A note on integer polynomials with small integrals. II

(Article begins on next page)

A NOTE ON INTEGER POLYNOMIALS WITH SMALL INTEGRALS II

DANILO BAZZANELLA

Abstract. The smart method of Gelfond–Shnirelman–Nair allows one 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 carry on the study of the properties of the sets of integer polynomials relevant for the method.

This is the authors' post-print version of an article published on *Acta Math. Hungar.* (2016), DOI:10.1007/s10474-016-0600-7.[1]

1. introduction

In 1851, Chebyshev [7] made the first step towards the Prime Number Theorem by proving that, given $\varepsilon > 0$,

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

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 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 [8].

In 1936 Gelfond and Shnirelman, see Gelfond's editorial remarks in the 1944 edition of Chebyshev's Collected Works [7, 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 [10] and [11]. The method of Gelfond–Shnirelman–Nair allows one to obtain in elementary way a lower bound for $\pi(x)$ in terms of integrals of suitable integer polynomials and it is based on the fact that the least common multiple of the integers not greater than N, say d_N, satisfied

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

2010 *Mathematics Subject Classification.* 11C08, 11A41.

Key words and phrases. Integer polynomials, Chebyshev problem, Prime counting function.

where p belongs to the set of prime numbers, which implies

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

Considering a polynomial of degree $N-1$ with integral coefficients

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

and letting

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

we note 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

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

From the above and (1) we get

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

By the definition of $I(P)$, it follows that the small positive value of $|I(P)|$ is $1/d_N$ and it is reached if

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

Since the integer coefficients $d_N, d_N/2, \ldots, d_N/N$ are relatively prime, we have that for all N there exists a polynomial of degree less than N such that $I(P) = 1/d_N$. This leads to define the following sets of polynomials.

Definition. *Let* $N \geq 2$. *We define*

$$Z_N = \{P(x) \in \mathbb{Z}[x], \deg(P) < N\},$$

$$R_N = \{P(x) \in \mathbb{Z}[x], \deg(P) < N, I(P) = 0\}$$

and

$$S_N = \{P(x) \in \mathbb{Z}[x], \deg(P) < N, I(P) = 1/d_N\},$$

where d_N *denotes the least common multiple of the integers* $1, 2, \ldots, N$.

It is simple to verify that, for every N, Z_N is a free $\mathbb{Z}$-module and R_N is a submodule of Z_N and then it is also free. S_N is the affine space of the integer polynomials with positive and minimal integral on $[0, 1]$.

In the precedent paper [3] we proved some results about the roots of polynomials of the sets S_N. In the present paper we carry on the study of the properties of the sets of integer polynomials relevant for the method.

2. Properties of the sets R_N

We start giving a theorem about the structure of the modules R_N.

Theorem 1. *A basis B_N of the module R_N can be constructed by adding to a basis B_{N-1} of the module R_{N-1} a suitable polynomial $q(x) \in R_N$. More precisely*

(1) *if N is a prime: $q(x) = 1 - Nx^{N-1}$;*
(2) *if N is a power of a prime: $q(x) = x^{n-1} - px^{N-1}$, where $N = p^k$ and $n = p^{k-1}$;*
(3) *otherwise: $q(x) = a_1 x^{n_1-1} + a_2 x^{n_2-1} - x^{N-1}$, where p_1 and p_2 are primes dividing N, a_1 and a_2 are such that $a_1p_1 + a_2p_2 = 1$, $n_1 = N/p_1$ and $n_2 = N/p_2$.*

Proof. Let N prime and $p(x) \in R_N$. Then we can write

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{N-1}x^{N-1}$$

with

$$a_0d_N + a_1\frac{d_N}{2} + a_2\frac{d_N}{3} + \cdots + a_{N-2}\frac{d_N}{N-1} + a_{N-1}\frac{d_N}{N} = 1.$$

Since N is a prime number we have that $d_N = Nd_{N-1}$ and then

$$N/d_N, N/\frac{d_N}{2}, N/\frac{d_N}{3}, \ldots N/\frac{d_N}{N-1}$$

and N does not divide d_N/N. From this it follows that a_{N-1}/N is an integer.

Now we define

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{N-2}x^{N-2} + \frac{a_{N-1}}{N},$$

which implies

$$p(x) = r(x) + a_{N-1}x^{N-1} - \frac{a_{N-1}}{N} = r(x) - \frac{a_{N-1}}{N}\left(1 - Nx^{N-1}\right).$$

Then (1) is proved, since $r(x) \in R_{N-1}$.

To prove (2) we let $N = p^k$. In this case $d_N = p\, d_{N-1}$ and more precisely

$$d_N = \prod_{q \le N} q^{[\ln q/\ln N]} = p^k \prod_{q \le N, q \ne p} q^{[\ln q/\ln N]} = Nm,$$

where $(m, p) = 1$ and q runs over primes. From this follows that

$$p/d_N, p/\frac{d_N}{2}, p/\frac{d_N}{3}, \ldots p/\frac{d_N}{N-1}$$

and p does not divide d_N/N, hence a_{N-1}/p is an integer.

Now we define $n = p^{k-1}$ and

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{N-2}x^{N-2} + \frac{a_{N-1}}{p}x^{n-1},$$

which implies

$$p(x) = r(x) + a_{N-1}x^{N-1} - \frac{a_{N-1}}{p}x^{n-1} = r(x) - \frac{a_{N-1}}{p}\left(x^{n-1} - px^{N-1}\right).$$

Then also (2) is proved, since $r(x) \in R_{N-1}$.

To prove (3) we observe that if N is neither prime nor power of a prime then there exist two primes $p_1 \neq p_2$ both dividing N. Let a_1 and a_2 integers such that $a_1p_1 + a_2p_2 = 1$, we define $n_1 = N/p_1$, $n_2 = N/p_2$ and

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{N-2}x^{N-2} + a_1a_{N-1}x^{n_1-1} + a_2a_{N-1}x^{n_2-1}.$$

We conclude that

$$p(x) = r(x) - a_{N-1}\left(a_1x^{n_1-1} + a_2x^{n_2-1} - x^{N-1}\right).$$

and then the proof of the theorem is complete, since $r(x) \in R_{N-1}$. □

Using Theorem 1 we can fully describe the sets R_N. By the definition we have

$$R_2 = \{p(x) \in \mathbb{Z}[x], p(x) = a_0 + a_1x, 2a_0 + a_1 = 0\} = \{p(x) \in \mathbb{Z}[x], p(x) = a_0(1-2x), a_0 \in \mathbb{Z}\}.$$

Then a basis B_2 of the set R_2 is

$$B_2 = \{1 - 2x\}.$$

Using several times Theorem 1 we can get a basis B_N of the set R_N for many values of N:

$B_3 = \{1-2x, 1-3x^2\}$,
$B_4 = \{1-2x, 1-3x^2, -x+2x^3\}$,
$B_5 = \{1-2x, 1-3x^2, -x+2x^3, 1-5x^4\}$,
$B_6 = \{1-2x, 1-3x^2, -x+2x^3, 1-5x^4, x(1-x-x^4)\}$,
$B_7 = \{1-2x, 1-3x^2, -x+2x^3, 1-5x^4, x(1-x-x^4), 1-7x^6\}$,
$B_8 = \{1-2x, 1-3x^2, -x+2x^3, 1-5x^4, x(1-x-x^4), 1-7x^6, x^3-2x^7\}$,
$B_9 = \{1-2x, 1-3x^2, -x+2x^3, 1-5x^4, x(1-x-x^4), 1-7x^6, x^3-2x^7, x^2-3x^8\}, \ldots$

3. Properties of the sets S_N

To describe the sets S_N is much more complicated. Since S_N are affine spaces, we can write

$$S_N = \{\overline{p}(x) + r(x) : r(x) \in R_N\},$$

where $\overline{p}(x)$ is a fixed polynomial of S_N. For small values of N it is simple to find such a suitable polynomial

N	$\overline{p}(x)$	N	$\overline{p}(x)$
3	$x(1-x)$	14	$x^7(1-x)^4(2x-1)(-3+4x)$
4	$x^2(1-x)$	15	$x^7(1-x)^6(2x-1)$
5	$x^2(1-x)(2x-1)$	16	$x^8(1-x)^6(4-7x)$
6	$x^3(1-x)^2$	17	$x^8(1-x)^6(2x-1)(4-5x)$
7	$x^3(1-x)^2(2x-1)$	18	$x^9(1-x)^6(2x-1)(3-4x)$
8	$x^4(1-x)^2(2-3x)$	19	$x^9(1-x)^6(2x-1)^2(53-77x)$
9	$x^4(1-x)^3(2x-1)$	20	$x^{10}(1-x)^6(2x-1)^2(42-59x)$
10	$x^4(1-x)^3(2x-1)$	21	$x^{10}(1-x)^7(2x-1)^2(-2+3x)$
11	$x^5(1-x)^3(2x-1)(-4+5x)$	22	$x^{12}(1-x)^6(2x-1)^2(17-23x)$
12	$x^6(1-x)^3(2x-1)(-3+4x)$	23	$x^{12}(1-x)^7(2x-1)^2(-62+87x)$
13	$x^6(1-x)^4(2x-1)(-4+5x)$	24	$x^{12}(1-x)^7(2x-1)^3(-3+4x)$

Unfortunately it is very difficult to find out such a polynomial for a generic value of N. However we may provide some theorems about their factorization.

Theorem 2. *For every $N \geq 3$ there exists a polynomial $p(x) \in S_N$ such that $p(0) = p(1) = 0$, namely $p(x) = x(1-x)q(x)$ with $q(x) \in \mathbb{Z}[x]$.*

Proof. The list of polynomials given before shows that the theorem is true for $3 \leq N \leq 7$. Then we let $N \geq 8$ and $p(x) \in S_N$, that is

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$$

and

$$a_0 d_N + a_1 \frac{d_N}{2} + a_2 \frac{d_N}{3} + a_3 \frac{d_N}{4} + \cdots + a_{N-2} \frac{d_N}{N-1} + a_{N-1} \frac{d_N}{N} = 1. \tag{3}$$

The Diophantine equation

$$a_3 \frac{d_N}{4} + a_4 \frac{d_N}{5} \cdots + a_{N-2} \frac{d_N}{N-1} + a_{N-1} \frac{d_N}{N} = 1$$

has an integer solution (a_3, a_4, a_{N-1}), since for $N \geq 8$ we have

$$\left(\frac{d_N}{4}, \frac{d_N}{5}, \ldots, \frac{d_N}{N-1}, \frac{d_N}{N} \right) = 1.$$

Setting $a_0 = 0$, $a_1 = 2(a_3 + a_4 + \cdots + q_{N-1})$ and $a_2 = -3(a_3 + a_4 + \cdots + q_{N-1})$ we have that $(a_0, a_1, a_2, \ldots, a_{N-1})$ is a solution of (3) and verify $p(0) = a_0 = 0$ and

$$p(1) = a_0 + a_1 + a_2 + \cdots + a_{N-1} = 0,$$

which concludes the proof of the theorem. □

At the cost of some complications we can prove a similar result also including the factor $(2x-1)$.

Theorem 3. *Let $N \geq 4$.*

(1) *If N is not a power of 2, then there exists a polynomial $p(x) \in S_N$ such that $p(0) = p(1) = p(1/2) = 0$, namely such that $p(x) = x(1-x)(2x-1)q(x)$ with $q(x) \in \mathbb{Z}[x]$;*
(2) *If N is a power of 2, then there not exists a polynomial $p(x) \in S_N$ such that $(2x-1)/p(x)$.*

Proof. Let $p(x) = (2x-1)(b_0 + b_1 x + b_2 x^2 + \cdots + a_{N-2}x^{N-2})$. The condition

$$\int_0^1 p(x)\,\mathrm{d}x = \frac{1}{d_N}$$

is equivalent to

$$\sum_{k=1}^{N-2} \frac{d_N\ k}{(k+1)(k+2)} b_k = 1. \tag{4}$$

If N is a power of 2, then all the coefficients

$$\frac{d_N\ k}{(k+1)(k+2)}$$

are even and thus the equation (4) has no solutions, therefore there not exists a polynomial $p(x) \in S_N$ such that $(2x-1)/p(x)$.

The list of polynomials given before shows that (1) is true for $4 \leq N \leq 24$ and then we need only to consider the case $N \geq 25$. If N is not a power of 2, then we are able to prove that the coefficients

$$\frac{d_N\ k}{(k+1)(k+2)}$$

are relatively prime. In order to prove the coprimality, we suppose on the contrary that there exists a prime p dividing

$$\frac{d_N\ k}{(k+1)(k+2)}$$

for every $k = 1, 2, \ldots, N-2$. Let $H = p^j$, with $j = \max\{i : p^i \leq N\}$ and observe that p does not divide d_N/H. Then at least one of the two coefficients

$$\frac{d_N\ (H-1)}{H(H+1)} \text{ and } \frac{d_N\ (H-2)}{(H-1)H},$$

is not divisible by p, a contradiction. By the coprimality of the coefficients of the Diophantine equation (4) follows that there exists $p(x) \in S_N$ such that $(2x-1)/p(x)$.

To have also the factors x and $(1-x)$ it is sufficent to note that the integer H defined above is greater than 7, since $N \geq 25$, and then there exists a solution $(b_4, b_5, \ldots, b_{N-2})$ of the Diophantine equation

$$\sum_{k=4}^{N-2} \frac{d_N\ k}{(k+1)(k+2)} b_k = 1. \tag{5}$$

We conclude the proof as above by setting $b_0 = b_1 = 0$, $b_2 = 9(b_4 + b_5 + \cdots + b_{N-2})$ and $b_3 = -10(b_4 + b_5 + \cdots + b_{N-2})$. □

Applying similar ideas we can prove the following theorem.

Theorem 4. *Let $N \geq 4$ and let $0 < m < n$ natural numbers such that $(n, m) = 1$.*

(1) *If N is not a power of a prime, then there exists $p(x) \in S_N$ such that $(nx - m)/p(x)$;*
(2) *If N is a power of a prime p, then there exists $p(x) \in S_N$ such that $(nx - m)/p(x)$ if and only if $(p, n) = 1$.*

Proof. Let $N \geq 4$ and $p(x) = (n\,x - m)(b_0 + b_1 x + b_2 x^2 + \cdots + a_{N-2}x^{N-2})$. The condition

$$\int_0^1 p(x)\,\mathrm{d}x = \frac{1}{d_N}$$

is equivalent to

$$\sum_{k=0}^{N-2} d_N \frac{(k+1)(n-m) - m}{(k+1)(k+2)}\, b_k = 1. \tag{6}$$

If N is not a power of a prime, then we are able to prove that the coefficients of the Diophantine equation (6) are relatively prime. In order to prove the coprimality, we suppose that there exists a prime q dividing

$$d_N \frac{(k+1)(n-m) - m}{(k+1)(k+2)}$$

for every $k = 1, 2, \ldots, N-2$, with the goal of obtaining a contradiction. Let $H = q^j$, with $j = \max\{i : q^i \leq N\}$ and consider the coefficient

$$d_N \frac{(H-1)(n-m) - m}{H(H-1)} = \frac{d_N}{H}\, n - \frac{d_N}{H-1}\, m, \tag{7}$$

which arise from $k = H - 2$. By the definition of H, q does not divide d_N/H and divides $d_N/(H-1)$. If q does not divide n then q does not divide (7) and we reach the desired contradiction. If instead q divides n, and then does not divide m, therefore q does not divide the coefficient

$$d_N \frac{H(n-m) - m}{H(H+1)} = d_N \frac{n}{H+1} - \frac{d_N}{H}\, m,$$

which arise from $k = H - 1$, and this leads again to contradiction.

If N is a power of a prime, namely $N = p^k$ with $k \geq 1$, and $(n, p) > 1$ this implies that p divides all the coefficients

$$d_N \frac{(k+1)(n-m) - m}{(k+1)(k+2)}$$

and then the equation (6) has no solutions.

Finally if $N = p^k$ and $(n, p) = 1$ then we suppose that a prime q divides all the coefficients of the equation (6) and find as above that one of such coefficient is not divisible by q, a contradiction. □

4. Integer polynomials in S_N non-negative in $[0,1]$

In the first paper of the series we proposed the following conjecture:

Conjecture. *For every N, or at least for infinitely many values of N, there exists an integer polynomial $p(x) \in S_N$ such that $p(x) \geq 0$ in the interval $[0,1]$.*

A straightforward way to obtain a negative conclusion about the existence of integer polynomials of S_N non-negative in $[0,1]$ is to consider $0 \leq x_1 < x_2 < x_3 \cdots < x_n \leq 1$ and a generic polynomial $p(x) \in S_N$ in the form

$$p(x) = \sum_{k=0}^{N-1} a_k x^k.$$

Since $p(x) \in S_N$, we have

$$\int_0^1 p(x)\,\mathrm{d}x = \frac{1}{d_N},$$

that is

$$\sum_{k=0}^{N-1} \frac{d_N}{k+1} a_k = 1$$

and consider the following linear Diophantine system composed of an equality and n inequalities

$$\begin{cases} \displaystyle\sum_{k=0}^{N-1} \frac{d_N}{k+1} a_k = 1 \\ p(x_1) \geq 0 \\ p(x_2) \geq 0 \\ \dots \\ p(x_n) \geq 0. \end{cases} \tag{8}$$

If we are able to prove that, for a fixed value of N, the above linear system have no integer solutions $a_1, a_2 \dots a_{N-1}$, we obtain that there not exists an integer polynomial $p(x) \in S_N$ such that $p(x) \geq 0$ in the interval $[0,1]$.

By the branch and cut algorithm, used in many mathematical software systems, we can verify in deterministic way that for $N = 5$ and $x_k = k/4$, with $k = 0, 1, \dots, 4$, the system (8) has no integer solutions, although it has infinitely many real solutions, which implies that there are no integer polynomials $p(x) \in S_5$ such that $p(x) \geq 0$ in the interval $[0,1]$. Hence we disproved the strong form of the conjecture.

For $N = 6$ there exists the polynomial $p(x) = x^3(1-x)^2 \in S_6$, non-negative for all values of $x \in [0,1]$. Then the case $N = 5$ might appears as an exceptional case. Instead we can verify that for many values of N there not exists a polynomial in S_N non-negative in $[0,1]$. More precisely we can verify that there not exists an integer polynomial $p(x) \in S_N$ such that $p(x) \geq 0$ in the interval $[0,1]$ for all $7 \leq N \leq 20$, with the only exclusion of the case $N = 10$, for which we have the polynomial $p(x) = x^3(1-x)^4(2x-1)^2$.

To find out any others non-negative polynomials it might be difficult because the calculations involved, but one can prove that such polynomials cannot exist for large values of N. A Nikolskii-type inequality gives that there is a constant $C > 0$ such that

$$\max_{x\in[0,1]} |p(x)| \leq CN^2 \int_0^1 |p(x)| \, \mathrm{d}x$$

for any polynomial $p(x)$ of degree $N-1$, see e.g. [16, Corollary 13.3.3]. If we suppose that there exists a sequence of non-negative polynomials $p_N(x) \in S_N$, we have

$$\frac{1}{d_N} = \int_0^1 p_N(x) \, \mathrm{d}x = \int_0^1 |p_N(x)| \, \mathrm{d}x \geq \frac{1}{CN^2} \max_{x\in[0,1]} |p_N(x)|$$

and hence

$$\lim_{N\to+\infty} \left(\max_{x\in[0,1]} |p_N(x)| \right)^{1/N} \leq \lim_{N\to+\infty} d_N^{-1/N}.$$

It follows from the Prime Number Theorem that

$$\lim_{N\to+\infty} d_N^{-1/N} = e,$$

see [12, page 180]. On the other hand, Gorshkov's bound [12, page 187] gives that

$$\lim_{N\to+\infty} \left(\max_{x\in[0,1]} |p_N(x)| \right)^{1/N} \geq 0.42,$$

which is a contradiction. This implies that there are only finitely many values of N for which there exists a non-negative polynomial in S_N and then we have also disproved the weak form of the Conjecture.

Acknowledgement. We are particularly indebted to the referee for a very thorough reading and for many useful suggestions.

References

[1] F. Amoroso, *Sur le diamètre transfini entier d'un 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] D. Bazzanella, *A note on integer polynomials with small integrals*, Acta Math. Hungar. **141** (2013), n. 4, 320-328.
[4] P. B. Borwein, T. Erdélyi, *Polynomials and polynomial inequalities*, Graduate Texts in Mathematics **161**, Springer-Verlag, New York, 1995.
[5] P. B. Borwein, I. E. Pritsker, *The multivariate integer Chebyshev problem*, Constr. Approx. **30** (2009), no. 2, 299-310.
[6] P. B. Borwein, T. Erdélyi, *The integer Chebyshev problem*, Math. Comp. **65** (1996), no. 214, 661-681.
[7] P. L. Chebyshev, *Collected Works, Vol. 1, Theory of Numbers*, Akad. Nauk. SSSR, Moskow, 1944.
[8] H. G. Diamond, *Elementary methods in the study of the distribution of prime numbers*, Bull. Amer. Math. Soc. **7** (1982), 553-589.
[9] V. Flammang, *Sur le diamètre transfini entier d'un intervalle à extrémités rationnelles*, Annales de l'Institut Fourier **45** (1995), no. 3, 779-793.
[10] M. Nair, *On Chebyshev's-type inequalities for primes*, Amer. Math. Montly **89** (1982), 126-129.

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

[12] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, Vol. **84**. American Mathematical Soc., 1994.

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

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

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

[16] Q. I. Rahman, G. Schmeisser, *Analytic Theory of Polynomials: Critical Points, Zeros and Extremal Properties*, Oxford University Press, 2002.

Dipartimento di Scienze Matematiche, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino — Italy

E-mail address: `danilo.bazzanella@polito.it`