A NOTE ON INTEGER POLYNOMIALS WITH SMALL INTEGRALS

DANILO BAZZANELLA

Abstract. The smart method of Gelfond–Shnirelman–Nair allows to obtain in elementary way a lower bound for the prime counting function $\pi(x)$ in terms of integrals of suitable integer polynomials. In this paper we studied the properties of the class of integer polynomials relevant for the method.

This is the authors' post-print version of an article published on *Acta Math. Hungar.* (2013), DOI:10.1007/s10474-013-0326-8.[1]

1. INTRODUCTION

Let $\pi(x)$ be the number of primes not exceeding x. The Prime Number Theorem (PNT), independently proved in 1896 by Hadamard and the de la Vallée Poussin, states that

$$\pi(N) \sim \frac{N}{\log N} \qquad N \to +\infty.$$

In 1851, Chebyshev [6] made the first step towards the PNT by proving that, given $\varepsilon > 0$,

$$(c_1 - \varepsilon)\frac{N}{\log N} \le \pi(N) \le (c_2 + \varepsilon)\frac{N}{\log N}$$

where $c_1 = \log(2^{1/2}3^{1/3}5^{1/5}/30^{1/30})$, $c_2 = 6c_1/5$ and N is sufficiently large. This result was proved using an elementary approaches, i.e. without use of complex analysis and the Riemann zeta function. A survey of elementary methods in the study of the distribution of prime numbers may be found in Diamond [7].

In 1936 Gelfond and Shnirelman, see Gelfond's editorial remarks in the 1944 edition of Chebyshev's Collected Works [6, pag. 287–288], proposed a new elementary and clever method for deriving a lower bound for the prime-counting functions $\pi(x)$ and $\psi(x)$. In 1982 the Gelfond-Shnirelman method was rediscovered and developed by Nair, see [9] and [10]. The method of Gelfond–Shnirelman–Nair allows to obtain in elementary way a lower bound for $\pi(x)$ in terms of integrals of suitable integer polynomials and runs as follows.

2010 *Mathematics Subject Classification.* 11C08, 11A41.
Key words and phrases. Integer polynomials, Chebyshev problem, Prime counting function.

Let d_N denote the least common multiple of the integers $1, 2, \ldots, N$ and observe that

$$d_N \leq \prod_{p \leq N} p^{\log N / \log p},$$

where p belongs to the set of prime numbers. Taking the logarithm of both sides gives

$$\log d_N \leq \log \left(\prod_{p \leq N} p^{\log N / \log p} \right) = \sum_{p \leq N} \log \left(p^{\log N / \log p} \right) = \pi(N) \log N$$

and then

$$\pi(N) \geq \frac{\log d_N}{\log N}. \tag{1}$$

From this we can obtain a lower bound for the prime counting function $\pi(N)$ from a lower bound for the least common multiple d_N. An elementary and smart way to proceed is to consider a polynomial with integral coefficients

$$P(x) = \sum_{n=0}^{N-1} a_n x^n$$

and let

$$I(P) = \int_0^1 P(x)\,\mathrm{d}x = \sum_{n=0}^{N-1} \frac{a_n}{n+1}.$$

Since $I(P)$ is a rational number whose denominator divides d_N, we see that $I(P)d_N$ is an integer, and hence if $I(P) \neq 0$ we have

$$d_N |I(P)| \geq 1$$

and then

$$d_N \geq \frac{1}{|I(P)|}.$$

Form the above and (1) we get

$$\pi(N) \geq \frac{\log(1/|I(P)|)}{\log N}. \tag{2}$$

The easiest way to proceed is to bound the absolute value of the integral $I(P)$

$$|I(P)| = \left| \int_0^1 P(x)\,\mathrm{d}x \right| \leq \int_0^1 |P(x)|\,\mathrm{d}x \tag{3}$$

and

$$\int_0^1 |P(x)|\,\mathrm{d}x \leq \max_{0 \leq x \leq 1} |P(x)| = ||P||_{[0,1]}, \tag{4}$$

obtaining

$$\pi(N) \geq \frac{\log\left(1/||P||_{[0,1]}\right)}{\log N}.$$

If we could find a sequence of integer polynomials p_n, of degree n, with sufficiently small supremum norms such that

$$\lim_{n\to+\infty}\log\left(||p_n||_{[0,1]}^{-1/n}\right)=\lim_{n\to+\infty}-\frac{1}{n}\log||p_n||_{[0,1]}=1,$$

we can obtain the best possible lower bound consistent with the Prime Number Theorem.

This motivates the study of the integer polynomials $P_N(x)$ and the quantities C_N such that

$$||P_N||_{[0,1]}=\min_{\substack{P(x)\in\mathbb{Z}[x]\\ \deg(P)=N,||P||_{[0,1]}>0}}||P||_{[0,1]}$$

and

$$C_N=-\frac{1}{N}\log||P_N||_{[0,1]},$$

the so-called integer Chebyshev problem. Much is known about $P_N(x)$ and C_N. It was proved by Snirelman, see [11], that the sequence C_N converges to a limit C. Borwein and Erdélyi [5] showed that $C\in(0.85866,0.86577)$ and the lower bound was improved by Flammang [8] to 0.85912. The best known result to date, due to Pritsker [12], is that $C\in(0.85991,0.86441)$. See also [1], [2], [3], [4], [5] and [14].

Therefore, following this line, we can get a lower bound in the form

$$\pi(N)\geq C\,\frac{N}{\log N},$$

only for constant C less than 0.87, which is quite far from what is expected by the PNT.

In order to avoid the trouble above, in this paper we deal with the problem in a different way. From the definition of $I(P)$ we have that

$$|I(P)|=\left|\int_0^1 P(x)\,\mathrm{d}x\right|=\left|\sum_{n=0}^{N-1}\frac{a_n}{n+1}\right|=\frac{1}{d_N}\left|\sum_{n=0}^{N-1}\frac{d_N}{n+1}a_n\right|.$$

Since $d_N/(n+1)$ and a_n are integers for every $n=0,1,\dots N_1$, we have that

$$\left|\sum_{n=0}^{N-1}\frac{d_N}{n+1}a_n\right|$$

is an integer and then the small positive value of $|I(P)|$ is $1/d_N$ and it is reached if

$$\sum_{n=0}^{N-1}\frac{d_N}{n+1}a_n=\pm1.$$

Without loss of generality we can deal with the linear diophantine equation

$$\sum_{n=0}^{N-1}\frac{d_N}{n+1}x_n=1$$

with integer coefficients $d_N/(n+1)$. Observing that the integer coefficients $d_N,d_N/2,\dots,d_N/N$ are relatively prime, we obtain that for every N there exists at least one polynomial of degree $N-1$ such that $I(P)=1/d_N$. Note that the set of the integer polynomials of fixed degree with integral on $[0,1]$ equal to zero is a vector space and then the set of the integer polynomials of fixed degree with integrals on $[0,1]$ equal to a constant is an affine space. This leads to define the following affine space of the polynomials with positive and minimal integral on $[0,1]$.

Definition. *Let* $S_N = \{P(x) \in \mathbb{Z}[x], \deg(P) = N-1, I(P) = 1/d_N\}$

In this paper we studied the properties of such a class of integer polynomials.

Acknowledgement. We would like to thank Professors E. Serra and P. Tilli for the long conversations we had on this subject.

2. Some properties of the set S_N

In the set S_N there are integer polynomials with many of the first coefficients equal to zero, and then with $x=0$ as a root of great degree.

Theorem 1. *For every N, there exists an integer polynomial*

$$P(x) = \sum_{n=K(N)}^{N-1} a_n x^n \in S_N$$

with

$$K(N) \sim \frac{N}{2}.$$

Proof. As usual, $(a_1, a_2, ..., a_j)$ denotes the greatest common divisor of the integers $a_1, a_2 \ldots, a_j$. We start to observe that if we have

$$\left(\frac{d_N}{k}, \frac{d_N}{k+1}, \ldots, \frac{d_N}{N}\right) = 1,$$

for a fixed natural k, it follows that

$$\left(\frac{d_N}{i}, \frac{d_N}{i+1}, \ldots, \frac{d_N}{N}\right) = 1,$$

for every $1 \le i \le k$ and for the same reason if we have

$$\left(\frac{d_N}{k}, \frac{d_N}{k+1}, \ldots, \frac{d_N}{N}\right) > 1,$$

for a fixed natural k, it follows that

$$\left(\frac{d_N}{i}, \frac{d_N}{i+1}, \ldots, \frac{d_N}{N}\right) > 1,$$

for every $k \le i \le N$. This allows to define $K(N)$ as the natural number such that

$$\left(\frac{d_N}{K(N)+1}, \frac{d_N}{K(N)+2}, \ldots, \frac{d_N}{N}\right) = 1 \tag{5}$$

and

$$\left(\frac{d_N}{K(N)+2}, \frac{d_N}{K(N)+3}, \dots, \frac{d_N}{N}\right) > 1. \tag{6}$$

From (5) it follows that the linear diophantine equation

$$\sum_{n=K(N)}^{N-1} \frac{d_N}{n+1} x_n = 1$$

has solutions and this implies that there exists an integer polynomial

$$P(x) = \sum_{n=K(N)}^{N-1} a_n x^n \in S_N.$$

Now we prove that

$$K(N) = \min\left\{p^m : p \text{ prime }, m \geq 1, p^m > N/2\right\} - 1 \tag{7}$$

Let $q = p^m$ such that $N/2 < q = p^m < N$. $q \leq N$ implies q/d_N and then

$$\left(\frac{d_N}{q+1}, \frac{d_N}{q+2}, \dots, \frac{d_N}{N}\right) \geq p,$$

since every natural number between $q+1$ and N has strictly less then m factors p in his prime decomposition. This prove

$$K(N) \leq \min\left\{p^m : p \text{ prime }, m \geq 1, p^m > N/2\right\} - 1. \tag{8}$$

On the other hand, by the definition of $K(N)$, we have

$$\left(\frac{d_N}{K(N)+2}, \frac{d_N}{K(N)+3}, \dots, \frac{d_N}{N}\right) > 1$$

which implies that there exists a prime number p such that

$$p \Big| \frac{d_N}{K(N)+2}, p \Big| \frac{d_N}{K(N)+3}, \dots, p \Big| \frac{d_N}{N}.$$

Let $m = \max\{i : p^i | d_N\}$ and therefore $p^m \leq N$. From this follows

$$p^m \not| (K(N)+2), p^m \not| (K(N)+3), \dots, p^m \not| N$$

and then

$$K(N) \geq \min\left\{p^m : p \text{ prime }, m \geq 1, p^m > N/2\right\} - 1. \tag{9}$$

From (8) and (9) it follows (7). Now the difference between $K(N)$ and $N/2$ can be bound by the maximum of the difference between consecutive elements of the set $\{p^m \leq N : p \text{ prime }, m \geq 1\}$, which is less than the maximum of the difference between consecutive primes less than N. This allow to write

$$K(N) = \frac{N}{2} + O(N^{7/12+\varepsilon}),$$

for every $\varepsilon > 0$, which concludes the proof of the theorem. □

Corollary 2. *For every N, there exists an integer polynomial $P(x) \in S_N$ with $x = 1$ as a root of degree $K(N)$ and*

$$K(N) \sim \frac{N}{2}.$$

Proof. The corollary follows immediately from the Theorem 1, observing that the change of variable $x \to (1 - x)$ don't change the absolute value of the integral $I(P)$. □

The second result is about the number of roots and the number of changes of sign of the integer polynomials in S_N.

Theorem 3. *For all even N, there exists an integer polynomial $P(x) \in S_N$ with $N - 1$ roots on $(0, 1)$ and $N - 1$ changes of sign.*

Proof. Let N even number and $R(x) = (Nx - 1)(Nx - 2) \cdots (Nx - (N - 1))$. $R(x)$ is a polynomial with integer coefficients of degree $N - 1$, has $N - 1$ roots on $(0, 1)$, $(N - 2)/2$ local maxima, $(N - 2)/2$ local minima and

$$I(R) = \int_0^1 R(x)\,\mathrm{d}x = 0,$$

since the symmetry of the function. Let $P(x)$ a fixed polynomial in $S_N, k \in \mathbb{Z}$ and $Q_k(x) = P(x) + kR(x)$. For every $k \in \mathbb{Z}$ we have $I(Q_k) = I(P) = 1/d_N$ and then $Q_k(x) \in S_N$. For every N there exists a constant k such that $Q_k(x)$ has $N - 1$ roots on $(0, 1)$ and $N - 1$ changes of sign. □

Corollary 4. *For every N, there exists an integer polynomial $P(x) \in S_N$ with at least $N - 2$ roots on $(0, 1)$ and $N - 2$ changes of sign.*

On the other side we can prove that in the set S_N there are also integer polynomials with at most one root and one change of sign.

Theorem 5. *For every N, there exists an integer polynomial $P(x) \in S_N$ with at most one root on $(0, 1)$ and at most one change of sign on $(0, 1)$.*

Proof. Let $P(x)$ a fixed polynomial in $S_N, k \in \mathbb{Z}$ and $Q_k(x) = P(x) + k(2x - 1)$. For every $k \in \mathbb{Z}$ we have $I(Q_k) = I(P) = 1/d_N$ and then $Q_k(x) \in S_N$. Now we observe that $Q_k(0) = P(0) - k$, $Q_k(1) = P(1) + k$ and $Q'_k(x) = P'(x) + 2k$ for every $x \in [0, 1]$.

For every N there exists a constant k such that $Q_k(0) < 0$, $Q_k(1) > 0$ and $Q'_k(x) > 0$ for every $x \in [0, 1]$ and this implies that the polynomial $Q_k(x)$ has exactly one root and one change of sign on $(0, 1)$. □

3. Open problem

In the standard method of Gelfond–Shnirelman–Nair we bound the absolute value of the integral

$$|I(P)| = \left| \int_0^1 P(x)\,\mathrm{d}x \right| \le \int_0^1 |P(x)|\,\mathrm{d}x \qquad (10)$$

and then

$$\int_0^1 |P(x)|\,\mathrm{d}x \le \max_{0\le x\le 1} |P(x)| = ||P||_{[0,1]}, \tag{11}$$

to obtain

$$\pi(N) \ge \frac{\log\left(1/||P||_{[0,1]}\right)}{\log N}.$$

As observed in the introduction, following this line we can get a lower bound in the form

$$\pi(N) \ge C\ \frac{N}{\log N},$$

only for constant C much less than 1. It is not clear if this is only a consequence of the use of supremum norm on the interval $[0,1]$ in (11) or if the inequality (10) is also involved.

If the set S_N contains polynomials of constant sign in $(0,1)$ for all N, or at least for infinite values of N, the limit of the method would be only due to the inequality (11).

It is simple to verify that for very small values of N these positive polynomials exist. For S_3, $\deg(P) = 2$ and $d_3 = 6$, we have the positive polynomial $P(x) = x(1-x)$ and for S_4, $\deg(P) = 3$ and $d_3 = 12$, we have the positive polynomial $P(x) = x^2(1-x)$. For S_N with greater values of N is not simple to determine what happens, and this leads to the following question.

Problem: for every N, or at least for infinite values of N, there exists an integer polynomial $P(x) \in S_N$ such that $P(x) \ge 0$?

References

[1] F. Amoroso, *Sur le diamètre transfini entier dun intervalle réel*, Ann. Inst. Fourier (Grenoble) **40** (1990), no. 4, 885–911.

[2] B. E. Aparicio, *On the asymptotic structure of the polynomials of minimal Diophantic deviation from zero*, J. Approx. Theory **55** (1988), no. 3, 270–278.

[3] P. B. Borwein, T. Erdélyi, *Polynomials and polynomial inequalities*, Graduate Texts in Mathematics **161**, Springer-Verlag, New York, 1995.

[4] P. B. Borwein, I. E. Pritsker, *The multivariate integer Chebyshev problem*, Constr. Approx. **30** (2009), no. 2, 299–310.

[5] P. B. Borwein, T. Erdélyi, *The integer Chebyshev problem*, Math. Comp. **65** (1996), no. 214, 661–681.

[6] P. L. Chebyshev, *Collected Works, Vol. 1, Theory of Numbers*, Akad. Nauk. SSSR, Moskow,1944.

[7] H. G. Diamond, *Elementary methods in the study of the distribution of prime numbers*, Bull. Amer. Math. Soc. **7** (1982), 553–589.

[8] V. Flammang, *Sur le diamètre transfini entier d'un intervalle à extrémités rationnelles*, Annales de l'Institut Fourier **45** (1995), no. 3, 779–793.

[9] M. Nair, *On Chebyshev's-type inequalities for primes*, Amer. Math. Montly **89** (1982), 126–129.

[10] M. Nair, *A new method in elementary prime number theory*, J. London Math. Soc. (2) **25** (1982), 385–391.

[11] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, AMS, CBMS Series No. **84**, 1994.

[12] I. E. Pritsker, *Small polynomials with integer coefficients*, J. Anal. Math., **96** (2005), pp. 151–190.

[13] I. E. Pritsker, *The Gelfond-Schnirelman method in prime number theory*, Canad. J. Math. **57** (2005), no. 5, 1080–1101.

[14] I. E. Pritsker, *Distribution of primes and a weighted energy problem*, Electron. Trans. Numer. Anal. **25** (2006), 259–277.

Dipartimento di Scienze Matematiche, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino — Italy
E-mail address: danilo.bazzanella@polito.it