การหาคำตอบของสมการไดโอแฟนไทน์เชิงเส้น โดยใช้คอมพิวเตอร์

DIOPHANTINE EQUATION

เกษสริน ศรีจันทร์
ขวัญใจ สายแสง
ปัทมา ปิจุลกิลิน

ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต
ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2547

DIOPHANTINE EQUATION

KESARIN SRIJUN

KHWUNJAI SAISANG

PATTHAMA PIJUNKILIN

A SPECIAL PROJECT SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIRMENT FOR THE DEGREE OF BACHELOR OF SCIENCE

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

FACULTY OF SCIENCE

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

ACADEMIC YEAR 2004

หัวข้อปัญหาพิเศษ	การหาคำตอบของสมการไดโอแฟนไทน์เชิงเส้นโดยใช้คอมพิวเตอร์ DIOPHANTINE EQUATION	
ชื่อนักศึกษา	นางสาวเกษสริน ศรีจันทร์	44050003
	นางสาวขวัญใจ สายแสง	44050004
	นางสาวปัทมา ปิจุลกิลิน	44050028
ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์	
สาขาวิชา	คณิตศาสตร์ประยุกต์	
ปีการศึกษา	2547	
อาจารย์ที่ปรึกษา	รศ.ภัคคินี ชิตสกุล	
	อ.วรรณพร สรรประเสริฐ	

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุมัติให้นับปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต สาขาคณิตศาสตร์ประยุกต์ ประจำปีการศึกษา 2547

คณะกรรมการสอบ		ลายมือชื่อ
ประธานกรรมการ	ผศ.กฤษฎา ไตรสุรัตน์	
กรรมการ	อ.ศิริกุล บัณฑิตเสาวภาคย์	
กรรมการและอาจารย์ที่ปรึกษา	รศ.ภัคคินี ชิตสกุล	
กรรมการและอาจารย์ที่ปรึกษา	อ.วรรณพร สรรประเสริฐ	

(รองศาสตราจารย์.ดร. วีระ บุญจริง)
หัวหน้าภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

หัวข้อปัญหาพิเศษ การหาคำตอบของสมการไดโอแฟนไทน์เชิงเส้นโดยใช้คอมพิวเตอร์

ชื่อนักศึกษา นางสาวเกษสริน ศรีจันทร์ 44050003

นางสาวขวัญใจ สายแสง 44050004

นางสาวปัทมา ปีจุลกิลิน 44050028

ปริญญา วิทยาศาสตรบัณฑิต

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

สาขาวิชา คณิตศาสตร์ประยุกต์

ปีการศึกษา 2547

อาจารย์ที่ปรึกษา รศ.ภัคคินี ชิตสกุล

อ.วรรณพร สรรประเสริฐ

บทคัดย่อ

มีปัญหาทางคณิตศาสตร์มากมายที่มีหลายตัวแปรในสมการเดียว โดยปกติแล้วถ้าเราต้องการหาผลเฉลยของสมการที่มี n ตัวแปร เราจะต้องมีสมการของตัวไม่ทราบค่าอย่างน้อย n สมการ เราสามารถหาผลเฉลยของสมการโดยอาศัยความรู้เรื่องการหารลงตัว ขั้นตอนวิธีการหาร และขั้นตอนวิธีของยูคลิด การหาผลเฉลยของสมการโดยวิธีตรงนั้นค่อนข้างยุ่งยาก ดังนั้นในการทำปัญหาพิเศษนี้จึงได้พยายามที่จะสร้างขั้นตอนวิธีที่ช่วยในการหาผลเฉลย โดยมีขอบเขตของปัญหาอยู่ที่สมการไดโอแฟนไทน์เชิงเส้นสองตัวแปรและสามตัวแปร

Special Project Title	DIOPHANTINE EQUATION
Students	Miss Kesarin Srijun 44050003
	Miss Khwunjai Saisang 44050004
	Miss Patthama Pijunkilin 44050028
Degree	Bachelor of Sciences
Department	Mathematics and Computer Science, Faculty of Science
Programme	Applied Mathematics
Academic Year	2004
Special Project Advisor	Assoc.Prof Pakkinee Chitsakul
	Wannaporn Sunprasert

ABSTRACT

There are many mathematical problems that can be represented by an equation with several variables. Normally, if we want to find n unknowns of equations, we must have at least n equations. A Linear Diophantine equation is an equation with several unknowns. Its solutions can be determind using a property of divisibility, division algorithm, and Euclidean algorithm. Therefore, this project proposes a new algorithm for determining Linear Diophantine equation with two and three variables.

กิตติกรรมประกาศ

ในการทำปัญหาพิเศษเรื่อง การหาคำตอบของสมการไดโอแฟนไทน์เชิงเส้นโดยใช้คอมพิวเตอร์สามารถสำเร็จลุล่วงได้ด้วยดีนั้น คณะผู้จัดทำต้องขอขอบพระคุณ

รองศาสตราจารย์ภัคคินี ชิตสกุล และ อาจารย์วรรณพร สรรประเสริฐ ซึ่งเป็นอาจารย์ที่ปรึกษาปัญหาพิเศษในหัวข้อนี้ ที่กรุณาให้คำแนะนำและเป็นที่ปรึกษาในการแก้ปัญหาต่างๆ รวมทั้งเป็นผู้ตรวจสอบความถูกต้องของปัญหาพิเศษนี้ด้วย

คณาจารย์ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ทุกท่านที่ได้ ประสิทธิ์ประสาทวิชาความรู้ ทั้งในภาคทฤษฎีและปฏิบัติ

นอกจากนี้ขอขอบพระคุณเจ้าหน้าที่ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ทุกท่านที่ให้ความสะดวกในการเบิกอุปกรณ์ต่างๆ ที่ใช้ในการทำปัญหาพิเศษนี้สัมฤทธิ์ผลได้ด้วยดี

และหาก “ความดี” ของปัญหาพิเศษในหัวข้อนี้จะพึงมีอยู่บ้าง คณะผู้จัดทำก็ขอมอบให้กับ บิดา มารดา ซึ่งเป็นบุคคลที่เลี้ยงดูมาจนเติบใหญ่ และให้โอกาสทางการศึกษาแก่คณะผู้จัดทำเป็นอย่างดีตลอดมา

คณะผู้จัดทำ

มีนาคม 2548

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของปัญหา

สมการไดโอแฟนไทน์เชิงเส้นเป็นเรื่องหนึ่งในวิชาคณิตศาสตร์ที่มุ่งศึกษาเกี่ยวกับขั้นตอนวิธีของยูคลิด นิยามและทฤษฎีบทต่างๆของสมการไดโอแฟนไทน์เชิงเส้น และสมบัติเบื้องต้นของสมภาค เนื่องจากเนื้อหาเกี่ยวกับสมการไดโอแฟนไทน์เชิงเส้นเป็นเรื่องที่แพร่หลายมานานแล้ว แต่ทำความเข้าใจได้ยาก ดังนั้นจึงนำคอมพิวเตอร์มาช่วยในการคำนวณเพื่อเป็นการสะดวกกับผู้ที่สนใจศึกษาค้นคว้าเกี่ยวกับเนื้อหาทางด้านนี้ จึงได้นำเสนอโปรแกรมช่วยสอนนี้ผ่านทางสื่ออินเตอร์เน็ท เพื่อเป็นการเสริมการศึกษา พัฒนาทักษะทางความคิด นอกเหนือจากการศึกษาในห้องเรียน และเสริมเพิ่มเติมให้เข้าใจในบทเรียนดียิ่งขึ้น การศึกษาจะเสริมสร้างความรู้ความสามารถทางด้านความคิด ความเข้าใจ และยังสามารถนำความรู้เหล่านี้ ไปใช้เป็นรากฐานในการศึกษาคณิตศาสตร์ชั้นสูงได้อีกด้วย

1.2 วัตถุประสงค์ของการทำ

1. เพื่อสร้างความเข้าใจเกี่ยวกับสมการไดโอแฟนไทน์เชิงเส้นแก่นักศึกษา และผู้ที่สนใจมากยิ่งขึ้น
2. สามารถนำสื่อการสอนนี้ไปในใช้ได้อย่างกว้างขวางบนสื่ออินเตอร์เน็ต
3. สามารถใช้งานได้ง่าย และสร้างความสนใจแก่ผู้ใช้งาน
4. เพื่อศึกษาเครื่องมือที่ใช้ในการพัฒนาบทเรียน ซึ่งสามารถใช้ในการสร้างและพัฒนาเรียนเรื่องอื่นๆ ต่อไป

1.3 ขอบเขตของปัญหา

ปัญหาพิเศษฉบับนี้เป็นเนื้อหาเกี่ยวกับสมการไดโอแฟนไทน์เชิงเส้น โดยจะครอบคลุมเนื้อหาในส่วนของการพิสูจน์และการคำนวณเอาไว้ทั้งหมด

1. ศึกษาเนื้อหาและรายละเอียดของสมการไดโอแฟนไทน์เชิงเส้น
2. ศึกษาการคำนวณสมการไดโอแฟนไทม์โดยใช้คอมพิวเตอร์
3. ศึกษาการคำนวณสมการไดโอแฟนไทน์โดยใช้ค่าที่เป็นจำนวนเต็มบวกเท่านั้น

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.ช่วยฝึกฝนความชำนาญในการแก้ปัญหาเรื่องสมการไดโอแฟนไทน์เชิงเส้น

2. ช่วยอำนวยความสะดวกในการศึกษาเนื้อหาเรื่องสมการไดโอแฟนไทน์เชิงเส้น

3. โปรแกรมมีความสะดวกและง่ายต่อการใช้งาน

1.5 ขั้นตอนในการดำเนินการ

1. ศึกษาเนื้อหาเกี่ยวกับสมการไดโอแฟนไทน์เชิงเส้น

2. ศึกษาภาษาทางคอมพิวเตอร์ในการเขียนโปรแกรม

3. ศึกษาการคำนวณสมการไดโอแฟนไทม์โดยใช้คอมพิวเตอร์

4. ทดสอบและแก้ไขโปรแกรมที่สร้างขึ้นมาให้มีประสิทธิภาพ

5. ปรับแต่งรูปแบบการนำเสนอ

1.6 อุปกรณ์ที่ใช้ในการทำปัญหาพิเศษ

1. กระดาษ A4

2. Mobile Rack

3. Hard disk 20.0 GB

4. คอมพิวเตอร์ Operation “window XP” Ram 64 MB up

บทที่ 2
การหารในระบบจำนวนเต็ม

2.1 การหารในระบบจำนวนเต็ม

2.1.1 ขั้นตอนการหาร

เราเริ่มรู้จักการหารครั้งแรกเป็นการหารจำนวนนับด้วยจำนวนนับ ซึ่งในบางครั้งจะพบว่ามีเศษเหลือจากการหารที่เป็นจำนวนนับซึ่งมีค่าน้อยกว่าตัวหารเสมอ

ดังเช่น ถ้าเรามีลูกอม 20 เม็ด ต้องการแจกให้เด็ก 3 คน คนละเท่าๆกัน โดยให้แต่ละคนได้ลูกอมมากที่สุดเท่าที่จะทำได้ เราอาจทำได้โดยแจกลูกอมคนละเม็ดวนทีละรอบไปเรื่อยๆ จนกว่าจะเหลือลูกอมน้อยกว่า 3 เม็ด จะพบว่าเด็กแต่ละคนจะได้ลูกอมคนละ 6 เม็ด และเหลือลูกอมอยู่อีก 2 เม็ด ลูกอม 2 เม็ดนี้เป็น “เศษ” ที่เหลือจากการ “แบ่ง” กรณีนี้เรากล่าวว่า 3 หาร 20 ได้ผลลัพธ์เป็น 6 เหลือเศษ 2 หรือเขียนได้เป็น

$$20 = 3 \cdot 6 + 2$$

เราสามารถสรุปวิธีการเช่นนี้ในรูปทฤษฎีบทดังนี้

ทฤษฎีบท 1 ขั้นตอนการหาร

ให้ m และ n เป็นจำนวนเต็มโดยที่ $n > 0$ จะได้ว่ามีจำนวนเต็ม q และ r เพียงชุดเดียวเท่านั้น ซึ่งทำให้ $m = nq + r$ โดยที่ $0 \le r \le n$ เราจะเรียก q ว่าผลหาร เรียก r ว่าเศษเหลือ ในการหาร m ด้วย n

<u>พิสูจน์</u>

ให้ $S = \{m - nx | x$ เป็นจำนวนเต็มและ $m - nx \ge 0\}$

$S \ne \phi$ เนื่องจาก $n \ge 1$ ทำให้

$$m - (-|m|)n = m + |m|n \ge m + |m| \ge 0$$

ดังนั้น $m - (-|m|)n \in S$

โดยหลักการจัดอันดับอย่างดี (หลักการจัดอันดับอย่างดีของ N มีหลักอยู่ว่า สับเซต S ของ N ซึ่งไม่ใช่เซตว่างย่อมมีสมาชิกที่มีค่าน้อยที่สุด นั่นคือ มี $s_0 \in S$ ซึ่ง $s_0 \le x$ ทุก $x \in S$) จะได้ว่า S มีสมาชิกที่มีค่าน้อยที่สุด เรียกสมาชิกตัวนี้ว่า r

เนื่องจาก r เป็นสมาชิกของ S จึงมีจำนวนเต็ม q ซึ่ง

$$r = m - nq \quad \text{และ} \quad r \ge 0$$

นั่นคือ $m = nq + r$ และ $0 \le r$

จะแสดงว่า $r < n$ โดยวิธี contradiction สมมติว่า $r \ge n$

จะได้ว่า $m-(q+1)n = (m-qn)-n = r-n \ge 0$

จึงทำให้ $m-(q+1) \in S$ แต่ $m-(q+1)n = r-n < r$

ขัดแย้งกับการเลือก r เป็นสมาชิกที่มีค่าน้อยที่สุดของ S ดังนั้น $r < n$

ต่อไปจะแสดงว่า q และ r มีเพียงชุดเดียวเท่านั้น

สมมติว่า q' และ r' เป็นจำนวนเต็มที่มีคุณสมบัติ

$$m = nq' + r' \quad \text{และ} \quad 0 \le r' \le n$$

จากก่อนหน้านี้ $m = nq + r$ และ $0 \le r \le n$

ทำให้ $r' - r = n(q - q')$

$$|r' - r| = n|q - q'|$$

จาก $0 \le r \le n$ จะได้ $-n < -r < 0$ และ $0 \le r' \le n$ จึงได้

$-n < r' - r < n$ นั่นคือ $|r' - r| < n$

ทำให้ $n|q - q'| < n$ นั่นคือ $0 \le |q - q'| < 1$

เนื่องจาก $|q - q'|$ เป็นจำนวนเต็ม เราจึงได้ว่า $|q - q'| = 0$ ดังนั้น $q = q'$

สรุปได้ว่า $r' = r$ #

โดยอาศัยทฤษฎีบทขั้นตอนการหาร เราสามารถจำแนกจำนวนเต็มโดยแบ่งกลุ่มตามเศษเหลือจากการหารด้วย n ได้ดังนี้

เมื่อ $n = 2$ เศษเหลือจากการหารด้วย 2 มี 2 แบบ คือ $r = 0$ และ $r = 1$ ดังนั้น จำนวนเต็มใดๆ จะอยู่ในรูป $2q$ ซึ่งเรียกว่า จำนวนคู่ หรืออยู่ในรูป $2q+1$ ซึ่งเรียกว่า จำนวนคี่

เมื่อ $n = 3$ เศษเหลือที่ได้จากการหารด้วย 3 มี 3 แบบ คือ $r = 0, r = 1$ และ $r = 2$ ดังนั้น จำนวนเต็มใดๆ จะอยู่ในรูป $3q$ หรือ $3q+1$ หรือ $3q+2$

กล่าวโดยทั่วไป ทฤษฎีบทขั้นตอนการหารมีประโยชน์ในการพิสูจน์หรือแก้ปัญหาในระบบจำนวนเต็ม โดยวิธีการแบ่งกรณีสามารถทำได้โดยแบ่งออกเป็น n กรณีตามเศษเหลือที่ได้จากการหารด้วย n กล่าวคือ จำนวนเต็มใดก็ตามจะอยู่ในรูปใดรูปหนึ่งต่อไปนี้เท่านั้น

$$nq, nq+1, nq+2, \ldots, nq+(n-1)$$

เมื่อเราเลือก n ให้เหมาะกับปัญหาจะทำให้การแก้ปัญหามีความสะดวกยิ่งขึ้น

ทฤษฎีบท 2 ถ้ากำหนดจำนวนเต็ม a,b ซึ่ง $b \neq 0$ แล้ว จะมีจำนวนเต็มอีกคู่หนึ่ง และคู่เดียว q,r ซึ่งทำให้ $a = bq + r$ เมื่อ $0 \leq r \leq |b|$

<u>แนวคิด</u> การพิสูจน์จะแบ่งเป็น 3 ตอนดังนี้

1. จะแสดงว่ามี q,r ที่ทำให้ $r = a - bq \geq 0$
2. ถ้าให้ r เป็นจำนวนน้อยที่สุด จะแสดงว่า $r < |b|$

   ตอนที่ 1 และ 2 เป็นการแสดงว่ามี q,r ที่ทำให้ $a = bq + r$ เมื่อ $0 \leq r \leq |b|$
3. จะแสดงว่ามี q,r อยู่เพียงคู่เดียว

<u>พิสูจน์</u>

1. พิจารณาอสมการ $a - bx \geq 0$ ว่ามี x ที่เป็นจำนวนเต็มหรือไม่ อสมการนี้สมมูลกับ $bx \leq a$

ถ้า $a > 0$ ให้ x เป็นจำนวนเต็มที่มีเครื่องหมายตรงข้ามกับ b ก็จะได้ทันที

ถ้า $a < 0$ กรณีที่ $b > 0$ คือ $b \geq 1$ ให้ $x = a$ จะได้ $ba \leq a$

กรณีที่ $b < 0$ คือ $b \leq -1$ ให้ $x = -a$ จะได้ $-ba \leq a$

จะเห็นว่ามีค่า x ที่ทำให้ $a - bx \geq 0$ ในทุกกรณี

ดังนั้น ถ้ากำหนดให้ $x = q$ และ r เป็นจำนวนเต็มที่น้อยที่สุดที่ทำให้

$r = a - bq > 0$

นั่นคือ มี q,r ซึ่งทำให้ $a = bq + r$ เมื่อ $r \geq 0$ #

2. จะแสดงว่า $r < |b|$ โดยกำหนดให้ r เป็นจำนวนน้อยที่สุด

สมมติให้ $r > |b|$ ดังนั้น $r - |b| \geq 0$

แต่ $r - |b| = (a - bq) - |b| = a - (bq - |b|) = a - b(q+1)$ ซึ่งอยู่ในรูป $a - bx \geq 0$

แต่ $r - |b| < r$ จะเห็นว่าขัดแย้งกับที่กำหนดว่า r เป็นจำนวนเต็มน้อยที่สุด

ซึ่งทำให้ $r = a - bq \geq 0$ ดังนั้นที่สมมติไว้ไม่จริง นั่นคือ $r < |b|$ #

จากตอนที่ 1 และ 2 แสดงว่ามี q,r ที่ทำให้ $a = bq + r$ เมื่อ $0 \leq r \leq |b|$

3. จะแสดงว่ามี q,r อยู่เพียงคู่เดียว

สมมติว่ามี q,r และอีกคู่หนึ่ง คือ q',r' ที่ทำให้

$a = bq + r$ เมื่อ $0 \leq r \leq |b|$ และ $a = bq' + r'$ เมื่อ $0 \leq r' \leq |b|$

ดังนั้น $bq+r=bq'+r'$

ได้ $b(q-q')=r-r'$ นั่นคือ $b\,|\,(r'-r)$ แต่ $|r'-r|<b$

ดังนั้น $r'-r=0$ หรือ $r'=r$

และจาก $b(q-q')=r-r'=0$ เมื่อ $b\neq 0$

ดังนั้น $q'-q=0$ หรือ $q'=q$

สรุปได้ว่ามี q,r อยู่เพียงคู่เดียว #

ตัวอย่าง 1 ให้ $a=17,b=5$ จะได้ $17=5(3)+2,q=3,r=2$

ให้ $a=-13,b=7$ จะได้ $-13=7(-2)+1,q=-2,r=1$ #

ทฤษฎีบท 3 เศษเหลือจากการหารผลบวก (ผลคูณ) ของจำนวนสองจำนวนด้วย n คือผลบวก (ผลคูณ) ของเศษเหลือจากการหารของจำนวนทั้งสองด้วย n (นั่นคือ ถ้า $m_1=nq_1+r_1$ และ $m_2=nq_2+r_2$ แล้ว $m_1+m_2=nq+(r_1+r_2)$ และ $m_1m_2=nq'+(r_1r_2)$)

<u>พิสูจน์</u>

ให้ $m_1=nq_1+r_1$ และ $m_2=nq_2+r_2$ โดยที่ $0\le r_1,r_2<|n|$

จะได้ว่า $m_1+m_2=n(q_1+q_2)+(r_1+r_2)$

$$m_1m_2=n(q_1+q_2)(r_1+r_2)$$
$$=n^2q_1q_2+nq_2r_1+nq_1r_2+r_1r_2$$
$$=n(nq_1q_2+q_2r_1+q_1r_2)+r_1r_2$$

#

2.1.2 การหารลงตัว

การหารลงตัว หมายถึง การหารซึ่งไม่มีเศษเหลือ ในขั้นตอนการหารเราทราบว่าสำหรับจำนวนเต็ม n และ m ซึ่ง $n\neq 0$ จะมีจำนวนเต็ม q และ r ซึ่ง $m=nq+r$ โดยที่ $|r|<|n|$

กรณีที่ $r=0$ เรากล่าวว่า n หาร m ได้ลงตัว

กรณีที่ $r\neq 0$ เรากล่าวว่า n หาร m ไม่ลงตัว

บทนิยาม ถ้า $a,b \in I$ ซึ่ง $a \neq 0$ จะกล่าวว่า จำนวน b ถูกหารลงตัวด้วยจำนวน a ก็ต่อเมื่อ มีจำนวนเต็ม c ซึ่งทำให้ $a \cdot c = b$ เราอาจกล่าวอีกอย่างหนึ่งว่า a หาร b ลงตัว เขียนแทนด้วยสัญลักษณ์ $a|b$

เรียก a ว่าเป็นตัวหาร (Devisor or Factor) ของ b

เรียก b ว่าเป็นผลคูณ (Multiple) ของ a

ในกรณีที่ a หาร b ไม่ลงตัว เราเขียนว่า $a \nmid b$

ตัวอย่าง 2 $2|6$ เพราะว่ามี $3 \in I$ ที่ทำให้ $2 \cdot 3 = 6$

$7 \nmid 13$ เพราะไม่มีจำนวนเต็ม c ใดๆ ที่ทำให้ $7 \cdot c = 13$ #

ข้อสังเกต ถ้า $a \mid b$ แล้ว $(-a) \mid b$ และ $a \mid (-b)$ และ $(-a) \mid (-b)$

$a \mid a$ สำหรับจำนวนเต็ม a ซึ่ง $a \neq 0$

$a \mid 0$ สำหรับจำนวนเต็ม a เพราะว่ามี $0 \in I$ ที่ทำให้ $a \cdot 0 = 0$

$1 \mid a$ สำหรับจำนวนเต็ม a เพราะว่ามี $a \in I$ ที่ทำให้ $1 \cdot a = a$

ทฤษฎีบท 4 กำหนด a,b,c และ m เป็นจำนวนเต็มใดๆ

1. ถ้า $a \mid b$ แล้ว $a \mid bc$ สำหรับจำนวนเต็ม c ใดๆ
2. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$
3. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bx + cy)$ สำหรับจำนวนเต็ม x, y ใดๆ
4. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = \pm b$
5. ถ้า $a \mid b, a > 0, b > 0$ แล้ว $a \leq b$
6. ถ้า $m \neq 0, a \mid b$ ก็ต่อเมื่อ $ma \mid mb$
7. ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$
8. ถ้า $a \mid b$ และ $|a| > |b|$ แล้ว $b = 0$

พิสูจน์ (2)

H: ถ้า $a \mid b$ และ $b \mid c$

C: แล้ว $a \mid c$

พิสูจน์ ถ้า $a \mid b$ แล้ว จะมีเลขจำนวนเต็ม s ที่ทำให้เกิด $b = s \cdot a$

ถ้า $b \mid c$ แล้ว จะมีเลขจำนวนเต็ม t ที่ทำให้เกิด $c = t \cdot b$

แทนค่า $b = s \cdot a$ ใน $c = t \cdot b$ ได้ $c = t \cdot (s \cdot a) = (t \cdot s) \cdot a$ โดยเหตุที่ว่า s และ t เป็นจำนวนเต็ม

ดังนั้น $s \cdot t$ ก็เป็นจำนวนเต็มด้วย สรุปได้ว่า $a \mid c$ #

พิสูจน์ (3)

H: ถ้า $a \mid b$ และ $a \mid c$

C: แล้ว $a \mid (bx + cy)$ สำหรับจำนวนเต็ม x, y ใดๆ

<u>พิสูจน์</u> ถ้า $a \mid b$ จะมีเลขจำนวนเต็ม s ที่ทำให้เกิด $b = a \cdot s$

ถ้า $a \mid c$ จะมีเลขจำนวนเต็ม t ที่ทำให้เกิด $c = a \cdot t$

ดังนั้น $bx + cy = (a \cdot s)x + (a \cdot t)y = a \cdot (sx + ty)$ โดยเหตุที่ $a \mid a \cdot (sx + ty)$ ดังนั้น $a \mid a.(bx + cy)$ จากคุณสมบัติข้อ 3 และความรู้เรื่องเซตจำกัด จะได้ว่า

ถ้า $a \mid b_1, a \mid b_2, ..., a \mid b_n$ แล้ว $a \mid \sum_{j=1}^{n} b_j x_j$ สำหรับจำนวนเต็มใดๆ #

พิสูจน์ (7)

H: ถ้า $a \mid b$ และ $b \neq 0$

C: แล้ว $|a| \leq |b|$

<u>พิสูจน์</u> ถ้า $a \mid b$ และ $b \neq 0$ แล้ว จะมีจำนวนเต็ม c ที่ทำให้เกิด $a \cdot c = b$

ดังนั้น $|a \cdot c| = |b|$

$|a| \cdot |c| = |b| \neq 0$

$a \neq 0, c \neq 0$ หรือ $|a| > 0, |b| > 0$

จากนิยามของค่าสัมบูรณ์ $1 \leq |c|$

$|a| \cdot 1 \leq |a| \cdot |c|$ แต่ $|a| \cdot |c| = |b|$

ดังนั้น $|a| \leq |b|$ #

บทนิยาม จำนวนเต็ม a เป็นจำนวนคู่ ก็ต่อเมื่อ มีจำนวนเต็ม c ที่ $a = 2c$

a เป็นจำนวนคี่ ก็ต่อเมื่อ มีจำนวนเต็ม c ที่ $a = 2c + 1$

จากบทนิยาม จะได้ว่า a เป็นจำนวนเต็มคู่ ก็ต่อเมื่อ $2 \mid a$

ตัวอย่าง 3 จงพิสูจน์ว่า สำหรับจำนวนเต็ม a ใดๆ $2 \mid a(a+1)$

ผลคูณของจำนวนเต็มที่เรียงกันสองจำนวนเป็นคู่เสมอ

<u>พิสูจน์</u>

ให้ a เป็นจำนวนเต็มใดๆ

กรณี 1 a เป็นจำนวนคู่

นั่นคือ $2 \mid a$ ดังนั้น จะได้ว่า $2 \mid a(a+1)$

กรณี 2 a เป็นจำนวนคี่

ดังนั้น จะมีจำนวนเต็ม c ที่ $a = 2c+1$ ทำให้ $a+1 = 2c+2 = 2(c+1)$

นั่นคือ $2 \mid (a+1)$ จึงได้ว่า $2 \mid a(a+1)$ #

2.2 การหาตัวหารร่วมมากโดยขั้นตอนวิธีของยูคลิด(Euclidean algorithm)

บทนิยาม ให้ a,b,c เป็นจำนวนเต็ม และ $a \neq 0$ ซึ่ง a เป็นตัวหารร่วม (ตัวประกอบร่วม) ของ b และ c ก็ต่อเมื่อ $a \mid b$ และ $a \mid c$

ตัวอย่าง 4 จงหาตัวหารร่วมของ 18 และ 24

<u>วิธีทำ</u> จำนวนที่หาร 18 ลงตัว คือ $1,-1,18,-18,2,-2,9,-9,3,-3,6,-6$

จำนวนที่หาร 24 ลงตัว คือ $1,-1,24,-24,2,-2,12,-12,3,-3,8,-8,4,-4,6,-6$

ตัวหารร่วมของ 18 และ 24 คือ $1,-1,2,-2,3,-3,6,-6$ #

บทนิยาม กำหนดให้ a และ b เป็นจำนวนเต็ม ซึ่งอย่างน้อยหนึ่งตัวไม่เป็นศูนย์ d จะเป็นตัวหารร่วมมากของ a และ b ก็ต่อเมื่อ d เป็นจำนวนเต็มบวก ซึ่ง

1. $d \mid a$ และ $d \mid b$
2. ถ้า c เป็นจำนวนเต็มบวก ซึ่ง $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$ ตัวหารร่วมมาก ของ a และ b เขียนแทนด้วย (a,b) เรียกย่อๆว่า ห.ร.ม. ของ a และ b

จากตัวอย่าง จะได้ตัวหารร่วมมากของ 18 และ 24 คือ $(18,24) = 6$ #

ตัวอย่าง 5 จงหาตัวหารร่วมมาก $(0,9)$ และ $(6,12)$

<u>วิธีทำ</u> จำนวนเต็มบวกที่หาร 0 ลงตัว ได้แก่ จำนวนเต็มบวกทุกตัว

จำนวนเต็มบวกที่หาร 9 ลงตัว ได้แก่ $1,3,9$

ตัวหารร่วมของ 0 และ 9 ได้แก่ $1,3,9$

ดังนั้น $(0,9)=9$

จำนวนเต็มบวกที่หาร 6 ลงตัว ได้แก่ $1,2,3,6$

จำนวนเต็มบวกที่หาร 12 ลงตัว ได้แก่ $1,2,3,4,6,12$

ตัวหารร่วมของ 6 และ 12 ได้แก่ $1,2,3,6$

ดังนั้น $(6,12)=6$ #

ทฤษฎีบท 5 ห.ร.ม. ของจำนวนเต็ม a และ b จะมีจำนวนเดียวเท่านั้น

<u>พิสูจน์</u> ให้ d เป็น ห.ร.ม. ของ a และ b จะได้ $d \mid a$ และ $d \mid b$

ให้ c เป็น ห.ร.ม. ของ a และ b จะได้ $c \mid a$ และ $c \mid b$

เนื่องจาก c เป็นตัวหารร่วมมากของ a และ b และ d เป็น ห.ร.ม. ดังนั้น $c \mid d$

เนื่องจาก d เป็นตัวหารร่วมมากของ a และ b และ c เป็น ห.ร.ม. ดังนั้น $d \mid c$

จาก $d \mid c$ และ $c \mid d$ และโดยที่ $c,d>0$ จะได้ $c=d$ #

2.2.1 ขั้นตอนวิธียูคลิด

ทฤษฎีบท 6 ขั้นตอนวิธีของยูคลิด (Euclidean algorithm)

กำหนดจำนวนเต็ม a และ b จากขั้นตอนวิธีการหารจะได้สมการ

$$a = q_1 b + r_1, 0 < r_1 < |b|$$

$$b = q_2 r_1 + r_2, 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, 0 < r_3 < r_2$$

$$r_2 = q_4 r_3 + r_4, 0 < r_4 < r_3$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

จะได้ว่า ห.ร.ม. ของ a และ b คือ $(a,b)=r_n$

เมื่อ r_n เป็นเศษตัวสุดท้ายที่ไม่เป็น 0

<u>พิสูจน์</u> ถ้า c เป็น ห.ร.ม. ของ a และ b จะได้ว่า $c|a$ และ $c|b$

แต่ $r_1 = a - q_1 b$ ดังนั้น $c|r_1$

และ $r_2 = b - q_2 r_2$ ดังนั้น $c|r_2$

$\vdots$

และ $r_n = r_{n-2} - q_n r_{n-1}$ ดังนั้น $c|r_n$ .....(1)

อนึ่ง $r_{n-1} = q_{n+1} r_n$ ดังนั้น $r_n|r_{n-1}$

จะได้ $r_n|(q_n r_{n-1} + r_n)$ แต่ $r_{n-2} = q_n r_{n-1} + r_n$

ดังนั้น $r_n|r_{n-2}$

ในทำนองเดียวกันจะได้ $r_n|r_{n-3}$ และ $r_n|r_{n-4}$ และ ... และ $r_n|r_1$

ดังนั้น $r_n|b$ และ $r_n|a$

แต่ $c = (a,b)$ ดังนั้น $r_n|c$ .....(2)

จาก (1) และ (2) และการที่ $r_n > 0$ จะได้ $r_n = c$

นั่นคือ $r_n = (a,b)$ #

ตัวอย่าง 5 จงหา ห.ร.ม. ของ 299 และ 364

<u>วิธีทำ</u>

$364 = 1(299) + 65$

$299 = 4(65) + 39$

$65 = 1(39) + 26$

$39 = 1(26) + 13$

$26 = 2(13)$

ห.ร.ม. ของ 299 และ 364 คือ 13

อาจเขียนขั้นตอนการคิดได้ดังนี้

299)<u>364</u>

1 เศษ 65)<u>299</u>

4 เศษ 39)<u>65</u>

1 เศษ 26)<u>39</u>

1 เศษ 13)<u>26</u>

วิธีเขียนขั้นตอนการคิดอีกวิธีหนึ่ง คือ แบบตั้งหาร

1	364 299	299 260	4
1	65 39	39 26	1
2	26 26	13	

1. นำ 299 ไปหาร 364 ได้ผลหาร 1 เศษ 65
2. นำเศษ 65 ไปหาร 299 ได้ผลหาร 4 เศษ 39
3. นำเศษ 39 ไปหาร 65 ได้ผลหาร 1 เศษ 26
4. นำเศษ 26 ไปหาร 39 ได้ผลหาร 1 เศษ 13
5. นำเศษ 13 ไปหาร 26 ได้ลงตัว

$(364, 299) = 13$ #

ตัวอย่าง 6 จงใช้ขั้นตอนของยูคลิดหา $(2475, 420)$

<u>วิธีทำ</u>

$$2475 = 420(5) + 375$$
$$420 = 375(1) + 45$$
$$375 = 45(8) + 15$$
$$45 = 15(3)$$

ดังนั้น $(2475, 420) = 15$ #

ตัวอย่าง 7 จงใช้ขั้นตอนของยูคลิดหา $(1381955, 690713)$

<u>วิธีทำ</u>

$$1381955 = 690713(2) + 529$$
$$690713 = 529(1305) + 368$$
$$529 = 368(1) + 161$$
$$368 = 161(3) + 46$$
$$46 = 23(2)$$

ดังนั้น $(1381955, 690713) = 23$

วิธีที่ 2

$$1381955 = 690713(2) + 529$$
$$690713 = 529(1306) - 161$$
$$529 = 161(3) + 46$$

$$161 = 46(3) + 23$$
$$46 = 23(2)$$ #

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

ค่าบวกที่เล็กที่สุดของ $ax + by$ จะเท่ากับ (a,b)

ต้องการหาจำนวนเต็ม x และ y ซึ่งเป็นผลเฉลยของ

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

จากการสังเกต จะเห็นว่า $ax + by$ ทุกจำนวนหารด้วย (a,b) ลงตัว และค่าบวกที่เล็กที่สุด ก็คือ (a,b) นั่นเอง

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

ถ้า a,b เล็กๆ เราอาจเดาคำตอบได้ เช่น สมการ

$$10x + 35y = 5$$

มี $x = -3$ และ $y = 1$ เป็นคำตอบ และสมการ

$$7x + 11y = 1$$

มี $x = -3$ และ $y = 2$ เป็นคำตอบ

เราจะสังเกตว่า ในสมการหนึ่งอาจมีมากว่า 1 คำตอบ เช่น

$x = 8$ และ $y = -5$ ก็เป็นคำตอบของสมการ $7x + 11y = 1$ เช่นเดียวกัน

แต่ถ้าค่า a,b และ มีค่ามากๆมันอาจจะยุ่งยากและเกิดข้อผิดพลาดได้มากมาย เราจึงใช้ยูคลิดอัลกอริทึมมาช่วยแก้สมการ

ตัวอย่าง 7 จงแก้สมการ

<u>วิธีทำ</u>

ขั้นที่ 1 หา ห.ร.ม. โดยใช้ยูคลิดอัลกอริทึม

$$60 = 22(2) + 16$$
$$22 = 16(1) + 6$$
$$16 = 6(2) + 4$$
$$6 = 4(1) + 2$$
$$4 = 2(1) + 0$$
$$(22,60) = 2$$

ขั้นแรก เขียนสมการแรกใหม่ได้ดังนี้

$$16 = a - 2b \qquad a = 60, b = 22$$

ต่อมา แทนค่านี้ลงสมการที่ 2 ที่มี 16 ปรากฏอยู่

$$b = 1\times 16 + 6 = 1\times(a - 2b) + 6 \qquad b = 22$$

จัดสมการใหม่ให้ 6 อยู่ทางซ้ายมือ

$$6 = b - (a - 2b) = -a + 3b$$

แทนค่า 16 และ 6 ในสมการถัดไป

$$a - 2b = 16 = 2\times 6 + 4 = 2\times(-a + 3b) + 4$$

จัดสมการใหม่ให้ 4 อยู่ทางซ้ายมือ

$$4 = (a - 2b) - 2\times(-a + 3b) = 3a - 8b$$

สุดท้าย แทนในสมการ $6 = 1\times 4 + 2$ จะได้

$$a - 3b = 6 = 1\times 4 + 2 = 1\times(3a - 8b) + 2$$

จัดสมการใหม่ จะได้ผลเฉลยที่ต้องการ

$$-4a + 11b = 2$$

(ตรวจคำตอบ $-4(60) + 11(22) = -240 + 242 = 2$)

สรุปการคำนวณได้ดังตาราง

ยูคลิดอัลกอริทึม	คำนวณผลเฉลยของสมการ $ax + by = (a,b)$
$a = 2\times b + 16$ $b = 1\times 16 + 6$	$16 = a - 2b$
$16 = 2\times 6 + 4$	$6 = b - 1\times 16$ $= b - 1\times(a - 2b)$ $= -a + 3b$
$6 = 1\times 4 + 2$	$4 = 16 - 2\times 6$ $= (a - 2b) - 2\times(-a + 3b)$ $= 3a - 8b$
$4 = 2\times 2 + 0$	$2 = 6 - 1\times 4$ $= (-a + 3b) - 1\times(3a - 8b)$ $= -4a + 11b$

เขียนในรูปทั่วไปได้ดังนี้

$$\begin{aligned} a &= q_1 \times b + r_1 \\ b &= q_2 \times r_1 + r_2 \\ r_1 &= q_3 \times r_2 + r_3 \\ &\vdots \end{aligned} \qquad \Big| \qquad \begin{aligned} r_1 &= a - q_1 \times b \\ r_2 &= b - q_2 \times r_1 \\ r_3 &= r_1 - q_3 \times r_2 \\ &\vdots \end{aligned}$$

จะเห็นว่า เราจะจัดสมการให้อยู่ในรูปของ

เศษ = ผลบวกของผลคูณของ a กับผลคูณของ b

ทำไปจนถึง เศษเหลือที่มีค่าเท่ากับ ห.ร.ม. เราจะได้ผลเฉลยของสมการ $ax+by=(a,b)$ ที่ต้องการ

ถ้ามีคำถามว่า ในสมการหนึ่งๆ จะมีผลเฉลยได้กี่ชุด

เราจะเริ่มศึกษาจากสมการที่มี ห.ร.ม. เป็น 1 ก่อน นั่นคือ

$$ax+by=1$$

สมมติให้ (x_1,y_1) เป็นผลเฉลยของสมการ

เราสามารถสร้างผลเฉลยใหม่ได้เป็น (x_1+kb,y_1-ka)

ตรวจคำตอบได้ดังนี้

$$a(x_1+kb)+b(y_1-ka)=ax_1+akb+by_1-bka=ax_1+by_1=1$$

เช่น ผลเฉลยเริ่มต้นของสมการ $5x+3y=1$ คือ $(-1,2)$

เราจะได้ผลเฉลยใหม่ คือ $(-1+3k,2-5k), k\in I$

ถ้าลองแทนค่า k ลงไปจะได้ผลเฉลย ดังนี้

$$\ldots,(-7,12),(-4,7),(-1,2),(2,-3),(5,-8),\ldots$$

เรายังคงพิจารณาในกรณีของ $(a,b)=1$ กันต่อ

สมมติ เราได้ผลเฉลย 2 ชุด เช่น (x_1,y_1) และ (x_2,y_2) สำหรับสมการ $ax+by=1$

นั่นคือ $ax_1+by_1=1$ และ $ax_2+by_2=1$

เราจะคูณสมการแรกด้วย y_1 คูณสมการที่ 2 ด้วย y_2 นำทั้งสองสมการมาลบกันเพื่อกำจัด b

จะได้ $ax_1y_2+by_1y_2=y_2$ และ $ax_2y_1+by_1y_2=y_1$

$$ax_1y_2-ax_2y_1=y_2-y_1$$

ในทำนองเดียวกับ ถ้าเราคูณสมการแรกด้วย x_2 คูณสมการที่ 2 ด้วย x_1 และนำทั้งสองสมการมาลบกันจะได้

$$bx_2y_1 - bx_1y_2 = x_2 - x_1$$

ถ้าให้ $k = x_2y_1 - x_1y_2$ จะได้

$$x_2 = x_1 + kb \text{ และ } y_2 = y_1 - ka$$

สรุป สมการ $ax + by = 1$ ที่มีผลเฉลยเริ่มต้น คือ (x_1, y_1)

จะมีผลเฉลยอื่นๆ คือ $(x_1 + kb, y_1 - ka)$

ในกรณีที่ $\gcd > 1$

ให้ g แทน $\gcd > 1$

จะได้ $ax + by = g$

แต่ g หาร a และ b ลงตัว

ดังนั้น $\frac{a}{g}x + \frac{b}{g}y = 1$

ทำให้สมการนี้มีผลเฉลยเริ่มต้นเป็น (x_1, y_1)

และมีผลเฉลยทั่วไปเป็น $(x_1 + k\frac{b}{g}, y_1 - k\frac{a}{g})$

จากการหาผลเฉลยของ $ax + by = g$ ดังกล่าว สามารถสรุปได้ดังทฤษฎีบทต่อไปนี้

2.2.3 Linear Equation Theorem

ให้ a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์ และให้ $g = \gcd(a,b)$ สมการ $ax + by = g$ จะมีผลเฉลยเป็นจำนวนเต็ม (x_1, y_1) เสมอ และผลเฉลยนี้สามารถหาโดยอัลกอริทึมของยูคลิด และทุกๆผลเฉลยสามารถหาได้โดยการแทนค่า k ลงในสูตร

$$(x_1 + k\frac{b}{g}, y_1 - k\frac{a}{g})$$

ตัวอย่าง 8 สมการ $60x + 22y = (60,22) = 2$

<u>วิธีทำ</u> มีผลเฉลย $x = -4, y = 11$ จาก Linear Equation Theorem กล่าวว่า

ทุกผลเฉลยสามารถหาได้จากสูตร $(-4 + 11k, 11 - 30k)$

ซึ่ง k เป็นจำนวนเต็มใดๆ

สรุป ในหัวข้อนี้เป็นการแสดงให้เห็นว่า $ax + by = \gcd(a,b)$ มีผลเฉลยเสมอ

ตัวอย่าง 9 จงหา $(316,140)$ และหาจำนวนเต็ม x, y ที่ทำให้ $(316,140) = 316x + 140y$

<u>วิธีทำ</u>

$$316 = 140(2) + 36$$
$$140 = 36(3) + 32$$
$$36 = 32(1) + 4$$
$$32 = 4(8)$$

เราจะได้ว่า $(316,140) = 4$

และ $4 = 36 - 32(1)$

$$= 36 - [140 - 36(3)](1)$$
$$= 36(4) + 140(-1)$$
$$= [316 - 140(2)](4) + 140(-1)$$
$$= 316(4) + 140(-8 - 1)$$
$$= 316(4) + 140(-9)$$

$(316,140) = 316x + 140y$

ดังนั้น $x = 4$ และ $y = -9$ #

ตัวอย่าง 10 จงหา ห.ร.ม. ของ 864 และ 354 และจงเขียน $(864,354)$ เป็นผลรวมเชิงเส้นของ 864 และ 354

<u>วิธีทำ</u>

$$864 = 2(354) + 156$$
$$354 = 2(156) + 42$$
$$156 = 3(42) + 30$$
$$42 = 1(30) + 12$$
$$30 = 2(12) + 6$$
$$12 = 2(6)$$

ดังนั้น $(864,354) = 6$

ห.ร.ม. ของ 864 และ 354 คือ 6

และจะได้ว่า

$6 = 30 - 2(12)$ แทนค่า 12 จะได้

$$= 30 - 2[42 - 1(30)]$$
$$= 3(30) - 2(42) \qquad \text{แทนค่า 30 จะได้}$$
$$= 3[156 - 3(42)] - 2(42)$$
$$= 3(156) - 11(42) \qquad \text{แทนค่า 42 จะได้}$$
$$= 3(156) - 11[354 - 2(156)]$$
$$= 25(156) - 11(354) \qquad \text{แทนค่า 156 จะได้}$$
$$= 25[864 - 2(354)] - 11(354)$$
$$= 25(864) - 61(354)$$

ผลรวมเชิงเส้น $ax + by = (a,b)$ $\qquad (864,354) = 864x + 354y$

ดังนั้น จะได้ $6 = 25(864) - 61(354)$ #

2.3 สมการไดโอแฟนไทด์เชิงเส้น

2.3.1 สมการไดโอแฟนไทด์ 2 ตัวแปร

การหาจุดบนกราฟของสมการเชิงเส้น $ax + by = c$ ซึ่ง a,b และ c เป็นจำนวนเต็ม ซึ่ง a และ b ไม่เป็นศูนย์ทั้งคู่ เราสามารถแก้สมการข้องต้นโดยอาจจะหาค่าของ y ก่อน จะได้ $y = (c - ax)/b$ แล้วหาจำนวนจริง x' ซึ่งแทน x แล้วสอดคล้องกับค่า y' ซึ่งเท่ากับ $(c - ax')/b$ ดังนั้นจะได้จำนวน x', y' ซึ่ง $ax' + by' = c$ หรือได้พิกัด (x', y') ของจุด P′ ของกราฟของสมการ $ax + by = c$ ซึ่งก็คือกราฟเส้นตรงนั่นเอง กล่าวคือ a,b และ c เป็นจำนวนเต็ม แต่ตอนนี้เราจะพิจารณาสมการเชิงเส้นที่มีเงื่อนไขบังคับ

$$ax + by = c \qquad \text{------- (1)}$$

ซึ่งอาจจะเป็นจำนวนบวก จำนวนลบ หรือจำนวนศูนย์ก็ได้ แต่ a และ b จะต้องไม่เป็นศูนย์ทั้งคู่ จากรูปกราฟที่ (1) อาจจะมี 1 จุดหรือมากกว่าที่พิกัดของมันเป็นจำนวนเต็มทั้งคู่ พิกัดที่เป็นจำนวนเต็มทั้งคู่เราจะเรียกว่า จุดแลตทิซ (lattice point) เราจะเรียกสมการ (1) ว่าสมการไดโอแฟนไทด์ ซึ่งจะมีผลเฉลยเป็นคู่ของจำนวนเต็ม x', y' ที่แทนค่าแล้วสอดคล้องกับสมการ และเราจะเรียกจำนวนเต็ม x และ y ว่า เป็นส่วนประกอบของผลเฉลย

การแก้สมการไดโอแฟนไทด์ หมายความว่าเราจะต้องหาคู่ของจำนวนเต็ม x และ y ซึ่งสอดคล้องกับสมการ นั่นคือเราจะต้องหาจุดแลตทิซทั้งหมดในกราฟของสมการนั้น

ตัวอย่าง 10 สมการไดโอแฟนไทด์ $2x+3y=11$ จะได้จุดแลตทิซ 2 จุดคือ $(1,3)$ และ $(7,-1)$ ในขณะที่ $(5,\frac{1}{3})$ ก็เป็นจุดบนกราฟเหมือนกัน แต่ไม่เป็นจุดแลตทิซเพราะพิกัด y ไม่เป็นจำนวนเต็ม

ตัวอย่างของสมการไดโอแฟนไทด์ ซึ่งไม่มีจุดแลตทิซแม้แต่จุดเดียว เช่น $2x+4y=3$ ถ้ามีจำนวนเต็ม x' และ y' ที่สอดคล้องกับสมการนี้ จะได้ว่า $2(x'+2y')=3$ แต่เป็นไปไม่ได้เนื่องจากข้างซ้ายของสมการต้องหารด้วย 2 ลงตัว แต่ข้างขวาไม่สามารถหารด้วย 2 ลงตัว #

ตัวอย่าง 11 จงวาดกราฟของ $3x+4y=15$ และหาจุดแลตทิซทั้งหมดในจตุภาคที่ 1 รวมทั้งจุดที่อยู่บนแกน

<u>วิธีทำ</u> หาจุดตัดแกน x โดยให้ $y=0$ ดังนั้นจะได้ $x=\frac{15}{3}=5$ นั่นคือจะตัดแกน x ที่จุด $(5,0)$

หาจุดตัดแกน y โดยให้ $x=0$ ดังนั้นจะได้ $y=\frac{15}{4}=3\frac{3}{4}$ นั่นคือจะตัดแกน y ที่จุด $(0,3\frac{3}{4})$

จะได้จุดแลตทิซ 2 จุดคือจุด $(1,3)$ และ $(5,0)$ #

การมีอยู่ของผลเฉลยของสมการไดโอแฟนไทด์เชิงเส้น

เราได้ทราบแล้วว่า ไม่ใช่ทุก ๆ สมการในรูปแบบ

$$ax+by=c \qquad \text{-------} (1)$$

จะมีผลเฉลยเสมอไป เนื่องจาก (a,b) หาร a และ b ซึ่งเป็นสัมประสิทธิ์ของ x และ y ลงตัว แสดงว่า (a,b) ต้องหาร c ซึ่งอยู่ด้านขวาของสมการลงตัวด้วย

สมมติให้ $d=(a,b)$ ซึ่ง $d \mid c$ จากสมการ (1) หารด้วย d ตลอด จะได้

$$\frac{a}{d}x+\frac{b}{d}y=\frac{c}{d} \qquad \text{--------} (2)$$

แต่ $a \mid d, b \mid d$ และ $c \mid d$ ซึ่งอยู่ในรูปของเศษส่วน และเป็นจำนวนเต็ม เพราะ d เป็นตัวหารของ a และ b และโดยสมมติฐาน d เป็นตัวหารของ c ด้วย ทำให้ได้ว่าจำนวนเต็ม $a \mid d$ และ $b \mid d$ เป็นจำนวนเฉพาะสัมพัทธ์ เพราะว่า d เป็นห.ร.ม.ของ a และ b ดังบทแทรก (1)

บทแทรก (1) ถ้า $d=(a,b)$ และ a และ b ถูกเขียนอยู่ในรูปแบบ $a=da'$ และ $b=db'$ แล้ว a' และ b' จะเป็นจำนวนเฉพาะสัมพัทธ์

จะเห็นว่า ค่า x และ y ที่สอดคล้องกับสมการ (1) จะสอดคล้องกับสมการ (2) ด้วย หรือในทางกลับกัน คือ x และ y ที่สอดคล้องกับสมการ (2) จะสอดคล้องกับสมการ (1) ด้วย ดังนั้นการแก้

สมการไดโอแฟนไทด์ในสมการ (1) สามารถจะแก้ในรูปแบบที่สมการไดโอแฟนไทด์มีสัมประสิทธิ์เป็นจำนวนเฉพาะสัมพัทธ์ของตัวแปร

เนื่องจาก $(a|d,b|d)=1$ จาก Propertys กล่าวว่าจะมีจำนวนเต็ม x_0, y_0 ซึ่ง

$$\left(\frac{a}{d}\right)x_0+\left(\frac{b}{d}\right)y_0=1 \qquad \text{---------- (3)}$$

และการหาจำนวนเต็ม x_0 และ y_0 อาจหาได้จากการเขียน x_0 และ y_0 ในรูปผลรวมเชิงเส้นของ 1 จากสมการ (3) เราคูณตลอดด้วย c จะได้

$$a\left(\frac{x_0c}{d}\right)+b\left(\frac{y_0c}{d}\right)=c \qquad \text{---------- (4)}$$

ซึ่งให้ $x_1=\frac{x_0c}{d}$ และ $y_1=\frac{y_0c}{d}$ ดังนั้นจะได้ $ax_1+by_1=c$

นั่นคือจะได้ผลเฉลยของ $ax+by=c$ เป็น $x_1=\frac{x_0c}{d}$, $y_1=\frac{y_0c}{d}$ และแน่นอนว่า x_1 และ y_1 เป็นจำนวนเต็ม เพราะ d เป็นตัวหารของ c ตามสมมติฐาน

ตัวอย่าง 12 จงหาผลเฉลยของ

<u>วิธีทำ</u> ในที่นี้ $a=4,b=6,c=12,d=2$

และจากสมการ (3) จะได้ $2x+3y=1$ ซึ่งสอดคล้องกับ $x_0=2,y_0=-1$

ดังนั้น $x_1=\frac{(2\times12)}{2}, y_1=\frac{(-1\times12)}{2}$ และ $x_1=12, y_1=-6$

เป็นผลเฉลยของ $4x+6y=12$

เราเคยพิสูจน์มาแล้วว่าสมการไดโอแฟนไทด์เชิงเส้น $ax+by=c$ จะมีผลเฉลย ก็ต่อเมื่อ $\frac{(a,b)}{c}$ ซึ่งจะได้ผลเฉลยเป็น

$$x_1=\frac{x_0c}{d}, y_1=\frac{y_0c}{d}$$

ซึ่ง x_0, y_0 เป็นผลเฉลยของ $(a|b)x+(b|d)y=1$ #

ตัวอย่าง 13 จงหาผลเฉลยของสมการไดโอแฟนไทด์ต่อไปนี้

(a) $6x+9y=2$

<u>คำตอบ</u> เนื่องจาก $(6,9)=3$ แต่ $3\nmid 2$ ดังนั้นสมการนี้ไม่มีผลเฉลย

(b) $117x+52y=26$

<u>คำตอบ</u> เนื่องจาก $a=117, b=52, c=26, d=(117,52)=13$ ซึ่ง $13 \mid 26$ ดังนั้นสมการนี้มีผลเฉลย จากสมการ (3) สมการนี้จะอยู่ในรูปแบบ $\left(\frac{117}{13}\right)x_0+\left(\frac{52}{13}\right)y_0=1$

หรือ $9x_0+4y_0=1$

ซึ่งสอดคล้องกับ $x_0=1$ และ $y_0=-2$ ดังนั้น $x_1=\frac{x_0c}{d}=\frac{(1)(26)}{13}=2$

และ $y_1=\frac{y_0c}{d}=\frac{(-2)(26)}{13}=-4$ เป็นผลเฉลยของ $117x+52y=26$

(ตรวจคำตอบ $117(2)+52(-4)=26$ จริง) #

2.3.2 การหาผลเฉลยโดยอาศัยอัลกอริทึมของยูคลิด

ถ้าสมการไดโอแฟนไทน์เชิงเส้นต่อไปนี้มีผลเฉลย

$$ax-by=c \qquad \text{---------- (1)}$$

และสมมติ a และ b เป็นจำนวนเฉพาะสัมพัทธ์ ซึ่งจะหาจำนวนเต็ม x' และ y' ซึ่ง

$$ax'-by'=1 \qquad \text{---------- (2)}$$

เนื่องจาก $(a,b)=1$ ถ้าคูณตลอดด้วย c จะได้ $a(cx')-b(cy')=c$

ให้ $cx'=x''$ และ $cy'=y''$ จะได้ $ax''-by''=c$ ดังนั้นจะได้ว่า

สมการมีผลเฉลยเสมอ คือ

$$x''=cx', y''=cy' \qquad \text{----------(3)}$$

ตัวอย่าง 14 กำหนดสมการไดโอแฟนไทน์ $119x-98y=-68$

จะได้ $a=199, b=98$ และ $c=-68$ ซึ่งเราต้องการหาจำนวนเต็ม x' และ y' ซึ่ง $ax'+by'=1$

โดยอัลกอริทึมของยูคลิดจะได้

$$199=2(98)+3$$
$$98=32(3)+2$$
$$3=1(2)+1$$
$$2=2(1)+0$$

ดังนั้น

$$\begin{aligned}1&=3-(2)\\&=3-[98-32(3)]\\&=199-2(98)-\{98-32[199-2(98)]\}\end{aligned}$$

$$= 199 - 2(98) - [98 - 32(199) + 64(98)]$$
$$= 199 - 2(98) - 98 + 32(199) - 64(98)$$
$$= 33(199) - 67(98)$$

ดังนั้น $x' = 33$ และ $y' = 67$ และจากสมการ (3) จะได้

$$x'' = cx' = (-68)(33) = -2244$$
$$y'' = cy' = (-68)(67) = -4556$$

เป็นผลเฉลยของสมการ $199x - 98y = -68$

ซึ่งตรวจคำตอบได้ดังนี้ $199(-2244) - 98(-4556) = -68$

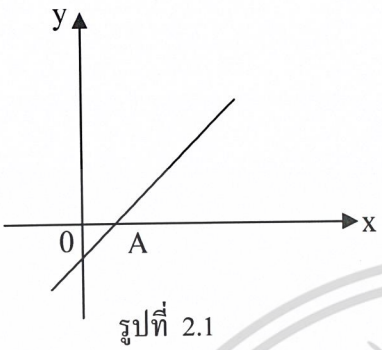
ซึ่งหมายความว่า $x'' = -2244, y' = -4556$ เป็นผลเฉลยหนึ่งของสมการ

$199x - 98y = -68$ ดังนั้นผลเฉลยทั้งหมดของสมการนี้คือ

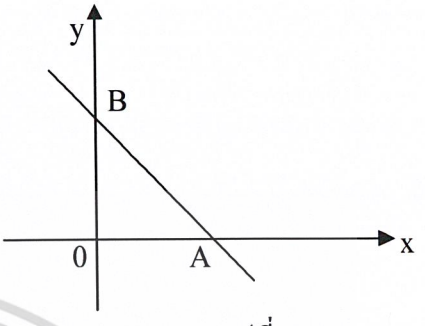
$$x = -2244 - 98t, y = -4556 - 199t$$ #

2.3.3 จุดแลตทิชที่เป็นบวกมีจำนวนจำกัดหรืออนันต์

ถ้าพิกัดของจุดแลตทิชทั้งสองจุด เป็นบวกหรือศูนย์ เราจะเรียกจุดแลตทิชบวก ซึ่งกราฟของสมการไดโอแฟนไทน์สามารถบอกเราได้ว่า จุดแลตทิชที่เป็นบวกมีจำนวนจำกัด หรืออนันต์ ทุกๆกราฟของสมการเชิงเส้น $ax + by = c$ จะเป็นเส้นตรงซึ่งความชันของเส้นตรงนี้คือ $-a/b$ และค่าความชันนี้จะเป็นบวก ถ้า a และ b มีเครื่องหมายตรงกันข้าม และมีความชันเป็นลบถ้า a และ b มีเครื่องหมายเดียวกัน แต่เส้นตรงที่มีความชันเป็นบวก มันจะเฉียงขึ้นจากซ้ายไปขวา ในขณะที่เส้นตรงที่มีความชันเป็นลบ มันจะพุ่งลงจากซ้ายไปขวา ซึ่งหมายความว่า เส้นตรงที่มีความชันเป็นบวก ไม่มีจุดแลตทิชที่เป็นบวก หรือหมายความว่ามีจุดแลตทิชที่เป็นบวกจำนวนอนันต์อยู่ในจตุภาคที่ 1 ซึ่งทั้ง x และ y เป็นบวกทั้งคู่ หรือเป็น ศูนย์ทั้งคู่ แต่ถ้าความชันเป็นลบจะมีส่วนของกราฟส่วนหนึ่งที่อยู่ในจตุภาคที่ 1 และจะได้ว่าจะมีจุดแลตทิชที่เป็นบวกเป็นจำนวนจำกัด ดังนั้น ในรูปที่ 2.1 ซึ่งความชันเป็นบวกจะมีจำนวนจุดแลตทิชที่ความชันเป็นบวก จำนวนอนันต์ อยู่บนส่วนของกราฟที่อยู่ทางด้านขวาของ A ในรูปที่ 2.2จะมีจำนวนจุดแลตทิชที่เป็นบวกจำนวนจำกัด(บางทีอาจไม่มีเลย) ซึ่งอยู่ระหว่าง B และ A ตัวอย่างเช่น สมการไดโอแฟนไทน์ $2x + 5y = 17$ ซึ่งความชัน $-\frac{2}{5}$ ดังนั้นมันจะมีจุดแลตทิชที่เป็นบวกเป็นจำนวนจำกัด ซึ่งมี 2 จุด คือ (1,3) และ (6,1) แต่อีกสมการหนึ่ง คือ $6x - 5y + 17 = 0$ ซึ่งมีความชันเป็นบวก คือ $\frac{6}{5}$ ดังนั้นกราฟของมันจะมีจำนวนจุดแลตทิชที่เป็นบวกจำนวนอนันต์ จุดแลตทิชจุดหนึ่งคือ (3,7)



รูปที่ 2.1



รูปที่ 2.2

สมการไดโอแฟนไทน์(Diophantine Equation) คือ สมการใดๆ ที่มีตัวไม่ทราบค่าตัวเดียวหรือมากกว่าหนึ่งตัวที่ต้องการหารากหรือผลเฉลยที่เป็นจำนวนเต็ม สมการไดโอแฟนไทน์แบบที่ง่ายที่สุดที่เราจะศึกษาในหัวข้อนี้คือ สมการในรูป

$$ax + by = c$$

โดยที่ a, b, c เป็นจำนวนเต็มที่กำหนดให้และไม่เป็น 0 รากหรือผลเฉลยของสมการนี้ก็คือ จำนวนเต็ม x_0, y_0 ที่เมื่อนำไปแทนในสมการที่ให้มาแล้วทำให้สมการเป็นจริง นั่นคือเราต้องการให้ได้ว่า $ax_0 + by_0 = c$

บทนิยาม สมการที่อยู่ในรูป $a_1x_1 + a_2x_2 + ... + a_nx_n = k$ เมื่อ $a_1, a_2, ..., a_n, k$ เป็นค่าคงตัวซึ่งเป็นจำนวนเต็มที่ไม่ใช่ 0 และ $x_1, x_2, ..., x_n$ เป็นตัวแปรซึ่งมีขอบเขตเป็นเซตของจำนวนเต็ม เรียกสมการดังกล่าวว่า สมการไดโอแฟนไทน์เชิงเส้นชนิด n ตัวแปร

ตัวอย่าง 14 $2x + 3y = 5$ เป็นสมการไดโอแฟนไทน์เชิงเส้นชนิด 2 ตัวแปร

$\sqrt{2}x + 5y = 7$ ไม่เป็นสมการไดโอแฟนไทน์เชิงเส้น เพราะ $\sqrt{2} \notin \mathrm{I}$

$5x - 7y + 9z - w = 1$ เป็นสมการไดโอแฟนไทน์เชิงเส้น ชนิด 4 ตัวแปร

$2x - xy + 5 = 0$ ไม่เป็นสมการเชิงเส้น เพราะมีพจน์ xy #

บทนิยาม เรียกจำนวนเต็มที่แทนค่าตัวแปรในสมการไดโอแฟนไทน์ แล้วทำให้สมการเป็นจริงว่า ผลเฉลย

ตัวอย่าง 15 $x=5, y=2$ เป็นผลเฉลยของสมการไดโอแฟนไทน์ $3x+4y=23$ เพราะเป็นจำนวนเต็มและทำให้

สมการเป็นจริง

แต่ $x=\frac{7}{3}, y=4$ ไม่เป็นผลเฉลยของสมการไดโอแฟนไทน์ $3x+4y=23$

เพราะ $\frac{7}{3}$ ไม่ใช่จำนวนเต็ม #

สมการไดโอแฟนไทน์สมการหนึ่งๆอาจมีรากได้หลายราก อย่างเช่นสมการ $3x+6y=18$ เราได้

$$3\cdot 4+6\cdot 1=18$$
$$3\cdot(-6)+6\cdot 6=18$$
$$3\cdot 10+6\cdot(-2)=18$$

แต่ก็มีบางกรณีเช่นกันที่สมการไม่มีราก อย่างเช่น $2x+10y=17$ ทั้งนี้เพราะไม่ว่าจะแทน x และ y ด้วยจำนวนเต็มใดๆ พจน์ทางซ้ายเป็นจำนวนคู่ในขณะที่พจน์ทางขวาเป็นจำนวนคี่ ในตอนนี้เราจะพิจารณาว่าภายใต้เงื่อนไขใดที่ทำให้สมการมีราก และถ้ามีรากจะหารากทุกชุดออกมาได้อย่างไร

ทฤษฎีบท 6 สมการไดโอแฟนไทน์ $ax+by=c$ ซึ่ง $d=(a,b)$ จะมีผลเฉลยเป็นจำนวนเต็มก็ต่อเมื่อ $d|c$

<u>พิสูจน์</u> ตอน 1 ให้ $ax+by=c$ มีผลเฉลยเป็นจำนวนเต็ม คือ $x=x_0$ และ $y=y_0$ ดังนั้น $ax_0+by_0=c$

เนื่องจาก $d=(a,b)$ ดังนั้น $d|a$ และ $d|b$

จะได้ $d|(ax_0+by_0)$ ดังนั้น $d|c$

ตอน 2 ให้ $d|c$ จะได้ว่ามีจำนวนเต็ม n ซึ่ง $dn=c$

เนื่องจาก $d=(a,b)$ ดังนั้นมีจำนวนเต็ม x_1, y_1 ซึ่ง $ax_1+by_1=d$

แทนค่า d จะได้ $(ax_1+by_1)n=c$ หรือ $ax_1n+by_1n=c$

จะได้ $x_0=x_1n, y_0=y_1n$ เป็นผลเฉลยของสมการ $ax+by=c$

นั่นคือ $ax+by=c$ มีผลเฉลยเป็นจำนวนเต็ม #

ตัวอย่าง 16 จงพิจารณาสมการไดโอแฟนไทน์ต่อไปนี้

1. $14x-45y=11$ มีผลเฉลยเพราะ $(14,-45)=1$ ซึ่ง $1|11$
2. $56x-50y=74$ มีผลเฉลยเพราะ $(56,-50)=2$ ซึ่ง $2|74$
3. $75x-50y=200$ มีผลเฉลยเพราะ $(75,50)=25$ ซึ่ง $25|200$
4. $48x-32y=30$ ไม่มีผลเฉลยเพราะ $(48,32)=16$ ซึ่ง $16\nmid 30$ #

ทฤษฎีบท 7 ถ้า $x=x_0,\ y=y_0$ เป็นผลเฉลยของสมการไดโอแฟนไทน์ $ax+by=c$ แล้วผลเฉลยทั้งหมดของสมการเขียนในรูปทั่วไป คือ

$$x=x_0+\frac{b}{d}t, y=y_0-\frac{a}{d}t$$

เมื่อ $d=(a,b)$ และ t เป็นจำนวนเต็มใดๆ

<u>พิสูจน์</u> ตอน 1 เราจะพิสูจน์ว่า $x=x_0+\frac{b}{d}t, y=y_0-\frac{a}{d}t$ เป็นผลเฉลยของสมการ เมื่อ t เป็นจำนวนเต็มใดๆ

โดยแทนค่า x,y ในข้างซ้ายของสมการจะได้

$$\begin{aligned} a(x_0+\frac{b}{d}t)+b(y_0-\frac{a}{d}t) &= ax_0+\frac{ab}{d}t+by_0-\frac{ab}{d}t \\ &= ax_0+by_0 \\ &= c \text{ เพราะ } x_0, y_0 \text{ เป็นผลเฉลยของสมการ} \end{aligned}$$

ดังนั้น $x=x_0+\frac{b}{d}t, y=y_0-\frac{a}{d}t$ เป็นผลเฉลยของสมการ เมื่อ t เป็นจำนวนเต็มใดๆ

ตอน 2 เราจะพิสูจน์ว่าทุกผลเฉลยของสมการจะสามารถเขียนในรูป

$x=x_0+\frac{b}{d}t, y=y_0-\frac{a}{d}t$

เมื่อ t เป็นจำนวนเต็มใดๆ

ให้ x,y เป็นผลเฉลยใดๆของสมการ และ x_0, y_0 เป็นผลเฉลยหนึ่ง

จะได้ $ax+by=c$ และ $ax_0+by_0=c$

ดังนั้น $ax+by=ax_0+by_0$

จะได้ $a(x-x_0)=b(y_0-y)$

เนื่องจาก $(a,b)=d$ จะได้ $(\frac{a}{d},\frac{b}{d})=1$

ให้ $r=\frac{a}{d}$ และ $s=\frac{b}{d}$

ดังนั้น $r(x-x_0)=s(y_0-y)$

จะได้ $r \mid s(y_0-y)$ แต่ $(r,s)=1$

ดังนั้น $r \mid (y_0-y)$

จะได้ว่ามีจำนวนเต็ม t ซึ่ง $y_0-y=rt$ นั่นคือ $y=y_0-rt$

แทนค่า $y_0-y=rt$ ใน $r(x-x_0)=s(y_0-y)$

จะได้ $r(x-x_0)=srt$

$$x-x_0=st$$

$$x=x_0+st$$

นั่นคือ ทุกผลเฉลยจะเขียนได้ในรูป $x=x_0+\frac{b}{d}t, y=y_0-\frac{a}{d}t$ #

ตัวอย่าง 17 จงหารากทั่วไปของสมการไดโอแฟนไทน์เชิงเส้น

$$172x+20y=1000$$

<u>วิธีทำ</u> ใช้ขั้นตอนวิธีแบบยูคลิดหา $(172,20)$ เราได้

$$172=8\cdot 20+12$$

$$20=1\cdot 12+8$$

$$12=1\cdot 8+4$$

$$8=2\cdot 4+0$$

ดังนั้น $(172,20)=4$ เนื่องจาก $4 \mid 1000$

เมื่อเขียน 4 เป็นผลรวมเชิงเส้น ของ 172 และ 20 โดยทำกระบวนการข้างต้นนี้ย้อนกลับ จะได้

$$4=12-8$$

$$=12-(20-12)$$

$$=2\cdot 12-20$$

$$=2(172-8\cdot 20)-20=2\cdot 172+(-17)20$$

คูณความสัมพันธ์นี้ด้วย 250 เราได้

$$1000=250\cdot 4=250(2\cdot 172+(-17)20)$$

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

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

$$x=500+(20/4)t=500+5t$$

$$y = -4250 - (172/4)t = -4250 - 43t$$ #

ในชีวิตจริงมีอยู่บ่อยครั้งที่เดียวที่เราต้องการแก้สมการในรูป $ax + by = c$ โดยที่เราต้องการคำตอบเป็นจำนวนเต็มบวก

ตัวอย่าง 18 คุณแม่ให้เงินแพรว 1,500 บาท เพื่อซื้อเสื้อยืดมาไว้ขาย แพรวซื้อเสื้อเสร็จแล้วนำเงินมาทอนคุณแม่ 363 บาท พร้อมกับบอกคุณแม่ว่าเสื้อยืดแขนสั้นราคาตัวละ 39 บาท เสื้อยืดแขนยาวราคาตัวละ 69 บาท จงหาว่าแพรวซื้อเสื้ออย่างละกี่ตัว

<u>วิธีทำ</u> สมมติว่าแพรวซื้อเสื้อแขนสั้น x ตัว และซื้อเสื้อแขนยาว y ตัว จะได้ว่า

$$39x + 69y = 1137$$

เราทอนเป็นสมการในรูปง่ายขึ้น

$$13x + 23y = 379$$

ใช้ขั้นตอนยูคลิดในการหา ห.ร.ม. ของ 13 และ 23 จะได้ว่า

$$23 = 13 \cdot 2 - 3$$

$$13 = 3 \cdot 4 + 1$$

$$3 = 1 \cdot 3$$

ฉะนั้น $(13,23) = 1$ และ

$$\begin{aligned} 1 &= 13 - 3 \cdot 4 \\ &= 13 - (13 \cdot 2 - 23) \cdot 4 \\ &= 13 \cdot (-7) + 23 \cdot 4 \end{aligned}$$

ดังนั้น $13 \cdot (-7 \cdot 379) + 23 \cdot (4 \cdot 379) = 379$

$$x = -2653 + 23t \text{ และ } y = 1516 - 13t$$

โดยที่ t เป็นจำนวนเต็ม

เราต้องการให้ $x \geq 0$ และ $y \geq 0$ จึงได้ว่า

$$t \geq \frac{2653}{23} = 115\frac{8}{23} \text{ และ } t \leq \frac{1516}{13} = 116\frac{8}{13}$$

ดังนั้น $t = 116$ ซึ่งทำให้ $x = 15$ และ $y = 8$

สรุปได้ว่า แพรวซื้อเสื้อยืดแขนสั้น 15 ตัว และซื้อเสื้อยืดแขนยาว 8 ตัว #

ตัวอย่าง 19 เขียวไปจ่ายตลาดซื้อผลไม้มาสองอย่าง คือ แตงโมและ สัปปะรด รวมกัน 12 ผล โดยจ่ายเงินไป 132 บาท ถ้าแตงโมแพงกว่าสัปปะรดผลละ 3 บาท และซื้อแตงโมมากกว่าสัปปะรด อยากทราบว่าเขียวได้แตงโมและสัปปะรดมาอย่างละกี่ผล

<u>วิธีทำ</u> ให้ x เป็นจำนวนแตงโม และ y เป็นจำนวนสัปปะรด ให้ z เป็นราคา (เป็นบาท) ของสัปปะรด จากเงื่อนไขของโจทย์เราได้

$$(z+3)x + zy = 132$$

หรือ

$$3x + (x+y)z = 132$$

เนื่องจาก $x+y=12$ ดังนั้น

$$3x + 12z = 132$$

หรือ

$$x + 4z = 44$$

ในการหาจำนวนเต็ม x และ z ที่สอดคล้องกับสมการ $x+4z=44$ สังเกตว่า $(1,4)=1$ และ $1 \mid 44$ ดังนั้นสมการดังกล่าวมีราก จากการคูณ $1 = 1(-3) + 4 \cdot 1$ ด้วย 44 เราได้

$$44 = 1(-132) + 4 \cdot 44$$

ซึ่งจะได้ต่อไปว่า $x_0 = -132, z_0 = 44$ เป็นรากหนึ่งของสมการ รากทั่วไปจะอยู่ในรูป

$$x = -132 + 4t, z = 44 - t$$

โดยที่ t เป็นจำนวนเต็ม แต่ค่า t ที่เราต้องการคือค่า t ที่ทำให้ $12 \geq x \geq 6$ นั่นคือ

$$12 \geq -132 + 4t > 6$$

ซึ่งจะได้ $34.5 < t \leq 36$ ดังนั้น $t = 35$ หรือ $t = 36$ ดังนั้นจึงมีทางที่เขียวจะซื้อผลไม้ได้คือ ซื้อแตงโมทั้ง 12 ผล ในราคาผลละ 11 บาท (กรณี $t = 36$) หรือ ซื้อแตงโม 8 ผลๆละ 12 บาท และ สัปปะรด 4 ผลๆละ 9 บาท (กรณี $t = 35$) แต่ตามเงื่อนไขของโจทย์ กรณีหลังจะเกิดขึ้นได้เพียงกรณีเดียว #

2.3.4 สมการไดโอแฟนไทน์เชิงเส้นที่มี 3 ตัวแปรหรือมากกว่า (Linear Congruence)

2.3.4.1 สมบัติเบื้องต้นของสมภาค

ในที่นี้เราจะศึกษาปัญหาการหารลงตัวในอีกแง่มุมหนึ่ง กล่าวคือ ศึกษาเลขคณิตของเศษเหลือ (remainder) หรือทฤษฎีของคอนกรูเอนซ์ ซึ่งในปัจจุบันเป็นที่รู้จักกันดี มโนทัศน์และสัญลักษณ์

เกี่ยวกับเรื่องนี้ เกาส์ (Carl Friedrich Gauss (1777-1855)) ได้นำมาใช้ในหนังสือ Disquisitiones Arithmeticae ที่เขาเขียนในปี ค.ศ. 1801 อันเป็นรากฐานของทฤษฎีจำนวนแนวใหม่ในปัจจุบัน

บทนิยาม ให้ a และ b เป็นจำนวนเต็ม ให้ n เป็นจำนวนเต็มที่ตรึงค่าจำนวนหนึ่ง ถ้า $n \mid a-b$ หรืออีกนัยหนึ่ง ถ้า $a-b=kn$ สำหรับจำนวนเต็ม k บางค่าแล้ว เรากล่าว **a คอนกรูเอนซ์กับ b มอดุโล n** (a is congruent to b modulo n) ในกรณีนี้เราเขียน

$$a \equiv b(\mathrm{mod}\, n)$$

ถ้า $n \nmid a-b$ เรากล่าวว่า **a ไม่คอนกรูเอนซ์กับ b มอดุโล n** (a is incongruent to b modulo n) ในกรณีนี้เราเขียน $a \equiv b(\mathrm{mod}\, n)$ จำนวนเต็ม n ในที่นี้เรียกว่า **มอดุโล** (modulo)

สังเกตว่า จำนวนเต็มสองจำนวนใดๆ จะคอนกรูเอนซ์มอดุโล 1 เสมอ และจำนวนเต็มสองจำนวนจะคอนกรูเอนซ์มอดุโล 2 ก็ต่อเมื่อจำนวนทั้งสองนั้นเป็นจำนวนคู่ทั้งคู่หรือเป็นจำนวนคี่ทั้งคู่ เนื่องจาก
คอนกรูเอนซ์มอดุโล 1 ไม่มีอะไรที่น่าสนใจมากนัก ดังนั้นโดยทั่วไปเราจะพิจารณาเฉพาะกรณี n > 1

ตัวอย่าง 20 สำหรับ $n=7$ เราได้

$$3 \equiv 24(\mathrm{mod}\, 7)$$
$$-15 \equiv -64(\mathrm{mod}\, 7)$$ #

ตัวอย่าง 21 $7 \equiv 8(\mathrm{mod}\, 5)$ เพราะ $5 \mid (7-2)$

$47 \equiv 35(\mathrm{mod}\, 6)$ เพราะ $6 \mid (47-35)$

เราเรียก m ว่า มอดูลัส
การดำเนินการภายใต้มอดูลัสเดียวกันมีสมบัติดังนี้

ถ้า $a_1 \equiv b_1(\mathrm{mod}\, m)$ และ $a_2 \equiv b_2(\mathrm{mod}\, m)$

แล้วจะได้ $a_1 \pm a_2 \equiv b_1 \pm b_2(\mathrm{mod}\, m)$ และ $a_1 a_2 \equiv b_1 b_2(\mathrm{mod}\, m)$

<u>ข้อควรระวัง</u>

1. ถ้า $ac \equiv bc(\mathrm{mod}\, m)$ มันไม่จำเป็นที่ $a \equiv b(\mathrm{mod}\, m)$ ตัวอย่างเช่น

$15 \cdot 2 \equiv 20 \cdot 2(\mathrm{mod}\, 10)$
แต่ $15 \not\equiv 20(\mathrm{mod}\, 10)$

2. มันเป็นไปได้ที่ $uv \equiv 0(\mathrm{mod}\, m)$ แต่ $u \equiv /0(\mathrm{mod}\, m)$ และ $v \equiv /0(\mathrm{mod}\, m)$ ตัวอย่างเช่น $6 \cdot 4 \equiv 0(\mathrm{mod}\, 12)$ แต่ $6 \not\equiv 0(\mathrm{mod}\, 12)$ และ $4 \not\equiv 0(\mathrm{mod}\, 12)$

ทฤษฎีบท 8 สำหรับจำนวนเต็ม a และ b ใดๆ $a \equiv b(\mathrm{mod}\, m)$ ก็ต่อเมื่อ a หารด้วย m และ b หารด้วย m จะเหลือเศษเท่ากัน

<u>พิสูจน์</u> ตอน 1 ให้ $a \equiv b(\mathrm{mod}\, m)$

ดังนั้น $m \mid (a-b)$ (จากบทนิยามคอนกรูเอนซ์)

จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a-b=km$ ดังนั้น $a=km+b$

นำ m ไปหาร b ได้เศษ r จากขั้นตอนวิธีการหารจะได้ว่า

มีจำนวนเต็ม q ซึ่ง $b=qm+r, 0<r<m$

จาก $a=km+b$

แทนค่า b จะได้ $a=km+(qm+r)=(k+q)m+r, 0<r<m$

จะได้ว่าเมื่อนำ m มาหาร a จะเหลือเศษเท่ากับ r

นั่นคือเมื่อนำ m ไปหาร a และ b จะเหลือเศษเท่ากัน

ตอน 2 ถ้านำ m ไปหาร a และ b แล้วเหลือเศษ r เท่ากัน

จะได้ว่ามีจำนวนเต็ม q_1, q_2 ซึ่ง $a=q_1m+r, 0<r<m$

$b=q_2m+r, 0<r<m$

ดังนั้น $a-b=(q_1-q_2)m$

แต่ q_1-q_2 เป็นจำนวนเต็มจะได้ $m \mid (a-b)$

นั่นคือ $a \equiv b(\mathrm{mod}\, m)$ #

ตัวอย่าง 22 ถ้านำจำนวนเต็มใดๆ มาหารด้วย 2

1. จงหาเศษการหารที่เป็นไปได้
2. จงจัดกลุ่มจำนวนเต็มให้สมาชิกในกลุ่มเป็นจำนวนที่หารด้วย 2 แล้วเหลือเศษเท่ากัน
3. จำนวนเต็มแต่ละคู่ในกลุ่มเดียวกัน จาก 2. จะคอนกรูเอนซ์กันในมอดุโล 2 หรือไม่

<u>วิธีทำ</u> 1. ให้ n เป็นจำนวนเต็มใดๆ พิจารณา n และจำนวนเต็ม 2

จากขั้นตอนวิธีการหารจะมี q และ r ซึ่ง $n=2q+r, 0<r<2$

จะได้ $r=0,1$ เป็นเศษที่เป็นไปได้

2. กลุ่มของจำนวนเต็มที่หารด้วย 2 แล้วเหลือเศษ 0 คือ เซตของจำนวนคู่

$\{...,-4,-1,0,2,4,...\} = \{2k \mid k \in \mathrm{I}\}$

กลุ่มของจำนวนเต็มที่หารด้วย 2 แล้วเหลือเศษ 1 คือ เซตของจำนวนคี่

$\{...,-3,-1,1,3,...\} = \{2k+1 \mid k \in \mathrm{I}\}$

3. จากทฤษฎีบท จะได้ว่า

$... \equiv -4 \equiv -2 \equiv 0 \equiv 2 \equiv 4 \equiv ...(\mathrm{mod}\, 2)$

$... \equiv -3 \equiv -1 \equiv 1 \equiv 3 \equiv ...(\mathrm{mod}\, 2)$ #

ตัวอย่าง 23 จงหาเศษที่เป็นไปได้จากการหารจำนวนเต็มใดๆ ด้วยจำนวนเต็มต่อไปนี้

1. หารด้วย 3
2. หารด้วย 4
3. หารด้วยจำนวนเต็มบวก m

<u>วิธีทำ</u> 1. จำนวนเต็มใดๆเมื่อหารด้วย 3 จะเหลือเศษที่เป็นไปได้คือ 0,1,2

2. จำนวนเต็มใดๆเมื่อหารด้วย 4 จะเหลือเศษที่เป็นไปได้คือ 0,1,2,3

3. จำนวนเต็มใดๆเมื่อหารด้วยจำนวนเต็มบวก m จะเหลือเศษที่เป็นไปได้คือ $0,1,2,...,m-1$ #

2.3.4.2 สมบัติของคอนกรูเอนซ์

ทฤษฎีบท 9 ให้ $m > 0$ และ a,b,c เป็นจำนวนเต็มใดๆ ต่อไปนี้เป็นจริง

1. $a \equiv a(\mathrm{mod}\, m)$
2. ถ้า $a \equiv b(\mathrm{mod}\, m)$ แล้ว $b \equiv a(\mathrm{mod}\, m)$
3. ถ้า $a \equiv b(\mathrm{mod}\, m)$ และ $b \equiv c(\mathrm{mod}\, m)$ แล้ว $a \equiv c(\mathrm{mod}\, m)$

<u>พิสูจน์ 1</u>. เนื่องจาก $m \mid (a-a)$ ดังนั้น $a \equiv a(\mathrm{mod}\, m)$

<u>พิสูจน์ 2</u>. จาก $a \equiv b(\mathrm{mod}\, m)$ จะได้ $m \mid (a-b)$

จะได้ $m \mid -1(b-a)$

ดังนั้น $m \mid (a-b)$

นั่นคือ $b \equiv a(\mathrm{mod}\, m)$

<u>พิสูจน์ 3</u>. จาก $a \equiv b(\mathrm{mod}\, m)$ และ $b \equiv c(\mathrm{mod}\, m)$

จะได้ $m \mid (a-b)$ และ $m \mid (b-c)$

จะได้ $m \mid (a-b+b-c)$

ดังนั้น $m \mid (a-c)$

นั่นคือ $a \equiv c(\text{mod}\, m)$

<u>หมายเหตุ</u> จากทฤษฎีกล่าวได้ว่า

1. คอนกรูเอนซ์มีสมบัติสะท้อน
2. คอนกรูเอนซ์มีสมบัติสมมาตร
3. คอนกรูเอนซ์มีสมบัติถ่ายทอด

และจากทั้ง 3 กล่าวได้ว่า คอนกรูเอนซ์ เป็นความสัมพันธ์สมมูล (equivalence relation)

ทฤษฎีบท 10 กำหนดจำนวนเต็ม $m > 0$ และ a, b, c เป็นจำนวนเต็มใดๆ ต่อไปนี้เป็นจริง

1. ถ้า $a \equiv b(\text{mod}\, m)$ และ $c \equiv d(\text{mod}\, m)$

   ก. $a + c \equiv b + d(\text{mod}\, m)$

   ข. $ac \equiv bd(\text{mod}\, m)$

2. ถ้า $a \equiv b(\text{mod}\, m)$ แล้ว

   ก. $a + c \equiv b + d(\text{mod}\, m)$

   ข. $ac \equiv bc(\text{mod}\, m)$

   ค. $ac \equiv bc(\text{mod}\, mc)$ ถ้า $c > 0$

   ง. $a^n \equiv b^n(\text{mod}\, m)$ สำหรับทุกจำนวนเต็มบวก n

<u>พิสูจน์ 1. ก.</u> จาก $a \equiv b(\text{mod}\, m)$ และ $c \equiv d(\text{mod}\, m)$

จะได้ $m \mid (a-b)$ และ $m \mid (c-d)$

จะได้ $m \mid \{(a-b)+(c-d)\}$

ดังนั้น $m \mid \{(a+c)-(b+d)\}$

นั่นคือ $a + c \equiv b + d(\text{mod}\, m)$

<u>พิสูจน์ 1. ข.</u> จาก $a \equiv b(\text{mod}\, m)$ และ $c \equiv d(\text{mod}\, m)$

จะได้ $m \mid (b-a)$ และ $m \mid (c-d)$

จะได้ $m \mid \{(b-a)(-c)+(c-d)b\}$

ดังนั้น $m \mid (ac-bd)$

นั่นคือ $ac \equiv bd(\text{mod}\, m)$

<u>พิสูจน์ 2. ก.</u> $a \equiv b(\text{mod}\, m)$ จะได้ $m \mid (a-b)$

จะได้ $m \mid (a-b+c-c)$

ดังนั้น $m \mid \{(a+c)-(b-c)\}$

นั่นคือ $a+c \equiv b+c \pmod{m}$

<u>พิสูจน์ 2. ข.</u> $a \equiv b \pmod{m}$ จะได้ $m \mid (a-b)$

จะได้ $m \mid (a-b)c$

ดังนั้น $m \mid (ac-bc)$

นั่นคือ $ac \equiv bc \pmod{m}$

<u>พิสูจน์ 2. ค.</u> $a \equiv b \pmod{m}$ จะได้ $m \mid (a-b)$

จะได้ $mc \mid (a-b)c$

ดังนั้น $mc \mid (ac-bc)$

นั่นคือ $ac \equiv bc \pmod{mc}$ ถ้า $c > 0$

<u>พิสูจน์ 2. ง.</u> ให้ P(n) แทน $a^n \equiv b^n \pmod{m}$

1.จาก $a \equiv b \pmod{m}$ ดังนั้น P(1) เป็นจริง

2. ถ้า P(k) เป็นจริง นั่นคือ $a^k \equiv b^k \pmod{m}$

จะได้ $a \cdot a^k \equiv b \cdot b^k \pmod{m}$

$a^{k+1} \equiv b^{k+1} \pmod{m}$ จะได้ P($k+1$) เป็นจริง

นั่นคือ P(n) เป็นจริงสำหรับจำนวนเต็มบวก n #

<u>ข้อสังเกต</u> จากทฤษฎี จะเห็นว่าคอนกรูเอนซ์ มีสมบัติบางอย่างที่เหมือนกับสมการ คือ การบวก การลบ การคูณด้วยจำนวนที่เท่ากัน และการยกกำลัง

ตัวอย่าง 24 จงแสดงว่า 41 หาร $2^{20}-1$ ลงตัว

<u>วิธีทำ</u> เนื่องจาก $2^5 \equiv -9 \pmod{41}$

จะได้ $(2^5)^4 \equiv (-9)^4 \pmod{41}$

จะได้ $2^{20} \equiv 81 \cdot 81 \pmod{41}$

แต่ $81 \equiv -1 \pmod{41}$

ดังนั้น $81 \cdot 81 \equiv 1 \pmod{41}$

จะได้ $2^{20} \equiv 1 \pmod{41}$ นั่นคือ $41 \mid (2^{20}-1)$ #

ตัวอย่าง 25 จงหาเศษจากการนำ 12 ไปหาร $1!+2!+3!+4!+\ldots+99!+100!$

<u>วิธีทำ</u> $4!\equiv 0(\mathrm{mod}\,12)$ เพราะ $4!=4\cdot 3\cdot 2\cdot 1$ ซึ่ง 12 หารลงตัว

$5!\equiv 0(\mathrm{mod}\,12)$ เพราะ $5!=5\cdot 4!$ ซึ่ง 12 หารลงตัว

$6!\equiv 0(\mathrm{mod}\,12)$ เพราะ $6!=6\cdot 5\cdot 4!$ ซึ่ง 12 หารลงตัว

เมื่อ $k\geq 4$ จะได้ $k!\equiv 0(\mathrm{mod}\,12)$

$1!+2!+3!+4!+\ldots+99!+100!\equiv 1!+2!+3!+0!\ldots+0(\mathrm{mod}\,12)$

$1!+2!+3!+4!+\ldots+99!+100!\equiv 9(\mathrm{mod}\,12)$

9 จึงเป็นเศษที่ต้องการ #

ตัวอย่าง 26 จงหาเศษเหลือจากการหาร 2^{2000} ด้วย 7

<u>วิธีทำ</u> พิจารณา $2,2^2,2^3,2^4,2^5,2^6$ จะพบว่า

$2\equiv 2(\mathrm{mod}\,7)$

$2^2\equiv 4(\mathrm{mod}\,7)$

$2^3\equiv 1(\mathrm{mod}\,7)$

$2^4\equiv 2(\mathrm{mod}\,7)$

$2^5\equiv 4(\mathrm{mod}\,7)$

นั่นคือ การหาร 2^k ด้วย 7 เป็นคาบ 3

ดังนั้น เราจึงหาเศษเหลือจากการหาร 2000 ด้วย 3

เนื่องจาก $2000\equiv 2(\mathrm{mod}\,3)$ เราจึงได้ว่า $2^{2000}\equiv 4(\mathrm{mod}\,7)$ #

ทฤษฎีบท 11 ถ้า $ca\equiv cb(\mathrm{mod}\,m)$ ต่อไปนี้เป็นจริง

1. ถ้า $c>0$ และ $c\mid m$ แล้ว $a\equiv b(\mathrm{mod}\frac{m}{c})$
2. $a\equiv b(\mathrm{mod}\frac{m}{(c,m)})$
3. ถ้า $(c,m)=1$ จะได้ $a\equiv b(\mathrm{mod}\,m)$

<u>พิสูจน์ 1.</u> จาก $ca\equiv cb(\mathrm{mod}\,m)$ จะได้ $m\mid(ca-cb)$ นั่นคือ $m\mid c(a-b)$

แต่ $c\mid m$ จะได้ $\frac{m}{c}\mid(a-b)$

นั่นคือ $a\equiv b(\mathrm{mod}\frac{m}{c})$

<u>พิสูจน์ 2.</u> ให้ $d=(c,m)$ จะได้ $\frac{c}{d}$ และ $\frac{m}{d}$ เป็นจำนวนเต็มและ $(\frac{c}{d},\frac{m}{d})=1$

จาก $ca \equiv cb(\mathrm{mod}\, m)$

จะได้ $m \mid (ca-cb)$ หรือ $ca-cb=mk$ สำหรับจำนวนเต็ม k บางจำนวน

หารด้วย d จะได้ $\frac{c}{d}(a-b)=\frac{m}{d}k$

ดังนั้น $\frac{m}{d} \mid \frac{c}{d}(a-b)$

แต่ $(\frac{m}{d},\frac{c}{d})=1$ ดังนั้น $\frac{m}{d} \mid (a-b)$

นั่นคือ $a \equiv b(\mathrm{mod}\frac{m}{(c,m)})$

<u>พิสูจน์ 3.</u> จาก 2. เราทราบว่า $a \equiv b(\mathrm{mod}\frac{m}{(c,m)})$

แต่ $(c,m)=1$

ดังนั้น $a \equiv b(\mathrm{mod}\, m)$ #

ตัวอย่าง 27 จงเขียนคอนกรูเอนซ์ใหม่โดยใช้สมบัติการหารจากทฤษฎีบท เพื่อทำให้ตัวเลขมีค่าน้อยที่สุดเท่าที่จะเป็นไปได้

1. $69 \equiv 75(\mathrm{mod}\, 6)$
2. $161 \equiv 77(\mathrm{mod}\, 12)$
3. $66 \equiv 48(\mathrm{mod}\, 9)$

<u>วิธีทำ</u> 1. $69 \equiv 75(\mathrm{mod}\, 6)$

หารด้วย 3 ทั้ง สามจำนวนจะได้

$23 \equiv 25(\mathrm{mod}\, 2)$

2. $161 \equiv 77(\mathrm{mod}\, 12)$

$(7,12)=1$ จะได้

$\frac{161}{7} \equiv \frac{77}{7}(\mathrm{mod}\, 12)$ หรือ $23 \equiv 11(\mathrm{mod}\, 12)$

3. $66 \equiv 48(\mathrm{mod}\, 9)$

$(6,9)=3$ จะได้

$\frac{66}{6} \equiv \frac{48}{6}(\mathrm{mod}\frac{9}{8})$ หรือ $11 \equiv 8(\mathrm{mod}\, 3)$ #

ข้อสังเกต คอนกรูเอนซ์ที่เขียนใหม่แต่ละข้อจะเป็นผลสรุปของคอนกรูเอนซ์เดิมกล่าวคือ คอนกรูเอนซ์เดิมจริงแล้ว คอนกรูเอนซ์ใหม่จะจริงด้วย

ตัวอย่าง 28 จงยกตัวอย่างเพื่อแสดงว่าข้อความต่อไปนี้ ไม่จริง

1. ถ้า $a^2 \equiv b^2 (\mathrm{mod}\, m)$ แล้ว $a \equiv b(\mathrm{mod}\, m)$
2. ถ้า $ca \equiv cb(\mathrm{mod}\, m)$ แล้ว $a \equiv b(\mathrm{mod}\, m)$
3. ถ้า $ab \equiv 0(\mathrm{mod}\, m)$ แล้ว $a \equiv 0(\mathrm{mod}\, m)$ หรือ $b = 0(\mathrm{mod}\, m)$
4. ถ้า $a \equiv b(\mathrm{mod}\, m)$ แล้ว $a^2 \equiv b^2 (\mathrm{mod}\, m^2)$

วิธีทำ 1. $5^2 \equiv 7^2 \pmod 8$ แต่ $5 \not\equiv 7 \pmod 8$

2. $5\times 10 \equiv 5\times 7 \pmod{15}$ แต่ $10 \not\equiv 7 \pmod{15}$

3. $2\times 3 \equiv 0$ แต่ $2 \neq 0 \pmod 6$ และ $3 \not\equiv 0 \pmod 6$

4. $5 \equiv 2 \pmod 3$ แต่ $5^2 \not\equiv 2^2 \pmod{3^2}$ #

ทฤษฎีบท 12 ก. $a \equiv r(\mathrm{mod}\, m)$ และ $0 \le r < m$ ก็ต่อเมื่อ r เป็นเศษเหลือจากการหาร a ด้วย m

ข. ให้ $0 \le r, s < m$ จะได้ว่า $r \equiv s(\mathrm{mod}\, m)$ ก็ต่อเมื่อ $r = s$

ค. $a \equiv b(\mathrm{mod}\, m)$ ก็ต่อเมื่อเศษเหลือจากการหาร a ด้วย m เท่ากัน

พิสูจน์ ก. $\rightarrow$ สมมติ $a \equiv r(\mathrm{mod}\, m)$ และ $0 \le r < m$

ดังนั้น $m \mid (a - r)$

ทำให้ได้ว่า มีจำนวนเต็ม q ที่ $a - r = mq$

นั่นคือ $a = mq + r$ โดย $0 \le r < m$

โดยขั้นตอนวิธีการหาร q คือผลลัพธ์

และ r คือ เศษเหลือจากการหาร a ด้วย m ซึ่งมีเพียงชุดเดียว

$\leftarrow$ สมมติ r เป็นเศษเหลือจากการหาร a ด้วย m

ดังนั้น มีจำนวนเต็ม q ที่ $a = mq + r$ โดย $0 \le r < m$

ทำให้ $m \mid (a - r)$

นั่นคือ $a \equiv r(\mathrm{mod}\, m)$ และ $0 \le r < m$

พิสูจน์ ข. $\rightarrow$ สมมติว่า $r \equiv s(\mathrm{mod}\, m)$

ดังนั้น $m \mid (r - s)$ แต่จาก $0 \le r, s < m$

จะได้ว่า $-m < -s \le r - s \le r < m$

ทำให้ได้ว่า $r-s=0$ นั่นคือ $r=s$

<u>พิสูจน์ ค</u>. ให้ r และ s เป็นเศษเหลือจากการหาร a และ b ด้วย m ตามลำดับ

นั่นคือ $a=mq+r$ และ $b=mq'+s$ โดยที่ $0\le r,s<m$

ดังนั้น โดย ก. $a\equiv r(\mathrm{mod}\,m)$ และ $b\equiv s(\mathrm{mod}\,m)$

จะได้ว่า $a\equiv b(\mathrm{mod}\,m)$ ก็ต่อเมื่อ $r\equiv s(\mathrm{mod}\,m)$

ก็ต่อเมื่อ $r=s$ #

การหาผลเฉลยของคอนกรูเอนซ์ สามารถทำได้เช่นเดียวกับการหาผลเฉลยของสมการ

ตัวอย่าง 29 ถ้าต้องการจะหาผลเฉลยของคอนกรูเอนซ์

$$x+12\equiv 5(\mathrm{mod}8)$$

เราจะลบ 12 ออกทั้งสองข้างของคอนกรูเอนซ์ ซึ่งจะได้

$$x\equiv 5-12\equiv -7(\mathrm{mod}8)$$

หรือ $x\equiv 1(\mathrm{mod}8)$ #

ตัวอย่าง 30 ต้องการจะหาผลเฉลยของ

$$4x\equiv 3(\mathrm{mod}19)$$

คูณทั้งสองข้างด้วย 5 จะได้

$$20x\equiv 15(\mathrm{mod}19)$$

แต่ $20\equiv 1(\mathrm{mod}19)$ ดังนั้น $20x\equiv x(\mathrm{mod}19)$

ดังนั้นผลเฉลย คือ $x\equiv 15(\mathrm{mod}19)$ ซึ่งสามารถตรวจคำตอบโดยการแทน 15 ในคอนกรูเอนซ์เริ่มต้น

ซึ่งจะเห็นว่า $4(15)\equiv 60\equiv 3(\mathrm{mod}19)$ นั่นคือ $19\mid(60-3)$ #

ที่ผ่านมาเราหาผลเฉลยของคอนกรูเอนซ์โดยใช้เทคนิค แต่เราสามารถหาผลเฉลยของคอนกรูเอนซ์ได้ โดยการแทนค่า $0,1,2,\ldots,m-1$ ลงไปในตัวแปร

ตัวอย่าง 31 ถ้าเราต้องการหาผลเฉลยของคอนกรูเอนซ์

$$x^2 + 2x - 1 \equiv 0 (\mathrm{mod}\, 7)$$

เราลองแทนค่า $x = 0, x = 1, \ldots, x = 6$ ซึ่งจะได้ผลเฉลย 2 ค่า คือ $x \equiv 2 (\mathrm{mod}\, 7)$ และ $x \equiv 3 (\mathrm{mod}\, 7)$

แน่นอนว่ายังมีผลเฉลยอื่นๆอีก เช่น $x \equiv 9 (\mathrm{mod}\, 7)$ แต่ 9 และ 2 เป็นผลเฉลยที่ไม่ต่างกัน เนื่องจากมันต่างก็มอดูโล 7 ดังนั้นในการหาผลเฉลยทั้งหมดของคอนกรูเอนซ์ เราจะหมายถึง ผลเฉลยที่ไม่คอนกรูเอนซ์กัน นั่นคือ ถ้านำผลเฉลยค่าหนึ่งไปคอนกรูเอนซ์กับผลเฉลยค่าอื่นๆ จะได้ว่ามันไม่คอนกรูเอนซ์กัน #

ในการหาผลเฉลยของ $ax \equiv c (\mathrm{mod}\, m)$ จะพบว่าบางคอนกรูเอนซ์ เช่น $6x \equiv 15 (\mathrm{mod}\, 514)$ ไม่มีผลเฉลย เพราะว่า 514 ต้องหาร $6x - 15$ ได้ลงตัว แต่ $6x - 15 = 2(3x - 8) + 1, (3x - 8 \in \mathrm{I})$ นั่นคือ $6x - 15$ เป็นจำนวนคี่ไม่ว่า x จะเป็นจำนวนเต็มใดก็ตาม ทำให้ $514 \mid 6x - 15$ นั่นคือ $6x \equiv 15 (\mathrm{mod}\, 514)$ ไม่มีผลเฉลย พิจารณาคอนกรูเอนซ์ $18x \equiv 8 (\mathrm{mod}\, 14)$ เราต้องการหาค่าของ x ซึ่ง $14 \mid (18x - 8)$

นั่นคือ เราจะหาค่า x ซึ่ง $18x - 8 = 14y$ สำหรับบาง y

นั่นคือเราต้องการหาผลเฉลยของสมการเชิงเส้น $18x - 14y = 8$ นั่นเอง

แต่จากความรู้เรื่องการแก้สมการเชิงเส้นจะได้

$$18u - 14v = (18, 14) = 2 \qquad \text{----------(1)}$$

ซึ่งจะได้ผลเฉลยคือ $u = 4$ และ $v = 5$ แต่เราต้องการหาผลเฉลยของสมการ $18x - 14y = 8$

ดังนั้นทำให้ขวามือของสมการ (1) เป็น 8 โดยคูณด้วย 4 จะได้

$$18 \cdot (4 \cdot 4) - 14 \cdot (5 \cdot 4) = 8$$

ดังนั้น $18 \cdot 16 \equiv 8 (\mathrm{mod}\, 14)$ ดังนั้นจะได้ $x \equiv 16 \equiv 2 (\mathrm{mod}\, 14)$ เป็นผลเฉลยแต่เราจะทราบในภายหลังว่า คอนกรูเอนซ์นี้มี 2 ผลเฉลยที่ต่างกัน มอดุโล 14 อีกผลเฉลยหนึ่งคือ $x \equiv 9 (\mathrm{mod}\, 14)$

การหาผลเฉลยคอนกรูเอนซ์ในรูปแบบ

$$ax \equiv c (\mathrm{mod}\, m)$$

เราต้องหาจำนวนเต็ม x ซึ่ง m หาร $ax - c$ ลงตัว นั่นคือ จะมีจำนวนเต็ม y ซึ่ง $ax - c = my$ ซึ่งเราพบว่า $ax \equiv c (\mathrm{mod}\, m)$ จะมีผลเฉลยก็ต่อเมื่อ สมการเชิงเส้น $ax - my = c$ มีผลเฉลย

ให้ $g=(a,m)$ จะพบว่าทุกๆจำนวนที่เป็นค่าคงที่ทางขวามือของ $ax-my$ จะต้องเป็นจำนวนเท่าของ g แต่ถ้า g หาร c ไม่ลงตัว จะได้ว่า $ax-my=c$ ไม่มีผลเฉลย ซึ่งทำให้ $ax\equiv c(\mathrm{mod}\,m)$ ไม่มีผลเฉลยด้วย

สมมติให้ g หาร c ลงตัว จาก Linear Equation Theorem จะได้ว่าสมการ

$$au+mv=g \qquad \text{----------(2)}$$

มีผลเฉลยเสมอ

สมมติให้ $u=u_0, v=v_0$ จากอัลกอริทึมของยูคลิด เนื่องจาก เราได้ g หาร c ลงตัวเรา สามารถคูณตลอดสมการ (2) ด้วย $\frac{c}{g}$ จะได้

$$a\frac{cu_0}{g}+m\frac{cv_0}{g}=c$$

นั่นคือ จะได้ $x_0\equiv\frac{cu_0}{g}(\mathrm{mod}\,m)$ เป็นผลเฉลยของคอนกรูเอนซ์ $ax\equiv c(\mathrm{mod}\,m)$

คำถาม มีผลเฉลยอื่นอีกไหม

สมมติให้ x_1 เป็นผลเฉลยอื่นของ $ax\equiv c(\mathrm{mod}\,m)$

ดังนั้น $ax_1\equiv ax_0(\mathrm{mod}\,m)$

จะได้ m หาร ax_1-ax_0 ลงตัว

นั่นคือ $\frac{m}{g}$ หาร $\frac{a(x_1-x_0)}{g}$ ลงตัว

และเรารู้ว่า $\frac{m}{g}$ และ $\frac{a}{g}$ ไม่มีตัวร่วม

ดังนั้น $\frac{m}{g}$ หาร x_1-x_0 ลงตัว หรือกล่าวว่ามีจำนวน k ซึ่ง

$$x_1=x_0+k\frac{m}{g}$$

ซึ่งจะสามารถหาผลเฉลยที่ต่างกันโดยแทน $k=0,1,2,\ldots,g-1$

สิ่งที่กล่าวมาข้างต้นสามารถสรุปเป็นทฤษฎีบทได้ดังนี้

2.3.5 Linear Congruence Theorem

ให้ a,c และ m เป็นจำนวนเต็มซึ่ง $m\geq 1$ และให้ $g=(a,m)$

1. ถ้า $g\nmid c$,คอนกรูเอนซ์ $ax\equiv c(\mathrm{mod}\,m)$ ไม่มีผลเฉลย
2. ถ้า $g\mid c$,คอนกรูเอนซ์ $ax\equiv c(\mathrm{mod}\,m)$ จะมีผลเฉลย g ที่ไม่คอนกรูเอนซ์กัน

ในการหาผลเฉลยจะเริ่มจากการหาผลเฉลยเริ่มต้น (u_0,v_0) ของสมการเชิงเส้น $au+mv=g$

ซึ่งจะได้ $x_0 = \frac{cu_0}{g}$ เป็นผลเฉลยของ $ax \equiv c(\mathrm{mod}\, m)$ และผลเฉลยอื่นๆที่เหลือ คือ

$x \equiv x_0 + k\frac{m}{g}(\mathrm{mod}\, m)$,สำหรับ $k = 0,1,2,..., g-1$

ตัวอย่าง 32 จงหาผลเฉลยของคอนกรูเอนซ์ $943x \equiv 381(\mathrm{mod}\, 2576)$

<u>วิธีทำ</u> เนื่องจาก $(943,2576) = 23$

ซึ่ง $23 \nmid 381$

ดังนั้น คอนกรูเอนซ์นี้ไม่มีผลเฉลย #

ทฤษฎีบท 13 สมการไดโอแฟนไทน์ $ax + by + cz = n$ มีผลเฉลยก็ต่อเมื่อ $d \mid n$

โดยที่ $d = (a,b,c)$

<u>พิสูจน์</u> จัดสมการ $ax + by + cz = n$ ใหม่จะได้

$$ax + by = n - cz$$

ซึ่งสมการนี้จะมีจำนวนเต็ม x, y ที่สอดคล้องสมการ ก็ต่อเมื่อ

$d_1 \mid (n - cz)$ โดยที่ $d_1 \mid (a,b)$

เขียนรูปคอนกรูเอนต์จะได้

$$cz \equiv n(\mathrm{mod}\, d_1)$$

ซึ่งคอนกรูเอนต์ดังกล่าวจะมีผลเฉลยเป็นจำนวนเต็มก็ต่อเมื่อ $d \mid n$ โดยที่

$$d = (d_1, c)$$

เนื่องจาก $d = (d_1, c) = ((a,b),c) = (a,b,c)$

ดังนั้น $ax + by + cz = n$ มีผลเฉลยก็ต่อเมื่อ $d \mid n$ โดยที่ $d = (a,b,c)$ #

ตัวอย่าง 33 จงหาผลเฉลยของสมการไดโอแฟนไทน์ $3x - 6y + 9z = 63$

<u>วิธีทำ</u> สมการ $3x - 6y + 9z = 63$,ผลเฉลยเพราะ $(3,-6,9) = 3$ ซึ่ง $3 \mid 63$

จัดสมการจะได้ $3x - 6y = 63 - 9z$ .....(1)

จะเห็นว่า $(3,-6) = 3$ และ $3 \mid (63 - 9z)$ เสมอไม่ว่า z จะเป็นจำนวนเต็มใด

จึงให้ $z = t_1$ เมื่อ $t_1 \in \mathrm{I}$

แทนค่า z ใน (1) จะได้ $3x - 6y = 63 - 9t_1$

หรือ $x - 2y = 21 - 3t_1$

จะเห็นว่า $(1,-2)=1$ ซึ่ง $1\mid(21-3t_1)$

ถ้าให้ $y=t_2$ เมื่อ $t_2\in \mathrm{I}$ จะได้ว่า $x=2t_1+21-3t_1$

ดังนั้นผลเฉลยของสมการคือ

$$\left.\begin{aligned} x &= 2t_1+21-3t_1 \\ y &= t_2 \\ z &= t_1 \end{aligned}\right\} \quad \text{เมื่อ } t_1,t_2\in \mathrm{I}$$

#

ในหัวข้อนี้เราจะหาพิจารณา หาผลเฉลยของ

$$ax\equiv b(\mathrm{mod}\, m) \qquad \text{----------(1)}$$

เมื่อกำหนด a,b มาให้

ถ้า x_1 เป็นผลเฉลยของ (1) และ $x_2\equiv x_1(\mathrm{mod}\, m)$ จะได้ว่า

$ax_2\equiv bx_1\equiv b(\mathrm{mod}\, m)$

นั่นคือ x_2 เป็นผลเฉลยด้วย

ดังนั้น ถ้าเราหาผลเฉลยที่ไม่คอนกรูเอนซ์กันมอดุโล m ทั้งหมดได้

เราก็จะได้ผลเฉลยที่เป็นจำนวนเต็มทั้งหมด

ในที่นี้เราจะหาผลเฉลยที่ไม่คอนกรูเอนซ์กันมอดุโล m ทั้งหมดของ (1)

ให้ $x=x_1$ เป็นผลเฉลยของ (1)

นั่นคือ $ax_1\equiv b(\mathrm{mod}\, m)$

ทำให้ $m\mid(b-ax_1)$ ดังนั้น จะมีจำนวนเต็ม y_1 ที่ $b-ax_1=my_1$

ทำให้ $x=x_1, y=y_1$ เป็นผลเฉลยของสมการไดโอแฟนไทน์

$$ax+my=b \qquad \text{----------(2)}$$

สรุปได้ว่า $x=x_1$ เป็นผลเฉลยของ (1) แล้วจะมี y_1 ที่ $x=x_1, y=y_1$

เป็นผลเฉลยของสมการ (2)

ในทางกลับกัน ให้ $x=x_1$ และ $y=y_1$ เป็นผลเฉลยของสมการ (2)

นั่นคือ $ax_1+my_1=b$ หรือ $b-ax_1=my_1$

ทำให้ $m\mid(b-ax_1)$ และ $ax_1\equiv b(\mathrm{mod}\, m)$

ดังนั้น $x=x_1$ เป็นผลเฉลยของ (1)

เราจึงพิสูจน์ได้ว่า $x = x_1$ เป็นผลเฉลยของ (1) ก็ต่อเมื่อมี y_1 ที่ทำให้ $x = x_1, y = y_1$ เป็นผลเฉลยของสมการ (2)

ถ้าให้ $d = (a,m)$ เราจะมี

สมการ (2) มีผลเฉลยก็ต่อเมื่อ $d \mid b$ และถ้า $x = x_1, y = y_1$ เป็นผลเฉลยแล้ว

ผลเฉลยทั้งหมดคือ $x = x_1 + k\frac{m}{d}, y = y_1 - k\frac{a}{d}$ เมื่อ $k \in \mathrm{Z}$

เราจะหาค่า k ทั้งหมด ที่ทำให้ได้ x ที่มีคอนกรูเอนซ์มอดุโล m ทั้งหมด ให้ k_1, k_2 เป็นจำนวนเต็มที่ $x_1 + k_1\frac{m}{d} \equiv x_1 + k_2\frac{m}{d} (\mathrm{mod}\, m)$ ทำให้ $m \mid (k_2 - k_1)(\frac{m}{d})$ นั่นคือ จะมีจำนวนเต็ม c ที่ทำให้ $(k_2 - k_1)(\frac{m}{d}) = mc$ ซึ่งทำให้ $k_2 - k_1 = cd$

ดังนั้น $k_2 \equiv k_1 (\mathrm{mod}\, d)$

เราจึงได้ว่า $x = x_1 + k(\frac{m}{d})$ โดยที่ $k = 1,2,3,...,d-1$

เป็นผลเฉลยที่ไม่คอนกรูเอนซ์กันมอดุโล m ทั้งหมดของ (2)

ทฤษฎีบท 14 ให้ m, a, b เป็นจำนวนเต็มที่ m เป็นบวก และ $d = (a,m)$ จะได้ว่า

$ax \equiv b (\mathrm{mod}\, m)$ มีผลเฉลย ก็ต่อเมื่อ $d \mid b$

และถ้า $x = x_1$ เป็นผลเฉลย แล้วผลเฉลยที่ไม่คอนกรูเอนซ์กันมอดุโล m ทั้งหมด d ค่าคือ

$x = x_1 + k(\frac{m}{d})$ เมื่อ $k = 0,1,2,3,...,d-1$

ตัวอย่าง 34 จงพิจารณาว่า คอนกรูเอนซ์ต่อไปนี้มีผลเฉลยหรือไม่ ถ้ามีจงหาผลเฉลยที่ไม่คอนกรูเอนซ์กันทั้งหมด

ก. $114x \equiv 78 (\mathrm{mod}\, 174)$

ข. $114x \equiv 92 (\mathrm{mod}\, 174)$

<u>วิธีทำ</u> ก. หา (114,174) โดยใช้ขั้นตอนวิธียูคลิด

จาก $174 = 114 \cdot 1 + 60$

$114 = 60 \cdot 1 + 54$

$60 = 54 \cdot 1 + 6$

$54 = 6 \cdot 9$

จึงได้ว่า $(114,174)=6$ และ $6 \mid 78$ ดังนั้น ก. มีผลเฉลยที่ไม่คอนกรูเอนซ์กันมอดุโล m 174 อยู่ 6 ค่า

และ $6=60-54\cdot 1=60-(114-60\cdot 1)=60\cdot 2-114\cdot 1$

$=(174-114\cdot 1)\cdot 2-114\cdot 1=174\cdot 2-114\cdot 3$

ทำให้ $78=6\cdot 3=174\cdot 26-114\cdot 39$

ดังนั้น $x=-39+k(\frac{174}{6})$ เมื่อ $k=0,1,2,3,4,5$

ซึ่งคือ $x=-39,-10,19,48,77,106$ เป็นผลเฉลยที่ไม่คอนกรูเอนซ์กันมอดุโล 174 ทั้งหมด

ข. จาก ก. $(114,174)=6$ และ $6 \nmid 92$ ดังนั้น ข. ไม่มีผลเฉลย #

ตัวอย่าง 35 จงหาผลเฉลยที่ไม่คอนกรูเอนซ์กันทั้งหมดของ $5x \equiv 100 (\mathrm{mod}\, 65)$

<u>วิธีทำ</u> เราจะเห็นว่า $x=20$ เป็นผลเฉลยหนึ่ง

และจำนวนผลเฉลยที่ไม่คอนกรูเอนซ์กันคือ $(5,65)=5$ ดังนั้นผลเฉลยคือ

$x=20, 20+1(\frac{65}{5})=33, 20+2(\frac{65}{5})=46, 20+3(\frac{65}{5})=59, 20+4(\frac{65}{5})=72$ #

ทฤษฎีบทเศษเหลือของจีน

ในสมัยโบราณชาวจีนมักนิยมถามปัญหา

จงหาจำนวนเต็ม ที่หารด้วย 11 เหลือเศษ 5 และหารด้วย 13 เหลือเศษ 9

นั่นคือ ต้องการหาจำนวนเต็ม x ที่สอดคล้องกับระบบ

$$x \equiv 5 (\mathrm{mod}\, 11)$$
$$x \equiv 9 (\mathrm{mod}\, 13)$$

นั่นเอง

เขียนในรูปทั่วไปได้ คือ ต้องการหาผลเฉลยของระบบ

$$x \equiv a_1 (\mathrm{mod}\, m_1)$$
$$x \equiv a_2 (\mathrm{mod}\, m_2)$$

เริ่มแรกเราพิจารณาในกรณีที่ $(m_1, m_2)=1$

ให้ $x=m_1 y+m_2 z$ เมื่อ y, z เป็นจำนวนเต็มใดๆ แทนในสมการข้างต้น จะได้

$$m_2 z \equiv a_1 (\mathrm{mod}\, m_1)$$
$$m_1 y \equiv a_2 (\mathrm{mod}\, m_2)$$

ดังนั้น เราต้องการหา z ที่ $m_2 z \equiv a_1 (\mathrm{mod}\, m_1)$ และ y ที่ $m_1 y \equiv a_2 (\mathrm{mod}\, m_2)$

ซึ่งสามารถหาได้ทั้งคู่ดังนี้

เนื่องจาก $(m_1, m_2) = 1$

ดังนั้น m_1 มีอินเวอร์สมอดุโล m_2 ให้เป็น y_1

และ m_2 มีอินเวอร์สมอดุโล m_1 ให้เป็น y_2

นั่นคือ $m_2 y_2 \equiv 1 (\mathrm{mod}\, m_1)$ และ $m_1 y \equiv 1 (\mathrm{mod}\, m_2)$

ให้ $y = a_2 y_1$ และ $z = a_1 y_2$

จึงได้ว่า $m_2 z = m_2 a_1 y_2 \equiv 1 \cdot a_1 = a_1 (\mathrm{mod}\, m_1)$ และ $m_1 y = m_1 a_2 y_1 \equiv 1 \cdot a_2 = a_2 (\mathrm{mod}\, m_2)$

ทำให้ $x = m_1 y + m_2 z$ สอดคล้องกับระบบ

ต่อไปสมมติว่า x' เป็นอีกผลเฉลยหนึ่งของระบบ

นั่นคือ

$$x' = a_1 (\mathrm{mod}\, m_1)$$
$$x' = a_2 (\mathrm{mod}\, m_2)$$

ทำให้ $x' \equiv x (\mathrm{mod}\, m_1)$ และ $x' \equiv x (\mathrm{mod}\, m_2)$

นั่นคือ $m_1 \mid x' - x$ และ $m_2 \mid x' - x$

แต่เนื่องจาก $(m_1, m_2) = 1$ ทำให้ $m_1 m_2 \mid x' - x$

เราจึงได้ทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 15 (ทฤษฎีบทเศษเหลือของจีน)

ให้ m_1, m_2 เป็นจำนวนเต็มบวกที่ $(m_1, m_2) = 1, a_1, a_2$ เป็นจำนวนเต็มใดๆ ให้ y_1, y_2 เป็นจำนวนเต็มซึ่ง $m_1 y_1 \equiv 1 (\mathrm{mod}\, m_2)$ และ $m_2 y_2 \equiv 1 (\mathrm{mod}\, m_1)$ จะได้ว่าระบบ

$$x = a_1 (\mathrm{mod}\, m_1)$$
$$x = a_2 (\mathrm{mod}\, m_2)$$

มีผลเฉลยคือ $x = a_2 m_1 y_1 + a_1 m_2 y_2$ และถ้า x' เป็นผลเฉลยของระบบนี้แล้ว $x' \equiv x (\mathrm{mod}\, m_1 m_2)$ นั่นคือ ระบบนี้มีผลเฉลยเดียวมอดุโล $m_1 m_2$

ต่อไปเราจะหาผลเฉลยของระบบที่กล่าวในตอนต้นของหัวข้อนี้

ตัวอย่าง 36 จงหาผลเฉลยที่เป็นค่าบวกน้อยสุดของระบบ

$$x \equiv 5(\text{mod}11)$$
$$x \equiv 9(\text{mod}13)$$

<u>วิธีทำ</u> $m_1 = 11, m_2 = 13, a_1 = 5, a_2 = 9$ จะได้ $m_1 m_2 = 11 \cdot 13 = 143$

จะหา y_1, y_2 ที่ $11y_1 = 1(\text{mod}13)$ และ $13y_2 = 1(\text{mod}11)$

จาก $13 = 11 \cdot 1 + 2$

$11 = 2 \cdot 5 + 1$

จะได้ $1 = 11 - 2 \cdot 5 = 11 - (13 - 11 \cdot 1)5 = 11 \cdot 6 + 13(-5)$

ให้ $y_1 = 6$ และ $y_2 = -5$

โดยทฤษฎีบทข้างต้น $x = 9 \cdot 5 \cdot 6 + 5 \cdot 13 \cdot (-5) = 594 - 325 = 269$ เป็นผลเฉลยหนึ่ง

และ $269 \equiv 126(\text{mod}143)$

ดังนั้น 126 เป็นผลเฉลยที่เป็นค่าบวกน้อยที่สุด

(ตรวจคำตอบ $126 \equiv 5(\text{mod}11)$ และ $126 \equiv 9(\text{mod}13)$ #

ทฤษฎีบท 16 พิจารณาระบบสมการ

$$x = a_1(\text{mod}\, m_1)$$
$$x = a_2(\text{mod}\, m_2)$$

1. ถ้า $(m_1, m_2) \nmid a_1 - a_2$ จะไม่มีผลเฉลย
2. ถ้า $(m_1, m_2) | a_1 - a_2$ จะมีผลเฉลยหนึ่งเดียว $\text{mod}[m_1, m_2]$

<u>ข้อสังเกต</u> ถ้า $(m_1, m_2) = 1$ จะเป็นไปตามกรณีที่ 2 และ $[m_1, m_2] = m_1 m_2$ #

ตัวอย่าง 37 จงแก้ระบบสมการ

$$x = 5(\text{mod}12)$$
$$x = 11(\text{mod}18)$$

เนื่องจาก $(12,18) = 6 | 11 - 5$ มีผลเฉลยหนึ่งเดียว $\text{mod}[12,18] = 36$

$$x = 5(\text{mod}12), x = 5 + 12s$$

เนื่องจาก $x = 11(\text{mod}18)$

$$5 + 12s 11(\text{mod}18), 12s = 6(\text{mod}18)$$

จะได้ว่า 6 หารทั้ง 12 และ 6 ลงตัว และ $(6,18) = 6$

ดังนั้น $2s = 1(\text{mod}3)$

จัดให้อยู่ในรูปสมการ $s = 2(\text{mod}3), s = 2 + 3t$

สุดท้ายจะได้

$$x = 5+12s = 5+12(2+3t) = 29+36t$$
$$x = 29(\text{mod}\,36)$$

#

บทที่ 3
แนวคิดและหลักการทำงานของโปรแกรม

แนวคิดและหลักการทำงานของโปรแกรม

ในการเขียนโปรแกรมเพื่อหาผลเฉลยของสมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปรและ 3 ตัวแปร มิได้เริ่มจากการเขียนโปรแกรมสมการไดโอแฟนไทน์ทันที แต่เริ่มจากการเขียนโปรแกรมการหาร , โปรแกรมยูคลิด, และนำความรู้พื้นฐานเหล่านั้นไปเขียน โปรแกรมสมการไดโอแฟนไทน์ 2 ตัวแปร ซึ่งในการเขียนโดยวิธีตรงในครั้งแรก โปรแกรมที่ได้ยังมีข้อจำกัดอยู่ จึงได้คิดหาวิธีในการแก้ปัญหาใหม่ แล้วเขียนโปรแกรมสมการไดโอแฟนไทน์ 2 ตัวแปรใหม่ ซึ่งมีประสิทธิภาพดีกว่าเดิม สามารถแก้ปัญหาได้ครอบคลุมทุกกรณี และได้นำหลักการเดียวกับการแก้สมการไดโอแฟนไทน์ 2 ตัวแปร มาประยุกต์ใช้ในการแก้ปัญหาสมการไดโอแฟนไทน์ 3 ตัวแปร ดังนั้นในการนำเสนอแนวคิดในการเขียนโปรแกรมจะขอเสนอตามลำดับดังนี้

1. ขั้นตอนวิธีการหาร + โปรแกรมขั้นตอนวิธีการหาร + ตัวอย่างแสดงผลการใช้งานโปรแกรมวิธีหาร
2. ขั้นตอนวิธียูคลิด + โปรแกรมขั้นตอนวิธียูคลิด + ตัวอย่างแสดงผลการใช้งานโปรแกรมยูคลิด
3. วิธีแก้สมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร
   - 3.1 แนะนำฟังก์ชันที่ใช้ในโปรแกรม
     - 3.1.1 ฟังก์ชัน GCD
     - 3.1.2 ฟังก์ชัน Linear
   - 3.2 ขั้นตอนวิธีการแก้สมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร
   - 3.3 ตัวอย่างโจทย์ที่แก้ตามขั้นตอนวิธีการแก้สมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร
   - 3.4 โปรแกรมการแก้สมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร
   - 3.5 ตัวอย่างแสดงผลการใช้งานโปรแกรมไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร
4. วิธีแก้สมการไดโอแฟนไทน์เชิงเส้น 3 ตัวแปร
   - 4.1 ขั้นตอนวิธีการแก้สมการไดโอแฟนไทน์เชิงเส้น 3 ตัวแปร
   - 4.2 ตัวอย่างโจทย์ที่แก้ตามขั้นตอนวิธีการแก้สมการไดโอแฟนไทน์เชิงเส้น 3 ตัวแปร
   - 4.3 โปรแกรมการแก้สมการ ไดโอแฟนไทน์เชิงเส้น 3 ตัวแปร
   - 4.4 ตัวอย่างแสดงผลการใช้งานโปรแกรมสมการไดโอแฟนไทน์เชิงเส้น 3 ตัวแปร

3.1. วิธีการหาร

ขั้นตอนวิธีการหาร

1. รับค่าตัวตั้ง โดยให้เก็บในตัวแปร a

ตรวจสอบว่าค่าตัวตั้งมีค่าเป็นจำนวนเต็มบวก หรือมากกว่า 0 หรือไม่ หากไม่มากกว่า 0 จะแสดงข้อความ " !!Number have value is less!!" แล้วให้รับค่า a ใหม่ รับจนกว่าจะเป็นจำนวนเต็มบวกตามที่ต้องการ

2. รับค่าตัวหาร โดยให้เก็บในตัวแปร b

ตรวจสอบว่าค่าตัวตั้งมีค่าเป็นจำนวนเต็มบวก หรือมากกว่า 0 หรือไม่ หากไม่มากกว่า 0 จะแสดงข้อความ " !!Number have value is less!!" แล้วให้รับค่า a ใหม่ รับจนกว่าจะเป็นจำนวนเต็มบวกตามที่ต้องการ

3. คำนวณผลการหารและแสดงผลออกมา ก็จะได้คำตอบของการหารตามที่ต้องการ

โปรแกรมขั้นตอนวิธีการหาร

```
#include "stdio.h"
#include "conio.h"

int A[100],B[100],C[100],R[100],a;

void main()
{
clrscr();
        printf("Enter the number\n");
        scanf("%d",&A[0]);

        while (A[0]<=0)
                {
                printf("!!Number have value is less!!\n");
                printf("Enter new value\n");
                scanf("%d",&A[0]);
                }

        printf("Enter the division\n");
        scanf("%d",&B[0]);
        while (B[0]<=0)
                {
                printf("!!Number have value is less!!\n");
                printf("Enter new value\n");
                scanf("%d",&B[0]);
                }
```

```
        C[0] = (A[0]/B[0]);
        R[0] = A[0]-(B[0]*C[0]);
        printf("\nResult = %d\n",C[0]);
        printf("R = %d\n",R[0]);
        printf("\n%d=%d*%d+%d",A[0],B[0],C[0],R[0]);


getch();
}
```

ตัวอย่างแสดงผลการใช้งานโปรแกรมการหาร

เมื่อเริ่มต้นโปรแกรมทางโปรแกรมจะให้ป้อนค่าตัวตั้ง ซึ่งจะได้หน้าจอแสดงผลดังข้างล่างนี้

รูปที่ 3.2 แสดงหน้าจอรับค่าตัวตั้ง

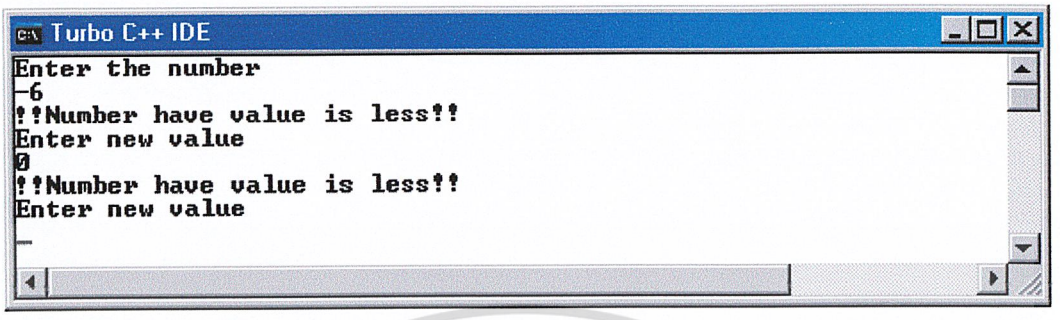
เมื่อป้อนค่าตัวตั้งแล้วต่อจากนั้นให้ป้อนค่าตัวหาร ซึ่งแสดงหน้าจอได้ดังนี้

รูปที่ 3.3 แสดงหน้าจอรับค่าตัวหาร

เมื่อป้อนค่าตัวหารแล้วจะได้ผลของการหารออกมาตามที่ต้องการ

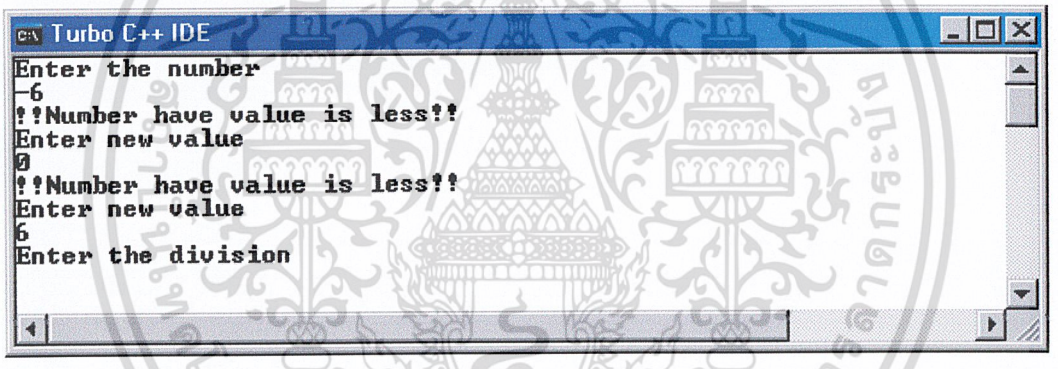
รูปที่ 3.4 แสดงหน้าจอการคำนวณผลการหาร

ถ้าป้อนค่าที่เป็น 0 หรือค่าที่เป็นลบไปหน้าจอจะแสดงผลดังนี้

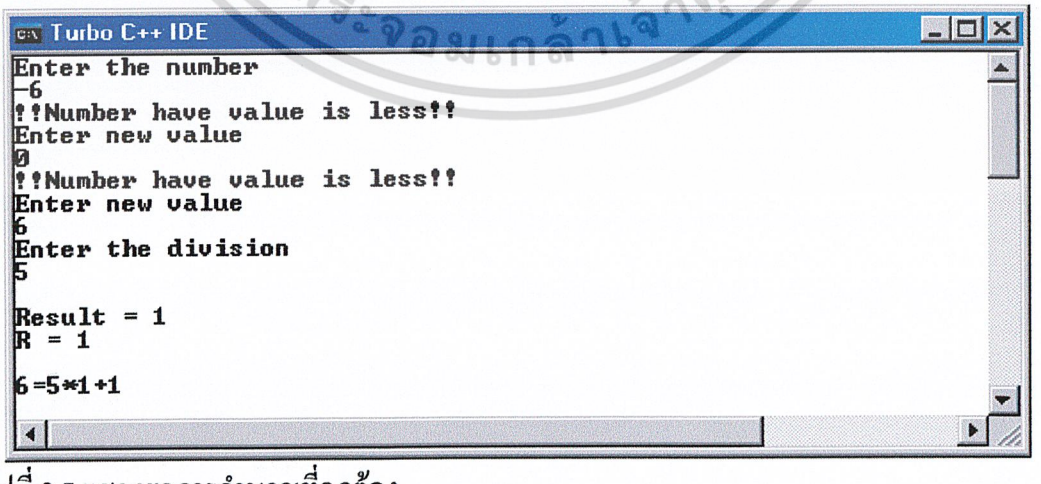


รูปที่ 3.5 แสดงหน้าจอเมื่อป้อนค่าข้อมูลไม่ตรงกับความต้องการ

และต้องป้อนค่าใหม่ให้ถูกต้อง คือต้องเป็นจำนวนเต็มบวกเท่านั้น



รูปที่ 3.6 แสดงหน้าจอป้อนค่าข้อมูลที่ถูกต้อง



รูปที่ 3.7 แสดงผลการคำนวณที่ถูกต้อง

3.2. การหา ห.ร.ม. โดยวิธีของยูคลิด

ขั้นตอนการหา ห.ร.ม. โดยวิธีของยูคลิด

1. รับค่าตัวตั้ง โดยให้เก็บในตัวแปร a

ตรวจสอบว่าค่าตัวตั้งมีค่าเป็นจำนวนเต็มบวก หรือมากกว่า 0 หรือไม่ หากไม่มากกว่า 0 จะแสดงข้อความ " !!Number have value is less!!" แล้วให้รับค่า a ใหม่ รับจนกว่าจะเป็นจำนวนเต็มบวกตามที่ต้องการ

2. รับค่าตัวหาร โดยให้เก็บในตัวแปร b

ตรวจสอบว่าค่าตัวตั้งมีค่าเป็นจำนวนเต็มบวก หรือมากกว่า 0 หรือไม่ หากไม่มากกว่า 0 จะแสดงข้อความ " !!Number have value is less!!" แล้วให้รับค่า a ใหม่ รับจนกว่าจะเป็นจำนวนเต็มบวกตามที่ต้องการ

3. เมื่อได้ค่า a และ b ตามที่ต้องการแล้ว

ตรวจสอบว่า ค่า a และ b ค่าใดมีค่ามากกว่ากัน ถ้าค่าใดมากให้ค่านั้นเป็นตัวตั้ง โดยให้เป็นค่า a แต่ถ้าค่าใดน้อยให้ค่านั้นเป็นตัวหาร คือให้เป็น b คือถ้าค่าที่ได้รับมา ค่า b มีค่าน้อยกว่า a ก็จะสลับค่ากันระหว่าง a และ b

4. ทำการหาร a และ b เมื่อ a เมื่อ a เป็นตัวตั้ง และ b เป็นตัวหาร ทำการหารและแสดงค่าออกมา จะได้ค่าของผลหารอยู่ในตัวแปร c และ เศษ อยู่ในตัวแปร r ทำการหารไปเรื่อยๆ โดยจะอยู่ในรูปของ

$$a = q_1 b + r_1, 0 < r_1 < |b|$$
$$b = q_2 r_1 + r_2, 0 < r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3, 0 < r_3 < r_2$$
$$r_2 = q_4 r_3 + r_4, 0 < r_4 < r_3$$
$$\vdots \qquad \vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n, 0 < r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n + 0$$

ทำจนกระทั่ง r เป็น 0 จะได้คำตอบของ การหา ห.ร.ม. โดยวิธีของยูคลิดตามต้องการ คือ ค่า c ที่เป็นผลตัวสุดท้ายที่ทำให้ r ทีได้เป็น 0 ค่านั้นคือ ห.ร.ม.ของ a และ b โดยเขียนได้ในรูปของ (a,b) = c

โปรแกรมการหา ห.ร.ม. โดยวิธีของยูคลิด

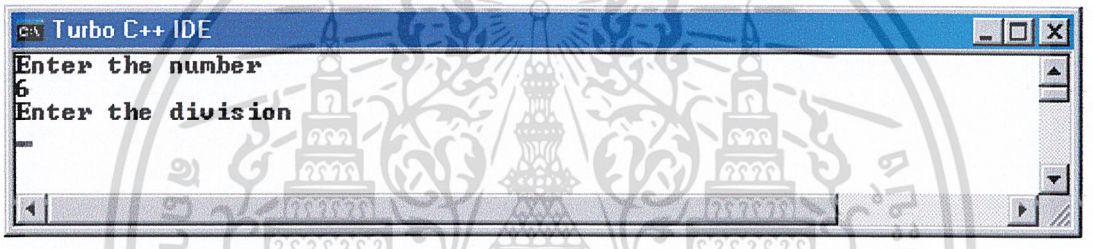
```
#include "stdio.h"
#include "conio.h"
int A[1000],B[1000],C[1000],R[1000],a;
int i,n;
void main()
{
clrscr();
        printf("Enter the number\n");
        scanf("%d",&A[0]);

        while (A[0]<=0)
                {
                printf("!!Number have value is less!!\n");
                printf("Enter new value\n");
                scanf("%d",&A[0]);
                }

        printf("\nEnter the division\n");
        scanf("%d",&B[0]);
        while (B[0]<=0)
                {
                printf("!!Number have value is less!!\n");
                printf("Enter new value\n");
                scanf("%d",&B[0]);
                }

        if (A[0]<B[0])
```

```
{
a=A[0];
A[0]=B[0];
B[0]=a;
}

C[0] = (A[0]/B[0]);
R[0] = A[0]-(B[0]*C[0]);
printf("\nResult = %d\n",C[0]);
printf("R = %d\n",R[0]);
printf("%d=(%d*%d)+%d\n",A[0],B[0],C[0],R[0]);

i=0;
while (R[i]!=0)
{
A[i+1]=B[i];
B[i+1]=R[i];
C[i+1]=A[i+1]/B[i+1];
R[i+1]=A[i+1]-(B[i+1]*C[i+1]);
printf("\nResult = %d\n",C[i+1]);
printf("R = %d\n",R[i+1]);
printf("%d=(%d*%d)+%d\n",A[i+1],B[i+1],C[i+1],R[i+1]);

i=i+1;
n=i;
}
printf("\n(%d,%d)=%d",A[0],B[0],B[n]);
getch();
}
```

ตัวอย่างแสดงผลการใช้งานโปรแกรมการหา ห.ร.ม. โดยวิธี ยูคลิด

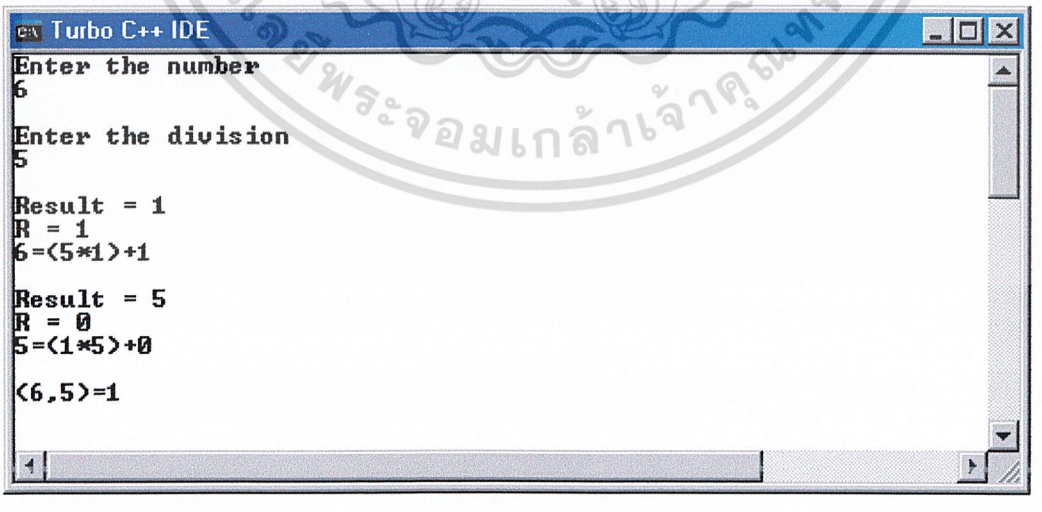
ขั้นตอนแรกป้อนค่าตัวตั้ง

รูปที่ 3.9 แสดงหน้าจอป้อนค่าตัวตั้ง



รูปที่ 3.10 แสดงหน้าจอป้อนค่าตัวหาร

หลังจากนั้นจะได้ผลลัพธ์ออกมาตามที่ต้องการ

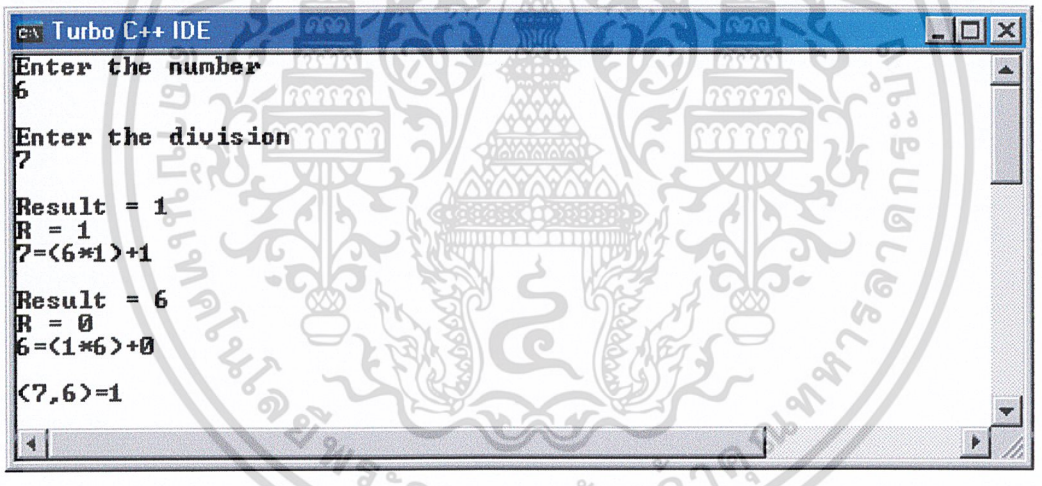


รูปที่ 3.11 แสดงหน้าจอการคำนวณหา ห.ร.ม. และผลเฉลย

แต่การหาร ห.ร.ม. โดยใช้วิธีการของยูคลิดนั้น ค่าใดจะเป็นตัวตั้ง หรือค่าใดจะเป็นตัวหารก็ได้

รูปที่ 3.12 แสดงหน้าจอการรับค่าตัวตั้งที่มากกว่าตัวหาร

ซึ่งจากโปรแกรมเราได้ทำการให้ค่าที่มากกว่าเป็นตัวตั้งและให้ค่าที่น้อยกว่าเป็นตัวหารก็จะได้ผลออกมาดังข้างล่างนี้



รูปที่ 3.13 แสดงการหาผลเฉลยของ ห.ร.ม. โดยให้ค่ามากเป็นตัวตั้ง

3.3. สมการไดโอแฟนไทน์ 2 ตัวแปร

แนะนำฟังก์ชันที่ใช้ในโปรแกรม

1. อธิบาย ฟังก์ชัน GCD

ฟังก์ชัน GCD ใช้ในการหา ห.ร.ม. ของค่าจำนวนเต็มบวก 2 ตัว โดยใช้แนวคิดมาจากอัลกอริทึมของยูคลิด

จากอัลกอริทึมยูคลิด

$$a = q_1 b + r_1, 0 < r_1 < |b|$$
$$b = q_2 r_1 + r_2, 0 < r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3, 0 < r_3 < r_2$$
$$r_2 = q_4 r_3 + r_4, 0 < r_4 < r_3$$
$$\vdots \qquad \vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n, 0 < r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n + 0$$

จะเห็นว่า ห.ร.ม. ของ a และ b คือ r_n เมื่อ r_n เป็นเศษตัวสุดท้ายที่ไม่เป็น 0 ในฟังก์ชัน GCD จึงให้ $r_1 = a\%b$ คือ r_1 เป็นเศษของ a/b แล้วเซต $a = b$ และ $b = r_1$ ตามอัลกอริทึมของยูคลิดด้านบนทำไปเรื่อยๆ จนกว่าจะได้เศษเป็น 0 คือ $r_1 = 0$ ซึ่ง r_1 ก็คือเศษตัวสุดท้าย จะเห็นว่าเศษตัวก่อนหน้าคือ r_n ซึ่งก็คือค่า a นั่นเอง

2. อธิบายฟังก์ชัน Linear

ฟังก์ชัน Linear เป็นฟังก์ชันที่คิดขึ้นมาเพื่อใช้ในการหาผลเฉลยที่เล็กที่สุดที่มีค่าเป็นบวกของสมการเชิงเส้น 2 ตัวแปร นั่นคือ $ax+by=g$ ซึ่ง $g=(a,b)$ นั่นคือ g เป็น ห.ร.ม. ของ a กับ b ตัวอย่างต่อไปนี้จะแสดงให้เห็นว่า ค่าที่เล็กที่สุดที่มีค่าเป็นบวกของ $ax+by$ คือ g และค่าอื่นๆ ล้วนแล้วแต่เป็นผลคูณจำนวนเท่าของ g

ตัวอย่าง ถ้าเราอยากรู้ว่าค่าที่เป็นจำนวนเต็มของ $42x+30y$ มีอะไรบ้าง เราอาจลองแทนค่า x และ y และคำนวณหาค่า $42x+30y$ ดังตารางด้านล่างนี้

y \ x	-3	-2	-1	0	1	2	3
-3	-216	-174	-132	-90	-48	-6	36
-2	-186	-144	-102	-60	-18	24	66
-1	-156	-114	-72	-30	12	54	96
0	-126	-84	-42	0	42	84	126
1	-96	-54	-12	30	72	114	156
2	-66	-24	18	60	102	144	186
3	-36	6	48	90	132	174	216

ซึ่งจากตารางจะพบว่าค่าที่เป็นค่าบวกที่เล็กที่สุด ก็คือ 6 ซึ่ง $6=(42,30)$ และค่าอื่นๆ ล้วนแต่เป็นผลคูณจำนวนเท่าของ 6 ทั้งสิ้น เช่น $-114=6(-19), 96=6(16), 186=6(31), -156=6(-26)$ เป็นต้น จากแนวคิดนี้ ฟังก์ชัน Linear จึงเป็นฟังก์ชันที่สร้างขึ้นมาเพื่อหาผลเฉลยที่เล็กที่สุดของสมการ $ax+by=g$ และสิ่งสำคัญอีกสิ่งหนึ่งที่ช่วยในการคิด ฟังก์ชัน Linear ก็คือ อัลกอริทึมยูคลิด

พิจารณาการหาผลเฉลยของสมการ $ax+by=g$ ซึ่งในที่นี้ขอยกตัวอย่างสมการ $60x+22y=2$ ให้ $a=60$ และ $b=22$ จากอัลกอริทึมของยูคลิด ถ้าเราเขียนจำนวน a และ b ในรูป $a=bq+r$ ซึ่ง $0\le r<b$ เขียนซ้ำไปเรื่อยๆ จน $r=0$ เราจะสามารถหา ห.ร.ม. ของ $ax+by=c$ ได้ ซึ่ง ห.ร.ม. ก็คือ คำตอบที่เป็นบวกที่เล็กที่สุดนั่นเอง สามารถแสดงผลการคำนวณได้ดังตารางต่อไปนี้

อัลกอริทึมของยูคลิด	จัดรูปใหม่ให้อยู่ในรูปผลรวมเชิงเส้นของ a และ b
$a = 2\times b + 16$	$16 = a - 2b$
$b = 1\times 16 + 6$	$6 = b - 1\times 16$
	$= -a + 3b$
$16 = 2\times 6 + 4$	$4 = 16 - 2\times 6$
	$= (a - 2b) - 2\times(-a + 3b)$
	$= 3a - 8b$
$6 = 1\times 4 + 2$	$2 = 6 - 1\times 4$
	$= (-a + 3b) - 1\times(3a - 8b)$
	$= -4a + 11b$
$4 = 2\times 2 + 0$	

จากตารางเราจะได้ คำตอบที่ต้องการคือ $-4a + 11b = 2$

(ตรวจคำตอบ $-4\times 60 + 11\times 22 = -240 + 242 = 2$) ซึ่งเขียนในรูปทั่วไปได้ดังนี้

$a = q_1 b + r_1$	$r_1 = a - q_1 b$
$b = q_2 r_1 + r_2$	$r_2 = b - q_2 r_1$
	$= b - q_2(a - q_1 b)$
	$= -q_2 a + (1 + q_1 q_2) b$
$r_1 = q_3 r_2 + r_3$	$r_3 = r_1 - q_3 r_2$
	$= (a - q_1 b) - q_3(-q_2 a + (1 + q_1 q_2) b)$
	$= (1 + q_2 q_3) a - (q_1 + q_3 + q_1 q_2 q_3) b$
⋮	⋮

ซึ่งเป็นการยากมากที่จะหาคำตอบโดยพยายามเขียนให้ ห.ร.ม. อยู่ในรูปของผลรวมเชิงเส้นของ a และ b ซึ่งต้องใช้อาเรย์ช่วยในการเก็บค่าต่างๆ และโปรแกรมยังมีข้อจำกัดไม่สามารถหาผลเฉลยได้

ถ้าจำนวนขั้นในการหา ห.ร.ม. ของยูคลิด มีมากกว่า 5 ขั้น (ซึ่งในรายงานนี้ได้แสดงอัลกอริทึมและรหัสของโปรแกรมไว้ในท้ายบทนี้ด้วย)

ดังนั้นจึงได้พยายามคิดวิธีใหม่ในการหาผลเฉลยของสมการ $ax+by=g$ โดยจากการสังเกตจากตารางข้างต้น จะเห็นว่าสัมประสิทธิ์หน้า a ยุ่งยากน้อยกว่าสัมประสิทธิ์หน้า b ดังนั้นเราจะหาสัมประสิทธิ์หน้า a ก่อน นั่นคือได้ค่า x แล้วค่อยหาค่า y จาก $y=\frac{(g-ax)}{b}$ (เพราะ $ax+by=g$) ซึ่งจากการทดลองหาค่าสัมประสิทธิ์หน้า a หลายๆ ครั้ง จนแน่ใจได้ว่า ฟังก์ชัน Linear สามารถคำนวณค่า a ได้ถูกต้อง ซึ่งจะได้อัลกอริทึมของฟังก์ชัน Linear ดังนี้

$ax+by=g$

1. Set $x=1, g=a, v=0$ and $w=b$
2. If $w=0$ then

   Set $y=\frac{(g-ax)}{b}, b\neq 0$ and return the values (g,x,y)
3. Divide g by w (g Div w) with remainder, $g=gw+t$

   Set $g=w$ with $0\leq t<w$
4. Set $s=x-qv$
5. Set $(x,y)=(v,w)$
6. Set $(v,w)=(s,t)$
7. Go to step (2)

คำถาม 1 เราแน่ใจได้อย่างไรว่าค่า $y=\frac{(g-ax)}{b}$ เป็นจำนวนเต็ม

<u>ตอบ</u> จากสมการ $ax+by=g$

จะเห็นว่า อินพุทของเราคือ a และ b ต่างก็เป็นจำนวนเต็ม ค่า ห.ร.ม. g ก็เป็นจำนวนเต็ม และเราหาผลเฉลยของ x ที่เป็นจำนวนเต็ม(สมการไอโอแฟนไทน์ สนใจเฉพาะผลเฉลยที่เป็นจำนวนเต็มเท่านั้น)

(จำนวนเต็ม)×(จำนวนเต็ม) + (จำนวนเต็ม) y = จำนวนเต็ม ดังนั้น y เป็นจำนวนเต็มแน่นอน

คำถาม 2 ทำไมถึงหาผลเฉลยของสมการ $ax+by=g$ แทนที่จะหาผลเฉลยของสมการ $ax+by=c$ ซึ่ง c เป็นค่าคงที่ใดๆ

<u>ตอบ</u> 1. เพราะเราแน่ใจได้แน่นอนว่าสมการ $ax+by=g$ มีผลเฉลย เนื่องจาก ทฤษฎีบท ที่กล่าวมา สมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร ($ax+by=c$) จะมีผลเฉลยต่อเมื่อ $(a,b)\mid c$ เพราะ $g=(a,b)$ ทำให้ $g\mid g$ เสมอ นั่นคือ สมการ $ax+by=g$ มีผลเฉลยแน่นอน

2. จากที่ได้กล่าวมาแล้วข้างต้นว่าค่าที่เล็กที่สุดของ $ax+by$ คือ g ส่วนค่าอื่นๆ ล้วนเป็นผลคูณเป็นจำนวนเท่าของ g ดังนั้นถ้าหากค่า x,y ที่ทำให้ $ax+by=g$ ได้ ก็สามารถหา $ax+by=c$ ได้ โดยนำ c คูณตลอดสมการ $ax+by=g$ ก็จะได้ $a(\frac{cx}{g})+b(\frac{cy}{g})=c$ ที่ต้องการ ให้ $x_1=\frac{cx}{g}, y_1=\frac{cy}{g}$ ก็จะได้คำตอบของสมการเป็น x_1 และ y_1

ข้อจำกัดของอัลกอริทึม Linear และแนวทางแก้ไข

1. อินพุทที่จะเข้ามา (ค่า a และ b ของสมการ $ax+by=g$) ต้องเป็นค่าบวกเท่านั้น และค่า a ต้องมากกว่า b ด้วย

อธิบาย เนื่องจาก ฟังก์ชัน Linear สร้างขึ้นโดยใช้แนวคิดจากอัลกอริทึมของยูคลิดซึ่งสามารถเขียนตัวตั้ง (a) ในรูปผลคูณของตัวหาร (b) บวกเศษ ดังนี้ $a=bq+r$ ซึ่ง q เป็นผลลัพธ์ และ $0\le r<b$ สมมติถ้าค่า $a=-60, b=22$ จะเขียน $a=bq+r$ ได้ดังนี้ $-60=22(-3)+6, 0\le b<22$ จะเห็นว่าเราไม่สามารถเขียน $-60=22(-2)+(-16)$ เพราะ $r=(-16)<0$ เพื่อขจัดปัญหาดังกล่าว จึงให้ค่าที่จะเข้ามาในฟังก์ชัน Linear เป็นบวกตลอดและแน่นอน $|a|$ ต้องมากกว่า $|b|$ เพราะ a เป็นตัวตั้ง และ b เป็นตัวหาร ดังนั้น จึงต้องเซตค่าสัมบูรณ์ของค่ามากให้เป็น a_1 (ตัวตั้ง) และค่าน้อยให้เป็น b_1 (ตัวหาร)

<u>แนวทางแก้ไข</u>

ใส่ค่าสัมบูรณ์ให้กับ a และ b และเปรียบเทียบค่าก่อนจะส่งค่าเข้าในฟังก์ชัน Linear ซึ่งหลังจากคำนวณจากฟังก์ชัน Linear ได้ค่า x,y แล้วค่อยนำค่า x,y ไปปรับเครื่องหมายภายหลัง (ซึ่งได้อธิบายไว้ในอัลกอริทึมของสมการไดโอแฟนไทน์ 2 ตัวแปร และ 3 ตัวแปร)

ต่อไปเป็นตัวอย่างการใช้อัลกอริทึม Linear ในการหาผลเฉลยเริ่มต้นของสมการไดโอแฟนไทน์ 2 ตัวแปรที่มีสัมประสิทธิ์และค่าคงที่ติดลบ

อยากรู้ว่าอัลกอริทึมสามารถใช้กับค่าลบได้หรือไม่

2. จะเห็นว่าในโปรแกรมแก้สมการไดโอแฟนไทน์ 2 ตัวแปร และ 3 ตัวแปร จะมีฟังก์ชัน Linear จริงๆ แล้วเป็นฟังก์ชันเดียวกัน แต่เนื่องจากข้อจำกัดของภาษาที่ใช้เขียนโปรแกรม คือ 1 ฟังก์ชันสามารถคืนค่าได้เพียงค่าเดียว แต่เราต้องการคืนค่า 2 ค่า คือ x และค่า y

<u>แนวทางแก้ไข</u>

เราจึงให้ฟังก์ชัน Linear คืนค่า x และค่า y

3. ฟังก์ชัน Linear จะคำนวณค่า y ผิดพลาด ถ้าค่า a และ b มีค่ามากๆ (คำนวณค่า x ไม่ผิดพลาดเพราะเราหาค่า x จาก $ax+by=g$ ซึ่ง g เป็นค่าบวกที่เล็กที่สุดที่เป็นผลบวกของ $ax+by$ จึงได้ค่า x เล็กอยู่แล้ว) แต่ค่า y จะผิดพลาดเพราะข้อจำกัดของภาษาเพราะข้อมูลจำนวนเต็มไม่สามารถรับค่าได้เกิน 32767

ตัวอย่าง เช่น สมการ $12453x+2347y=1$ ถ้าใช้อัลกอริทึม Linear จะได้ค่า $x=304$ แต่ค่า y เกิดจาก $y=\frac{(g-ax)}{6}$ นั่นคือ $y=\frac{[1-(12453)(304)]}{2347}$ จะเห็นว่า 12453×304 ก็เกิน 32767 แล้ว จึงได้ค่า y ที่ผิดพลาด

ขั้นตอนวิธีการแก้สมการไดโอแฟนไทน์ 2 ตัวแปร

Input รับค่าสัมประสิทธิ์ a,b และค่าคงที่ c (ต้องเป็นจำนวนเต็ม)

1. ตรวจสอบว่ามีตัวใดเป็น ศูนย์ หรือไม่ ถ้ามีตัวที่เป็น 0 ให้ คืนค่าข้อความ

"This is not linear Diophantine Equation of 2 variables"

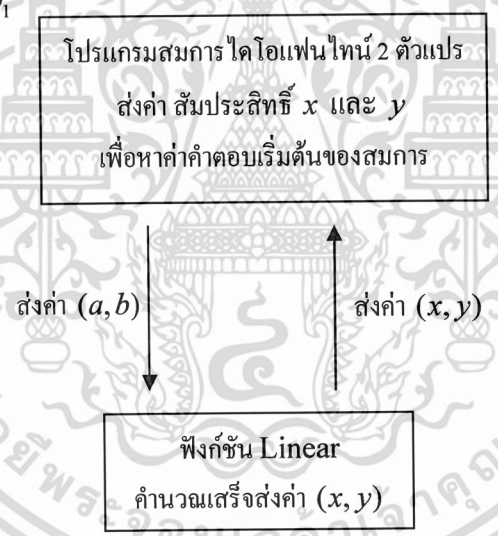
และ ออกไปที่หน้าจอหลัก

2. ถ้าไม่มีตัวใดเป็นศูนย์เลย ให้ตรวจสอบว่าสมการมีผลเฉลยหรือไม่

นั่นคือ $(|a|,|b|)|c$ (ส่งค่า a,b ไปหา ห.ร.ม. แล้วกลับมาหาร c)

3. ถ้าสมการมีผลเฉลยจะหาผลเฉลยโดย ฟังก์ชัน Linear (หาผลเฉลยของ $ax+by=g$)

ก่อนจะเข้าฟังก์ชัน Linear ตรวจสอบก่อนว่าค่าสัมบูรณ์ของสัมประสิทธิ์หน้า x และ y ตัวใดมากกว่ากัน นั่นคือ เปรียบเทียบ $|a|,|b|$ ตัวใดมากเอาใส่ในตัวแปร a_1 ตัวใดน้อยกว่าใส่ในตัวแปร b_1



รับค่า x,y มาไว้ในตัวแปร x_1,y_1 ตามลำดับ

If $|a|<|b|$ ให้สลับค่า x_1 กับ $y_1 (w=x_1, x_1=y_1, y_1=w)$

End if

If $a<0$ then $x_0=(-1)\times x_1$

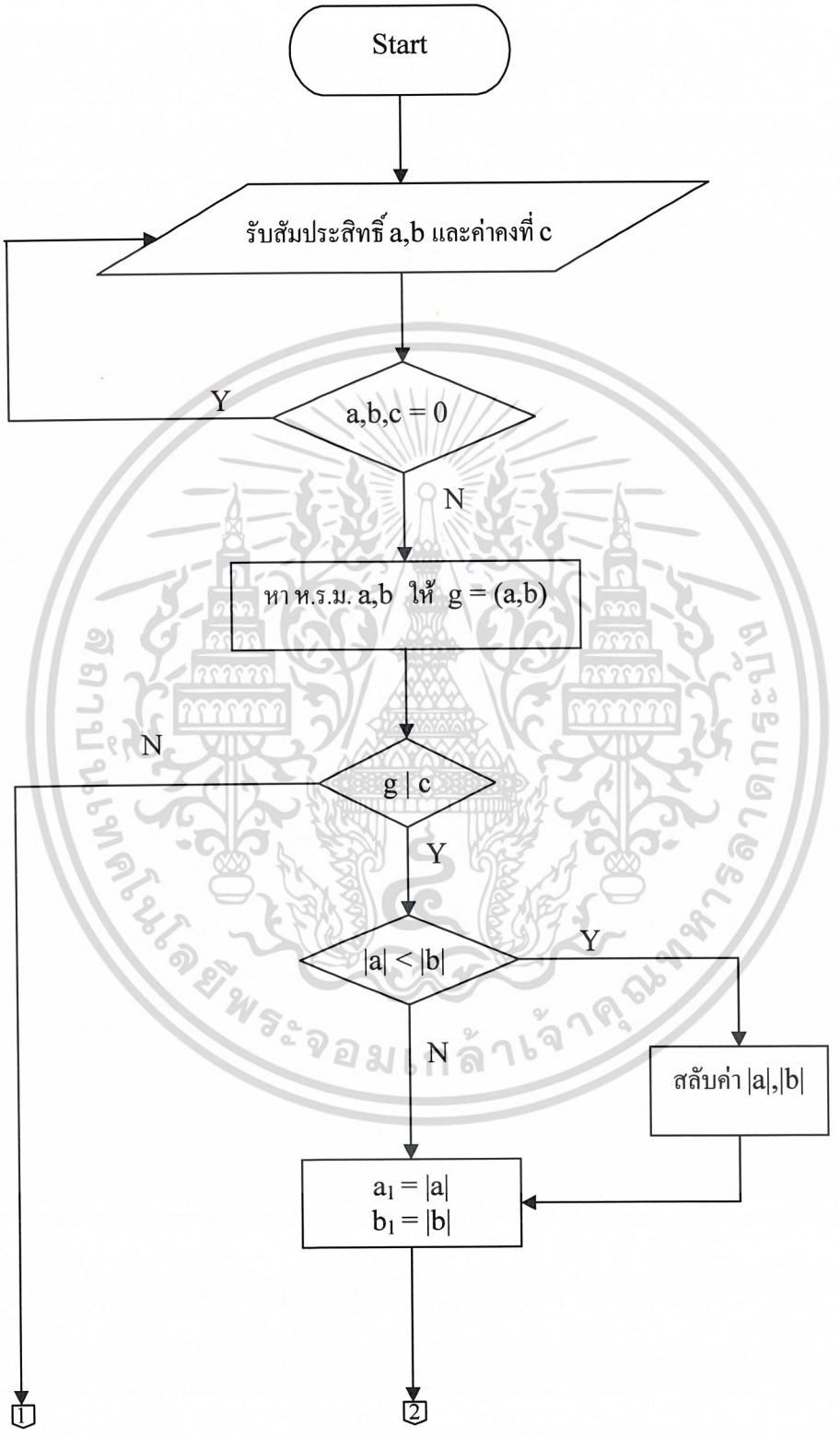
If $b<0$ then $y_0=(-1)\times y_1$

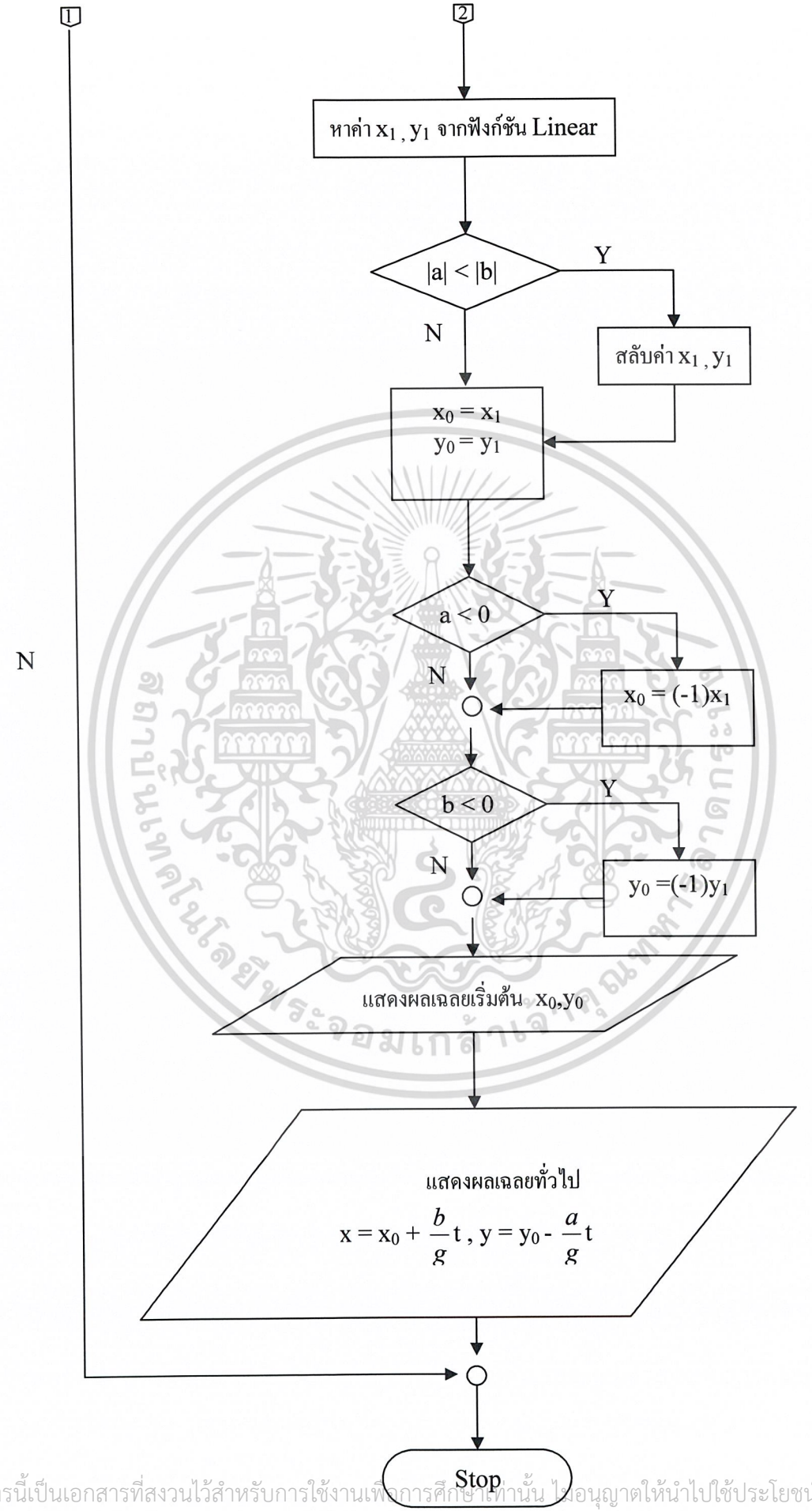
ให้ $k=c/g$ และ $x_1=k\times x_1, y_1=k\times y_1$

Writeln คำตอบทั่วไป คือ $x=x_0+\frac{b}{g}t, y=y_0-\frac{a}{g}t$

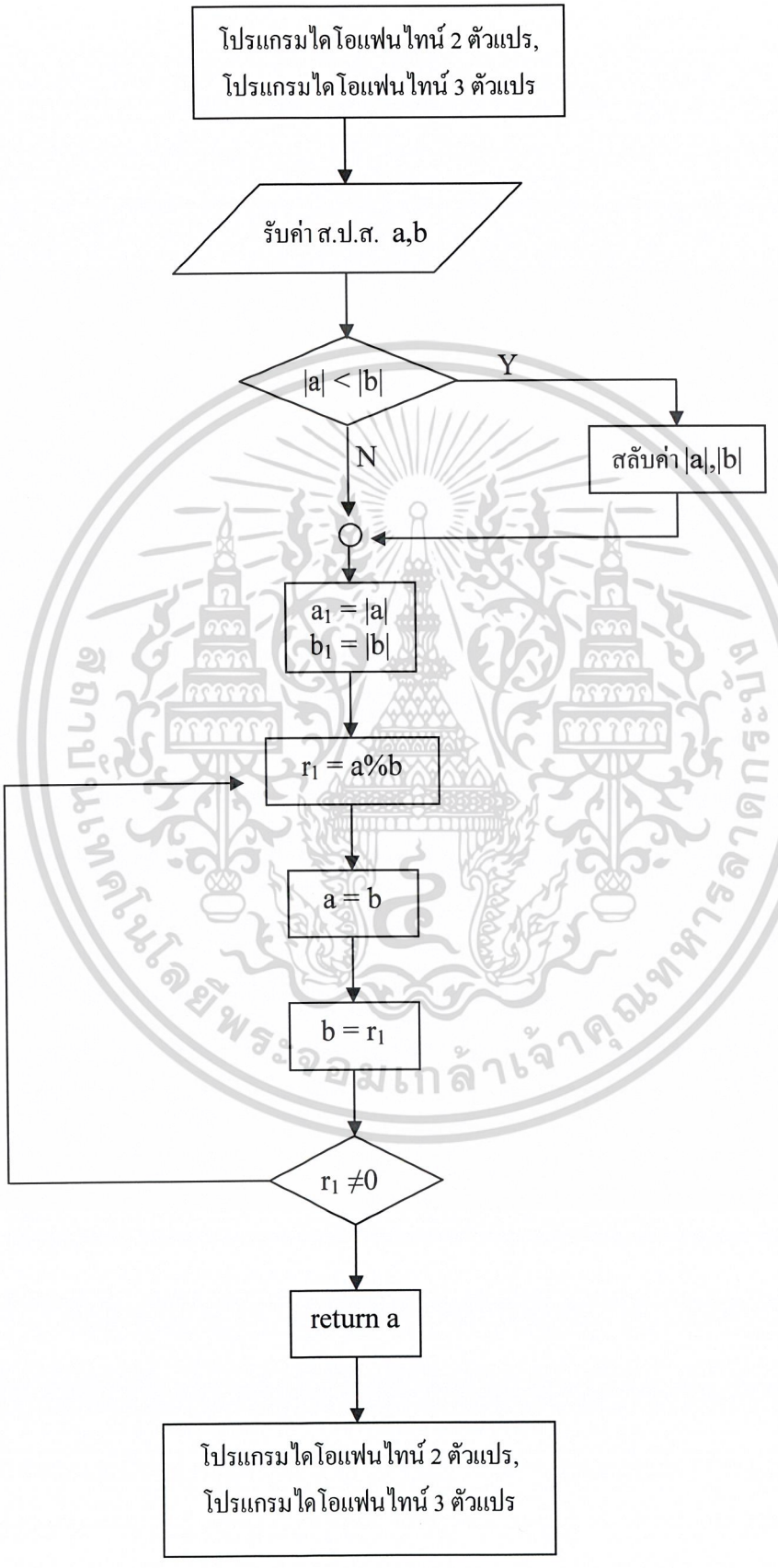
แสดงการตรวจคำตอบให้ดูและ run ผลลัพธ์ แสดงค่า t จำนวนหนึ่ง

แผนผังแสดงการทำงานของโปรแกรมไดโอแฟนไทน์ 2 ตัวแปร

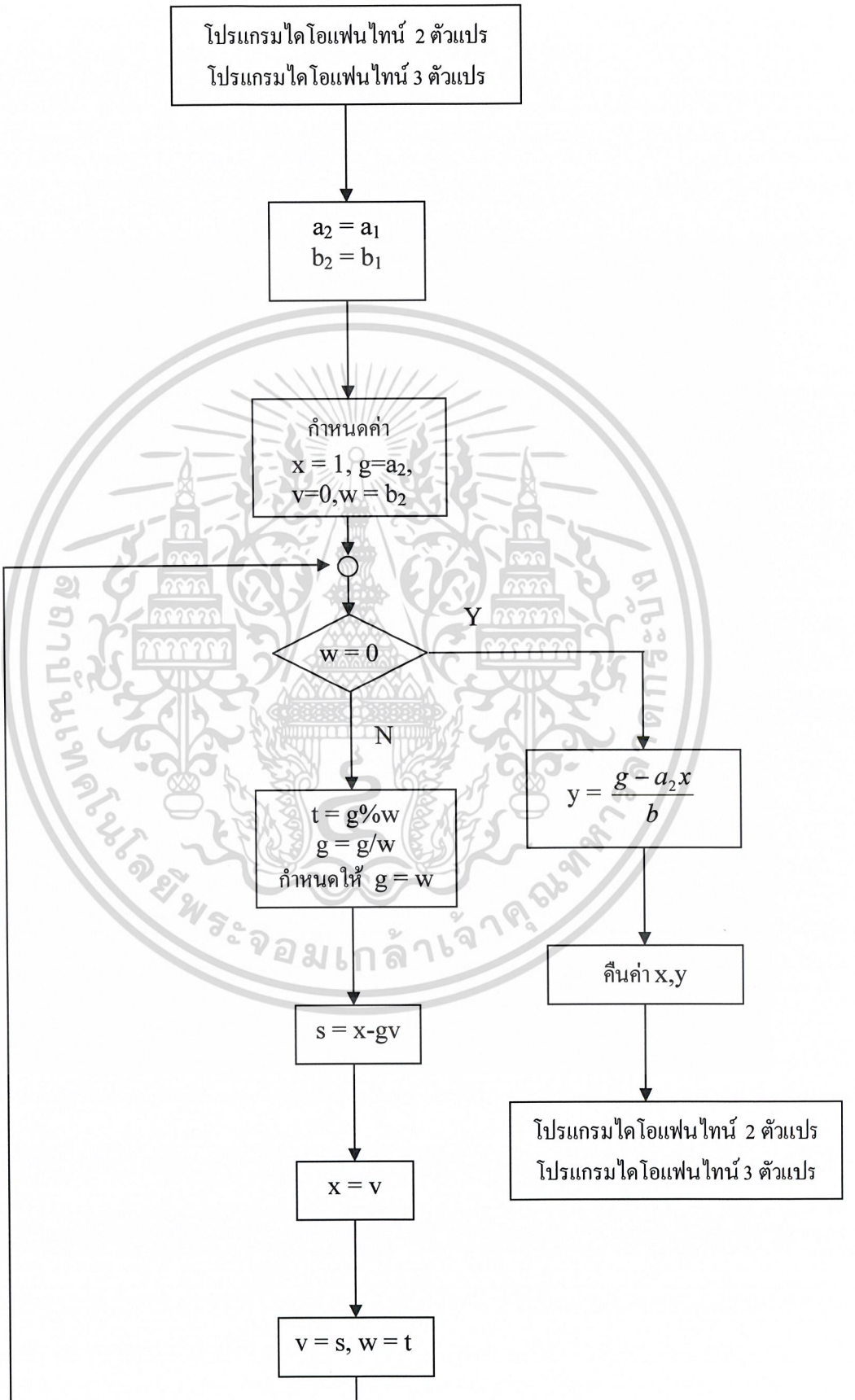




ฟังก์ชัน GCD (การหารร่วมมาก)



ฟังก์ชัน Linear (หาค่าตัวแปร)



ตัวอย่างโจทย์ที่แก้ตามขั้นตอนวิธีการแก้สมการไดโอแฟนไทน์ 2 ตัวแปร

ตัวอย่าง 1

$$60x + 22y = (60,22) = 2$$

(1) ให้ $x = 1, g = 60, v = 0, w = 22$

(2) If $22 \neq 0$ then

(3) 60 Div 22 = 2 , $60 = 2(22) + 16,$ set $g = 22$

(4) ให้ $g = x - qv$ (นั่นคือ $s = 1 - 2(0)$) $\therefore s = 1$

(5) Set $(x, y) = (0,22)$

(6) Set $(v, w) = (1,16)$

ตอนนี้ $w = 16$ $\therefore w \neq 0$ ยังไม่ต้อง return ค่า

(3) 22 Div 16 = 1 ,$22 = 1(16) + 6$ Set $g = 16$

(4) $s = 0 - 1(1) = -1$

(5) $(x, y) = (1,16)$

ตอนนี้ $w = 6, w \neq 0$

(3) 16 Div 6 = 2 ,$16 = 2(6) + 4$ Set $g = 6$

(4) $s = 1 - 2(-1) = 3$

(5) $(x, y) = (-1,6)$

(6) $(v, w) = (3,4)$

ตอนนี้ $w = 4, w \neq 0$

(3) 6 Div 4 = 1 ,$6 = 1(4) + 2$ Set $g = 4$

(4) $s = -1 - 1(3) = -4$

(5) $(x, y) = (3,4)$

(6) $(v, w) = (-4,2)$

ตอนนี้ $w = 2, w \neq 0$

(3) 4 Div 2 = 2 ,$4 = 2(2) + 0$ Set $g = 2$

(4) $s = 3 - 2(-4) = 11$

(5) $(x, y) = (-4,2)$

(6) $(v, w) = (11,0)$

ซึ่งตอนนี้ $w = 0$ แล้ว ดังนั้น Set $y = \dfrac{(2 - (60)(-4))}{22} = 11$ ซึ่งจะได้คำตอบ คือ

$x = 4, y = 22$ (ตรวจคำตอบโดยนำไปแทนค่าในสมการเริ่มต้นจะได้ $60(-4) + 22(11) = 2$ จริง)

ตัวอย่าง 2 $4x - 83y = -6$

เนื่องจาก $|-83| > |4|$ จะเห็นว่า ค่าสัมบูรณ์ของ x น้อยกว่าค่าสัมบูรณ์ของ y

ดังนั้นให้ $a = 83, b = 4$

(1) $x = 1, g = 83, v = 0, w = 4$

(2) $w \neq 0$

(3) 83 Div 4 = 20 ,$83 = 4(20) + 3, g = 4$

(4) $g = 1$

(5) $(x, y) = (0,4)$

(6) $(v, w) = (1,3)$

(2) $w \neq 0$

(3) 4 Div 3 = 1 ,$4 = 3(1) + 1, g = 3$

(4) $s = 0 - 1(1) = -1$

(5) $(x, y) = (1,3)$

(6) $(v, w) = (-1,1)$

(2) $w \neq 0$

(3) 3 Div 1 = 3 ,$3 = 1(3) + 0, g = 1$

(4) $s = 1 - (3)(-1) = 4$

(5) $(x, y) = (-1,1)$

(6) $(v, w) = (4,0)$

(2) $w = 0$ แล้ว Set $y = 1 - 83(-1) = 84/4 = 21$

$\therefore x = -1, y = 21$

เอา $\dfrac{c}{g}$ คูณคำตอบ $\dfrac{c}{g} = -6/1 = -6$

จะได้ $x_0 = (-1)(-6) = 6$ และ $y_0 = 21(-6) = -126$ เสร็จแล้วสลับค่า x, y ที่ได้ (เพราะ $|x| < |y|$) จะได้ $x = -126, y_0 = 6$

ตรวจสอบเครื่องหมายของสมการเริ่มต้น พบว่าสัมประสิทธิ์หน้า y ติดลบให้เอา -1 คูณ y_0 จะได้ $x_0 = -126$ และ $y_0 = -6$ ลองตรวจคำตอบดู

$4(-126) - 83(-6) = -6$ เป็นจริง

คำตอบทั่วไปคือ $x = -126 + (\frac{-83}{1})t, y = -6 - \frac{4}{1}t$ #

โปรแกรมสมการไดโอแฟนไทน์ 2 ตัวแปร $ax + by = c$

```
#include "stdio.h"
#include "conio.h"
#include "stdlib.h"
#include "math.h"

int Gcd(int a0,int b0);
int LinearI(int a,int b);
/* LinearII(int a5,int b5);  */

int Gcd(int a0,int b0)                    //ฟังก์ชันการหาตัวหารร่วมมาก
{
        int a,b,r1,temp1,q;
        a=a0;   b=b0;

        if(a-b<0)
        //ถ้าค่าที่รับเข้ามาตัวแรกน้อยกว่าตัวหลังให้ทำการสลับค่ากัน
        {
                temp1=a;        a=b;     b=temp1;
        }

        do                  //หาตัวหารร่วมมากโดยค่าที่ได้คือค่า q
        {
                q=a/b;
                r1=a-b*q;       a=b;     b=r1;
        }while(r1!=0);  //ออกจากลูปนี้เมื่อเศษเป็นศูนย์
        return a;
}
```

```
int LinearI(int a,int b)          //ฟังก์ชันเพื่อหาค่า x
{
        int x,g,v,w,q,t,s;
        x=1;    g=a;    v=0;    w=b;
        do                        //จะเข้าลูปนี้เมื่อค่าที่รับเข้ามาไม่เป็นศูนย์เท่านั้น
        {       q=g/w;
                t=g-q*w;
                g=w;
                s=x-(q*v);
                x=v;
                v=s;    w=t;
         }while(w!=0);

         return(x);
}

LinearII(int a5,int b5)           //ฟังก์ชันเพื่อหาค่า y
{
        int x,g,v,w,q,t,s; int y;
        x=1;    g=a5;   v=0;    w=b5;
        do                        ////จะเข้าลูปนี้เมื่อค่าที่รับเข้ามาไม่เป็นศูนย์เท่านั้น
        {
                t=g%w;            //t คือตัวเศษที่ได้จากการหาร g ด้วย w
                q=g/w;
                g=w;
                s=x-(q*v);
                x=v;    y=w;
                v=s;    w=t;
          }while(w!=0);
```

```
        y=(g-(a5*x))/b5;
        return(y);
}

void main()
{
        int a,b,c,a1,b1,g,Test,a2,b2,x1,temp,k,x0,y0,k2,k3,c1,t1, y1,q1;
        char ans;
        clrscr();
        printf("\n This is the program for solving Linear Diophantine ax+by=c");
        //      แสดงข้อความว่านี่คือโปรแกรมที่ใช้แก้สมการไดโอแฟนไทน์ ax+by=c

        printf("\n Enter coefficient of x:");
        scanf("%d",&a);
        //      รับค่า a ซึ่งเป็นสัมประสิทธิ์ของ x

        printf("\n Enter coefficient of y:");
        scanf("%d",&b);
        //      รับค่า b ซึ่งเป็นสัมประสิทธิ์ของ y

        printf("\n Enter constant c:");
        scanf("%d",&c);
        //      รับค่าคงที่ของสมการ

 if ((a==0)||(b==0)||(c==0))      //ตรวจสอบว่าค่าทั้งสามที่รับเข้ามามีตัวใดเป็นศูนย์หรือไม่
  {
        printf("\n This is not Linear Diophantine Equation of 2 variables");
        //      ถ้ามี ให้แสดงข้อความว่าสมการนี้ไม่เป็นสมการเชิงเส้น
  }
```

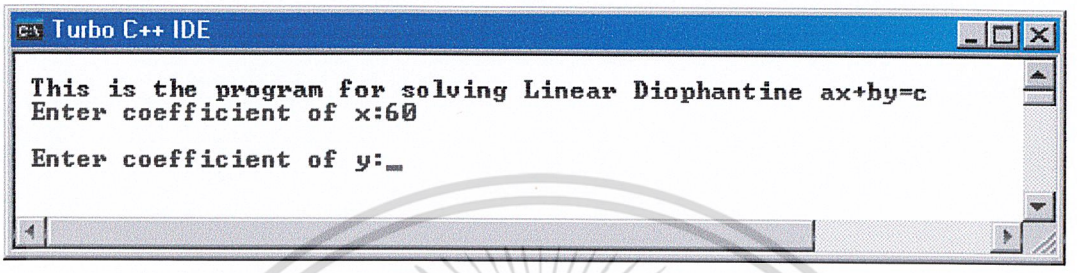
```
//ทำการแปลงทุกค่า a และ b ให้มีค่าเป็นบวกโดยการใส่ค่าสัมบูรณ์
a1=fabs(a);                b1= fabs(b);
 g=Gcd(a,b);               //เข้าฟังก์ชันการหาตัวหารร่วมมาก
printf("\n gcd=%d",g); //แสดงค่าตัวหารร่วมมากของสมการ
 q1=c/g;
 Test=c-q1*g;   a2=a1;            b2=b1;

 if(Test!=0)
          printf("\n This equation has no solution!");
          //แสดงว่าสมการนี้ไม่มีผลเฉลย
 else
 {
          if(a2-b2<0)
          {
          temp=a2; a2=b2; b2=temp;
          }

          x1=LinearI(a2,b2);
          y1=LinearII(a2,b2);

          k=c/g;  x1=k*x1;          y1=k*y1;
          //        หาคำตอบของสมการในรูปแบบ ax+by=c
          if(a1-b1<0)       //ถ้าค่า a น้อยกว่า b ให้ทำการสลับค่าของ x1 และ y1
          {
                    temp=x1; x1=y1; y1=temp;
          }

          if(a<0)             //ถ้าค่า a เป็นลบให้คูณค่า x1 ด้วย -1
          {
```

```
x1=-1*x1;
}

if(b<0)          ////ถ้าค่า b เป็นลบให้คูณค่า y1 ด้วย -1
{
        y1=-1*y1;
}
x0=x1;  y0=y1;
printf("\n The initial solutions of %dx+%dy=%d:",a,b,c);
//      แสดงผลเฉลยเริ่มต้นของสมการ ax + by = c
printf("\n x0=%d",x0);
//      แสดงค่า x0
printf("\n y0=%d",y0);
//      แสดงค่า yo

k2=b/g;         k3=a/g;
printf("\n The general solutions of %dx+%dy=%d:",a,b,c);
//      แสดงผลเฉลยทั่วไปของสมการ ax + by = c
printf("\n x=%d+(%d)t,t be integers",x0,k2);
//      แสดงค่า x=x0 + k2
printf("\n y=%d-(%d)t,t be integers",y0,k3);
//      แสดงค่า x=y0 + k3
printf("\n Do you want to check your answers? y/n");
scanf("%c",&ans);
//      ถ้าต้องการตรวจสอบคำตอบให้เข้าลูปนี้
if(ans=='y')
{
c1=a*x0+b*y0+a*k2+b*-1*k3;
printf("\n %d(%d+(%d)t)+%d(%d-(%d)t)=%d",a,x0,k2,b,y0,k3,c1);
```

```
//          แสดงค่า a(x0+k2)t + b(y0+k3)t=c1
}
printf("\n This will show you some answers from difference values of t");
//          แสดงผลเฉลยของสมการที่มีค่าต่างๆกันซึ่งแปรผันกับค่าของ t
printf("\n t                x=%d+(%d)t              y=%d-(%d)t",x0,k2,y0,k3);
// โดยค่า  t  จะเริ่มตั้งแต่ 1 ถึง 20
for(t1=-10;t1<=20;t1++)
 {
        int x=x0+k2*t1;          int y=y0-k3*t1;
        printf("\n%d              %d              %d",t1,x,y);
 }
}
}
```

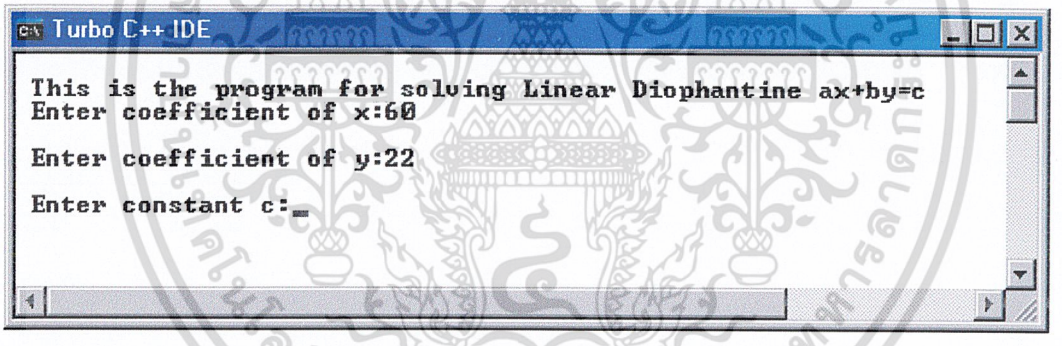
ตัวอย่างแสดงผลการใช้งานโปรแกรมสมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร

ใส่ค่าที่ต้องการหา คือ สัมประสิทธิ์หน้า x

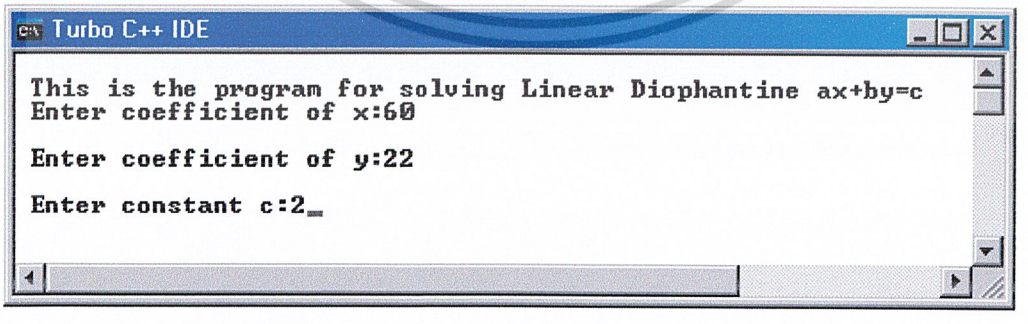


รูปที่ 3.18 แสดงการป้อนค่าสัมประสิทธิ์หน้า x

และสัมประสิทธิ์หน้า y

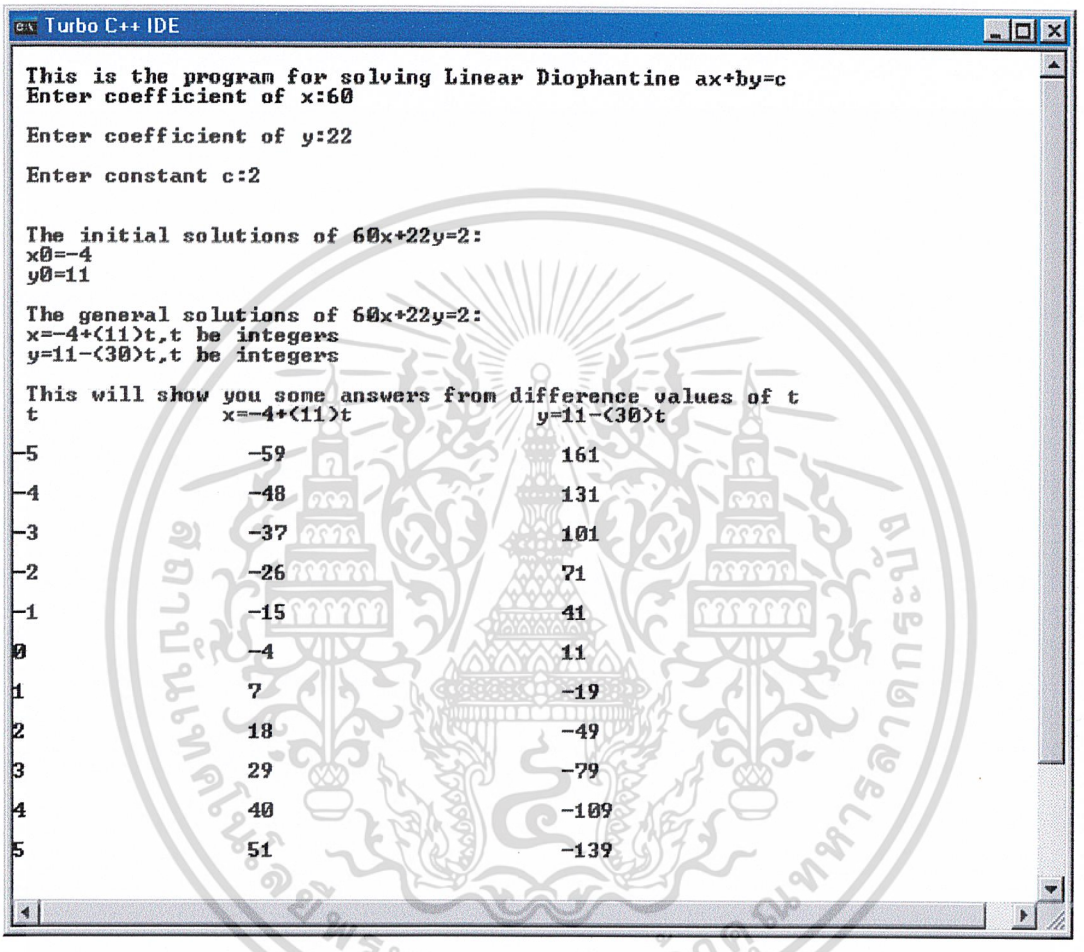


รูปที่ 3.19 แสดงการป้อนค่าสัมประสิทธิ์หน้า y



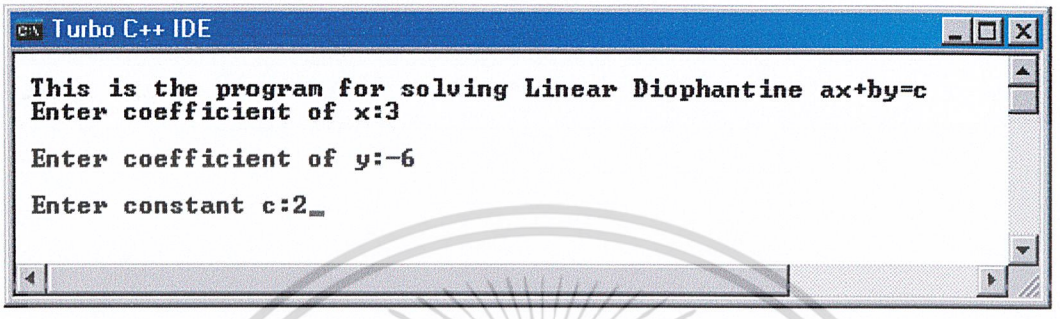
รูปที่ 3.20 แสดงการป้อนค่าคงที่ c

ซึ่งสมการไดโอแฟนไทน์นี้ จะสามารถหาค่าได้ ก็ต่อเมื่อ ค่าคงที่ c ที่ป้อนเข้าไป สามารถหารกับ ห.ร.ม. ของ a และ ลงตัว จะได้ผลดังนี้



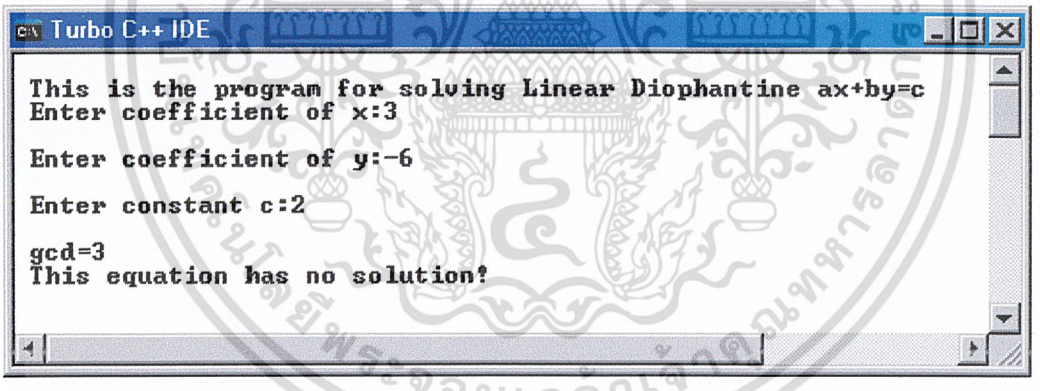
รูปที่ 3.21 แสดงผลการคำนวณออกมา

แต่ถ้าค่าคงที่ c ไม่สามารถหาร ห.ร.ม. ของ a และ b ลงตัวแล้ว



รูปที่ 3.22 แสดงการป้อนค่าคงที่ซึ่งไม่เป็นไดโอแฟนไทน์

จะได้ผลออกมาดังนี้



รูปที่ 3.23 แสดงหน้าจอซึ่งแสดงค่าออกมาว่าสมการไม่สามารถหาค่าคำตอบได้

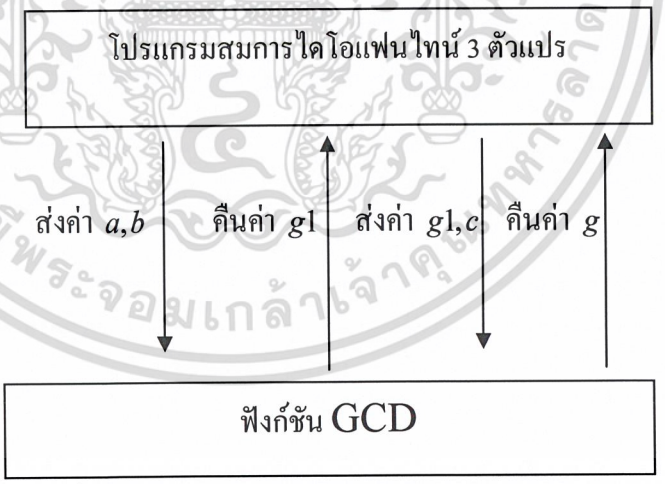
3.4. สมการไดโอแฟนไทน์ 3 ตัวแปร

ขั้นตอนวิธีการแก้สมการไดโอแฟนไทน์ 3 ตัวแปร $ax+by+cz=n$

ขั้นที่ 1 รับค่า a,b และ c ซึ่งเป็นสัมประสิทธิ์ของตัวแปร x,y และ z ตามลำดับ รวมทั้งค่าคงที่ของสมการ ซึ่งในที่นี้ใช้ค่า n

ขั้นที่ 2 ทำการตรวจสอบค่าที่รับเข้ามาว่ามีค่าใดเป็นศูนย์หรือไม่ ถ้ามีให้แจ้งข้อความเตือนและทำการรับค่านั้นใหม่

ขั้นที่ 3 เมื่อผ่านการตรวจสอบในขั้นตอนที่ 2 แล้วให้ทำการตรวจดูว่าสมการนี้มีผลเฉลยหรือไม่ ซึ่งถ้า ตัวหารร่วมมากของ a,b และ c สมมติแทนด้วยตัวแปร g หาร n ได้ลงตัวก็จะสรุปได้ว่าสมการนี้มีผลเฉลย ซึ่งในการหาตัวหารร่วมมาก g ต้องทำการหา 2 ครั้ง ครั้งแรกหาตัวหารร่วมมากของ a กับ b ให้แทนด้วยตัวแปร $g1$ แล้วค่อยหาตัวหารร่วมมากของ $g1$ และ c ก็จะได้ตัวหารร่วมมาก g นั่นเอง ซึ่งสามารถแสดงการหาตัวหารร่วมมาก g ได้ดังแผนภาพดังนี้



ขั้นที่ 4 ถ้าสมการมีผลเฉลย ก็จะทำการหาผลเฉลยของสมการ ซึ่งจะทำการหาผลเฉลยของสมการ $ax+by+cz=g$ ก่อน

4.1 หาค่า $z0$ ก่อน

อธิบาย จากสมการ $ax+by+cz=g$

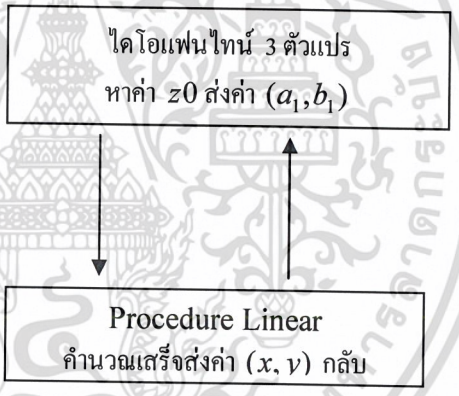
จะได้ $ax+by=g-cz$

จะมีคำตอบเมื่อ $(a,b)=g1/(g-cz)$

นั่นคือ มีจำนวนเต็ม k ที่ทำให้ $g1\times k=g-cz$

หรือ $cz+g1k=g$

จากนั้นก็ทำการเปรียบเทียบว่าค่าสัมบูรณ์ของ c กับค่าสัมบูรณ์ของ $g1$ ตัวใดมีค่ามากให้ใส่ค่าในตัวแปร $a1$ ส่วนตัวที่มีค่าน้อยให้ใส่ค่าในตัวแปร $b1$ เราจะหาค่า $z0$ โดยส่งค่าตัวแปร $a1,b1$ ไปในฟังก์ชัน Linear ดังแผนภาพดังนี้



รับค่า x,y มาไว้ในตัวแปร $x1,y1$ ตามลำดับ แล้วพิจารณาเครื่องหมายของตัวแปรดังนี้

ถ้า ค่าสัมบูรณ์ของ c น้อยกว่า $g1$ แล้ว สลับค่า $x1,y1$

ถ้าตัวแปร c มีค่าน้อยกว่า 0 แล้ว $x1=(-1)\times x1$

ถ้าตัวแปร $g1$ มีค่าน้อยกว่า 0 แล้ว $y1=(-1)\times y1$

ซึ่งจะได้ $z0=x1$ และผลเฉลยทั่วไปคือ $z0=z0+g1t1$

ขั้นที่5 ทำการหาค่า x และ y

อธิบาย เอา $z0$ ไปแทนในสมการเริ่มต้นจะได้

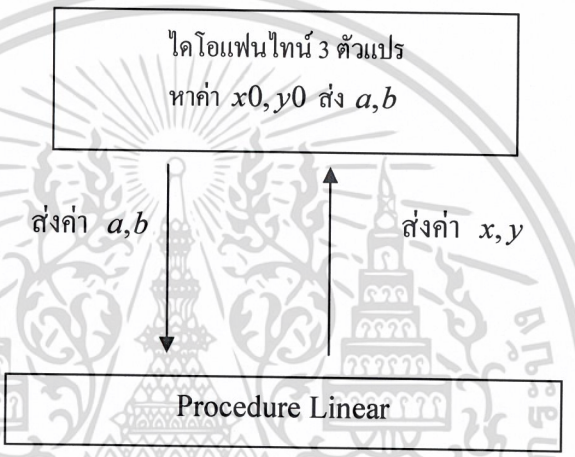
$ax+by=1-cz0$

ซึ่งจะมีคำตอบเมื่อ $(a,b)|(1-cz0)$

5.1 ให้ $m=1-cz0$ _____*

5.2 ทำการเปรียบเทียบว่าค่า $|a|$ หรือ $|b|$ ตัวใดมีค่ามากให้ใส่ค่าให้ตัวแปร a ตัวที่มีค่าน้อยให้ใส่ค่าในตัวแปร b

แล้วส่งค่า a,b ไปคำนวณหาค่า x,y ใน ฟังก์ชัน Linear ดังแผนภาพ



รับค่า x,y มาไว้ในตัวแปร $x2,y2$ ตามลำดับ แล้วพิจารณาเครื่องหมายของตัวแปรดังนี้

ถ้า ค่าสัมบูรณ์ของ a น้อยกว่าค่าสัมบูรณ์ของ b แล้ว สลับค่า $x2,y2$

ถ้า ค่าตัวแปร a มีค่าน้อยกว่า 0 แล้ว $x2=(-1)\times x2$

ถ้า ค่าตัวแปร b มีค่าน้อยกว่า 0 แล้ว $y2=(-1)\times y2$

5.3 ให้ $k2=\dfrac{m}{g1}$ _____**

5.4 ให้ $x3=k2\times x2$ และ $y3=k2\times y2$

5.5 ให้ $x4=x3, y4=y3$

5.6 คำตอบเริ่มต้นจริงๆ ให้นำ $\dfrac{n}{g}$ คูณตลอดสมการ

ให้ $k=\dfrac{n}{g}$

นั่นคือ

$$Z0 = k \times z2$$

$$X0 = k \times x2$$

$$Y0 = k \times y2$$

5.7 ให้ $k2 = \frac{b}{g1}, k3 = x3c, k4 = \frac{a}{g1}$

$$K5 = y4c$$

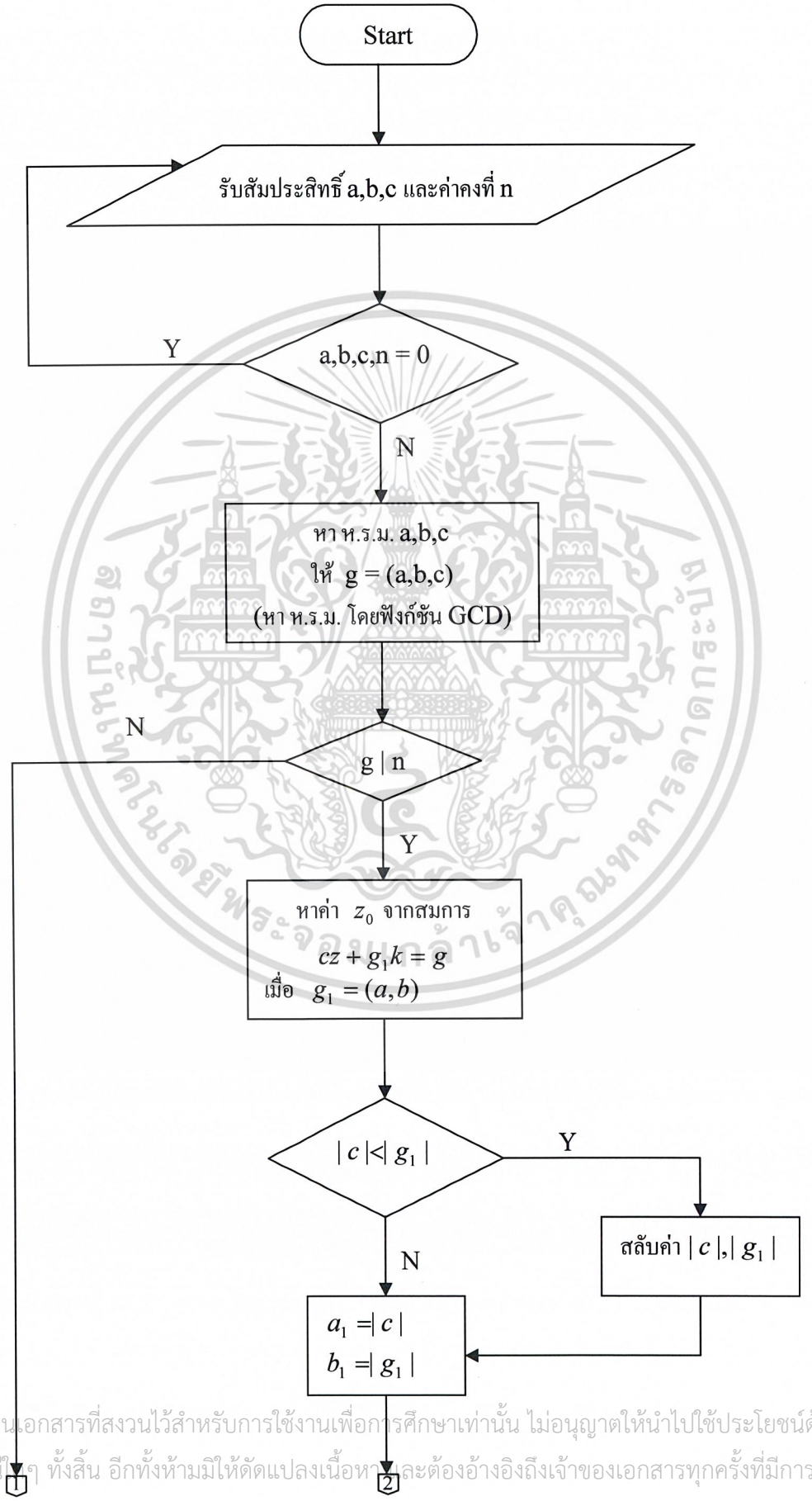
จะได้คำตอบทั่วไปคือ

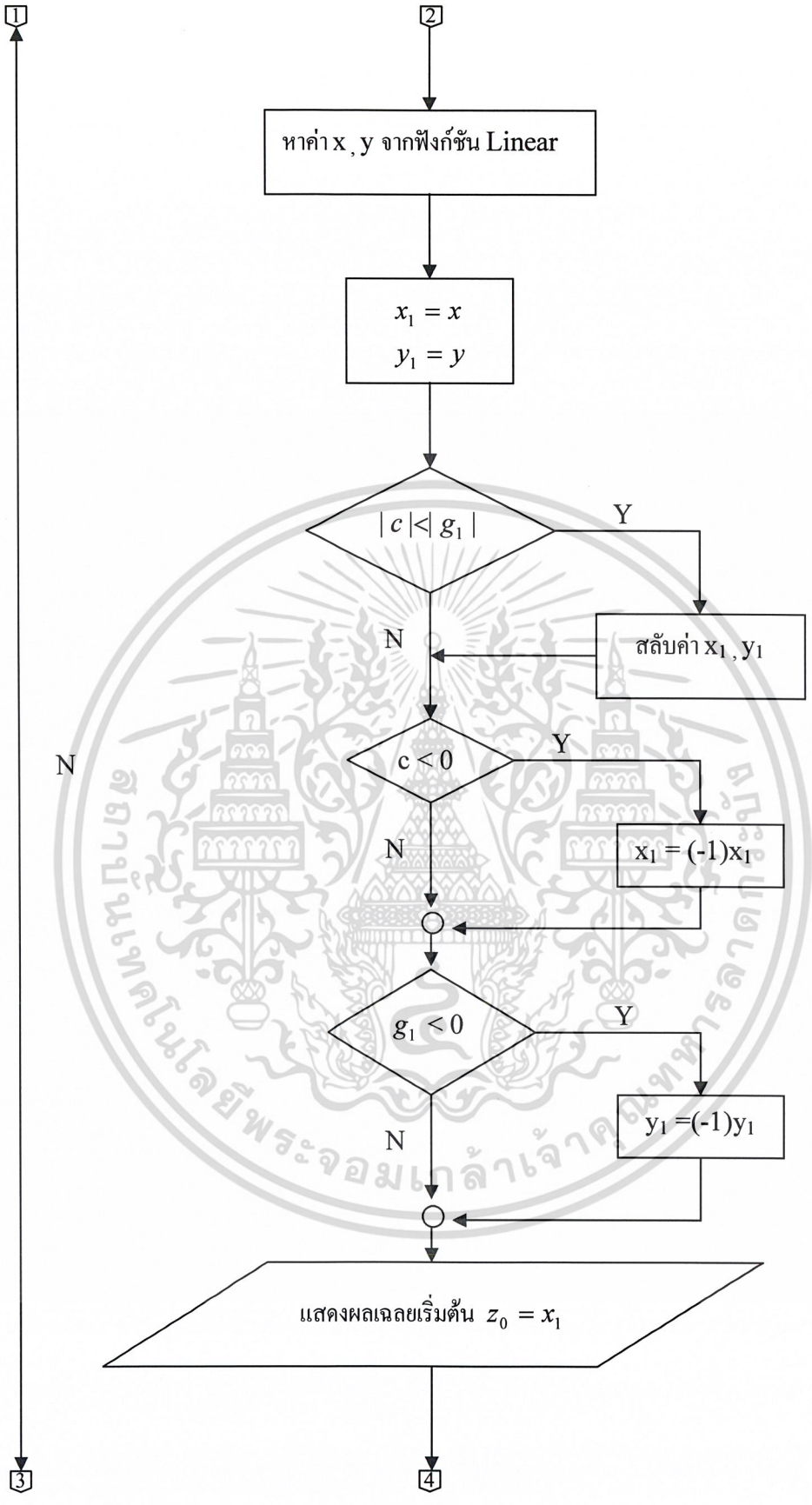
$$X = x0 + k2t2 - k3t1$$

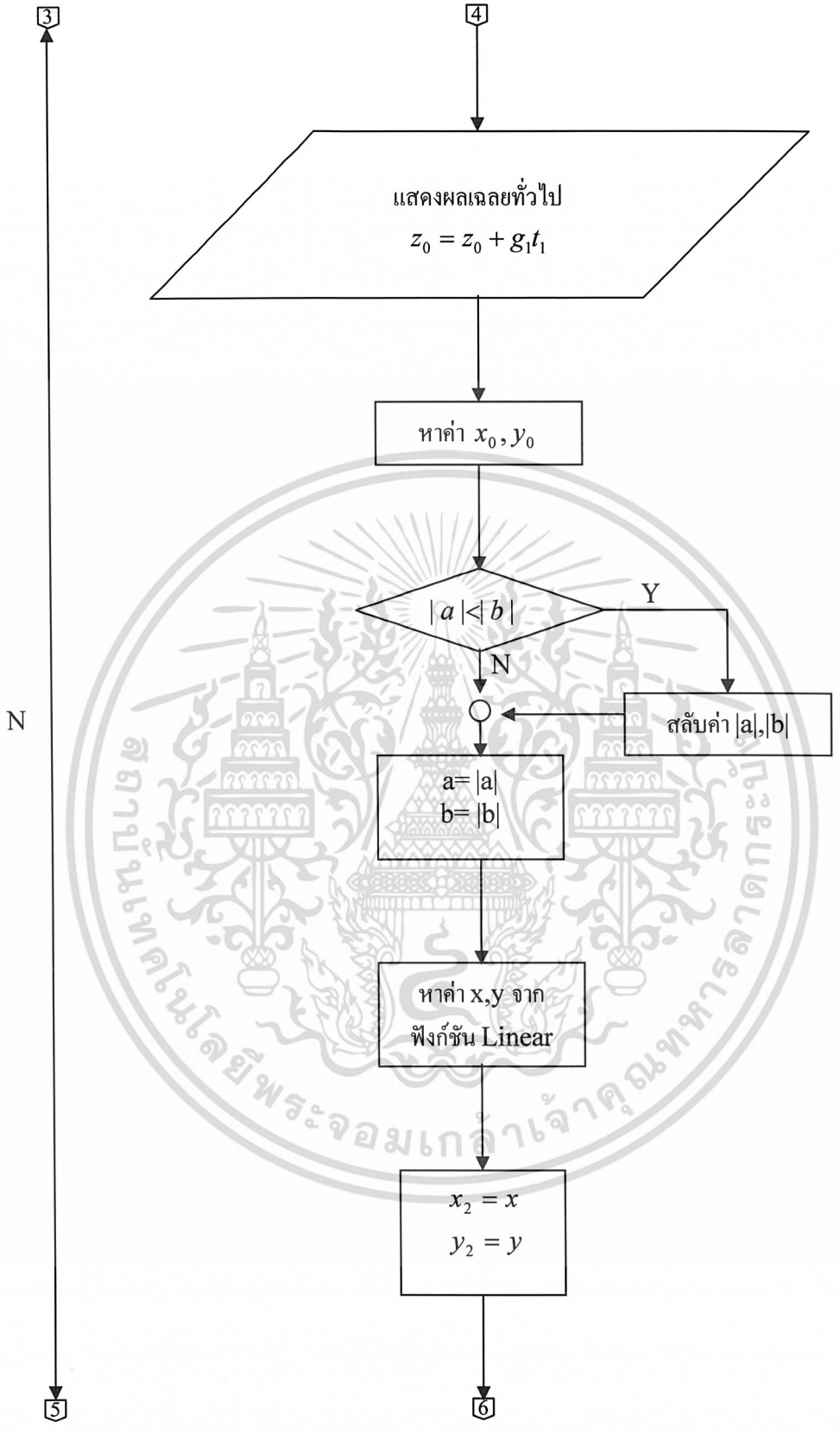
$$Y = y0 - k4t2 - k5t1 \quad ***$$

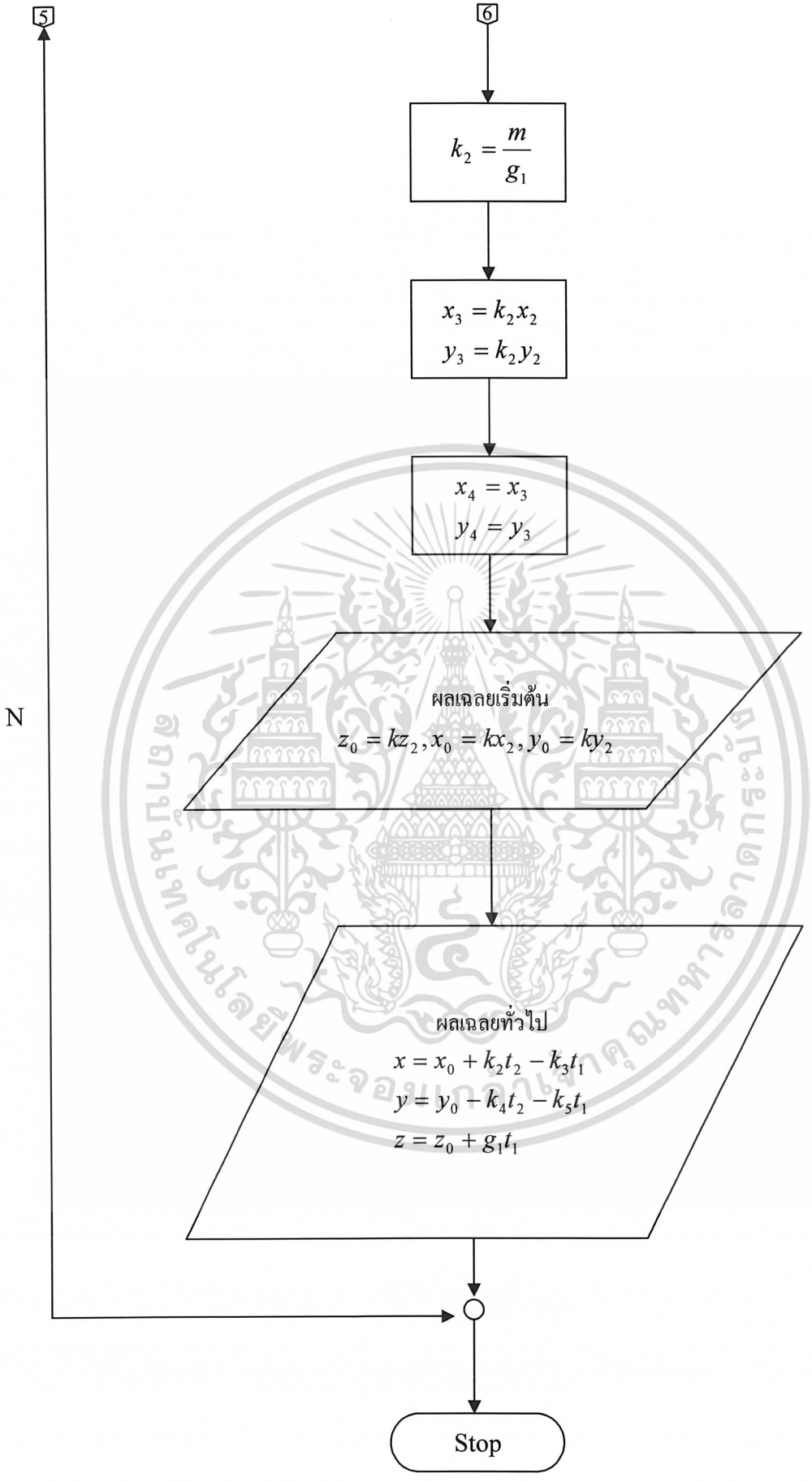
$$Z = z0 + g1t1$$

แผนผังแสดงการทำงานของโปรแกรมไดโอแฟนไทน์ 3 ตัวแปร









ตัวอย่างโจทย์ที่แก้ตามขั้นตอนวิธีการแก้สมการไดโอแฟนไทน์ 3 ตัวแปร

ตัวอย่าง การแก้สมการไดโอแฟนไทน์ 3 ตัวแปร ตามอัลกอริทึมที่สร้างขึ้น

1. $3x-6y+2z=11$ เนื่องจาก $(3,-6,2)=1$ และ $1|11$

จะหาคำตอบของสมการ

$3x-6y+2z=1$ แทน $3x-6y=1-2z$

จะมีคำตอบเมื่อ $(3,-6)=3/(1-2z)$

นั่นคือมีจำนวนเต็ม k ซึ่ง $3k=1-2z$ หรือ $2z+3k=1$

$3>2$ (สัมประสิทธิ์ x น้อยกว่า y)

$\therefore a=3,b=2$

1). $x=1,g=3,v=0,w=2$

2). $w\neq 0$

3). $3 Div 2=1,3=2(1)+1,g=2$

4). $s=1$

5). $(x,y)=(0,2)$

6). $(v,w)=(1,1)$

2). $w\neq 0$

3). $2 Div 1=2,2=1(2)+0,g=1$

4). $s=0-(2)(1)=-2$

5). $(x,y)=(1,1)$

6). $(v,w)=(-2,0)$

2). $w=0$ แล้ว set $y=1-(3)(1)=-1$

$\therefore x=1,y=-1$

แต่สัมประสิทธิ์หน้า x น้อยกว่า y $\therefore$ สลับค่า x,y

จะได้ $x_0=-1,y_0=1$ (สัมประสิทธิ์หน้าตัวแปรเป็นบวกหมดไม่ต้องคูณ (-1))

จะได้ $z_0=-1,z_1=-1+3t_1$ นำค่า $z_0=-1$ ไปแทนในสมการ (2)

$3x-6y+2(-1)=1$

$3x-6y=3$ ----------(3)

ซึ่งสมการ (3) จะมีคำตอบเมื่อ $(3,-6)=3/3$

จะเห็นว่า $|3|<|-6|$

ให้ $a=6,b=3$

1). Set $x=1,g=6,v=0,w=3$

2). $w\neq 0$

3). $6 Div 3=2,6=3(2)+0,g=3$

4). $s=1$

5). $(x,y)=(0,3)$

6). $(v,w)=(1,0)$

2). $w=0$ แล้ว set $y=\dfrac{3-6(0)}{3}=1$

$\therefore x=0,y=1$

แต่ $|3|<|-6|$

$\therefore x_0=1,y_0=0$ แต่สัมประสิทธิ์หน้า y เป็นลบ

$y_0=0(-1)=0$ เอา c คูณตลอด $(c=11)$

$\therefore x_0=11,y_0=0,z=-11$

คำตอบทั่วไป $x=1+(\dfrac{-6}{3})t_2-(-1)(2)t_1=1-2t_2-2t_1$

$y=0-\dfrac{3}{3}(t_2-(0)(2)t_1=-t_2)$

และ $z=-1+3t_1$

ตรวจคำตอบโดยแทนในสมการ (2) $3x-6y+2z=1$

$$3(1-2t_2-2t_1)-6(-t_2)+2(-1-3t_1)=3-6t_2-6t_1+6t_2-2+6t_1=1$$

คำตอบทั่วไปจริงๆ ให้เอา $\frac{c}{g}$ คูณตลอด นั่นคือ เอา $\frac{11}{1}$ คูณตลอด

$$\left.\begin{aligned} x &= 11-2t_2-2t_1 \\ y &= -t_2 \\ z &= -11+3t_1 \end{aligned}\right\} \qquad t_1, t_2 \in \mathrm{I}$$

โปรแกรมสมการไดโอแฟนไทน์ 3 ตัวแปร $ax + by + cz = n$

```
#include "stdio.h"
#include "conio.h"
#include "stdlib.h"
#include "math.h"
int Gcd(int a0,int b0);
int LinearI(int a,int b);
int LinearII(int a,int b);

int Gcd(int a0,int b0)              // ฟังก์ชันการหาตัวหารร่วมมาก
{
        int a,b,r1,temp1,q;
        a=a0;    b=b0;
        if(a-b<0)
        {
            temp1=a; a=b; b=temp1;
        }
        do
        {
                q=a/b;
                r1=a-b*q;        a=b;     b=r1;
         }while(r1!=0);

         return a;
 }

 int LinearI(int a,int b)           //ฟังก์ชันการหาค่า x1
 {
```

```
        int x,g,v,w,q,t,s;
        x=1;    g=a;    v=0;    w=b;
        do{
        q=g/w;
        t=g-q*w;        g=w;
        s=x-(q*v);
        x=v;
        v=s;    w=t;
        }while(w!=0);

        return(x);
}

LinearII(int a5,int b5)         // ฟังก์ชันการหาค่า y1
{
        int x,g,v,w,q,t,s; int y;
        x=1;    g=a5;   v=0;    w=b5;
        do
        {
                t=g%w; q=g/w; g=w;
                s=x-(q*v);
                x=v;    y=w;
                v=s;    w=t;
          }while(w!=0);

          y=(g-(a5*x))/b5;
          return(y);
 }
```

```
void main()
{
        int a,b,c,n,a1,b1,c1,g,g1,Test,c2,g2,x1,y1,x2,y2,a3,b3,x3,y3,temp2;
        int k1,k,x0,y0,z0,k2,k3,k4,k5,t1,t2,temp,x,y,z,y4,x4,n1,a2,b2,c3,m;
        char ans;
 clrscr();
         printf("\n This is the program for solving Linear Diophantine ax+by+cz=n");
        //      แสดงข้อความว่า นี่คือโปรแกรมสำหรับหาผลเฉลยของสมการไดโอแฟนไทน์
                ax + by + cz = n
         printf("\n Enter coefficient of x:");
         scanf("%d",&a);
        //      รับค่า a ซึ่งเป็นสัมประสิทธิ์ของค่า x
         printf("\n Enter coefficient of y:");
         scanf("%d",&b);
        //      รับค่า b ซึ่งเป็นสัมประสิทธิ์ของค่า y
         printf("\n Enter coefficient of z:");
         scanf("%d",&c);
        //      รับค่า c ซึ่งเป็นสัมประสิทธิ์ของค่า z
         printf("\n Enter constant n:");
         scanf("%d",&n);
        //      รับค่า n ซึ่งเป็นค่าคงที่ของสมการ
         if ((a==0)||(b==0)||(c==0)||(n==0))       //ตรวจสอบว่ามีค่าใดเป็นศูนย์หรือไม่
         {
                printf("\n This is not Linear Diophantine Equation of 3 variables");
        //      ไม่ใช่สมการไดโอแฟนไทน์เชิงเส้น 3 ตัวแปร
         }

        //ทำสัมประสิทธิ์ทุกตัวให้มีค่าเป็นบวกโดยการใส่ค่าสัมบูรณ์
         a1=fabs(a);     b1= fabs(b);     c1=fabs(c);
```

```
//เข้าฟังก์ชันการหาตัวหารร่วมมาก
 g1=Gcd(a1,b1);          g=Gcd(g1,c1);
printf("\n gcd=%d",g);
//แสดงค่าตัวหารร่วมมากของสมการ
 Test=n%g;
 a2=a1;          b2=b1;          g2=g1;  c2=c1;


if(Test!=0)
        printf("\n This equation has no solution!");
else
{
        if(c2-g2<0)
        {
                temp=c2; c2=g2; g2=temp;
        }
                printf("\n somsoy %d,%d",c2,g2);

                 x1=LinearI(c2,g2);
                //เข้าฟังก์ชันการหาค่า x1
                 y1=LinearII(c2,g2);
                 x2=x1; y2=y1;
                //เข้าฟังก์ชันการหาค่า x1
                if(c<g1)
                {
                temp2=x2; x2=y2; y2=temp2;
                }
                if(c<0)
                 {
```

```
            x2=-1*x2;
}
            z0=x2;

m=1-(c*z0);
a3=a1;  b3=b1;

if(a3-b3<0)
{
            temp=a3; a3=b3; b3=temp;
}

x2=LinearI(a3,b3);          y2=LinearII(a3,b3);

x3=x2;  y3=y2;
// ถ้า  a1 มีค่าน้อยกว่าค่า b1 ให้สลับค่า x กับ y
if(a1-b1<0)
{
            temp=x3; x3=y3; y3=temp;
}
if(a<0)          //          ถ้าค่า a ติดลบ  ต้องนำ -1 มาคูณค่า x3
{
            x3=-1*x3;
}
if(b<0)          //          ถ้าค่า b ติดลบ  ต้องนำ -1 มาคูณค่า y3
{
            y3=-1*y3;
}
             x4=x3; y4=y3;
```

```
k1=m/g1;        x3=k1*x3;        y3=k1*y3;
k=n/g;
z0=k*z0;        x0=k*x3;         y0=k*y3;

printf("\n The initial solutions of %dx+%dy+%dz=%d:",a,b,c,n);
// แสดงค่าผลเฉลยเริ่มต้นของสมการ ax + by + cz = n
printf("\n x0=%d",x0);
// แสดงค่า x0
printf("\n y0=%d",y0);
// แสดงค่า y0
printf("\n z0=%d",z0);
// แสดงค่า z0
 k2=b/g1;        k3=x4*c;        k4=a/g1;        k5=y4*c;
printf("\n The general solutions of %dx+%dy+%dz=%d:",a,b,c,n);
// แสดงผลเฉลยในรูปทั่วไปของ ax + by + cz = n
printf("\n x=%d+(%d)t2-(%d)t1,t1,t2 be integers",x0,k2,k3);
//  แสดงค่า x= x0 + k2*t2 – k3*t1
printf("\n y=%d-(%d)t2-(%d)t1,t1,t2 be integers",y0,k4,k5);
// แสดงค่า y= y0 – k4*t2 – k5*t1
printf("\n z=%d+(%d)t1,t1 be integers",z0,g1);
// แสดงค่า z= z0 + g1*
}

printf("\n This will show you some answers from difference values of t1,t2");
//        แสดงค่าผลเฉลยที่มีค่าแปรผันตามค่า t1 และ t2
printf("\n t1     t2                x=%d+(%d)t2-(%d)t1          y=%d-(%d)t2-(%d)t1
z=%d+(%d)t1",x0,k2,k3,y0,k4,k5,z0,g1);

for(t1=-5;t1<=5;t1++)
```

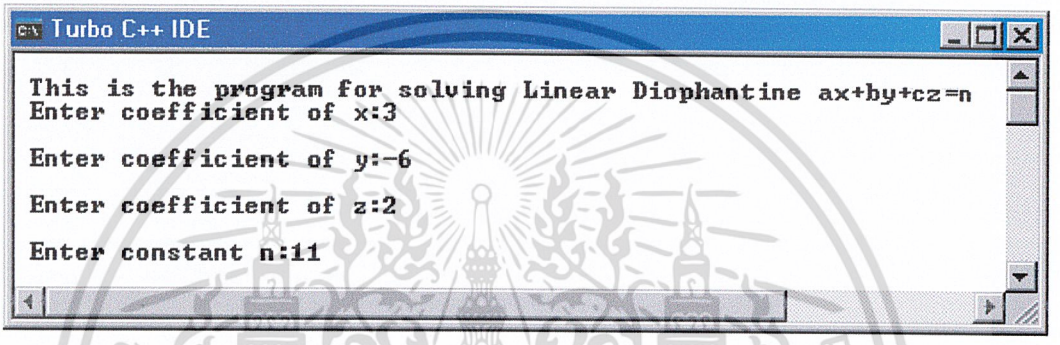
```
        {
                for(t2=-5;t2<=5;t2++)
                {
                        x=x0+(k2*t2)-(k3*t1);          y=y0-(k4*t2)-(k5*t1);
                        z=z0+(g1*t1);
                        printf("\n %d          %d          %d          %d
        %d",t1,t2,x,y,z);
                        getch();
                }
        }
}
  getch();
  return 0;

 }
```

ตัวอย่างแสดงผลการใช้งานโปรแกรมไดโอแฟนไทน์เชิงเส้น 3 ตัวแปร

ในกรณีที่โจทย์ปัญหามาในรูปปกติ คือเป็นไดโอแฟนไทน์ 3 ตัวแปร โดยทั่วไปจะได้ดัง

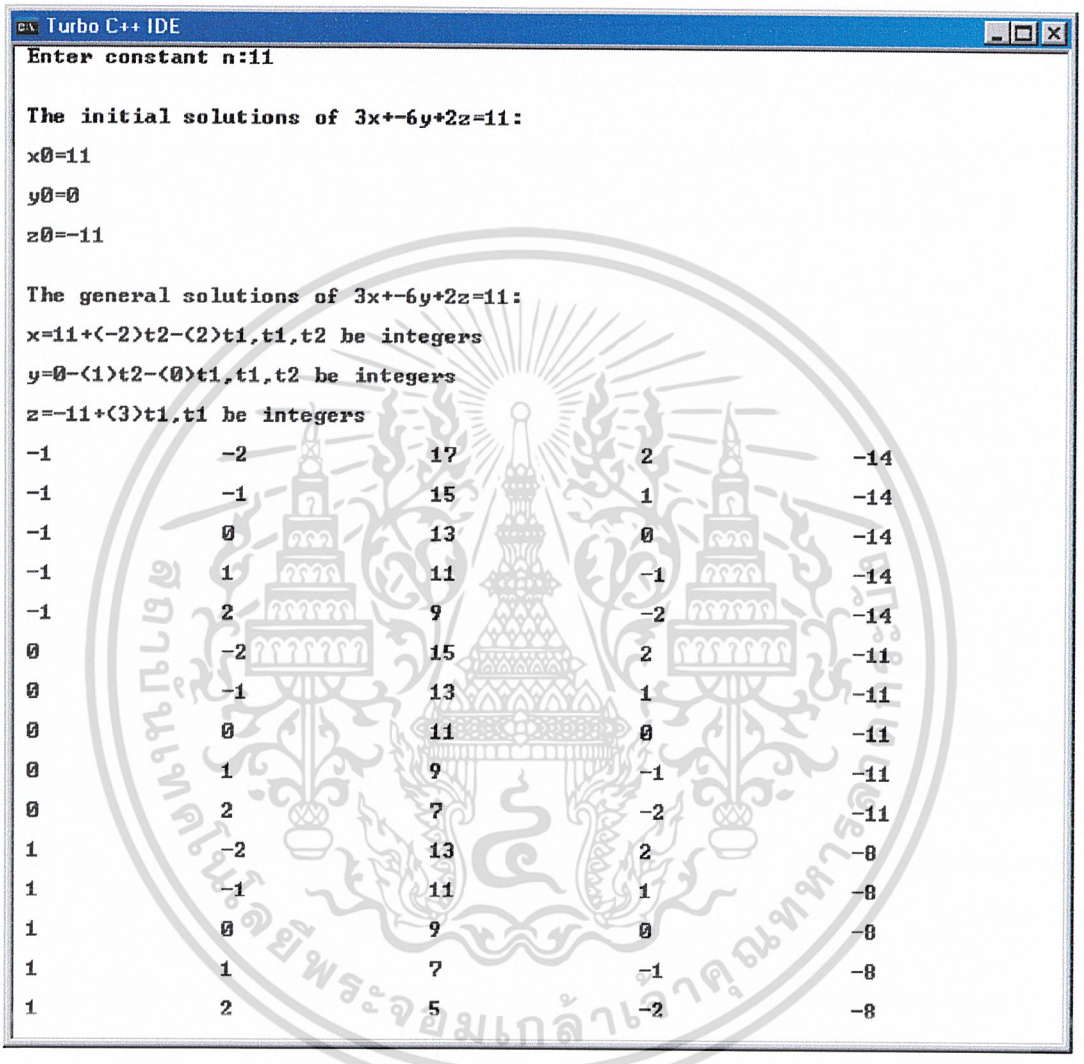
ตัวอย่าง $3x-6y+2z=11$

จะได้หน้าจอแสดงผลดังนี้



รูปที่ 3.25 แสดงการป้อนค่าคงที่ที่ต้องการหาค่า

จะได้ค่าออกมาดังที่ปรากฏ เมื่อป้อนข้อมูลเสร็จแล้วจึงกด Enter เพื่อทำการรันโปรแกรม ก็จะได้ผลออกมาดังนี้



รูปที่ 3.26 แสดงค่าคำตอบที่ต้องการออกมา

บทที่ 4
ข้อสรุปและข้อเสนอแนะ

4.1. ข้อสรุป

สมการไดโอแฟนไทน์เชิงเส้นเป็นสมการเชิงเส้นที่มีหลายตัวแปรในสมการเดียว และมีผลเฉลยของสมการเป็นจำนวนเต็ม ในการหาผลเฉลยด้วยวิธีตรงนี้ค่อนข้างยุ่งยาก จึงได้คิดโปรแกรมที่ช่วยในการหาผลเฉลยของสมการไดโอแฟนไทน์ โดยมีขอบเขตอยู่ที่ 2 ตัวแปรและ 3 ตัวแปร ถึงแม้โปรแกรมที่ได้อาจไม่ใช่โปรแกรมที่ช่วยอำนวยความสะดวกต่อผู้ใช้ในการใช้งานก็ตาม แต่ในการทำปัญหาพิเศษนี้ก็ได้ฝึกให้คณะผู้จัดทำ รู้จักคิดแบบนักวิทยาศาสตร์อย่างแท้จริง รู้จักนำความรู้พื้นฐานทางคณิตศาสตร์ไปประยุกต์ใช้ในการแก้ปัญหาต่างๆ จนสามารถแก้ปัญหาลุล่วงได้ด้วยดี

4.2. ข้อเสนอแนะ

1. สำหรับผู้ที่สนใจในสมการไดโอแฟนไทน์เชิงเส้น ท่านสามารถนำแนวคิดพื้นฐานนี้ไปใช้ในการคิดขั้นตอนวิธีในการแก้ปัญหาในกรณีทั่วไปต่อไป
2. ในการเขียนโปรแกรมอาจมีข้อจำกัดบางประการ เช่น
   2.1 ข้อจำกัดทางภาษา เช่น ฟังก์ชันในภาษา c สามารถค้นค่าได้เพียงค่าเดียวในหนึ่งฟังก์ชัน ซึ่งได้กล่าวถึงวิธีแก้ปัญหาไว้แล้วในเรื่องฟังก์ชัน Linear
   2.2 ข้อจำกัดของเครื่องคอมพิวเตอร์ กล่าวคือ ไม่สามารถรับค่าจำนวนเต็มได้เกิน 32767 ถ้าเกินจะทำให้ค่าที่คำนวณได้ผิดพลาด
   2.3 ทางคณะผู้จัดทำได้จัดทำปัญหาพิเศษนี้ขึ้นในขอบเขตของการแก้สมการไดโอแฟนไทน์เชิงเส้นโดยค่าที่ใช้จะเป็นจำนวนเต็มบวกเท่านั้น ถ้าผู้ใดสนใจจะนำปัญหาพิเศษนี้ไปพัฒนาให้สามารถใช้ครอบคลุมจำนวนเต็มทั้งหมดได้ กลุ่มข้าพเจ้าก็จะยินดีเป็นอย่างยิ่ง

บรรณานุกรม

ผศ. ดร. พัฒนี อุดมกะวานิช. 2545. ทฤษฎีจำนวนเบื้องต้น. สมาคมวิทยาศาสตร์แห่งประเทศไทย ในพระบรมราชูปถัมภ์, กรุงเทพฯ.

ผศ. ดร. สมวงษ์ แปลงประสพโชค. 2545. ทฤษฎีจำนวน Theory of Number. สถาบันราชภัฏพระนคร, กรุงเทพฯ.

รศ. ดร. สมใจ จิตพิทักษ์. 2545. ทฤษฎีจำนวน (พิมพ์ปรับปรุงครั้งที่ 2). ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยทักษิณ, สงขลา.

Bernett, I. A. Elements of number theory. OHIO UNIVERSITY.

Silverman, Joseph H. A friendly introduction to number theory. 2nd ed. United States of America : Frentice Hall, 2001.