A factor of integer polynomials with minimal integrals

This is the author's manuscript

Original Citation:

Availability:
This version is available http://hdl.handle.net/2318/1647071 since 2017-08-22T18:56:19Z

Published version:
DOI:10.5802/jtnb.994

Terms of use:
Open Access
Anyone can freely access the full text of works made available as "Open Access". Works made available under a Creative Commons license can be used according to the terms and conditions of said license. Use of all other works requires consent of the right holder (author or publisher) if not exempted from copyright protection by the applicable law.

(Article begins on next page)
A FACTOR OF INTEGER POLYNOMIALS WITH MINIMAL INTEGRALS

CARLO SANNA

Abstract. For each positive integer \( N \), let \( S_N \) be the set of all polynomials \( P(x) \in \mathbb{Z}[x] \) with degree less than \( N \) and minimal positive integral over \([0,1]\). These polynomials are related to the distribution of prime numbers since \( \int_0^1 P(x) \, dx = \exp(-\psi(N)) \), where \( \psi \) is the second Chebyshev function. We prove that for any positive integer \( N \) there exists \( P(x) \in S_N \) such that \( x(1-x)\lfloor N/3 \rfloor \) divides \( P(x) \) in \( \mathbb{Z}[x] \). In fact, we show that the exponent \( \lfloor N/3 \rfloor \) cannot be improved. This result is analog to a previous of Aparicio concerning polynomials in \( \mathbb{Z}[x] \) with minimal positive \( L^\infty \) norm on \([0,1]\). Also, it is in some way a strengthening of a result of Bazzanella, who considered \( x\lfloor N/2 \rfloor \) and \( (1-x)\lfloor N/2 \rfloor \) instead of \( x(1-x)\lfloor N/3 \rfloor \).

1. Introduction

It is well-known that the celebrated Prime Number Theorem is equivalent to the assertion:

\[ \psi(x) \sim x, \text{ as } x \to +\infty. \]

Here \( \psi(x) \) is the second Chebyshev function, defined for \( x \geq 0 \) as

\[ \psi(x) := \sum_{p \leq x} \log p, \]

where the sum is extended over all the prime numbers \( p \) and all the positive integers \( m \) such that \( p^m \leq x \).

In 1936, Gelfond and Shnirelman proposed an elementary and clever method to obtain lower bounds for \( \psi(x) \) (see Gelfond’s comments in [5, pp. 285–288]). In 1982, the same method was rediscovered and developed by Nair [9, 10].

The main idea of the Gelfond–Shnirelman–Nair method is the following: Given a positive integer \( N \), let \( P_N(x) \) be a polynomial with integer coefficients and degree less than \( N \), say

\[ P_N(x) = \sum_{n=0}^{N-1} a_n x^n, \]

with \( a_0, \ldots, a_{N-1} \in \mathbb{Z} \). Now consider the integral of \( P_N(x) \) over \([0,1]\), that is

\[ I(P_N) := \int_0^1 P_N(x) \, dx = \sum_{n=0}^{N-1} \frac{a_n}{n+1}. \]

Clearly, \( I(P_N) \) is a rational number whose denominator divides

\[ d_N := \text{lcm}\{1, 2, \ldots, N\}, \]

hence \( d_N | I(P_N) | \) is an integer. In particular, if we suppose \( I(P_N) \neq 0 \), then \( d_N | I(P_N) | \geq 1 \). Now \( d_N = \exp(\psi(N)) \), so we get

\[ \psi(N) \geq \log \left( \frac{1}{|I(P_N)|} \right). \]

Finally, from the trivial upper bound

\[ |I(P_N)| = \left| \int_0^1 P_N(x) \, dx \right| \leq \int_0^1 |P_N(x)| \, dx \leq \max_{x \in [0,1]} |P_N(x)| =: \|P_N\|, \]

2010 Mathematics Subject Classification. 11A41, 11C08, 11A63.

Key words and phrases. Integer polynomials; Chebyshev problem; prime numbers.
we obtain
\begin{equation}
\psi(N) \geq \log \left( \frac{1}{\|P_N\|} \right).
\end{equation}

At this point, if we choose $P_N$ to have a sufficiently small norm $\|P_N\|$, then a lower bound for $\psi(x)$ follows from (1.2). For example, the choice

$$P_N(x) = (x(1 - x))^{2((N-1)/2]}$$

gives the lower bound

$$\psi(N) \geq \log 2 \cdot (N - 2) > 0.694 \cdot (N - 2).$$

This motivates the study of the quantities

$$\ell_N := \min \{\|P\| : P(x) \in \mathbb{Z}[x], \deg(P) < N, \|P\| > 0\},$$

$$C_N := \frac{1}{N} \log \left( \frac{1}{\ell_N} \right),$$

and the set of polynomials

$$T_N := \{P(x) \in \mathbb{Z}[x] : \deg(P) < N, \|P\| = \ell_N\};$$

the so-called Integer Chebyshev Problem [4].

In particular, Aparicio [1] proved the following theorem about the structure of polynomials in $T_N$.

**Theorem 1.1.** Given any sufficiently large positive integer $N$, for all $P \in T_N$ it holds

$$(x(1 - x))^{1_{\lambda_1 N}}(2x - 1)^{1_{\lambda_2 N}}(5x^2 - 5x + 1)^{1_{\lambda_3 N}} | P(x)$$

in $\mathbb{Z}[x]$, where

$$\lambda_1 \in [0.1456, 0.1495], \lambda_2 \in [0.0166, 0.0187], \lambda_3 \in [0.0037, 0.0053]$$

are some constants.

It is known that $C_N$ converges to a limit $C$, as $N \to +\infty$ (see [8, Chapter 10]). Furthermore, Pritsker [11, Theorem 3.1] showed that

$$C \in [0.85991, 0.86441],$$

and this is the best estimate of $C$ known to date.

As a consequence of Pritsker’s result, the Gelfond–Shnirelman–Nair method cannot lead to a lower bound better than

$$\psi(x) \geq 0.86441 \cdot x,$$

which is quite far from what is expected by the Prime Number Theorem.

To deal with this problem, Bazzanella [2, 3] suggested to study the polynomials $P_N$ such that $|I(P_N)|$ is nonzero and minimal, or, without loss of generality, such that $I(P_N)$ is positive and minimal.

We recall the following elementary lemma about the existence of solutions of some linear diophantine equations.

**Lemma 1.2.** Fix some integers $c_1, \ldots, c_k$. Then the diophantine equation

$$\sum_{i=1}^{k} c_i x_i = 1$$

has a solution $x_1, \ldots, x_k \in \mathbb{Z}$ if and only if $\gcd\{c_1, \ldots, c_k\} = 1$. Moreover, if a solution exists, then there exist infinitely many solutions.

On the one hand, because of the above considerations, we known that if $I(P_N) > 0$ then $I(P_N) \geq 1/d_N$. On the other hand, $I(P_N) = 1/d_N$ if and only if

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

and it is easy to see that each of the coefficients $d_N/(n+1)$ is an integer and

$$\gcd\left\{ \frac{d_N}{n+1} : n = 0, \ldots, N-1 \right\} = 1.$$

Hence, by Lemma 1.2, there exist infinitely many polynomials $P_N$ such that $I(P_N) = 1/d_N$, so that (1.1) holds with the equality.
This leads to define the following set of polynomials
\[ S_N := \{ P(x) \in \mathbb{Z}[x] : \deg(P) < N, I(P) = 1/d_N \}. \]

Bazzanella proved some results about the roots of the polynomials in \( S_N \). In particular, regarding the multiplicity of the roots \( x = 0 \) and \( x = 1 \), he gave the following theorem [2, Theorem 1], which is vaguely similar to Theorem 1.1.

**Theorem 1.3.** For each positive integer \( N \), there exists \( P(x) \in S_N \) such that
\[ x^{[N/2]} \mid P(x) \]
in \( \mathbb{Z}[x] \). Moreover, the exponent \([N/2]\) cannot be improved, i.e., there exist infinitely many positive integers \( N \) such that
\[ x^{[N/2]+1} \mid P(x) \]
for all \( P(x) \in S_N \). The same results hold if the polynomial \( x^{[N/2]} \) is replaced by \((1-x)^{[N/2]}\).

Actually, what Bazzanella proved is that the maximum nonnegative integer \( K(N) \) such that there exists a polynomial \( P(x) \in S_N \) divisible by \( x^{K(N)} \), respectively by \((1-x)^{K(N)}\), is given by
\[ K(N) = \min\{p^m - 1 : p \text{ prime}, m \geq 1, p^m > N/2\}, \]
so that Theorem 1.3 follows quickly.

Despite the similarity between Theorems 1.1 and 1.3, note that the statement of Theorem 1.1 holds “for all \( P(x) \in T_N \)”, while Theorem 1.3 only says that “there exists \( P(x) \in S_N \)”. However, this distinction is unavoidable, indeed: On the one hand, \( T_N \) is a finite set, even conjectured to be a singleton for any sufficiently large \( N \) [4, Sec. 5, Q2]. On the other hand, \( S_N \) is an infinite set and if \( P(x) \in S_N \) then \((dN + 1)P(x) - 1 \in S_N \), hence the elements of \( S_N \) have no common nontrivial factor in \( \mathbb{Z}[x] \).

The purpose of this paper is to move another step further in the direction of a stronger analog of Theorem 1.1 for the set of polynomials \( S_N \). For we prove the following theorem.

**Theorem 1.4.** For each positive integer \( N \), there exist infinitely many \( P(x) \in S_N \) such that
\[ (x(1-x))^{[N/3]} \mid P(x) \]
in \( \mathbb{Z}[x] \). Moreover, the exponent \([N/3]\) cannot be improved, i.e., there exist infinitely many positive integers \( N \) such that
\[ (x(1-x))^{[N/3]+1} \mid P(x), \]
for all \( P(x) \in S_N \).

We leave the following informal question to the interested readers:

**Question.** Let \( \{Q_N(x)\}_{N \geq 1} \) be a sequence of “explicit” integer polynomials such that for each positive integer \( N \) it holds \( Q_N(x) \mid P(x) \) in \( \mathbb{Z}[x] \), for some \( P(x) \in S_N \). In light of Theorems 1.3 and 1.4, three examples of such sequences are given by \( \{x^{[N/2]}\}_{N \geq 1} \), \( \{(1-x)^{[N/2]}\}_{N \geq 1} \), and \( \{(x(1-x))^{[N/3]}\}_{N \geq 1} \).

How big can be
\[ \delta := \lim_{N \to +\infty} \inf \frac{\deg(Q_N)}{N} \]
Can \( \delta \) be arbitrary close to 1, or even equal to 1?

Note that the sequences of Theorem 1.3 give \( \delta = 1/2 \), while the sequence of Theorem 1.4 gives \( \delta = 2/3 \).

2. Preliminaries

In this section, we collect a number of preliminary results needed to prove Theorem 1.4. The first is a classic theorem of Kummer [7] concerning the \( p \)-adic valuation of binomial coefficients.

**Theorem 2.1.** For all integers \( u, v \geq 0 \) and any prime number \( p \), the \( p \)-adic valuation of the binomial coefficient \( \binom{u+v}{u} \) is equal to the number of carries that occur when \( u \) and \( v \) are added in the base \( p \).

Now we can prove the following lemma.
Lemma 2.2. For any positive integer \( N \), and for all integers \( u, v \geq 0 \) with \( u + v < N \), we have that
\[
\frac{d_N}{(u + v + 1)\binom{u+v}{u}}
\]
is an integer.

Proof. We have to prove that for any prime number \( p \leq N \) the \( p \)-adic valuation of the denominator of (2.1) does not exceed \( \nu_p(d_N) = \lfloor \log_p N \rfloor \). Write \( u + v + 1 \) in base \( p \), that is
\[
0 + v = \sum_{i=0}^{s} d_i p^i,
\]
where \( i_0 := \nu_p(u + v + 1) \) and \( d_0, \ldots, d_s \in \{0, \ldots, p-1\} \), with \( d_0, d_s > 0 \). Hence, the expansion of \( u + v \) in base \( p \) is
\[
\sum_{i=0}^{s} d_i p^i = (u + 1)(v + 1) - 1
\]
In particular, by (2.2), we have that \( u + 1 \) written in base \( p \) has exactly \( s + 1 \) digits, of which the \( i_0 \) least significant are all equal to \( p - 1 \). Therefore, in the sum of \( u \) and \( v \) in base \( p \) there occur at most \( s - i_0 \) carries. Since, thanks to Theorem 2.1, we know that \( i_1 := \nu_p\left(\binom{u+v}{u}\right) \) is equal to the number of carries occurring in the sum of \( u \) and \( v \) in base \( p \), it follows that \( i_1 \leq s - i_0 \).

In conclusion,
\[
\nu_p\left(\binom{u+v+1}{u}\right) = i_0 + i_1 \leq s \leq \lfloor \log_p N \rfloor,
\]
where the last inequality holds since \( u + v + 1 \leq N \).

We recall the value of a well-known integral (see, e.g., [6, Sec. 11.1.7.1, Eq. 2]).

Lemma 2.3. For all integers \( u, v \geq 0 \), it holds
\[
\int_0^1 x^u(1-x)^v dx = \frac{1}{(u + v + 1)\binom{u+v}{u}}.
\]

We conclude this section with a lemma that will be fundamental in the proof of Theorem 1.4.

Lemma 2.4. Let \( N \) and \( m \) be integers such that \( N \geq 1 \) and \( 0 \leq m \leq (N - 1)/2 \). The following statements are equivalent:

(i) There exist infinitely many \( P(x) \in S_N \) such that \((x(1-x))^m | P(x) \) in \( \mathbb{Z}[x] \).

(ii) For each prime number \( p \leq N \), there exists an integer \( h_p \) such that \( h_p \in [m, N - m - 1] \) and
\[
\nu_p\left(\binom{h_p + m + 1}{h_p + m}\right) = \lfloor \log_p N \rfloor.
\]

Proof. Let \( P(x) \in \mathbb{Z}[x] \) be such that \( \deg(P) < N \) and
\[
(x(1-x))^m | P(x)
\]
in \( \mathbb{Z}[x] \). Hence,
\[
P(x) = (x(1-x))^m \sum_{h=m}^{N-m-1} b_h x^{h-m},
\]
for some \( b_m, \ldots, b_{N-m-1} \in \mathbb{Z} \). Then, by Lemma 2.3, it follows that
\[
I(P) = \sum_{h=m}^{N-m-1} b_h \int_0^1 x^h(1-x)^m dx = \sum_{h=m}^{N-m-1} \frac{b_h}{(h + m + 1)\binom{h+m}{m}}.
\]
Now we have \( P(x) \in S_N \) if and only if \( I(P) = 1/d_N \), i.e., if and only if
\[
\sum_{h=m}^{N-m-1} d_N \frac{b_h}{(h + m + 1)\binom{h+m}{m}} = 1.
\]
Therefore, thanks to Lemma 2.2 and Lemma 1.2, we get infinitely many \( P(x) \in S_N \) if and only if
\[
gcd\left\{ \frac{d_N}{(h + m + 1)\binom{h+m}{m}} : h = m, \ldots, N - m - 1 \right\} = 1.
\]
At this point, recalling that \( \nu_p(d_N) = \lfloor \log_p N \rfloor \) for each prime number \( p \), the equivalence of (i) and (ii) follows easily. \( \square \)

3. Proof of Theorem 1.4

We are ready to prove Theorem 1.4. Put \( m := \lfloor N/3 \rfloor \), \( s := \lfloor \log_p N \rfloor \), and pick a prime number \( p \leq N \). In light of Lemma 2.4, in order to prove the first part of Theorem 1.4 we have to show the existence of an integer \( h_p \in [m, N - m - 1] \) such that

\[
(3.1) \quad \nu_p \left( \frac{(h_p + m + 1)(h_p + m)}{m} \right) = s.
\]

Let us write \( N = \ell p^s + r \), for some \( \ell \in \{1, \ldots, p - 1\} \) and \( r \in \{0, \ldots, p^s - 1\} \). We split the proof in three cases:

**Case** \( \ell \geq 2 \). It is enough to take \( h_p := \ell p^s - m - 1 \). In fact, on the one hand, it is straightforward that (3.1) holds. On the other hand, since \( \ell \geq 2 \), we have

\[
h_p = \ell p^s - m - 1 \geq \frac{2}{3}(\ell + 1)p^s - m - 1 > \frac{2}{3}N - m - 1 \geq m - 1,
\]

while clearly \( h_p \leq N - m - 1 \), hence \( h_p \in [m, N - m - 1] \), as desired.

**Case** \( m < p^s - 1 \). It holds

\[
p^s - \frac{2}{3} < m + 1 \leq p^s - 1,
\]

hence \( p = 2 \). Now it is enough to take \( h_2 := 2^s - m - 1 \). In fact, on the one hand, it is again straightforward that (3.1) holds. On the other hand, since \( m < 2^{s-1} \), we have

\[
h_2 = 2^s - m - 1 > 2^s - 2^{s-1} - 1 = 2^{s-1} - 1 \geq m,
\]

while obviously \( h_2 \leq N - m - 1 \), hence \( h_2 \in [m, N - m - 1] \), as desired.

**Case** \( \ell = 1 \) and \( m \geq p^s - 1 \). This case requires more effort. We have

\[
p^s - \frac{2}{3} < \frac{p^s + r}{3} < \frac{2p^s}{3} < p^s,
\]

hence the expansion of \( m \) in base \( p \) is

\[
m = \sum_{i=0}^{s-1} d_i p^i,
\]

for some \( d_0, \ldots, d_{s-1} \in \{0, \ldots, p - 1\} \), with \( d_{s-1} > 0 \).

Let \( i_1 \) be the least nonnegative integer not exceeding \( s \) such that

\[
d_i \geq \frac{p - 1}{2}, \quad \forall i \in \mathbb{Z}, \quad i_1 \leq i < s.
\]

Moreover, let \( i_2 \) be the greatest integer such that \( i_1 \leq i_2 \leq s \) and

\[
d_i = \frac{p - 1}{2}, \quad \forall i \in \mathbb{Z}, \quad i_1 \leq i < i_2.
\]

Note that, by the definitions of \( i_1 \) and \( i_2 \), we have

\[
d_i > \frac{p - 1}{2}, \quad \forall i \in \mathbb{Z}, \quad i_2 \leq i < s.
\]

Clearly, it holds

\[
m = \sum_{i_2 \leq i < s} d_i p^i + \sum_{i_1 \leq i < i_2} \frac{p - 1}{2} p^i + \sum_{0 \leq i < i_1} d_i p^i.
\]

Define now

\[
h_p := \sum_{i_2 \leq i < s} d_i p^i + \sum_{i_1 \leq i < i_2} \frac{p - 1}{2} p^i + \sum_{0 \leq i < i_1} (p - d_i - 1)p^i.
\]

Note that (3.5) is actually the expansion of \( h_p \) in base \( p \), that is, all the coefficients of the powers \( p^i \) belong to the set of digits \( \{0, \ldots, p - 1\} \). At this point, looking at (3.4) and (3.5), and taking into account (3.3), it follows easily that in the sum of \( h_p \) and \( m \) in base \( p \) there occur exactly \( s - i_2 \) carries. Therefore, by Theorem 2.1 we have

\[
(3.6) \quad \nu_p \left( \frac{(h_p + m)}{m} \right) = s - i_2.
\]
Furthermore, from (3.4) and (3.5) we get
\[ h_p + m + 1 = 2 \sum_{i_2 \leq i < s} d_i p^i + \sum_{0 \leq i < i_2} (p-1)p^i + 1 = 2 \sum_{i_2 \leq i < s} d_i p^i + p^{i_2}, \]
hence
\[ (3.7) \quad \nu_p(h_p + m + 1) = i_2. \]
Therefore, putting together (3.6) and (3.7) we obtain (3.1).

It remains only to prove that \( h_p \in [m, N - m - 1] \). If \( i_2 = s \), then from (3.7) it follows that
\[ h_p + m + 1 = 0 + p^s \leq N, \]
hence \( h_p \leq N - m - 1 \). If \( i_2 < s \), then from (3.2) it follows \( d_{i_2} \geq (p-1)/2 \), hence \( d_{i_2} \geq 1 \) and from (3.7) and (3.4) we obtain
\[ h_p + m + 1 \leq 2 \sum_{i_2 \leq i < s} d_i p^i + d_{i_2}p^{i_2} \leq 2m + m = 3m \leq N, \]
so that again \( h_p \leq N - m - 1 \). If \( i_1 = 0 \), then by (3.4) and (3.5) we have immediately that \( h_p = m \). If \( i_1 > 0 \), then by the definition of \( i_1 \), we have \( d_{i_1-1} < (p-1)/2 \), i.e., \( d_{i_1-1} < p - d_{i_1-1} - 1 \), thus looking at the expansions (3.4) and (3.5) we get that \( h_p > m \). Hence, in conclusion we have \( h_p \in [m, N - m - 1] \), as desired.

Regarding the second part of Theorem 1.4, take \( N := 3q \), where \( q > 3 \) is a prime number. Put \( m := \lfloor N/3 \rfloor + 1 = q + 1 \), and let \( h \in [m, N - m - 1] \) be an integer. On the one hand, it is straightforward that \( q \not|\ h + m + 1 \). On the other, it is also easy to see that in the sum of \( h \) and \( m \) in base \( q \) there is no carry, hence, by Theorem 2.1, we have that \( q \not|\ \left(\frac{h+m}{m}\right) \). Therefore,
\[ \nu_q\left(\left(\frac{h+m}{m}\right)\right) = 0 < 1 - \lfloor \log_q N \rfloor, \]
so that, thanks to Lemma 2.4, we have \((x(1-x))^m \not|\ P(x)\) in \( \mathbb{Z}[x]\), for all \( P(x) \in S_N \). This completes the proof.

References