J.L. Ramírez Alfonsín and M. Skałba

**Primes in numerical semigroups**


<https://doi.org/10.5802/crmath.104>
Primes in numerical semigroups

J.L. Ramírez Alfonsín*<sup>a</sup> and M. Skałba<sup>b</sup>

<sup>a</sup> UMI2924 - Jean-Christophe Yoccoz, CNRS-IMPA, Brazil and Univ. Montpellier, CNRS, Montpellier, France
<sup>b</sup> Institute of Mathematics, University of Warsaw, Banacha 2, 02-097 Warszawa, Poland

E-mails: jorge.ramirez-alfonsin@umontpellier.fr (J.L. Ramírez Alfonsín), skalba@mimuw.edu.pl (M. Skałba)

Abstract. Let 0 < a < b be two relatively prime integers and let ⟨a, b⟩ be the numerical semigroup generated by a and b with Frobenius number g(a, b) = ab − a − b. In this note, we prove that there exists a prime number p ∈ ⟨a, b⟩ with p < g(a, b) when the product ab is sufficiently large. Two related conjectures are posed and discussed as well.

2020 Mathematics Subject Classification. 11D07, 11N13.

Funding. J.L. Ramírez Alfonsín was partially supported by Grant MATHAM-SUD 18-MATH-01, Project FLaNASAGraTA and INSMI-CNRS.

Manuscript received 22nd July 2020, revised and accepted 30th July 2020.

Let 0 < a < b be two relatively prime integers. Let S = ⟨a, b⟩ = {n | n = ax + by, x, y ∈ Z, x, y ≥ 0} be the numerical semigroup generated by a and b. A well-known result due to Sylvester [5] states that the largest integer not belonging to S, denoted by g(a, b), is given by ab − a − b. g(a, b) is called the Frobenius number (we refer the reader to [3] for an extensive literature on the Frobenius number).

We clearly have that any prime p larger than g(a, b) belongs to ⟨a, b⟩. A less obvious and more intriguing question is whether there is a prime p ∈ ⟨a, b⟩ with p < g(a, b) when the product ab is sufficiently large. The latter is a straightforward consequence of the below Theorem.

Let 0 < u < v be integers. We define

\[ \pi_S[u, v] = |\{p \text{ prime} \mid p \in S, u \leq p \leq v\}|. \]

For short, we may write \( \pi_S \) instead of \( \pi_S[0, g(a, b)] \).

**Theorem 1.** Let 3 ≤ a < b be two relatively prime integers and let S = ⟨a, b⟩ be the numerical semigroup generated by a and b. Then, for any fixed \( \varepsilon > 0 \) there exists \( C(\varepsilon) > 0 \) such that

\[ \pi_S > C(\varepsilon) \frac{g(a, b)}{\log(g(a, b))^{2+\varepsilon}} \]
for \(ab\) sufficiently large.

Let us quickly introduce some notation and recall some facts needed for the proof of Theorem 1.

Let \(S = \langle a, b \rangle\) and let \(0 < u < v\) be integers. We define

\[ n_S[u, v] = |\{ n \in \mathbb{N} | u \leq n \leq v, n \in S \}| \]

and

\[ n_S^c[u, v] = |\{ n \in \mathbb{N} | u \leq n \leq v, n \not\in S \}|. \]

For short, we may write \(n_S\) instead of \(n_S[0, g(a, b)]\) and \(n_S^c\) instead of \(n_S^c[0, g(a, b)]\). The set of elements in \(n_S^c = \mathbb{N} \setminus S\) are usually called the gaps of \(S\).

It is known [3] that \(S\) is always symmetric, that is, for any integer \(0 \leq s \leq g(a, b)\)

\[ s \in S \text{ if and only if } g(a, b) - s \not\in S. \]

It follows that

\[ n_S = \frac{g(a, b) + 1}{2}. \]

We may now prove Theorem 1.

**Proof of Theorem 1.** Let \(\varepsilon > 0\) be fixed. We distinguish two cases.

**Case 1.** Suppose that \(a > (\log(ab))^{1+\varepsilon}\). Let us take \(c = ab/(\log(ab))^{1+\varepsilon}\). It is known [1] that if \(k \in [0, \ldots, g(a, b)]\) then

\[ n_S[0, k] = \sum_{i=0}^{\left\lfloor \frac{k}{ab} \right\rfloor} \left( \left\lfloor \frac{k - ib}{a} \right\rfloor + 1 \right). \]

In our case, we obtain that

\[
\begin{align*}
    n_S[0, c] &\leq \left\lfloor \frac{c}{a} \right\rfloor + \left\lfloor \frac{c}{b} \right\rfloor + \left\lfloor \frac{c - b}{a} \right\rfloor + 1 + 1 \\
    &\leq \left\lfloor \frac{c}{a} \right\rfloor + \left\lfloor \frac{c}{b} \right\rfloor + \left\lfloor \frac{c}{a} \right\rfloor + 1 + 1 \\
    &\leq \frac{c}{a} + \frac{c}{b} + \frac{c^2}{ab} + 1 = \frac{bc + ac + c^2 + ab}{ab} < \frac{2c^2 + c^2 + c^2}{ab} = \frac{4c^2}{ab} = \frac{4ab}{(\log(ab))^{2+2\varepsilon}}
\end{align*}
\]

where the last inequality holds since \(c > b > a\).

Due to the symmetry of \(S\), we have

\[
    n_S^c[g(a, b) - c, g(a, b)] = n_S[0, c] < \frac{4ab}{(\log(ab))^{2+2\varepsilon}}.
\]

Let \(\pi(x)\) be the number of primes integers less or equals to \(x\). We have

\[
    \pi(g(a, b)) - \pi(g(a, b) - c) \gg \frac{c}{\log(ab)} = \frac{ab}{(\log(ab))^{2+2\varepsilon}}
\]

when \(ab\) is large enough. The latter follows from Prime Number Theorem for short intervals (when \(c = ab/(\log(ab))^{1+\varepsilon}\) is large enough in comparison to \(g(a, b) = ab - a - b\).

Finally, by combining equations (1) and (2), we obtain

\[
    \pi_S \geq \pi_S[g(a, b) - c, g(a, b)] \geq \pi(g(a, b)) - \pi(g(a, b) - c) - n_S^c[g(a, b) - c, g(a, b)]
\]

\[
    \gg \frac{ab}{(\log(ab))^{2+2\varepsilon}} - \frac{4ab}{(\log(ab))^{2+2\varepsilon}} > 0
\]

where the last inequality holds since \((\log(ab))^{\varepsilon} > 4\) for \(ab\) large enough for the fixed \(\varepsilon\). The above leads to the desired estimate of \(\pi_S\).
Case 2. Suppose that $3 \leq a \leq (\log(ab))^{1+\varepsilon}$.

If $p \in [b, \ldots, g(a, b)]$ is a prime and $p \equiv b \pmod{a}$ then $p$ is clearly representable as $p = b + \frac{p-b}{a}a$. By Siegel–Walfisz theorem [2, 7], the number of such primes $p$, denoted by $N$, is

$$N = \frac{1}{\varphi(a)} \int_{b}^{g(a, b)} \frac{du}{\log u} + R$$

where $\varphi$ is the Euler totient function and $|R| < D'(\varepsilon) \frac{g(a, b)}{\log(g(a, b))^{2+2\varepsilon}}$ uniformly in $a$ and $g(a, b)$.

Since the function $1/\log u$ is decreasing on the interval $[b, g(a, b)]$ then

$$\int_{b}^{g(a, b)} \frac{du}{\log u} > (g(a, b) - b) \cdot \frac{1}{\log g(a, b)}$$

and therefore

$$N > \frac{1}{\varphi(a)} \cdot \frac{g(a, b) - b}{\log(g(a, b))} - D'(\varepsilon) \frac{g(a, b)}{(\log(g(a, b)))^{2+2\varepsilon}}.$$  \hspace{1cm} (3)

Now, we have that

$$\frac{1}{\varphi(a)} \cdot \frac{g(a, b) - b}{\log(g(a, b))} = \frac{1}{\varphi(a)} \log(g(a, b))^{1+\varepsilon} \left(1 - \frac{b}{g(a, b)}\right)$$

$$> \frac{1}{\log(ab)^{1+\varepsilon}} \log(g(a, b))^{1+\varepsilon} \left(1 - \frac{b}{g(a, b)}\right) \quad \text{(since}(\log(ab))^{1+\varepsilon} \geq a > \varphi(a))$$

$$> \left(\frac{\log(ab) - \log(3)}{\log(ab)}\right)^{1+\varepsilon} \frac{1}{5} > F > 0 \quad \text{since} \ g(a, b) > ab/3 \quad \text{and} \quad \frac{b}{g(a, b)} \leq \frac{4}{5}$$

for some absolute $F > 0$, uniformly for $ab \geq D''(\varepsilon)$ with $a \geq 3$. It yields to

$$\frac{1}{\varphi(a)} \cdot \frac{g(a, b) - b}{\log(g(a, b))} \geq F \frac{g(a, b)}{(\log(g(a, b)))^{2+\varepsilon}}$$  \hspace{1cm} (4)

and combining equations (3) and (4) we obtain

$$N > F \frac{g(a, b)}{(\log(g(a, b)))^{2+\varepsilon}}$$

for $ab$ large enough for the fixed $\varepsilon$. The latter leads to the desired estimate of $\pi_S$ also in this case.

\[\square\]

1. Concluding remarks

A number of computer experiments lead us to the following.

Conjecture 2. Let $2 \leq a < b$ be two relatively prime integers and let $S$ be the numerical semigroup generated by $a$ and $b$. Then,

$$\pi_S > 0.$$
Conjecture 3. Let $2 \leq a < b$ be two relatively prime integers and let $S$ be the numerical semigroup generated by $a$ and $b$. Then,

$$
\pi_S \sim \frac{\pi(g(a, b))}{2} \text{ for } a \to \infty.
$$

In the same spirit as the prime number theorem, this conjecture seems to be out of reach. The famous Linnik's theorem asserts that there exist absolute constants $C$ and $L$ such that: for given relatively prime integers $a, b$ the least prime $p$ satisfying $p \equiv b \pmod{a}$ is less than $Ca^L$. It is conjectured that one can take $L = 2$, but the current record is only that $L \leq 5$ is allowed, see [8].

On the same flavor of Linnik's theorem that concerns the existence of primes of the form $ax + b$, Theorem 1 is concerning the existence of primes of the form $ax + by$ with $x, y \geq 1$ less than $ab$ for sufficiently large $ab$. This relation could shed light on in either direction.

References