Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2023, Volume 29, Number 4, 724–736
DOI: 10.7546/nntdm.29.4.724-736

Binary expansions of prime reciprocals

Brenda Navarro-Flores[1], José M. González-Barrios[2] and Raúl Rueda[3]

[1] Department of Probability and Statistics, IIMAS,
Universidad Nacional Autónoma de México, Mexico City, Mexico
e-mail: brendanavarro@comunidad.unam.mx

[2] Department of Probability and Statistics, IIMAS,
Universidad Nacional Autónoma de México, Mexico City, Mexico
e-mail: gonzaba@sigma.iimas.unam.mx

[3] Department of Probability and Statistics, IIMAS,
Universidad Nacional Autónoma de México, Mexico City, Mexico
e-mail: pinky@sigma.iimas.unam.mx

Received: 10 November 2022 **Revised:** 27 July 2023
Accepted: 13 November 2023 **Online First:** 21 November 2023

Abstract: Prime numbers have been always of great interest. In this work, we explore the prime numbers from a sieve other than the Eratosthenes sieve. Given a prime number p, we consider the binary expansion of $\frac{1}{p}$ and, in particular, the size of the period of $\frac{1}{p}$. We show some results that relate the size of the period to properties of the prime numbers.
Keywords: Prime numbers, Order induced by binary expansions, New sieve.
2020 Mathematics Subject Classification: 11A41, 11B83.

1 Introduction

Prime numbers have been studied since the beginning of mathematics. Euclid in his work *Elements* circa 300 BC, showed that there are an infinite number of them. Many great mathematicians have worked with them, such as Euclid, Bertran, Legendre, Riemann (see [9]), Fermat, Leibnitz, Wiles (see [7]), Wilson, Lagrange (see [19]), Oppermann [18], Rosser (see [22]), among others. And also, there are many conjectures about these numbers, such as the conjecture that *there are an infinite number of Mersenne primes*, a *Mersenne Prime* is a prime number of the form $M_n = 2^n - 1$ for some integer n. They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17-th century. There are many more open conjectures, such as Andrica's conjecture [1], Goldbach's conjecture, Brocard's conjecture (see [19]), Artin's conjecture (see [2] and [13]), among others. See also [11, 12, 14, 21].

In this work, we explore some properties of prime numbers using binary expansions of the reciprocals of primes.

2 Binary expansions

We start with a Lemma which may be known, but we have not found its proof. We made its proof with elementary tools such as geometric series and the following definitions, we did not include the proof but you can ask any of the authors for it if needed.

Let for every $n \in \mathbb{N}$ the set of positive integers, we define

$$D_n = \{r \in \mathbb{N} \mid r|n \text{ and } r \neq 1, n\}.$$

We observe that D_n is the empty set if $n = 1$ or n is a prime number. For every $n, m \in \mathbb{N}$ such that $1 \leq m < n$ and n is not a prime number, we used in the proof of Lemma 2.1

$$\gamma_m = \sum_{i=0}^{\lfloor \frac{n}{m} \rfloor - 1} 2^{im} \quad \text{and} \quad \Gamma_n = \{l \in \mathbb{N} \mid \gamma_m \not| \, l \text{ for every } m \in D_n\}.$$

Lemma 2.1. *Let q be a rational number in the unit closed interval $I = [0, 1]$. Then it is well known that the binary expansion of q is given by*

$$q = 0.a_1a_2\ldots a_m\overline{b_1b_2\ldots b_n} \tag{2.1}$$

where $a_1, \ldots, a_m, b_1, \ldots, b_n \in \{0, 1\}$, $m \in \mathbb{N} \cup \{0\}$ and $n \in \mathbb{N}$. The overlined terms is the periodic part of the number q, which includes zeros and ones if $n > 1$, and n is the size of the shortest period. Then

- *i)* $m = 0$ *and* $n = 1$ *if and only if* $q = 0$ *or* $q = 1$.
- *ii)* $m = 0$ *and* $n > 1$ *if and only if* $q = \frac{l}{2^n - 1}$ *for some integer* $1 \leq l \leq 2^n - 2$ *such that* $l \in \Gamma_n$.
- *iii)* $m \geq 1$ *and* $n = 1$ *if and only if* $q = \frac{l}{2^m}$ *for some odd integer* $1 \leq l \leq 2^m - 1$.
- *iv) If* $m \geq 1$ *and* $n > 1$, *then* $q = \frac{l}{2^m(2^n - 1)}$ *for some integer* $1 \leq l \leq 2^m(2^n - 1) - 1$.

Note that the converse of Lemma 2.1 part *iv)* is not true. For example, for $n = 2$ and $m = 1$, $1 \leq l \leq 2^m(2^n - 1) - 1 = 5$ and $2^m(2^n - 1) = 6$. With $\frac{1}{2} = \frac{3}{6} = 0.1\overline{0} = 0.0\overline{1}$, so for $l = 3$, $\frac{l}{2^m(2^n-1)}$ does not have binary expansion with $m = 1$ and $n = 2$. Remember that n must be the shortest possible period.

Remark 2.1. *Note that in part $ii)$ of Lemma 2.1 we have that for every $l \in \{1, 2, ..., 2^n-3, 2^n-2\}$ the following equation holds*

$$\frac{l}{2^n - 1} = 0.\overline{b_1 \dots b_n}$$

for some $b_1, \dots, b_n \in \{0, 1\}$. However, n ***may not be the shortest period of*** $\frac{l}{2^n-1}$.

Now we state a very well known result, whose proof follows directly from Fermat's little Theorem. We can find the proof of this theorem in [23].

Lemma 2.2. *Let p be a prime number greater than 2. Then $p|(2^{p-1} - 1)$.*

It is well known that, the converse of Lemma 2.2 does not hold. For example if $q = 341$, q is not prime: $341 = 11 \cdot 31$, this was proved first by Sarrus in 1819. In the literature these counterexamples are called "pseudoprime numbers" (to base 2), that is, an integer q such that q divides $2^{q-1}-1$, but q is not actually a prime, the least pseudoprime is $q = 341$ and $q|\,(2^{q-1} - 1)$, see for example [20].

Some of the Lemmas in this paper are used also in the theory of pseudoprime numbers.

Corollary 2.1. *Let p be a prime number greater than 2. Then $0 < \frac{1}{p} \leq \frac{1}{3}$ and*

$$\frac{1}{p} = \frac{r}{2^{p-1} - 1} \tag{2.2}$$

for some integer $1 \leq r \leq 2^{p-1} - 3$. Besides, $\frac{1}{p}$ has a binary expansion which satisfies

$$\frac{1}{p} = 0.\overline{b_1 b_2 \dots b_{p-1}}, \tag{2.3}$$

with $b_1 = 0$ and $b_{p-1} = 1$. Note also that the period in Equation (2.3) *may not be the shortest one.*

Proof. If p is a prime number greater than 2, it is obvious that $0 < \frac{1}{p} \leq \frac{1}{3}$, and by Lemma 2.2 p divides $2^{p-1} - 1$, so there exists an integer r such that $p \cdot r = 2^{p-1} - 1$. Therefore, Equation (2.2) follows, and by Remark 2.1 we have that $\frac{1}{p}$ has the binary expansion given by Equation (2.3). Since $\frac{1}{p} \leq \frac{1}{3}$, then $b_1 = 0$, and since p is an odd integer, then $b_{p-1} = 1$. The last note can be observed, for example when $p = 7$, in the next paragraph. □

For example, if $p = 3$, then $2^{p-1} - 1 = 3$ and in this case $\frac{1}{3} = 0.\overline{01}$. If $p = 5$, then $2^{p-1} - 1 = 15 = 3 \cdot 5$ and in this case $\frac{1}{5} = 0.\overline{0011}$. If $p = 7$, then $2^{p-1} - 1 = 63 = 3 \cdot 3 \cdot 7$ and in this case $\frac{1}{7} = 0.\overline{001001}$, here we observe that $2^3 - 1 = 7$, that is why $\frac{1}{7}$ has a shorter period of only three numbers, that is, $\frac{1}{7} = 0.\overline{001}$. This last example motivates the definition given below. If $p = 11$, then $2^{p-1} - 1 = 1023 = 3 \cdot 11 \cdot 31$ and in this case $\frac{1}{11} = 0.\overline{0001011101}$. Note that $p = 3 = 2^2 - 1$, $p = 7 = 2^3 - 1$, $p = 31 = 2^5 - 1$ and $p = 127 = 2^7 - 1$ are Mersenne's primes, but $p = 2047 = 2^{11} - 1 = 23 \cdot 89$ is not a prime, but a composite number.

A natural order to generate prime numbers p is to consider the size of the shortest period of the binary expansion of $\frac{1}{p}$.

Definition 2.1. *Let $n \in \mathbb{N}$ and let p be a prime number such that $p|(2^n - 1)$. We will say that p is a* **primitive prime divisor** *of $2^n - 1$ if and only if $p \not| (2^q - 1)$ for every $2 \leq q < n$. If $n = p - 1$, we will say that p is a* **long prime***, and if $n < p - 1$, we will say that p is a* **short prime**. See [26].

From the example above $p = 3$, $p = 5$ and $p = 11$ are long primes, but $p = 7$ and $p = 31$ are short primes, since 7 divides $2^3 - 1$ and 31 divides $2^5 - 1$. Of course, 31 also divides $2^{30} - 1 = 1073741823 = 3 \cdot 3 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$. We will use later on the above definition to generate prime numbers using numbers of the form powers of two minus one. Let us mention another useful result. Its proof is well-known and elementary.

Lemma 2.3. *Let $p, q \in \mathbb{N}$ such that $q|p$. Then $(2^q - 1)|(2^p - 1)$.*

Since $3|6$, then $7 = 2^3 - 1|2^6 - 1 = 63 = 3 \cdot 3 \cdot 7$, so 7 is a short prime, and since $2|6$, then $3 = 2^2 - 1|2^6 - 1 = 63 = 3 \cdot 3 \cdot 7$, so 3 is a long prime. We will see that the case $2^6 - 1$ is an interesting exceptional case, when we consider all the numbers of the form $2^n - 1$, for any integer $n \geq 2$.

In Table 3 to Table 5, we found the value of $2^n - 1$ for $2 \leq n \leq 100$ we give the prime decomposition of $2^n - 1$ **underlining** the new primes, which we have not found previously, and for $76 \leq n \leq 100$ we only provide the decompositions. The underlined primes will be of great importance in the interpretation of these tables, and they will also help in finding the prime decomposition of the numbers $2^n - 1$ when n is not a prime number. We will also observe how to find the short primes when we evaluate the prime decompositions of the numbers $2^n - 1$ when n varies from 2 up to N for $N \leq 100$.

First, we note that from Lemma 2.2, if n is a prime greater than 2, then $n|(2^{n-1} - 1)$. So, if we find the prime decomposition of $2^m - 1$ for every $m \in \mathbb{N}$, then for every prime p greater than 2 we will find an $m \in \mathbb{N}$, such that $p|2^m - 1$, of course this holds for $m = p - 1$.

Let us assume that we are trying to find the prime decomposition of $2^n - 1$ when n is not a prime number. If n is not too large, it is possible to find its prime decomposition using for example the package Mathematica, which by the way has an amazing range to perform this task. Let us assume that $q_1 \leq q_2 \leq \cdots \leq q_{k-1} \leq q_k$ are the prime numbers such that

$$n = q_1 \cdot q_2 \cdots q_{k-1} \cdot q_k, \quad \text{where} \quad k \in \mathbb{N}, \tag{2.4}$$

where (2.4) is of course the prime decomposition of n. Let

$$1 < r_1 < r_2 < r_3 < \cdots < r_{m-1} < r_m$$

be all the different divisors of n obtained by multiplying one or more primes given in Equation (2.4), of course $r_m = n$. So, for example, if $n = 40$, its prime decomposition is given by $n = 2 \cdot 2 \cdot 2 \cdot 5$, that is, $k = 4$, and the different divisors of n greater than 1 are $2 < 4 < 5 < 8 < 10 < 20 < 40$, so, $m = 7$.

Now, we observe that the **only value of n**, for $2 \leq n \leq 100$, such that the decomposition of $2^n - 1$ does not include a new prime in its prime decomposition, is when $\boldsymbol{n = 6}$, see Table 3 to Table 5. We will see that this holds for every $n > 100$. We also observe that as n increases, the number of new primes also increases. From Table 1 we observe that $2^{11} - 1$ includes for the first time two new primes, that $2^{29}-1$ for the first time includes three new primes, and that $2^{92}-1$ includes four new primes for the first time, etc. The last observations take us to a new conjecture, which we will state in Conjecture 2.1.

We will see that for every $n \in \mathbb{N}$, with $n \neq 6$, there is a prime number p such that $\frac{1}{p}$ has binary expansion of size n. The first to prove this result was the Norwegian mathematician A. S. Bang in 1886 [4, 5]. In 1892 the Austrian professor Zsigmondy proved a more general result [28].

The proof of the following theorem is given in [6]. Its proof uses the **cyclotomic polynomials** of complex variable as a tool.

Theorem 2.1. (Zsigmondy's Theorem) *Let $a > b \geq 1$ be coprime integers and let $n \geq 2$ be an integer. Then there exists a primitive prime divisor of $a^n - b^n$, except when:*

$i)$ $n = 2$ and $a + b$ is a power of 2; or

$ii)$ $a = 2$, $b = 1$ and $n = 6$.

Remark 2.2. *Observe that if p is a primitive prime divisor for $2^n - 1$ with $n \in \mathbb{N} \setminus \{6\}$, then $p|(2^n - 1)$ and $p = \frac{l}{2^n-1}$ for some $1 \leq l \leq 2^n - 2$. By Remark 2.1,*

$$\frac{1}{p} = 0.\overline{b_1 \dots b_n} \quad \textit{for some} \quad b_1, \dots, b_n \in \{0, 1\} \tag{2.5}$$

If n is not the size of the period of $\frac{1}{p}$, then let $k < n$ the size of the period of $\frac{1}{p}$. From Lemma 2.1, part $ii)$, $\frac{1}{p} = \frac{s}{2^k-1}$ for some $1 \leq s \leq 2^k - 2$ with $s \in \Gamma_k$. So, $ps = 2^k - 1$ and $p|(2^k - 1)$ with $k < n$. This contradicts Equation (2.5). Since, n is the size of the period of $\frac{1}{p}$.

Zsigmondy's theorem gives us the following theorem:

Theorem 2.2. *For every integer $n \geq 2$ with $n \neq 6$ the prime decomposition of the number $2^n - 1$ includes at least a new prime q_n such that q_n does not divide $2^m - 1$ for every $2 \leq m < n$.*

Part $ii)$ of the Theorem 2.1 proves that $n = 6$ is the only exception to the existence of primitive prime divisors for $2^n - 1$.

It is noticeable that the last Theorem is related to the fact that between any natural number n and $2 \cdot n$ there exists a prime number p, but actually it is quite stronger, because it states that for every $n \geq 2$ with $n \neq 5$, if we consider the list of all prime numbers that have appeared in the prime decompositions of $2^k - 1$ for every $2 \leq k \leq n$, then we can find at least one new prime number in the prime decomposition of $2^{n+1} - 1 = 2 \cdot (2^n - 1) + 1$. Of course, in this case the new prime number found does not need to be between $2^n - 1$ and $2^{n+1} - 1$.

Let us assume that we want to find the prime decomposition of $2^{40} - 1$. As we observed above the divisors less than $p = 40$ are: $q \in \{2, 4, 5, 8, 10, 20\}$. Then using Lemma 2.3 we have that $2^2 - 1|2^{40} - 1$, $2^4 - 1|2^{40} - 1$, $2^5 - 1|2^{40} - 1$, $2^8 - 1|2^{40} - 1$, $2^{10} - 1|2^{40} - 1$ and $2^{20} - 1|2^{40} - 1$. Observing Table 3 to Table 5 we have that $3, 5, 31, 17, 11, 41$ all divide $2^{40} - 1$. Then $2^{40} - 1 = 1099511627775$, so $\frac{2^{40}-1}{3 \cdot 5 \cdot 11 \cdot 17 \cdot 31 \cdot 41} = 308405$. So, it is clear that the last number is divisible by 5 again and $\frac{308405}{5} = 61681$ and in a table of primes we find that $r = 61681$ is a prime number, which has not appeared in the new sieve of primes up to $n = 39$, see Table 3.

Even if it is not reported here, we have obtained the equivalence of Table 3 to Table 5 for $n = 1206$. In Table 6, we report for $n = 50, 100, 150, 200, 250, \ldots$ and $n = 1000$, the number of different primes obtained from $2^m - 1$ when $2 \leq m \leq n$. These values are somehow related to the well known function $\pi(n)$ which counts the number of primes less than or equal n, which by the way has no close formula and it has been suggested that it may not exist, due to the capricious distribution of the primes. However, a nice approximation of this function is given by $\pi(n) \sim \frac{n}{\ln(n)}$ for large values of n. The first result for $\pi(n)$ was given by Carl Friedrich Gauss, in 1793, see [7] and [10].

In Table 1 for $1 \leq m \leq 10$ we have the first n such that $2^n - 1$ has m new primes in its decomposition of primes numbers. Also, we have how many of the $1 \leq k \leq n$, $2^k - 1$ includes one new prime, two new primes, and so on up to m new primes.

We also observe in Table 1 that $2^{113} - 1$ includes five new primes, $2^{223} - 1$ includes six new primes, $2^{295} - 1$ includes seven new primes, $2^{333} - 1$ includes eight new primes, $2^{397} - 1$ includes nine new primes and 2^{1076} includes ten new primes. Hence, we may conjecture that for any $m \in \mathbb{N}$ there exists a value of n such that $2^n - 1$ includes m new primes for the first time.

We obtained Table 1 with the help of Wolfram Mathematica and [17]. Figure 1 includes the values of n such that for the first time appear m new primes in the binary expansion of $\frac{1}{2^n-1}$ and it is standardized to be a probability density function, see [3].

n \ m	1	2	3	4	5	6	7	8	9	10
$2^2 - 1$	1	0	0	0	0	0	0	0	0	0
$2^{11} - 1$	8	1	0	0	0	0	0	0	0	0
$2^{29} - 1$	22	4	1	0	0	0	0	0	0	0
$2^{92} - 1$	44	31	14	1	0	0	0	0	0	0
$2^{113} - 1$	47	42	20	1	1	0	0	0	0	0
$2^{223} - 1$	65	80	52	17	6	1	0	0	0	0
$2^{295} - 1$	69	105	72	32	11	3	1	0	0	0
$2^{333} - 1$	71	114	85	41	13	5	1	1	0	0
$2^{397} - 1$	77	126	105	55	21	7	1	2	1	0
$2^{1076} - 1$	107	240	260	208	134	79	23	19	4	1

Table 1. First n such that $2^n - 1$ has m primitive prime divisors

Samuel Yates defined an **unique-prime** to be a prime p such that the decimal expansion of $\frac{1}{p}$ has a period that it shares with no other prime, see [27]. In general for decimal expansions Chris Caldwell and Harvey Dubner defined **bi-unique-primes** to be pairs of primes which have a period shared by no other primes. In a similar way, they defined **tri-unique-primes** and so on, see [8]. The analogous concept for *binary expansions* can be found in Table 1.

In Table 1 the first column for $m = 1$ we have the total of unique primes for the binary expansion of $\frac{1}{p}$ from $2^n - 1$ varying n in the set $\{2, 11, 29, 92, 113, 223, 295, 333, 397, 1076\}$, which corresponds to first time that we obtain $m = 1, m = 2, \ldots, m = 10$ new primes for $2^n - 1$.

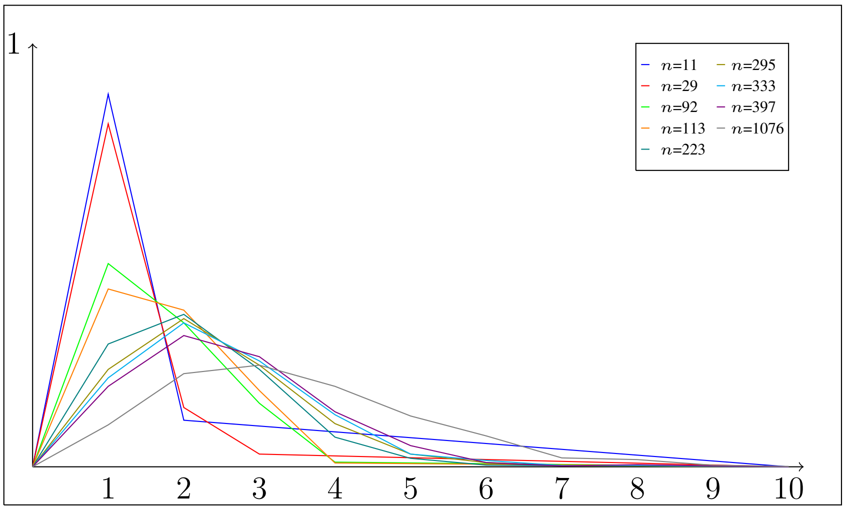

Figure 1. First n such that $2^n - 1$ has m primitive prime divisors

Of course, the second column for $m = 2$ includes the total number of bi-unique primes, for $m = 3$ the column includes the total number of tri-unique primes, etc.

Figure 1 is a graphic representation of the results of the rows in Table 1 standardized by the sum of the rows. Now we state our conjecture based on the results of Table 1.

Conjecture 2.1. *For every $m \in \mathbb{N}$, there exists an $n \in \mathbb{N}$ such that the number of primitive prime divisors of $2^n - 1$ is m.*

3 The last digit of the new prime numbers obtained using the binary sieve

Let p be a prime number and consider the field $\mathbb{Z}_p^* = \{[1]_p, \ldots, [p-1]_p\}$. Then $(\mathbb{Z}_p^*, \cdot)$ is the group of units of $\mathbb{Z}_p$ and it has $p - 1$ elements. For every $[s]_p \in \mathbb{Z}_p^*$, if $m = \text{order}([s]_p)$, then m is the smallest natural number such that $[s]_p^m = [1]_p$ and m divides $|\mathbb{Z}_p^*| = p - 1$. See Lagrange's Theorem 2.81 and Proposition 2.72 in [23]. Also, $[s]_p^n = [1]_p$ if and only if $m|n$, see Lemma 2.53 in [23].

Note that if we want to see what is the last digit of an integer z, it is enough to see what is the remainder of dividing z by 10. That is, using Euclid's algorithm, we find $w \in \mathbb{Z}$ such that $z = 10w + r$ with $0 \leq r < 10$. This gives us that $z - r = 10w$ and $10|(z - r)$. So $z \equiv r \pmod{10}$ and r is the last digit in the decimal expansion of z.

Theorem 3.1. *If n is a multiple of 5, the last digit of the primitive prime divisors of $2^n - 1$ is always 1 in their decimal expansion.*

Proof. Let $n \in \mathbb{N}$ such that $n = 5k$ for some $k \in \mathbb{N}$. Let p be a primitive prime divisor of $2^n - 1$, so $p \neq 2$ and $p - 1$ is even. Thus $2|p - 1$.

Also, $2^n \equiv 1 \pmod{p}$ and $n = \text{order}([2]_p)$. By Lemma 2.2, $p|(2^{p-1} - 1)$, that is, $2^{p-1} \equiv 1 \pmod{p}$. So, we have that $n|(p-1)$. Then, $2|(p-1)$ and $5k = n|(p-1)$. By the Fundamental Theorem of Arithmetic $10 = 5 \cdot 2|(p-1)$, that is, $p \equiv 1 \pmod{10}$. The last digit of p is 1. □

In Figure 2 the graph shows the distribution of the last digit in the decimal expansions with the new order that we are considering taking up to $2^{1206}-1$. Of course, the number 5 is the only prime whose last decimal digit is 5. Using [17] and R-studio, we obtain that there are 1609 primes whose last decimal digit is 1, there are 879 primes whose last decimal digit is 3, there are 902 primes whose last decimal digit is 7 and finally, there are 884 primes whose last decimal digit is 9.

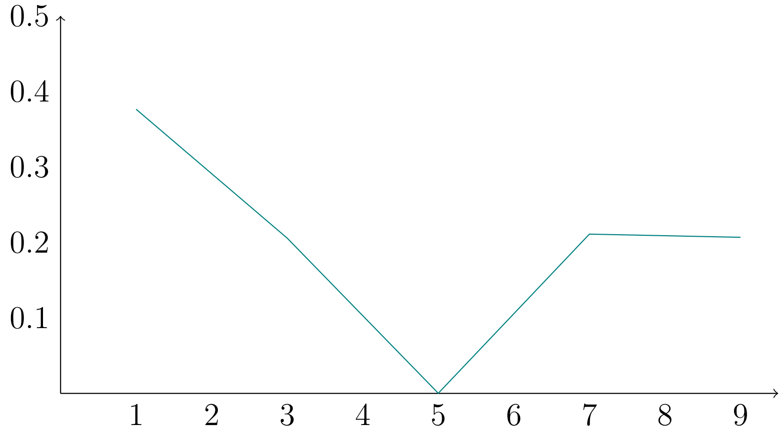

Figure 2. Graph of distribution in the last digit.

Open Question 3.1. *Why, in Figure 2 giving the last digit in the decimal expansions of primes in the new sieve, the number* 1 *appears almost twice more often than the digits* 3*,* 7 *and* 9 *?*

4 Antisymmetric numbers

Let r, m be positive integers, then r is called an **antisymmetric number of size** m if and only if $1/r$ has a binary expansion with period of size $2m$, and the expansion is given by

$$\frac{1}{r}=0.\overline{a_1a_2\dots a_m\hat{a}_1\hat{a}_2\dots\hat{a}_m}$$

for some $a_1,a_2,\dots,a_m\in\{0,1\}$ and $\hat{a}_i=1-a_i$ for every $i\in\{1,2,\dots,m\}$.

Observe that if r is an antisymmetric number of size m, then the binary expansion of $1/r$ has a periodic part of even size, that is, $2m$.

The first idea of our antisymmetric numbers appeared first in [15], in a more restricted case. In the case of decimal expansions there is a similar result in the case of fractions with prime denominators first proved by E. Midy and generalized by A. Tripathi, see [16] and [25].
For every $m\geq 1$, let

$$S_m=\sum_{k=0}^{\infty}\frac{1}{(2^{2m})^k}=\frac{2^{2m}}{2^{2m}-1}. \tag{4.1}$$

Let k be a positive integer such that for some integer $m\geq 1$,

$$\frac{1}{k}=0.\overline{11\dots100\dots0} \tag{4.2}$$

where the last one is in the m-th position and it is followed by m consecutive zeros. Then k is an antisymmetric number of size m, in fact **the largest possible**, and

$$\frac{1}{k} = \frac{2^{2m-1} + 2^{2m-2} + \cdots + 2^{2m-m}}{2^{2m}} \sum_{k=0}^{\infty} \frac{1}{(2^{2m})^k} = \frac{2^m}{2^m+1}. \tag{4.3}$$

On the other hand, if k is the counterpart of Equation (4.2), that is, an antisymmetric number of size m, such that

$$\frac{1}{k} = 0.\overline{00\ldots011\ldots1} \tag{4.4}$$

then $1/k$ is **the smallest possible** number with k antisymmetric of size m and

$$\frac{1}{k} = \frac{2^{m-1} + 2^{m-2} + \cdots + 2^1 + 2^0}{2^{2m}} \sum_{k=0}^{\infty} \frac{1}{(2^{2m})^k} = \frac{1}{2^m+1}. \tag{4.5}$$

Lemma 4.1. *Let $k \geq 2$ be an integer. If k is antisymmetric of size m for some integer $m \geq 1$, then $\frac{1}{k} = \frac{l}{2^m+1}$ where l is an integer satisfying $1 \leq l \leq 2^m$. Furthermore, for every $l \in \{1, 2, \ldots, 2^m\}$, $\frac{l}{2^m+1}$ is antisymmetric of size less than or equal to m.*

Proof. Let $k \geq 2$ be an antisymmetric integer of size $m \in \mathbb{N}$, that is,

$$\frac{1}{k} = 0.\overline{a_1 \ldots a_m \hat{a}_1 \ldots \hat{a}_m}$$

where $\hat{a}_i = 1 - a_i$ for every $i \in \{1, 2, \ldots, m\} = M$. We define $J \subseteq M$ such that $a_i = 1$ for every $i \in J$ and $a_i = 0$ for every $i \in M \setminus J$. If $J = \varnothing$, then $M \setminus J = M$, which is the case given in Equation (4.4), and by Equation (4.5), $\frac{1}{k} = \frac{1}{2^m+1}$. If $J = M$, then $M \setminus J = \varnothing$, which is the case given in Equation (4.2), and by Equation (4.3), $\frac{1}{k} = \frac{2^m}{2^m+1}$.

So, assume that $\varnothing \subsetneq J \subsetneq M$ and let $J = \{u_1, \ldots, u_s\}$ with $1 \leq u_1 < \cdots < u_s \leq m$ where $1 \leq s < m$. And let $M \setminus J = \{v_1, \ldots, v_r\}$ where $1 \leq v_1 < \cdots < v_r \leq m$ and $1 \leq r < m$. Clearly $J \cap (M \setminus J) = \varnothing$, so $s + r = m$. Then

$$\begin{aligned}
\frac{1}{k} &= 0.\overline{a_1 \ldots a_m \hat{a}_1 \ldots \hat{a}_m} \\
&= \sum_{i=0}^{\infty} \frac{1}{2^{2mi+u_1}} + \cdots + \sum_{i=0}^{\infty} \frac{1}{2^{2mi+u_s}} + \sum_{i=0}^{\infty} \frac{1}{2^{2mi+m+v_1}} + \cdots + \sum_{i=0}^{\infty} \frac{1}{2^{2mi+m+v_r}} \\
&= \frac{1}{2^m+1} \left[\sum_{j=1}^{s} 2^{m-u_j} + 1 \right].
\end{aligned}$$

If $l = \sum_{i=1}^{s} 2^{m-u_i} + 1$, then $1 \leq l \leq 2^m$.

For the converse, we have these observations:

i) For each $l \in \{1, \ldots, 2^m - 1\}$, $l = \sum_{k \in \Omega} 2^k$ where $\Omega \subseteq \{0, \ldots, m-1\}$ and $\Omega \neq \varnothing$.

ii) For each $l \in \{1, \ldots, 2^m - 1\}$, $\frac{l+1}{2^m+1}$ has an antisymmetric binary expansion. In fact, let $l \in \{1, \ldots, 2^m - 1\}$, then $l = \sum_{k \in J} 2^k$ with $J \subseteq \{0, \ldots, m-1\} = N$. Then $J = \{i_1, \ldots, i_r\}$ with $0 \leq i_1 < \cdots < i_r \leq m - 1$ for some $1 \leq r \leq m$. Observe that $S = m - J := \{m - i_r, \ldots, m - i_1\} \subseteq \{1, \ldots, m\} = M$.

Let $a_i = 1$ for every $i \in S$, $a_i = 0$ for every $i \in M \setminus S$ and $\hat{a}_i = 1 - a_i$ for every $i \in M$. We note that $2^m - \sum_{j \in N \setminus J} 2^j = l + 1$ because $2^m - 1 = \sum_{k=0}^{m-1} 2^k$, so $2^m = \sum_{k=0}^{m-1} 2^k + 1$ and $2^m - \sum_{j \in N \setminus J} 2^j = \sum_{k=0}^{m-1} 2^k - \sum_{j \in N \setminus J} 2^j + 1 = \sum_{j \in J} 2^j + 1 = l + 1$. Then, using Equation (4.1)

$$
\begin{aligned}
0.\overline{a_1 \dots a_m \hat{a}_1 \dots \hat{a}_m} &= \frac{\sum_{k=0}^{2m-1} 2^k - \sum_{j \in J} 2^j - \sum_{j \in N \setminus J} 2^{m+j}}{2^{2m}} S_m \\
&= \frac{2^m \left(2^m - \sum_{j \in N \setminus J} 2^j \right) - (l+1)}{2^{2m} - 1} \\
&= \frac{(l+1)\,(2^m - 1)}{(2^m+1)(2^m-1)} = \frac{l+1}{2^m+1}.
\end{aligned}
$$

Note that if $2m$ is not the shortest period of $\frac{l+1}{2^m+1}$, then in any way it has an antisymmetric binary expansion.

iii) $\frac{1}{2^m+1}$ has an antisymmetric binary expansion of size m. See Equations (4.4) and (4.5).

Let $m = 3$, $\frac{1}{k} = 0.\overline{a_1 a_2 a_3 \hat{a}_1 \hat{a}_2 \hat{a}_3} = 0.\overline{101010} = \frac{6}{2^3+1}$. But k is an antisymmetric number with size $m = 1$, since $\frac{1}{k} = 0.\overline{10} = \frac{2}{2^1+1}$. □

The following remark gives us a similar version of Midy's Theorem but with binary expansions, see [16].

Remark 4.1. *Let p be a prime number with period of size $2m$, that is, $\frac{1}{p} = 0.\overline{b_1 \dots b_{2m}}$ with $m \geq 1$. Then p is an antisymmetric number of size m.*

Proof. Let p be a prime number such that $\frac{1}{p}$ has a binary expansion with period of size $2m$. Then $2m$ is the smallest number such that $p | (2^{2m} - 1)$.

We have that $p | (2^{2m} - 1) = (2^m - 1)(2^m + 1)$. Using properties of prime numbers we have that $p | 2^m + 1$ or $p | 2^m - 1$. The case $p | 2^m - 1$ is impossible. Then $p | 2^m + 1$ and using Lemma 4.1 we have that p is an antisymmetric number of size m. □

Now let m be a positive integer and let $q_m := 2^m + 1$. Then q_m is an odd integer for every $m \geq 1$. Let $\{r_1, r_2, \dots, r_{k(m)}\}$ be the prime decomposition of q_m, then $q_m = r_1 \cdot r_2 \cdots r_{k(m)}$ where we assume that $2 \leq r_1 \leq r_2 \leq \cdots \leq r_{k(m)}$, and $k(m)$ is a positive integer depending on m. In Table 2 we give the prime decomposition of $q_m = 2^m + 1$ for values of m between 1 and 10. In addition, we give the binary expansion of the new primes of q_m

In Table 7 we included all binary expansions of the reciprocal primes $\frac{1}{p}$ up to $p = 521$. The last column indicates if the primes are short (S) or long (L), see Definition 2.5.

There exist different sieves based on the prime decomposition, for example of numbers of the form $10^n - 1$. This sieve does not include $p = 2$ and $p = 5$, since $10 = 2 \cdot 5$, see [24].

m	**prime decomposition of $q_m = 2^m + 1$**	**expansion of $1/q$ for new q prime**
1	3	$1/3 = 0.\overline{0 \cdot 1}$
2	5	$1/5 = 0.\overline{00 \cdot 11}$
3	$3 \cdot 3$	it does not exist
4	17	$1/17 = 0.\overline{0000 \cdot 1111}$
5	$3 \cdot 11$	$1/11 = 3/33 = 0.\overline{00010 \cdot 11101}$
6	$5 \cdot 13$	$1/13 = 5/65 = 0.\overline{000100 \cdot 111011}$
7	$3 \cdot 43$	$1/43 = 3/129 = 0.\overline{0000010 \cdot 1111101}$
8	257	$1/257 = 0.\overline{00000000 \cdot 11111111}$
9	$3 \cdot 3 \cdot 3 \cdot 19$	$1/19 = 0.\overline{000011010 \cdot 111100101}$
10	$5 \cdot 5 \cdot 41$	$1/41 = 25/1025 = 0.\overline{0000011000 \cdot 1111100111}$

Table 2. Binary expansion of the first ten antisymmetric numbers.

Using the order given by the size of the binary period of the reciprocals of prime numbers we have found new primes whose decimal expression have more of 200 digits, so it may be useful in order to generate security codes in cryptography. Also using the new sieve we can study properties of the prime numbers using probabilistic and statistical methods, see for example Figure 1.

Tables 3, 4, 5, 6 and 7, and some final notes on antisymmetric numbers and Fermat's numbers are available on internet at `https://sites.google.com/ciencias.unam.mx/binary-expansions/inicio`.

Acknowledgements

We would like to thank the two anonymous reviewers and the academic editor for their valuable suggestions and comments, which greatly improved our manuscript.

References

[1] Andrica, D. (1986). Note on a conjecture in prime number theory. *Studia Universitatis Babeș-Bolyai Mathematica*, 31, 44–48.

[2] Artin, E. (1965). *The Collected Papers of Emil Artin.* Addison-Wesley. *Mathematical Reviews*, 31, #1159.

[3] Ash, R. B. (1972). *Real Analysis and Probability.* Academic Press, New York.

[4] Bang, A. S. (1886). Taltheoretiske Undersøgelser. *Tidsskrift for Mathematik. FEMTE RÆKKE*, 4, 70–80.

[5] Bang, A. S. (1886). Taltheoretiske Undersøgelser (continued). *Tidsskrift for Mathematik. FEMTE RÆKKE*, 4, 130–137.

[6] Birkhoff, G. D., & Vandiver, H. S. (1904). On the integral divisors of $a^n - b^n$. *Annals of Mathematics*, 5, 173–180.

[7] Burton, D. M. (2011). *The History of Mathematics: An Introduction* (7th ed.). McGraw-Hill, New York.

[8] Caldwell, C., & Dubner, H. (1998). Unique-period primes. *Journal of Recreational Mathematics*, 29(1), 43–48.

[9] Conway, H. J., & Guy, R. K. (1995). *The Book of Numbers.* Copernicus, Springer-Verlag, New York.

[10] Gauss, C. F. (1863). *Werke, Vol. 2* (1st ed.), Göttingen: Teubner, 444–447.

[11] Hardy, G. H., & Wright, E. M. (2008). *An Introduction to the Theory of Numbers* (6th ed.). Oxford University Press, Oxford.

[12] Hoffman, P. (1998). *The Man Who Loved Only Numbers* (1st ed.). Hyperion Books, New York.

[13] Hooley, C. (1967). On Artin's conjecture. *Journal für die reine und angewandte Mathematik*, 225, 209–220.

[14] Koshy, T. (2002). *Elementary Number Theory with Applications*. Harcourt/Academic Press, San Diego.

[15] Meijer, A. R. (1995). The binary expansion of $\frac{1}{p}$. *The American Mathematical Monthly*, 102(5), 427–430.

[16] Midy, E. (1836). *De Quelques Propriétés des Nombres et des Fractions Decimales Périodiques.* Nantes, France.

[17] OEIS Foundation Inc. (2022). Entry A108974. *The On-Line Encyclopedia of Integer Sequences*. Available online at: `https://oeis.org/A108974`.

[18] Oppermann, L. (1882). Om vor Kundskab om Primtallenes Mængde mellem givne Grændser. *Oversigt over det Kongelige Danske Videnskabernes Selskabs Forhandlinger og dets Medlemmers Arbejder*, 169–179.

[19] Ribenboim, P. (1988). *The Book of Prime Number Records* (1st ed.). Springer-Verlag, New York.

[20] Ribenboim, P. (1996). *The New Book of Prime Number Records.* (1st. ed.). Springer, New York.

[21] Rosen, K. H. (1992). *Elementary Number Theory and its Applications* (6th ed.). Addison-Wesley, Reading, MA.

[22] Rosser, J. B. (1938). The n-th prime is greater than $n \log(n)$. *Proceedings of The London Mathematical Society*, 45, 21–44.

[23] Rotman, J. (2005). *A First Course in Abstract Algebra*. Prentice Hall, New Jersey.

[24] Silvester, J. R. (1999). Decimal déjà vu. *The Mathematical Gazette*, 83(498), 453–463.

[25] Tripathi, A. (2012). A curious property of the decimal expansion of reciprocals of primes. *The Pi Mu Epsilon Journal*, 13(7), 427–430.

[26] Weisstein, E. W. "Primitive Prime Factor." *MathWorld – A Wolfram Web Resource*. Available online at: `https://mathworld.wolfram.com/PrimitivePrimeFactor.html`

[27] Yates, S. (1980). Periods of unique primes. *Mathematics Magazine*, 53(5), 314–314.

[28] Zsigmondy, K. (1892). Zur Theorie der Potenzreste. *Journal Monatshefte für Mathematik*, 3(1), 265–284.