PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série tome 50 (64), 1991, 159–162

A WAY OF REDUCING THE FACTORIZATION PROBLEM IN Z[x] TO THE FACTORIZATION PROBLEM IN Z

S. Prešić

Abstract. Let $p(x) \in \mathbf{Z}[x]$ be a given polynomial. Then there exists and can be effectively determined a natural number M such that the factorization problem of $p(x)$ in $\mathbf{Z}[x]$ is logically equivalent to the problem of finding some particular factorization of the number $p(M)$.

1. We start with some general facts.

LEMMA 1. *Let M (>1) be a given natural number and k an integer. Then every integer $a \neq 0$ can be uniquely expressed in the form*

$$a = q_n M^n + q_{n-1} M^{n-1} + \cdots + q_0 \tag{1}$$

where $n \in \mathbf{N}$, $q_i \in \{k, k+1, \dots, k+M-1\}$ and $q_n \neq 0$.

This is a slight variation of the well-known fact when $k = 0$. Let, for instance, $M = 5$, $k = -2$. Then we have $14 = 1 \cdot 5^2 + (-2) \cdot 5 + (-1) \cdot 1$, $-42 = (-2) \cdot 5^2 + 2 \cdot 5 + (-2) \cdot 1$.

LEMMA 2. *Let $p(x) = a_n x^n + \cdots + a_0$ $(a_i \in \mathbf{Z},\ a_n \neq 0,\ n \geq 1)$ be a given polynomial and B any upper bound of the moduli $|x_1|, \dots, |x_n|$, where $x_1, \dots, x_n$ are all zeros of the polynomial $p(x)$. Assume that $f(x) = b_p x^p + \cdots + b_0$ $(b_i \in \mathbf{Z},$ $b_p \neq 0,\ p \geq 1)$ divides $p(x)$. Then*

$$\max_{0 \leq i \leq p} |b_i| \leq \max_{1 \leq i \leq n-1} \left\{ |a_0|, |a_n|, |a_n| \binom{n-1}{i} \cdot B^i \right\}. \tag{2}$$

Proof. Obviously, $|b_p| \leq |a_n|$ and $|b_0| \leq |a_0|$. Furthermore, for any coefficient b_{p-k}, where $1 \leq k \leq p-1$, we have by Viète theorem (assuming $y_1, \dots, y_p$ are all zeros of $f(x)$)

$$\left| \frac{b_{p-k}}{b_p} \right| = \left| \sum_{1 \leq i_1 < \dots < i_k \leq i_p} y_{i_1} \cdot \dots \cdot y_{i_k} \right| \leq \binom{p}{k} B^k.$$

AMS Subject Classification (1985): Primary 60 F 05

Hence,

$$|b_{p-k}| \le |a_n| \cdot \binom{p}{k} B^k \le |a_n| \binom{n-1}{k} B^k,$$

which completes the proof.

Lemma 3. *Let $p(x) = a_n x^n + \cdots + a_0 \in \mathbf{Z}[x]$, with $a_n \neq 0$, be a given polynomial and M some odd natural number such that*

$$a_n M^n + \cdots + a_0 = (b_p M^p + \cdots + b_0) \cdot (c_q M^q + \cdots + c_0) \qquad (3)$$
$$(p, q \ge 1,\ p + q = n;\ b_i, c_j \in \mathbf{Z}).$$

Let also[1)]

$$|a_i| \le [M/2] \qquad (i = 0, \dots, n) \qquad \text{and} \qquad (4)$$

$$\Bigg| \sum_{i+j=p+q-r} b_i c_j \Bigg| \le [M/2] \qquad (r = 0, \dots, p+q). \qquad (5)$$

Then the polynomial equality

$$a_n x^n + \cdots + a_0 = (b_p x^p + \cdots + b_0) \cdot (c_q x^q + \cdots + c_0) \qquad (6)$$

holds.

Proof. The equality (3) implies

$$a_n M^n + \cdots + a_0 = b_p c_q M^{p+q} + \cdots + \Bigg(\sum_{i+j=p+q-r} b_i c_j \Bigg) M^{p+q-r} + \cdots + b_0 c_0, \quad \text{i.e.}$$

$$a_n M^n + \cdots + a_0 = b_p c_q M^n + \cdots + \Bigg(\sum_{i+j=n-r} b_i c_j \Bigg) M^{n-r} + \cdots + b_0 c_0.$$

In view of (4), (5) and Lemma 1 (with $k = -[M/2]$), one immediately concludes

$$a_n = b_p c_q, \quad \dots, \quad a_{n-r} = \sum_{i+j=n-r} b_i c_j, \quad \dots, \quad a_0 = b_0 c_0$$

i.e., the equality (6). The proof is completed.

In what follows the conditions (3), (4), (5) will play the key role. Denote (3) by $\psi(M)$. Then, according to Lemma 3, the conjunction $(3) \wedge (4) \wedge (5)$ is equivalent to the conjunction

$$\psi(M) \wedge \psi(m_1) \wedge \ldots \wedge \psi(m_n), \qquad (7)$$

where $M, m_1, \dots, m_n$ are arbitrary different integers.

[1)] $[x]$ means the greatest integer part of x.

2. Suppose now that $M\ (=2K+1)$ is a given odd natural number. According to Lemma 1, every integer a can be uniquely expressed in the form (1) with[2)] $k=-K$. Let further a_i, b_j, c_k be any integers and $p, q, n \in \mathbf{N}$. We introduce the following definition.

Definition 1. Any number-factorization of the form

$$a_n M^n + \cdots + a_0 = (b_p M^p + \cdots + b_0)\cdot(c_q M^q + \cdots + c_0) \tag{8}$$
$$(b_p, c_q, a_n \neq 0,\ p+q=n,\ p,q \geq 1)$$

is called M-free iff the conditions (4) and (5) are satisfied.

Obviously, putting together this definition and Lemma 3 we obtain the following

LEMMA 4. *The factorization* (8) *is M-free if and only if the polynomial equality*

$$a_n x^n + \cdots + a_0 = (b_p x^p + \cdots + b_0)\cdot(c_q x^q + \cdots + c_0) \tag{9}$$

is true.

As we see, the problem of finding all identities of the form (9), that is, the problem of factorization in $\mathbf{Z}[x]$ is related to the problem of finding M-free factorizations in $\mathbf{Z}$. More precisely, we have the following result.

THEOREM 1. *Let $p(x) = a_n x^n + \cdots + a_0$ ($a_i \in \mathbf{Z}$, $a_n \neq 0$, $n > 0$) be a given polynomial and let B be any upper bound of the moduli $|x_1|, \ldots, |x_n|$, where $x_1, \ldots, x_n$ are all zeros of p. Let K and M be the natural numbers defined by*

$$K = \max_{0\leq i\leq n,\,1\leq j\leq n-1}\left\{|a_i|, \left[|a_n|\binom{n-1}{j}B^j\right]\right\}, \qquad M = 2K+1. \tag{10}$$

Then to each M-free factorization of the form

$$a_n M^n + \cdots + a_0 = (b_p M^p + \cdots + b_0)\cdot(c_q M^q + \cdots + c_0) \tag{11}$$
$$(p,q \geq 1,\ p+q=n,\ b_i, c_j \in \mathbf{Z},\ b_p \neq 0,\ c_q \neq 0)$$

there corresponds the $\mathbf{Z}[x]$-factorization of $p(x)$

$$a_n x^n + \cdots + a_0 = (b_p x^p + \cdots + b_0)\cdot(c_q x^q + \cdots + c_0). \tag{12}$$

Moreover, in such a way one obtains all $\mathbf{Z}[x]$-factorizations of $p(x)$.

Proof. According to Definition 1 it is clear that to each M-free factorization of the form (11) there corresponds a $\mathbf{Z}[x]$-factorization of $p(x)$ given by (12). To complete the proof suppose that

$$a_n x^n + \cdots + a_0 = (b_p x^p + \cdots + b_0)\cdot(c_q x^q + \cdots + c_0) \tag{13}$$
$$(p+q=n,\ b_i, c_j \in \mathbf{Z},\ b_p \neq 0,\ c_q \neq 0)$$

[2)] which implies the inequalities $|q_i| \leq K$, $i = 0, \ldots, n$.

is any $\mathbf{Z}[x]$-factorization of $p(x)$. From (13) it follows that

$$a_nM^n + \cdots + a_0 = (b_pM^p + \cdots + b_0) \cdot (c_qM^q + \cdots + c_0). \tag{14}$$

In view of Lemma 1, using (13) we obtain the inequalities

$$\begin{aligned} |b_pc_q| &\le K \qquad (\text{since } b_pc_q = a_n),\\ |b_pc_{q-1} + b_{p-1}c_q| &\le K \qquad (\text{since } b_pc_{q-1} + b_{p-1}c_q = a_{n-1}),\\ \cdots \quad &\cdots \end{aligned}$$

which imply that the number-factorization (13) is M-free.

Based on Theorem 1, we give a $\mathbf{Z}[x]$-factorization algorithm for a given polynomial $p(x) \in \mathbf{Z}[x]$:

1° In the first step one finds a number M using (10). In addition, by a result due to Cauchy, B may be defined by

$$B = 1 + \max_{0 \le i \le n-1} (|a_i|/|a_n|).$$

2° In the second step one calculates $p(M)$.

3° In the third step, among all number-factorizations of $p(M)$ one selects[3)] M-free factorizations, if any.

4° Finally, the obtained list of all M-free factorizations determines the list of all $\mathbf{Z}[x]$-factorizations of the given polynomial $p(x)$ (as a product of *two* polynomials).

For instance, if $p(x) = x^4 - x^3 + 3x^2 - x + 2$ then according to (10) and the Cauchy formula (see 1° above) we can take $K = 64$, $M = 129$. The list of all factors a ($M - K \le a \le \left[\sqrt{p(M)}\right]$) of the number $p(M)$ reads: 92, 106, 157, 212, 314, 359, 628, 718, 1219, 1436, 2438, 3611, 4876, 7222, 8257, 8321, 14444, 16514. Representing these numbers in the form (1) and applying Definition 1 one can easily conclude that there is exactly one M-free factorization of the number $p(M)$:

$$p(M) = 16514 \cdot 16642 = (M^2 + 1)(M^2 - M + 2)$$

Consequently, the given polynomial $p(x)$ factorizes as

$$p(x) = (x^2 + 1)(x^2 - x + 2).$$

REFERENCE

[1] B. L. van der Waerden, *Algebra I*, 8th edition, Springer-Verlag, 1971, §32, p. 98.

Matematički fakultet
Studentski trg 16
11001 Beograd, p.p. 550
Yugoslavia

(Received 26 04 1990)
(Revised 05 11 1990)

3) Checking the equality (3) for n different values $m_1, m_2, \ldots, m_n$ ($m_i \ne M$) or checking the equalities $a_{n-k} = b_pc_{q-k} + \cdots + b_{p-k}c_q$ ($k = 0, 1, \ldots, n$).