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

IMNS2012

July 20th, Vila Real

Shalom Eliahou

(with Jorge Ramírez Alfonsín)

Motivation

For $g \in \mathbb{N}$, let $N(g) =$ the number of numerical semigroups $S \subset \mathbb{N}$ of genus g.

Conjecture (Bras-Amorós): $N(g) \geq N(g-1) + N(g-2)$.

* * *

For $g, e \in \mathbb{N}$, denote $N_e(g) =$ the number of numerical semigroups $S \subset \mathbb{N}$ of genus g and embedding dimension e.

Question. Might it be true that $N_e(g) \geq N_e(g-1) + N_e(g-2)$?

The case $e = 2$

Question. Is it true that $N_2(g) \geq N_2(g-1) + N_2(g-2)$?

* * *

Sylvester (1867). If $\gcd(a,b) = 1$, then $S = \langle a, b \rangle$ has genus

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

Consequently, $N_2(g)$ counts special factorizations of $2g$:

$$N_2(g) = |\{u \leq v \in \mathbb{N} \mid 2g = uv \text{ and } \gcd(u+1, v+1) = 1\}|.$$

(Set $u = a - 1$, $v = b - 1$.)

Thus, determining $N_2(g)$ should be hard in general, since it requires knowing the factorization of g.

* * *

However, there are cases where:

- We don't know the factorization of g, but we can determine $N_2(g)$.
- We know the factorization of g, but we can't determine $N_2(g)$.

First results

Proposition 1. $N_2(g) \geq 1$ *for all* g.

Proof. Factor $2g$ as $1 \cdot 2g$. Thus, $S = \langle 2, 2g+1 \rangle$ has genus g. □

Proposition 2. *Assume* $g \geq 3$ *and* $2g-1$ *prime. Then* $N_2(g) = d(2g)/2$, *where* $d(n)$ *is the number of divisors of* n.

Proof. All factorizations of $2g$ are special! Why? Let $2g = uv$. We claim $\gcd(u+1, v+1) = 1$. Indeed, let

$$\delta = \gcd(u+1, v+1).$$

Then $u \equiv v \equiv -1 \bmod \delta$. So $uv \equiv 1 \bmod \delta$. So $2g \equiv 1 \bmod \delta$. So δ divides $2g-1$. But $\delta < 2g-1$ as easily seen. Whence $\delta = 1$. □

When $g = 2^k$

Proposition 3. *Let $g = 2^k$. Let s be the largest odd factor of $k+1$. Then*

$$N_2(g) = \frac{s+1}{2}.$$

Proof. (Sketch) Factorizations of $2g$:

$$2^i 2^{k+1-i}$$

for $0 \leq i \leq k+1-i$. One finds that those i for which

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

are characterized by the condition $\nu_2(i) < \nu_2(k+1)$. □

A consequence

We have seen:

$$N_2(2^k) = \frac{s+1}{2},$$

where $s =$ largest odd factor of $k+1$.

For $s = 1$, we get $N_2(g) = 1$. This occurs for $k+1 = 2^t$, i.e. for $g = 2^{2^t-1}$. Thus in this case, we have

$$1 = N_2(g) < N_2(g-1) + N_2(g-2).$$

(This says nothing about the conjecture of Bras-Amorós.)

Case $g = p^k$ with p odd prime

From now on, let p be an odd prime and $g = p^k$. The list of factorizations of $2g$ is: $p^i \cdot 2p^{k-i}$, $0 \le i \le k$.

We shall see that determining $N_2(p^k)$ is

- very hard for k large,
- more manageable for k small.

* * *

- k large: consider $k = 4097 = 2^{12} + 1$.

Claim. Determining $N_2(p^{4097})$ for all p requires the (unknown!) factorization of the 12th Fermat number

$$F_{12} = 2^{2^{12}} + 1.$$

Proof. $N_2(p^k) =$ the number of special factorizations of $2p^k$, i.e. number of $i \in \{0, \ldots, k\}$ such that

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

Let $i = k - 1$. **Claim:** in $\mathbb{Z}[2^{-1}]$, we have

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

For $k = 2^t + 1$, this gives

$$\gcd(p^{2^t} + 1, 2p + 1) \;=\; \gcd(2^{2^t} + 1, 2p + 1).$$

Thus, as long as the factors of $2^{2^t} + 1$ remain unknown, there can be no general formula in p revealing when this gcd equals 1. $\square$

$k = 1, 2, 3$

Proposition 4. *Let p be an odd prime. We have:*

- $N_2(p) = \begin{cases} 2 & \text{if } p \not\equiv 2 \bmod 3, \\ 1 & \text{else} \end{cases}$
- $N_2(p^2) = 3$,
- $N_2(p^3) = \begin{cases} 1 & \text{if} \quad \rho_{3,5}(p) = (2, 2) \\ 2 & \text{if} \quad \rho_{3,5}(p) = (2, \neg 2) \\ 3 & \text{if} \quad \rho_{3,5}(p) = (\neg 2, 2) \\ 4 & \text{if} \quad \rho_{3,5}(p) = (\neg 2, \neg 2), \end{cases}$

where $\rho_{3,5} : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ is the bireduction map, and where $\neg 2$ means $\neq 2$. Note: $N_2(p^3)$ is determined by the class of p mod 15.

$k = 4, 5$

Proposition 5. *We have:*

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

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

Note: $N_2(p^5)$ is determined by the class of p mod 255.

$$6 \leq k \leq 10$$

Proposition 6. *The value of $N_2(p^k)$ is determined by the class of p mod*

$$\begin{cases} 31 & \text{for } k = 6, \\ 36465 & \text{for } k = 7, \\ 27559 & \text{for } k = 8, \\ 30998055 & \text{for } k = 9, \\ 1103249 & \text{for } k = 10. \end{cases}$$

Is there any general statement?

The main result

Let

$$M(k) \;=\; \mathrm{rad}\Big(\prod_{i=1}^{k}\Big(2^{i/\gcd(i,k)} - (-1)^{k/\gcd(i,k)}\Big)\Big),$$

where rad(n) = largest square-free divisor of n.

Theorem 7. *For all $k \geq 1$, the value of $N_2(p^k)$ is determined by the class of p mod $M(k)$.*

The main technical tool is a reduction of

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

to a simpler form:

Proposition 8. *Let $\alpha, \beta \in \mathbb{N}$. Then there exists $\rho \in \mathbb{Z}$ such that*

$$\gcd(p^\alpha + 1, 2p^\beta + 1) = \gcd(p^{\gcd(\alpha,\beta)} \pm 2^\rho, cte),$$

in the UFD ring $\mathbb{Z}[2^{-1}]$, where $cte = 2^{\alpha/\delta} - (-1)^{(\alpha-\beta)/\delta}$.

Proof. Involved, and involves the continued fraction expansion of α/β. □

The building blocks $X_{a,q}$

Let $a, q \in \mathbb{N}$ with q prime. We define

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

by

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

If q is not prime, let $q_1, \ldots, q_t$ be its distinct prime factors. Then we set

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

$k = 9, 10$

Theorem 9. *Let p be an odd prime. Then*

$$\begin{aligned} N_2(p^9) = \quad & 1 + 2X_{3,5}(p) + X_{9,17}(p) + X_{128,257}(p) \\ & + X_{2,3}(p) \cdot (3 + X_{2,11}(p) + X_{8,43}(p)). \end{aligned}$$

$$\begin{aligned} N_2(p^{10}) = \quad & 7 + X_{3,7}(p) \cdot (1 + X_{36,73}(p)) \\ & + X_{5,17}(p) X_{12,17}(p) + X_{123,127}(p). \end{aligned}$$

In particular, $N_2(p^k)$ is determined by the class of p mod

- $5 \cdot 17 \cdot 257 \cdot 3 \cdot 11 \cdot 43$ for $k = 9$,
- $7 \cdot 73 \cdot 17 \cdot 127$ for $k = 10$.

- S.E. & J.R.A, Two-generator numerical semigroups and Fermat and Mersenne numbers, SIAM J. Discrete Math. 25 (2011) 622–630.

- S.E. & J.R.A, On the number of numerical semigroups $\langle a, b \rangle$ of prime power genus, submitted.

Thank you.