PRIMES IN NUMERICAL SEMIGROUPS

J.L. RAMÍREZ ALFONSÍN[1] AND M. SKAŁBA

ABSTRACT. Let $0 < a < b$ be two relatively prime integers and let $\langle a, b\rangle$ 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 $p \in \langle a, b\rangle$ with $p < g(a, b)$ when the product ab is sufficiently large. Two related conjectures are posed and discussed as well.

Let $0 < a < b$ be two relatively prime integers. Let $S = \langle a, b\rangle = \{n \mid n = ax + by, x, y \in \mathbb{Z}, x, y \geq 0\}$ 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 $\langle a, b\rangle$. A less obvious and more intriguing question is whether there is a prime $p \leq g(a, b)$ belonging to $\langle a, b\rangle$.

In this note, we show that there always exists a prime $p \in \langle a, b\rangle, p < g(a, b)$ when the product ab is sufficiently large. The latter is a straight forward 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 π_S instead of $\pi_S[0, g(a, b)]$.

Theorem 1. *Let $3 \leq a < b$ be two relatively prime integers and let $S = \langle a, b\rangle$ 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.

2010 *Mathematics Subject Classification.* Primary 11D07, 11N13.

Key words and phrases. Primes, numerical semigroups, Frobenius number.

[1] Partially supported by Program MATH AmSud, Grant MATHAMSUD 18-MATH-01, Project FLaNASAGraTA.

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

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

and

$$n_S^c[u,v] = |\{n \in \mathbb{N} \mid u \le n \le v,\ n \notin S\}|.$$

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 $0 \le s \le g(a,b)$

$$s \in S \text{ if and only if } g(a,b) - s \notin S.$$

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

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

In our case, we obtain that

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

where the last inequality holds since $c > b > a$.

Due to the symmetry of S, we have

$$n_S^c[g(a,b) - c, g(a,b)] = n_S[0,c] < \frac{4ab}{(\log(ab))^{2+2\varepsilon}}. \tag{1}$$

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

$$\pi(g(a,b)) - \pi(g(a,b) - c) >> \frac{c}{\log(ab)} = \frac{ab}{(\log(ab))^{2+\varepsilon}} \tag{2}$$

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

$$\pi_S \geq \pi_S[g(a,b)-c, g(a,b)] \geq \pi(g(a,b)) - \pi(g(a,b)-c) - n_S^c[g(a,b)-c, g(a,b)]$$
$$> \frac{ab}{(\log(ab))^{2+\varepsilon}} - \frac{4ab}{(\log(ab))^{2+2\varepsilon}} > 0$$

where the last inequality holds since $(\log(ab))^\varepsilon > 4$ for ab large enough for the fixed ϵ. The above leads to the desired estimate of π_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 φ is the *Euler totient function* and $|R| < D'(\varepsilon)\frac{g(a,b)}{(\log(g(a,b)))^{2+2\varepsilon}}$ uniformly in $[a, \ldots, g(a,b)]$.

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

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

Now, we have that

$\frac{1}{\varphi(a)} \cdot \frac{g(a,b)-b}{\log(g(a,b))} \cdot \frac{(\log(g(a,b)))^{2+\varepsilon}}{g(a,b)}$
$= \frac{1}{\varphi(a)} \log(g(a,b))^{1+\varepsilon}\left(1 - \frac{b}{g(a,b)}\right)$
$> \frac{1}{\log(ab)^{1+\varepsilon}} \log(g(a,b))^{1+\varepsilon}\left(1 - \frac{b}{g(a,b)}\right)$ (since $(\log(ab))^{1+\varepsilon} \geq a > \varphi(a)$)
$> \left(\frac{\log(ab)-\log(3)}{\log(ab)}\right)^{1+\varepsilon} \frac{1}{5} > F > 0$ (since $g(a,b)) > ab/3$ and $\frac{b}{g(a,b)} \leq \frac{4}{5}$)

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

It yields to

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

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 ϵ. The latter leads to the desired estimate of π_S also in this case. □

1. Concluding remarks

A number of computer experiments lead us to the following.

Conjecture 1. *Let $2 \le a < b$ be two relatively prime integers and let S be the numerical semigroup generated by a and b. Then,*

$$\pi_S > 0.$$

In analogy with the symmetry of $\langle a, b\rangle$ mentioned above, our task of looking for primes in $\langle a, b\rangle$ is related with the task of finding primes in $[g(a,b)-1)/2, \dots, g(a,b)]$. From this point of view, Conjecture 1 can be thought of as a counterpart of the famous Chebyshev theorem stating that there is always a prime in $[n, \dots, , 2n]$ for any $n \ge 2$, see [4, Chapter 3]. A way to attack Conjecture 1 could be by applying *effective versions* of Siegel-Walfisz theorem. For instance, one may try to use [6, Corollary 8.31] in order to get computable constants in our estimates. However, it is not an easy task to trace all constants appearing in the relevant estimates of $L(x, \chi)$ (but in principle possible). The remaining cases for *small* values ab must to be treated by computer.

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

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

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 $L \le 5$ 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 $x, y \ge 1$ less than ab for sufficiently large ab. This relation could shed light on in either direction.

References

[1] G. Márquez-Campos, J.L. Ramírez Alfonsín, J.M. Tornero, Integral points in rational polygons: a numerical semigroup approach, *Semigroup Forum* **94**(1) (2017), 123-138.

[2] K. Prachar, Primzahlverteilung, Die Grundlehren der Mathematischen Wissenschaften XCI, Springer-Verlag 1957.

[3] J.L. Ramírez Alfonsín, The Diophantine Frobenius Problem, Oxford Lecture Ser. in Math. and its Appl. 30, Oxford University Press 2005.

[4] W. Sierpinski, Elementary Theory of Numbers, Second Ed., PWN-Polish Scientific Publisher and North-Holland 1988,

[5] J.J. Sylvester *Question 7382*, Mathematical Questions from Educational Times 41, 1884.

[6] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, Third Edition, Graduate Studies in Mathematics 163, AMS 2015.

[7] A. Walfisz, Zur additiven Zahlentheorie. II *Mathematische Zeitschrift* **40**(1) (1936) 592-607.

[8] T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, Dissertation, Bonn 2011.

IMAG, Univ. Montpellier, CNRS, Montpellier, France and UMI2924 - Jean-Christophe Yoccoz, CNRS-IMPA

Email address: jorge.ramirez-alfonsin@umontpellier.fr

Institute of Mathematics, University of Warsaw, Banacha 2, 02-097 Warszawa, Poland

Email address: skalba@mimuw.edu.pl