碩 士 學 位 論 文

Extended Quotient-Remainder Theorem on a Polynomial Ring

濟州大學校 大學院

數 學 科

李 廷 鉉

2012年 11月

Extended Quotient-Remainder Theorem on a Polynomial Ring

指導敎授 宋 錫 準

李 廷 鉉

이 論文을 理學 碩士學位 論文으로 提出함

2012年 11月

李廷鉉의 理學 碩士學位 論文을 認准함

審査委員長 ________________ 印

委 員 ________________ 印

委 員 ________________ 印

濟州大學校 大學院

2012年 11月

Extended Quotient-Remainder Theorem on a Polynomial Ring

Jung Hyun Lee
(Supervised by professor Seok Zun Song)

A thesis submitted in partial fulfillment of the requirement
for the degree of Master of Science

2012. 11.

Department of Mathematics
GRADUATE SCHOOL
CHEJU NATIONAL UNIVERSITY

CONTENTS

<Abstract >

Extended Quotient-Remainder Theorem on a Polynomial Ring

There have been many researches on the polynomial division. With the fast development of computer calculation, the classical problem of a polynomial division with a remainder has been changed to find fast algorithms to computing the coefficients of the quotients $q(x)=\sum_{i=0}^{n-m} q_i x^i$ and of remainder $r(x)=\sum_{i=0}^{m-1} r_i x^i$ on the division of $f(x)=\sum_{i=0}^{n} a_i x^i$ by $g(x)=\sum_{i=1}^{m} b_i x^i$, $n \geq m$. In [3], D. Bini and V. Pan introduced various known polynomial division algorithms(see [2], [4], [5], [8]), and compared them with their new algorithm. From these algorithms, we obtain motivation to consider extended division algorithm of polynomials with related to the remainder theorem.

In this thesis, we shall be interested in the dividing $f(x)$ by $g(x)$ of degree higher than 1. Moreover, we use the determinant of coefficient matrix to obtain extended quotient and remainder theorems in a polynomial ring. The main theorem is the following.

Extended Quotient-Remainder Theorem :

If b_i are all distinct, and we divide $f(x)=a_0+a_1x+a_2x^2+\dots\dots+a_nx^n$ by

$$g(x)=(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots\ (x-b_s)^{m_s},$$ *then we obtain quotient*

$$q(x)=a_nx^{n-m}+r_s(x) \quad \textit{and remainder } r(x)=r_0+\sum_{j=1}^{s-1} r_j(x)\prod_{i=1}^{j}(x-b_j)^{m_i},$$

where $$r_j(x)=\sum_{i=0}^{m_{j+1}-1}\frac{(x-b_{j+1})^i q_j^{(i)}(b_{j+1})}{i!} \quad j=0,1,\cdots,s.$$

Extended Quotient-Remainder Theorem on a Polynomial Ring

1. Introduction and Preliminaries

There have been many researches on the polynomial division. With the fast development of computer calculation, the classical problem of a polynomial division with a remainder has been changed to find fast algorithms to computing the coefficients of the quotients $q(x) = \sum_{i=0}^{n-m} q_i x^i$ and of remainder $r(x) = \sum_{i=0}^{n-1} r_i x^i$ on the dividing $f(x) = \sum_{i=0}^{n} a_i x^i$ by $g(x) = \sum_{i=1}^{m} b_i x^i$, $n \geq m$. In [3], D. Bini and V. Pan introduced various known polynomial division algorithms(see [2], [4], [5], [8]), and compared them with their new algorithm. From these algorithms, we obtain motivation to consider extended division algorithm of polynomials with related to the remainder theorem.

We introduce some definitions and well-known facts.

A *ring* is a nonempty set R with equipped with two binary operations, addition and multiplication, that satisfy the following axioms. For all $a,b,c \in R$:

1. If $a \in R$ and $b \in R$, then $a+b \in R$. [closure for addition]
2. $a+(b+c)=(a+b)+c$. [associative addition]
3. $a+b=b+a$. [commutative addition]

4. There is an element 0_R in R such that $a+0_R=a=0_R+a$ for every $a \in R$. [additive identity or zero element]

5. For each $a \in R$, the equation $a+x = 0_R$ has a solution in R.

6. If $a \in R$ and $b \in R$, then $ab \in R$. [closure for multiplication]

7. $a(bc)=(ab)c$. [associative multiplication]

8. $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$. [distributive laws]

A *commutative ring* is a ring R that satisfies this axiom:

9. $ab=ba$ for all $a,b \in R$.[commutative multiplication]

A *ring with identity* is a ring R that contains an element 1_R satisfying this axiom:

10. $a1_R = a = 1_R a$ a for all $a \in R$. [multiplicative identity]

We have many examples of rings, say $\mathbb{Z}$, the set of integers, $\mathbb{Z}_n$, the set of integers modulo n, $\mathbb{R}$, the set of reals, and so on.

An *integral domain* is a commutative ring with identity $1_R \neq 0_R$ that satisfies this axiom :

11. For each $a, b \in R$, $ab=0$ implies $a=0$ or $b=0$.

A *field* is a commutative ring R with identity $1_R \neq 0_R$ that satisfies this axiom :

12. For each $a \neq 0_R$ in R, the equation $ax=1_R$ has a solution in R.

For examples of field, we have the set of reals, the set of integers modulo prime number p, the set of complex numbers, and so on.

Theorem 1.1 *(The Division Algorithm for Integers) [4] Let* $\mathbb{Z}$ *be a ring of integers. Let a and b be elements in* $\mathbb{Z}$. *Then there exist q and r in* $\mathbb{Z}$ *such that* $a = b \cdot q + r$, *where q is the quotient and r is the remainder with* $0 \leq r < b$.

Definition 1.2 Let F be a field and x be an indeterminate. A polynomial with coefficients in F is an expression of the form $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_n x^n$, where n is a nonnegative integer and $a_i \in F$. The ring of polynomials with coefficients in F will be denoted by $F[x]$, that is

$$F[x] = \{f(x) | f(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n, a_i \in F\}$$

In this polynomial ring, we have the addition of two polynomials
$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots.. + a_n x^n$ and
$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots\ldots + b_m x^m$
as
$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots\ldots + (a_m + b_m)x^m + \ldots\ldots + a_n x^n$,
and the multiplication of them as
$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots\ldots + a_n b_m x^{m+n}$.

Definition 1.3 Let F be a field and x be an indeterminate. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots.. + a_n x^n$ be a polynomial in $F[x]$ with $a_n \neq 0$. Then a_n is called *the leading coefficient* of $f(x)$. The *degree* of $f(x)$ is the integer n; it is denoted "*deg* $f(x)$". The elements of F, considered as polynomials in $F[x]$, are called *constant polynomials*.

In the followings, we denote a field of reals as F.

Theorem 1.4 *(The Division Algorithm in* $F[x]$*)*[4]. *Let* $f(x)$, $g(x) \in F[x]$ *with* $g(x) \neq 0$. *Then there exist unique polynomials* $q(x)$ *and* $r(x)$ *in* $F[x]$ *such that* $f(x) = g(x)q(x) + r(x)$ *and either* $r(x) = 0$ *or deg* $r(x) <$ *deg* $g(x)$.

Definition 1.5 Let $f(x)$, $g(x) \in F(x)$ with $f(x)$ nonzero. We say that $f(x)$ *divides* $g(x)$ [or $f(x)$ is a *factor* of $g(x)$], and write $f(x)|g(x)$, if $g(x) = f(x)h(x)$ for some $h(x) \in F[x]$

Definition 1.6 Let $f(x) \in F[x]$. An element a of F is said to be a *root* of the polynomial $f(x)$ if $f(a)=0$.

Theorem 1.7 *(The Remainder Theorem)*[4] *Let* $f(x) \in F[x]$ *and* $a \in F$. *Then the remainder when* $f(x)$ *is divided by polynomial* $x - a$ *is* $f(a)$.

This theorem says, for example, that the remainder when the polynomial $f(x) = x^3 - 4x^2 + 3x + 5$ is divided by $x - 2$ is $f(2) = 2^3 - 4 \cdot 2^2 + 3 \cdot 2 + 5 = 3$.

Theorem 1.8 *(The Factor Theorem)*[4] *Let* $f(x) \in F[x]$ *and* $a \in F$.

Then a is a root of the polynomial $f(x)$ if and only if $x-a$ is a factor of $f(x)$.

Lemma 1.9 *Let $g_1(x)$ be the polynomial*

$g_1(x)=\frac{1}{b_m}g(x)=\frac{b_0}{b_m}+\frac{b_1}{b_m}x+......+\frac{b_{m-1}}{b_m}x^{m-1}+x^m$. *If we divide $f(x)$ by $g_1(x)$ and $g(x)$ respectively, that is,*

$$f(x)=g_1(x)q_1(x)+r_1(x) \quad \text{and } f(x)=g(x)q(x)+r(x)$$

then the quotients and remainders are related as

$$q_1(x)=b_m q(x) \text{ and } \quad r(x)=r_1(x). \qquad (1.1)$$

Proof. By Theorem 1.4 (the Division Algorithm), there exist a unique $q_1(x)$ and $r_1(x)$ in $F[x]$ such that

$f(x)=g_1(x)q_1(x)+r_1(x)$,

where $r_1(x)=0$ or $\deg r_1(x)<\deg g_1(x)$. Thus

$$f(x)=q_1(x)(\frac{b_0}{b_m}+\frac{b_1}{b_m}x+\frac{b_2}{b_m}x^2+......+\frac{b_{m-1}}{b_m}x^{m-1}+x^m)+r_1(x)$$

$$= q_1(x)\frac{1}{b_m}(b_0+b_1x+b_2x^2+......+b_{m-1}x^{m-1}+b_mx^m)+r_1(x)$$

$$= \{\frac{1}{b_m}q_1(x)\}g(x)+r_1(x)$$

$$= q(x)g(x)+r(x).$$

Therefore $q(x)=\frac{1}{b_m}q_1(x)$ and $r(x)=r_1(x)$. ■

Example 1.10 Let us consider $f(x)=4x^5+3x^4+3x^3+x+5$,

$g(x) = 2x^3 + 4x^2 + 5x + 3$ and $g_1(x) = x^3 + 2x^2 + \frac{5}{2}x + \frac{3}{2}$. Then

$q(x) = 2x^2 - \frac{5}{2}x + \frac{3}{2}$, $r(x) = \frac{1}{2}x^2 + x + \frac{1}{2}$, $q_1(x) = 4x^2 - 5x + 3$

and $r_1(x) = \frac{1}{2}x^2 + x + \frac{1}{2}$. ■

This Lemma 1.9 implies that we may use some monic polynomial $g(x)$ as a divisor on polynomial divisions without loss of generality. So we use the monic polynomial $g(x)$ as a divisor in the following.

In this thesis, we shall be interested in the dividing $f(x)$ by $g(x)$ and use this dividing method to extend the remainder theorem to polynomials $g(x)$ of degree higher than 1. Moreover, we use the determinant of coefficient matrix to obtain extended quotient and remainder theorems in a polynomials ring $F[x]$.

2. The remainder on dividing $f(x)$ by $(x-b)^m$

In this section we give the method for calculating the remainder on dividing $f(x)$ of degree n by the divisor $g(x)$ of degree $m \le n$:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots.. + a_n x^n \qquad (2.1)$$

and

$$g(x) = (x-b)^m. \qquad (2.2)$$

Moreover, we obtain the extended theorem for the Remainder Theorem.

In this section we use the two polynomials $f(x)$, $g(x)$ as in the notation in (2.1) and (2.2), respectively.

Now, Theorem 1.4 (the Division Algorithm in $F[x]$) gives us

$$f(x) = g(x)q(x) + (c_0 + c_1 x + \ldots\ldots + c_{m-1} x^{m-1}) \qquad (2.3)$$

for some $q(x) \in F[x]$ and $c_i \in F$ for $i = 0, 1, \ldots\ldots, \ m-1$.

Let us denote $\frac{d}{dx} f(x) = f^{(1)}(x)$, $\frac{d^2}{dx^2} f(x) = f^{(2)}(x)$, and so on.

If we differentiate $f(x)$ in (2.3) at $x = b$, then we have a system of linear equations of m equations and m unknowns over F as follows :

$$f(b) = c_0 + c_1 b + \ldots\ldots + c_{m-1} b^{m-1}$$

$$f^{(1)}(b) = 0 + c_1 + 2c_2 b + \ldots\ldots + (m-1) c_{m-1} b^{m-2}$$

$$f^{(2)}(b) = 0 + 0 + 2! c_2 + 6 c_3 b + \ldots\ldots + (m-1)(m-2) c_{m-1} b^{m-3}$$

$$f^{(3)}(b) = 0+0+0+3!c_3 + ... + (m-1)(m-2)(m-3)c_{m-1}b^{m-4}$$

....

$$f^{(m-1)}(b) = 0+0+0+ ...... +0+(m-1)!c_{m-1}$$

In order to express this system of m linear equations as a matrix equation, we write

$$C^t = [c_0 \quad c_1 \quad c_2 \quad ...... \quad c_{m-1}], \qquad Y^t = [f(b) \quad f^{(1)}(b) \quad ...... \quad f^{(m-1)}(b)] \tag{2.4}$$

and the coefficient matrix A is the Wronskian matrix

$$A = \begin{pmatrix} 1 & b & b^2 & b^3 & \cdots & b^{m-1} \\ 0 & 1! & 2b & 3b^2 & \cdots & (m-1)b^{m-2} \\ 0 & 0 & 2! & 6b & \cdots & (m-1)(m-2)b^{m-3} \\ \vdots & & & & & \\ 0 & 0 & 0 & 0 & \cdots & (m-1)! \end{pmatrix} \tag{2.5}$$

Then $AC = Y$, that is

$$\begin{pmatrix} 1 & b & b^2 & b^3 & \cdots & b^{m-1} \\ 0 & 1 & 2b & 3b^2 & \cdots & (m-1)b^{m-2} \\ 0 & 0 & 2! & 6b & \cdots & (m-1)(m-2)b^{m-3} \\ \vdots & & & & & \\ 0 & 0 & 0 & 0 & \cdots & (m-1)! \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{m-1} \end{pmatrix} = \begin{pmatrix} f(b) \\ f^{(1)}(b) \\ f^{(2)}(b) \\ \vdots \\ f^{m-1}(b) \end{pmatrix}.$$

Lemma 2.1 *Let* $C = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \ldots & \ldots & \cdots & \ldots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ *and* $D = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & u_1 \\ \ldots & \ldots & \cdots & \ldots & \ldots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & u_n \\ v_1 & v_2 & \ldots & v_n & w \end{pmatrix} = \begin{pmatrix} C & \vec{u} \\ \vec{v}^t & w \end{pmatrix}$,

where $\vec{u} = [u_1 \quad u_2 \quad \ldots \quad u_n]^t$ *and* $\vec{v} = [v_1 \quad v_2 \quad \ldots \quad v_n]^t$.

Then $\det D = -\vec{v}^t \bullet adj\, C \bullet \vec{u} + w \bullet \det C$.

Proof. Expanding $\det D$ from the last row,

$$\det D = \sum_{r=1}^{n} (-1)^{n+1+r} v_r \det \begin{pmatrix} a_{11} & \ldots & a_{1r-1} & a_{1r+1} & \ldots & a_{1n} & u_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nr-1} & a_{nr+1} & \ldots & a_{nn} & u_n \end{pmatrix} + w \det C$$

$$= \sum_{r=1}^{n} (-1)^{n+1+r+(n-r)} v_r \det \begin{pmatrix} a_{11} & \ldots & a_{1r-1} & u_1 & a_{1r+1} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nr-1} & u_n & a_{nr+1} & \ldots & a_{nn} \end{pmatrix} + w \det C \ .$$

Expanding each determinant here from the column containing the u's,

$$\det D = -\sum_{r=1}^{n} v_r \sum_{s=1}^{n} u_s C_{rs} + w det C$$

$$= -(v_1 \ldots v_n) \begin{pmatrix} u_1 C_{11} + u_2 C_{12} + \ldots + u_n C_{1n} \\ \ldots\ldots \\ \ldots\ldots \\ u_1 C_{n1} + u_2 C_{n2} + \ldots + u_n C_{nn} \end{pmatrix} + w \det C$$

$$= -(v_1 \ldots v_n) \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ \ldots & \ldots & \cdots & \ldots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ . \\ . \\ u_n \end{pmatrix} + w \det C \ . \qquad \blacksquare$$

Lemma 2.2 *For the* $f(x)$ *and* $g(x)$*, the remainder on dividing* $f(x)$ *by* $g(x)$ *is* $r(x)=f(x)-\dfrac{\det B}{\det A}$*, where* $B=\begin{pmatrix} A & Y \\ X^t & f(x) \end{pmatrix}$*,* Y *in (2.4),* A *in (2.5) and* $X^t=[1 \quad x \quad \cdots \quad x^{m-1}]$.

Proof. The determinant of B is

$$\det B = -X^t \cdot adj A \cdot Y + f(x) \cdot \det A \tag{2.6}$$

from Lemma 2.1. Since the determinant of A is $0!1!2!\cdots(m-1)! = \prod_{k=0}^{m-1} k! \neq 0$, A is invertible matrix and its inverse is $A^{-1}=\dfrac{1}{\det A} adj A$.

Now, $AC=Y$ implies that $C=A^{-1}Y=\dfrac{1}{\det A} adj A \cdot Y$. Multiply both side by X^t, then we have

$$X^t \frac{1}{\det A} adj A \cdot Y = X^t C = r(x). \tag{2.7}$$

Therefore we have $r(x)=f(x)-\dfrac{\det B}{\det A}$ from (2.6) and (2.7). ■

Now, we calculate the remainder on dividing $f(x)$ by $g(x)$.

Theorem 2.3 *If we write* $f(x)=g(x)q(x)+r(x)$ *then*

$$r(x)=\sum_{i=0}^{m-1} \frac{(x-b)^i f^{(i)}(b)}{i!} \tag{2.8}$$

Proof. From Lemma 2.2, we need to calculate the determinant of the matrix B. Consider the $(m+1)$-square matrix

$$B=\begin{pmatrix} A & Y \\ X^T & f(x)\end{pmatrix}=\begin{pmatrix} 0! & b & b^2 & b^3 & \cdots & b^{m-1} & f^{(0)}(b) \\ 0 & 1! & 2b & 3b^2 & \cdots & (m-1)b^{m-2} & f^{(1)}(b) \\ 0 & 0 & 2! & 6b & \cdots & (m-1)(m-2)b^{m-3} & f^{(2)}(b) \\ 0 & 0 & 0 & 3! & \cdots & (m-1)(m-2)(m-3)b^{m-4} & f^{(3)}(b) \\ \vdots & & & & & & \\ 0 & 0 & 0 & 0 & \cdots & (m-1)! & f^{(m-1)}(b) \\ 1 & x & x^2 & x^3 & \cdots & x^{m-1} & f(x)\end{pmatrix}.$$

In order to obtain $\det B$ we apply the elementary column operations as follows :

Add $(-b)$ times the $(j-1)$-*th* column of B to the j-*th* column from $j=2$ to m, and add $-\frac{1}{i!}f^{(i)}(b)$ times the first column of B to the $(m+1)$-*th* column. And then expand the determinant on the first row. In each step we reduce a common factor in every row out of the determinant. Then after $m-1$ steps we have

$$\det B = 0!1!2!3!\cdots(m-1)!\{f(x)-f^{(0)}(b) - \frac{f^{(1)}(b)}{1!}(x-b) - \frac{f^{(2)}(b)}{2!}(x-b)^2 - \cdots - \frac{1}{(m-1)!}f^{(m-1)}(b)(x-b)^{m-1}\}$$

$$= \prod_{k=0}^{m-1}k!\left\{f(x)-(x-b)^m\sum_{i=0}^{m-1}\frac{f^{(i)}(b)}{i!(x-b)^{m-i}}\right\}.$$

By (2.4), we obtain that

$$r(x)=f(x)-\frac{\det B}{\det A}=f(x)-\frac{1}{1!2!\cdots(m-1)!}[(1!2!3!\cdots(m-1)!)\{f(x)-f^{(0)}(b)$$

$$-\frac{f^{(1)}(b)}{1!}(x-b)-\frac{f^{(2)}(b)}{2!}(x-b)^2-\cdots-\frac{1}{(m-1)!}f^{(m-1)}(b)(x-b)^{m-1}\}\Big]$$

$$=f^{(0)}(b)+\frac{f^{(1)}(b)}{1!}(x-b)+\frac{f^{(2)}(b)}{2!}(x-b)^2+\cdots$$

$$+\frac{1}{(m-1)!}\ f^{(m-1)}(b)(x-b)^{m-1}$$

$$=\sum_{i=0}^{m-1}\frac{1}{i!(x-b)^{m-i}}(x-b)^m f^{(i)}(b)=\sum_{i=0}^{m-1}\frac{(x-b)^i f^{(i)}(b)}{i!} \quad ,$$

which is the required. ■

Example 2.4 For the detailed calculation of the $\det B$ we show the case $m=4$. Let

$$B_4=\begin{pmatrix}1 & b & b^2 & b^3 & f^{(0)}(b)\\ 0 & 1! & 2b & 3b^2 & f^{(1)}(b)\\ 0 & 0 & 2! & 6b & f^{(2)}(b)\\ 0 & 0 & 0 & 3! & f^{(3)}(b)\\ 1 & x & x^2 & x^3 & f(x)\end{pmatrix}.$$

Add $(-b)$times the $(j-1)$th column of B_4 to the jth column from $j=2$ to 4, and $-f^{(0)}(b)$ times the first column of B_4 to the 5th column. Thus

$$\det B_4 = \det\begin{pmatrix}1 & 0 & 0 & 0 & 0\\ 0 & 1! & b & b^2 & f^{(1)}(b)\\ 0 & 0 & 2! & 4b & f^{(2)}(b)\\ 0 & 0 & 0 & 3! & f^{(3)}(b)\\ 1 & x-b & x^2-bx & x^3-bx^2 & f(x)-f^{(0)}(b)\end{pmatrix}.$$

If we expand $\det B_4$ in the 1st row, we get

$$\det B_4 = 1 \cdot \det\begin{pmatrix} 1! & b & b^2 & f^{(1)}(b) \\ 0 & 2! & 4b & f^{(2)}(b) \\ 0 & 0 & 3! & f^{(3)}(b) \\ x-b & x(x-b) & x^2(x-b) & f(x)-f^{(0)}(b) \end{pmatrix}.$$

Similarly, we repeat the above method.

Add $(-b)$times the $(j-1)$column of the above matrix to the jth column from $j=2$ to 3, and $-f^{(1)}(b)$ times the first column to the 4th column :

$$\det B_4 = \det\begin{pmatrix} 1! & 0 & 0 & 0 \\ 0 & 2! & 2b & f^{(2)}(b) \\ 0 & 0 & 3! & f^{(3)}(b) \\ x-b & (x-b)^2 & (x-b)^3 & f(x)-f^{(0)}(b)-f^{(1)}(b)(x-b) \end{pmatrix}.$$

If we expand $\det B_4$ in the 1st row, we get

$$\det B_4 = 1!\det\begin{pmatrix} 2! & 2b & f^{(2)}(b) \\ 0 & 3! & f^{(3)}(b) \\ (x-b)^2 & (x-b)^3 & f(x)-f^{(0)}(b)-f^{(1)}(b)(x-b) \end{pmatrix}.$$

Also, repeat the above method.

Add $(-b)$times the 1st column of above matrix to the 2nd column, and $-\frac{1}{2!}f^{(2)}(b)$times the 1st column to the 3rd column. Then

$$\det B_4 = 1!\det\begin{pmatrix} 2! & 0 & 0 \\ 0 & 3! & f^{(3)}(b) \\ (x-b)^2 & (x-b)^3 & f(x)-f^{(0)}(b)-f^{(1)}(b)(x-b)-\frac{f^{(2)}(b)}{2!}(x-b)^2 \end{pmatrix}.$$

If we expand $\det B_4$ in the 1st row, we get

$$\det B_4 = 1!2!\det\begin{pmatrix} 3! & f^{(3)}(b) \\ (x-b)^3 & f(x)-f^{(0)}(b)-f^{(1)}(b)(x-b)-\dfrac{f^{(2)}(b)}{2!}(x-b)^2 \end{pmatrix}$$

$$= 1!2!3!\left\{f(x)-f^{(0)}(b)-f^{(1)}(b)(x-b)-\frac{f^{(2)}(b)}{2!}(x-b)^2-\frac{1}{3!}f^{(3)}(b)(x-b)^3\right\}$$

which is the required value in the proof of Theorem 2.3. ■

3. The quotient on dividing $f(x)$ by $(x-b)^m$

In this section we give the method for calculating the quotient on dividing $f(x)$ of degree n by the divisor $g(x)$ of degree $m \leq n$:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots.. + a_n x^n \qquad (3.1)$$

and

$$g(x) = (x-b)^m . \qquad (3.2)$$

Moreover, we obtain the extended theorem for the Remainder Theorem.

In this section we use the two polynomials $f(x)$, $g(x)$ as in the notation in (3.1) and (3.2), respectively.

Lemma 3.1 *For a given f(x), we have a unique expression as*

$$f(x) = c_0 + c_1(x-b) + c_2(x-b)^2 + \cdots + c_n(x-b)^n \qquad (3.3)$$

with $c_i \in F$, $i = 0, 1, \cdots, n$.

Proof. By the Theorem 1.4 (the division algorithm in $F[x]$) with $g(x) = x-b$, we obtain the unique quotient $q_1(x)$ of degree $n-1$, and the unique remainder c_0 in F such that

$$f(x) = (x-b)q_1(x) + c_0 \ .$$

Similarly we get

$$q_1(x) = (x-b)q_2(x) + c_1 \ ,$$

where the unique quotient $q_2(x)$ in $F[x]$ is of degree $n-2$, and the unique remainder is c_1 in F.

Continuing this process, we have

$$q_{n-2}(x) = (x-b)q_{n-1}(x) + c_{n-2} \text{ and } q_{n-1}(x) = (x-b)q_n(x) + c_{n-1} \ ,$$

where deg $q_n(x) = 0$, and the unique $c_{n-2,} \quad c_{n-1} \in F$.

Let $q_n(x) = c_n$, which is a constant in F. Then combining these equations by backward substitution, we obtain the required formula

$$f(x) = c_n(x-b)^n + c_{n-1}(x-b)^{n-1} + \cdots + c_1(x-b) + c_0 \ ,$$

where each c_i is the unique constant in F. ■

Theorem 3.2 *If we divide $f(x)$ by $g(x)$, then the quotient is*

$$q(x) = a_n(x-b)^{n-m} + \sum_{i=0}^{n-m-1} \frac{f^{(m+i)}b}{(m+1)!}(x-b)^i \ . \qquad (3.4)$$

Proof. Let $h(x) = g(x)(x-b)^{n-m} = (x-b)^n$. Using Theorem 2.3, the remainder on dividing $f(x)$ by $h(x)$ is

$$r_h(x) = \sum_{i=0}^{n-1} \frac{(x-b)^i f^{(i)}(b)}{i!}. \qquad (3.5)$$

From (3.3), we have the unique expression

$$f(x) = c_0 + c_1(x-b) + c_2(x-b)^2 + \cdots + c_m(x-b)^m + \cdots + c_n(x-b)^n \qquad (3.6)$$

and $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Thus we have

$$c_n = a_n \qquad (3.7)$$

From (3.6), we have $f(x) = a_n h(x) + r_h(x)$,

where $r_h(x) = c_0 + c_1(x-b) + \cdots + c_{n-1}(x-b)^{n-1}$, which is the same as the value in (3.5) by the uniqueness of the remainder. Thus we obtain

$$c_i = \frac{f^{(i)}(b)}{i!} \quad . \qquad (3.8)$$

where $i = 0, 1, \cdots, n-1$.

Now, we also have the following form from (3.6)

$$\begin{aligned} f(x) &= \left\{c_m(x-b)^m + \cdots + c_{n-1}(x-b)^{n-1} + a_n(x-b)^n\right\} \\ &\quad + \left\{c_0 + c_1(x-b) + \cdots + c_{m-1}(x-b)^{m-1}\right\} \\ &= \left\{c_m + \cdots + c_{n-1}(x-b)^{n-m-1} + a_n(x-b)^{n-m}\right\}(x-b)^m \\ &\quad + \left\{c_0 + c_1(x-b) + \cdots + c_{m-1}(x-b)^{m-1}\right\} \end{aligned}$$

$$= q(x)g(x) + r(x),$$

where $r(x) = c_0 + c_1(x-b) + \cdots + c_m(x-b)^{m-1}$ and

$$q(x) = c_m + \cdots + c_{n-1}(x-b)^{n-m-1} + a_n(x-b)^{n-m} \tag{3.9}$$
$$= a_n(x-b)^{n-m} + \sum_{i=0}^{n-m-1} c_{m+i}(x-b)^i$$

Substituting each c_i in (3.9) by the value in (3.8), we have

$$q(x) = a_n(x-b)^{n-m} + \sum_{i=1}^{n-m-1} \frac{f^{(m+i)}(b)}{(m+i)!}(x-b)^i. \qquad \blacksquare$$

Corollary 3.3 (The Quotient Theorem) *If we divide $f(x)$ by $(x-b)$, then the quotient is*

$$q(x) = a_n(x-b)^{n-1} + \sum_{i=0}^{n-2} \frac{f^{(i+1)}(b)}{(i+1)!}(x-b)^i.$$

Proof. In the above Theorem 3.2, we replace m by 1 to obtain the result. ■

Corollary 3.4 *For a polynomial $f(x)$, we have a unique expression*

$$f(x) = \frac{f(b)}{0!} + \frac{f^{(1)}(b)}{1!}(x-b) + \cdots + \frac{f^{(n-1)}(b)}{(n-1)!}(x-b)^{n-1} + a_n(x-b)^n$$

$$= a_n(x-b)^n + \sum_{j=0}^{n-1} \frac{f^{(j)}(b)}{j!}(x-b)^j.$$

Proof. In the equation (3.3), we replace all c_i $(i=1, \cdots, n-1)$ the value in (3.8) and $c_n = a_n$ from (3.6). This expression is the Taylor Expansion for polynomials in $F[x]$.

4. The remainders on dividing $f(x)$ by the factors of $(x-b_1)^{m_1}(x-b_2)^{m_2}....(x-b_s)^{m_s}$

In this section we obtain an expression of $f(x)$ by the factors of $(x-b_1)^{m_1}(x-b_2)^{m_2}....(x-b_s)^{m_s}$ of degree $m=m_1+m_2+ ...... +m_s$ for positive integers m_i , where

$$f(x)=a_0+a_1x+a_2x^2+.....+a_nx^n \quad . \tag{4.1}$$

Theorem 4.1 *If* $n \le m_1+m_2+\cdots+m_s=m$, *and* b_i *are all distinct reals for* $i=1,\cdots,s$, *then there exists unique expression of* $f(x)$ *as follows :*

$$f(x)=r_0(x)+r_1(x)(x-b_1)^{m_1}+r_2(x)(x-b_1)^{m_1}(x-b_2)^{m_2}+\cdots \quad (4.2)$$
$$+r_s(x)(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_s)^{m_s}.$$

where $r_j(x)=\sum_{i=0}^{m_{j+1}-1}\frac{(x-b_{j+1})^i q_j^{(i)}(b_{j+1})}{i!}$, $j=0,1, \cdots, s.$

Proof. If we divide $f(x)$ by $(x-b_1)^{m_1}$, then we have the form $f(x)=(x-b_1)^{m_1}q_1(x)+r_0(x)$ for some $q_1(x)$ of *deg* $n-m_1$ and $r_0(x)$ of degree m_1-1 or less. Using Theorem 2.3 and 3.2, we obtain

$$r_0(x)=\sum_{i=0}^{m_1-1}\frac{(x-b_1)^i q_0^{(i)}(b_1)}{i!} \tag{4.3}$$

and

$$q_1(x) = a_n(x-b_1)^{n-m_1} + \sum_{i=0}^{n-m_1-1} \frac{q_0^{(m_1+i)}(b_1)}{(m_1+i)}(x-b_1)^i \quad . \tag{4.4}$$

Now, if we divide $q_1(x)$ by $(x-b_2)^{m_2}$, then we have the form $q_1(x) = (x-b_2)^{m2} q_2(x) + r_1(x)$ for some $q_2(x)$ of *deg* $n-m_1-m_2$ and $r_1(x)$ of degree m_2-1 or less. Using Theorem 2.3 and 3.2, we obtain

$$r_1(x) = \sum_{i=1}^{m_2-1} \frac{(x-b_2)^i q_1^{(i)}(b_2)}{i!} \tag{4.5}$$

and

$$q_2(x) = a_n(x-b_2)^{n-m_1-m_2} \quad + \sum_{i=0}^{n-m_1-m_2-1} \frac{q_1^{(m_1+i)}(b_2)}{(m_2+i)!}(x-b_2)^i . \tag{4.6}$$

Since $n \leq m$, there exists k, with 1≤k≤s, such that this proceed may stop at $k-2$ steps yielding

$$q_{k-2}(x) = (x-b_{k-1})^{m_{k-1}} q_{k-1}(x) + r_{k-2}(x) \tag{4.7}$$

$$q_{k-1}(x) = (x-b_k)^{m_k} q_k(x) + r_{k-1}(x), \tag{4.8}$$

where

$$r_j(x) = \sum_{i=0}^{m_{j+1}-1} \frac{(x-b_{j+1})^i q_j^{(i)}(b_{j+1})}{i!} \tag{4.9}$$

and

$$q_j(x) = a_n(x-b_j)^{n-m_1-\cdots-m_j} + \sum_{i=0}^{n-m_1-m_2-\cdots-m_j-1} \frac{q_{j-1}^{(m_j+i)}(b_j)}{(m_j+i)!}(x-b_j)^i. \quad (4.10)$$

for $j=1,2,\cdots,k$. Moreover, we have deg $q_k(x) < m_{k+1}$. So $q_k(x) = (x-b_{k+1})^{m_{k+1}} \bullet 0 + r_k(x)$ and hence

$$r_k(x) = q_k(x), \quad (4.11)$$

and define $r_{k+1}(x) = \cdots = r_s(x) = 0$.

Now, substituting (4.11) into (4.8), substituting (4.8) into (4.7), and so on, we have

$$f(x) = r_0(x) + (x-b_1)^{m_1}(x-b_2)^{m_2} q_2(x) + r_1(x)$$

$$= r_0(x) + r_1(x)(x-b_1)^{m_1} + (x-b_1)^{m_1}(x-b_2)^{m_2} q_2(x)$$

$= \cdots$

$$= f(x) = r_0(x) + r_1(x)(x-b_1)^{m_1} + r_2(x)(x-b_1)^{m_1}(x-b_2)^{m_2} + \cdots$$

$$+ r_s(x)(x-b_1)^{m_1}(x-b_2)^{m_2} \cdots (x-b_s)^{m_s},$$

which is the equation (4.2). In each step, the remainder $r_j(x)$ were determined uniquely. ■

Example 4.2 In order to show the justification of the result in Theorem 4.1, consider

$$f(x) = x^8 - 2x^7 - 4x^6 + 8x^5 + 5x^4 - x^3 - 10x^2 - 12x - 3 \text{ and}$$

$$g(x) = (x-1)^3(x+1)^2(x-2)(x+2)^3.$$

To find the unique expression of $f(x)$ by the factors of $g(x)$, we apply the method of the Theorem 4.1. Then

$$
\begin{aligned}
f(x) &= r_0(x) + r_1(x)(x-2) + r_2(x)(x-2)(x+1)^2 + r_3(x)(x-2)(x+1)^2(x-1)^3 \\
&\quad + r_4(x)(x+2)^3(x-2)(x+1)^2(x-1)^3 \\
&= 5 + (2x+3)(x-2) + (x^2+2x+2)(x-2)(x+1)^2 \\
&\quad + (x^2+x+1)(x-2)(x+1)^2(x-1)^3 + 0 \cdot (x+2)^3(x-2)(x+1)^2(x-1)^3
\end{aligned}
$$

where $r_4(x)=0$ $\deg r_3(x) = \deg(x^2+x+1)$, $\deg r_2(x) = (x^2+2x+2) = 2$, $\deg r_1(x) = \deg(2x+3) = 1$ and $\deg r_0(x) = \deg 5 = 0$. ■

5. Extended Quotient-Remainder Theorem

In this section we give the extended quotient-remainder theorem on dividing $f(x)$ of degree n by the divisor $g(x)$ of degree $m \leq n$ such that:

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \qquad (5.1)$$

and

$$g(x) = (x - b_1)^{m_1}(x - b_2)^{m_2} \cdots (x - b_s)^{m_s}, \qquad (5.2)$$

with $m = m_1 + m_2 + ... + m_s$.

Throughout this section, we use the two polynomials $f(x)$, $g(x)$ as in the equations in (5.1) and (5.2), respectively.

Theorem 5.1 (Extended Quotient-Remainder Theorem) *If b_i are all distinct, and we divide $f(x)$ by $g(x)$, then we obtain the quotient*

$q(x) = a_n x^{n-m} + r_s(x)$ *and the remainder*

$$r(x) = r_0 + \sum_{j=1}^{s-1} r_j(x) \prod_{i=1}^{j} (x - b_j)^{m_i}, \qquad (5.3)$$

where $r_j(x) = \sum_{i=0}^{m_{j+1}-1} \frac{(x - b_{j+1})^i q_j^{(i)}(b_{j+1})}{i!}$, $j = 0, 1, \cdots, s$.

Proof. Let $g_1(x)=(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_s)^{m_s}(x-0)^{m_s+1}$, with $m_{s+1}=n-m$ and $m=m_1+m_2+\dots\dots+m_s$. Then by Theorem 4.1 we obtain the unique expression of $f(x)$ as follows :

$$f(x)=r_0(x)+r_1(x)(x-b_1)^{m_1}+r_2(x)(x-b_1)^{m_1}(x-b_2)^{m_2}+\cdots$$
$$+r_s(x)(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_s)^{m_s}$$
$$+r_{s+1}(x)(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_s)^{m_s}(x-0)^{m_s+1}\ , \qquad (5.4)$$

where $r_j(x)=\sum_{i=0}^{m_{j+1}-1}\frac{(x-b_{j+1})^i q_j^{(i)}(b_{j+1})}{i!}$ with $j=0,1,\cdots,s.$

Since $\deg f(x)=n=m+m_{s+1}=\sum_{i=1}^{s+1}m_i$, we have the leading coefficient of $f(x)$ must be $r_{s+1}(x)$, which is a_n.

From (5.4), let us express the quotient and the remainder differently according to the degree as follows:

$$f(x)=\{r_s(x)(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_s)^{m_s}$$
$$+a_n(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_s)^{m_s}(x-0)^{n-m}\}$$
$$+\{r_0(x)+r_1(x)(x-b_1)^{m_1}+r_2(x)(x-b_1)^{m_1}(x-b_2)^{m_2}+$$
$$\cdots+r_{s-1}(x)(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_{s-1})^{m_{s-1}}\}$$

$$=\{r_s(x)+a_nx^{n-m}\}\{(x-b_1)^{s_1}(x-b_2)^{s_2}\cdots(x-b_s)^{m_s}\}$$

$$+\left\{r_0(x)+r_1(x)(x-b_1)^{m_1}+\cdots+r_{s-1}(x)\prod_{i=1}^{s-1}(x-b_i)^{m_i}\right\}$$

$$=q(x)g(x)+r(x).$$

Thus we have quotient $q(x)=a_n x^{n-m}+r_s(x)$, and the remainder $r(x)=r_0(x)+\sum_{j=1}^{s-1} r_j(x)\prod_{i=0}^{j}(x-b_i)^{m_i}$. ■

Example 5.2 In order to find the unique quotient and remainder by the method in the proof of Theorem 5.1, consider

$f(x)=4x^8-11x^7-2x^6+29x^5-4x^4-31x^3-20x^2-11x-2$ and
$g(x)=(x+1)^2(x-2)(x+2)^3$.

To find the unique quotient and remainder of the division $f(x)\div g(x)$, we apply the method of the Theorem 5.1. Then

$$\begin{aligned} f(x)&=r_0(x)+r_1(x)(x-2)+r_2(x)(x-2)(x+1)^2 \\ &\quad+(4x^2+r_3(x))(x-2)(x+1)^2(x-1)^3 \\ &=5+(2x+3)(x-2)+(x^2+2x+2)(x-2)(x+1)^2 \\ &\quad+(4x^2+x+1)(x-2)(x+1)^2(x-1)^3, \end{aligned}$$

where $a_8=4$, $r_3(x)=x+1$, $r_2(x)=x^2+2x+2$, $r_1(x)=2x+3$ and $r_0(x)=5$. Thus the quotient is $a_n x^{n-m}+r_3(x)=4x^2+x+1$, the remainder is $5+(2x+3)(x-2)+(x^2+2x+2)(x-2)(x+1)^2$. ■

5. References

[1] H. Anton, Elementrary Linear Algebra(9th), John Wiley & Sons, Inc. Korean translation, ISBN 89-7129-175-3, 2005.

[2] D. Bini, Parallel solution of certain Toeplitz linear systems, SIAM J. Comput. 13(2) (1984), 268-276.

[3] D. Bini and V. Pan, Polynomial division and its computational complexity, Journal of Complexity 2 (1986), 179-203.

[4] A. Borodin, S. Cook and N. Pippenger, Parallel computation for well-endowed rings and space-bounded prababilistic machines, Information and Control 58 (1983), 113-116.

[5] A. Bordin, J. Gathen and J. Hopcroft, Fast parallel matrix and GCD computations, Information and Control 53 (1982), 241-256.

[6] R. A. Horn and C. R. Johnson, Matrix Analysis, Cambridge University Press, Cambridge, ISBN 0-521-38632-2, 1985.

[7] T. W. Hungerford, Abstract Algebra (2nd), Saunders College Publishing, New York, London, Tokyo, ISBN 0-03-010559-5, 1997.

[8] A. Schonhage, Asymtotically fast algorithm for the numerical multiplications and division of polynomials with complex coefficients, Proceedings, EUROCAM, Marseille (1982).

<國文抄錄>

多項式 環에서 확장된 몫과 나머지 定理

多項式의 나눗셈에 대한 硏究는 매우 많다. 컴퓨터 計算의 빠른 발달로 인하여, 多項式 나눗셈의 전통적인 問題는 $f(x)=\sum_{i=0}^{n} a_i x^i$를 $g(x)=\sum_{i=1}^{m} b_i x^i (n \geq m)$로 나눌 때 몫 $q(x)=\sum_{i=0}^{k-1} q_i x^i$ 와 나머지 $r(x)=\sum_{i=0}^{n-1} r_i x^i$ 의 係數들을 구하기 위한 빠른 計算方法을 찾는 問題로 변화되고 있다. 參考文獻 [3]에서 D. Bini와 V. Pan은 參考文獻 [2], [4], [6], [8] 들에서 硏究되어 알려진 여러 가지 나눗셈 計算方法을 소개하고 자신들이 개발한 計算方法과 比較分析하였다. 이러한 나눗셈 計算方法들로부터 나머지 定理와 관련된 多項式의 확장된 나눗셈 計算方法을 硏究할 動機를 얻었다. 곧 1차식인 $g(x)$를 m차의 多項式 $(x-b)^m$으로 나눗셈 定理의 확장을 시도하여 몫과 나머지를 計算하였다. 더욱이 $g(x)$를 $(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_s)^{m_s}$으로 더 확장하여 몫과 나머지를 구하는 理論을 정립하고 이를 行列式의 計算法으로 證明하였다. 核心定理는 다음과 같다.

확장된 몫과 나머지 定理

모든 b_i들이 서로 다를 때 $f(x)=a_0+a_1x+a_2x^2+.....+a_nx^n$ *를* $g(x)=(x-b_1)^{m_1}(x-b_2)^{m_2}\cdots(x-b_s)^{m_s}$*로 나누면 몫은* $q(x)=a_nx^{n-m}+r_s(x)$*이고, 나머지는* $r(x)=r_0+\sum_{j=1}^{s-1} r_j(x)\prod_{i=1}^{j}(x-b_j)^{m_i}$ *이며, 여기서* $j=1, 2, ..., s$*에 대하여* $r_j(x) = \sum_{i=0}^{m_{j+1}-1} \frac{(x-b_{j+1})^i q_j^{(i)}(b_{j+1})}{i!}$ *이다.*

감사의 글

수학이 좋아서 깊이 있는 학문 연구를 통해 나 자신을 발전시키고자 대학원에 입학하였습니다. 그러나 학문의 난해함과 환경의 어려움까지 겹쳐 중간에 포기하고 싶은 마음도 많았습니다. 그렇지만 이미 시작한 일을 어렵다고 해서 포기하는 모습을 자녀와 가르치는 학생들에게 보이고 싶지 않았습니다. 열심히 하다보면 모든 것이 좋아지리라 긍정적으로 생각하면서 조금씩 극복하고 나아가다 보니 어느새 석사학위 과정을 마치게 되었습니다.

지나간 시간 속에서 저를 도와주셨던 감사한 분들이 생각납니다.

우선 항상 배려해주시고 세심하고 꼼꼼하게 논문을 지도해주신 송석준 교수님께 감사의 말씀을 전하고 싶습니다. 그리고 양영오교수님, 방은숙교수님, 정승달교수님, 윤용식교수님, 진현성교수님, 유상욱교수님, 강경태박사님께 감사의 마음을 드립니다. 교수님들의 훌륭한 가르침은 마음에 잘 간직하겠습니다.

같은 연구실을 쓰며 즐겁게 지냈던 동생들 나영, 승표, 수산, 현아, 재우에게 그동안 세대차가 나는 나를 편안하게 대해주고 모임에도 항상 불러줘서 고맙다고 말하고 싶습니다.

또한 선수과목을 공부하며 학우의 정을 나누게 된 미현이와 은별이는 밤이건 새벽이건 가리지 않고 풀리지 않는 문제들을 같이 고민하고 연구해주는 좋은 멘토였습니다.

팔순을 바라보시는 고령에도 딸을 위해 항상 기도하시고 격려해 주시는 사랑하는 부모님과 며느리가 공부하는 것을 흔쾌히 허락하고 지지해주셨던 며칠전 소천하신 그리운 시어머님께도 깊은 감사의 말씀을 전합니다.

학업에 전념하는 동안 아이들 양육과 가사의 많은 부분을 도와준 나의 남편 강영수선생에게 감사와 사랑과 존경의 마음을 드립니다. 엄마가 잘 챙겨주지 못했지만 자기 일을 스스로 잘 감당해준 자랑스런 딸 효정이와 잔병치레 없이 씩씩하게 자라준 귀여운 아들 예성이에게도 엄마가 많이 사랑하고 고마워한다고 말하고 싶습니다.

마지막으로 좋은 사람들과 만날 수 있도록 만남의 축복을 주시고 무사히 석사학위 과정을 마칠 수 있도록 지혜와 건강을 주신 하나님 아버지께 감사와 영광을 올립니다.