



**HAL**  
open science

# On the number of numerical semigroups of prime power genus

Shalom Eliahou, Jorge Ramirez Alfonsin

► **To cite this version:**

Shalom Eliahou, Jorge Ramirez Alfonsin. On the number of numerical semigroups of prime power genus. 2012. hal-00732344

**HAL Id: hal-00732344**

**<https://hal.science/hal-00732344>**

Preprint submitted on 14 Sep 2012

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# On the number of numerical semigroups $\langle a, b \rangle$ of prime power genus

Shalom Eliahou\* and Jorge Ramírez Alfonsín†

September 14, 2012

## Abstract

Given  $g \geq 1$ , the number  $n(g)$  of numerical semigroups  $S \subset \mathbb{N}$  of genus  $|\mathbb{N} \setminus S|$  equal to  $g$  is the subject of challenging conjectures of Bras-Amorós. In this paper, we focus on the counting function  $n(g, 2)$  of *two-generator* numerical semigroups of genus  $g$ , which is known to also count certain special factorizations of  $2g$ . Further focusing on the case  $g = p^k$  for any odd prime  $p$  and  $k \geq 1$ , we show that  $n(p^k, 2)$  only depends on the class of  $p$  modulo a certain explicit modulus  $M(k)$ . The main ingredient is a reduction of  $\gcd(p^\alpha + 1, 2p^\beta + 1)$  to a simpler form, using the continued fraction of  $\alpha/\beta$ . We treat the case  $k = 9$  in detail and show explicitly how  $n(p^9, 2)$  depends on the class of  $p \bmod M(9) = 3 \cdot 5 \cdot 11 \cdot 17 \cdot 43 \cdot 257$ .

**Keywords.** Gap number; Sylvester's theorem; Special factorizations; Euclidean algorithm; Continued fractions; RSA.

## 1 Introduction

A *numerical semigroup* is a subset  $S \subset \mathbb{N}$  containing 0, stable under addition and with finite complement in  $\mathbb{N}$ . The cardinality of  $\mathbb{N} \setminus S$  is then called the *gap number* or the *genus* of  $S$ . It is well known that, given  $g \in \mathbb{N}$ , there are only finitely many numerical semigroups of genus  $g$ . Yet the question of *counting them* seems to be a very hard problem, analogous to the one of

---

\*eliahou@lmpa.univ-littoral.fr.

†jramirez@math.univ-montp2.fr

counting numerical semigroups by Frobenius number. See [1, 2] for some nice conjectures about it. The problem becomes more tractable when restricted to semigroups  $S = \langle a, b \rangle = \mathbb{N}a + \mathbb{N}b$  with two generators. So, let us denote by  $n(g, 2)$  the number of numerical semigroups  $S = \langle a, b \rangle$  of genus  $g$ . On the one hand, determining  $n(g, 2)$  is linked to hard factorization problems, like factoring Fermat and Mersenne numbers [3]. On the other hand, the value of  $n(g, 2)$  is known for all  $g = 2^k$  with  $k \geq 1$ , and for all  $g = p^k$  with  $p$  an odd prime and  $k \leq 8$ . Indeed, exact formulas are provided in [3], showing in particular that  $n(p^k, 2)$  for  $k = 1, 2, 3, 4, 5, 6, 7$  and  $8$  only depends on the class of  $p$  modulo  $3, 1, 15, 7, 255, 31, 36465$  and  $27559$ , respectively. See also Section 7, where these formulas are given in a new form.

Our purpose in this paper is to extend our understanding of  $n(p^k, 2)$  to arbitrary exponents  $k \in \mathbb{N}$ . Giving exact formulas in all cases is out of reach since, for instance, a formula for  $n(p^{4097}, 2)$  would require the still unknown factorization of the 12th Fermat number  $2^{2^{12}} + 1$ . However, what can and will be done here is to show that, *for all  $k \geq 1$ , the value of  $n(p^k, 2)$  only depends on the class of  $p$  modulo some explicit modulus  $M(k)$ .*

This result is formally stated and proved in Section 4. Here is how  $M(k)$  is defined:

$$M(k) = \text{rad}\left(\prod_{i=1}^k (2^{i/\text{gcd}(i,k)} - (-1)^{k/\text{gcd}(i,k)})\right),$$

where  $\text{rad}(n)$  denotes the product of the distinct prime factors of  $n$ , i.e. the largest square-free divisor of  $n$ . We start by recalling in Section 2 that  $n(g, 2)$  can be identified with the counting function of certain special factorizations of  $2g$ . In Section 3, we reduce  $\text{gcd}(p^\alpha + 1, 2p^\beta + 1)$  for  $\alpha, \beta \in \mathbb{N}$  to the simpler form

$$\text{gcd}(p^{\text{gcd}(\alpha,\beta)} \pm 2^\rho, c)$$

where  $\rho, c \in \mathbb{Z}$  only depend on  $\alpha, \beta$  and not on  $p$ . This reduction uses the continued fraction of  $\alpha/\beta$  and directly leads to our main result in Section 4. In Section 5, we introduce basic binary functions  $X_{a,q}$  which will serve as building blocks in our formulas. The case  $k = 9$  is treated in detail in Section 6, where we give an explicit formula for  $n(p^9, 2)$  depending on the class of  $p \bmod M(9) = 3 \cdot 5 \cdot 11 \cdot 17 \cdot 43 \cdot 257$ . We also provide a formula in the case  $k = 10$  with somewhat less details. Finally, in the last section we give and prove new formulas for  $n(p^k, 2)$  with  $k \leq 8$  in terms of the  $X_{a,q}$ .

Background information on numerical semigroups can be found in the books [4, 5].

## 2 Special factorizations of $2g$

We first recall from [3] that  $n(g, 2)$  can be identified with the counting number of factorizations  $uv$  of  $2g$  in  $\mathbb{N}$  satisfying  $\gcd(u+1, v+1) = 1$ . In formula:

$$n(g, 2) = \#\{\{u, v\} \subset \mathbb{N} \mid uv = 2g, \gcd(u+1, v+1) = 1\}. \quad (1)$$

This follows from the classical theorem of Sylvester [6] stating that whenever  $\gcd(a, b) = 1$ , the genus  $g$  of the numerical semigroup  $S = \langle a, b \rangle$  is given by

$$g = \frac{(a-1)(b-1)}{2}.$$

For  $g = p^k$  with  $p$  an odd prime, an immediate consequence of (1) is the following formula.

**Proposition 2.1** *For any odd prime  $p$  and exponent  $k \geq 1$ , we have*

$$n(p^k, 2) = \#\{0 \leq i \leq k \mid \gcd(p^i + 1, 2p^{k-i} + 1) = 1\}. \blacksquare$$

Thus, in order to understand the behavior of  $n(p^k, 2)$ , we need to gain some control on

$$\gcd(p^\alpha + 1, 2p^\beta + 1)$$

for  $\alpha, \beta \in \mathbb{N}$ , and hopefully find ways to determine when this greatest common divisor equals 1. This is addressed in the next section.

## 3 On $\gcd(p^\alpha + 1, 2p^\beta + 1)$

Here is the key technical tool which will lead to our main result in Section 4. Given  $\alpha, \beta \in \mathbb{N}$ , we shall reduce the greatest common divisor

$$\gcd(p^\alpha + 1, 2p^\beta + 1)$$

to the simpler form

$$\gcd(p^\delta \pm 2^\rho, c),$$

where  $\delta = \gcd(\alpha, \beta)$  and where  $\rho, c \in \mathbb{Z}$  only depend on  $\alpha, \beta$  and not on  $p$ . For this purpose, it is more convenient to work in the ring  $\mathbb{Z}[2^{-1}]$  where 2 is made invertible. Moreover, one may effortlessly replace  $\mathbb{Z}[2^{-1}]$  by any unique factorization domain  $A$ , and 2 by any invertible element  $u$  in  $A$ . Of course then, the gcd is only defined up to invertible elements of  $A$ . The proof in this more general context remains practically the same.

**Proposition 3.1** *Let  $A$  be a unique factorization domain and let  $x, u \in A$  with  $u$  invertible. Let  $\alpha, \beta \in \mathbb{N}$  and set  $\delta = \gcd(\alpha, \beta)$ . Then there exists  $\rho \in \mathbb{Z}$  such that*

$$\gcd(x^\alpha + 1, ux^\beta + 1) = \gcd(x^\delta \pm u^\rho, u^{\alpha/\delta} - (-1)^{(\alpha-\beta)/\delta}).$$

The proof is based on a careful study of the successive steps in the Euclidean algorithm for computing gcd's.

**Proof.** First note that, since  $u$  is invertible, we have

$$\gcd(x^\alpha + 1, ux^\beta + 1) = \gcd(x^\alpha + 1, x^\beta + u^{-1}).$$

Set  $r_0 = \alpha, r_1 = \beta$ . Consider the Euclidean algorithm to compute  $\gcd(r_0, r_1)$ :

$$r_i = a_i r_{i+1} + r_{i+2} \tag{2}$$

for all  $0 \leq i \leq n-1$ , where  $0 \leq r_{i+1} < r_i$  for all  $1 \leq i \leq n-1$ ,  $r_{n+1} = 0$ ,  $r_n = \gcd(r_0, r_1)$ . Of course, the  $a_i$ 's are the *partial quotients* of the continued fraction  $[a_0, a_1, \dots, a_n]$  of  $\alpha/\beta$ . We have

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{i+1} \\ r_{i+2} \end{pmatrix} \tag{3}$$

for all  $0 \leq i \leq n-1$ . Set  $(s_0, s_1) = (1, 1)$  and  $(t_0, t_1) = (0, -1)$ . Then we have

$$\begin{aligned} x^{r_0} + 1 &= x^{r_0} - (-1)^{s_0} u^{t_0}, \\ x^{r_1} + u^{-1} &= x^{r_1} - (-1)^{s_1} u^{t_1}. \end{aligned}$$

For  $i = 0, \dots, n-1$ , recursively define

$$\begin{aligned} s_{i+2} &= s_i - a_i s_{i+1}, \\ t_{i+2} &= t_i - a_i t_{i+1}. \end{aligned}$$

Then as in (3), we have

$$\begin{pmatrix} s_i \\ s_{i+1} \end{pmatrix} = \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} s_{i+1} \\ s_{i+2} \end{pmatrix}, \tag{4}$$

$$\begin{pmatrix} t_i \\ t_{i+1} \end{pmatrix} = \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} t_{i+1} \\ t_{i+2} \end{pmatrix} \tag{5}$$

for all  $0 \leq i \leq n-1$ . Finally, for all  $0 \leq j \leq n+1$ , set

$$f_j = x^{r_j} - (-1)^{s_j} u^{t_j}.$$

Note that  $f_0 = x^{r_0} + 1$ ,  $f_1 = x^{r_1} + u^{-1}$ , and

$$f_{n+1} = 1 - (-1)^{s_{n+1}} u^{t_{n+1}} \quad (6)$$

since  $r_{n+1} = 0$ .

**Claim.** For all  $0 \leq i \leq n-1$ , we have

$$\gcd(f_i, f_{i+1}) = \gcd(f_{i+1}, f_{i+2}). \quad (7)$$

Indeed, it follows from (2) that

$$\begin{aligned} f_i &= x^{r_i} - (-1)^{s_i} u^{t_i} \\ &= (x^{r_{i+1}})^{a_i} x^{r_{i+2}} - (-1)^{s_i} u^{t_i}. \end{aligned}$$

Now, since

$$x^{r_{i+1}} \equiv (-1)^{s_{i+1}} u^{t_{i+1}} \pmod{f_{i+1}},$$

we find

$$\begin{aligned} f_i &\equiv ((-1)^{s_{i+1}} u^{t_{i+1}})^{a_i} x^{r_{i+2}} - (-1)^{s_i} u^{t_i} \pmod{f_{i+1}} \\ &\equiv (-1)^{a_i s_{i+1}} u^{a_i t_{i+1}} x^{r_{i+2}} - (-1)^{s_i} u^{t_i} \pmod{f_{i+1}}. \end{aligned}$$

Thus,

$$\begin{aligned} (-1)^{-a_i s_{i+1}} u^{-a_i t_{i+1}} f_i &\equiv x^{r_{i+2}} - (-1)^{s_i - a_i s_{i+1}} u^{t_i - a_i t_{i+1}} \pmod{f_{i+1}} \\ &\equiv x^{r_{i+2}} - (-1)^{s_{i+2}} u^{t_{i+2}} \pmod{f_{i+1}} \\ &\equiv f_{i+2} \pmod{f_{i+1}}. \end{aligned}$$

Consequently, we have  $f_i \equiv (-1)^{a_i s_{i+1}} u^{a_i t_{i+1}} f_{i+2} \pmod{f_{i+1}}$ . Using the equality

$$\gcd(f, g) = \gcd(g, h)$$

whenever  $f \equiv h \pmod{g}$  for elements in  $A$ , we conclude that

$$\begin{aligned} \gcd(f_i, f_{i+1}) &= \gcd(f_{i+1}, (-1)^{a_i s_{i+1}} u^{a_i t_{i+1}} f_{i+2}) \\ &= \gcd(f_{i+1}, f_{i+2}) \end{aligned}$$

since  $(-1)^{a_i s_{i+1}} u^{a_i t_{i+1}}$  is a unit in  $A$ . This proves the claim.

As a first consequence, we get

$$\gcd(f_0, f_1) = \gcd(f_n, f_{n+1}). \quad (8)$$

Denote now

$$A = \prod_{i=0}^{n-1} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}.$$

We have  $\det A = (-1)^n$ , and it follows from repeatedly applying (3) that

$$\begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = A \begin{pmatrix} r_n \\ 0 \end{pmatrix}.$$

This implies, in particular, that  $\alpha_{11} = r_0/r_n$  and  $\alpha_{21} = r_1/r_n$ . Similarly, using (5) repeatedly, we have

$$A^{-1} \begin{pmatrix} t_0 \\ t_1 \end{pmatrix} = \begin{pmatrix} t_n \\ t_{n+1} \end{pmatrix}.$$

Since  $A^{-1} = (-1)^n \begin{pmatrix} \alpha_{22} & -\alpha_{12} \\ -\alpha_{21} & \alpha_{11} \end{pmatrix}$  and  $\begin{pmatrix} t_0 \\ t_1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$ , this implies that

$$t_{n+1} = (-1)^{n+1} \alpha_{11} = (-1)^{n+1} r_0/r_n.$$

Finally, using (4) repeatedly, we have

$$A^{-1} \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} = \begin{pmatrix} s_n \\ s_{n+1} \end{pmatrix}.$$

As above, and since  $\begin{pmatrix} s_0 \\ s_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ , we find that

$$s_{n+1} = (-1)^n (-\alpha_{21} + \alpha_{11}) = (-1)^n (r_0 - r_1)/r_n.$$

Summarizing, it follows from the equality (8), the expression (6) for  $f_{n+1}$ , and the above values of  $s_{n+1}, t_{n+1}$ , that

$$\begin{aligned} \gcd(x^\alpha + 1, ux^\beta + 1) &= \gcd(f_n, f_{n+1}) \\ &= \gcd(x^{r_n} - (-1)^{s_n} u^{t_n}, 1 - (-1)^{s_{n+1}} u^{t_{n+1}}) \\ &= \gcd(x^\delta - (-1)^{s_n} u^{t_n}, u^{\alpha/\delta} - (-1)^{(\alpha-\beta)/\delta}). \end{aligned}$$

■

The special case of interest to us, namely where  $A = \mathbb{Z}[2^{-1}]$  and  $u = 2$ , reduces to the following statement.

**Corollary 3.2** *Let  $1 \leq i \leq k$  be given integers, and set  $\delta = \gcd(i, k)$ . Then there exists  $\rho \in \mathbb{Z}$  such that for any odd prime  $p$ , we have*

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

**Proof.** First observe that  $\gcd(p^i + 1, 2p^{k-i} + 1)$  is odd since the second argument is, so we may as well work in  $\mathbb{Z}[2^{-1}]$  when computing this gcd. Set  $\alpha = i$ ,  $\beta = k - i$ . Since  $\gcd(i, k - i) = \gcd(i, k)$ , the values of  $\delta$  in Proposition 3.1 and here are the same. Now  $(\alpha - \beta)/\delta = (2i - k)/\delta$ , and so

$$(-1)^{(\alpha-\beta)/\delta} = (-1)^{k/\delta}.$$

The claimed formula for  $\gcd(p^i + 1, 2p^{k-i} + 1)$  now follows directly from that in Proposition 3.1. ■

Consequently, given  $1 \leq i \leq k$ , an odd prime  $p$  satisfies the condition

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

if and only if  $p$  belongs to a certain union of classes mod  $(2^{i/\delta} - (-1)^{k/\delta})$ , where as above  $\delta = \gcd(i, k)$ . This is the key to our main result below.

## 4 The main result

For a positive integer  $n$ , let  $\text{rad}(n)$  denote the *radical* of  $n$ , i.e. the product of the distinct primes factors of  $n$ . For instance,  $\text{rad}(4) = 2$  and  $\text{rad}(6) = \text{rad}(12) = \text{rad}(18) = 6$ . Given  $k \geq 1$ , let us define

$$M(k) = \text{rad}\left(\prod_{i=1}^k (2^{i/\gcd(i,k)} - (-1)^{k/\gcd(i,k)})\right).$$

Note that if  $k$  is odd, the formula becomes

$$M(k) = \text{rad}\left(\prod_{i=1}^k (2^{i/\gcd(i,k)} + 1)\right),$$

whereas if  $k$  is even there is no such reduction in general, since the exponent  $k/\gcd(i, k)$  may assume both parities. Here is our main result.



**Theorem 4.1** For any odd prime  $p$  and  $k \geq 1$ , the value of  $n(p^k, 2)$  only depends on the class of  $p$  modulo  $M(k)$ .

**Proof.** Recall the formula given by Proposition 2.1:

$$n(p^k, 2) = \#\{0 \leq i \leq k \mid \gcd(p^i + 1, 2p^{k-i} + 1) = 1\}. \quad (9)$$

If  $i = 0$ , then  $\gcd(2, 2p^k + 1) = 1$  always, since  $p$  is odd. Assume now  $1 \leq i \leq k$ , and set

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

By Corollary 3.2, the value of  $\gcd(p^i + 1, 2p^{k-i} + 1)$  only depends on the class of  $p \bmod m_k(i)$ . Therefore, it follows from (9) and this property of  $m_i(k)$  that if we set

$$M(k) = \text{rad}\left(\prod_{i=1}^k m_k(i)\right),$$

the value of  $n(p^k, 2)$  only depends on the class of  $p \bmod M(k)$ . ■

For concreteness, Table 1 gives the value of  $M(k)$  for  $1 \leq k \leq 10$ . We have seen that  $n(p^k, 2)$  only depends on the class of  $p$  modulo  $M(k)$ . But  $M(k)$  is not necessarily the *smallest* modulus with this property, only a multiple of it. For instance, we have  $M(4) = 21$ , but the value of  $n(p^4, 2)$  only depends on the class of  $p \bmod 7$ , as stated in the Introduction. However, for all *odd*  $k$  in the range  $1 \leq k \leq 9$ , the modulus  $M(k)$  actually turns out to be optimal for the desired property. (See [3] and Section 7.)

$k$	1	2	3	4	5	6	7	8	9	10
$M(k)$	3	3	15	21	255	465	36465	82677	30998055	16548735

Table 1: First 10 values of  $M(k)$ .

## 5 The basic functions $X_{a,q}$

We now introduce numerical functions  $X_{a,q}$ , with values in  $\{0, 1\}$ , which will subsequently serve as building blocks in our explicit formulas for  $n(p^k, 2)$

with  $k \leq 10$ . Given integers  $a, q$  with  $q \geq 2$ , the definition of

$$X_{a,q} : \mathbb{Z} \rightarrow \{0, 1\}$$

depends on the distinct prime factors of  $q$ , as follows.

- If  $q$  is prime, then  $X_{a,q}$  is the indicator function of the complement of the subset  $a + q\mathbb{Z}$  in  $\mathbb{Z}$ , i.e.

$$X_{a,q}(n) = \begin{cases} 1 & \text{if } n \not\equiv a \pmod{q}, \\ 0 & \text{if } n \equiv a \pmod{q}. \end{cases}$$

- If  $q_1, \dots, q_t$  are the distinct prime factors of  $q$ , then we set

$$X_{a,q} = \prod_{i=1}^t X_{a,q_i}.$$

In particular, since  $X_{a,q}$  only depends on the prime factors of  $q$ , we have

$$X_{a,q} = X_{a,\text{rad}(q)}.$$

Note that  $X_{a,q}$  *only depends on the class of  $a$  mod  $q$* . It is also plain that  $X_{a,q}(n)$  only depends on the class of  $n$  mod  $q$ .

We now establish a few more properties of these functions. The first one links  $X_{a,q}(n)$  with  $\gcd(n - a, q)$ , and so will be useful to capture occurrences of the equality  $\gcd(p^i + 1, 2p^{k-i} + 1) = 1$ .

**Proposition 5.1** *Let  $a, q$  be integers with  $q \geq 2$ . For all  $n \in \mathbb{Z}$ , we have*

$$X_{a,q}(n) = \begin{cases} 1 & \text{if } \gcd(n - a, q) = 1, \\ 0 & \text{if not.} \end{cases}$$

**Proof.** Let  $q_1, \dots, q_t$  be the distinct prime factors of  $q$ . Then we have

$$\begin{aligned} X_{a,q}(n) = 1 &\iff X_{a,q_i}(n) = 1 \ \forall i \\ &\iff n \not\equiv a \pmod{q_i} \ \forall i \\ &\iff \gcd(n - a, q_i) = 1 \ \forall i \\ &\iff \gcd(n - a, q) = 1. \end{aligned}$$

Since  $X_{a,q}(n)$  only takes values in  $\{0, 1\}$ , this implies that  $X_{a,q}(n) = 0$  if and only if  $\gcd(n - a, q) \neq 1$ . ■

Next, for determining  $n(p^k, 2)$ , we often need to evaluate  $X_{a,q}(p^s)$  with  $s \geq 2$ . The next two properties help remove that exponent  $s$ . The first one reduces the task to the case where  $s$  divides  $q - 1$ . It suffices to consider the case where  $q$  is prime.

**Proposition 5.2** *Let  $q$  be a prime number, and let  $a, s$  be integers with  $s \geq 2$ . Write  $s = te$  with  $t = \gcd(s, q - 1)$ , so that  $\gcd(e, q - 1) = 1$ . Let  $d \in \mathbb{N}$  satisfy  $de \equiv 1 \pmod{q - 1}$ . Then*

$$X_{a,q}(n^s) = X_{a^d,q}(n^t)$$

for all integers  $n$ .

**Proof.** This is the heart of the RSA cryptographic protocol, which relies on the fact that exponentiation to the power  $e$  in  $\mathbb{Z}/q\mathbb{Z}$  is a bijection, whose inverse is exponentiation to the power  $d$ . We have

$$\begin{aligned} X_{a,q}(n^s) = 0 &\iff n^s \equiv a \pmod{q} \\ &\iff (n^t)^e \equiv a \pmod{q} \\ &\iff (n^t)^{de} \equiv a^d \pmod{q} \\ &\iff n^t \equiv a^d \pmod{q} \\ &\iff X_{a^d,q}(n^t) = 0. \end{aligned}$$

■

Thus, we may now assume that the exponent  $s$  divides  $q - 1$ .

**Proposition 5.3** *Let  $q$  be a prime number, and let  $a, s$  be integers with  $s$  dividing  $q - 1$ . Let  $g \in \mathbb{N}$  be an integer whose class mod  $q$  generates the multiplicative group of non-zero elements in  $\mathbb{Z}/q\mathbb{Z}$ . We have:*

- If  $a$  is not an  $s$ -power mod  $q$ , then  $X_{a,q}(n^s) = 1$  for all  $n$ .
- If  $a$  is an  $s$ -power mod  $q$ , then  $a \equiv g^{si} \pmod{q}$  for some integer  $i$  such that  $0 \leq i \leq (q - 1)/s - 1$ , and

$$X_{a,q}(n^s) = \prod_{j=0}^{s-1} X_{g^{i+j(q-1)/s},q}(n)$$

for all integers  $n$ .

**Proof.** In the group  $(\mathbb{Z}/q\mathbb{Z})^*$  of nonzero classes mod  $q$ , the set of  $s$ -powers is of cardinality  $(q-1)/s$  and coincides with

$$\{g^{si} \bmod q \mid 0 \leq i \leq (q-1)/s - 1\}.$$

First, if  $a$  is not an  $s$ -power mod  $q$ , then  $n^s \not\equiv a \bmod q$  for all  $n$ , implying  $X_{a,q}(n^s) = 0$  for all  $n$ . Assume now  $a$  is an  $s$ -power mod  $q$ . By the above remark, there exists  $0 \leq i \leq (q-1)/s - 1$  such that  $a \equiv g^{si} \bmod q$ . We have

$$\begin{aligned} X_{a,q}(n^s) = 0 &\iff n^s \equiv a \bmod q \\ &\iff n^s \equiv g^{si} \bmod q \\ &\iff \left(\frac{n}{g^i}\right)^s \equiv 1 \bmod q. \end{aligned}$$

This means that  $n/g^i$  is of order dividing  $s$  in the group  $(\mathbb{Z}/q\mathbb{Z})^*$ . Now, the elements of order dividing  $s$  in this group constitute a subgroup of order  $s$  generated by  $g^{j(q-1)/s}$ . Thus, there exists an integer  $j$  such that  $0 \leq j \leq s-1$  and satisfying

$$\frac{n}{g^i} \equiv g^{j(q-1)/s} \bmod q,$$

yielding

$$X_{a,q}(n^s) = 0 \iff n \equiv g^{i+j(q-1)/s} \bmod q.$$

Summarizing, for  $a \equiv g^{si} \bmod q$ , we have established the equivalence

$$X_{a,q}(n^s) = 0 \iff \prod_{j=0}^{s-1} X_{g^{i+j(q-1)/s},q}(n) = 0,$$

whence the claimed equality  $X_{a,q}(n^s) = \prod_{j=0}^{s-1} X_{g^{i+j(q-1)/s},q}(n)$ . ■

**Example 5.4** In order to establish our formula for  $n(p^{10}, 2)$  in Section 6, the term  $X_{8,17}(p^2)$  turns out to be involved. Now 8 is a square mod 17, namely  $8 \equiv 5^2 \equiv 12^2 \bmod 17$ . Thus, the above result yields

$$X_{8,17}(p^2) = X_{5,17}(p)X_{12,17}(p).$$

## 6 The cases $k = 9, 10$

Explicit formulas for  $n(p^k, 2)$  with  $p$  an odd prime and  $k \leq 6$  or  $k = 8$  are given in [3]. Here we go further and treat the case  $k = 9$  in detail. This will show how Corollary 3.2 can be applied, and will also give a sense of the increasing complexity of these formulas. We also briefly address the case  $k = 10$ . The main ingredients are the basic functions  $X_{a,q}$  defined in the preceding section.

Here comes our formula for  $n(p^9, 2)$ . The fact that it depends on the class of  $p \pmod{M(9)}$  follows from this prime decomposition:

$$M(9) = 30998055 = 5 \cdot 17 \cdot 257 \cdot 3 \cdot 11 \cdot 43.$$

**Theorem 6.1** *Let  $p$  be an odd prime. Then we have*

$$n(p^9, 2) = 1 + 2X_{3,5}(p) + X_{9,17}(p) + X_{128,257}(p) + X_{2,3}(p) \cdot (3 + X_{2,11}(p) + X_{8,43}(p)).$$

**Proof.** By Proposition 2.1, in order to determine  $n(p^9, 2)$ , it suffices to count those exponents  $i$  between 0 and 9 satisfying  $\gcd(p^i + 1, 2p^{9-i} + 1) = 1$ . Using Corollary 3.2 and the calculations leading to it, these gcd's may be reduced as follows:

$$\begin{aligned} \gcd(p^0 + 1, 2p^9 + 1) &= 1 \\ \gcd(p^1 + 1, 2p^8 + 1) &= \gcd(p + 1, 3) \\ \gcd(p^2 + 1, 2p^7 + 1) &= \gcd(2p - 1, 5) \\ \gcd(p^3 + 1, 2p^6 + 1) &= \gcd(p^3 + 1, 3) = \gcd(p + 1, 3) \\ \gcd(p^4 + 1, 2p^5 + 1) &= \gcd(2p - 1, 17) \\ \gcd(p^5 + 1, 2p^4 + 1) &= \gcd(p - 2, 33) \\ \gcd(p^6 + 1, 2p^3 + 1) &= \gcd(2p^3 + 1, 5) \\ \gcd(p^7 + 1, 2p^2 + 1) &= \gcd(p - 8, 129) \\ \gcd(p^8 + 1, 2p^1 + 1) &= \gcd(2p + 1, 257) \\ \gcd(p^9 + 1, 2p^0 + 1) &= \gcd(p^9 + 1, 3) = \gcd(p + 1, 3). \end{aligned}$$

Now, by Proposition 5.1 and the properties of the functions  $X_{a,q}$ , these equal-

ities imply the following equivalences:

$$\begin{aligned}
\gcd(p^0 + 1, 2p^9 + 1) = 1 & \quad \text{always} \\
\gcd(p^1 + 1, 2p^8 + 1) = 1 & \iff X_{2,3}(p) = 1 \\
\gcd(p^2 + 1, 2p^7 + 1) = 1 & \iff X_{3,5}(p) = 1 \\
\gcd(p^3 + 1, 2p^6 + 1) = 1 & \iff X_{2,3}(p) = 1 \\
\gcd(p^4 + 1, 2p^5 + 1) = 1 & \iff X_{9,17}(p) = 1 \\
\gcd(p^5 + 1, 2p^4 + 1) = 1 & \iff X_{2,33}(p) = 1 \\
\gcd(p^6 + 1, 2p^3 + 1) = 1 & \iff X_{3,5}(p) = 1 \\
\gcd(p^7 + 1, 2p^2 + 1) = 1 & \iff X_{8,129}(p) = 1 \\
\gcd(p^8 + 1, 2p^1 + 1) = 1 & \iff X_{128,257}(p) = 1 \\
\gcd(p^9 + 1, 2p^0 + 1) = 1 & \iff X_{2,3}(p) = 1.
\end{aligned}$$

Read sequentially, this table directly yields the following first formula for  $n(p^9, 2)$ , with 10 summands, in terms of the functions  $X_{a,q}$ :

$$\begin{aligned}
n(p^9, 2) &= 1 + X_{2,3}(p) + X_{3,5}(p) + X_{2,3}(p) + X_{9,17}(p) + X_{2,33}(p) \\
&\quad + X_{3,5}(p) + X_{8,129}(p) + X_{128,257}(p) + X_{2,3}(p) \\
&= 1 + 3X_{2,3}(p) + 2X_{3,5}(p) + X_{9,17}(p) + X_{2,33}(p) + X_{8,129}(p) \\
&\quad + X_{128,257}(p).
\end{aligned}$$

Among the moduli involved above, the only non-prime ones are  $33 = 3 \cdot 11$  and  $129 = 3 \cdot 43$ . By definition of  $X_{a,q}$  for non-prime  $q$ , we have

$$\begin{aligned}
X_{2,33} &= X_{2,3}X_{2,11} \\
X_{8,129} &= X_{8,3}X_{8,43}.
\end{aligned}$$

Moreover, since  $X_{a,q}$  only depends on the class of  $a \pmod q$ , we have

$$X_{8,3} = X_{2,3}.$$

Substituting these equalities in the above formula for  $n(p^9, 2)$ , we get

$$n(p^9, 2) = 1 + 2X_{3,5}(p) + X_{9,17}(p) + X_{128,257}(p) + X_{2,3}(p) \cdot (3 + X_{2,11}(p) + X_{8,43}(p)),$$

as claimed. ■

We now derive another version of our formula for  $n(p^9, 2)$ , from which its values are easier to read. Given positive integers  $q_1, \dots, q_t$ , we denote by

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

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

$$\rho_{5, 17, 257}(p) = (3, -9, -128)$$

means  $p \equiv 3 \bmod 5$ ,  $p \not\equiv 9 \bmod 17$  and  $p \not\equiv 128 \bmod 257$ .

**Corollary 6.2** *Let  $p$  be an odd prime. Consider the following functions of  $p$  depending on its classes mod 5, 17, 257 and 11, 43, respectively:*

$$\lambda(p) = \begin{cases} 1 & \text{if } \rho_{5, 17, 257}(p) = (3, 9, 128) \\ 2 & \text{if } \rho_{5, 17, 257}(p) \in \{(3, 9, -128), (3, -9, 128)\} \\ 3 & \text{if } \rho_{5, 17, 257}(p) \in \{(3, -9, -128), (-3, 9, 128)\} \\ 4 & \text{if } \rho_{5, 17, 257}(p) \in \{(-3, 9, -128), (-3, -9, 128)\} \\ 5 & \text{if } \rho_{5, 17, 257}(p) = (-3, -9, -128), \end{cases}$$

$$\mu(p) = \begin{cases} 3 & \text{if } \rho_{11, 43}(p) = (2, 8) \\ 4 & \text{if } \rho_{11, 43}(p) \in \{(2, -8), (-2, 8)\} \\ 5 & \text{if } \rho_{11, 43}(p) = (-2, -8). \end{cases}$$

Then we have

$$n(p^9, 2) = \begin{cases} \lambda(p) & \text{if } p \equiv 2 \bmod 3, \\ \lambda(p) + \mu(p) & \text{if } p \not\equiv 2 \bmod 3. \end{cases}$$

**Proof.** This directly follows from the preceding result and the easy to prove equalities

$$\begin{aligned} \lambda(p) &= 1 + 2X_{3,5}(p) + X_{9,17}(p) + X_{128,257}(p), \\ \mu(p) &= 3 + X_{2,11}(p) + X_{8,43}(p). \end{aligned}$$

■

It is still clearer now that  $n(p^9, 2)$  is determined by the class of  $p \bmod M(9) = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 11 \cdot 43$ , and that  $M(9)$  is the smallest modulus with this property.

We close this section by briefly treating the case  $k = 10$ . The formula obtained shows that  $n(p^{10}, 2)$ , for  $p$  an odd prime, is determined by the class of  $p$  modulo  $M(10)/15 = 7 \cdot 17 \cdot 73 \cdot 127$ .

**Theorem 6.3** *Let  $p$  be an odd prime. Then we have*

$$n(p^{10}, 2) = 7 + X_{3,7}(p)(1 + X_{36,73}(p)) + X_{5,17}(p)X_{12,17}(p) + X_{123,127}(p).$$

**Proof.** After reducing  $\gcd(p^i + 1, 2p^{10-i} + 1)$  for  $0 \leq i \leq 10$  as in Corollary 3.2, and using Proposition 5.1 involving the functions  $X_{a,q}$ , we obtain this first raw formula:

$$\begin{aligned} n(p^{10}, 2) = & 2 + X_{-1,3}(p^2) + X_{3,7}(p) + X_{-2,5}(p^2) + 1 + X_{2,9}(p^2) + X_{123,127}(p) \\ & + X_{8,17}(p^2) + X_{255,511}(p) + X_{-1,3}(p^{10}). \end{aligned}$$

We now invoke Proposition 5.3 several times. Since  $-1$  is not a square mod 3, we have  $X_{-1,3}(p^2) = 1$ . The same reason yields  $X_{2,9}(p^2) = X_{-1,3}(p^{10}) = 1$ . Similarly, we have  $X_{-2,5}(p^2) = 1$  as  $-2$  is not a square mod 5. As already explained in Example 5.4, we have  $X_{8,17}(p^2) = X_{5,17}(p)X_{12,17}(p)$ . Finally, since  $511 = 7 \cdot 73$ , and since 255 is congruent to 3 mod 7 and to 36 mod 73, we have

$$X_{255,511}(p) = X_{3,7}(p)X_{36,73}(p).$$

Inserting these reductions into the raw formula gives the stated one, where now the only argument of the various basic functions  $X_{a,q}$  is  $p$  and all involved  $q$ 's are primes. ■

## 7 The cases $k \leq 8$ revisited

While explicit formulas for  $n(p^k, 2)$  with  $k \leq 6$  and  $k = 8$  are given in [3], we provide here new, shorter formulas in terms of the basic functions  $X_{a,q}$  for  $k \leq 8$ , including  $k = 7$ . The construction method is similar to the cases  $k = 9, 10$  and relies on the reduction of  $\gcd(p^i + 1, 2p^{k-i} + 1)$  provided by Corollary 3.2.



**Theorem 7.1** *Let  $p$  be an odd prime. Then we have*

$$\begin{aligned}
n(p^1, 2) &= 1 + X_{2,3}(p) \\
n(p^2, 2) &= 3 \\
n(p^3, 2) &= 1 + 2X_{2,3}(p) + X_{2,5}(p) \\
n(p^4, 2) &= 4 + X_{3,7}(p) \\
n(p^5, 2) &= 1 + 3X_{2,3}(p) + X_{3,5}(p) + X_{8,17}(p) \\
n(p^6, 2) &= 6 + X_{15,31}(p) \\
n(p^7, 2) &= 1 + X_{2,3}(p)(3 + X_{7,11}(p)) + X_{2,5}(p)(1 + X_{6,13}(p)) + X_{2,17}(p) \\
n(p^8, 2) &= 6 + X_{5,7}(p) + X_{23,31}(p) + X_{63,127}(p).
\end{aligned}$$

**Proof.** Corollary 3.2 and its proof method yield the following reductions of  $\gcd(p^i + 1, 2p^{k-i} + 1)$  for  $i = 1, \dots, k$ . The case  $i = 0$  is omitted, as  $\gcd(p^0 + 1, 2p^k + 1) = 1$  always. A few more arithmetical reductions are also applied. For instance, the equality  $\gcd(p^2 + 1, 3) = 1$  below follows from the fact that  $-1$  is not a square mod 3. This is one easy case of Proposition 5.3.

$$\begin{aligned}
k &= 1 : \\
\gcd(p^1 + 1, 2p^0 + 1) &= \gcd(p + 1, 3)
\end{aligned}$$

$$\begin{aligned}
k &= 2 : \\
\gcd(p^1 + 1, 2p^1 + 1) &= \gcd(2p + 1, 1) = 1 \\
\gcd(p^2 + 1, 2p^0 + 1) &= \gcd(p^2 + 1, 3) = 1
\end{aligned}$$

$$\begin{aligned}
k &= 3 : \\
\gcd(p^1 + 1, 2p^2 + 1) &= \gcd(p + 1, 3) \\
\gcd(p^2 + 1, 2p^1 + 1) &= \gcd(2p + 1, 5) \\
\gcd(p^3 + 1, 2p^0 + 1) &= \gcd(p^3 + 1, 3) = \gcd(p + 1, 3)
\end{aligned}$$

$$\begin{aligned}
k &= 4 : \\
\gcd(p^1 + 1, 2p^3 + 1) &= \gcd(p + 1, 1) = 1 \\
\gcd(p^2 + 1, 2p^2 + 1) &= \gcd(2p^2 + 1, 1) = 1 \\
\gcd(p^3 + 1, 2p^1 + 1) &= \gcd(2p + 1, 7) \\
\gcd(p^4 + 1, 2p^0 + 1) &= \gcd(p^4 + 1, 3) = 1
\end{aligned}$$

$$k = 5 :$$

$$\begin{aligned} \gcd(p^1 + 1, 2p^4 + 1) &= \gcd(p + 1, 3) \\ \gcd(p^2 + 1, 2p^3 + 1) &= \gcd(2p - 1, 5) \\ \gcd(p^3 + 1, 2p^2 + 1) &= \gcd(p - 2, 9) \\ \gcd(p^4 + 1, 2p^1 + 1) &= \gcd(2p + 1, 17) \\ \gcd(p^5 + 1, 2p^0 + 1) &= \gcd(p^5 + 1, 3) = \gcd(p + 1, 3) \end{aligned}$$

$$k = 6 :$$

$$\begin{aligned} \gcd(p^1 + 1, 2p^5 + 1) &= \gcd(p + 1, 1) = 1 \\ \gcd(p^2 + 1, 2p^4 + 1) &= \gcd(p^2 + 1, 3) = 1 \\ \gcd(p^3 + 1, 2p^3 + 1) &= \gcd(2p^3 + 1, 1) = 1 \\ \gcd(p^4 + 1, 2p^2 + 1) &= \gcd(2p^2 + 1, 5) = 1 \\ \gcd(p^5 + 1, 2p^1 + 1) &= \gcd(2p + 1, 31) \\ \gcd(p^6 + 1, 2p^0 + 1) &= \gcd(p^6 + 1, 3) = 1 \end{aligned}$$

$$k = 7 :$$

$$\begin{aligned} \gcd(p^1 + 1, 2p^6 + 1) &= \gcd(p + 1, 3) \\ \gcd(p^2 + 1, 2p^5 + 1) &= \gcd(2p + 1, 5) \\ \gcd(p^3 + 1, 2p^4 + 1) &= \gcd(2p - 1, 9) \\ \gcd(p^4 + 1, 2p^3 + 1) &= \gcd(p - 2, 17) \\ \gcd(p^5 + 1, 2p^2 + 1) &= \gcd(p + 4, 33) \\ \gcd(p^6 + 1, 2p^1 + 1) &= \gcd(2p + 1, 65) \\ \gcd(p^7 + 1, 2p^0 + 1) &= \gcd(p^7 + 1, 3) = \gcd(p + 1, 3) \end{aligned}$$

$$k = 8 :$$

$$\begin{aligned} \gcd(p^1 + 1, 2p^7 + 1) &= \gcd(p + 1, 1) = 1 \\ \gcd(p^2 + 1, 2p^6 + 1) &= \gcd(p^2 + 1, 1) = 1 \\ \gcd(p^3 + 1, 2p^5 + 1) &= \gcd(p + 2, 7) \\ \gcd(p^4 + 1, 2p^4 + 1) &= \gcd(2p^4 + 1, 1) = 1 \\ \gcd(p^5 + 1, 2p^3 + 1) &= \gcd(4p + 1, 31) \\ \gcd(p^6 + 1, 2p^2 + 1) &= \gcd(2p^2 + 1, 7) = 1 \\ \gcd(p^7 + 1, 2p^1 + 1) &= \gcd(2p + 1, 127) \\ \gcd(p^8 + 1, 2p^0 + 1) &= \gcd(p^8 + 1, 3) = 1. \end{aligned}$$

As in the case  $k = 9$ , the claimed formulas follow by reading these tables sequentially and using properties of the functions  $X_{a,q}$  from Section 5. ■

In particular, these formulas confirm that for  $k = 1, \dots, 8$ , the value of  $n(p^k, 2)$  at an odd prime  $p$  is determined by the class of  $p$  modulo 3, 1,  $3 \cdot 5$ , 7,  $3 \cdot 5 \cdot 17$ , 31,  $3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$  and  $7 \cdot 31 \cdot 127$ , respectively.

## 8 A question

We shall conclude this paper with an open question. On the one hand, we have obtained explicit formulas for  $n(p^k, 2)$  in all cases  $k \leq 10$ . On the other hand, we know from [3] that no such formula can be expected in the case  $k = 4097$ , at least as long as the prime factors of the 12th Fermat number  $2^{2^{12}} + 1$  remain unknown. Well then, what happens in the intermediate range  $11 \leq k \leq 4096$ ? Are there fundamental obstacles which would prevent us to obtain exact formulas for  $n(p^k, 2)$  all the way up to  $k = 4096$ ?

## 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] S. ELIAHOU AND J.L. RAMÍREZ ALFONSÍN, Two-generator numerical semigroups and Fermat and Mersenne numbers, *SIAM J. Discrete Math.* 25 (2011) 622–630.
- [4] J.L. RAMÍREZ ALFONSÍN, *The Diophantine Frobenius problem*. Oxford Lecture Series in Mathematics and its Applications 30, Oxford University Press, Oxford, 2005.
- [5] J.C. ROSALES AND P.A. GARCÍA-SÁNCHEZ, *Numerical semigroups*. Developments in Mathematics, 20. Springer, New York, 2009.
- [6] 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<sup>a,b,c</sup>,

<sup>a</sup>Univ Lille Nord de France, F-59000 Lille, France

<sup>b</sup>ULCO, LMPA J. Liouville, B.P. 699, F-62228 Calais, France

<sup>c</sup>CNRS, FR 2956, France

- 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