Permuting Operations on Strings and the Distribution of Their Prime Numbers

Peter R.J. Asveld
Department of Computer Science, Twente University of Technology
P.O. Box 217, 7500 AE Enschede, the Netherlands
e-mail: P.R.J.Asveld@utwente.nl, P.R.J.Asveld@xs4all.nl

Abstract — Several ways of interleaving, as studied in theoretical computer science, and some subjects from mathematics can be modeled by length-preserving operations on strings, that only permute the symbol positions in strings. Each such operation X gives rise to a family $\{X_n\}_{n\geq 2}$ of similar permutations. We call an integer n *X-prime* if X_n consists of a single cycle of length n ($n \geq 2$). For some instances of X —such as shuffle, twist, operations based on the Archimedes' spiral and on the Josephus problem— we investigate the distribution of X-primes and of the associated (ordinary) prime numbers, which leads to variations of some well-known conjectures on the density of certain sets of prime numbers.

Keywords: shuffle, twist, Archimedes' spiral, Josephus problem, Queneau number, distribution of prime numbers, Artin's conjecture (on primitive roots).

"A Tale of Ten Tables"

1 Introduction

Interleaving is a central notion in theoretical computer science: it plays an important part when we model phenomena like concurrency and synchronization. Shuffling a deck of cards is a very simple form of interleaving, but the shuffle operation and its variants are used extensively in modeling concurrency [11]. On the other hand, interleaving aspects are also present in the Josephus problem ("eeny, meeny, miny, moe") [25, 7] which may be considered as a rather complicated form of interleaving. In between these extreme ways of interleaving are the twist operation and its generalizations (as introduced in Section 7). Both the shuffle and the twist operation are also investigated in automata theory; see, e.g., [12, 13, 14]. It turns out, as shown in [2], that these quite different forms of interleaving can be related by means of several types of Archimedes' spirals.

In this context the following observation is crucial. In essence, we deal with length-preserving operations on strings of symbols that only permute the symbol positions in the string. With each such operation X we can associate an infinite sequence $\{X_n\}_{n\geq 2}$ of similar permutations with $X_n \in \mathfrak{S}_n$ where $\mathfrak{S}_n$ is the symmetric group on n elements. Each

permutation X_n generates a cyclic subgroup $\langle X_n \rangle$ of $\mathfrak{S}_n$. Some permutations X_n in this sequence are of special interest; viz.

Definition 1.1. Let X be a permuting operation on strings. A number n ($n \geq 2$) is called X-*prime* if X_n consists of a single cycle of length n or, equivalently, $\langle X_n \rangle$ is of order n. The set of X-primes is denoted by $P(X)$. □

The present paper is a companion to [2] and it is organized as follows. In Section 2 we recall the definitions and notation of some permuting operations on strings from [2]: shuffle operations (viz. S and its dual $\overline{S}$), twist operation T, operations based on the Archimedes' spiral (viz. A_0, A_1, A_1^+ and A_1^-) and on the Josephus problem (viz. J_2 and its dual $\overline{J_2}$). For motivation, examples of permutations X_n and of $\langle X_n \rangle$, as well as the concept of duality, we refer to [2]. Section 3 is devoted to a few characterization results for X-primes from [2] that play an important part in Sections 5 and 6. Then in Section 4 we count X-primes —just as one counts ordinary prime numbers— where X equals S, $\overline{S}$, T, A_0, A_1, A_1^+, A_1^-, J_2 and $\overline{J_2}$. Section 5 deals with ordinary prime numbers associated to X-primes, the so-called x-primes. In Section 6 we study the distribution of these x-primes in relation to the distribution of ordinary prime numbers, i.e., we focus our attention to the density of x-primes in the ordinary primes. In this section we stumble against some well-known mathematical conjectures, viz. the Generalized Riemann Hypothesis (GRH) and Artin's Conjecture on Primitive Roots (ACPR). Our main results of Section 6 are placed in a broader context in Section 7 (generators of $\mathbb{Z}_p^\star$ or primitive roots modulo p). Finally, Section 8 consists of a few concluding remarks.

2 Permuting Operations on Strings

Let $\mathbb{N}_2 = \{n \in \mathbb{N} \mid n \geq 2\}$, and let $\Sigma_n = \{a_1, a_2, \ldots, a_n\}$ be an alphabet of n different symbols that is linearly ordered by $a_1 < a_2 < \cdots < a_n$ ($n \in \mathbb{N}_2$). The string or word α_n over Σ_n, defined by $\alpha_n = a_1 a_2 \cdots a_n$, is called the *standard word* of length n [15].

Shuffling a deck of cards can be modeled by the permuting operation S, defined by

$$S(\alpha_n) = a_k a_1 a_{k+1} a_2 a_{k+2} a_3 \cdots \qquad \text{with } k = \lceil (n+1)/2 \rceil,$$

which results —cf. §3.4 in [9]— in a family of permutations $\{S_n\}_{n \geq 2}$ with

$$\begin{aligned} &S_n(m) \equiv 2m \pmod{n+1}, && n \text{ even; } 1 \leq m \leq n, \\ &S_n(m) \equiv 2m \pmod{n}, && n \text{ odd; } 1 \leq m < n, \\ &S_n(n) = n && n \text{ odd.} \end{aligned}$$

The permuting operation $\overline{S}$ results from perfectly shuffling a deck of an even number of cards that has first been put upside down. For an odd number of cards we remove the last card, put the remaining deck upside down, shuffle it, and finally put this card on top of the shuffled deck:

$$\begin{aligned} &\overline{S}(\alpha_n) = a_{k-1} a_{n-1} a_{k-2} a_{n-2} \cdots a_1 a_k a_n && \text{if } n \text{ is odd,} \\ &\overline{S}(\alpha_n) = a_{k-1} a_n a_{k-2} a_{n-1} \cdots a_1 a_k && \text{if } n \text{ is even,} \end{aligned}$$

where $k = \lceil (n+1)/2 \rceil$. The corresponding shuffle permutations can be defined by

$$\begin{aligned}
&\overline{S}_n(m) \equiv -2m \pmod{n+1}, && n \text{ even; } 1 \le m \le n,\\
&\overline{S}_n(m) \equiv -2m \pmod{n}, && n \text{ odd; } 1 \le m < n,\\
&\overline{S}_n(n) = n, && n \text{ odd.}
\end{aligned}$$

The twist operation T is another way of permuting a deck of cards: before we interleave the two parts of the deck we put the second half upside down, i.e., T is defined by

$$T(\alpha_n) = a_n a_1 a_{n-1} a_2 a_{n-2} a_3 \cdots,$$

which induces a family of permutations $\{T_n\}_{n\ge 2}$ with

$$\begin{aligned}
&T_n(m) \equiv +2m \pmod{2n+1}, && 1 \le m < k = \lceil (n+1)/2 \rceil, \text{ and}\\
&T_n(m) \equiv -2m \pmod{2n+1}, && k \le m \le n.
\end{aligned}$$

The Archimedes permuting operations A_0, A_1, A_1^+ and A_1^- are based on the Archimedes' spiral. So consider an Archimedes' spiral with polar equation $r = c\,\theta$ ($c > 0$; $\theta \ge 0$ is the angle) and place the first symbol a_1 from the standard word α_n at the origin ($\theta = 0$) in the XY-plane. Each time, as θ increases, that r intersects the X-axis we put the next symbol from α_n on the X-axis. Finally, we read the symbols placed on the X-axis from left to right to obtain $A_0(\alpha_n)$:

$$\begin{aligned}
&A_0(\alpha_n) = a_n a_{n-2} \cdots a_4 a_2 a_1 a_3 a_5 \cdots a_{n-3} a_{n-1} && \text{if } n \text{ is even, and}\\
&A_0(\alpha_n) = a_{n-1} a_{n-3} \cdots a_4 a_2 a_1 a_3 a_5 \cdots a_{n-2} a_n && \text{if } n \text{ is odd.}
\end{aligned}$$

A_0 induces a family of permutations $\{A_{0,n}\}_{n\ge 2}$ with, for $1 \le m \le n$,

$$A_{0,n}(m) = \lceil (n+1)/2 \rceil + (-1)^{m-1} \lceil (m-1)/2 \rceil.$$

The permuting operation A_1 is defined as a variation of A_0; viz. by starting with the Archimedes-like spiral defined by the polar equation $r = c(\theta + \pi)$ with $\theta \ge 0$. Then

$$\begin{aligned}
&A_1(\alpha_n) = a_{n-1} a_{n-3} \cdots a_3 a_1 a_2 a_4 \cdots a_{n-2} a_n && \text{if } n \text{ is even, and}\\
&A_1(\alpha_n) = a_n a_{n-2} \cdots a_3 a_1 a_2 a_4 \cdots a_{n-3} a_{n-1} && \text{if } n \text{ is odd.}
\end{aligned}$$

Then the corresponding family of permutations $\{A_{1,n}\}_{n\ge 2}$ satisfies, for $1 \le m \le n$,

$$A_{1,n}(m) = \lceil n/2 \rceil + (-1)^m \lceil (m-1)/2 \rceil.$$

It happens to be useful to subdivide $P(A_1)$ as follows. A number n in $\mathbb{N}_2$ is A_1^+-*prime* if it is an A_1-prime and $n \equiv 1 \pmod 4$. And n in $\mathbb{N}_2$ is an A_1^--*prime* if it is an A_1-prime and $n \equiv 3 \pmod 4$. Then we have $P(A_1) = P(A_1^+) \cup P(A_1^-)$ with $P(A_1^+) \cap P(A_1^-) = \varnothing$.

The permuting operation J_2 stems from the Josephus problem [25]; it may be viewed as the simplest instance of "eeny, meeny, miny, moe". There are various ways to describe this operation from which we choose the method given in §3.3 of [7].

We walk in a cyclic way through the standard word α_n and we assign numbers to symbol indices (symbol positions in α_n). In the first sweep through α_n we assign the numbers 1, 2, $\cdots$ n to the symbol positions 1, 2, $\cdots$ n, respectively; positions that got an even number are "marked". In the next sweep through α_n the "unmarked" symbol positions are number consecutively; a_1 gets n+1, a_2 is marked, a_3 gets n+2, a_4 is marked, a_5 gets n+3, etc. We continue this process until we reach the number $2n$, i.e., until all symbols are marked. Reading the marked symbols in order of increasing even assigned numbers yields $J_2(\alpha_n)$.

For the family of permutations $\{J_{2,n}\}_{n\geq 2}$ we obtained in [2], for $1 \leq m \leq n$,

$$J_{2,n}(m) = (2n+1-\lVert 2n+1-m\rVert)/2,$$

where $\lVert x\rVert$ is the odd part of x, i.e., the unique odd number such that $x/\lVert x\rVert$ is a power of 2. For instance, we have $\lVert 16\rVert = 1$, $\lVert 24\rVert = 3$ and $\lVert 360\rVert = 45$.

In [2] we introduced a permuting operation $\overline{J_2}$ based on a modified Josephus problem. Viz. in numbering the symbol positions in the standard word α_n —still from left to right— we distinguish between even and odd (numbered) sweeps through α_n:

- In odd sweeps we number downwards starting with $2n$ in the first sweep.
- In even sweeps we number upwards starting with 1 in the second sweep.
- The numbering ends when all numbers from 1 to $2n$ are assigned to symbol positions.

As in the case of J_2 the even numbers in the numbering/marking process determine the value of $\overline{J_{2,n}}(m)$: the jth symbol to be marked receives number $2j$ in the marking process.

For the family of permutations $\{\overline{J_{2,n}}\}_{n\geq 2}$ we inferred in [2] that, for $1 \leq m \leq n$,

$$\overline{J_{2,n}}(m) = (2n+1-\lVert m\rVert^-_{2n+1})/2,$$

where $\lVert x\rVert^-_q$ is the odd number such that $1 \leq \lVert x\rVert^-_q < q$ and $x \equiv \lVert x\rVert^-_q(-2)^t \pmod q$ for the smallest $t \geq 0$. As examples, we mention that $\lVert 6\rVert^-_{29} = 21$ and $\lVert 2\rVert^-_{35} = 23$, since $6 \equiv 21(-2)^3 \pmod{29}$ with $t = 3$, and $2 \equiv 23(-2)^6 \pmod{35}$ with $t = 6$, respectively. Clearly, for each odd x with $1 \leq x < q$, we have $\lVert x\rVert^-_q = x$ as $t = 0$ applies.

Table 1 contains for each X, the first elements of $P(X)$; more elements can be found in the respective entries in the On-line Encyclopedia of Integer Sequences (OEIS) [26].

Note that T-primes are often referred to as Queneau numbers [3, 4, 5, 24] which are defined as T^{-1}-primes; but it is easy to see that $P(T^{-1}) = P(T)$. The A_0-primes are just the even Queneau numbers and the A_1-primes are the odd Queneau numbers [2].

3 Characterization of X-primes

In this section we quote a few characterization results from [2]; we refer to this reference for a more complete overview of characterizations as well as a short history of earlier, similar (partial) results as in [3, 9, 4, 5]; cf. [6] for some more recent characterizations.

Let $\mathbb{Z}$ be the set of all integers. For a prime p, $\mathbb{Z}_p$ denotes the finite field of integers modulo p and $\mathbb{Z}_p^\star$ denotes the cyclic multiplicative group of $\mathbb{Z}_p$. Recall that $\mathbb{Z}_p^\star$ has order $p-1$. Let G_p be the set of all possible generators of $\mathbb{Z}_p^\star$ (the elements in $\mathbb{Z}_p^\star$ of order $p-1$).

First, we consider the several types of Archimedes primes.

Theorem 3.1. [2]

(1) *A number n in $\mathbb{N}_2$ is A_0-prime if and only if n is even, $2n+1$ is a prime number, and both -2 and $+2$ are a generator of $\mathbb{Z}^\star_{2n+1}$: $\{-2,+2\} \subseteq G_{2n+1}$.*

(2) *A number n in $\mathbb{N}_2$ is A_1-prime if and only if n is odd, $2n+1$ is a prime number, and only one of -2 and $+2$ is a generator of $\mathbb{Z}^\star_{2n+1}$: $\{-2,+2\} \cap G_{2n+1}$ is a singleton.*

(3) *A number n in $\mathbb{N}_2$ is A_1^+-prime if and only if $n \equiv 1 \pmod 4$, $2n+1$ is a prime number, and $+2$ is a generator of $\mathbb{Z}^\star_{2n+1}$, but -2 is not: $+2 \in G_{2n+1}$ and $-2 \notin G_{2n+1}$.*

X	$P(X)$	OEIS
S	2, 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82, 100, 106, 130, 138, 148, 162, 172, 178, 180, 196, 210, 226, 268, 292, 316, 346, 348, 372, ...	A071642
$\overline{S}$	4, 6, 12, 22, 28, 36, 46, 52, 60, 70, 78, 100, 102, 148, 166, 172, 180, 190, 196, 198, 238, 262, 268, 270, 292, 310, 316, 348, 358, 366, ...	A163776
T	2, 3, 5, 6, 9, 11, 14, 18, 23, 26, 29, 30, 33, 35, 39, 41, 50, 51, 53, 65, 69, 74, 81, 83, 86, 89, 90, 95, 98, 99, 105, 113, 119, 131, 134, 135, 146, 155, 158, 173, 174, 179, 183, 186, 189, 191, 194, 209, 210, ...	A054639
A_0	2, 6, 14, 18, 26, 30, 50, 74, 86, 90, 98, 134, 146, 158, 174, 186, 194, 210, 230, 254, 270, 278, 306, 326, 330, 338, 350, 354, 378, 386, ...	A163777
A_1	3, 5, 9, 11, 23, 29, 33, 35, 39, 41, 51, 53, 65, 69, 81, 83, 89, 95, 99, 105, 113, 119, 131, 135, 155, 173, 179, 183, 189, 191, 209, 221, ...	A163778
A_1^+	5, 9, 29, 33, 41, 53, 65, 69, 81, 89, 105, 113, 173, 189, 209, 221, 233, 245, 261, 273, 281, 293, 309, 329, 393, 413, 429, 441, 453, 473, ...	A163779
A_1^-	3, 11, 23, 35, 39, 51, 83, 95, 99, 119, 131, 135, 155, 179, 183, 191, 231 239, 243, 251, 299, 303, 323, 359, 371, 375, 411, 419, 431, 443, ...	A163780
J_2	2, 5, 6, 9, 14, 18, 26, 29, 30, 33, 41, 50, 53, 65, 69, 74, 81, 86, 89, 90, 98, 105, 113, 134, 146, 158, 173, 174, 186, 189, 194, 209, 210, 221, ...	A163782
$\overline{J_2}$	2, 3, 6, 11, 14, 18, 23, 26, 30, 35, 39, 50, 51, 74, 83, 86, 90, 95, 98, 99, 119, 131, 134, 135, 146, 155, 158, 174, 179, 183, 186, 191, 194, ...	A163781

Table 1: Small elements in $P(X)$.

(4) *A number n in $\mathbb{N}_2$ is A_1^--prime if and only if $n \equiv 3 \pmod 4$, $2n+1$ is a prime number, and -2 is a generator of $\mathbb{Z}^\star_{2n+1}$, but $+2$ is not: $-2 \in G_{2n+1}$ and $+2 \notin G_{2n+1}$.* □

Since there are no A_0-primes with $n \equiv 0 \pmod 4$ [2], we may replace "n is even" in Theorem 3.1(1) by "$n \equiv 2 \pmod 4$".

We consider these brands of Archimedes primes as building blocks to formulate characterizations for other X-primes.

For a permuting operation X, we define $H(X)$ by $H(X) = \{n/2 \mid n \in P(X) - \{2\}\}$.

Theorem 3.2. [2]

(1) $P(J_2) = H(S) = P(A_0) \cup P(A_1^+)$,

(2) $P(\overline{J_2}) = H(\overline{S}) = P(A_0) \cup P(A_1^-)$, *and*

(3) $P(T) = P(A_0) \cup P(A_1) = P(A_0) \cup P(A_1^+) \cup P(A_1^-)$

in which $P(A_0)$, $P(A_1^+)$ and $P(A_1^-)$ are mutually disjoint sets. Consequently,

(4) $P(T) = P(J_2) \cup P(\overline{J_2}) = H(S) \cup H(\overline{S})$, *with*

(5) $P(J_2) \cap P(\overline{J_2}) = H(S) \cap H(\overline{S}) = P(A_0)$. □

Earlier we called $\overline{S}$ and $\overline{J_2}$ the dual operations of S and J_2, respectively. For the formal definition of duality we refer to Section 6 of [2], but Theorems 3.1 and 3.2 may give a hint.

n		$\pi(S,n)$	$\pi(\overline{S},n)$	$\pi(T,n)$	$\pi(A_0,n)$	$\pi(A_1,n)$
	N	$\pi(s,I)$	$\pi(\overline{s},I)$	$\pi(t,N)$	$\pi(a_0,N)$	$\pi(a_1,N)$
10^1	$2{\cdot}10^1{+}1$	3	2	5	2	3
10^2	$2{\cdot}10^2{+}1$	13	12	30	11	19
10^3	$2{\cdot}10^3{+}1$	67	69	177	61	116
10^4	$2{\cdot}10^4{+}1$	470	465	1257	418	839
10^5	$2{\cdot}10^5{+}1$	3603	3612	10084	3378	6706
10^6	$2{\cdot}10^6{+}1$	29341	29438	83584	27882	55702
10^7	$2{\cdot}10^7{+}1$	248491	248761	713154	237676	475478
10^8	$2{\cdot}10^8{+}1$	2154733	2153846	6214402	2071170	4143232

Table 2: Counting X- and x-primes; $X \in \{S, \overline{S}, T, A_0, A_1\}$, $x \in \{s, \overline{s}, t, a_0, a_1\}$; $I = (N{+}1)/2$.

To complete the picture we mention that A_1^- is the dual of A_1^+ (and vice versa) and that the operations T, A_0 and A_1 are self-dual, i.e, they themselves may serve as their dual.

4 Counting X-primes

We count the several X-primes in a way similar to counting ordinary prime numbers —as in, for instance, §1.5 of [28]— and we comment on their distribution.

Let $\pi(X,n)$ be the number of X-primes less than or equal to n. Then our counting results are summarized in Tables 2 and 3. In Table 2 we should ignore the second row and the second column for the moment; the resulting smaller table will be referred to as Table 2A. Similarly, we obtain Table 3A by deleting the second row and the second and last columns in Table 3.

As to be expected Tables 2A and 3A confirm the equalities of Theorem 3.2. So we have, e.g., $\pi(T,n) = \pi(A_0,n) + \pi(A_1^+,n) + \pi(A_1^-,n)$. The verification of the other equalities of Theorem 3.2 is left to the reader; cf. Table 1 as well.

Table 4 shows that the distributions of the S-, $\overline{S}$-, T-, A_0-, A_1-, A_1^+-, A_1^--, J_2- and $\overline{J_2}$-primes exhibit a "Prime Number Theorem-like" behavior.

Let $\mathbb{P}$ the set of odd prime numbers and let $\pi(\mathbb{P},n)$ the number of odd prime numbers less than or equal to n. Remember that the Prime Number Theorem reads as:

Prime Number Theorem. *The function $\pi(\mathbb{P},n)$ is asymptotic to $n/\ln n$. That is* $\lim_{n\to\infty} \pi(\mathbb{P},n) \ln n/n = 1$. □

From Table 4 we observe that the distributions of X-primes show limiting values

$\Lambda(X) = \lim_{n\to\infty} \pi(X,n) \ln n/n$

unequal to 1. Of course, it is possible to infer some rough estimates for $\Lambda(X)$ from Table 4, but we will not do so. Instead we will follow a detour in the next sections.

n		$\pi(A_1^+,n)$	$\pi(A_1^-,n)$	$\pi(J_2,n)$	$\pi(\overline{J_2},n)$	
	N	$\pi(a_1^+,N)$	$\pi(a_1^-,N)$	$\pi(j_2,N)$	$\pi(\overline{j_2},N)$	$\pi(\mathfrak{P},N)$
10^1	$2{\cdot}10^1{+}1$	2	1	4	3	3
10^2	$2{\cdot}10^2{+}1$	10	9	21	20	21
10^3	$2{\cdot}10^3{+}1$	55	61	116	122	147
10^4	$2{\cdot}10^4{+}1$	421	418	839	836	1125
10^5	$2{\cdot}10^5{+}1$	3328	3378	6706	6756	8977
10^6	$2{\cdot}10^6{+}1$	27861	27841	55743	55723	74416
10^7	$2{\cdot}10^7{+}1$	237656	237822	475332	475498	635170
10^8	$2{\cdot}10^8{+}1$	2072304	2070928	4143474	4142098	5538820

Table 3: Counting X-, x- and $\mathfrak{P}$-primes; $X \in \{A_1^+, A_1^-, J_2, \overline{J_2}\}$, $x \in \{a_1^+, a_1^-, j_2, \overline{j_2}\}$.

5 Associated Prime Numbers: x-primes

Now we assign to each X-prime an ordinary prime number in an obvious way.

Definition 5.1. Let X be equal to T, A_0, A_1, A_1^+, A_1^-, J_2, or $\overline{J_2}$. If n is X-prime, then the number $2n+1$ is called the prime number associated with n; we also call $2n+1$ an *x-prime*. The set of all x-primes $\{2n+1 \mid n \in P(X)\}$ is denoted by $P(x)$.

If X is equal to S or $\overline{S}$, then the x-prime associated with the X-prime n, is $n+1$, and $P(x) = \{n+1 \mid n \in P(X)\}$. □

Counting x-primes is summarized in Table 2B (obtained from Table 2 by deleting the first row and the first column) and Table 3B (which results from Table 3 when we ignore the first row, the first and the last columns). For the distribution of x-primes we refer to Table 5 (cf. Table 4 for the distribution of the corresponding X-primes). In Table 5 the s- and $\overline{s}$-primes are scaled differently (Definition 5.1): it allows a comparison with the j_2- and the $\overline{j_2}$-primes, respectively; cf. Theorem 5.4(1)-(2) and Corollary 5.7(1)-(2).

An odd prime number is called *Pythagorean* if it is the hypotenuse of a right triangle with integer sides. Typical examples are 5 and 13 since $5^2 = 3^2 + 4^2$ and $13^2 = 5^2 + 12^2$; cf. A002144 in [26]. Let $\mathfrak{P}$ denote the set of Pythagorean primes. We recall the following two characterizations of $\mathfrak{P}$.

Proposition 5.2. *Let p be an odd prime number. Then*

(1) *$p \in \mathfrak{P}$ if and only if $p \equiv 1 \pmod 4$.*

(2) *$p \in \mathfrak{P}$ if and only if for all g in G_p, $-g$ belongs to G_p as well.* □

Theorems 3.1 and 3.2 yield the following characterizations of x-primes, respectively.

Theorem 5.3. *Let $p \geq 5$ be a prime number. Then*

(1) *$p \in P(a_0)$ if and only if $p \equiv 5 \pmod 8$, and -2 is in G_p.*

(2) *$p \in P(a_0)$ if and only if $p \equiv 5 \pmod 8$, and $+2$ is in G_p.*

n	$\pi(X,n)\ln n/n$								
	S	$\overline{S}$	T	A_0	A_1	A_1^+	A_1^-	J_2	$\overline{J_2}$
10^1	0.6908	0.4605	1.1513	0.4605	0.4605	0.4605	0.2303	0.9210	0.6908
10^2	0.5987	0.5526	1.3816	0.5066	0.8750	0.4605	0.4145	0.9671	0.9210
10^3	0.4628	0.4766	1.2227	0.4214	0.8013	0.3799	0.4214	0.8013	0.8427
10^4	0.4329	0.4283	1.1577	0.3850	0.7727	0.3878	0.3850	0.7727	0.7700
10^5	0.4148	0.4158	1.1610	0.3889	0.7721	0.3832	0.3889	0.7721	0.7778
10^6	0.4054	0.4067	1.1548	0.3852	0.7696	0.3849	0.3846	0.7701	0.7698
10^7	0.4005	0.4010	1.1495	0.3831	0.7664	0.3831	0.3833	0.7661	0.7664
10^8	0.3969	0.3967	1.1447	0.3815	0.7632	0.3817	0.3815	0.7633	0.7630

Table 4: Distribution of S-, $\overline{S}$-, T-, A_0-, A_1-, A_1^+-, A_1^--, J_2- and $\overline{J_2}$-primes.

(3) $p \in P(a_1)$ *if and only if* $p \equiv 3 \pmod 4$, *and only one of* -2 *and* $+2$ *is in* G_p.
(4) $p \in P(a_1^+)$ *if and only if* $p \equiv 3 \pmod 8$, *and* $+2$ *is in* G_p, *but* -2 *is not.*
(5) $p \in P(a_1^-)$ *if and only if* $p \equiv 7 \pmod 8$, *and* -2 *is in* G_p, *but* $+2$ *is not.*

Proof. The statements 5.3(3), 5.3(4) and 5.3(5) directly follow from Theorem 3.1(2), 3.1(3) and 3.1(4), respectively.

Similarly, we obtain from Theorem 3.1(1), that $p \in P(a_0)$ if and only if $p \equiv 5 \pmod 8$, and both -2 and $+2$ are in G_p. But if $p \equiv 5 \pmod 8$, then p is Pythagorean by Proposition 5.2(1), and Proposition 5.2(2) implies that one of the two conditions on G_p may be dropped, which yields both 5.3(1) and 5.3(2). □

Theorem 5.4.
(1) $P(j_2) = P(s) = P(a_0) \cup P(a_1^+)$,
(2) $P(\overline{j_2}) = P(\overline{s}) = P(a_0) \cup P(a_1^-)$, *and*
(3) $P(t) = P(a_0) \cup P(a_1) = P(a_0) \cup P(a_1^+) \cup P(a_1^-)$
in which $P(a_0)$, $P(a_1^+)$ *and* $P(a_1^-)$ *are mutually disjoint sets. Consequently,*
(4) $P(t) = P(j_2) \cup P(\overline{j_2}) = P(s) \cup P(\overline{s})$, *with*
(5) $P(j_2) \cap P(\overline{j_2}) = P(s) \cap P(\overline{s}) = P(a_0)$. □

Example 5.5. (1) If n is A_0-prime, then $2n+1$ is a_0-prime and by Theorem 5.3 and Proposition 5.2(1) a Pythagorean prime. But $P(a_0)$ is a proper subset of $\mathfrak{P}$: $109 \in \mathfrak{P}$ but 109 is not a_0-prime because 54 is not A_0-prime. Note that $G_{109} = \{\pm 6, \pm 10, \pm 11, \pm 13, \pm 14, \pm 18, \pm 24, \pm 30, \pm 37, \pm 39, \pm 40, \pm 42, \pm 44, \pm 47, \pm 50, \pm 51, \pm 52, \pm 53\}$, and G_{109} contains neither $+2$ nor -2.
(2) The first few t-primes are: 5, 7, 11, 13, 19, 23, 29 and 37. Clearly, 17 and 31 are in $\mathbb{P}$ but not in $P(t)$, as neither $+2$ nor -2 are in G_{17} or G_{31}: $G_{17} = \{\pm 3, \pm 5, \pm 6, \pm 7\}$ and $G_{31} = \{-14, -10, -9, -7, 3, 11, 12, 13\}$. □

N	$\pi(x,I)\ln I/I$		$\pi(x,N)\ln N/N$						
	s	$\overline{s}$	t	a_0	a_1	a_1^+	a_1^-	j_2	$\overline{j_2}$
$2{\cdot}10^1{+}1$	0.6540	0.4360	0.7249	0.2900	0.4349	0.2900	0.1450	0.5799	0.4349
$2{\cdot}10^2{+}1$	0.5940	0.5483	0.7915	0.2902	0.5013	0.2638	0.2375	0.5541	0.5277
$2{\cdot}10^3{+}1$	0.4624	0.4762	0.6724	0.2317	0.4407	0.2089	0.2317	0.4407	0.4635
$2{\cdot}10^4{+}1$	0.4328	0.4282	0.6224	0.2070	0.4154	0.2085	0.2069	0.4154	0.4139
$2{\cdot}10^5{+}1$	0.4148	0.4158	0.6154	0.2062	0.4093	0.2031	0.2062	0.4093	0.4123
$2{\cdot}10^6{+}1$	0.4054	0.4067	0.6063	0.2023	0.4041	0.2021	0.2020	0.4044	0.4042
$2{\cdot}10^7{+}1$	0.4005	0.4010	0.5995	0.1998	0.3997	0.1998	0.1999	0.3995	0.3997
$2{\cdot}10^8{+}1$	0.3969	0.3968	0.5939	0.1979	0.3960	0.1980	0.1979	0.3960	0.3959

Table 5: Distribution of s-, $\overline{s}$-, t-, a_0-, a_1-, a_1^+-, a_1^--, j_2- and $\overline{j_2}$-primes; $I=(N{+}1)/2$.

In view of Theorem 5.3 it is useful to look at the odd prime numbers modulo 8, for which we need Euler's totient function and a strong version of Dirichlet's Theorem.

Remember that Euler's totient function $\varphi:\mathbb{N}\to\mathbb{N}$ is defined by: $\varphi(n)$ is the number of integers k $(1\le k<n)$ that are relatively prime to n, i.e., $\gcd(k,n)=1$.

In the sequel we use the following sets of odd prime numbers:

$\pi(\mathbb{P},N)=\#\{p\in\mathbb{P}\mid p\le N\}$,

$\pi(\mathbb{P},N;a,b)=\#\{p\in\mathbb{P}\mid p\le N,\ p\equiv a\,(\mathrm{mod}\ b)\}$,

$\pi(x,N)=\#\{p\in P(x)\mid p\le N\}$, and

$\pi(x,N;a,b)=\#\{p\in P(x)\mid p\le N,\ p\equiv a\,(\mathrm{mod}\ b)\}$,

where $\#F$ is the number of elements of the finite set F.

Dirichlet's Theorem. *Let a and b be positive numbers with* $\gcd(a,b)=1$. *Then*

$$\lim_{N\to\infty}\frac{\pi(\mathbb{P},N;a,b)}{\pi(\mathbb{P},N)}=\frac{1}{\varphi(b)}\quad,$$

i.e., the set of odd primes that are congruent to a modulo b has density $1/\varphi(b)$ in $\mathbb{P}$. □

Consequently, for $b=8$ we have $\varphi(8)=4$ and the odd prime numbers are equally distributed over the four residue classes 1, 3, 5, 7 modulo 8; see also Table 6.

Example 5.6. Counting results for Pythagorean primes are in Table 3. Note that by Proposition 5.2, $\pi(\mathfrak{P},N)=\pi(\mathbb{P},N;1,4)$ and so $\pi(\mathfrak{P},N)=\pi(\mathbb{P},N;1,8)+\pi(\mathbb{P},N;5,8)$; cf. Tables 3 and 6. □

From Theorem 5.4 we obtain the following equalities.

Corollary 5.7. *For each positive integer N, we have*

(1) $\pi(j_2,N)=\pi(s,N)=\pi(a_0,N)+\pi(a_1^+,N)$,

N	$\pi(\mathbb{P}, N; a, 8)$				$\pi(\mathbb{P}, N)$	$\pi(\mathbb{P}, N) \ln N/N$
	$a=1$	$a=3$	$a=5$	$a=7$		
$2{\cdot}10^1{+}1$	1	3	2	1	7	1.01484081
$2{\cdot}10^2{+}1$	8	12	13	12	45	1.18730707
$2{\cdot}10^3{+}1$	68	77	79	78	302	1.14723813
$2{\cdot}10^4{+}1$	556	571	569	565	2261	1.11953894
$2{\cdot}10^5{+}1$	4466	4495	4511	4511	17983	1.09750398
$2{\cdot}10^6{+}1$	37116	37261	37300	37255	148932	1.08040120
$2{\cdot}10^7{+}1$	317477	317768	317693	317668	1270606	1.06802325
$2{\cdot}10^8{+}1$	2769023	2770106	2769797	2770010	11078936	1.05880438

Table 6: Counting odd primes modulo 8.

(2) $\pi(\overline{j_2}, N) = \pi(\overline{s}, N) = \pi(a_0, N) + \pi(a_1^-, N)$,

(3) $\pi(t, N) = \pi(a_0, N) + \pi(a_1, N) = \pi(a_0, N) + \pi(a_1^+, N) + \pi(a_1^-, N)$,

(4) $\pi(t, N) = \pi(j_2, N) + \pi(\overline{j_2}, N) - \pi(a_0, N)$,

(5) $\pi(t, N) = \pi(s, N) + \pi(\overline{s}, N) - \pi(a_0, N)$. □

Apart from twin primes —i.e., pairs $(p, p{+}2)$ such that both p and $p{+}2$ are prime numbers— there are other ways to couple prime numbers to sibling primes. In this context we quote two results from [3] on T-primes (Theorem 5.8); by Definition 5.1 we obtain similar results for t-primes (Corollary 5.9) and, consequently, two example families of such sibling primes.

Theorem 5.8. [3]

(1) *If both p and $2p{+}1$ are prime numbers, then p is a T-prime.*

(2) *If both p and $4p{+}1$ are prime numbers, then $2p$ is a T-prime.* □

Corollary 5.9.

(1) *If both p and $2p{+}1$ are prime numbers, then $2p{+}1$ is a t-prime.*

(2) *If both p and $4p{+}1$ are prime numbers, then $4p{+}1$ is a t-prime.* □

Numbers p with the property that both p and $2p{+}1$ are prime, are the so-called Sophie Germain prime numbers; cf. A005384 in [26]. So if p is a Sophie Germain prime, then $2p{+}1$ is a t-prime by Corollary 5.9(1) and, consequently, p is a T-prime.

Generalizing Corollary 5.9 to a statement of the form "If both p and $2kp{+}1$ are prime numbers, then $2kp{+}1$ is a t-prime" will not work. For $k = 3$ the smallest counter-example is $p = 5$, as 31 is not a t-prime. For $k = 4$ the situation is even more dramatic: no number n with $n \equiv 1 \pmod 8$ is t-prime, because all numbers equivalent $0 \pmod 4$ are not T-prime [3, 2]. And notice that replacing $2k$ by $2k{+}1$ will be unsuccessful for all $k \geq 1$ and all odd prime numbers p, because $(2k{+}1)p{+}1$ is even.

6 Distribution of the Associated Prime Numbers

In this section we will first apply the main result from [17] (Theorem 6.3) to some x-primes (Theorem 6.4). Then we will take an alternative approach based on Artin's conjecture on primitive roots; see Theorems 6.5, 6.7 and 6.8. These latter two theorems heavily rely on a result on the distribution of prime numbers p with a prescribed generator of $\mathbb{Z}_p^\star$ over residue classes (Theorem 3 in [19]).

But first we need a definition and a few results from number theory.

Definition 6.1. Let p be an odd prime. The number a is a *quadratic residue of* p if the congruence $x^2 \equiv a \pmod{p}$ has a solution. When no such solution exists, the number a is called a *quadratic non-residue of* p. □

Proposition 6.2.

(1) *The number* $+2$ *is a quadratic residue of primes of the form* $8k \pm 1$ *and a quadratic non-residue of primes of the form* $8k \pm 3$.

(2) *The number* -2 *is a quadratic residue of primes of the form* $8k+1$ *and* $8k+3$*, and a quadratic non-residue of primes of the form* $8k+5$ *and* $8k+7$. □

Proposition 6.2(1) is well-known; for a proof we refer to Theorem 95 in [8], Theorem 3.103 in [1], or §4.1 in [16]. And Proposition 6.2(2) can be proven as Theorem 95 in [8]; cf. Example 4.1.18 in [16]. Proposition 6.2 plays an important role in establishing characterization results for T-primes (Queneau numbers); see [3, 6, 2].

Let p be an odd prime and a any number not divisible by p. Then *Legendre's symbol* (a/p) is defined by

$(a/p) = +1$ if a is a quadratic residue of p, and

$(a/p) = -1$ if a is a quadratic non-residue of p.

The main result from [17] now reads as follows. Note that "generator of $\mathbb{Z}_p^\star$" is usually referred to as "primitive root modulo p" in number theory [8, 1, 16].

Theorem 6.3. [17] *Let* $g \in \mathbb{Z}$ *be unequal to* -1, 0 *and* $+1$*, and let* h *be the largest integer such that* g *is an* h*-th power. Let* $\pi_g(\mathbb{P}, N; a, b)$ *denote the number of odd primes less than or equal to* N *such that* $p \equiv a \pmod{b}$ *and* g *is a primitive root modulo* p*. Then, under the Generalized Riemann Hypothesis,*

$$\pi_g(\mathbb{P}, N; a, b) = 2 \cdot \sum_{\substack{2<p\le N \\ (g/p)=-1 \\ p\equiv a \pmod{b} \\ \gcd(p-1,h)=1}} \frac{\varphi(p-1)}{p-1} \quad + \quad R_N$$

where φ *is Euler's totient function and* R_N *satisfies* $R_N \in O(N \log\log N / \log^2 N)$. □

The exact formulation of the Generalized Riemann Hypothesis (GRH) is less relevant in the present context; it suffices to remark that it is used in the proof of Theorem 6.3 to show that R_N is sufficiently small, viz. $R_N \in O(N \log\log N / \log^2 N)$.

We apply Theorem 6.3 to obtain the distribution for some of the x-primes.

Theorem 6.4. *Under the Generalized Riemann Hypothesis, we have*

(1) $\pi(a_0, N) = 2 \cdot \sum_{2<p\le N,\ p\equiv 5 \pmod 8} \frac{\varphi(p-1)}{p-1} \ + \ R_N$,

(2) $\pi(a_1^+, N) = 2 \cdot \sum_{2<p\le N,\ p\equiv 3 \pmod 8} \frac{\varphi(p-1)}{p-1} \ + \ R_N$,

(3) $\pi(a_1^-, N) = 2 \cdot \sum_{2<p\le N,\ p\equiv 7 \pmod 8} \frac{\varphi(p-1)}{p-1} \ + \ R_N$,

where φ is Euler's totient function and R_N is as in Theorem 6.3.

Proof. We first observe that by Theorem 5.3(1), 5.3(2), 5.3(4) and 5.3(5) we have

$\pi(a_0, N) = \pi_{-2}(\mathbb{P}, N; 5, 8) = \pi_{+2}(\mathbb{P}, N; 5, 8)$,

$\pi(a_1^+, N) = \pi_{+2}(\mathbb{P}, N; 3, 8)$, and

$\pi(a_1^-, N) = \pi_{-2}(\mathbb{P}, N; 7, 8)$.

Next we apply Theorem 6.3; note that in all three cases we have $h = 1$, and therefore $\gcd(p-1, h) = 1$.

(1) By Proposition 6.2(2) we obtain $(-2/p) = -1$ since $p \equiv 5 \pmod 8$. Similarly, Proposition 6.2(1) yields $(+2/p) = -1$ as well.

(2) $p \equiv 3 \pmod 8$ and Proposition 6.2(1) imply $(+2/p) = -1$.

(3) From Proposition 6.2(2) and $p \equiv 7 \pmod 8$, it follows that $(-2/p) = -1$. □

Similar distributions can be obtained for a_1-, j_2-, $\overline{j_2}$-, s-, $\overline{s}$- and t-primes by Theorem 6.4 and Corollary 5.7.

With Dirichlet's Theorem and Theorem 6.4 in mind, we are tempted to conjecture that $\Lambda(a_0) = \Lambda(a_1^+) = \Lambda(a_1^-)$, provided the function $\varphi(p-1)/(p-1)$ behaves in some uniform fashion over the residue classes 1, 3, 5 and 7 modulo 8; cf. Theorems 6.7 and 6.8.

Although the distributions in Theorem 6.4 are simple as compared to the one in Theorem 6.3, they are rather unsatisfactory from a computational point of view. Therefore we will continue into another direction.

When we compare Tables 2B, 3B and 6 we observe that in each interval we have $\pi(a_0, N) < \pi(\mathbb{P}, N; 5, 8)$, $\pi(a_1^+, N) < \pi(\mathbb{P}, N; 3, 8)$ and $\pi(a_1^-, N) < \pi(\mathbb{P}, N; 7, 8)$. This should not come as a surprise since we ignored the additional restrictions on the generators of $\mathbb{Z}_p^\star$ (or, primitive roots modulo p); cf. Theorem 3.1.

This leads us to the following well-known conjecture in which $\mathbb{S}(g)$ is the set of prime numbers p such that g is a primitive root modulo p, i.e., g generates the cyclic group $\mathbb{Z}_p^\star$.

Artin's Conjecture on Primitive Roots (**ACPR**). *Let g be an integer which is not a perfect square and not equal to -1, and let $g = g_0 h^2$ with g_0 square-free. Then*

(1) *$\mathbb{S}(g)$ is infinite, and $\mathbb{S}(g)$ has a positive asymptotic density in $\mathbb{P}$.*

(2) *If in addition g is not a perfect power and if g_0 is not congruent 1 modulo 4, this density is independent of g and equals Artin's constant* **A**. □

Artin's constant **A** is defined as the infinite product

$$\mathbf{A} = \prod_{p \text{ is prime}} \left(1 - \frac{1}{p(p-1)}\right) = 0.37395581361920228805472805434641641 51\cdots .$$

Theorem 6.5. *Under the assumption of ACPR, we have*

$\Lambda(j_2) = \Lambda(\overline{j_2}) = \Lambda(s) = \Lambda(\overline{s}) = \mathbf{A}$.

Proof. From Theorems 5.3(2), 5.3(4), 5.4(1), together with ACPR applied to $g = g_0 = 2$ and $h = 1$, we obtain that $P(j_2) = \mathbb{S}(2)$, $P(j_2)$ is infinite, and $\Lambda(j_2) = \mathbf{A}$.

In a similar way Theorems 5.3(1), 5.3(5), 5.4(2), and ACPR yield $P(\overline{j_2}) = \mathbb{S}(-2)$, $P(\overline{j_2})$ is infinite, and $\Lambda(\overline{j_2}) = \mathbf{A}$.

Finally, Theorem 5.4(1)1–(2) or Corollary 5.7(1)–(2) implies $\Lambda(s) = \Lambda(\overline{s}) = \mathbf{A}$. □

Hooley [10] proved that ACPR follows from the Generalized Riemann Hypothesis (GRH); so in Theorems 6.5 we may replace ACPR by GRH as well.

Next we will show, under the assumption of GRH, that $\Lambda(a_0) = \mathbf{A}/2$; cf. Theorem 6.7. It is possible to infer this equality by going step by step through Artin's heuristic approach —as given in, e.g., [27] or [20]— together with the additional requirement that $p \equiv 1 \pmod 4$ and relying on an application of Dirichlet's Theorem, which results in $\Lambda(a_0) = \mathbf{A}/\varphi(4) = \mathbf{A}/2$. However, we prefer to derive Theorem 6.7 from one of the main results of [19] which we also need in Section 7. We do not use the complete, most general version of Theorem 3 of [19], since for our purposes a special instance (Theorem 6.6) suffices. For other similar statements that are particular instances of Theorems 1–3 in [19] we refer to [18, 27]. Again we need some concepts from number theory.

The *Möbius function* $\mu : \mathbb{N} \to \{-1, 0, +1\}$ is defined by

- $\mu(n) = +1$ if n is squarefree and n has an even number of prime factors,
- $\mu(n) = -1$ if n is squarefree and n has an odd number of prime factors,
- $\mu(n) = 0$ if n is not squarefree.

Let $n \neq 0$ be an integer with prime factorization $n = u \cdot p_1^{e_1} \cdots p_k^{e_k}$, where $u \in \{+1, -1\}$ and p_i are primes. Let a be an integer. Then the *Kronecker symbol* $(a|n)$ is defined by

$$(a|n) = (a|u) \cdot \prod_{i=1}^{k} (a|p_i)^{e_i}.$$

If p_i is odd, then $(a|p_i) = (a/p_i)$ (Legendre symbol); for $p_1 = 2$, $(a|2)$ is defined by

- $(a|2) = 0$ if a is even,
- $(a|2) = +1$ if $a \equiv \pm 1 \pmod 8$, and
- $(a|2) = -1$ if $a \equiv \pm 3 \pmod 8$.

Finally, $(a|1) = 1$, and $(a|-1) = 1$ if $a \geq 0$ and $(a|-1) = -1$ otherwise.

Let $\Lambda_g(a, b)$ be the density defined by $\Lambda_g(a, b) = \lim_{n\to\infty} \pi_g(\mathbb{P}, n; a, b)/\pi(\mathbb{P}, n)$ or, equivalently, by $\Lambda_g(a, b) = \lim_{n\to\infty} \pi_g(\mathbb{P}, n; a, b) \ln n/n$.

Remember that $\|n\|$ denotes the odd part of n, i.e., the odd number such that $n/\|n\|$ is a power of 2.

Theorem 6.6. (Theorem 3 from [19] with $f = 2^k$, $k \geq 1$). *Let g be an integer not equal to -1 or a square; let $h \geq 1$ be the largest integer such that g is an h-th power. Write $g = g_1 g_2^2$, with g_1 squarefree and both g_1 and g_2 integer. Let a and b be natural numbers with $1 \leq a < b = 2^k$ for some $k \geq 1$, and a odd. Let*

$$\beta = [\![g_1]\!] \ , \qquad \gamma = (-1)^{(\beta-1)/2} \gcd(g_1, b)$$

and

$$A(h) = \frac{1}{2} \cdot \prod_{\substack{p \geq 3 \\ p|h}} \left(1 - \frac{1}{p-1}\right) \prod_{\substack{p \geq 3 \\ p \nmid h}} \left(1 - \frac{1}{p(p-1)}\right)$$

if $\gcd(a-1, b, h) = 1$ *and* $A(h) = 0$ *otherwise, where* p *runs through all the prime numbers.*

Then, under the Generalized Riemann Hypothesis, we have

$$\Lambda_g(a, b) = \frac{A(h)}{\varphi(b)} \left(1 - (\gamma|a) \frac{\mu(|\beta|)}{\prod_{p|\beta,\ p|h}(p-2) \prod_{p|\beta,\ p \nmid h}(p^2-p-1)}\right)$$

if $g_1 \equiv 1 \pmod 4$ *or* $g_1 \equiv 2 \pmod 4$ *and* $k \geq 3$ *or* $g_1 \equiv 3 \pmod 4$ *and* $k \geq 2$*, and*

$$\Lambda_g(a, b) = \frac{A(h)}{\varphi(b)}$$

otherwise. □

Theorem 6.7. *Under the assumption of GRH, we have* $\Lambda(a_0) = \mathbf{A}/2$.

Proof. By Theorem 5.3(2) we have $\Lambda(a_0) = \Lambda_2(5, 8)$. Thus we apply Theorem 6.6 with $g = g_1 = 2$, $h = 1$, $a = 5$, $b = 8$ $(k = 3)$, $\beta = 1$, $\mu(|\beta|) = 1$, and $\gamma = 2$. Consequently, we obtain

$$A(1) = \frac{1}{2} \cdot \prod_{p \geq 3} \left(1 - \frac{1}{p(p-1)}\right) = \prod_{p \geq 2} \left(1 - \frac{1}{p(p-1)}\right) = \mathbf{A},$$

and $\Lambda(a_0) = \Lambda_2(5, 8) = A(1)(1 - (2|5))/\varphi(8) = \mathbf{A}(1+1)/4 = \mathbf{A}/2$. □

Theorem 6.8. *Under the assumption of GRH, we have*

$\Lambda(a_1^+) = \Lambda(a_1^-) = \mathbf{A}/2$,

$\Lambda(a_1) = \mathbf{A}$, *and*

$\Lambda(t) = 3\mathbf{A}/2$.

Proof. From Corollary 5.7 we obtain by taking limits for $N \to \infty$:

$\Lambda(j_2) = \Lambda(a_0) + \Lambda(a_1^+)$,

$\Lambda(\overline{j_2}) = \Lambda(a_0) + \Lambda(a_1^-)$,

$\Lambda(a_1) = \Lambda(a_1^+) + \Lambda(a_1^-)$, and

$\Lambda(t) = \Lambda(a_0) + \Lambda(a_1)$.

Now, using Theorems 6.5 and 6.7 it is straightforward to obtain the results. □

Thus the set $P(t)$ of prime numbers associated with the Queneau numbers has density $3\mathbf{A}/2$ in $\mathbb{P}$, the set $P(a_0)$ of prime numbers associated with the even Queneau numbers has density $\mathbf{A}/2$ in $\mathbb{P}$, and the set $P(a_1)$ of prime numbers associated with the odd Queneau numbers has density $\mathbf{A}$ in $\mathbb{P}$.

g	$+2$	-2	$+3$	-3	$+5$	-5	$+6$
$d_g^+(N)$	0.374031		0.226523		0.139052		0.055954
$d_g^\pm(N)$	0.374031	0.373947	0.181194	0.142723	0.068735	0.073519	0.030383
g	-6	$+7$	-7	$+10$	-10	$+11$	-11
$d_g^+(N)$		0.068789		0.023048		0.037256	
$d_g^\pm(N)$	0.030337	0.035154	0.034617	0.016340	0.016330	0.018119	0.018070
g	$+12$	-12	$+13$	-13	$+14$	-14	$+15$
$d_g^+(N)$	0.003268		0.023168		0.008276		0.004226
$d_g^\pm(N)$	0.000496	0.000428	0.012191	0.012204	0.005509	0.005504	0.002326
g	-15	$+17$	-17	$+18$	-18	$+19$	-19
$d_g^+(N)$		0.011582		0.000408		0.007601	
$d_g^\pm(N)$	0.002282	0.006319	0.006311	0.000374	0.000374	0.004425	0.004426

Table 7: $d_g^+(N)$ and $d_g^\pm(N)$ for odd primes that have g as minimal generator of $\mathbb{Z}_p^\star$ (minimal primitive root modulo p) for $N = 150000001$.

7 Generators (Primitive Roots) Other Than $+2$ and -2

In the previous sections the numbers $+2$ and -2 played an important part as generator of $\mathbb{Z}_p^\star$. Now 0 and $+1$ never can be such a generator, and this observation also applies to -1 whenever $p \neq 3$. Consequently, $+2$ and -2 can be considered as minimal generators of $\mathbb{Z}_p^\star$. In looking for minimal generators we can distinguish two points of view.

In the first and usual one, the residue classes modulo p are represented by the numbers 0, 1, ... , $p-1$ and we determine the smallest g with $2 \leq g < p-1$ that generates $\mathbb{Z}_p^\star$; see [21, 22] for results along this approach.

Alternatively, we can represent the residue classes modulo p with $p = 2n+1$ by $-n, \ldots, -1, 0, +1, \ldots, +n$, where $n+1, n+2, \ldots, 2n$ are represented by $-n, -n+1, \ldots, -1$, respectively. This representation is useful in dealing with Queneau numbers (T^{-1}-primes) [3] or T-primes [2]. For each of these representatives, we can define its absolute value [3], and so we are looking for the smallest $|g|$ with $2 \leq |g| \leq n$ such that g generates $\mathbb{Z}_p^\star$.

Of course, for Pythagorean prime numbers both approaches yield closely connected results, but in general there is a considerable difference in values between those two points of view. Table 7 contains, for small values of $|g|$, numerical approximations of the densities (or, actually, the relative frequencies) $d_g^+(N)$ and $d_g^\pm(N)$ of odd primes less than or equal to N that have g as minimal generator: for $d_g^+(N)$ we search in the interval $2 \leq g \leq p-1$ and for $d_g^\pm(N)$ in the interval $2 \leq |g| \leq n$. In Table 3 of [22] more accurate values of $d_g^+(N)$ are given based on a much larger interval (viz. $N = 4 \cdot 10^{10}$). Notice that the values of $d_{+2}^+(N)$, $d_{+2}^\pm(N)$ and $d_{-2}^\pm(N)$ tend to $\mathbf{A}$ as the interval length N increases; cf. Theorems 5.3, 5.4, 6.5, 6.7 and 6.8.

						$a=$	1	3	5	7	9	11	13	15
g	g_1	h	β	$\mu(\lvert\beta\rvert)$	γ		$(\gamma\lvert a)$							
2	2	1	1	1	2		1	−1	−1	1	1	−1	−1	1
−2	−2	1	−1	1	−2		1	1	−1	−1	1	1	−1	−1
3	3	1	3	−1	−1		1	−1	1	−1	1	−1	1	−1
−3	−3	1	−3	−1	1		1	1	1	1	1	1	1	1
−4	−1	1	−1	1	−1		1	−1	1	−1	1	−1	1	−1
5	5	1	5	−1	1		1	1	1	1	1	1	1	1
−5	−5	1	−5	−1	−1		1	−1	1	−1	1	−1	1	−1
6	6	1	3	−1	−2		1	1	−1	−1	1	1	−1	−1
−6	−6	1	−3	−1	2		1	−1	−1	1	1	−1	−1	1
7	7	1	7	−1	−1		1	−1	1	−1	1	−1	1	−1
−7	−7	1	−7	−1	1		1	1	1	1	1	1	1	1
8	2	3	1	1	2		1	−1	−1	1	1	−1	−1	1
−8	−2	3	−1	1	−2		1	1	−1	−1	1	1	−1	−1
−9	−1	1	−1	1	−1		1	−1	1	−1	1	−1	1	−1
10	10	1	5	−1	2		1	−1	−1	1	1	−1	−1	1
−10	−10	1	−5	−1	−2		1	1	−1	−1	1	1	−1	−1

Table 8: Relevant data for the proof of Theorem 7.1.

To place our results from Section 6 (Theorems 6.5, 6.7 and 6.8) in a broader context we will now look at the distribution of prime numbers with small primitive roots (other than $+2$ or -2) over the residue classes a modulo b where a is odd and $b = 2^k$ for $1 \leq k \leq 4$.

Theorem 7.1. *Let g be a natural number with $2 \leq |g| \leq 10$, $g \neq 4$ and $g \neq 9$. Then for natural numbers a and b with $1 \leq a < b = 2^k$ $(1 \leq k \leq 4)$ and a odd, the value of $\Lambda_g(a,b)$ is, under the assumption of GHR, as in Tables 9 and 10.*

Proof. First, we establish the values of $\Lambda_g(a,b)$ as mentioned in Table 10: $b = 16$ and a is odd with $1 \leq a < 16$. Table 8 contains the relevant data for these cases in order to apply Theorem 6.6. In the proof of Theorem 6.7 we showed that $A(1) = \mathbf{A}$. Similarly, we have

$$A(3) = \frac{1}{2} \cdot \prod_{p=3} \left(1 - \frac{1}{p-1}\right) \prod_{p \geq 5} \left(1 - \frac{1}{p(p-1)}\right) = \frac{1}{2} \cdot \frac{1}{2} \cdot \mathbf{A} \cdot \left(\frac{1}{2} \cdot \frac{5}{6}\right)^{-1} = 3\mathbf{A}/5.$$

Now it is straightforward to compute all entries of Table 10; we give two sample computations, viz. for g equal to 7 we have

$$\Lambda_7(1,16) = \Lambda_7(5,16) = \Lambda_7(9,16) = \Lambda_7(13,16) = \frac{\mathbf{A}}{8} \cdot \left(1 - 1 \cdot \frac{-1}{7^2 - 7 - 1}\right) = 21\mathbf{A}/164,$$

g	$\Lambda_g =$ $\Lambda_g(1,2)$	$\Lambda_g(a,4)$		$\Lambda_g(a,8)$			
		$a=1$	$a=3$	$a=1$	$a=3$	$a=5$	$a=7$
2	$\mathbf{A}$	$\mathbf{A}/2$	$\mathbf{A}/2$	0	$\mathbf{A}/2$	$\mathbf{A}/2$	0
-2	$\mathbf{A}$	$\mathbf{A}/2$	$\mathbf{A}/2$	0	0	$\mathbf{A}/2$	$\mathbf{A}/2$
3	$\mathbf{A}$	$3\mathbf{A}/5$	$2\mathbf{A}/5$	$3\mathbf{A}/10$	$\mathbf{A}/5$	$3\mathbf{A}/10$	$\mathbf{A}/5$
-3	$6\mathbf{A}/5$	$3\mathbf{A}/5$	$3\mathbf{A}/5$	$3\mathbf{A}/10$	$3\mathbf{A}/10$	$3\mathbf{A}/10$	$3\mathbf{A}/10$
-4	$\mathbf{A}$	0	$\mathbf{A}$	0	$\mathbf{A}/2$	0	$\mathbf{A}/2$
5	$20\mathbf{A}/19$	$10\mathbf{A}/19$	$10\mathbf{A}/19$	$5\mathbf{A}/19$	$5\mathbf{A}/19$	$5\mathbf{A}/19$	$5\mathbf{A}/19$
-5	$\mathbf{A}$	$10\mathbf{A}/19$	$9\mathbf{A}/19$	$5\mathbf{A}/19$	$9\mathbf{A}/38$	$5\mathbf{A}/19$	$9\mathbf{A}/38$
6	$\mathbf{A}$	$\mathbf{A}/2$	$\mathbf{A}/2$	$3\mathbf{A}/10$	$3\mathbf{A}/10$	$\mathbf{A}/5$	$\mathbf{A}/5$
-6	$\mathbf{A}$	$\mathbf{A}/2$	$\mathbf{A}/2$	$3\mathbf{A}/10$	$\mathbf{A}/5$	$\mathbf{A}/5$	$3\mathbf{A}/10$
7	$\mathbf{A}$	$21\mathbf{A}/41$	$20\mathbf{A}/41$	$21\mathbf{A}/82$	$10\mathbf{A}/41$	$21\mathbf{A}/82$	$10\mathbf{A}/41$
-7	$42\mathbf{A}/41$	$21\mathbf{A}/41$	$21\mathbf{A}/41$	$21\mathbf{A}/82$	$21\mathbf{A}/82$	$21\mathbf{A}/82$	$21\mathbf{A}/82$
8	$3\mathbf{A}/5$	$3\mathbf{A}/10$	$3\mathbf{A}/10$	0	$3\mathbf{A}/10$	$3\mathbf{A}/10$	0
-8	$3\mathbf{A}/5$	$3\mathbf{A}/10$	$3\mathbf{A}/10$	0	0	$3\mathbf{A}/10$	$3\mathbf{A}/10$
-9	$\mathbf{A}$	0	$\mathbf{A}$	0	$\mathbf{A}/2$	0	$\mathbf{A}/2$
10	$\mathbf{A}$	$\mathbf{A}/2$	$\mathbf{A}/2$	$5\mathbf{A}/19$	$9\mathbf{A}/38$	$9\mathbf{A}/38$	$5\mathbf{A}/19$
-10	$\mathbf{A}$	$\mathbf{A}/2$	$\mathbf{A}/2$	$5\mathbf{A}/19$	$5\mathbf{A}/19$	$9\mathbf{A}/38$	$9\mathbf{A}/38$

Table 9: Distribution of odd primes modulo 2, 4 and 8, respectively, with prescribed generator g.

and

$$\Lambda_7(3,16) = \Lambda_7(7,16) = \Lambda_7(11,16) = \Lambda_7(15,16) = \frac{\mathbf{A}}{8} \cdot \left(1 - (-1) \cdot \frac{-1}{7^2 - 7 - 1}\right) = 5\mathbf{A}/41.$$

We leave the computation of the remaining entries in Table 10 to the reader.

Obviously, we may obtain Table 9 in a similar way, but it is less tedious to sum up the appropriate columns using $\Lambda_g(a, b/2) = \Lambda_g(a, b) + \Lambda(a + b/2, b)$, where a is odd with $1 \le a < b = 2^k$ ($k = 2, 3, 4$). □

Notice that in the right upper corner of Table 9 the identities $\Lambda(a_0) = \Lambda_2(5,8) = \Lambda_{-2}(5,8) = \mathbf{A}/2$, $\Lambda(a_1^+) = \Lambda_2(3,8) = \mathbf{A}/2$ and $\Lambda(a_1^-) = \Lambda_{-2}(7,8) = \mathbf{A}/2$ from Theorems 6.7 and 6.8 reappear.

This observation arises the obvious question whether we can introduce new permuting operations X on strings that leads us via their families of permutations $\{X_n\}_{n\ge2}$, and characterizations of their sets $P(X)$ and $P(x)$ of X-primes and associated ordinary prime numbers to entries in Tables 9 and 10 different from the ones for g equal to $+2$ or -2.

Considering the Josephus permuting operations J_k for $k \ge 3$ provides no answer to this question. In Table 1 of [2] the first few J_k-primes for $3 \le k \le 20$ are given: the

g	$\Lambda_g(a,16)$							
	$a=1$	$a=3$	$a=5$	$a=7$	$a=9$	$a=11$	$a=13$	$a=15$
2	0	$\mathbf{A}/4$	$\mathbf{A}/4$	0	0	$\mathbf{A}/4$	$\mathbf{A}/4$	0
-2	0	0	$\mathbf{A}/4$	$\mathbf{A}/4$	0	0	$\mathbf{A}/4$	$\mathbf{A}/4$
3	$3\mathbf{A}/20$	$\mathbf{A}/10$	$3\mathbf{A}/20$	$\mathbf{A}/10$	$3\mathbf{A}/20$	$\mathbf{A}/10$	$3\mathbf{A}/20$	$\mathbf{A}/10$
-3	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$3\mathbf{A}/20$
-4	0	$\mathbf{A}/4$	0	$\mathbf{A}/4$	0	$\mathbf{A}/4$	0	$\mathbf{A}/4$
5	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$5\mathbf{A}/38$
-5	$5\mathbf{A}/38$	$9\mathbf{A}/76$	$5\mathbf{A}/38$	$9\mathbf{A}/76$	$5\mathbf{A}/38$	$9\mathbf{A}/76$	$5\mathbf{A}/38$	$9\mathbf{A}/76$
6	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$\mathbf{A}/10$	$\mathbf{A}/10$	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$\mathbf{A}/10$	$\mathbf{A}/10$
-6	$3\mathbf{A}/20$	$\mathbf{A}/10$	$\mathbf{A}/10$	$3\mathbf{A}/20$	$3\mathbf{A}/20$	$\mathbf{A}/10$	$\mathbf{A}/10$	$3\mathbf{A}/20$
7	$\frac{21}{164}\mathbf{A}$	$\frac{5}{41}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{5}{41}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{5}{41}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{5}{41}\mathbf{A}$
-7	$\frac{21}{164}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$	$\frac{21}{164}\mathbf{A}$
8	0	$3\mathbf{A}/20$	$3\mathbf{A}/20$	0	0	$3\mathbf{A}/20$	$3\mathbf{A}/20$	0
-8	0	0	$3\mathbf{A}/20$	$3\mathbf{A}/20$	0	0	$3\mathbf{A}/20$	$3\mathbf{A}/20$
-9	0	$\mathbf{A}/4$	0	$\mathbf{A}/4$	0	$\mathbf{A}/4$	0	$\mathbf{A}/4$
10	$5\mathbf{A}/38$	$9\mathbf{A}/76$	$9\mathbf{A}/76$	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$9\mathbf{A}/76$	$9\mathbf{A}/76$	$5\mathbf{A}/38$
-10	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$9\mathbf{A}/76$	$9\mathbf{A}/76$	$5\mathbf{A}/38$	$5\mathbf{A}/38$	$9\mathbf{A}/76$	$9\mathbf{A}/76$

Table 10: Distribution of odd primes modulo 16 with prescribed generator g.

values in this table suggest that $\Lambda(J_k) = 0$ for $3 \leq k \leq 20$. In addition we mention that a characterization of $P(J_k)$ for $k \neq 2$ in terms of finite fields of prime order is very unlikely [2]. Consequently, notions like "j_k-prime", "$P(j_k)$" and "$\Lambda(j_k)$" are meaningless for $k \geq 3$.

More promising is an approach by Roubaud [23] and Dumas [5, 6]. Their generalization of the "quenine" (i.e., the Queneau-Daniel spiral permutation or, equivalently, T_n^{-1}) to the "g-quenine" (spiral permutation with multiplier g) suggests the following generalization of the twist operation on strings.

The *zigzag* operation on strings Z_g models the cutting of a deck of n cards in g (almost) equal parts $D_1, \ldots, D_g$, putting the even numbered parts upside down and interleaving (shuffling) the g resulting parts (in order $D_2D_4D_6 \cdots D_g \cdots D_3D_1$ provided g divides n).

Example 7.2. We consider $Z_3(\alpha_{15})$: so we divide α_{15} in 3 equal parts D_1, D_2 and D_3 of which we put D_2 upside down. This results in $a_1a_2a_3a_4a_5$, $a_{10}a_9a_8a_7a_6$ and $a_{11}a_{12}a_{13}a_{14}a_{15}$. Interleaving/shuffling with order of parts equal to $D_2D_3D_1$ yields

$Z_3(\alpha_{15}) = a_{10}a_{11}a_1a_9a_{12}a_2a_8a_{13}a_3a_7a_{14}a_4a_6a_{15}a_5$,

$\langle Z_{3,15} \rangle = (1\ 3\ 9\ 4\ 12\ 5\ 15\ 14\ 11\ 2\ 6\ 13\ 8\ 7\ 10)$, $\#\langle Z_{3,15} \rangle = 15$ which means that 15 is Z_3-prime. Analogously, we have for $Z_4(\alpha_{12})$ with order $D_2D_4D_3D_1$:

$Z_4(\alpha_{12}) = a_6a_{12}a_7a_1a_5a_{11}a_3a_8a_4a_{10}a_9a_2$,

$\langle Z_{4,12}\rangle = (1\ 4\ 9\ 11\ 6)(2\ 8\ 7\ 3\ 12)(5)(10)$, $\#\langle Z_{4,12}\rangle = 5$ and hence 12 is not Z_4-prime. □

Rather than formally defining this permuting operation on strings —which is a bit complicated— we directly turn to the family of corresponding permutation $\{Z_{g,n}\}_{n\geq 2}$. This family defines Z_g indirectly and it can be defined concisely in case n is a multiple of g and if $\gcd(g, 2n{+}1) = 1$ (as in Example 7.2); viz. for $1 \leq k \leq g$ and $1 \leq m \leq n$,

$$Z_{g,n}(m) \equiv o_k\, g\, m \,(\mathrm{mod}\ 2n{+}1), \qquad \text{if } (k{-}1)n < gm \leq kn,$$

where o_k is the parity function with $o_k = +1$ if k is odd and $o_k = -1$ if k is even.

When n is not a multiple of g, we have to decide to which part we assign the "remaining elements" before we start the interleaving process (which in turn happens to be more complicated in this case). However, in special cases we can rely on a slight generalization of a definition of Dumas [5, 6].

Definition 7.3. Let g and n be integers such that $1 \leq g \leq n$ and $\gcd(g, 2n{+}1) = 1$. The *zigzag permutation* $Z_{g,n}$ is the permutation

$$\begin{aligned} Z_{g,n}(m) &\equiv +gm \,(\mathrm{mod}\ 2n{+}1), && \text{if } 2kn < gm \leq (2k+1)n \text{ with } 0 \leq k \leq \lceil (g-1)/2 \rceil, \\ Z_{g,n}(m) &\equiv -gm \,(\mathrm{mod}\ 2n{+}1), && \text{otherwise.} \end{aligned}$$

The g subintervals of $[1, n]$ where the sign of the multiplication is constant are called the *regions* of $Z_{g,n}$. □

These regions are in fact the parts $D_1, \ldots, D_g$ in the interleaving process: the parts D_i have a factor $+g$ in the multiplication if i is odd, and the parts D_i have a factor $-g$ if i is even. It is easy to see that Z_1 is the identity operation.

Dumas' original definition [5, 6] requires that "$2n{+}1$ is a prime number" instead of "$\gcd(g, 2n{+}1) = 1$". Now Definition 7.3 implies that Z_2 equals the twist operation T, i.e., $Z_{2,n} = T_n$ for each n and not only for those n for which $2n{+}1$ is a prime number. Definition 7.3 also allows us to consider permutations, like $Z_{4,12}$ as in Example 7.2, for which $2n{+}1$ is not a prime number. Dropping the condition "$\gcd(g, 2n{+}1) = 1$" might, however, result in mappings $Z_{g,n}$ that are not a permutation.

Example 7.4. For $n = 11$, $g = 3$ and $g = 5$ with $\gcd(g, 23) = 1$, Definition 7.3 yields: $Z_{3,11} = (1\ 3\ 9\ 4\ 11\ 10\ 7\ 2\ 6\ 5\ 8)$ and, respectively, $Z_{5,11} = (1\ 5\ 2\ 10\ 4\ 3\ 8\ 6\ 7\ 11\ 9)$. Since $\#\langle Z_{3,11}\rangle = \#\langle Z_{5,11}\rangle = 11$, we have that 11 is Z_3-prime and also Z_5-prime.

A graphical representation of $Z_{3,11}$ shows that the interleaving order is $D_2D_3D_1$ with $D_1 = a_1a_2a_3$, $D_2 = a_4a_5a_6a_7$ and $D_3 = a_8a_9a_{10}a_{11}$. And for $Z_{5,11}$ the interleaving order is $D_4D_3D_2D_5D_1$ with $D_1 = a_1a_2$, $D_2 = a_3a_4$, $D_3 = a_5a_6$, $D_4 = a_7a_8a_9$ and $D_5 = a_{10}a_{11}$. □

We are now ready to quote one of the main results from [5, 6] which, of course, relies on Dumas' original definition. But, obviously, this characterization applies to Z_g as given in Definition 7.3 as well.

Theorem 7.5. [5, 6] *Let g and n be a natural numbers such that $2n{+}1$ is a prime number and $g \leq n$. Then n is Z_g-prime if and only if one of the following conditions holds.*

(1) *g is of order $2n$ in $\mathbb{Z}^\star_{2n+1}$ or, equivalently, g generates $\mathbb{Z}^\star_{2n+1}$.*

(2) *n is odd and g is of order n in $\mathbb{Z}^\star_{2n+1}$.* □

Example 7.6. Since 23 is prime and 5 is of order 22 in $\mathbb{Z}_{23}^{\star}$, we have by Theorem 7.5(1) that 11 is Z_5-prime. And from Theorem 7.5(2) and the facts that 11 is odd and 3 has order 11 in $\mathbb{Z}_{23}^{\star}$, we obtain that 11 is also Z_3-prime; cf. Example 7.4. □

Theorem 7.5 is a promising starting point to characterize the sets $P(Z_g)$, the sets of associated prime numbers $P(z_g)$ and their densities in $\mathbb{P}$, which might correspond to entries in Tables 9–10 other than the ones for $g = +2$ and $g = -2$.

8 Concluding Remarks

In the previous sections we counted X-primes for X in $\{S, \overline{S}, T, A_0, A_1, A_1^+, A_1^-, J_2, \overline{J_2}\}$ and their associated prime numbers (x-primes). Then we investigated the distribution of these prime numbers. Going from X-primes to x-primes has the advantage that $\Lambda(x)$ can be interpreted as the density of $P(x)$ in $\mathbb{P}$. Of course, the values of $\Lambda(X)$ do not allow such an interpretation: note in particular that $\Lambda(T) > 1$ (Table 4). When we return from x-primes to X-primes we obtain the following $\Lambda(X)$-values:

$$\begin{aligned} &\Lambda(X) = 2 \cdot \Lambda(x), \quad && X \in \{T, A_0, A_1, A_1^+, A_1^-, J_2, \overline{J_2}\} \\ &\Lambda(X) = \Lambda(x), && X \in \{S, \overline{S}\}. \end{aligned}$$

Our main results on the density of x-primes in $\mathbb{P}$ (Theorems 6.5, 6.7 and 6.8) as well as the entires in Tables 9–10 are —strictly spoken— mere conjectures rather than genuine theorems because they rely on unproven statements like GRH and/or ACPR.

On the other hand, Theorems 6.5, 6.7 and 6.8 are supported by numerical evidence; see the entries in Table 5 and note that $\mathbf{A}/2 = 0.18697790680960114402\cdots$, and $3\mathbf{A}/2 = 0.56093372042880343208\cdots$. The deviations of 6% are as to be expected for $N = 2{\cdot}10^8{+}1$; cf. Table 6. For smaller deviations —and more support— we have to extend Table 5 considerably, e.g., to $2 \cdot 10^{20}{+}1$ as Table 1.8 in [28]. Using the logarithmic integral or the Riemann function —cf. §1.5 in [28]— instead of $N/\ln N$ yields tables similar to Table 5, smaller deviations (viz. less than 0.05% for $N = 2 \cdot 10^8{+}1$) and so additional support; cf. Tables 1.9 and 1.11 in [28].

Clearly, the zigzag permuting operation Z_g deserves more attention. Based on Definition 7.3 we need characterization results like Theorems 3.2(3), 5.4(3), Corollary 5.7(3) and Theorem 6.8 for Z_g and z_g. In this approach we are looking for spiral permutations that will take the role of Archimedes' spirals and of the sets $P(a_0)$, $P(a_1^+)$ and $P(a_1^-)$ as played in the present paper; the work of Roubaud [23] and Dumas [5, 6] is a good source for such spirals.

References

1. J.A. Anderson & J.M. Bell, *Number Theory with Applications* (1997), Prentice-Hall, Upper Saddle River, NJ.
2. P.R.J. Asveld, Permuting operations on strings and their relation to prime numbers, *Discr. Appl. Math.* **159** (2011) 1915-1932.

3. M. Bringer, Sur un problème de R. Queneau, *Math. Sci. Humaines/Math. Soc. Sci.* **27** (1969) 13–20.

4. C.W. Carroll & W.F. Orr, On the generalization of the sestina, *Delta (Waukesha)* **5** (1975) 32–44.

5. J.-G. Dumas, Caractérisation des quenines et leur représentation spirale, *Math. Sci. Humaines/Math. Soc. Sci.* **184** (2008) 9–23.

6. J.-G. Dumas, Les rayons des permutations spirales, *Math. Sci. Humaines/Math. Soc. Sci.* **192** (2010) 5–27.

7. R.L. Graham, D.E. Knuth & O. Patashnik, *Concrete Mathematics* (1989), Addison-Wesley, Reading, MA.

8. G.H. Hardy & E.M. Wright, *An Introduction to the Theory of Numbers* (1938), Fourth edition (1959), Oxford University Press, Oxford, UK.

9. I.N. Herstein & I. Kaplansky, *Matters Mathematical* (1974), Harper & Row, New York.

10. C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967) 209–220.

11. M. Jantzen, The power of synchronizing operations on strings, *Theoret. Comput. Sci.* **14** (1981) 127–154.

12. M. Jantzen, On twist-closed trios: a new morphic characterization of r.e. sets, *Found. of Comput. Sci.* 97, Lect. Notes in Comput. Sci. **1337** (1997) Springer, Berlin, pp. 143–152.

13. M. Jantzen, Hierarchies of principal twist-closed trios, *STACS* 98, Lect. Notes in Comput. Sci. **1373** (1998) Springer, Berlin, pp. 344–355.

14. M. Jantzen & A. Kurgansky, Refining the hierarchy of blind multicounter languages and twist-closed trios, *Inform. Comput.* **185** (2003) 158–181.

15. M. Lothaire, *Combinatorics on Words* (1983), Addison-Wesley, Reading, MA.

16. R.A. Mollin, *Fundamental Number Theory with Applications* (1998), CRC Press, Boca Raton, FL.

17. P. Moree, On primes in arithmetic progression having a prescribed primitive root, *J. Number Theory* **78** (1999) 85–98.

18. P. Moree, Uniform distribution of primes having a prescribed primitive root, *Acta Arithmetica* **LXXXIX** (1999) 9–21.

19. P. Moree, On primes in arithmetic progression having a prescribed primitive root II, *Funct. Approx. Comment. Math.* **39** (2008), part 1, 133–144.

20. M.R. Murty, Artin's conjecture for primitive roots, *Math. Intell.* **10** (1988) 59–67.

21. A. Paszkiewicz & A. Schinzel, On the least prime primitive root modulo a prime, *Math. of Comput.* **71** (2002) 1307-1321.

22. A. Paszkiewicz & A. Schinzel, Numerical calculation of the density of prime numbers with a given least primitive root, *Math. of Comput.* **71** (2002) 1781-1797.

23. J. Roubaud, Réflexions historiques et combinatoires sur la n-ine autrement dit quenine, *La bibliothèque Oulipienne* 5/66 (2000) 99–124 [Contribution à la réunion 395 de l'Oulipo, le 17 septembre 1993].

24. M.P. Saclolo, How a medieval troubadour became a mathematical figure, *Notices Amer. Math. Soc.* **58** (2011) 682–687; correction/addition *Notices Amer. Math. Soc.* **58** (2011) 895.

25. P. Schumer, The Josephus problem; once more around, *Math. Mag.* **75** (2002) 12–17.

26. N.J.A. Sloane, `http://oeis.org/Seis.html` — *On-Line Encyclopedia of Integer Sequences*, An earlier, non-electronic version appeared as: N.J.A. Sloane & S. Plouffe, *The Encyclopedia of Integer Sequences* (1995), Academic Press, San Diego CA, etc.

27. P. Stevenhagen. The correction factor in Artin's primitive root conjecture, *J. Théor. Nombres Bordeaux* **15** (2003) 383-391.

28. S.Y. Yan, *Number Theory for Computing* (2000), Springer-Verlag, Berlin – Heidelberg – New York.