn] \mid (k^j-1)x \equiv 0 \bmod (kn+1)\} \\ &= \sum_{j=0}^{\mathsf{ord}(k,kn+1)-1} \#\{x \in [1,kn] \mid (k^j-1)x \equiv 0 \bmod (kn+1)\}, \end{aligned}$$

so that we have

$$U(n) = \sum_{j=0}^{\mathsf{ord}(k,kn+1)-1} \#\{x \in [1,kn] \mid (k^j-1)x \equiv 0 \bmod (kn+1)\}. \tag{14}$$

For $j \in [0, \mathsf{ord}(k,kn+1)-1]$, let $d := \gcd(k^j-1, kn+1)$. Since $(k^j-1)/d$ is coprime to $(kn+1)/d$, we have

$$(k^j-1)x \equiv 0 \bmod (kn+1) \Leftrightarrow \frac{k^j-1}{d}x \equiv 0 \bmod \frac{kn+1}{d} \Leftrightarrow x \equiv 0 \bmod \frac{kn+1}{d}.$$

This condition together with the fact that $1 \leq x < kn+1$ is equivalent to saying that there exists an integer $\lambda \in [1, d) = [1, d-1]$ such that $x = \lambda \frac{kn+1}{d}$. Therefore,

$$\begin{aligned}\#\{x \in [1, kn] \mid (k^j - 1)x \equiv 0 \bmod (kn+1)\} &= \#\left\{\lambda \in [1, d-1] \mid \lambda \frac{kn+1}{d} \in [1, kn+1)\right\} \\ &= d - 1 \\ &= \gcd(k^j - 1, kn+1) - 1,\end{aligned}$$

so using (14), we find

$$\frac{U(n)}{\mathsf{ord}(k, kn+1)} = \frac{1}{\mathsf{ord}(k, kn+1)} \left(\sum_{j=0}^{\mathsf{ord}(k,kn+1)-1} \gcd(k^j - 1, kn+1) \right) - 1. \tag{15}$$

Comparing (13) and (15) gives

$$\sum_{\substack{d \mid kn+1 \\ d \neq 1}} \frac{\varphi(d)}{\mathsf{ord}(k, d)} = \frac{1}{\mathsf{ord}(k, kn+1)} \left(\sum_{j=0}^{\mathsf{ord}(k,kn+1)-1} \gcd(k^j - 1, kn+1) \right) - 1,$$

which, after adding 1 on each side and re-absorbing it in the sum in the left-hand side as the term $\frac{\varphi(1)}{\mathsf{ord}(k,1)}$ for $d = 1$ equals 1, yields the desired result. □

Algebraic proof of Proposition 3.2. For the sake of readability, let $m = kn + 1$. The equality we need to prove is equivalent to

$$\sum_{d \mid m} \varphi(d) \frac{\mathsf{ord}(k, m)}{\mathsf{ord}(k, d)} = \sum_{j=0}^{\mathsf{ord}(k,m)-1} \gcd(k^j - 1, m). \tag{16}$$

Since k and m are coprime, k belongs to the group $(\mathbb{Z}/m\mathbb{Z})^\times$ of invertible elements of $\mathbb{Z}/m\mathbb{Z}$. Let $\langle k \rangle_m$ be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by k: it is a group of order $\mathsf{ord}(k, m)$.

Let d be a divisor of m. There exists a unique ring morphism from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/d\mathbb{Z}$, which is surjective and its kernel is the ideal $d(\mathbb{Z}/m\mathbb{Z})$. The induced morphism from $(\mathbb{Z}/m\mathbb{Z})^\times$ to $(\mathbb{Z}/d\mathbb{Z})^\times$ maps $\langle k \rangle_m$ to $\langle k \rangle_d$. Consequently, $\langle k \rangle_d$ is the quotient of $\langle k \rangle_m$ by the sub-group $\{y \in \langle k \rangle_m : y \equiv 1 \bmod d\}$. By Lagrange's theorem, the left-hand side of (16) becomes

$$\begin{aligned}\sum_{d \mid m} \varphi(d) \frac{\mathsf{ord}(k, m)}{\mathsf{ord}(k, d)} &= \sum_{d \mid m} \varphi(d) \frac{\#\langle k \rangle_m}{\#\langle k \rangle_d} \\ &= \sum_{d \mid m} \varphi(d) \cdot \#\{y \in \langle k \rangle_m \mid y \equiv 1 \bmod d\} \\ &= \sum_{d \mid m} \varphi(d) \cdot \#\{j \in [0, \mathsf{ord}(k, m) - 1] \mid d \text{ divides } (k^j - 1)\}.\end{aligned}$$

The formula in (6) yields

$$\sum_{d \mid m} \varphi(d) \frac{\mathsf{ord}(k, m)}{\mathsf{ord}(k, d)} = \sum_{j \in [0, \mathsf{ord}(k,m)-1]} \sum_{\substack{d \mid m \\ d \mid (k^j - 1)}} \varphi(d) = \sum_{j=0}^{\mathsf{ord}(k,m)-1} \sum_{d \mid \gcd(k^j - 1, m)} \varphi(d).$$

Now the formula of Lemma 1.3 gives the right-hand side of (16), as desired. □

Applying Proposition 3.2 to the specific case $k = 2$ gives the equality between (3) and (4).

Corollary 3.4. *For each odd integer $m \geq 3$, we have*

$$\sum_{\substack{d|m \\ d\neq 1}} \frac{\varphi(d)}{\mathsf{ord}(2,d)} = \left(\frac{1}{\mathsf{ord}(2,m)} \sum_{j=0}^{\mathsf{ord}(2,m)-1} \gcd(2^j-1,m) \right) - 1.$$

Proof. From Proposition 3.2 applied to the case $k=2$, we obtain

$$\sum_{d|m} \frac{\varphi(d)}{\mathsf{ord}(2,d)} = \frac{1}{\mathsf{ord}(2,m)} \sum_{j=0}^{\mathsf{ord}(2,m)-1} \gcd(2^j-1,m).$$

As the term corresponding to $d=1$ in the left-hand side of the previous equality is equal to $\frac{\varphi(d)}{\mathsf{ord}(2,d)} = 1$, we obtain the desired result. □

Actually a third quantity is equal to both members of the equality in Proposition 3.2. Before stating this equality in Corollary 3.7 below, we will give two lemmas.

Lemma 3.5 (Apostol)**.** *If a, b, m, n are positive integers with a and b relatively prime and $a > b$, then $\gcd(a^n - b^n, a^m - b^m) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$.*

Proof. This result is well-known for the particular case $b=1$ (which is actually the one we will use). The general case can be found as a problem posed in [32, page 49], with a solution given in [30, pages 86–87]. □

Lemma 3.6. *For all integers $k \geq 2$ and $n \geq 1$, we have the following equalities:*

$$\begin{aligned}\sum_{j=0}^{\mathsf{ord}(k,kn+1)-1} \gcd(k^j-1,kn+1) &= \sum_{j=1}^{\mathsf{ord}(k,kn+1)} \gcd(k^j-1,kn+1) \\ &= \sum_{d|\mathsf{ord}(k,kn+1)} \varphi\left(\frac{\mathsf{ord}(k,kn+1)}{d}\right) \gcd(k^d-1,kn+1).\end{aligned}$$

Proof. The first equality was already indicated in (12) of Remark 3.3. We now turn to the proof of the second equality. In order to simplify notation in the proof, we fix k and n, and we write $\theta := \theta(k,n) := \mathsf{ord}(k,kn+1)$ and, for the left-hand side of the equality that we want to prove,

$$A := A(k,n) := \sum_{1\leq j\leq \theta} \gcd(k^j-1,kn+1).$$

We group terms in A according to the value of $\gcd(\theta,j)$. Since the values of this gcd are divisors of θ, we have

$$A = \sum_{d|\theta} \sum_{\substack{1\leq j\leq \theta \\ \gcd(\theta,j)=d}} \gcd(k^j-1,kn+1). \tag{17}$$

Now, since we have $k^\theta \equiv 1 \bmod (kn+1)$, there exists a positive integer x such that $k^\theta - 1 = x(kn+1)$. Thus,

$$x\gcd(k^j-1,kn+1) = \gcd(x(k^j-1),x(kn+1)) = \gcd(x(k^j-1),k^\theta-1). \tag{18}$$

If we let $\gcd(\theta,j)=d$, we have that the right-hand side of (18) is equal to

$$\gcd(x(k^j-1),k^\theta-1) = (k^d-1)\gcd\left(x\frac{k^j-1}{k^d-1}, \frac{k^\theta-1}{k^d-1}\right). \tag{19}$$

By Lemma 3.5, we have $\gcd(k^j-1,k^\theta-1)=k^d-1$, so $\frac{k^j-1}{k^d-1}$ and $\frac{k^\theta-1}{k^d-1}$ are coprime. Thus, we have

$$\gcd\left(x\frac{k^j-1}{k^d-1},\frac{k^\theta-1}{k^d-1}\right)=\gcd\left(x,\frac{k^\theta-1}{k^d-1}\right)$$

and the right-hand side of (19) is equal to

$$\begin{aligned}\gcd(x(k^j-1),k^\theta-1)&=\gcd(x(k^d-1),k^\theta-1)=\gcd(x(k^d-1),x(kn+1))\\&=x\gcd(k^d-1,kn+1).\end{aligned}$$

Comparing with (18) yields $\gcd(k^j-1,kn+1)=\gcd(k^d-1,kn+1)$. Finally, (17) becomes

$$\begin{aligned}A&=\sum_{d\mid\theta}\sum_{\substack{1\le j\le\theta\\ \gcd(\theta,j)=d}}\gcd(k^d-1,kn+1)\\&=\sum_{d\mid\theta}\gcd(k^d-1,kn+1)\sum_{\substack{1\le j\le\theta\\ \gcd(\theta,j)=d}}1\\&=\sum_{d\mid\theta}\gcd(k^d-1,kn+1)\varphi\left(\frac{\theta}{d}\right),\end{aligned}$$

where, for the third equality, we have used that

$$\sum_{\substack{1\le j\le\theta\\ \gcd(\theta,j)=d}}1=\sum_{\substack{1\le j'\le\theta/d\\ \gcd(\theta/d,j')=1}}1\;=\;\varphi\left(\frac{\theta}{d}\right),$$

which finishes the proof. □

As a corollary and using Proposition 3.2, we have the following result, which is the case $a=k$ and $m=kn+1$ of [19, Theorem page 2].

Corollary 3.7. *For all integers $k\ge 2$ and $n\ge 1$, we have*

$$i_k(kn+1)=\frac{1}{\mathsf{ord}(k,kn+1)}\sum_{d\mid\mathsf{ord}(k,kn+1)}\varphi\left(\frac{\mathsf{ord}(k,kn+1)}{d}\right)\gcd(k^d-1,kn+1).$$

Remark 3.8. For an even more detailed study of various similar families of permutations, the reader can consult [47].

4 Asymptotics

Now we look at the asymptotics of the sequences $(C_k(n))_{n\ge1}$ and $(i_k(kn+1))_{n\ge1}$ (also see [4, Corollaires page 8] for the case $k=2$). In the following, we let log denote the natural logarithm (in base e). For two sequences $(U(n))_{n\ge0}$ and $(V(n))_{n\ge0}$, we also recall the notation $U(n)=O(V(n))$ if there exists a positive constant c such that $|U(n)|\le c|V(n)|$ for every sufficiently large n.

Proposition 4.1. *For all integers $k\ge2$ and $n\ge1$, we have*

$$C_k(n)=O\left(\frac{n}{\log n}\right)\ \text{and}\ \ i_k(kn+1)=O\left(\frac{n}{\log n}\right).$$

Proof. To prove the statement, the idea is to split the summation range in $i_k(kn+1)$ into two parts, one with "small" divisors of $kn+1$ and the other with "large" ones. More precisely, we separate the set of d's dividing $\mathsf{ord}(k,kn+1)$ into the set of d's that are less than or equal to

$(kn+1)^\alpha$ and the set of those with are larger than $(kn+1)^\alpha$ for some "small" α that will be chosen later on. Let us write

$$\sum_{d|kn+1} \frac{\varphi(d)}{\mathsf{ord}(k,d)} = S_1(n) + S_2(n),$$

with

$$S_1(n) := \sum_{\substack{d|kn+1 \\ d\le(kn+1)^\alpha}} \frac{\varphi(d)}{\mathsf{ord}(k,d)} \quad \text{and} \quad S_2(n) := \sum_{\substack{d|kn+1 \\ d>(kn+1)^\alpha}} \frac{\varphi(d)}{\mathsf{ord}(k,d)}.$$

To obtain the desired result, we bound each term S_1 and S_2.

To obtain an upper bound for S_1, we use the fact that $\mathsf{ord}(k,d) \ge 1$ and the observation that, if $d \le (kn+1)^\alpha$, then $\varphi(d) \le d \le (kn+1)^\alpha$. Therefore

$$S_1(n) \le (kn+1)^\alpha \left(\sum_{\substack{d|kn+1 \\ d\le(kn+1)^\alpha}} 1 \right) \le (kn+1)^\alpha \quad \#\{d \in [1, kn+1] \mid d \text{ divides } (kn+1)\}.$$

Since the number of divisors of a positive integer m satisfies the inequality

$$\#\{d \in [1,m] \mid d \text{ divides } m\} \le 2\sqrt{m}$$

(we may group the divisors of m pairwise, i.e., d and m/d, and one of them is $\le \sqrt{m}$), we have

$$S_1(n) \le 2(kn+1)^{\alpha+1/2} = O(n^{\alpha+1/2}) = O\Big(\frac{n}{\log n}\Big) \tag{20}$$

for $\alpha < 1/2$.

To obtain an upper bound for S_2, we note that if $k^\ell \equiv 1 \bmod d$ with $\ell \ne 0$ and $d \ne 1$, then $k^\ell \ge d+1$, so $\ell \ge \log(d+1)/\log k$. So, for the summation indices d that appear in $S_2(n)$, we have

$$\mathsf{ord}(k,d) \ge \frac{\log(d+1)}{\log k} \ge \frac{\alpha \log(kn+1)}{\log k},$$

since $d > (kn+1)^\alpha$. It follows that

$$S_2(n) \le \left(\sum_{\substack{d|kn+1 \\ d>(kn+1)^\alpha}} \varphi(d) \right) O\Big(\frac{1}{\log n}\Big) \le \left(\sum_{d|kn+1} \varphi(d) \right) O\Big(\frac{1}{\log n}\Big) = (kn+1)\, O\Big(\frac{1}{\log n}\Big),$$

where we used the well-known formula of Lemma 1.3 for the last equality. We obtain

$$S_2(n) = O\Big(\frac{n}{\log n}\Big). \tag{21}$$

Putting together (20) and (21) gives the desired asymptotics results. □

Remark 4.2. We note that [4, Corollaires page 8] already indicates the optimality of the previous bound for $(C_2(n))_{n\ge1}$. Here we show that, more generally, $n/\log n$ is the *right order of magnitude* for $i_k(kn+1)$. Namely, let $\ell \ge 2$ be an integer, and set $n := k^\ell - k^{\ell-1} - 1$. Thus, $kn+1 = (k^\ell-1)(k-1)$. In particular, if d divides $(k^\ell-1)$, then d also divides $(kn+1)$, and furthermore $\mathsf{ord}(k,d) \le \mathsf{ord}\big(k, k^\ell-1\big) \le \ell$. Hence we get

$$i_k(kn+1) = \sum_{d|(kn+1)} \frac{\varphi(d)}{\mathsf{ord}(k,d)} \ge \sum_{d|(k^\ell-1)} \frac{\varphi(d)}{\mathsf{ord}(k,d)} \ge \sum_{d|(k^\ell-1)} \frac{\varphi(d)}{\ell} = \frac{k^\ell-1}{\ell},$$

where Lemma 1.3 is used for the last equality. Now, we are done, since when $\ell \to \infty$, which implies that $n \to \infty$, we have

$$\frac{k^\ell - 1}{\ell} \sim \frac{k^\ell}{\ell} \quad \text{and} \quad \frac{n}{\log n} \sim \left(\frac{k-1}{k \log k}\right) \frac{k^\ell}{\ell},$$

where, as usual, the notation $f(x) \sim g(x)$ means that $f(x)/g(x)$ tends to 1, when x goes to infinity.

5 Unexpected occurrences of doubling modulo odd integers and other occurrences of the map i_k

In this section we propose to review some other occurrences of the doubling-modulo-an-odd-integer map, as well as occurrences of the map i_k.

5.1 Toeplitz transforms and apwenian sequences

We begin this section by recalling the context for Toeplitz transforms and apwenian sequences that lead us to write this note.

$*$ In [4] a notion of Toeplitz transform was studied, consisting of inserting a sequence with holes into itself and iterating the process until all holes have disappeared. To illustrate the concept, we give the example of the regular paperfolding sequence.

Example 5.1. We start with the sequence $w = 0 \diamond 1 \diamond 0 \diamond 1 \diamond 0 \diamond 1 \diamond \cdots$, which consists of repeating the pattern $(0 \diamond 1 \diamond)$ infinitely many times. The symbol $\diamond$ is the *hole* and the next step is to insert the first sequence inside the holes, which yields the new sequence $001 \diamond 011 \diamond 00 \cdots$. Repeating this procedure a second time gives the new sequence $0010011 \diamond 00 \cdots$, and so on and so forth. The limit sequence obtained after infinitely many such insertions is called the *Toeplitz transform* of the initial sequence w.

One of the questions addressed in [4] consists in characterizing the binary periodic sequences having a periodic Toeplitz transform. In particular, it is shown that the number of such sequences of period $(2n+1)$ is equal to $2^{C_2(n)+1}$, where we recall that $C_2(n)$ is the number of cycles of the $(2,n)$-perfect shuffle permutation σ_n defined in (2).

$*$ Now we turn to the concept of apwenian sequences and show how they relate to doubling modulo odd integers. In [28], a sequence $d = d_0 d_1 d_2 \cdots$ taking value over $\{+1, -1\}$ is said to be *apwenian* if, for every integer $n \geq 1$, its Hankel determinant $H_n(d)$ satisfies the congruence

$$\frac{H_n(d)}{2^{n-1}} \equiv 1 \bmod 2.$$

In their study of apwenian sequences that are fixed points of constant-length morphisms of the free monoid generated by $\{-1, +1\}$, the authors of [28] introduce the permutation τ_m defined in (1). More precisely, this permutation and its cycle decomposition allows them to count the number of apwenian sequences satisfying certain properties, see [28, Section 1.1].

5.2 Dynamical systems

Let X be a compact metric space and $T\colon X \to X$ be a continuous transformation. We call (X,T) a *topological dynamical system*. Let Y be a closed nonempty subset of X such that $T(Y) \subset Y$. Then the restriction of T on Y induces a topological dynamical system on Y, denoted (Y,T) and called a *subsystem* of (X,T). Such a subsystem is called a *minimal component* of (X,T) if (Y,T) is minimal, i.e., for each $y \in Y$, the orbit $\{T^m y : m \geq 0\}$ is dense in Y. Let $k \geq 2$ and $n \geq 1$ be integers, and consider the topological dynamical system $(X, \sigma_{k,n})$, where the finite set $X = (\mathbb{Z}/(kn+1)\mathbb{Z}) \setminus \{0\}$ (endowed with the trivial metric) is compact. The results in the present

note can be reformulated as dynamical properties of $(X, \sigma_{k,n})$. For example, $C_k(n)$ is just the number of minimal components contained in $(X, \sigma_{k,n})$.

More generally, let a, b, m be fixed integers with $m \geq 2$, and consider the topological dynamical system $(\mathbb{Z}/m\mathbb{Z}, T_{a,b,m})$, where $T_{a,b,m}(x) = ax + b$, for each $x \in \mathbb{Z}/m\mathbb{Z}$. It is known that the system $(\mathbb{Z}/m\mathbb{Z}, T_{a,b,m})$ is minimal if and only if it is transitive, which is equivalent to saying that b is coprime with m, $a-1$ is a multiple of p for every prime p dividing m, and $a-1$ is a multiple of 4 if m is a multiple of 4 (e.g., see [33, Theorem A, page 17]. Also see [35]). In particular, the system $(\mathbb{Z}/m\mathbb{Z}, T_{a,0,m})$ cannot be minimal. If a is coprime with m, one can consider the multiplicative dynamical system $((\mathbb{Z}/m\mathbb{Z})^\times, T_{a,0,m})$, and it is minimal if and only if $\mathsf{ord}(a, m) = \varphi(m)$.

By taking the projective limit of $\mathbb{Z}/p^\ell\mathbb{Z}$ $(\ell \geq 1)$, one can extend the above results to p-adic dynamical systems. For example, the topological dynamical system $(\mathbb{Z}_p, T_{\alpha,\beta})$ is minimal if and only if $\alpha \in 1 + p^{r_p}\mathbb{Z}_p$ and $\beta \in \mathbb{Z}_p^\times$ (see [6], also see [25]), and if the system is not minimal, it can be decomposed into minimal components, here $\mathbb{Z}_p$ is the ring of p-adic integers, $\mathbb{Z}_p^\times$ is the group of invertible elements in $\mathbb{Z}_p$, and we suppose that $\alpha, \beta \in \mathbb{Z}_p$, $r_2 = 2$, $r_p = 1$ for $p \geq 3$, and $T_{\alpha,\beta}(x) = \alpha x + \beta$, for each $x \in \mathbb{Z}_p$ (see [25]). In the case that $\alpha \in \mathbb{Z}_p^\times$, one can also consider the multiplicative dynamical system $(\mathbb{Z}_p^\times, T_{\alpha,0})$, and discuss its minimality and its decomposition into minimal components (also see [25]).

5.3 The map i_k

Note that other properties and interpretations of the map i_k defined in (11) and other generalizations may be found, for example, in the works [16, 17, 18, 19, 36, 44, 45, 49, 50, 51, 57, 62, 67, 68, 70].

$*$ For example, in [19], already cited above, the following result gives a characterization of Mersenne primes.

Corollary 5.2 ([19, Corollaries 1 and 6]). *Let $k, n \geq 2$ be integers. Then*

$$n i_k(k^n - 1) = \sum_{d|n} \varphi\Big(\frac{n}{d}\Big)(k^d - 1) \geq \sum_{d|n} \frac{n}{d}\varphi(k^d - 1). \tag{22}$$

In particular, $k^n - 1$ is a (Mersenne) prime if and only if (22) is an equality.

$*$ Another occurrence of the map i_k (and several of its properties) can be found in [45] where *very odd sequences* are studied. Let $(a_i)_{1\leq i\leq n}$ be a sequence of n integers in $\{0, 1\}$ (otherwise stated, a binary sequence of length n) and set $A_\ell = \sum_{1\leq i\leq n-\ell} a_i a_{i+\ell}$, for $\ell \in [0, n-1]$. The sequence $(a_i)_{1\leq i\leq n}$ is called a *very odd sequence* if A_ℓ is odd for each $\ell \in [0, n-1]$.

Proposition 5.3 ([45, Proposition 2]). *For each integer $n \geq 1$, the number $S(n)$ of very odd sequences of length n is given by*

$$S(n) = \begin{cases} 0, & \text{if } \mathsf{ord}(2, 2n-1) \text{ is even;} \\ \sqrt{2}^{\,i_2(2n-1)-1}, & \text{otherwise.} \end{cases}$$

We have already cited in Remark 3.1 a statement that can be found, e.g., in [45, Lemma 5], namely that, if q is the order of a finite field, then $i_q(qn+1)$ is the number of distinct irreducible factors of the polynomial $X^{qn+1} - 1$ on $\mathbb{F}_q$. Actually one also finds the following result.

Proposition 5.4 ([45, Remark, page 224]). *Let p be a prime number. Then for each integer n with $p \nmid n$, $i_p(n)$ counts the total number of prime ideals that the ideal (p) factorizes in, in all the cyclotomic subfields of $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity.*

$*$ In the papers [67, 49] the quantity i_k appears in the study of the parametric family of elliptic curves $\mathbf{E}_d:\ y^2 + xy = x^3 - t^d$, over the function field $\mathbb{F}_q(t)$, where d is a positive integer. In the same vein, one can look at [68, Corollary 5.3] and [18, Theorem 2.2] (also see [51]).

$*$ In [57, page 320] one finds (a slight variation on) i_k with the following statement. For a finite set G and a map $f\colon G \to G$ from G to itself, let $\mathrm{graph}_f(G)$ be the directed graph whose vertices are the elements of G with a directed edge from x to $f(x)$ for every $x \in G$.

Proposition 5.5 ([57, page 320])**.** *Let k, m, n be positive integers with m odd and $n = 2^k m$. Then the number of cycles of* $\mathrm{graph}_f(\mathbb{Z}/n\mathbb{Z})$ *relative to $f(x) := x^2$ is equal to $i_k(m)$.*

Also see [57, Section 5] for other results with i_k in this context. For results about iterations of maps and counting cycles, see [70] and its bibliography (in particular [16]), also see [17, Theorem 1]; for more recent occurrences of (variants of) i_k, e.g., see [62, Proposition 3.1 (6)], [50] and [36].

5.4 The Luhn algorithm

There is one more example of doubling modulo an odd integer, somehow "simple" but widely used nowadays, namely the *Luhn algorithm* or *Luhn formula* originally described by Luhn in 1960 [40]. In this particular case, we write numbers in base 10 but we double some digits modulo 9 and the goal is to distinguish valid numbers from incorrect ones and to detect errors in writing numbers. More precisely, with each integer n written in base 10, say $n = a_d a_{d-1} \dots a_0$ with $a_i \in [0, 9]$ for every i, is associated the integer $n' = a'_d a'_{d-1} \dots a'_0$ obtained with the following rules: for $j = d, d-2, d-4, \dots$, we set $a'_j = a_j$, and for $j = d-1, d-3, d-5, \dots$, we set $a'_j = 2a_j \bmod 9$, where $m \bmod 9$ is the integer congruent to m modulo 9 that belongs to $[0, 8]$. Then there are two possible uses: either the sum $S := \sum_j a'_j$ of new digits is "checked" to be divisible by 10, or S is used to generate a *key* x, where x is defined by $x \in [0, 9]$ and $S + x$ divisible by 10.

5.5 Card-shuffling

Shuffling cards has always been somewhere between magic and mathematics. The mathematical study of card shuffle goes back at least to Monge [43] in the 18th century. A particular card shuffling is called *le battement de Monge* in French and *Monge card shuffle* in English (see [12, Problem 15, pages 214–222] and [14]; also see [59, 60]), it is associated with the permutation, called the *Monge permutation* and defined by

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & \dots & 2n-2 & 2n-1 & 2n \\ 2n & 2n-2 & 2n-4 & \dots & 2 & 1 & \dots & 2n-5 & 2n-3 & 2n-1 \end{pmatrix}$$

for some integer $n \geq 1$. Observe that the latter permutation is similar to (but different from) the permutation σ_n from (2). Also note that a variant of the Monge card shuffle occurs in [56, Section 4] in relation with quadratic residues and primitive roots.

A particular card-shuffling and the mathematics behind were explicitly described in several papers. Let us cite [20, 23, 46]. For example one can read in [24] the following comment about the permutation $x \mapsto 2x \bmod (n+1)$ over $[1, n]$, called *the perfect shuffle permutation of order n*:

> *The name is taken from that method of shuffling a deck of cards that cuts the deck into halves and then interleaves the two halves perfectly.*

Note that in the book [21], one can find (on page 166) the map $x \to 2x \bmod 11$. Among several other papers on the subject, let us only cite the four papers [42] (where the heaps are shuffled according to some permutation, and where—on page 6—the permutation $\sigma_{k,n}$ is denoted by w_{rev}), [54, 53], and [34].

5.6 Juggling

First we mention the nice book [48] that tells everything one always wanted to know about mathematics and juggling. In particular, a reformulation of the statement on top of [48, page 36], where one takes $q = 3$ and $p = 2n + 1$ (with $n \not\equiv 1 \bmod 3$) gives the following result.

Proposition 5.6. *Let n be a positive integer with $n \not\equiv 1 \bmod 3$. Then the permutation σ_n gives a* magic juggling sequence *when extending it to a map on $[0, 2n]$ by setting $\sigma_n(0) := 0$.*

5.7 Bell-ringing

Bell-ringing is both an art and a science. For example, the abstract of a lecture given at Gresham College by Hart and entitled "The Mathematics of Bell Ringing" [29] begins with the following lines:

> *This lecture will look at change ringing, which is ringing a series of tuned bells (as you might find in the bell tower of a church) in a particular sequence, and this has exciting mathematical properties*,

while one can read on [55, page 116]:

> *Compositions in ringing are designed to include musically attractive sequences, which are usually based on sequences running up or down the scale ("roll-ups"), sometimes with single notes omitted to produce slightly larger intervals of pitch.*

For more on bell-ringing, also see [64, 31, 55], [48, Chapter 6], the first page of [41], and the nice video [29].

Now, looking at [55, page 116] again, one can read:

> *Taking every other note of the scale, and running through the scale twice so as to include all the bells, produces* 135246 *on six bells, or* 13572468 *on eight. This is the best known of these favourite rows; it is called* Queens*, because a Queen of England is said to have commented on how nice the bells sounded when she heard it being rung.*
>
> *Reversing the first half of Queens on six bells produces Whittingtons:* 531246*; when heard by Dick Whittington leaving London as "Turn again, Whittington; Lord May'r of London", it persuaded him to return and, eventually, become Lord Mayor.*

The reader has certainly "recognized" the permutations 135246 and 13572468 that have the same flavor as our $\sigma_3 = (2\ 4\ 6\ 1\ 3\ 5)$ and $\sigma_4 = (2\ 4\ 6\ 8\ 1\ 3\ 5\ 7)$ as above with (2) for $n = 3, 4$. Actually there is more than a common flavor as shown below.

Lemma 5.7. *Let n be a positive integer. Define the Queens permutation θ_n on $[1, 2n]$ by*

$$\theta_n := \begin{pmatrix} 1 & 2 & \cdots & n & n+1 & n+2 & \cdots & 2n \\ 1 & 3 & \cdots & 2n-1 & 2 & 4 & \cdots & 2n \end{pmatrix}. \tag{23}$$

Then, the restriction of θ_n to $[2, 2n-1]$ is the same, up to notation, as the permutation $\sigma_{2,n-1}$.

Proof. Note that excluding 1 and $2n$ is somehow "natural" since the *Queens* permutation maps the first bell to the first and the last bell to the last. Now the restriction of θ_n to $[2, 2n-1]$ gives

$$\theta_n|_{[2,2n-1]} := \begin{pmatrix} 2 & 3 & \cdots & n & n+1 & n+2 & \cdots & 2n-1 \\ 3 & 5 & \cdots & 2n-1 & 2 & 4 & \cdots & 2n-2 \end{pmatrix}.$$

After the change of variable $k \mapsto k-1$, we obtain the permutation

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n & n+1 & \cdots & 2n-2 \\ 2 & 4 & \cdots & 2n-2 & 1 & 3 & \cdots & 2n-3 \end{pmatrix},$$

which is exactly the permutation $\sigma_{2,n-1}$ (defined on $[1, 2n-2]$) from (2). □

5.8 Poetry

A variant of the permutation $\sigma_{2,3}$ can be found in various papers on poetry and literature with connections to mathematics; (e.g., see [58], [10, page 65], [9, 15, 22, 52, 65]; also see the paper [11] and the book [37]). This permutation is given by

$$\nu_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}$$

and is related to the so-called *sextine* in French and *sestina* in English. (Note that this permutation ν_6 is the inverse of the Queneau-Daniel permutation μ_6 defined in Section 2, see Remark 5.8 below.) In this form of poetry, the last words of a *stanza* of six lines are permuted according to the previous permutation and used as ending words in the next stanza of six lines. It was invented by the 12th century poet Arnaut Daniel (for his poem and an English translation, e.g., see [61]). Over time, cases with n elements instead of 6, as well as variations around these permutations were studied, both on the literary and the mathematical sides. In particular, we mention the book [60], with its chapter called *Le battement de Monge* [60, pages 145–163] (for more on *tropical partitions* described there, see [27]); also see [13].

Remark 5.8. We cannot resist to mention that the permutation ν_6 above resembles very much permutations in the family studied by Lévy in [38, Chapter 1]. Namely, this variant ν_6 of $\sigma_{2,3}$ is the case $n = 6$ of the permutation ν_n defined for $x \in [1, n]$ by

$$\nu_n(x) = \begin{cases} 2x, & \text{if } 2x \le n; \\ 2n + 1 - 2x, & \text{otherwise,} \end{cases}$$

while the permutation ρ_n studied by Lévy is defined in [38, Chapter 1] for $x \in [1, n]$ by

$$\rho_n(x) = \begin{cases} 2x - 1, & \text{if } 2x \le n + 1; \\ 2n + 2 - 2x, & \text{otherwise.} \end{cases}$$

Recall that $\sigma_{2,n}$ can also be defined for $x \in [1, 2n]$ by

$$\sigma_{2,n}(x) = \begin{cases} 2x, & \text{if } x \le n; \\ 2x - 1 - 2n, & \text{otherwise.} \end{cases}$$

Note that easy identities can be proved, e.g., $\forall k \in [2, n]$, we have $\rho_n(k) = \nu_{n-1}(k - 1) + 1$, or, as already mentioned in Section 2, ν_n is the inverse of the Queneau-Daniel permutation μ_n defined on $[1, n]$ by $\mu_n(k) = k/2$ if k is even, and $\mu_n(k) = n - (k - 1)/2$ if k is odd, [15].

Thus we see that all these permutations share a common flavor. It is interesting to read the opinion of Lévy on mathematical problems of this sort (see [39, page 151]):

> *Je ne m'exagère pas l'importance du problème, qui se rattache à l'analyse combinatoire et à la théorie des groupes, dont je vais parler maintenant. Aux yeux d'un mathématicien plus jeune que je ne le suis, cela ne peut être qu'une toute petite chose. Mais il me semble qu'il peut y avoir intérêt à montrer que, dans l'esprit des mathématiques classiques, il y a encore de jolis problèmes à traiter. En outre, la manière dont je fus conduit à poser celui dont je vais parler est assez amusante* [...].

5.9 Musical composition

One can ask whether the permutations studied here have been used in musical composition beyond bell-ringing. The answer is of course positive. First, let us mention the must-read [5] and its bibliography. The interested reader can also look at [2] where the authors are interested in which permutations σ_n satisfy an extra property. One can in particular listen to the piece *Science Fictions* for two pianos by Adler (see [1]).

The curious reader can also be interested in the use of sestinas (see Section 5.8) in music: we will only cite the *Sestina* of Monteverdi; e.g., listen to `https://www.youtube.com/playlist?list=PL2k8ekJXk4nVHGs3glCLvc9EwD_GUEpQ-`.

6 Conclusion and open directions

In this paper, we have proven in Section 3 the equality between the quantities (3) and (4) by considering a generalized permutation of $[1, kn]$ that can be written as $x \mapsto kx \bmod (kn+1)$, where k, n are positive integers. In addition to studying various properties of this permutation in Sections 2 and 4, we have listed some of its many occurrences in the literature in Section 5. Going even beyond, the reader might wonder whether other generalizations are possible. We point out the map $x \mapsto kx \bmod (kn+j)$ where j, k, n are integers. Observe that when k, j are not coprime, then the map is not a bijection, e.g., $x \mapsto 2x \bmod (2n+4)$ maps, for $n = 2$, $(1, 2, 3, 4, 5, 6)$ to $(2, 4, 6, 8, 0, 2)$. In the case where k, j are coprime, we think that the results of this paper can be adapted, for which we leave the details to the reader, especially the precise description of the cycles of Theorem 2.4 by Ellis, Fan, and Shallit.

Acknowledgments

The first author proposed the equality stated in Corollary 3.4 as one of the subjects of the "Concours SMF Junior 2022" (organized by the French Mathematical Society). He thanks the participants for their work and suggestions. The three authors want to warmly thank Michèle Audin, Rémy Bellenger, Pieter Moree, Olivier Salon, and Jeffrey Shallit for highlighting discussions and providing several useful references.

References

[1] Adler, C.: Science Fictions (2021), https://christopheradler.com/compositions/chamber-ensemble/western_chamber/science_fictions/

[2] Adler, C., Allouche, J.-P.: Finite self-similar sequences, permutation cycles, and music composition. J. Math. Arts **16**(3), 244–261 (2022), https://dx.doi.org/10.1080/17513472.2022.2116745

[3] Aitken, A.C.: On induced permutation matrices and the symmetric group. Proc. Edinb. Math. Soc., II. Ser. **5**, 1–13 (1936), https://dx.doi.org/10.1017/S0013091500008208

[4] Allouche, J.-P.: Suites infinies à répétitions bornées. In: Séminaire de théorie des nombres, Bordeaux, 1983–1984 (Talence, 1983/1984), pp. Exp. No. 20, 11. Univ. Bordeaux I, Talence (1984), https://eudml.org/doc/182192

[5] Amiot, E.: Autosimilar melodies. J. Math. Music **2**(3), 157–180 (2008), https://dx.doi.org/10.1080/17459730802598146

[6] Anashin, V.: Ergodic transformations in the space of p-adic integers. In: p-adic mathematical physics, AIP Conf. Proc., vol. 826, pp. 3–24. Amer. Inst. Phys., Melville, NY (2006), https://doi.org/10.1063/1.2193107

[7] Asveld, P.R.J.: Permuting operations on strings and their relation to prime numbers. Discrete Appl. Math. **159**(17), 1915–1932 (2011), https://dx.doi.org/10.1016/j.dam.2011.07.019

[8] Asveld, P.R.J.: Queneau numbers–recent results and a bibliography (2013), CTIT Technical Report Series Publisher, University of Twente, Centre for Telematica and Information Technology (CTIT), TR–CTIT–13–16, https://research.utwente.nl/en/publications/queneau-numbers-recent-results-and-a-bibliography

[9] Audin, M.: Poésie, spirales, et battements de cartes : D'Arnaut Daniel à Jacques Roubaud en passant par Gaspard Monge et quelques autres, Images des Mathématiques, CNRS, 2020; Published on December 9, 2020; https://images-archive.math.cnrs.fr/Poesie-spirales-et-battements-de-cartes.html

[10] Audin, M.: Mathématiques et littérature—un article avec des mathématiques et de la littérature. Math. Sci. Hum. Math. Soc. Sci. **178**, 63–86 (2007), https://dx.doi.org/10.4000/msh.4232

[11] Audin, M.: Histoire du pli cacheté 7115 incluant une véridique histoire des nombres "de Queneau" (2013), https://www.oulipo.net/fr/histoire-du-pli-cachete-7115/dantoine-tavera

[12] Bachet, C.G.: Problèmes plaisants & délectables, qui se font par les nombres. Gauthier-Villars, Paris (1874), 3ième éd, Revue, simplifiée et augmentée par A. Labosne

[13] Bédouret-Larraburu, S., Barbieri-Viale, L., Uhlig, M.: Le sonnet et la sextine : deux formes contemporaines "créantes". In: Quaderni di stilistica e metrica italiana, vol. 12, pp. 65–290. SISMEL - Edizioni del Galluzzo, Firenze (2023), https://www.mirabileweb.it/edgalluzzo/miscellanee/m/1253

[14] Bourget, J.: Sur un problème de permutations successives nommé Battement de Monge. J. Math. Pures Appl. **8**, 413–434 (1882), http://www.numdam.org/item/JMPA_1882_3_8__413_0.pdf

[15] Bringer, M.: Sur un problème de R. Queneau. Math. Sci. Humaines **27**, 13–20 (1969), http://www.numdam.org/article/MSH_1969__27__13_0.pdf

[16] Chassé, G.: Applications d'un corps fini dans lui-même, Thèse de Doctorat, Université Rennes I, UER de Mathématiques et Informatique, Rennes, Vol. 149 (1984)

[17] Chou, W.S., Shparlinski, I.E.: On the cycle structure of repeated exponentiation modulo a prime. J. Number Theory **107**, 345–356 (2004), https://doi.org/10.1016/j.jnt.2004.04.005

[18] Conceição, R.P., Hall, C., Ulmer, D.: Explicit points on the Legendre curve II. Math. Res. Lett. **21**, 261–280 (2014), https://doi.org/10.4310/MRL.2014.v21.n2.a5

[19] Deaconescu, M.: An identity involving multiplicative orders. Integers **8**, A9, 5 p. (2008), https://eudml.org/doc/116955

[20] Diaconis, P., Graham, R.L., Kantor, W.M.: The mathematics of perfect shuffles. Adv. in Appl. Math. **4**(2), 175–196 (1983), https://doi.org/10.1016/0196-8858(83)90009-X

[21] Diaconis, P., Graham, R.: The magic of Charles Sanders Peirce. In: Beineke, J., Rosenhouse, J. (eds.) The mathematics of various entertaining subjects. Vol. 3, pp. 161–203. Princeton Univ. Press, Princeton, NJ (2019)

[22] Dumas, J.G.: Caractérisation des quenines et leur représentation spirale. Math. Sci. Hum. Math. Soc. Sci. **184**, 9–23 (2008), https://dx.doi.org/10.4000/msh.10946

[23] Ellis, J., Fan, H., Shallit, J.: The cycles of the multiway perfect shuffle permutation. Discrete Math. Theor. Comput. Sci. **5**(1), 169–180 (2002), https://eudml.org/doc/122362

[24] Ellis, J., Krahn, T., Fan, H.: Computing the cycles in the perfect shuffle permutation. Inform. Process. Lett. **75**(5), 217–224 (2000), https://dx.doi.org/10.1016/S0020-0190(00)00103-4

[25] Fan, A.-H., Li, M.-T., Yao, J.-Y., Zhou, D.: Strict ergodicity of affine p–adic dynamical systems on $\mathbb{Z}_p$. Adv. Math. **214**(2), 666–700 (2007), https://doi.org/10.1016/j.aim.2007.03.003

[26] Graham, R.L., Knuth, D.E., Patashnik, O.: Concrete mathematics. Addison-Wesley Publishing Company, Reading, MA, second edn. (1994), a foundation for computer science

[27] Guilbaud, G.T.: Permutations tropicales. In: Permutations (Actes Colloq., Univ. René-Descartes, Paris, 1972), pp. 271–276. Mathématiques et Sciences de l'Homme, XX, Gauthier-Villars, Paris-Brussels-Montreal, Que. (1974), https://doi.org/10.1515/9783112311943-025

[28] Guo, Y., Han, G., Wu, W.: Criteria for apwenian sequences. Adv. Math. **389**, Paper No. 107899, 37 (2021), https://dx.doi.org/10.1016/j.aim.2021.107899

[29] Hart, S.: The mathematics of bell ringing, talk given on January 5, 2021; part of the series of talks on "Mathematics in Music and Writing" at Gresham College; https://www.gresham.ac.uk/watch-now/maths-bellringing

[30] Heuer, G.A., Stratton, T., Smith, D.A., Hammer, F.D., Sastry, K.R.S., Orno, P., Rickey, V.F., Good, I.J., Jensen, D.R., McWorter, Jr., W.A., Broline, D., Apostol, T.M., Creech, R.L., Nelsen, R.B.: Problems. Math. Mag. **54**, 84–87 (1981), https://www.jstor.org/stable/2690443

[31] Jaulin, B.: Sur l'art de sonner les cloches. Math. Sci. Humaines **60**, 5–20 (1977), http://www.numdam.org/article/MSH_1977__60__5_0.pdf

[32] Klamkin, M.S., Apostol, T.M., Creech, R.L., Austin, A.K., Motteler, Z.C., Hammer, F.D., Fox, W.F., Orno, P., Clark, R., Ampe, J., Cherry, J.C., Eves, H., Philippou, A.N., Todd, P., Moran, D.A., Brackett, A.D.: Problems. Math. Mag. **53**, 49–54 (1980), https://www.jstor.org/stable/2690032

[33] Knuth, D.: The art of computer programming. Vol. 2. Seminumerical algorithms. Addison-Wesley, Reading, MA, third edn. (1998)

[34] Lachal, A.: Perfect shuffles of cards. I: In-shuffles and out-shuffles. Quadrature **76**, 13–25 (2010)

[35] Larin, M.: Transitive polynomial transformations of residue rings. Diskret. Mat. **14**(2), 20–32 (2002), translation in Discrete Math. Appl. **12**(3) (2002), 127–140, https://doi.org/10.1515/dma-2002-0204

[36] Larson, M.: Power maps in finite groups. Integers **19**, Paper No. A58, 15 pp. (2019)

[37] Lartigue, P.: L'Hélice d'écrire. La sextine. Les Belles-Lettres (1994)

[38] Lévy, P.: Sur quelques classes de permutations. Compositio Math. **8**, 1–48 (1950-1951), http://www.numdam.org/article/CM_1951__8__1_0.pdf

[39] Lévy, P.: Quelques aspects de la pensée d'un mathématicien. Introduction. Première partie : Souvenirs mathématiques. Deuxième partie : Considérations philosophiques. Librairie Scientifique et Technique Albert Blanchard, Paris (1970)

[40] Luhn, H.P.: Computer for verifying numbers, US patent 2950048A, published August 23, 1960. https://patents.google.com/patent/US2950048A/en

[41] Mayfield, K.: Calling call changes, https://www.barrowbells.org.uk/Training/CallingCallChanges.pdf

[42] Medvedoff, S., Morrison, K.: Groups of perfect shuffles. Math. Mag. **60**(1), 3–14 (1987), https://dx.doi.org/10.2307/2690131

[43] Monge, G.: Réflexions sur un tour de cartes. Mémoires des Savants étrangers, Académie des Sciences, Paris, Imprimerie Royale, Paris, 1776 (1773)

[44] Moree, P.: Artin's primitive root conjecture – a survey. Integers **12**(6), 1305–1416, A13 (2012), https://dx.doi.org/10.1515/integers-2012-0043

[45] Moree, P., Solé, P.: Around Pelikán's conjecture on very odd sequences. Manuscr. Math. **117**(2), 219–238 (2005), https://dx.doi.org/10.1007/s00229-005-0554-5

[46] Morris, S.B., Hartwig, R.E.: The generalized faro shuffle. Discrete Math. **15**, 333–346 (1976), https://doi.org/10.1016/0012-365X(76)90047-9

[47] Patil, D.P., Storch, U.: Group actions and elementary number theory. J. Indian Inst. Sci. **91**, 1–45 (2011)

[48] Polster, B.: The mathematics of juggling. Springer-Verlag, New York (2003)

[49] Pomerance, C., Shparlinski, I.E.: Rank statistics for a family of elliptic curves over a function field. Pure Appl. Math. Q. **6**(1), 21–40 (2010), https://dx.doi.org/10.4310/PAMQ.2010.v6.n1.a2

[50] Pomerance, C., Shparlinski, I.E.: Connected components of the graph generated by power maps in prime finite fields. Integers **18A**, Paper No. A16, 8 pp. (2018)

[51] Pomerance, C., Ulmer, D.: On balanced subgroups of the multiplicative group. In: Number theory and related fields, Springer Proc. Math. Stat., vol. 43, pp. 253–270. Springer, New York (2013), https://doi.org/10.1007/978-1-4614-6642-0_14

[52] Queneau, R.: Note complémentaire sur la Sextine, suivie d'un Éloge de la SPIRALE par J. Bernoulli. Subsidia Pataphysica **1**, 79–80 (1967)

[53] Quintero, R.: Moving cards arbitrarily with perfect k-shuffles. Bol. Asoc. Mat. Venez. **17**(1), 41–48 (2010), https://dialnet.unirioja.es/servlet/articulo?codigo=3718139

[54] Ramnath, S., Scully, D.: Moving card i to position j with perfect shuffles. Math. Mag. **69**, 361–365 (1996), https://dx.doi.org/10.2307/2691282

[55] Roaf, D., White, A.: Ringing the changes: bells and mathematics. In: Music and mathematics, pp. 113–129. Oxford Univ. Press, Oxford (2003)

[56] Roberts, J.B.: Integral power residues as permutations. Amer. Math. Monthly **76**, 379–385 (1969), https://dx.doi.org/10.2307/2316429

[57] Rogers, T.D.: The graph of the square mapping on the prime fields. Discrete Math. **148**(1-3), 317–324 (1996), https://dx.doi.org/10.1016/0012-365X(94)00250-M

[58] Roubaud, J.: Un problème combinatoire posé par la poésie lyrique des troubadours. Math. Sci. Humaines **27**, 5–12 (1969), https://eudml.org/doc/94050

[59] Roubaud, J.: Battement de Monge, vol. 158. La Bibliothèque oulipienne, Paris (2006)

[60] Roubaud, J.: Octogone. Livre de poésie, quelquefois prose. Gallimard, Collection Blanche (2014)

[61] Saclolo, M.P.: How a medieval troubadour became a mathematical figure. Notices Amer. Math. Soc. **58**(5), 682–687 (2011), https://www.ams.org/notices/201105/rtx110500682p.pdf

[62] Sha, M.: On the cycle structure of repeated exponentiation modulo a prime power. Fibonacci Quart. **49**, 340–347 (2011)

[63] Sloane, N.J.A., et al.: The On-Line Encyclopedia of Integer Sequences, https://oeis.org

[64] Stedman, F.: Campanalogia: or The art of ringing improved. With plain and easie rules to guide the practitioner in the ringing all kinds of changes, to which is added, great variety of new peals. Godbid, W., London (1677), https://www.gutenberg.org/ebooks/73423

[65] Tavera, A.: Arnaut Daniel et la Spirale. Subsidia Pataphysica **1**, 73–78 (1967)

[66] Tenenbaum, G.: Introduction to analytic and probabilistic number theory, Cambridge Studies in Advanced Mathematics, vol. 46. Cambridge University Press, Cambridge (1995), translated from the second French edition (1995) by C. B. Thomas

[67] Ulmer, D.: Elliptic curves with large rank over function fields. Ann. Math. (2) **155**(1), 295–315 (2002), https://dx.doi.org/10.2307/3062158

[68] Ulmer, D.: Explicit points on the Legendre curve. J. Number Theory **136**, 165–194 (2014), https://doi.org/10.1016/j.jnt.2013.09.010

[69] Vallet, V.: Entre mathématiques et littérature : les nombres de Queneau. L'ouvert **118**, 19–37 (2010), https://bibnum.publimath.fr/IST/IST10015.pdf

[70] Vasiga, T., Shallit, J.: On the iteration of certain quadratic maps over GF(p). Discrete Math. **277**(1-3), 219–240 (2004), https://dx.doi.org/10.1016/S0012-365X(03)00158-4