สมาชิกของริงที่สอดคล้องกับการหารลงตัวบางรูปแบบ
The Element of a Ring Satisfying some Divisibility

ญาณภัทร ทองร่อน[1] *สุภัทรา เกิดมงคล*[1] *นิติภูมิ อัศวธิติสกุล*[1] *วราภรณ์ สุ่มมาตย์*[2]
และกัญญาภัค ภัยแคล้ว[1*]

Yanapat Tongron[1]*, Supattra Kerdmongkon*[1]*, Nitiphoom Adsawatithisakul*[1]*, Waraporn Summart*[2]
and Kanyaphak Paikhlaew[1*]

รับบทความ 2 สิงหาคม 2566/ ปรับแก้ไข 6 มกราคม 2567/ ตอบรับบทความ 6 มิถุนายน 2567
Received: August 2, 2023/ Revised: January 6, 2024/ Accepted: June 7, 2024

บทคัดย่อ

กำหนดให้ R เป็นริงสลับที่ที่มีเอกลักษณ์ 1 และ $m \geq n$ เราสนใจหา $d \in R$ ที่สอดคล้องเงื่อนไขสองข้อต่อไปนี้

1. $(bx^n - b) \mid (ax^m + d)$ ถ้า $b \mid a$ และ
2. $(bx^n - 1) \mid (ax^m + d)$ ถ้า $b^k \mid a$

โดยที่ k คือผลหารจากการหาร m ด้วย n และ $a, b \in R$ สมาชิก $d \in R$ ที่สอดคล้องกับเงื่อนไข 1 คือ $d = (bx^n - b)e - ax^{m-kn}$ และสมาชิก $d \in R$ ที่สอดคล้องกับเงื่อนไข 2 คือ $d = (bx^n - 1)e - cx^{m-kn}$ สำหรับทุก $e \in R$

คำสำคัญ : ริงสลับที่ที่มีเอกลักษณ์ การหารลงตัว การหารยาว

Abstract

Let R be a commutative ring with identity 1 and $m \geq n$. We are interested in establish $d \in R$ satisfying each of the following two conditions:

1. $(bx^n - b) \mid (ax^m + d)$ if $b \mid a$ and
2. $(bx^n - 1) \mid (ax^m + d)$ if $b^k \mid a$,

where k is the quotient from dividing m by n and $a, b \in R$. The element $d \in R$ satisfying the condition 1 is $d = (bx^n - b)e - ax^{m-kn}$, while the element $d \in R$ satisfying the condition 2 is $d = (bx^n - 1)e - cx^{m-kn}$ for any $e \in R$.

Keywords: Commutative ring with identity, Divisibility, Long division

[1] Department of Mathematics, Faculty of Science and Technology, Nakhon Ratchasima Rajabhat University, Nakhon Ratchasima 30000, Thailand.

[2] General Education Affair, Thonburi University, Bangkok 10160, Thailand.

* Corresponding Author: kanyaphak.p@nrru.ac.th

Introduction

Recently in 2022, a team of students enrolling in Mathematical mini-Project contest of Nakhon Ratchasima Rajabhat University Science Week, Thailand, introduces us a way to find the smallest positive integer k satisfying that $2^x - 1$ divides $2^y + k$ with only condition that x and y are positive integers. They solve the problem by long division of polynomials (Stitz & Zeager, 2013) as follows:

$$
\begin{array}{r|llllll}
 & 2^{y-x} & +2^{y-2x} & +2^{y-3x} & +\cdots & +2^{y-nx} & \\ \hline
2^x - 1 & 2^y & & & & & +k \\
 & 2^y & -2^{y-x} & & & & \\ \cline{2-3}
 & & 2^{y-x} & & & & \\
 & & 2^{y-x} & -2^{y-2x} & & & \\ \cline{3-4}
 & & & 2^{y-2x} & & & \\
 & & & 2^{y-2x} & -2^{y-3x} & & \\ \cline{4-5}
 & & & & \vdots & \vdots & \\ \cline{5-6}
 & & & & & 2^{y-(n-1)x} & \\
 & & & & & 2^{y-(n-1)x} & -2^{y-nx} \\ \cline{6-7}
 & & & & & & 2^{y-nx} \quad +k
\end{array}
$$

for some unknown n. In other word, they prove that

$$2^y + k = (2^x - 1)(2^{y-x} + 2^{y-2x} + 2^{y-3x} + \cdots + 2^{y-nx}) + (2^{y-nx} + k)$$

and reach the conclusion that the smallest positive integer k satisfying that $2^x - 1$ divides $2^y + k$ is of the form

$$k = 2^x - 1 - 2^{y-nx}.$$

Although they confusingly write and present the proof or reason, their idea is quite interesting. This motivates us to study their idea in a commutative ring with an identity. An element a of a commutative ring R is divisible by another element $b \in R$ if (Durbin, 2009; Lovett, 2015; Malik et al., 1997) there exists $c \in R$ such that $a = bc = cb$. One also says that b divides a and a is said to be a multiple of b, while b is a divisor of a. The divisibility of a by b is denoted by the symbol $b \mid a$. In this paper, we determine the element d of a commutative ring R with identity 1 satisfying each condition: For and $a, b \in R$,

1. $(bx^n - b) \mid (ax^m + d)$ if $b \mid a$ and
2. $(bx^n - 1) \mid (ax^m + d)$ if $b^k \mid a$,

where $m \geq n$ and k is the quotient from dividing m by n. See (Durbin, 2009; Malik et al., 1997) for more information about ring

Main Results

Let a, b, c, d be elements in a commutative ring R with identity 1 such that $a = bc$ and m, n be nonnegative integers so that $m \geq n$. By Division Algorithm (Burton, 2011; Niven et al., 1991), there exists unique nonnegative integer k and l with $0 \leq l < n$ such that

$$m = kn + l.$$

Consider the following long division for polynomials:

$$
\begin{array}{r|llllll}
 & cx^{m-n} & +cx^{m-2n} & +cx^{m-3n} & +\cdots & +cx^{m-kn} & \\
\hline
bx^n - b & ax^m & & & & & +d \\
 & ax^m & -ax^{m-n} & & & & \\
\cline{2-3}
 & & ax^{m-n} & & & & \\
 & & ax^{m-n} & -ax^{m-2n} & & & \\
\cline{3-4}
 & & & ax^{m-2n} & & & \\
 & & & ax^{m-2n} & -ax^{m-3n} & & \\
\cline{4-5}
 & & & & \vdots & \vdots & \\
\cline{5-6}
 & & & & & ax^{m-(k-1)n} & \\
 & & & & & ax^{m-(k-1)n} & -ax^{m-kn} \\
\cline{6-7}
 & & & & & & ax^{m-kn} \quad +d \\
\end{array}
$$

Then

$$ax^m + d = (bx^n - b)(cx^{m-n} + cx^{m-2n} + \cdots + cx^{m-kn}) + (ax^{m-kn} + d).$$

This implies that $(bx^n - b) \mid (ax^m + d)$ if and only if $(bx^n - b) \mid (ax^{m-kn} + d)$. The following theorem is a consequence of this fact:

Theorem 1. Let a, b, d be elements in a commutative ring R with identity 1 such that $b \mid a$ and m, n be nonnegative integers so that $m \geq n$. If k is the quotient from dividing m by n, then
$(bx^n - b) \mid (ax^m + d)$ if and only if $d = (bx^n - b)e - ax^{m-kn}$
for any $e \in R$.

The following two corollaries is derived from Theorem 1 when $n \mid m$ and $b = 1$, respectively.

Corollary 2. Let a, b, d be elements in a commutative ring R with identity 1 such that $b \mid a$ and m, n be nonnegative integers so that $n \mid m$. Then

$(bx^n - b) \mid (ax^m + d)$ if and only if $d = (bx^n - b)e - a$

for any $e \in R$.

Corollary 3. Let a, d be elements in a commutative ring R with identity 1 and m, n be nonnegative integers so that $m \geq n$. If k is the quotient from dividing m by n, then

$(x^n - 1) \mid (ax^m + d)$ if and only if $d = (x^n - 1)e - ax^{m-kn}$

for any $e \in R$.

Observe from Corollary 3 that if we put $R = \mathbb{Z}$ (the set of all integers), $a = 1$, $x = 2$, and $e = 1$, then we have

$d = 2^n - 1 - 2^{m-kn}$ implies $(2^n - 1) \mid (2^m + d)$.

This is as same as the result of those students.

Now assume further that $a = b^k c$. Consider the following long division for polynomials:

$$
\begin{array}{r|llllll}
 & b^{k-1}cx^{m-n} & +b^{k-2}cx^{m-2n} & +b^{k-3}cx^{m-3n} & +\cdots & +cx^{m-kn} & \\
\hline
bx^n - 1 & ax^m & & & & & +d \\
 & ax^m & -b^{k-1}cx^{m-n} & & & & \\
\cline{2-3}
 & & b^{k-1}cx^{m-n} & & & & \\
 & & b^{k-1}cx^{m-n} & -b^{k-2}cx^{m-2n} & & & \\
\cline{3-4}
 & & & b^{k-2}cx^{m-2n} & & & \\
 & & & b^{k-2}cx^{m-2n} & -b^{k-3}cx^{m-3n} & & \\
\cline{4-5}
 & & & & \vdots & \vdots & \\
\cline{5-6}
 & & & & & bcx^{m-(k-1)n} & \\
 & & & & & bcx^{m-(k-1)n} & -cx^{m-kn} \\
\cline{6-7}
 & & & & & & cx^{m-kn} \quad +d \\
\end{array}
$$

Then

$$ax^m + d = (bx^n - 1)(b^{k-1}cx^{m-n} + b^{k-2}cx^{m-2n} + \cdots + cx^{m-kn}) + (cx^{m-kn} + d).$$

This implies that $(bx^n - 1) \mid (ax^m + d)$ if and only if $(bx^n - 1) \mid (cx^{m-kn} + d)$. The following theorem is a consequence of this fact:

Theorem 4. Let a, b, d be elements in a commutative ring R with identity 1 and m, n be nonnegative integers so that $m \geq n$. If k is the quotient from dividing m by n and $b^k \mid a$, then $a = b^k c$ for some $c \in R$ and so

$$(bx^n - 1) \mid (ax^m + d) \text{ if and only if } d = (bx^n - 1)e - cx^{m-kn}$$

for any $e \in R$.

Note that $b = 1$ in Theorem 4 implies Corollary 3. The following corollary is derived from Theorem 4 when $n \mid m$.

Corollary 5. Let a, b, d be elements in a commutative ring R with identity 1 and m, n be nonnegative integers so that $n \mid m$. If $b^{m/n} \mid a$, then $a = b^{m/n}c$ for some $c \in R$ and so

$$(bx^n - 1) \mid (ax^m + d) \text{ if and only if } d = (bx^n - 1)e - c$$

for any $e \in R$.

Examples

This section shows examples related to our main results.

Example 6. Consider the commutative ring $\mathbb{Z}$ of all integers with identity 1.

(i) Put $a = 4, b = 2, n = 3, m = 5$, and $e = 1$ in Theorem 1. Then $k = 1$ and so

$$d = (2x^3 - 2) - 4x^2 \text{ implies } (2x^3 - 2) \mid (4x^5 + d).$$

If $x = 2$, then $d = -2$ and

$$4x^5 + d = 126 = (14)9 = (2x^3 - 2)9.$$

(ii) Put $a = 9, b = 3, n = 2, m = 6$, and $e = 2$ in Corollary 2. Then

$$d = (3x^2 - 3)2 - 9 \text{ implies } (3x^2 - 3) \mid (9x^6 + d).$$

If $x = -3$, then $d = 39$ and

$$9x^6 + d = 6600 = (24)275 = (3x^3 - 3)275.$$

(iii) Put $a = 10, n = 4, m = 14$, and $e = 3$ in Corollary 3. Then $k = 3$ and so

$$d = (x^4 - 1)3 - 10x^2 \text{ implies } (x^4 - 1) \mid (10x^{14} + d).$$

If $x = 4$, then $d = 605$ and

$$10x^{14} + d = 2684355165 = (255)10526883 = (x^4 - 1)10526883.$$

(iv) Put $a = 12, b = 2, n = 3, m = 7$, and $e = 1$ in Theorem 4. Then $k = 2, b^k = 4$, and so

$$d = (2x^3 - 1) - 3x \text{ implies } (2x^3 - 1) \mid (12x^7 + d).$$

If $x = -2$, then $d = -11$ and

$$12x^7 + d = -1547 = (-17)91 = (2x^3 - 1)91.$$

(v) Put $a = 81, b = 3, n = 2, m = 6$, and $e = 2$ in Corollary 5. Then $b^{m/n} = 27$ and so

$$d = (3x^2 - 1)2 - 3 \text{ implies } (3x^2 - 1) \mid (81x^6 + d).$$

If $x = 1$, then $d = 1$ and

$$81x^6 + d = 82 = (2)41 = (3x^2 - 1)41.$$

In addition to the example of the commutative ring $\mathbb{Z}$, we also apply our results on the unfamiliar ring $(\mathcal{P}(X),\triangle,\cap)$. Let $\mathcal{P}(X)$ be the power set of a set X. Define the addition $\triangle$ on $\mathcal{P}(X)$ by

$$A \triangle B = (A - B) \cup (B - A)$$

for any $A, B \in \mathcal{P}(X)$ and define the multiplication $\cap$ as a usual intersection of sets. It is not hard to see that $(\mathcal{P}(X),\triangle,\cap)$ is a commutative ring with identity X. We also observe that

1. the zero element of $\mathcal{P}(X)$ is $\emptyset$,
2. the additional inverse of $A \in \mathcal{P}(X)$ is also A itself,
3. for $A, B \in \mathcal{P}(X)$, $B \mid A$ if and only if $A = B \cap C$ for some $C \in \mathcal{P}(X)$ if and only if $A \subseteq B$, and
4. for $A \in \mathcal{P}(X)$,

$$A^n = \overbrace{A \cap A \cap \cdots \cap A}^{n \text{ terms}} = A \text{ for any positive integer } n.$$

These facts yield the following two corollary deduced from the Theorem 1 and Theorem 4, respectively:

Corollary 7. Let A, B, D, x be elements in $(\mathcal{P}(X),\triangle,\cap)$ such that $A \subseteq B$. Then

$$A \cap x \triangle D \subseteq B \cap x \triangle B \text{ if and only if } D = (B \cap x \triangle B) \cap E \triangle A \cap x$$

for any $E \in \mathcal{P}(X)$.

Corollary 8. Let A, B, D, x be elements in $(\mathcal{P}(X),\triangle,\cap)$ such that $A \subseteq B$. Then $A = B \cap C$ for some $C \in \mathcal{P}(X)$ and so

$$A \cap x \triangle D \subseteq B \cap x \triangle X \text{ if and only if } D = (B \cap x \triangle X) \cap E \triangle C \cap x$$

for any $e \in R$.

Example 9. Denote the set I_n for a positive integer n by $I_n = \{1,2,3, \dots, n\}$.

(i) Put $X = I_9$, $A = \{1,2,3\}$, $B = \{1,2,3,5\}$, and $E = \{1\}$ in Corollary 7. Then

$$D = (\{1,2,3,5\} \cap x \triangle \{1,2,3,5\}) \cap \{1\} \triangle \{1,2,3\} \cap x \text{ implies}$$
$$\{1,2,3\} \cap x \triangle D \subseteq \{1,2,3,5\} \cap x \triangle \{1,2,3,5\}.$$

If $x = \{5\}$, then $D = \{1\}$ and

$$\{1,2,3\} \cap x \triangle D = \{1\} \subseteq \{1,2,3\} = \{1,2,3,5\} \cap x \triangle \{1,2,3,5\}.$$

(ii) Put $X = I_{40}$, $A = \{10,11,12, \dots ,20\}$, $B = \{10,11,12, \dots ,30\}$, $e = \{10,11,12, \dots ,15\}$ in Corollary 8. Then $A = B \cap \{10,11,12, \dots ,20,35,40\}$ and so

$$D = (\{10,11, \dots ,30\} \cap x \triangle I_{40}) \cap \{10,11, \dots ,15\} \triangle \{10,11, \dots ,20,35,40\} \cap x$$

implies

$$\{10,11, \dots ,20\} \cap x \triangle D \subseteq \{10,11, \dots ,30\} \cap x \triangle I_{40}.$$

If $x = \{20,30,40\}$, then $D = \{10,11, \dots ,15,20,40\}$ and

$$\{10,11, \dots ,20\} \cap x \triangle D = \{10,11, \dots ,15,40\} \subseteq I_{40} - \{20,30\} = \{10,11, \dots ,30\} \cap x \triangle I_{40}.$$

Example 10. Let $\mathbb{R}$ denote the set of all real numbers and $\mathbb{N}$ denote the set of all positive integers.

(i) Put $X = \mathbb{R}$, $A = [20,30)$, $B = [10, \infty)$, and $E = (0,10)$ in Corollary 7. Then

$$D = \big([10, \infty) \cap x \triangle [10, \infty)\big) \cap (0,10) \triangle [20,30) \cap x \text{ implies}$$
$$[20,30) \cap x \triangle D \subseteq [10, \infty) \cap x \triangle [10, \infty).$$

If $x = (25,35]$, then $D = (25,30)$ and

$$[20,30) \cap (25,35] \triangle (25,30) = \emptyset \subseteq [10,25] \cup (35, \infty) = [10, \infty) \cap (25,35] \triangle [10, \infty).$$

(ii) Put $X = \mathbb{R}$, $A = \mathbb{N}$, $B = \mathbb{Z}$, and $E = \mathbb{N} \cup \{0\}$ in Corollary 8. Then $A = B \cap \mathbb{R}^+$, where $\mathbb{R}^+$ is the set of all positive real numbers, and so

$$D = (\mathbb{Z} \cap x \triangle \mathbb{R}) \cap (\mathbb{N} \cup \{0\}) \triangle \mathbb{R}^+ \cap x \text{ implies}$$
$$\mathbb{N} \cap x \triangle D \subseteq \mathbb{Z} \cap x \triangle \mathbb{R}.$$

If $x = (-1,1]$, then $D = \mathbb{N} - \{1\}$ and

$$\mathbb{N} \cap (-1,1] \triangle \mathbb{N} - \{1\} = \mathbb{N} - \{1\} \subseteq \mathbb{R} - \{0,1\} = \mathbb{Z} \cap (-1,1] \triangle \mathbb{R}.$$

Conclusions

Let a, b, d be elements in a commutative ring R with identity 1 and m, n be nonnegative integers so that $m \geq n$. Assume that k is the quotient from dividing m by n. Then we obtain the following two main results:

(i) If $b \mid a$, then

$$(bx^n - b) \mid (ax^m + d) \text{ if and only if } d = (bx^n - b)e - ax^{m-kn}$$

for any $e \in R$.

(ii) If $b^k \mid a$, then $a = b^k c$ for some $c \in R$ and so

$$(bx^n - 1) \mid (ax^m + d) \text{ if and only if } d = (bx^n - 1)e - cx^{m-kn}$$

for any $e \in R$.

References

Burton D. M., (2011). *Elementary Number Theory.* New York: The McGraw-Hill Companies, Inc.

Durbin J. R. (2009). *Modern Algebra: An Introduction* (6th ed). New York: The University of Texas at Austin. John Wiley & Sons, Inc.

Lovett S. (2015). *Abstract Algebra: Structures and Applications.* New York: Chapman and Hall/CRC.

Malik D. S., Mordeson John M. and Sen M. K. (1997). *Fundamentals of abstract algebra.* New York: The McGraw-Hill Companies, Inc.

Niven I., Zuckerman H. S. and Montgomery H. L. (1991). *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons, Inc.

Stitz C. and Zeager J. (2013). *College Algebra.* Retrieved Oct 10, 2022, from https://www.stitz-zeager.com/szca07042013.pdf.