Number theoretic aspects of a combinatorial function

Lorenz Halbeisen[1] and Norbert Hungerbühler

Abstract

We investigate number theoretic aspects of the integer sequence $\mathrm{seq}^{1\text{-}1}(n)$ with identification number A000522 in Sloane's On-Line Encyclopedia of Integer Sequences: $\mathrm{seq}^{1\text{-}1}(n)$ counts the number of sequences without repetition one can build with n distinct objects. By introducing the the notion of the "shadow" of an integer function, we examine divisibility properties of the combinatorial function $\mathrm{seq}^{1\text{-}1}(n)$: We show that $\mathrm{seq}^{1\text{-}1}(n)$ has the reduction property and its shadow d therefore is multiplicative. As a consequence, the shadow d of $\mathrm{seq}^{1\text{-}1}(n)$ is determined by its values at powers of primes. It turns out that there is a simple characterization of regular prime numbers, i.e. prime numbers p for which the shadow d of $\mathrm{seq}^{1\text{-}1}$ has the socket property $d(p^k) = d(p)$ for all integers k. Although a stochastic argument supports the conjecture that infinitely many irregular primes exist, there density is so thin that there is only one irregular prime number less than $2.5 \cdot 10^6$, namely 383.

1 Introduction

The sequence we are interested in has the ID number A000522 in Sloane's On-Line Encyclopedia of Integer Sequences (http://www.research.att.com/~njas/sequences). Former identification numbers of this sequence were M1497 in [SP] and N0589 in [Sl].

The sequence A000522 has many faces (see, e.g., [Ga], [Si] or [Ri]). The most accessible one is its combinatorial interpretation:

Definition 1 *For* $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ *let* $\mathrm{seq}^{1\text{-}1}(n)$ *denote the number of one-to-one sequences – these are sequences without repetitions – we can build with* n *distinct objects.*

[1] The author would like to thank the *Swiss National Science Foundation* for supporting him.

2000 Mathematics Subject Classification: **11A51** 11B50 11B75 11A41

Notice that for $l \leqslant n$, each one-to-one function from $\{0, \dots, l-1\}$ to $\{0, \dots, n-1\}$ corresponds in a unique way to a sequence without repetitions of $\{0, \dots, n-1\}$ of length l. For example, for two objects, say a_1 and a_2, we can build the following sequences:

$$\langle\ \rangle \text{ (= the empty sequence)}, \langle a_1 \rangle, \langle a_2 \rangle, \langle a_1, a_2 \rangle, \langle a_2, a_1 \rangle.$$

Hence, $\mathrm{seq}^{1\text{-}1}(2) = 5$. Of course, it is easy to find a general expression for $\mathrm{seq}^{1\text{-}1}(n)$. Since there are $\binom{k}{n}$ possible ways to choose k objects from a set of n (distinct) objects, and since k (distinct) objects give rise to $k!$ permutations, we get the following

Lemma 2 $\mathrm{seq}^{1\text{-}1}(n) = \sum_{k=0}^{n} \binom{n}{k} k! = \sum_{j=0}^{n} \frac{n!}{j!}$. ■

Also the next representation for $\mathrm{seq}^{1\text{-}1}(n)$ is elementary.

Lemma 3 *For all positive $n \in \mathbb{N}$ we have*

$$\mathrm{seq}^{1\text{-}1}(n) = \lfloor e\, n! \rfloor.$$

Remark: For $n = 0$ the formula does not hold, since $\mathrm{seq}^{1\text{-}1}(0) = 1 < 2 = \lfloor e\, 0! \rfloor$.

Proof of Lemma 3. According to Lemma 2 we have

$$\begin{aligned} en! &= \mathrm{seq}^{1\text{-}1}(n) + \sum_{j=n+1}^{\infty} \frac{n!}{j!} \\ &= \mathrm{seq}^{1\text{-}1}(n) + \\ &\quad + \underbrace{\frac{1}{n+1}\Big(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \frac{1}{(n+2)(n+3)(n+4)} + \dots\Big)}_{\leqslant \frac{1}{n+1}(e-1) < 1 \text{ for } n \geqslant 1}. \end{aligned}$$

■

The following recursive relation for $\mathrm{seq}^{1\text{-}1}(n)$ is an immediate consequence of the second formula in Lemma 2.

Lemma 4 *For all positive $n \in \mathbb{N}$ we have* $\mathrm{seq}^{1\text{-}1}(n) = n\, \mathrm{seq}^{1\text{-}1}(n-1) + 1$. ■

Using this formula, we finally get the following integral representation of $\mathrm{seq}^{1\text{-}1}(n)$.

Lemma 5 *For all $n \in \mathbb{N}$ we have*

$$\mathrm{seq}^{\text{1-1}}(n) = e \int_1^\infty t^n e^{-t} dt\,.$$

Proof. The formula is correct for $n = 0$. Moreover, by integration by parts, we have inductively

$$\begin{aligned}\mathrm{seq}^{\text{1-1}}(n) = e \int_1^\infty \underbrace{t^n}_{\downarrow} \underbrace{e^{-t}}_{\uparrow} dt &= e\left(-t^n e^{-t}\right)\Big|_1^\infty + e \int_1^\infty n t^{n-1} e^{-t} dt \\ &= 1 + n\,\mathrm{seq}^{\text{1-1}}(n-1)\end{aligned}$$

■

Just for the sake of completeness we like to mention that the exponential generating function $g(z)$ of $\mathrm{seq}^{\text{1-1}}(n)$ is given by $g(z) = \frac{e^z}{1-z}$. This is easily checked directly, or deduced, e.g. by Oberschelp's technique (see [Ob]).

In the sequel, to keep the formulas short, let $n^\star := \mathrm{seq}^{\text{1-1}}(n)$.

Notation: Throughout this text we adopt the standard notation $a|b$ to express that a divides b for $a, b \in \mathbb{N}$. Moreover, if $b \geqslant 1$ then $\mathrm{Mod}(a, b) := a - b\lfloor \frac{a}{b} \rfloor$ denotes the reminder of the division of a by b; and (a, b) denotes the greatest common divisor of a and b.

2 The divisibility of $n^\star$

We start our investigation on divisibility properties of $n^\star$ with a simple fact which has first been proved in [HS].

Lemma 6 *For natural numbers $n, k \in \mathbb{N}$, the following implication holds: If $2^k|n^\star$, then $2^k|(n+2^k)^\star$ and $2^k \nmid (n+t)^\star$ for any t with $0 < t < 2^k$.*

Proof. The implication $2^k|n^\star \implies 2^k|(n+2^k)^\star$ follows easily from the reduction property of the sequence $\mathrm{seq}^{\text{1-1}}(n)$ (see Lemma 9 below). So, we only have to prove here that if $2^k|n^\star$, then $2^k \nmid (n+t)^\star$ for any t with $0 < t < 2^k$.

For $k \leqslant 4$, an easy calculation modulo 2^k shows that for each n we have: If $2^k \mid n^\star$, then $2^k \nmid (n+t)^\star$ for $0 < t < 2^k$ (cf. also Lemma 9).

Assume there is a smallest k ($k \geqslant 4$) such that $2^{k+1}|n^\star$ and $2^{k+1} \mid (n+t)^\star$ for some t with $0 < t < 2^{k+1}$. Then, because $2^k|2^{k+1}$, we have $2^k|n^\star$ and $2^k|(n+t)^\star$. Since k

is by definition the smallest such number, we know that t must be 2^k.

$$
\begin{array}{rlllllr}
(n+2^k)^\star = \sum_{i=0}^{n+2^k} \frac{(n+2^k)!}{i!} = & 1\cdot 2\cdot & \ldots & \cdot 2^k\cdot (2^k+1)\cdot & \ldots & \cdot(2^k+n) & (1) \\
+ & 2\cdot & \ldots & \cdot 2^k\cdot & \ldots & \cdot(2^k+n) & (2) \\
 & & \ddots & & & & \vdots \\
+ & & & 2^k\cdot & \ldots & \cdot(2^k+n) & (2^k) \\
 & & & & \ddots & & \vdots \\
+ & & & & & (2^k+n) & (2^k+n) \\
+ & & & & & 1 & (2^k+n+1)
\end{array}
$$

It is easy to see that 2^{k+1} divides lines (1) – (2^k) since $k \geqslant 2$ and $n \geqslant 2$.

If we expand the products in the lines (2^k+1) – (2^k+n+1), we can collect all terms which are obviously divisible by 2^{k+1}. So, for a suitable natural number m we get

$$(n+2^k)^\star = 2^k \cdot \left(\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i\cdot j!} \right) + n^\star + 2^{k+1}\cdot m\,. \tag{1}$$

Remember that we have assumed $2^{k+1}|n^\star$, where $n \geqslant 3$ and $k \geqslant 4$. Thus, $n^\star$ is even and hence n has to be odd. If j is $n-1$, $n-2$ or $n-3$, then $\sum_{i>j}^{n} \frac{n!}{i\cdot j!}$ is odd. Moreover, if $0 \leqslant j \leqslant (n-4)$, then $\sum_{i>j}^{n} \frac{n!}{i\cdot j!}$ is even and therefore, $\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i\cdot j!}$ is odd. Hence, by (1) and $2^{k+1}|n^\star$ we get $2^{k+1} \nmid (n+2^k)^\star$, which is a contradiction.

■

Remark. The Lemma 6 is the crucial point in the proof – which does not make use of the axiom of choice – of the following fact (cf. [HS, Theorem 4]): For any infinite set M, there exists no bijection between the power-set of M and the set of all finite one-to-one sequences of M.

A natural question that arises in connection with Lemma 6 is whether for every $k \in \mathbb{N}$ there exists an $n \in \mathbb{N}$ such that $2^k \mid n^\star$. To answer this and related questions involving divisibility properties of integer sequences in general and of the sequence $\mathrm{seq}^{1\text{-}1}(n)$ in particular, we introduce the notion of the "shadow" of a sequence.

Definition 7 *If $\{f(n)\}_{n\in\mathbb{N}}$ is a sequence of natural numbers, we define its* **shadow** *to be the sequence $\{d(h)\}_{h\in\mathbb{N}}$ given by*

$$d(h) := |D(h)|,$$

where $D(h) := \big\{n \in \mathbb{N} : (n < h) \wedge (h \mid f(n))\big\}$ are the **shadow sets** *of the sequence f.*

The shadow $d(h)$ counts the sequence entries $f(0), f(1), \ldots, f(h-1)$ which are divisible by h. So, the shadow measures (to a certain extent) how "divisible" the entries of the sequence $f(n)$ are: For example, if only prime numbers occur in the sequence, then its shadow will reflect this fact by being small. If the entries of $f(n)$ have many divisors, the shadow will typically be large.

Remark. Lemma 6 implies that the shadow of $f(n) = \mathrm{seq}^{1\text{-}1}(n)$ has the following property: For all $k \in \mathbb{N}$, there holds $d(2^k) \leqslant 1$. Actually, as a consequence of Lemma 15, it will turn out that $d(2^k) = 1$ for all k.

Examples. If $f(n) = c \in \mathbb{N}$ is a constant function, then the shadow of f is

$$d(h) = \begin{cases} h & \text{if } h|c \text{ and } h > 1, \\ 0 & \text{otherwise.} \end{cases}$$

If $f(n)$ is an arithmetic sequence of first order, then its shadow is periodic, and for the shadow of Euler's φ-function we have $d(h) = 1$ for all $h \geqslant 1$. ○

The shadow gives a certain amount of information on the divisibility of the entries of a sequence. Nevertheless, two different sequences can "cast" the same shadow as the following example shows.

Example. If for a function f there exists an $n_0 \in \mathbb{N}$ such that for all $h \geqslant n_0$ we have $d(h) = 0$, then for all $h \geqslant n_0$ we have $f(h) \leqslant h$. Vice versa, if $f(h) \leqslant h$ for all $h \in \mathbb{N}$, then $d(h)$ equals the number of zeros in $(f(0), f(1), \ldots, f(h-1))$. Hence, it is easy to construct different functions which have the same shadow:

n	0	1	2	3	4	5	6	7	...
$f_1(n)$	0	1	2	3	4	5	6	7	...
$f_2(n)$	0	1	1	2	3	4	5	6	...
$f_3(n)$	0	1	1	1	2	3	4	5	...
shadow	0	1	1	1	1	1	1	1	...

○

Now, we want to investigate the shadow of $\mathrm{seq}^{1\text{-}1}(n)$. First, we show that this particular shadow is multiplicative and it turns out that the reason for this is the fact that $\mathrm{seq}^{1\text{-}1}$ has the reduction property:

Definition 8 *A sequence $\{f(n)\}_{n\in\mathbb{N}}$ is said to have the reduction property, if for all $n, q \in \mathbb{N}$, $q \geqslant 1$, we have*

$$\mathrm{Mod}(f(n), q) = \mathrm{Mod}(f(\mathrm{Mod}(n, q)), q).$$

Lemma 9 *The sequence $\{\mathrm{seq}^{1\text{-}1}(n)\}_{n\in\mathbb{N}}$ has the reduction property.*

Proof. For $q = 1$ or $q > n$, the statement is trivial. So, we may assume $1 < q \leqslant n$.

First we consider the case when $\mathrm{Mod}(n, q) = 0$. By Lemma 4 we have $\mathrm{seq}^{\text{1-1}}(n) = n \cdot \mathrm{seq}^{\text{1-1}}(n-1) + 1$ and hence by $\mathrm{Mod}(n, q) = 0$ we get $\mathrm{seq}^{\text{1-1}}(n) \equiv 1 \mod q$, which implies $\mathrm{Mod}(\mathrm{seq}^{\text{1-1}}(n), q) = \mathrm{Mod}(\mathrm{seq}^{\text{1-1}}(\mathrm{Mod}(n, q)), q)$, because $\mathrm{seq}^{\text{1-1}}(0) = 1$.

Now assume that $\mathrm{Mod}(n+1, q) \neq 0$ and that the statement holds for n. Again by Lemma 4 we have $\mathrm{seq}^{\text{1-1}}(n+1) = (n+1) \cdot \mathrm{seq}^{\text{1-1}}(n) + 1$ and by the assumption we get

$$\begin{aligned} \mathrm{seq}^{\text{1-1}}(n+1) &\equiv \mathrm{Mod}((n+1), q) \cdot \mathrm{seq}^{\text{1-1}}(\mathrm{Mod}(n, q)) + 1 \mod q \\ &\equiv \mathrm{seq}^{\text{1-1}}(\mathrm{Mod}(n+1, q)) \mod q. \end{aligned}$$

Therefore, $\mathrm{Mod}(\mathrm{seq}^{\text{1-1}}(n+1), q) = \mathrm{Mod}(\mathrm{seq}^{\text{1-1}}(\mathrm{Mod}(n+1, q)), q)$ is validated. ■

Lemma 10 *The shadow d of a sequence $f(n)$ which has the reduction property is multiplicative, i.e. if $(a, b) = 1$, then $d(ab) = d(a)d(b)$.*

Proof. Suppose $(a, b) = 1$, then we have by the reduction property

$$\begin{aligned} D(ab) &= \{n \in \mathbb{N} : n < ab \wedge ab | f(n)\} \\ &= \{n \in \mathbb{N} : n < ab \wedge a | f(n) \wedge b | f(n)\} \\ &= \{n \in \mathbb{N} : n < ab \wedge a | f(\mathrm{Mod}(n, a)) \wedge b | f(\mathrm{Mod}(n, b))\}. \end{aligned}$$

This means that a natural number n is an element of the shadow set $D(ab)$ if and only if it lies in the intersection of the two sets

$$A := \{i + ax : i \in D(a) \wedge x \in \{0, 1, \ldots, b-1\}\}$$

and

$$B := \{j + by : j \in D(b) \wedge y \in \{0, 1, \ldots, a-1\}\}.$$

In other words $D(ab) = A \cap B$.

Observe that since $(a, b) = 1$, we have that for all $\langle i, j \rangle \in \{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\}$ there exists a unique $\langle x, y \rangle \in \{0, 1, \ldots, b-1\} \times \{0, 1, \ldots, a-1\}$ such that $i + ax = j + by$. This implies that $|A \cap B| = |D(a)|\,|D(b)|$ and hence,

$$d(ab) = |D(ab)| = |A \cap B| = |D(a)|\,|D(b)| = d(a)\,d(b).$$ ■

As an immediate consequence we get the following

Corollary 11 *If d is the shadow of* $\mathrm{seq}^{1\text{-}1}$ *and if $n = \prod_{i=1}^{k} p_i^{k_i}$ is the prime decomposition of n, then*

$$d(n) = \prod_{i=1}^{k} d(p_i^{k_i}). \qquad \blacksquare$$

Therefore, the shadow d of $\mathrm{seq}^{1\text{-}1}$ is fully determined by its values on the powers of prime numbers. But what can we say about $d(p^k)$ for p prime? Let us start our discussion of this question by the following observation.

By the reduction property, all elements $m \in D(p^{k+1})$ must be of the form $m = n + l\,p^k$ for some $n \in D(p^k)$ and some $l \in \{0, 1, \ldots, p-1\}$. Hence, we get inductively that if $d(p) = 0$, then $d(p^k) = 0$ for all positive $k \in \mathbb{N}$.

Definition 12 *A prime number p with $d(p) = 0$ is called* **annihilating**.

Example. The sequence of annihilating primes is 3, 7, 11, 17, 47, 53, 61, 67, 73, 79, 89, 101, 139, 151, 157, 191, 199, ... ○

From the observation above and the multiplicativity property, we have

Proposition 13 *If $n \in \mathbb{N}$ is divisible by an annihilating prime, then $d(n) = 0$.* $\blacksquare$

What can we say about primes that are not annihilating? For positive numbers $p, k, l, n \in \mathbb{N}$ we have the following:

$$
\begin{aligned}
(n + l\,p^k)^\star &= \sum_{j=0}^{l\,p^k+n} \frac{(l\,p^k+n)!}{j!} \\
&= \frac{(l\,p^k+n)!}{0!} + \ldots + \frac{(l\,p^k+n)!}{(l\,p^k-1)!} + \frac{(l\,p^k+n)!}{(l\,p^k)!} + \ldots + \frac{(l\,p^k+n)!}{(l\,p^k+n)!} \\
&= \frac{(l\,p^k+n))!}{(l\,p^k-1)!}\,(l\,p^k-1)^\star + \sum_{j=l\,p^k}^{l\,p^k+n} \frac{(l\,p^k+n)!}{j!} \\
&= \Big((l\,p^k)\,(l\,p^k+1)\,\ldots(l\,p^k+n)\Big)\,(l\,p^k-1)^\star + \sum_{j=l\,p^k}^{l\,p^k+n} \frac{(l\,p^k+n)!}{j!} \\
&\equiv l\,p^k\,n!\,(l\,p^k-1)^\star + \sum_{j=l\,p^k}^{l\,p^k+n} \frac{(l\,p^k+n)!}{j!} \mod p^{k+1} \\
&\equiv l\,p^k\,n!\,(l\,p^k-1)^\star + l\,p^k \sum_{j=0}^{n-1}\sum_{i>j}^{n} \frac{n!}{j!\,i} + n^\star \mod p^{k+1} \\
&\equiv l\,p^k \left(n!\,(l\,p^k-1)^\star + \sum_{i=1}^{n}\sum_{j=0}^{i-1} \frac{n!}{j!\,i}\right) + n^\star \mod p^{k+1} \\
&\equiv l\,p^k \left(n!\,(l\,p^k-1)^\star + \sum_{j=0}^{n-1} \frac{n!}{(j+1)!}\,j^\star\right) + n^\star \mod p^{k+1} \\
&\equiv n^\star + l\,p^k \underbrace{\left(n!\,(p-1)^\star + \sum_{j=0}^{n-1} \frac{n!}{(j+1)!}\,j^\star\right)}_{=:s_{p,n}} \mod p^{k+1} \qquad (2)
\end{aligned}
$$

From this calculation it is clear that the numbers $s_{p,n}$ defined in the previous line are crucial for a further investigation of the shadow of seq[1-1].

Definition 14 *The number*

$$X(p) := \prod_{n\in D(p)} \mathrm{Mod}(s_{p,n}, p)$$

is called the **excess** *of the prime p. A prime number p with $X(p) \neq 0$ is called* **regular** *and otherwise* **irregular**.

Example. Since the empty product is by definition equal to 1, all annihilating primes are regular. The smallest irregular prime number is 383, all other primes less than $2.5 \cdot 10^6$ are regular.

Lemma 15 *If p is a regular prime number, then the shadow d of* $\mathrm{seq}^{1\text{-}1}$ *has the socket property at powers of p, i.e. $d(p^k) = d(p)$ holds for all positive $k \in \mathbb{N}$.*

Before we prove Lemma 15, we state the following consequence.

Proposition 16 *If d is the shadow of* $\mathrm{seq}^{1\text{-}1}$ *and if $n = \prod_{i=1}^{k} p_i^{k_i}$ is the prime decomposition of n, then*

$$d(n) = \prod_{i=1}^{k} d(p_i)$$

provided each prime p_i is regular or one of the primes is annihilating. ■

To prepare the proof of Lemma 15, we need a property of $s_{p,n}$, which is given in the following

Lemma 17 *If p and n are natural numbers, then*

$$s_{p,n} \equiv s_{p,n+p} \mod p.$$

Proof. Let $r := \mathrm{Mod}(n,p)$, then $n = ap + r$ for some $a \in \mathbb{N}$. We first consider the case $n \geqslant p$, thus $a \neq 0$. Because $n \geqslant p$ we have $n! \equiv 0 \mod p$ and therefore $s_{p,n} \equiv \sum\limits_{j=0}^{n-1} \frac{n!}{(j+1)!} j^\star \mod p$. Further we get

$$\begin{aligned}
\sum_{j=0}^{n-1} \frac{n!}{(j+1)!} j^\star &= \sum_{j=0}^{ap-2} \frac{n!}{(j+1)!} j^\star + \sum_{j=ap-1}^{n-1} \frac{n!}{(j+1)!} j^\star \\
&\equiv \sum_{j=ap-1}^{n-1} \frac{n!}{(j+1)!} j^\star \mod p \\
&\equiv \sum_{j=-1}^{r-1} \frac{r!}{(j+1)!} (p+j)^\star \mod p \\
&\equiv r!(p-1)^\star + \sum_{j=0}^{r-1} \frac{r!}{(j+1)!} j^\star \mod p\,.
\end{aligned}$$

If $n < p$, then $\mathrm{Mod}(n,p) = n$ and we get $r = n$. Hence, we have for all $p, n \in \mathbb{N}$ that

$$s_{p,n} \equiv r!(p-1)^\star + \sum_{j=0}^{r-1} \frac{r!}{(j+1)!} j^\star \mod p\,,$$

where $r := \mathrm{Mod}(n,p)$. ■

Proof of Lemma 15. Let p be a regular prime number. We proceed inductively: For $k = 1$ there is nothing to show. For exponents larger than 1 we recall that all elements $m \in D(p^{k+1})$ must be of the form $m = n + l\,p^k$ for some $n \in D(p^k)$ and some $l \in \{0, 1, \ldots, p-1\}$. By the calculation (2) above, we have

$$(n + l\,p^k)^\star \equiv n^\star + l\,p^k s_{p,n} \mod p^{k+1}.$$

Hence, it suffices to show, that

$$n \in D(p^k) \implies s_{p,n} \not\equiv 0 \mod p \tag{3}$$

In fact, since p is prime, if the conclusion of (3) holds, the congruence $n^\star + lp^k s_{p,n} \equiv 0 \mod p^{k+1}$ has a unique solution $l \in \{0, 1, \ldots, p-1\}$ and therefore, the sets $D(p^k)$ and $D(p^{k+1})$ have the same cardinality, which implies $d(p^k) = d(p^{k+1})$.

On the other hand, by Lemma 17, (3) holds for all k if it is true for $k = 1$. But this, by definition, is exactly the case for regular primes p. ■

3 How peculiar are irregular primes?

In this section we investigate the value of $d(p^k)$ for irregular primes p and $k \geqslant 1$, but first we recall some facts concerning regular primes.

For a regular prime p we have $d(p^k) = d(p)$ for any positive $k \in \mathbb{N}$. Further, by definition, a prime number p is annihilating if and only if $d(p) = 0$. Remember that all annihilating prime numbers are regular. Now, fix an irregular prime number p. What can we say for $k \geqslant 1$ about $d(p^k)$?

Example. If we consider the smallest irregular prime number $p = 383$, it turns out that $d(383) = 3$, but $d(383^k) = 2$ for all $k \geqslant 2$. The reason for this shall be explained below. ○

First note that – because p is not annihilating – $d(p) > 0$. Because p is assumed to be irregular, there exists at least one $n \in D(p)$ such that $\mathrm{Mod}(s_{p,n}, p) = 0$ and therefore, by Lemma 17, we have $\mathrm{Mod}(s_{p,n+lp}, p) = 0$ for all $l \in \mathbb{N}$.

For $k \geqslant 1$ and any $n \in D(p^k)$ with $\mathrm{Mod}(s_{p,n}, p) = 0$ we have either the case $p^{k+1} \nmid n^\star$ or the case $p^{k+1} \mid n^\star$.

If $n \in D(p^k)$ with $\mathrm{Mod}(s_{p,n}, p) = 0$ – depending in which case we are – we have either $p^{k+1} \nmid (n + l\,p)^\star$ (for all $l \in \mathbb{N}$) or $p^{k+1} \mid (n + l\,p)^\star$ (for all $l \in \mathbb{N}$). To see this, remember that by (2), for any $n, l \in \mathbb{N}$ we have

$$(n + l\,p^k)^\star \equiv n^\star + l\,p^k \cdot s_{p,n} \mod p^{k+1}\,.$$

Therefore, if $p^{k+1} \mid n^\star$ (or $p^{k+1} \nmid n^\star$) and $p \mid s_{p,n}$, then we get $p^{k+1} \mid (n + l\,p^k)^\star$ (or $p^{k+1} \nmid (n + l\,p^k)^\star$, respectively) for any $l \in \mathbb{N}$.

Now let

$$\delta(p) := |\{n \in D(p) : \mathrm{Mod}(s_{p,n}, p) \neq 0\}|\,,$$

and for $k \geqslant 2$ let

$$\varepsilon(p^k) := |\{n \in D(p^{k-1}) : \mathrm{Mod}(s_{p,n}, p) = 0 \,\wedge\, p^k \mid n^\star\}|\,.$$

Notice that if $\varepsilon(p^{k_0}) = 0$ for some $k_0 \geqslant 2$, then $\varepsilon(p^k) = 0$ for any $k \geqslant k_0$. By the facts given above, it is not hard to verify that for $k \geqslant 2$ we have

$$d(p^k) = \delta(p) + p \cdot \varepsilon(p^k)\,.$$

Example. If we consider again the smallest irregular prime number $p = 383$, where $D(383) = \{296,\, 340,\, 353\}$ and therefore $d(383) = 3$, it turns out that $\delta(383) = 2$ and $\varepsilon(383^2) = 0$. This we get because $\mathrm{Mod}(s_{383,\,296}, 383) = 0$ and $383^2 \nmid 296^\star$. Thus, $d(383^k) = \delta(383) = 2$ for all $k \geqslant 2$. ○

4 How rare are irregular primes?

We recall that a prime number p is irregular, if there exists an $n \in D(p)$ with $\mathrm{Mod}(s_{p,n}, p) = 0$. The function $n \mapsto \mathrm{Mod}(s_{p,n}, p)$ shows (for different primes p) a rather random-like behavior. The idea is now, to replace $n \mapsto \mathrm{Mod}(s_{p,n}, p)$ by equidistributed independent random variables $X_{p,n}$ which take values in $\{0, 1, \ldots, p-1\}$, i.e. the probability that $X_{p,n} = i$ is $\frac{1}{p}$ for each $i \in \{0, 1, \ldots, p-1\}$. From $X_{p,n}$ we construct a new random variable Y_p which takes, for each prime number p, the value 1 if $X_{p,n} = 0$ for some $n \in D(p)$ and zero otherwise. In other words, instead of looking whether $\mathrm{Mod}(s_{p,n}, p) = 0$ for $n \in D(p)$, we throw a dice with p faces $\{0, 1, \ldots, p-1\}$ for each $n \in D(p)$. Therefore, the values p for which $Y_p = 1$ are now called randomly irregular primes. The idea is, that randomly irregular primes should have approximately the same distribution as the ordinary irregular prime numbers. The probability that p is randomly regular is

$$P(p \text{ is randomly regular}) = \left(1 - \frac{1}{p}\right)^{d(p)}.$$

Thus, we have

$$\begin{aligned} P(p_1, p_2, \dots, p_k \text{ are all randomly regular}) &= \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)^{d(p_i)} \\ &= \exp \sum_{i=1}^{k} d(p_i) \log\left(1 - \frac{1}{p_i}\right). \end{aligned}$$

Observe, that $\log(1-x) \leqslant -x$ for $x \geqslant 0$ (and $|\log(1-x)+x| = O(x^2)$ for $x \to 0$). Thus, we can estimate

$$P(p_1, p_2, \dots, p_k \text{ are all randomly regular}) \lesssim \exp\left(-\sum_{i=1}^{k} \frac{d(p_i)}{p_i}\right).$$

If we suppose for the moment – and experiments support this to some extent – that in average $d(p) \approx c > 0$ is approximately constant (with a numerical value of $c \approx 0.9$), then we have

$$P(p_1, p_2, \dots, p_k \text{ are all randomly regular}) \lesssim \exp\left(-c\sum_{i=1}^{k} \frac{1}{p_i}\right). \tag{4}$$

Now, the sum of inverse primes is divergent, and hence,

$$P(p_1, p_2, \dots, p_k \text{ are all randomly regular}) \to 0 \quad \text{for } k \to \infty.$$

In other words, the probability that after a certain prime number no other randomly irregular prime number occurs is – under the made hypothesis on $d(p)$ – zero. So, we should expect that infinitely many irregular prime numbers exist.

On the other hand, what can we say about the frequency of occurrence of (randomly) irregular primes? In order to answer this question, we close this discussion by calculating the distribution function of randomly irregular prime numbers. In other words we ask: How many randomly irregular primes may we expect in the set $\{p_1, p_2, \dots, p_k\}$. This is simply

$$E\left[\sum_{i=1}^{k} \tilde{Y}_{p_i}\right] = \sum_{i=1}^{k} E[\tilde{Y}_{p_i}] = \sum_{i=1}^{k} \frac{d(p_i)}{p_i}.$$

Example. The expected number of randomly irregular prime numbers in the range $\{2,\ldots,10^3\}$ is $1.99703\ldots$ (the actual number of irregular primes in this interval is 1). Further, the expected number of randomly irregular primes in the interval $\{2,\ldots,10^6\}$ is about 2.67758, so still far below 3, and the expected number of randomaly irregular primes in the interval $\{385,\ldots,2.5\cdot 10^6\}$ is about 0.874123 (the actual number of irregular primes in this interval is 0). $\bigcirc$

Again, under the assumption that $d(p)$ is in average a positive constant c, we can now state the following conjecture:

Conjecture 18 *There exist infinitely many irregular primes. Furthermore the distribution function of the irregular primes is asymptotically*

$$\bigl|\{p \leqslant n : p \text{ is an irregular prime number}\}\bigr| \sim c \sum_{\substack{p\leqslant n\\ p \text{ prime}}} \frac{1}{p}$$

for a positive constant c.

Remark. If we consider the random variable Z which takes the value p where p is the smallest randomly irregular prime, then a similar calculation as above shows that the expected value of Z is $E[Z]=\infty$.

As a final remark we should mention that similar arguments as above support the conjecture that there are infinitely many prime numbers p, such that

$$2^{p-1} \equiv 1 \mod p^2 \tag{5}$$

This conjecture is related to generalized Carmichael numbers (see [HH]). The prime numbers satisfying (5) seem to have a similar distribution as irregular primes, which makes them equally hard to find. In fact, at the moment, the only known prime numbers which satisfy (5) are 1093 and 3511.

Acknowledgment. We wish to thank Stephanie Halbeisen for writing all the C-programs, which built the touchstones for our conjectures.

References

[Ga] J. M. Gandhi: On logarithmic numbers. *The Mathematics Student* **31** (1963), 73–83.

[HS] L. Halbeisen and S. Shelah: Consequences of arithmetic for set theory. *Journal of Symbolic Logic* **59** (1994), 30–40.

[HH] L. Halbeisen and N. Hungerbühler: On generalized Carmichael numbers. *Hardy-Ramanujan Journal* **22** (1999), 8–22.

[Ob] W. Oberschelp: Solving linear recurrences from differential equations in the exponential manner and vice versa, *in* "Applications of Fibonacci numbers, Vol. 6," (G. E. Bergum, A. N. Philippou and A. F. Horadam, Ed.), 365–380, Kluwer Acad. Publ., (Dordrecht), 1996.

[Ri] J. Riordan: "An Introduction to Combinatorial Analysis." Princeton University Press, Princeton, New Jersey (1980).

[Si] D. Singh: The numbers $L(m, n)$ and their relations with prepared Bernoulli and Eulerian numbers. *The Mathematics Student* **20** (1952), 66–70.

[Sl] N. J. A. Sloane: "A Handbook of Integer Sequences." Academic Press, New York (1973).

[SP] N. J. A. Sloane and S. Plouffe: "The Encyclopedia of Integer Sequences." Academic Press, San Diego (1995).

Lorenz Halbeisen
Dept. of Mathematics
U.C. Berkeley
Evans Hall 938
Berkeley, CA 94720
USA
halbeis@math.berkeley.edu

Norbert Hungerbühler
Dept. of Mathematics
U.A. Birmingham
452 Campbell Hall
Birmingham, AL 35294-1170
USA
buhler@math.uab.edu