Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 8, Number 4 (2012), pp. 371–377

http://www.ripublication.com/gjpam.htm

On The Division Algorithm For Polynomials

Abdelhalim M. Zaiqan[1] **and Ragheb Yaseen**

Department of Mathematics and Statistics,
Arab American University, Jenin, Palestine.
E-mail: azaiqan@aauj.edu

Abstract

In this paper we consider the polynomial division algorithm and give compact formulas for the coefficients of the quotient and the remainder polynomials. We also organize the coefficients of the dividend and the divisor in an efficient way to simplify the evaluations of the requested coefficients. The described method avoids the complications of the manual calculations.

AMS subject classification:
Keywords: Division algorithm, synthetic division, factor theorem.

1. Introduction

The division algorithm for polynomials play an important role in algebra. The need to such process appears in, for example, coding theory, cryptography and many concepts of abstract algebra. Also, it is a classical technique in factoring polynomials. In college algebra textbooks, the long division, when the degree of the divisor is greater than one, seems to be very exhausted. Our aim in this paper is to simplify the manual calculations of the division algorithm using only the coefficients of the dividend and the divisor polynomials.

The polynomials division algorithm has been investigated by many authors. A remarkable criterion was given by F.G. Eisenstein to determine the irreducibility of a polynomial (cf. [3], Sec. 9.4). Bini and Pan [1] and [2] presented parallel algorithm for the division algorithm over an arbitrary constant field. FAN [4] in his generalized theorem gave two separated formulas for the coefficients of the quotient and the remainder. Idarraga and Salas[5] showed that under certain conditions for a given polynomial there exists a factor of the form $x^m - b$.

[1]Corresponding author.

2. The Division Algorithm

Let $f(x) = \sum_{i=0}^{n} c_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$ be two polynomials, such that $c_n \neq 0$, $b_m \neq 0$, and $m \leq n$. From the division algorithm, we have

$$f(x) = g(x)h(x) + r(x) \tag{1}$$

where $h(x) = \sum_{i=0}^{k} a_i x^i, a_k \neq 0$ such that $k = n - m$, and r is a polynomial of degree $t < m$. Without loss of generality we may assume that $t = m - 1$. So, we let $r(x) = \sum_{i=0}^{m-1} d_i x^i$. Then equation (1) becomes

$$\sum_{i=0}^{n} c_i x^i = (\sum_{i=0}^{m} b_i x^i)(\sum_{i=0}^{k} a_i x^i) + \sum_{i=0}^{m-1} d_i x^i \tag{2}$$

The coefficients $c_i, i = 0, \ldots, n$, can be calculated using the following two formulas for $0 \leq p \leq k$

$$c_{n-p} = \sum_{i+j=n-p} a_i \ b_j \tag{3}$$

and for $0 \leq p_0 \leq m - 1$

$$c_{t-p_0} = \sum_{i+j=t-p} a_i \ b_j + d_{t-p_0} \tag{4}$$

In fact, equation (2) is equivalent to the following linear system (Ref. [1]):

$$\begin{bmatrix} c_0 \\ \vdots \\ c_m \\ \vdots \\ c_n \end{bmatrix}_{(n+1)\times 1} = \begin{bmatrix} b_0 & 0 & \cdots & 0 & 0 \\ b_1 & b_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_m & b_{m-1} & \cdots & & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_0 \\ \vdots & \vdots & b_m & \cdots & b_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & b_m \end{bmatrix}_{(n+1)\times(k+1)} \begin{bmatrix} a_0 \\ \vdots \\ a_k \end{bmatrix} + \begin{bmatrix} d_0 \\ \vdots \\ d_{m-1} \\ 0 \\ \vdots \\ 0 \end{bmatrix}_{(n+1)\times 1}$$

Now, Let

$$\triangle_{i1} = \begin{vmatrix} b_m & c_n \\ b_{m-i} & c_{n-i} \end{vmatrix}, 1 \leq i \leq m \tag{5}$$

$$\triangle_{ij} = \begin{vmatrix} b_m & \triangle_{1j-1} \\ b_{m-i} & \triangle_{i+1j-1} \end{vmatrix}, 1 \leq i \leq m-1, 2 \leq j \leq k+1 \tag{6}$$

and

$$\triangle_{mj} = \begin{vmatrix} b_m^j & \triangle_{1j-1} \\ b_0 & c_{n-j+1} \end{vmatrix}, 2 \leq j \leq k+1 \tag{7}$$

Theorem 2.1. For any two polynomials $f(x) = \sum_{i=0}^{n} c_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ with nonzero leading coefficients and $m \leq n$, there exist two polynomials $h(x) = \sum_{i=0}^{k} a_i x^i$ and $r(x) = \sum_{i=0}^{m-1} d_i x^i$ such that $f(x) = g(x)h(x) + r(x)$. The coefficients of h and r can be obtained as follows:

$$a_k = \frac{c_n}{b_m} \tag{8}$$

$$a_{k-p} = \frac{\triangle_{1p}}{b_m^{p+1}}, p = 1, \ldots, k. \tag{9}$$

$$d_{t-p_0} = \frac{\triangle_{p_0+1k+1}}{b_m^{k+1}}, p_0 = 0, ..., m-1. \tag{10}$$

Proof. To see formula (9) we use induction on p. When $p = 1$, from equation (3) we have

$$c_{n-1} = a_k b_{m-1} + a_{k-1} b_m. \tag{11}$$

Now, substituting the value of a_k in equation (11) to get

$$b_m^2 a_{k-1} = b_m c_{n-1} - b_{m-1} c_n = \triangle_{11}$$

Assume that equation (9) is true for $p < k$. For $p = k$, equation (3) gives

$$\begin{aligned} a_0 b_m &= c_m - a_k b_{m-k} - a_{k-1} b_{m-k+1} - \cdots - a_2 b_{m-2} - a_1 b_{m-1} \\ &= c_m - \frac{c_n}{b_m} b_{m-k} - \frac{\triangle_{11}}{b_m^2} b_{m-k+1} - \cdots - \frac{\triangle_{1k-2}}{b_m^{k-1}} b_{m-2} - \frac{\triangle_{1k-1}}{b_m^k} b_{m-1} \end{aligned}$$

Multiply the last equation by b_m^k to get

$$a_0 b_m^{k+1} = b_m^k c_m - b_m^{k-1} b_{m-k} c_n - \cdots - b_m \Delta_{1k-2} b_{m-2} - b_{m-1} \Delta_{1k-1} \tag{12}$$

Now, from equation (6)

$$\Delta_{1k} = b_m \Delta_{2k-1} - b_{m-1}\Delta_{1k-1} \tag{13}$$

and

$$\Delta_{2k-1} = b_m \Delta_{3k-2} - b_{m-2}\Delta_{1k-2} \tag{14}$$

replace the value of Δ_{2k-1} in equation (14) by its value in equation (13) to get

$$\Delta_{1k} = b_m^2 \Delta_{3k-2} - b_m b_{m-2}\Delta_{1k-2} - b_{m-1}\Delta_{1k-1} \tag{15}$$

Notice that the last two terms in the right hand side of (15) are exactly the last two terms in the right hand side of (12). Continuing in this way, one can get the following formula

$$\Delta_{1k} = b_m^{k-1}\Delta_{k1} - b_m^{k-2} b_{m-k+1}\Delta_{11} - \cdots - b_m b_{m-2}\Delta_{1k-2} - b_{m-1}\Delta_{1k-1} \tag{16}$$

On the other hand, since $\Delta_{k1} = b_m c_m - b_{m-k} c_n$, then

$$b_m^k c_m = b_m^{k-1}\Delta_{k1} + b_m^{k-1} b_{m-k} c_n \tag{17}$$

from equations (17) and (12) we have

$$a_0 b_m^{k+1} = b_m^{k-1}\Delta_{k1} - b_m^{k-2} b_{m-k+1}\Delta_{11} - \cdots - b_m b_{m-2}\Delta_{1k-2} - b_{m-1}\Delta_{1k-1} \tag{18}$$

Hence, equation (16) together with equation (18) give $b_m^{k+1} a_0 = \Delta_{1k}$. Next, to see formula (10) we use induction on p_0. When $p_0 = t$, from equation (4) we have $d_0 = c_0 - a_0 b_0 = c_0 - b_0 \dfrac{\Delta_{1k}}{b_m^{k+1}}$. Therefore, $b_m^{k+1} d_0 = b_m^{k+1} c_0 - b_0 \Delta_{1k} = \Delta_{mk+1}$. Assume that formula (10) it is true for $0 < p_0 \le t$. The last step is to show formula (10) for $p_0 = 0$. From equation (4), we have

$$\begin{aligned} c_t &= \sum_{i+j=t} a_i b_j + d_t \\ &= a_k b_{t-k} + a_{k-1} b_{t-k+1} + \cdots + a_2 b_{t-2} + a_1 b_{t-1} + a_0 b_t + d_t \\ &= \frac{c_n}{b_m} b_{t-k} + \frac{\Delta_{11}}{b_m^2} b_{t-k+1} + \cdots + \frac{\Delta_{1k-2}}{b_m^{k-1}} b_{t-2} + \frac{\Delta_{1k-1}}{b_m^k} b_{t-1} + \frac{\Delta_{1k}}{b_m^{k+1}} b_t + d_t \end{aligned}$$

Therefore,

$$b_m^{k+1} d_t = b_m^{k+1} c_t - b_m^k c_n b_{t-k} - b_m^{k-1}\Delta_{11} b_{t-k+1} \cdots . - b_m \Delta_{1k-1} b_{t-1} - \Delta_{1k} b_t \tag{20}$$

On the other hand, $\Delta_{1k+1} = b_m \Delta_{2k} - b_{m-1}\Delta_{1k}$. But, $t = m-1$ and $\Delta_{2k} = b_m \Delta_{3k-1} - b_{m-2}\Delta_{1k-1}$. Hence,

$$\Delta_{1k+1} = b_m^2 \Delta_{3k-1} - b_m b_{m-2}\Delta_{1k-1} - b_t \Delta_{1k}$$

Repeat the process of replacing $\Delta_{ik-i+2}, i = 2, \dots, k+1$, by its value from equation (7) to get

$$\Delta_{1k+1} = b_m^k \Delta_{k+11} - b_m^{k-1} \Delta_{11} b_{t-k+1} - \cdots - b_m b_{m-2} \Delta_{1k-1} - b_t \Delta_{1k}$$

Now, since $\Delta_{k+11} = b_m c_{n-k-1} - b_{m-k-1} c_n$, $k = n - m, m - k - 1 = t - k$ and $n - k - 1 = t$, then

$$\Delta_{1k+1} = b_m^{k+1} c_t - b_m^k c_n b_{t-k} - b_m^{k-1} \Delta_{11} b_{t-k+1} - \cdots - b_m b_{m-2} \Delta_{1k-1} - b_t \Delta_{1k} \quad (21)$$

Finally, from equations (21) and (20) we conclude that $\Delta_{1k+1} = b_m^{k+1} d_t$. ■

Remark 2.2. Using the above notations we can introduce the following array to describe the method numerically:

$$\begin{array}{cccccc} b_m & c_n & \Delta_{11} & \dots & \Delta_{1k} & \Delta_{1k+1} \\ b_{m-1} & c_{n-1} & \Delta_{21} & \cdots & \Delta_{2k} & \Delta_{2k+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_1 & c_{n-m+1} & \Delta_{m1} & \cdots & \Delta_{mk} & \Delta_{mk+1} \\ b_0 & c_{n-m} & c_{n-m-1} & \cdots & c_0 & \end{array} \quad (22)$$

The coefficients of the quotient and the remainder can be calculated from following relations:

$$b_m a_k = c_n, b_m^2 a_{k-1} = \Delta_{11}, \dots, b_m^{k+1} a_0 = \Delta_{1k}$$

and

$$\Delta_{1k+1} = b_m^{k+1} d_t, \dots, \Delta_{mk+1} = b_m^{k+1} d_0$$

3. Applications

In this section, we present examples to show how the method works.

Example 3.1. Let $f(x) = 2x^3 + x^2 + 4$ and $g(x) = 2x^2 + 3$.

To find the quotient and the remainder polynomials, we have to arrange the coefficients of $f(x)$ and $g(x)$ as follows:

$$\begin{array}{ccc} 2 & 2 & \\ 0 & 1 & \\ 3 & 0 & 4 \end{array}$$

the second step is to evaluate the entries above the value 4 which are exactly: $2 \times 1 - 0 \times 2$ and $2 \times 0 - 3 \times 2$.

$$\begin{array}{ccc} 2 & 2 & 2 \\ 0 & 1 & -6 \\ 3 & 0 & 4 \end{array}$$

In the third step, we ignore the second column in the previous step and compute the entries of the last column :$2 \times -6 - 0 \times 2$ and $2^2 \times 4 - 3 \times 2$.

$$\begin{array}{cccc} 2 & 2 & 2 & -12 \\ 0 & 1 & -6 & 10 \\ 3 & 0 & 4 & \end{array}$$

Therefore, $h(x) = \frac{2}{2}x + \frac{2}{2^2} = x + \frac{1}{2}$ and $r(x) = \frac{-12}{2^2}x + \frac{10}{2^2} = -3x + \frac{5}{2}$.

Example 3.2. Let $f(x) = 2x^6 + 4x^5 + 3x^4 + x^3 + 3x + 1$ and $g(x) = 2x^3 + x + 4$.

From Remark 2.1 we have the following array:

$$\begin{array}{cccccc} 2 & 2 & 8 & 8 & -40 & -144 \\ 0 & 4 & 4 & -20 & -72 & 24 \\ 1 & 3 & -6 & -32 & -8 & 176 \\ 4 & 1 & 0 & 3 & 1 & \end{array}$$

Hence, $h(x) = \frac{2}{2}x^3 + \frac{8}{2^2}x^2 + \frac{8}{2^3}x - \frac{40}{24} = x^3 + 2x^2 + x - \frac{5}{2}$ and

$$r(x) = \frac{-144}{2^4}x^2 + \frac{24}{2^4}x + \frac{176}{2^4} = -9x^2 + \frac{3}{2}x + 11.$$

In the following example (see [5]) we show how the presented method can be used to factorize a polynomial.

Example 3.3. Consider the polynomial $f(x) = \sum_{i=0}^{5} c_i x^i$. We apply the presented method to see under what conditions $f(x)$ has a factor of the form $g(x) = x^2 - b$.

$$\begin{array}{cccccc} 1 & c_5 & c_4 & c_3 + bc_5 & c_2 + bc_4 & c_1 + bc_3 + b^2c_5 \\ 0 & c_4 & c_3 + bc_5 & c_2 + bc_4 & c_1 + bc_3 + b^2c_5 & c_1 + bc_3 + b^2c_5 \\ -b & c_3 & c_2 & c_1 & c_0 & \end{array}$$

So, if $c_1 + bc_3 + b^2c_5 = 0$ and $c_1 + bc_3 + b^2c_5 = 0$, then $g(x)$ is a factor of $f(x)$.

References

[1] Binin, D. and Pan, V., 1986, Fast Parallel Algorithm for Polynomial Division over an Arbitrary Field of Constant, *Comp. and Maths with Applications*, 12A(11):1105–1118.

[2] Binin, D. and Pan, V., 1986, Polynomial Division and its computational Complexity, *Journal of complexity 2*, pp 179–203.

[3] Dummit, David S. and Foote, Richard M., 1991, Abstract Algebra, Prentice-Hall International, Inc.

[4] FAN, Lianghuo, 2003, A generalization of Synthetic Division and A general Theorem of Division of Polynomials, *Mathematical Medley*, 30(1):30–37.

[5] Idarraga I., Ricardo A. and Salas, Alvaro H., 2011, A Generalized Factor Theorem, *International Journal of Algebra*, 5(17):809–816.