# Two-generator numerical semigroups and Fermat and Mersenne numbers

Shalom Eliahou and Jorge Ramírez Alfonsín

**Abstract**

Given $g \in \mathbb{N}$, what is the number of numerical semigroups $S = \langle a, b \rangle$ in $\mathbb{N}$ of genus $|\mathbb{N} \setminus S| = g$? After settling the case $g = 2^k$ for all $k$, we show that attempting to extend the result to $g = p^k$ for all odd primes $p$ is linked, quite surprisingly, to the factorization of Fermat and Mersenne numbers.

**Keywords:** Semigroups, factorization, Fermat, Mersenne.
**MSC 2010:** 05A15, 11A05, 11A51, 20M14

## 1 Introduction

A *numerical semigroup* is a subset $S$ of $\mathbb{N}$ containing 0, stable under addition, and with finite complement $G(S) = \mathbb{N} \setminus S$. The elements of $G(S)$ are called the *gaps* of $S$, and their number is denoted $g(S)$ and called the *genus* of $S$. The *Frobenius number* of $S$ is its largest gap. See [6] for more details. If $a_1, \dots, a_r$ are positive integers with $\gcd(a_1, \dots, a_r) = 1$, then they generate a numerical semigroup $S = \mathbb{N}a_1 + \cdots + \mathbb{N}a_r$, denoted $S = \langle a_1, \dots, a_r \rangle$. For example, the numerical semigroup $S = \langle 4, 5, 7 \rangle$ has gaps $G(S) = \{1, 2, 3, 6\}$, whence genus $g(S) = 4$ and Frobenius number 6. It is well known that every numerical semigroup admits a unique finite minimal generating set [3].

Given $g \in \mathbb{N}$, what is the number $n_g$ of numerical semigroups $S$ of genus $g$? Maria Bras-Amorós recently determined $n_g$ for all $g \leq 50$ by computer. On this basis, she made three conjectures suggesting that the numbers $n_g$ behave closely like the Fibonacci numbers [1, 2]. For instance, the inequality $n_g \geq n_{g-1} + n_{g-2}$, valid for $g \leq 50$, is conjectured to hold for all $g$.

We propose here the refined problem of counting numerical semigroups $S$ of genus $g$ with a specified number of generators.

**Notation 1.1** *Given $g, r \geq 1$, let $n(g,r)$ denote the number of numerical semigroups $S$ of genus $g$ having a minimal generating set of cardinality $r$.*

Of course $n_g = \sum_{r\geq 1} n(g,r)$. Is there an explicit formula for $n(g,r)$, and might it be true that $n(g,r) \geq n(g-1,r) + n(g-2,r)$?

In this paper, we focus on the case $r = 2$, i.e. on numerical semigroups $S = \langle a, b\rangle$ with $\gcd(a,b) = 1$. The genus of $S$ is equal to $(a-1)(b-1)/2$, by a classical theorem of Sylvester. This allows us to show in Section 2 that $n(g,2)$ depends on the factorizations of both $2g$ and $2g-1$, and to determine $n(g,2)$ when $2g-1$ is prime. In Section 3, we determine $n(g,2)$ for $g = 2^k$ and all $k \geq 1$. We then tackle the case $g = p^k$ for odd primes $p$ in Section 4. On the one hand, we provide explicit formulas for $n(p^k, 2)$ when $k \leq 6$. On the other hand, we show that obtaining similar formulas for all $k \geq 1$ is linked to the factorization of Fermat and Mersenne numbers. We conclude with a few open questions about $n(g,2)$.

# 2 Basic properties of $n(g,2)$

We will show that $n(g,2)$ is linked with the factorizations of $2g$ and $2g-1$. For this, we need the following theorem of Sylvester [7].

**Theorem 2.1** *Let $a, b$ be coprime positive integers, and let $S = \langle a, b\rangle$. Then $\max G(S) = ab - a - b$, and for all $x \in \{0, 1, \ldots, ab-a-b\}$, one has*

$$x \in G(S) \iff ab - a - b - x \in S.$$

*In particular, $g(S) = (a-1)(b-1)/2$.*

## 2.1 Link with factorizations of $2g$ and $2g-1$

We first derive that $n(g,2)$ is the counting function of certain particular factorizations of $2g$. As usual, the cardinality of a set $X$ will be denoted $|X|$.

**Proposition 2.2** *Let $g \geq 1$ be a positive integer. Then we have*

$$n(g,2) \;=\; |\{(u,v) \in \mathbb{N}^2 \mid 1 \leq u \leq v,\; uv = 2g,\; \gcd(u+1, v+1) = 1\}|.$$

**Proof.** Indeed, let $S = \langle a, b \rangle$ with $1 \le a \le b$ and $\gcd(a, b) = 1$, and assume that $g(S) = g$. By Theorem 2.1, we have $g = (a-1)(b-1)/2$, i.e. $2g = (a-1)(b-1)$. The claim follows by setting $u = a-1, v = b-1$. ■

A first consequence is that every $g \ge 1$ is the genus of an appropriate 2-generator numerical semigroup.

**Corollary 2.3** *$n(g, 2) \ge 1$ for all $g \ge 1$.*

**Proof.** This follows from the factorization $2g = uv$ with $u = 1, v = 2g$. Concretely, the numerical semigroup $S = \langle 2, 2g+1 \rangle$ has genus $g$. ■

Our next remark shows that $n(g, 2)$ is also linked with the factors of $2g-1$.

**Lemma 2.4** *Let $g \ge 1$ be a positive integer, and let $2g = uv$ with $u, v$ positive integers. Then $\gcd(u+1, v+1)$ divides $2g-1$.*

**Proof.** Set $\delta = \gcd(u+1, v+1)$. Then $u \equiv v \equiv -1 \bmod \delta$, and therefore $2g = uv \equiv 1 \bmod \delta$. ■

## 2.2 The case where $2g-1$ is prime

We can now determine $n(g, 2)$ when $2g-1$ is prime. As customary, for $n \in \mathbb{N}$ we denote by $d(n)$ the number of divisors of $n$ in $\mathbb{N}$.

**Proposition 2.5** *Let $g \ge 3$, and assume that $2g-1$ is prime. Then*

$$n(g, 2) = d(2g)/2.$$

*In particular, $n(g, 2) = d(g)$ if $g$ is odd.*

**Proof.** Let $2g = uv$ be any factorization of $2g$ in $\mathbb{N}$. We claim that $\gcd(u+1, v+1) = 1$. Indeed, by Lemma 2.4 we know that $\gcd(u+1, v+1)$ divides $2g-1$. Assume for a contradiction that $\gcd(u+1, v+1) \ne 1$. Then $\gcd(u+1, v+1) = 2g-1$, since $2g-1$ is assumed to be prime. It follows that $u, v \ge 2g-2$, implying

$$2g = uv \ge 4(g-1)^2.$$

However, the inequality $2g \geq 4(g-1)^2$, while true at $g=2$, definitely fails for $g \geq 3$ as assumed here. Thus $\gcd(u+1, v+1) = 1$, as claimed. Hence, by Proposition 2.2, we have

$$n(g,2) = \big|\{(u,v) \in \mathbb{N}^2 \mid u \leq v, 2g = uv\}\big|. \tag{1}$$

Clearly $2g$ counts as many divisors $u < \sqrt{2g}$ as divisors $v > \sqrt{2g}$. Moreover $2g$ is not a perfect square. This is clear for $g = 3$ or 4. If $g \geq 5$ and $2g = a^2$ with $a \in \mathbb{N}$, then $a \geq 3$ and $2g-1 = a^2-1 = (a-1)(a+1)$, contradicting the primality of $2g-1$. We conclude from (1) that $n(g,2) = d(2g)/2$. Finally, if $g$ is further assumed to be odd, then clearly $d(2g)/2 = d(g)$. ■

Proposition 2.5 cannot be extended to $g = 2$, even though $2g-1$ is prime. Indeed $n(2,2) = 1$ as easily seen, whereas $d(4)/2$ is not even an integer.

Since $n(g,2)$ is controlled by the factorizations of both $2g$ and $2g-1$, its determination is expected to be hard in general, even if the factors of $g$ are known. Nevertheless, below we determine $n(g,2)$ when $g = 2^k$ for all $k \in \mathbb{N}$, despite the fact that the prime factors of $2^{k+1}-1$ are generally unknown.

# 3 The case $g = 2^k$

Let $g = 2^{p-1}$ with $p$ an odd prime, and assume that $2g-1$ is prime.[1] Proposition 2.5 then applies, and gives

$$n(2^{p-1}, 2) = d(2^p)/2 = (p+1)/2.$$

But we shall now determine $n(2^k, 2)$ for all $k \in \mathbb{N}$, and show that its value only depends on the largest odd factor $s$ of $k+1$.

**Theorem 3.1** *Let $g = 2^k$ with $k \in \mathbb{N}$. Write $k+1 = 2^\mu s$ with $\mu \in \mathbb{N}$ and $s$ odd. Then*

$$n(2^k, 2) \ = \ (s+1)/2.$$

**Proof.** Since $2g = 2^{k+1}$, the only integer factorizations $2g = uv$ with $1 \leq u \leq v$ are given by

$$u = 2^i, \ v = 2^{k+1-i}$$

[1]In fact a *Mersenne prime*, since $2g-1 = 2^p - 1$. See also Section 4.2.

with $0 \leq i \leq (k+1)/2$. In order to determine $n(2^k, 2)$ with Proposition 2.2, we must count those $i$ in this range for which $\gcd(2^i+1, 2^{k+1-i}+1) = 1$. This condition is taken care of by the following claim.

**Claim.** We have $\gcd(2^i+1, 2^{k+1-i}+1) = 1$ if and only if $2^\mu$ divides $i$.

The claim is proved by examining separately the cases where $2^\mu$ divides $i$ or not.

• *Case 1: $2^\mu$ divides $i$.* Assume for a contradiction that there is a prime $p$ dividing $\gcd(2^i+1, 2^{k+1-i}+1)$. Then $p$ is odd, and we have

$$2^i \equiv 2^{k+1-i} \equiv -1 \bmod p. \tag{2}$$

It follows that

$$2^{2i} \equiv 2^{k+1} \equiv 1 \bmod p. \tag{3}$$

Let $m$ denote the multiplicative order of 2 mod $p$. It follows from (3) that $m$ *divides* $\gcd(2i, k+1)$. Now, in the present case, we have

$$\gcd(2i, k+1) = \gcd(i, k+1),$$

since $2^\mu$ divides $i$ and $k+1$, while $2^{\mu+1}$ divides $2i$ without dividing $k+1$. Consequently $m$ *divides* $i$, not only $2i$. Hence $2^i \equiv 1 \bmod p$, in contradiction with (2). Therefore $\gcd(2^i+1, 2^{k+1-i}+1) = 1$, as desired.

• *Case 2: $2^\mu$ does not divide $i$.* We may then write $i = 2^\nu j$ with $j$ odd and $\nu < \mu$. Set $q = 2^{2^\nu}+1$, and note that $q \geq 3$. We claim that $q$ divides $\gcd(2^i+1, 2^{k+1-i}+1)$. Indeed, observe that

$$2^{2^\nu} \equiv -1 \bmod q,$$

by definition of $q$. Since $i = 2^\nu j$ with $j$ odd, we have

$$2^i + 1 = (2^{2^\nu})^j + 1 \equiv (-1)^j + 1 \equiv 0 \bmod q.$$

Similarly, we have $k+1-i = 2^\nu j'$ where $j' = 2^{\mu-\nu}s - j$. Then $j'$ is odd, since $\mu - \nu > 0$ and $j$ is odd. As above, this implies that

$$2^{k+1-i} = (2^{2^\nu})^{j'} + 1 \equiv 0 \bmod q.$$

It follows that $q$ divides $\gcd(2^i+1, 2^{k+1-i}+1)$, thereby settling the claim.

We may now conclude the proof. Indeed, the above claim yields

$$\begin{aligned} n(2^k,2) &= \left|\{i \mid 0 \le i \le (k+1)/2,\ i \equiv 0 \bmod 2^\mu\}\right| \\ &= \left|\{j \mid 0 \le j \le (k+1)/2^{\mu+1}\}\right| \\ &= \left\lfloor (k+1)/2^{\mu+1} + 1 \right\rfloor = (s+1)/2. \end{aligned}$$

■

**Corollary 3.2** *For every $N \ge 1$, there are infinitely many $g \ge 1$ such that $n(g,2) = N$.*

**Proof.** Let $s = 2N - 1$. Then $s$ is odd, and for all $k = 2^\mu s - 1$ with $\mu \in \mathbb{N}$, we have $n(2^k,2) = (s+1)/2 = N$ by Theorem 3.1. ■

In particular, there are infinitely many $g \ge 1$ for which $n(g,2) = 1$. Since $n(h,2) \ge 1$ for all $h \ge 1$, the inequality $n(g,2) \ge n(g-1,2) + n(g-2,2)$ fails to hold infinitely often. This says nothing, of course, about the original conjecture $n_g \ge n_{g-1} + n_{g-2}$ of Bras-Amorós.

# 4 The case $g = p^k$ for odd primes $p$

We have determined $n(2^k,2)$ for all $k \ge 1$. Attempting to similarly determine $n(p^k,2)$ for odd primes $p$ leads to a somewhat paradoxical situation. Indeed, while the case where $k$ is small is relatively straightforward, formidable difficulties arise when $k$ grows. This Jekyll-and-Hyde behavior is shown below.

## 4.1 When $k$ is small

Given positive integers $q_1, \dots, q_t$, we denote by

$$\rho_{q_1,\dots,q_t} : \mathbb{Z} \to \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_t\mathbb{Z}$$

the canonical reduction morphism $\rho_{q_1,\dots,q_t}(n) = (n \bmod q_1, \dots, n \bmod q_t)$, and shall write $n \equiv \neg a \bmod q$ instead of $n \not\equiv a \bmod q$. For example, the condition

$$\rho_{3,5,17}(p) = (2, \neg 3, \neg 8)$$

means that $p \equiv 2 \bmod 3$, $p \not\equiv 3 \bmod 5$ and $p \not\equiv 8 \bmod 17$.

**Proposition 4.1** *Let $p$ be an odd prime number. Then we have:*

1. $n(p,2) = \begin{cases} 1 & \text{if} \quad \rho_3(p) = 2 \\ 2 & \text{if} \quad \rho_3(p) = \neg 2, \end{cases}$

2. $n(p^2,2) = 3,$

3. $n(p^3,2) = \begin{cases} 1 & \text{if} \quad \rho_{3,5}(p) = (2,2) \\ 2 & \text{if} \quad \rho_{3,5}(p) = (2,\neg 2) \\ 3 & \text{if} \quad \rho_{3,5}(p) = (\neg 2, 2) \\ 4 & \text{if} \quad \rho_{3,5}(p) = (\neg 2,\neg 2), \end{cases}$

4. $n(p^4,2) = \begin{cases} 4 & \text{if} \quad \rho_7(p) = 3 \\ 5 & \text{if} \quad \rho_7(p) = \neg 3, \end{cases}$

5. $n(p^5,2) = \begin{cases} 1 & \text{if} \quad \rho_{3,5,17}(p) = (2,3,8) \\ 2 & \text{if} \quad \rho_{3,5,17}(p) = (2,3,\neg 8) \text{ or } (2,\neg 3,8) \\ 3 & \text{if} \quad \rho_{3,5,17}(p) = (2,\neg 3,\neg 8) \\ 4 & \text{if} \quad \rho_{3,5,17}(p) = (\neg 2,3,8) \\ 5 & \text{if} \quad \rho_{3,5,17}(p) = (\neg 2,3,\neg 8) \text{ or } (\neg 2,\neg 3,8) \\ 6 & \text{if} \quad \rho_{3,5,17}(p) = (\neg 2,\neg 3,\neg 8), \end{cases}$

6. $n(p^6,2) = \begin{cases} 6 & \text{if} \quad \rho_{31}(p) = 15 \\ 7 & \text{if} \quad \rho_{31}(p) = \neg 15. \end{cases}$

With the Chinese Remainder Theorem, the above result implies that $n(p^3,2)$ depends on the class of $p$ modulo 15, and that $n(p^4,2)$, $n(p^5,2)$ and $n(p^6,2)$ depend on the class of $p$ modulo 7, 255 and 31, respectively.

**Proof.** Let $k \leq 6$. We determine $n(p^k,2)$ using Proposition 2.2. As $p$ is an odd prime, counting the factorizations $2p^k = uv$ with $u \leq v$ and $\gcd(u+1,v+1) = 1$ amounts to count the number of exponents $i$ in the range $0 \leq i \leq k$ satisfying the condition

$$\gcd(p^i+1, 2p^{k-i}+1) = 1.$$

A convenient way to ease the computation of this gcd is to replace $p$ by a variable $x$ and to reduce, in the polynomial ring $\mathbb{Z}[x]$, the greatest common divisor of $x^i+1$ and $2x^j+1$ to the simpler form

$$\gcd(x^i+1, 2x^j+1) \;=\; \gcd(f,g), \tag{4}$$

where either polynomial $f$ or $g$ is constant. Polynomials are used here precisely for allowing such degree considerations. Since $\gcd(p^i+1, 2p^j+1)$ is odd, we may equivalently work in the rings $\mathbb{Z}[2^{-1}]$ or $\mathbb{Z}[2^{-1}, x]$, where 2 is made invertible. Note that these rings are still unique factorization domains.

We obtain the following table, with a method explained below. For simplicity, we write $(f, g)$ rather than $\gcd(f, g)$, and 1 whenever either $f$ or $g$ is invertible in the ring $\mathbb{Z}[2^{-1}, x]$. The cases $i = 0$ and $j = 0$ are not included, since then $x^i + 1$ and $2x^j + 1$ are already constant, respectively.

| gcd | $2x+1$ | $2x^2+1$ | $2x^3+1$ | $2x^4+1$ | $2x^5+1$ | $2x^6+1$ |
|---|---|---|---|---|---|---|
| $x+1$ | 1 | $(x+1,3)$ | 1 | $(x+1,3)$ | 1 | $(x+1,3)$ |
| $x^2+1$ | $(2x+1,5)$ | 1 | $(2x-1,5)$ | $(x^2+1,3)$ | $(2x+1,5)$ | 1 |
| $x^3+1$ | $(2x+1,7)$ | $(x-2,9)$ | 1 | $(2x-1,9)$ | $(x+2,7)$ | $(x^3+1,3)$ |
| $x^4+1$ | $(2x+1,17)$ | $(2x^2+1,5)$ | $(x-2,17)$ | 1 | $(2x-1,17)$ | $(2x^2-1,5)$ |
| $x^5+1$ | $(2x+1,31)$ | $(x+4,33)$ | $(4x+1,31)$ | $(x-2,33)$ | 1 | $(2x-1,33)$ |
| $x^6+1$ | $(2x+1,65)$ | $(2x^2+1,7)$ | $(2x^3+1,5)$ | $(x^2-2,9)$ | $(x-2,65)$ | 1 |

Table 1: Reduction of $\gcd(x^i+1, 2x^j+1)$ for $1 \le i, j \le 6$.

In order to construct this table, we use the most basic trick for computing gcd's in a unique factorization domain $A$, namely:

$$g_1 \equiv g_2 \bmod f \;\Rightarrow\; \gcd(f, g_1) = \gcd(f, g_2) \tag{5}$$

for all $f, g_1, g_2 \in A$. As an illustration, let us reduce $\gcd(x^2+1, 2x^3+1)$ to the form (4) in the ring $\mathbb{Z}[2^{-1}, x]$. We have

$$\begin{aligned} \gcd(x^2+1, 2x^3+1) &= \gcd(x^2+1, -2x+1) && (6)\\ &= \gcd(2^{-2}+1, -2x+1) && (7)\\ &= \gcd(1+2^2, 2x-1), && (8) \end{aligned}$$

where steps (6) and (7) follow from (5) and the respective congruences

$$\begin{aligned} x^2 &\equiv -1 \bmod (x^2+1),\\ x &\equiv 2^{-1} \bmod (-2x+1). \end{aligned}$$

Hence $\gcd(x^2+1, 2x^3+1) = \gcd(2x-1, 5)$, as displayed in Table 4.1.

Now, from that table, it is straightforward to determine those pairs of exponents $i, j$ with $i + j \leq 6$ and those odd primes $p$ for which

$$\gcd(p^i + 1, 2p^j + 1) = 1,$$

and hence to obtain the stated formulas for $n(p^k, 2)$. Consider, for instance, the case $k = 3$. We shall count those exponents $i \in \{0, 1, 2, 3\}$ for which

$$\gcd(p^i + 1, 2p^{3-i} + 1) = 1. \tag{9}$$

$\underline{i = 0}$: Condition (9) is always satisfied.

$\underline{i = 1}$: Table 4.1 gives $\gcd(p+1, 2p^2+1) = \gcd(p+1, 3)$, which equals 1 exactly when $p \not\equiv 2 \bmod 3$.

$\underline{i = 2}$: Table 4.1 gives $\gcd(p^2 + 1, 2p + 1) = \gcd(2p + 1, 5)$, which equals 1 exactly when $p \not\equiv 2 \bmod 5$.

$\underline{i = 3}$: Finally, we have $\gcd(p^3 + 1, 3) = 1$ exactly when $p \not\equiv 2 \bmod 3$.

It follows that $n(p^3, 2)$ is entirely determined by the classes of $p$ mod 3 and 5, with a value ranging from 1 to 4 depending on whether $\rho_{3,5}(p)$ equals $(2, 2), (2, \neg 2), (\neg 2, 2)$ or $(\neg 2, \neg 2)$, as stated.

The cases $k = 1, 2, 4, 5, 6$ are similar and left to the reader. ■

We leave the determination of $n(p^7, 2)$ as an exercise to the reader. Let us just mention that the value of this function depends on the class of the prime $p$ mod $3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$, and that its range is equal to $\{1, 2, \ldots, 8\}$. The case $k = 8$ is much simpler. We state the result without proof.

**Proposition 4.2** *Let $p$ be an odd prime number. Then we have:*

$$n(p^8, 2) = \begin{cases} 6 & \textit{if} \quad \rho_{7,31,127}(p) = (5, 23, 63) \\ 7 & \textit{if} \quad \rho_{7,31,127}(p) = (\neg 5, 23, 63),\ (5, \neg 23, 63)\ \textit{or}\ (5, 23, \neg 63) \\ 8 & \textit{if} \quad \rho_{7,31,127}(p) = (\neg 5, \neg 23, 63),\ (\neg 5, 23, \neg 63)\ \textit{or}\ (5, \neg 23, \neg 63) \\ 9 & \textit{if} \quad \rho_{7,31,127}(p) = (\neg 5, \neg 23, \neg 63). \quad ■ \end{cases}$$

That was the gentle side of the story. Here comes the harder one.

## 4.2 When $k$ grows

When $k$ grows arbitrarily, the task of determining $n(p^k, 2)$ for all odd primes $p$ using Proposition 2.2 becomes much more complicated, and turns out to be linked to hard problems. Let us focus on one specific factorization of $2p^k$, namely $2p^k = uv$ with

$$u = p^{k-1},\ v = 2p.$$

In order to find when this factorization contributes 1 to $n(p^k, 2)$, we need to decide when $\gcd(p^{k-1} + 1, 2p + 1)$ is equal to 1. Here is the key reduction.

**Lemma 4.3** *Let $p$ be an odd prime and let $m \in \mathbb{N}$. Then*

$$\gcd(p^m + 1, 2p + 1) = \begin{cases} \gcd(2^m + 1, 2p + 1) & \text{if } m \text{ is even,} \\ \gcd(2^m - 1, 2p + 1) & \text{if } m \text{ is odd.} \end{cases}$$

**Proof.** As earlier, we will reduce $\gcd(x^m + 1, 2x + 1)$ in $\mathbb{Z}[2^{-1}, x]$ to the form $\gcd(f, g)$, where either $f$ or $g$ is a constant polynomial. Since $x \equiv -2^{-1} \bmod (2x + 1)$, trick (5) yields

$$\begin{aligned} \gcd(x^m + 1, 2x + 1) &= \gcd((-2)^{-m} + 1, 2x + 1) \\ &= \gcd(2^m + (-1)^m, 2x + 1). \end{aligned}$$

Substituting $x = p$ gives the stated formula. ■

Hence, in order to determine when $\gcd(p^m + 1, 2p + 1)$ equals 1, we need to know the prime factors of $2^m + 1$ for $m$ even, and of $2^m - 1$ for $m$ odd. This is an ancient open problem. It is not even known at present whether there are finitely or infinitely many Fermat or Mersenne primes, i.e. primes of the form $F_t = 2^{2^t} + 1$ or $M_q = 2^q - 1$ with $t \geq 0$ and $q$ prime, respectively.

• Assume for instance that $k = 2^t + 1$ for some $t \geq 1$. Then $k - 1$ is even, and thus Lemma 4.3 yields

$$\gcd(p^{k-1} + 1, 2p + 1) = \gcd(F_t, 2p + 1). \tag{10}$$

Therefore, as long as the prime factors of the Fermat number $F_t$ remain unknown, we cannot determine those primes $p$ for which the gcd in (10) equals 1, and hence write down an exact formula for $n(p^k, 2)$ in the spirit of Proposition 4.1. For the record, as of 2010, the prime factorization of $F_t$ is completely known for $t \leq 11$ only [5].

• Assume now that $k = q + 1$ for some large prime $q$. Then $k - 1 = q$ is odd, and Lemma 4.3 yields

$$\gcd(p^{k-1} + 1, 2p + 1) = \gcd(2^q - 1, 2p + 1). \tag{11}$$

Here again, we do not know the prime factors of $M_q = 2^q - 1$ in general; it may even happen that $2^q - 1$ hits some unknown Mersenne prime. Thus, we will not know for which primes $p$ the gcd in (11) equals 1, i.e. when the specific factorization $2p^k = p^{k-1} \cdot 2p$ contributes 1 to $n(p^k, 2)$. For the record, the largest prime currently known is the Mersenne prime $p = 2^{43,112,609} - 1$, found in August 2008 [4].

The above difficulties concern the specific factorization $2p^k = p^{k-1} \cdot 2p$. However, most other ones will also lead to trouble for some exponents $k$. For instance, consider the factorization $2p^k = p^{k-2} \cdot 2p^2$, and let $k = 2^{t+1} + 2$. Then, a computation as in the proof of Lemma 4.3 yields

$$\gcd(p^{k-2} + 1, 2p^2 + 1) = \gcd(F_t, 2p^2 + 1).$$

Once again, not knowing the prime factors of $F_t = 2^{2^t} + 1$ prevents us to know for which primes $p$ this gcd equals 1.

# 5 Concluding remarks and open questions

We have determined $n(g, 2)$ when $2g-1$ is prime, for $g = 2^k$ for all $k \geq 1$, and for $g = p^k$ for all odd primes $p$ and $k \leq 6$. The general case is probably out of reach. However, here are a few questions which might be more tractable, yet which we cannot answer at present.

1. *Is there an explicit formula for $n(3^k, 2)$ as a function of $k$? Is it true that $n(3^k, 2)$ goes to infinity as $k$ does?*

   Here are the values of this function for $k = 1, 2, \ldots, 20$:

   $$2, 3, 4, 4, 5, 7, 8, 9, 8, 9, 11, 13, 11, 15, 16, 14, 14, 18, 20, 21.$$

2. *Can one characterize those integers $g \geq 1$ for which $n(g, 2) = 1$?*

   In special cases, we know enough to get a complete answer, for instance when $g$ is prime using Proposition 4.1, or when $g = 2^k$ using

Theorem 3.1. However, the general case seems to be very hard. As an appetizer, let us mention that a prime $p$ satisfies $n(p^{21}, 2) = 1$ if and only if $p \equiv 8 \bmod 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$; the smallest such prime is

$$p = 12,884,901,893.$$

3. *Let $r \in \mathbb{N}$, $r \geq 1$. Does $n(p_1 \cdots p_r, 2)$ attain every value $i \in \{1, 2, \ldots, 2^r\}$ for suitable distinct primes $p_1, \ldots, p_r$, and infinitely often so?*

4. *Let $l \in \mathbb{N}$, $l \geq 1$. Does $n(p^{2l-1}, 2)$ attain every value $i \in \{1, 2, \ldots, 2l\}$ for suitable odd primes $p$, and infinitely often so?*

5. *In contrast, is it true that $\min\{n(p^{2l}, 2) \mid p$ odd prime$\}$ goes to infinity with $l$?*

Using the above methods, and a classical theorem of Dirichlet, it is fairly easy to show that, independently of the parity of $k$, the function $n(p^k, 2)$ attains its maximal value $k + 1$ infinitely often.

# References


[1] M. Bras-Amorós, Fibonacci-like behavior of the number of numerical semigroups of a given genus, Semigroup Forum 76 (2008) 379–384.

[2] M. Bras-Amorós, Bounds on the number of numerical semigroups of a given genus, J. Pure and Applied Algebra 213 (2009) 997–1001.

[3] R. Fröberg, C. Gottlieb, R. Häggkvist, On numerical semigroups, Semigroup Forum 35 (1987) 63–83.

[4] GIMPS, Great Internet Mersenne Prime Search, `http://www.mersenne.org/`.

[5] W. Keller, Prime factors $k \cdot 2^n + 1$ of Fermat numbers $F_m$ and complete factoring status, web page available at `http://www.prothsearch.net/fermat.html`.

[6] J.L. Ramírez Alfonsín, The Diophantine Frobenius problem, Oxford Lecture Series in Mathematics and its Applications 30, Oxford University Press, Oxford, (2005).

[7] J.J. Sylvester, On subinvariants, i.e. semi-invariants to binary quantities of an unlimited order, Amer. J. Math. 5 (1882) 119–136.

**Authors addresses:**

• Shalom Eliahou[a,b,c],
[a]Univ Lille Nord de France, F-59000 Lille, France
[b]ULCO, LMPA J. Liouville, B.P. 699, F-62228 Calais, France
[c]CNRS, FR 2956, France
e-mail: eliahou@lmpa.univ-littoral.fr

• Jorge Ramírez Alfonsín,
Institut de Mathématiques et de Modélisation de Montpellier
Université Montpellier 2
Case Courrier 051
Place Eugène Bataillon
34095 Montpellier, France
UMR 5149 CNRS
e-mail: jramirez@math.univ-montp2.fr