ขั้นตอนวิธีแบบยุคลิด : วิธีการแบบเมทริกซ์

Euclidean Algorithm : Matrix Method

ประพจน์ อนันตวรพจน์ วท.บ. (คณิตศาสตร์)
Prapoj Anantaworapot B.Sc. (Mathematics)
นิสิต ป.บัณฑิต มหาวิทยาลัยทักษิณ
Graduate Student, Thaksin University.

สมใจ จิตพิทักษ์ วท.ม. (คณิตศาสตร์) กศ.ด. (พัฒนศึกษาศาสตร์)
Somjai Jitpitak M.Sc. (Mathematics) Ed.D. (Dev. Ed.)
รองศาสตราจารย์ ภาควิชาคณิตศาสตร์ มหาวิทยาลัยทักษิณ
Assoc. Prof. Department of Mathematics, Thaksin University.

1. บทนำ

การหาตัวหารร่วมมากของจำนวนเต็มสองจำนวน a และ b ที่ไม่เป็นศูนย์พร้อมกัน ด้วยวิธีการแบบเมทริกซ์ (matrix method) เริ่มด้วย

$$\left[\begin{array}{cc:c} 1 & 0 & a \\ 0 & 1 & b \end{array}\right]$$

โดยใช้วิธีการดำเนินการตามแถวเบื้องต้น (elementary row operations: ERO) สามารถที่จะหาตัวหารร่วมมาก (a, b) และเขียน (a, b) เป็นผลรวมเชิงเส้นได้จากเมทริกซ์ที่เศษตัวสุดท้ายไม่เป็นศูนย์ โดยผลลัพธ์ที่ได้จะอยู่ในรูปของ (a, b) = r = ax +by สำหรับ x, y และ r เป็นจำนวนเต็มบางค่า นอกจากนี้มีการใช้โปรแกรมภาษาซีช่วยในการวิเคราะห์ในการหาตัวหารร่วมมาก ตลอดจนผลรวมเชิงเส้นของจำนวนเต็มสองจำนวน

2. พื้นฐานความรู้

ในการศึกษาเรื่องขั้นตอนวิธีแบบยุคลิด : วิธีการแบบเมทริกซ์ เป็นเรื่องที่เกี่ยวข้องกับการหาตัวหารร่วมมากและผลรวมเชิงเส้นของจำนวนเต็มสองจำนวน จึงจำเป็นที่จะต้องใช้บทนิยามและทฤษฎีบทที่เกี่ยวข้องเพื่อเป็นประโยชน์ในการศึกษาและเป็นแนวทางในการพิสูจน์ ดังต่อไปนี้

บทนิยาม 2.1 ให้ a และ b เป็นจำนวนเต็มโดยที่ $b \neq 0$ และถ้ามีจำนวนเต็ม c ที่ทำให้ $a = bc$ แล้วเรากล่าวว่า b **หาร** a **ลงตัว** (b divides a) และจะเขียนด้วย $b \mid a$ ถ้า b **หาร** a **ไม่ลงตัว** จะเขียนด้วย $b \nmid a$

ทฤษฎีบท 2.2 ขั้นตอนวิธีการหาร (Division Algorithm) ให้ a และ b เป็นจำนวนเต็ม โดยที่ $b > 0$ จะได้ว่ามีจำนวนเต็ม q และ r คู่หนึ่งและคู่เดียวที่

$$a = bq + r,\ 0 \leq r < b$$

จำนวนเต็ม q และ r เรียกว่า **ผลลัพธ์หรือผลหาร** (quotient) และ**เศษหรือเศษเหลือ** (remainder) ตามลำดับที่ได้จากการหาร a ด้วย b

บทแทรก 2.3 ถ้า a และ b เป็นจำนวนเต็ม โดยที่ $b \neq 0$ จะได้ว่ามีจำนวนเต็ม q และ r คู่หนึ่งและคู่เดียวเท่านั้นที่

บทนิยาม 2.4 ให้ a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกัน **ตัวหารร่วมมาก** (greatest common divisor) ของ a และ b เขียนแทนด้วย (a, b) คือ จำนวนเต็มบวก d ซึ่งมีสมบัติต่อไปนี้

1. $d \mid a$ และ $d \mid b$
2. ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$

บทนิยาม 2.5 ให้ a และ b เป็นจำนวนเต็มซึ่งต่างไม่เท่ากับศูนย์ ถ้า $(a, b) = 1$ เรากล่าวว่า a และ b เป็น **จำนวนเฉพาะสัมพัทธ์** (relatively prime)

ทฤษฎีบท 2.6 ให้ a และ b เป็นจำนวนเต็ม โดยที่ a และ b ไม่เป็นศูนย์พร้อมกันจะได้ว่า มีจำนวนเต็ม x และ y ที่

$$(a, b) = ax + by$$

ทฤษฎีบท 2.7 ให้ a และ b เป็นจำนวนเต็มซึ่งต่างไม่เท่ากับศูนย์ จะได้ว่า a และ b เป็นจำนวนเฉพาะสัมพัทธ์ก็ต่อเมื่อมีจำนวนเต็ม x และ y ที่ $1 = ax + by$

ทฤษฎีบท 2.8 สมการไดโอแฟนไทน์เชิงเส้น $ax + by = c$ มีรากก็ต่อเมื่อ $d \mid c$ โดยที่ $d = (a, b)$ ถ้า x_0, y_0 เป็นรากเฉพาะรากหนึ่งแล้วรากทั่วไปจะอยู่ในรูป

$$x = x_0 + (b / d)t,\quad y = y_0 - (a / d)t$$

โดยที่ t เป็นจำนวนเต็มใดๆ

ทฤษฎีบท 2.9 ถ้า $a = bq + r$ แล้ว $(a,b) = (b,r)$

การพิสูจน์ ให้ $d = (a,b)$ และ $d' = (b,r)$ จาก $d \mid a$ และ $d \mid b$ จะได้ $d \mid (a - qb)$ นั่นคือ $d \mid r$ ดังนั้น $d \mid d'$ จาก $d' \mid b$ และ $d' \mid r$ จะได้ $d' \mid (qb + r)$ นั่นคือ $d' \mid a$ ดังนั้น $d' \mid d$ เพราะฉะนั้น $d' = d$ นั่นคือ $(a,b) = (b,r)$ □

เมทริกซ์และระบบสมการเชิงเส้น

กำหนดระบบสมการเชิงเส้นที่มี m สมการ และมีตัวแปร n ตัว คือ $x_1, x_2, \ldots, x_n$ ดังนี้

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \vdots \quad & \quad \vdots \quad \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned} \tag{1}$$

ระบบสมการเชิงเส้นนี้มีความสัมพันธ์กับเมทริกซ์ดังนี้ สมมติให้

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \quad X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

จะพบว่า

$$AX = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \vdots \quad \quad \vdots \quad \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = B$$

ดังนั้น ระบบสมการเชิงเส้น (1) สามารถเขียนให้อยู่ในรูปสมการของเมทริกซ์ A, X และ B ได้ดังนี้

$$AX = B \tag{2}$$

โดยที่เมทริกซ์ A, X และ B มีชื่อเรียกดังนี้ A เรียกว่า **เมทริกซ์สัมประสิทธิ์** (coefficient matrix) X เรียกว่า **เมทริกซ์ตัวแปร** (variable matrix) และ B เรียกว่า **เมทริกซ์ค่าคงตัว** (constant matrix)

ต่อไป การหาคำตอบของระบบสมการเชิงเส้น (1) จะพิจารณาสมการของเมทริกซ์ (2) แทนเมทริกซ์ที่มีส่วนสำคัญในการหาคำตอบของระบบสมการเชิงเส้นอีกหนึ่งเมทริกซ์คือ เมทริกซ์ที่เกิดจาก A และ B ซึ่งเรียกว่า **เมทริกซ์แต่งเติม** (augmented matrix) เขียนแทนด้วยสัญลักษณ์ $[A \mid B]$ ซึ่งนิยามดังนี้

$$[A \mid B] = \left[\begin{array}{cccc:c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right] \quad (3)$$

การแก้ระบบสมการ เราจะใช้การดำเนินการตามแถวเบื้องต้น (elementary row operations:ERO) กับเมทริกซ์แต่งเติม ดังนี้

1. การคูณแถวใดแถวหนึ่งของเมทริกซ์แต่งเติมด้วยค่าคงตัวที่ไม่เป็นศูนย์ (cR_i)
2. การสลับระหว่างแถวสองแถวของเมทริกซ์แต่งเติม ($R_i \leftrightarrow R_j$)
3. การบวกแถวหนึ่งของเมทริกซ์แต่งเติมด้วยผลคูณของแถวอื่นกับค่าคงตัว ($R_i + cR_j$)

โดยใช้การดำเนินการตามแถวเบื้องต้น จากเมทริกซ์ (3) จะได้

$$[A' \mid B'] \quad (4)$$

ซึ่งเมทริกซ์ (4) สมมูลกับเมทริกซ์ (3) เขียนแทนด้วย

$$[A \mid B] \leftrightarrow [A' \mid B'] \quad (5)$$

และสมการของเมทริกซ์

$$A'X = B' \quad (6)$$

สมมูลกับ $AX = B$ นั่นคือมีรากชุดเดียวกัน

3. ผลลัพธ์หลัก

ก่อนอื่นจะกล่าวถึงขั้นตอนวิธีแบบยุคลิด (Euclidean Algorithm) ซึ่งจะมีการนำไปใช้บางส่วนในวิธีการแบบเมทริกซ์ โดยจะเริ่มต้นด้วยการ ให้ a และ b เป็นจำนวนเต็มสองจำนวนที่ต้องการหาตัวหารร่วมมาก เนื่องจาก $(|a|, |b|) = (a,b)$ และ $(a,b) = (b,a)$ จึงไม่เป็นการเสียนัยทั่วไปที่จะสมมติให้ $a \geq b > 0$ เริ่มโดยใช้ขั้นตอนวิธีการหารเข้ากับ a และ b จะได้

$$a = bq_1 + r_1 \ , \ 0 \leq r_1 < b$$

สำหรับจำนวนเต็ม q_1 และ r_1 บางค่า ถ้า $r_1 = 0$ หยุด จะได้ $b \mid a$ และ $(a, b) = b$
ถ้า $r_1 \neq 0$ หาร b ด้วย r_1 โดยขั้นตอนวิธีการหารจะมีจำนวนเต็ม q_2 และ r_2 บางค่าที่

$$b = r_1q_2 + r_2 \ , \ 0 \leq r_2 < r_1$$

ถ้า $r_2 = 0$ เราหยุดเพียงแค่นี้ แต่ถ้า $r_2 \neq 0$ เราทำต่อทำนองเดียวกับข้างต้น จะได้

$$r_1 = r_2q_3 + r_3 \ , \ 0 \leq r_3 < r_2$$

ทำกระบวนการนี้ต่อเนื่องไปจนกระทั่งได้เศษเป็นศูนย์ (เศษเป็นศูนย์จะต้องเกิดขึ้นอย่างแน่นอน เพราะ $b > r_1 > r_2 > \ldots \geq 0$) สมมติว่าได้เศษเป็นศูนย์ในขั้นที่ $n+1$:

$$\begin{aligned}
a &= bq_1 + r_1, & 0 \leq r_1 < b \\
b &= r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned}$$

เราจะแสดงว่า เศษตัวสุดท้ายที่ไม่เป็นศูนย์ ในที่นี้คือ r_n เป็นตัวหารร่วมมากของ a และ b การพิสูจน์ข้อความดังกล่าวอาศัยทฤษฎีบท 2.9 ได้ว่า จากระบบสมการดังกล่าวข้างต้นเราจะได้

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n$$

นั่นคือตัวหารร่วมมากของ a และ b คือ เศษตัวสุดท้ายที่ไม่เท่ากับศูนย์ในขั้นตอนวิธีแบบยุคลิด

จากทฤษฎีบท 2.6 (a, b) สามารถเขียนได้เป็นผลรวมเชิงเส้นในรูป $ax + by$ ซึ่งเราสามารถหาค่า x และ y ได้โดยการย้อนกลับไปดูขั้นตอนวิธีแบบยุคลิดและใช้กระบวนการทำย้อนกลับจากบรรทัดรองสุดท้ายในขั้นตอนวิธีดังกล่าวเราได้

$$r_n = r_{n-2} - q_n r_{n-1}$$

ต่อไปหา r_{n-1} จากสมการที่ถัดขึ้นไปแล้วแทนค่าลงในสมการข้างต้นนี้ จะได้

$$\begin{aligned}
r_n &= r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) \\
&= (1 + q_n q_{n-1}) r_{n-2} + (- q_n) r_{n-3}
\end{aligned}$$

ซึ่งจะได้ว่า r_n เป็นผลรวมเชิงเส้นของ r_{n-2} และ r_{n-3} ทำกระบวนการย้อนกลับแบบเดียวกับข้างต้นจนถึงสมการแรก ในที่สุดเราสามารถขจัดเศษ $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$ ทีละขั้นจนกระทั่งได้ $r_n = (a, b)$ เป็นผลรวมเชิงเส้นของ a และ b :

$$r_n = (a, b) = ax + by$$

สำหรับจำนวนเต็ม x, y บางค่า

ตัวอย่าง 3.1 ในการหา (507,391) และเขียนเป็นผลรวมเชิงเส้นของ 507 และ 391 โดยขั้นตอนวิธีการหาร เราจะได้ระบบสมการ

$$507 = 391 \cdot 1 + 116$$
$$391 = 116 \cdot 3 + 43$$
$$116 = 43 \cdot 2 + 30$$
$$43 = 30 \cdot 1 + 13$$
$$30 = 13 \cdot 2 + 4$$
$$13 = 4 \cdot 3 + 1$$
$$4 = 1 \cdot 4 + 0$$

เศษตัวสุดท้ายในที่นี้คือ 1 ดังนั้น 1 เป็นตัวหารร่วมมากของ 507 และ 391 นั่นคือ $1 = (507,391)$

ในการเขียน 1 เป็นผลรวมเชิงเส้นของ 507 และ 391 เราเริ่มจากบรรทัดรองสุดท้ายในระบบสมการข้างต้นและขจัดเศษ 4, 13, 30, 43, 116 ทีละขั้น จะได้

$$\begin{aligned}
1 &= 13 - 4 \cdot 3 \\
&= 13 - 3(30 - 13 \cdot 2) \\
&= 7 \cdot 13 - 3 \cdot 30 \\
&= 7(43 - 30 \cdot 1) - 3 \cdot 30 \\
&= 7 \cdot 43 - 10 \cdot 30 \\
&= 7 \cdot 43 - 10(116 - 43 \cdot 2) \\
&= 27 \cdot 43 - 10 \cdot 116 \\
&= 27(391 - 116 \cdot 3) - 10 \cdot 116 \\
&= 27 \cdot 391 - 91 \cdot 116 \\
&= 27 \cdot 391 - 91(507 - 391 \cdot 1) \\
&= 118 \cdot 391 - 91 \cdot 507
\end{aligned}$$

ดังนั้น $1 = (507,391) = 507x + 391y$ โดยที่ $x = -91$ และ $y = 118$

กระบวนการวิธีการแบบเมทริกซ์

ให้ a และ b เป็นจำนวนเต็มสองจำนวนที่ต่างไม่เท่ากับศูนย์ที่ต้องการหาตัวหารร่วมมาก โดยเริ่มที่เมทริกซ์

$$\left[\begin{array}{cc:c} 1 & 0 & a \\ 0 & 1 & b \end{array}\right]$$

สมมติ ให้ $a \geq b > 0$ จากทฤษฎีขั้นตอนวิธีการหาร จะมีจำนวนเต็ม q_1 และ r_1 ที่ $a = bq_1 + r_1$ โดยที่ $0 \leq r_1 < b$ นำ $-q_1$ คูณแถว R_2 บวกกับแถว R_1 นั่นคือ แถวที่ 1 เปลี่ยนเป็น $R_1 + (-q_1) R_2$ ดังนั้น จะได้ $r_1 = a - bq_1$ และได้เมทริกซ์ที่สมมูลกันคือ

$$\begin{bmatrix} 1 & -q_1 & \vdots & r_1 \\ 0 & 1 & \vdots & b \end{bmatrix}$$

ถ้า $r_1 = 0$ หยุด จะได้ $(a, b) = b$ และผลรวมเชิงเส้นคือ $ax + by = b$ $(x = 0, y = 1)$ ถ้า $r_1 \neq 0$ จากทฤษฎีขั้นตอนวิธีการหาร จะมีจำนวนเต็ม q_2 และ r_2 ที่ $b = r_1 q_2 + r_2$ โดยที่ $0 \leq r_2 < r_1$ นำ $-q_2$ คูณแถว R_1 บวกกับแถว R_2 นั้นคือ แถวที่ 2 เปลี่ยนเป็น $R_2 + (-q_2) R_1$ ดังนั้น จะได้ $r_2 = b - r_1 q_2$ และได้เมทริกซ์ที่สมมูลกันคือ

$$\begin{bmatrix} 1 & -q_1 & \vdots & r_1 \\ -q_2 & 1 + q_1 q_2 & \vdots & r_2 \end{bmatrix}$$

ถ้า $r_2 = 0$ หยุดเพียงแค่นี้ จะได้ว่า $(b, r_1) = r_1$ และผลรวมเชิงเส้นคือ $ax + by = r_1$ $(x = 1, y = -q_1)$ ถ้า $r_2 \neq 0$ จากทฤษฎีขั้นตอนวิธีการหาร จะมีจำนวนเต็ม q_3 และ r_3 ที่ $r_1 = r_2 q_3 + r_3$ โดยที่ $0 \leq r_3 < r_2$ นำ $-q_3$ คูณแถว R_2 บวกกับแถว R_1 นั้นคือ แถวที่ 1 เปลี่ยนเป็น $R_1 + (-q_3) R_2$ ดังนั้น จะได้ $r_3 = r_1 - r_2 q_3$ และได้เมทริกซ์ที่สมมูลกันคือ

$$\begin{bmatrix} 1 + q_2 q_3 & -q_1 & -q_3 (1 + q_1 q_2) & \vdots & r_3 \\ -q_2 & & 1 + q_1 q_2) & \vdots & r_2 \end{bmatrix}$$

ทำกระบวนการนี้ต่อเนื่องไปจนกระทั่งได้เศษเป็นศูนย์ (เศษเป็นศูนย์จะต้องเกิดขึ้นอย่างแน่นอน เพราะ $b > r_1 > r_2 > \ldots \geq 0$) สมมติว่าได้เศษเป็นศูนย์ในขั้นที่ $n + 1$: ให้

$$M_1 = \begin{bmatrix} 1 & 0 & \vdots & a \\ 0 & 1 & \vdots & b \end{bmatrix} = \begin{bmatrix} 1 & 0 & \vdots & bq_1 + r_1 \\ 0 & 1 & \vdots & b \end{bmatrix}$$

จะได้

$R_1 + (-q_1) R_2$

$$M_1 \leftrightarrow M_2 = \begin{bmatrix} 1 & -q_1 & \vdots & r_1 \\ 0 & 1 & \vdots & b \end{bmatrix} = \begin{bmatrix} 1 & -q_1 & \vdots & r_1 \\ 0 & 1 & \vdots & r_1 q_2 + r_2 \end{bmatrix}$$

$R_2 + (-q_2) R_1$

$$M_2 \leftrightarrow M_3 = \begin{bmatrix} 1 & -q_1 & \vdots & r_1 \\ -q_2 & 1 + q_1 q_2 & \vdots & r_2 \end{bmatrix} = \begin{bmatrix} 1 & -q_1 & \vdots & r_2 q_3 + r_3 \\ -q_2 & 1 + q_1 q_2 & \vdots & r_2 \end{bmatrix}$$

$\vdots$

$R_1 + (-q_{n-1}) R_2$

$$M_{n-2} \leftrightarrow M_{n-1} = \begin{bmatrix} x_{n-1} & y_{n-1} & \vdots & r_{n-1} \\ x_{n-2} & y_{n-2} & \vdots & r_{n-2} \end{bmatrix} = \begin{bmatrix} x_{n-1} & y_{n-1} & \vdots & r_{n-1} \\ x_{n-2} & y_{n-2} & \vdots & r_{n-1} q_n + r_n \end{bmatrix}$$

$R_2 + (-q_n) R_1$

$$M_{n-1} \leftrightarrow M_n = \begin{bmatrix} x_{n-1} & y_{n-1} & \vdots & r_{n-1} \\ x_n & y_n & \vdots & r_n \end{bmatrix} = \begin{bmatrix} x_{n-1} & y_{n-1} & \vdots & r_n q_{n+1} + 0 \\ x_n & y_n & \vdots & r_n \end{bmatrix}$$

$R_1 + (-q_{n+1}) R_2$

$$M_n \leftrightarrow M_{n+1} = \begin{bmatrix} x_{n+1} & y_{n+1} & \vdots & 0 \\ x_n & y_n & \vdots & r_n \end{bmatrix}$$

สำหรับ $x_{n+1}, x_n, x_{n-1}, y_{n+1}, y_n, y_{n-1}$ เป็นจำนวนเต็มบางค่า

ดังนั้น จากขั้นตอนวิธีแบบยุคลิด ถ้าเศษเป็นศูนย์ในขั้นที่ n + 1 จะได้ว่า ตัวหารร่วมมากของ a และ b คือเศษตัวสุดท้ายที่ไม่เป็นศูนย์ ในที่นี้ คือ (r_n) จากเมทริกซ์

$$\left[\begin{array}{cc|c} x_{n+1} & y_{n+1} & 0 \\ x_n & y_n & r_n \end{array}\right]$$

เราสามารถเขียน r_n เป็นผลรวมเชิงเส้นของ a และ b ได้ดังนี้

$$ax_n + by_n = r_n$$

โดยที่ $r_n = (a, b)$ และ x_n, y_n เป็นจำนวนเต็มบางค่า

ตัวอย่าง 3.2 ในการหา (507,391) และเขียนเป็นผลรวมเชิงเส้นของ 507 และ 391 เราเริ่มจาก

$$M_1 = \left[\begin{array}{cc|c} 1 & 0 & 507 \\ 0 & 1 & 391 \end{array}\right]$$

จะได้ว่า

$R_1 + (-1)R_2$
$M_1 \leftrightarrow M_2 = \left[\begin{array}{cc|c} 1 & -1 & 116 \\ 0 & 1 & 391 \end{array}\right]$

$R_2 + (-3)R_1$
$M_2 \leftrightarrow M_3 = \left[\begin{array}{cc|c} 1 & -1 & 116 \\ -3 & 4 & 43 \end{array}\right]$

$R_1 + (-2)R_2$
$M_3 \leftrightarrow M_4 = \left[\begin{array}{cc|c} 7 & -9 & 30 \\ -3 & 4 & 43 \end{array}\right]$

$R_2 + (-1)R_1$
$M_4 \leftrightarrow M_5 = \left[\begin{array}{cc|c} 7 & -9 & 30 \\ -10 & 13 & 13 \end{array}\right]$

$R_1 + (-2)R_2$
$M_5 \leftrightarrow M_6 = \left[\begin{array}{cc|c} 27 & -35 & 4 \\ -10 & 13 & 13 \end{array}\right]$

$R_2 + (-3)R_1$
$M_6 \leftrightarrow M_7 = \left[\begin{array}{cc|c} 27 & -35 & 4 \\ -91 & 118 & 1 \end{array}\right]$

$$R_1 + (-4)\,R_2 \qquad \begin{bmatrix} 391 & -507 & 0 \\ -91 & 118 & 1 \end{bmatrix}$$
$$M_7 \leftrightarrow M_8 \quad =$$

เศษตัวสุดท้ายในที่นี้คือ 1 ดังนั้น 1 เป็นตัวหารร่วมมากของ 507 และ 391 และเขียน 1 เป็นผลรวมเชิงเส้นของ 507 และ 391 ได้ว่า

$$507 \cdot (-91) + 391 \cdot (118) = 1$$

เมื่อเราทราบวิธีการหาตัวหารร่วมมากและผลรวมเชิงเส้น ด้วยวิธีการแบบเมทริกซ์แล้ว ต่อไปเราจะนำผลลัพธ์ทั้งสองผลลัพธ์นี้ ไปประยุกต์สู่สมการไดโอแฟนไทน์ $ax + by = c$ เพื่อที่จะหารากทั่วไปของสมการไดโอแฟนไทน์เชิงเส้น

ตัวอย่าง 3.3 ในการหารากทั่วไปของสมการไดโอแฟนไทน์เชิงเส้น

$$172x + 20y = 1000$$

โดยใช้วิธีการแบบเมทริกซ์ หา $(172,20)$ โดยให้

$$M_1 = \begin{bmatrix} 1 & 0 & 172 \\ 0 & 1 & 20 \end{bmatrix}$$

จะได้

$$R_1 + (-8)\,R_2 \qquad \begin{bmatrix} 1 & -8 & 12 \\ 0 & 1 & 20 \end{bmatrix}$$
$$M_1 \leftrightarrow M_2 \quad =$$

$$R_2 + (-1)\,R_1 \qquad \begin{bmatrix} 1 & -8 & 12 \\ -1 & 9 & 8 \end{bmatrix}$$
$$M_2 \leftrightarrow M_3 \quad =$$

$$R_1 + (-1)\,R_2 \qquad \begin{bmatrix} 2 & -17 & 4 \\ -1 & 9 & 8 \end{bmatrix}$$
$$M_3 \leftrightarrow M_4 \quad =$$

$$R_2 + (-2)\,R_1 \qquad \begin{bmatrix} 2 & -17 & 4 \\ -5 & 43 & 0 \end{bmatrix}$$
$$M_4 \leftrightarrow M_5 \quad =$$

ดังนั้น $(172,20) = 4$ เนื่องจาก $4 \mid 1000$ สมการที่ให้มาหารากได้ เขียน 4 เป็นผลรวมเชิงเส้นของ 172 และ 20 ได้ว่า

$$172 \cdot (2) + 20 \cdot (-17) = 4$$

คูณความสัมพันธ์นี้ด้วย 250 เราได้

$$1000 = 172 \cdot (500) + 20 \cdot (-4250)$$

ดังนั้น $x = 500$ และ $y = -4250$ เป็นรากเฉพาะรากหนึ่ง สำหรับรากทั่วไปจะเขียนได้ในรูป

$$x = 500 + \left(\frac{20}{4}\right)t = 500 + 5t$$

$$y = -4250 - \left(\frac{172}{4}\right)t = -4250 - 43t$$

เมื่อ t เป็นจำนวนเต็มใดๆ

ในบางครั้งเราต้องการหารากที่เป็นบวกนั่นคือ ต้องการ $x > 0$ และ $y > 0$ ในกรณีนี้ต้องหา t ที่สอดคล้องกับอสมการ

$$x_0 + \left(\frac{b}{d}\right)t > 0, \qquad y_0 - \left(\frac{a}{d}\right)t > 0$$

จากตัวอย่าง 3.3 ถ้าต้องการหารากที่เป็นจำนวนบวก เราต้องหา t ที่สอดคล้องกับอสมการ

ซึ่งพบว่า $-98.8 > t > -100$ เพราะฉะนั้นสมการมีรากที่เป็นบวกเพียงรากเดียวคือ $x = 5, y = 7$ ที่ สมนัยกับ $t = -99$

มีข้อที่ควรสังเกตอีกอย่างหนึ่งคือ แนวคิดของตัวหารร่วมมากสามารถขยายไปยังกรณีที่มีจำนวนเต็มมากกว่าสองจำนวนได้ ในกรณีที่มีจำนวนเต็มสามจำนวนกล่าวคือ a, b และ c ที่ต่างไม่เท่ากับศูนย์ **ตัวหารร่วมมาก** (a, b, c) ให้นิยามเป็นจำนวนเต็มบวก d ที่มีสมบัติดังต่อไปนี้

(1) d เป็นตัวหารของ a, b และ c

(2) ถ้า e เป็นตัวหารใดๆ ของ a, b และ c แล้ว $e \mid d$

ตัวอย่างเช่น

$(39, 42, 54) = 3$, $(49, 210, 350) = 7$, $(63, 77, 99) = 1$

จากวิธีการหาตัวหารร่วมมากของจำนวนเต็มสองจำนวน เราสามารถนำมาใช้หาตัวหารร่วมมากของจำนวนเต็มสามจำนวนกล่าวคือ a, b และ c เมื่อกำหนดให้ $a \geq b \geq c > 0$ โดยเริ่มที่เมทริกซ์ดังนี้

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \end{array}\right]$$

ใช้การดำเนินการตามแถวเบื้องต้นทีละคู่จนได้เศษตัวสุดท้ายไม่เป็นศูนย์

กรณีทั่วไป คือการหา ห.ร.ม. ของจำนวนเต็ม n จำนวน ดูเพิ่มเติมได้จาก [2].

ตัวอย่าง 3.4 ในการหา (99, 77, 63) เราเริ่มจาก

$$M_1 = \left[\begin{array}{ccc|c} 1 & 0 & 0 & 99 \\ 0 & 1 & 0 & 77 \\ 0 & 0 & 1 & 63 \end{array}\right]$$

จะได้

$$R_2 + (-1)R_3 \quad M_1 \leftrightarrow M_2 = \left[\begin{array}{ccc|c} 1 & 0 & 0 & 99 \\ 0 & 1 & -1 & 14 \\ 0 & 0 & 1 & 63 \end{array}\right]$$

$$R_3 + (-4)R_2 \quad M_2 \leftrightarrow M_3 = \left[\begin{array}{ccc|c} 1 & 0 & 0 & 99 \\ 0 & 1 & -1 & 14 \\ 0 & -4 & 5 & 7 \end{array}\right]$$

$$R_2 + (-2)R_3 \quad M_3 \leftrightarrow M_4 = \left[\begin{array}{ccc|c} 1 & 0 & 0 & 99 \\ 0 & 9 & -11 & 0 \\ 0 & -4 & 5 & 7 \end{array}\right]$$

$$R_1 + (-14)R_3 \quad M_4 \leftrightarrow M_5 = \left[\begin{array}{ccc|c} 1 & 56 & -70 & 1 \\ 0 & 9 & -11 & 0 \\ 0 & -4 & 5 & 7 \end{array}\right]$$

$$R_3 + (-7)R_1 \quad M_5 \leftrightarrow M_6 = \left[\begin{array}{ccc|c} 1 & 56 & -70 & 1 \\ 0 & 9 & -11 & 0 \\ -7 & -396 & 495 & 0 \end{array}\right]$$

เศษตัวสุดท้ายในที่นี้คือ 1 ดังนั้น 1 เป็นตัวหารร่วมมากของ 99, 77 และ 63 และเขียน 1 เป็นผลรวมเชิงเส้นของ 99, 77 และ 63 ได้ว่า

$$99 \cdot (1) + 77 \cdot (56) + 63 \cdot (-70) = 1$$

4. ขั้นตอนวิธี (Algorithm)

จากที่กล่าวมาข้างต้นทั้งหมด เพียงพอที่จะสร้างขั้นตอนวิธีแบบยุคลิดโดยวิธีการแบบเมทริกซ์ได้ดังนี้

$$\left[\begin{array}{cc:c} 1 & 0 & a \\ 0 & 1 & b \end{array}\right]$$

โดยเริ่มจาก กำหนดค่าเริ่มต้น a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกัน และทำซ้ำโดยใช้การดำเนินการตามแถวเบื้องต้น (elementary row operations : ERO) บนเมทริกซ์ และตรวจสอบเศษตัวสุดท้ายในขั้นที่ n + 1 ว่าเป็นศูนย์หรือไม่ โดยใช้ขั้นตอนวิธีแบบยุคลิด ถ้า $r_{n+1} = 0$ จะได้ว่า r_n คือตัวหารร่วมมากของ a และ b และผลรวมเชิงเส้นของ a และ b คือ $ax_n + by_n = r_n$ มิฉะนั้นให้ทำซ้ำต่อไป ซึ่งเราสามารถเขียนเป็นขั้นตอนวิธี (algorithm) ได้ดังนี้

ให้ a และ b เป็นจำนวนเต็มที่ต้องการหาตัวหารร่วมมาก

วัตถุประสงค์: ต้องการหาตัวหารร่วมมากของ a, b และเขียนผลรวมเชิงเส้นของ a, b

ข้อมูลเข้า : ค่าเริ่มต้น a, b

เมทริกซ์ 2 x 3 โดย AX = B, $M_1 = \left[\begin{array}{cc:c} 1 & 0 & a \\ 0 & 1 & b \end{array}\right]$

ข้อมูลออก : ตัวหารร่วมมากของ a และ b

ผลรวมเชิงเส้น ax + by = r โดยที่ x และ y เป็นจำนวนเต็ม

ขั้นตอนวิธี 1. เริ่ม k = 0

2. **ตรวจสอบ** ค่า a และ b

2.1 ถ้า a > b ทำ **ข้อ 3**

2.2 ถ้า a < b ทำ

2.2.1 k = a และ l = b

2.2.2 a = l และ b = k

2.2.3 ทำ **ข้อ 3**

2.3 ถ้า a = b ทำ ข้อ 3

3. **ทำซ้ำ** k = k + 1

3.1 ถ้า k mod 2 = 1 ทำ

3.1.1 m = a และ n = b

3.1.2 $X = \frac{m}{n}$ เมื่อ X เป็นจำนวนเต็ม

3.1.3 คำนวณ

$M_1[0][0] = M_1[0][0] - (M_1[1][0] \times X)$

$M_1[0][1] = M_1[0][1] - (M_1[1][1] \times X)$

$M_1[0][2] = M_1[0][2] - (M_1[1][2] \times X)$

3.2 ถ้า $k \bmod 2 = 0$ ทำ

3.2.1 $m = b$ และ $n = a$

3.2.2 $X = \frac{m}{n}$ เมื่อ X เป็นจำนวนเต็ม

3.2.3 คำนวณ

$M_1[1][0] = M_1[1][0] - (M_1[0][0] \times X)$

$M_1[1][1] = M_1[1][1] - (M_1[0][1] \times X)$

$M_1[1][2] = M_1[1][2] - (M_1[0][2] \times X)$

จนกระทั่ง $M_1[0][2] = 0$ หรือ $M_1[1][2] = 0$

"แสดงผล" และหยุด

4. แสดงผล

4.1 ถ้า $M_1[0][2] \neq 0$ ทำ

4.1.1 ตัวหารร่วมมากของ a และ b คือ $r = M_1[0][2]$

4.1.2 ผลรวมเชิงเส้นคือ $ax + by = r$

4.2 ถ้า $M_1[1][2] \neq 0$ ทำ

4.2.1 ตัวหารร่วมมากของ a และ b คือ $r = M_1[1][2]$

4.2.2 ผลรวมเชิงเส้นคือ $ax + by = r$

และหยุด

5. กิตติกรรมประกาศ

ขอขอบคุณอาจารย์สมภพ ลำวัฒนพร และอาจารย์อลงกรณ์ แซ่ตั้ง ที่ได้อ่านต้นฉบับและให้คำแนะนำตรวจทานแก้ไขเบื้องต้น ขอขอบคุณอาจารย์ไภษัช แซ่จู และอาจารย์สุดา เธียรมนตรี ที่ให้คำแนะนำในการเขียนโปรแกรมภาษาซี

และขอขอบคุณผู้ทรงคุณวุฒิที่บรรณาธิการเชิญเป็นผู้กลั่นกรองและประเมินบทความและให้คำแนะนำที่เป็นประโยชน์

6. เอกสารอ้างอิง

[1] สมใจ จิตพิทักษ์. (2547). ทฤษฎีจำนวน. (พิมพ์ครั้งที่ 3). สงขลา : โครงการบริการวิชาการมหาวิทยาลัยทักษิณ.

[2] Beardon, A. F. (2000, July). "Reflection on Euclid's Algorithm," The Mathematical Gazette. 84 : 294-296.

[3] Humphreys, J. F. and M. Y. Prest. (2004). Numbers, Groups and Codes. Cambridge : Cambridge University Press.