แผนบริหารการสอนประจำบทที่ 3

หัวข้อเนื้อหาประจำบท

3.1 ความนำ

3.2 ขั้นตอนวิธี

- 3.2.1 ขั้นตอนวิธีที่ดี
- 3.2.2 ขั้นตอนวิธีการค้นหา

3.3 ความซับซ้อนของขั้นตอนวิธี

- 3.3.1 ความซับซ้อนเชิงเวลา
- 3.3.2 ความซับซ้อนเชิงพื้นที่ว่าง

3.4 เลขจำนวนเต็มและการหาร

- 3.4.1 วิธีการหาร
- 3.4.2 ขั้นตอนวิธีการหาร
- 3.4.3 หารร่วมมากและคูณร่วมน้อย
- 3.4.4 เลขคณิตว่าด้วยการหารเอาเศษ
- 3.4.5 การประยุกต์ใช้สมภาค

3.5 เลขจำนวนเต็มและขั้นตอนวิธี

- 3.5.1 ขั้นตอนวิธีของยูคลิด
- 3.5.2 การแทนกันของเลขจำนวนเต็ม
- 3.5.3 ขั้นตอนวิธีสำหรับตัวดำเนินการของเลขจำนวนเต็ม

3.6 การประยุกต์ของทฤษฎีจำนวน

3.6.1 สมภาคเชิงเส้น

3.6.2 ทฤษฎีบทเศษเหลือของจีน

3.6.3 เลขคณิตคอมพิวเตอร์กับเลขจำนวนเต็มขนาดใหญ่

3.6.4 เลขจำนวนเฉพาะเทียม

3.6.5 การเข้ารหัสลับกับกุญแจสาธารณะ

วัตถุประสงค์เชิงพฤติกรรม

1. เพื่อให้ผู้ศึกษาสามารถเขียนขั้นตอนวิธีที่ดี และประยุกต์ไปสู่ขั้นตอนวิธีการค้นหาได้
2. เพื่อให้ผู้ศึกษาสามารถหาความซับซ้อนของขั้นตอนวิธี
3. เพื่อให้ผู้ศึกษาเกิดความเข้าใจเกี่ยวกับเลขจำนวนเต็มและขั้นตอนวิธีการหาร
4. เพื่อให้ผู้ศึกษาเรียนรู้การประยุกต์ของทฤษฎีจำนวน
5. เพื่อให้ผู้ศึกษาสามารถเข้าใจเกี่ยวกับการเข้ารหัสลับกับกุญแจสาธารณะ

วิธีสอนและกิจกรรม

1. แบบบรรยายและสาธิตศึกษาจากเอกสารประกอบการสอน
2. ค้นคว้าเพิ่มเติมจากแหล่งทรัพยากรอื่น
3. ตอบคำถามท้ายบทและโต้ตอบระหว่างเรียน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. เครื่องคอมพิวเตอร์
3. สื่อการสอนอิเล็กทรอนิกส์ ได้แก่ โปรแกรมนำเสนอเนื้อหาวิชา
4. เว็ปเพจอ้างอิงความรู้ ได้แก่ http://noppanun.lpru.ac.th

การวัดและประเมินผล

1. สังเกตการร่วมกิจกรรมการเรียนการสอน
2. สังเกตการซักถามคำถามและการตอบคำถาม
3. สังเกตการฝึกปฏิบัติจากแบบฝึกหัดท้ายบท

บทที่ 3
ขั้นตอนวิธีและเลขจำนวนเต็ม

3.1 ความนำ

ในการแก้ปัญหาต่าง ๆ โดยเฉพาะโปรแกรมบนคอมพิวเตอร์นั้น จะต้องสร้างแบบจำลอง ที่จะแปลงปัญหาไปเป็นแบบจำลองทางคณิตศาสตร์ เนื่องจากคณิตศาสตร์เป็นศาสตร์ที่พิสูจน์ความถูกต้องได้ การเขียนโปรแกรมภาษาคอมพิวเตอร์ที่ดีต้องมีการออกแบบ และอธิบายขั้นตอนการทำงานก่อนที่จะลงเมือเขียน เสมือนการสร้างบ้านต้องมีแบบบ้านที่ดีและถูกต้องตรงตามความต้องการ ขั้นตอนวิธีเป็นแบบจำลองชนิดหนึ่งที่สามารถอธิบายได้ว่ามีการทำงานอย่างมีลำดับอะไรบ้าง ส่วนเลขจำนวนเต็มส่วนหนึ่งของดิสครีตประกอบด้วยเลขจำนวนเต็มและคุณสมบัติ ซึ่งเป็นส่วนหนึ่งของสาขาทางคณิตศาสตร์ที่เรียกว่า ทฤษฎีจำนวน โดยมีหลักการพื้นฐาน 3 ส่วน คือ การหาร การหารร่วมมากและคูณร่วมน้อย และเลขคณิตว่าด้วยการหารเอาเศษ สามารถนำไประยุกต์ในงานคอมพิวเตอร์ได้หลายสาขา อาทิ การจัดการกับเลขขนาดใหญ่ การตรวจสอบข้อมูลที่ได้รับมาว่าถูกต้องหรือไม่ และการเข้ารหัสข้อมูล เป็นต้น

3.2 ขั้นตอนวิธี

การอธิบายขั้นตอนวิธีด้วยประโยคธรรมดานั้นก็เข้าใจง่าย แต่ไม่เหมาะที่จะนำไปใช้งานบนคอมพิวเตอร์ สิ่งที่จะเหมาะก็คือการใช้ภาษาทางคอมพิวเตอร์ในการอธิบาย แต่ภาษาทางคอมพิวเตอร์มีข้อจำกัดมาก เช่น คำสั่งต่าง ๆ จะสามารถใช้ได้กับภาษาทางคอมพิวเตอร์นั้น ๆ ซึ่งทำให้ยากในการเข้าใจ ดังตัวอย่างที่ 3.1 ภาษาทางคอมพิวเตอร์ยังมีมากมายหลายแบบไม่เหมือนกัน ดังนั้นการใช้คำสั่งเทียม (pseudocode) จะเป็นสิ่งที่อยู่ตรงกลางระหว่างภาษาธรรมชาติ กับ ภาษาทาง

คอมพิวเตอร์ ทำให้สามารถจะเข้าใจได้ง่าย นำไปใช้งานกับภาษาทางคอมพิวเตอร์ หรือคอมพิวเตอร์ชนิดใดก็ได้ ดังตัวอย่างที่ 3.2

นิยามที่ 3.1 ขั้นตอนวิธี (algorithm) คือกระบวนการที่แน่นอน ชัดเจน สำหรับแก้ปัญหา โดยจำนวนขั้นตอนต่าง ๆ ที่ใช้นั้นมีอย่างจำกัด

ตัวอย่างที่ 3.1 จงอธิบาย ขั้นตอนวิธี ที่จะใช้ในการหาค่าเลขจำนวนเต็มที่ใหญ่ที่สุด จากลำดับที่จำกัดของเลขจำนวนเต็ม

วิธีทำ ขั้นตอนวิธีอาจจะอธิบาย ด้วยประโยคธรรมดาดังต่อไปนี้

1. กำหนดค่า max เท่ากับเลขจำนวนเต็มตัวแรกลำดับ
2. เปรียบเทียบกับเลขจำนวนเต็มตัวถัดไป ถ้าเลขจำนวนเต็มตัวถัดไปใหญ่กว่า ให้กำหนดค่า max เท่ากับเลขจำนวนเต็มตัวนั้น
3. ทำซ้ำขั้นตอนที่ 2 ถ้ายังมีเลขจำนวนเต็มเหลืออยู่ในลำดับ
4. หยุดการทำงาน เมื่อ ไม่มีเลขจำนวนเต็มเหลืออยู่ในลำดับ และ max ก็จะเป็นเลขจำนวนเต็มที่ใหญ่ที่สุดในลำดับนั้น ▌

ตัวอย่างที่ 3.2 จงเขียนคำสั่งเทียมในการหาค่าสูงสุดของสมาชิกในลำดับ

วิธีทำ

procedure max $(a_1,a_2,\ldots,a_n$: int)

max = a_1

for i = 2 to n

if max < a_i then max = a_i

{max จะเก็บค่าของสมาชิกที่มากที่สุด} ▌

3.2.1 ขั้นตอนวิธีที่ดี

ขั้นตอนวิธีที่ดีต้องมีคุณสมบัติโดยทั่ว ๆ ไปดังนี้

3.1.1.1 การรับเข้า (input) มีเซตของการรับเข้าที่กำหนดแน่นอน

3.1.1.2 ผลลัพธ์ (output) แต่ละเซตของการรับเข้าจะสร้างผลลัพธ์ซึ่งเป็นคำตอบ

3.1.1.3 มีการกำหนดการประมวลผลที่แน่นอนและถูกต้อง

3.1.1.4 มีขั้นตอนคงที่สำหรับแต่ละเซตของการรับเข้า และแต่ละขั้นตอนจะใช้เวลาตามที่กำหนด

3.1.1.5 ใช้แก้ปัญหากับเซตของการรับเข้าอื่น ๆ ได้ ไม่ใช่ เฉพาะเซตของการรับเข้าเซตใดเซตหนึ่งเท่านั้น

3.2.2 ขั้นตอนวิธีการค้นหา

การค้นหาสมาชิกในลำดับมีหลายแบบ อาทิ การค้นหาคำศัพท์ในพจนานุกรม ซึ่งต้องมีการเรียงคำศัพท์ต่าง ๆ ไว้เป็นลำดับก่อนตามดัชนี ซึ่งโดยมากดัชนีที่ใช้เรียงตามตัวอักษร ปัญหาการค้นหาว่าจะพบสิ่งที่ต้องการค้นหรือไม่เรียกว่า ปัญหาของการค้นหา (searching problems) โดยทั่ว ๆ ไป ใช้หลักของการค้นทุก ๆ สมาชิก อาทิ หารค้นหา x ในลำดับของ $a_1,a_2,\ldots,a_n$ ผลลัพธ์ของการค้นหาจะเป็นตำแหน่งของพจน์ที่อยู่ในลำดับ i ซึ่ง $a_i = x$ (ถ้า x ไม่อยู่ในลำดับจะทำให้ค้นไม่พบ) วิธีการค้นหามีดังต่อไปนี้

3.2.2.1 การค้นหาเชิงเส้น (linear search) หรือการค้นหาแบบลำดับ (sequential search) เป็นการค้นหา x ในลำดับโดยเริ่มค้นตั้งแต่ลำดับที่มีตำแหน่งต่ำที่สุด i=1 เทียบค่ากับ x ทีละสมาชิกในตำแหน่ง ถ้า $x = a_i$ ณ ตำแหน่ง i ใด ๆ ถือว่าพบข้อมูล การค้นหาเชิงเส้นสามารถเขียนเป็นขั้นตอนวิธีได้ดังนี้

Procedure linear search (x : int; $a_1, a_2, \ldots a_n$: distinct integer)

While ($i \leq n$ and $x \neq a_i$)

$i := i+1$

If $i \leq n$ then location = I

Else location = 0

{ตำแหน่งของพจน์ i ที่มีค่า = x , หรือ 0 ถ้าหา x ไม่พบ }

3.2.2.2 การค้นหาแบบทวิภาค (binary search) จะใช้ได้ถ้ามีการเรียงลำดับของพจน์ต่าง ๆ ที่อยู่ในเซต ไม่ว่าจะเรียงลำดับจากมากไปน้อย หรือเรียงจากน้อยไปมาก หรือเรียงตามตัวอักษร วิธีการคือ

1. เปรียบเทียบ x กับตัวที่อยู่ลำดับตรงกลาง
2. ถ้ายังไม่พบจะแบ่งเซตออกเป็น 2 ส่วน
3. ถ้า x > ตัวที่อยู่ตรงกลางทำต่อกับส่วนที่อยู่ด้านกลางถึงปลาย
4. ถ้า x < ตัวที่อยู่ตรงกลางทำต่อกับส่วนที่อยู่ต้นถึงกลางทาง

ตัวอย่างที่ 3.3 จงเขียนขั้นตอนวิธีและคำสั่งเทียมในการค้นหาแบบทวิภาคของเลข 19 ในลำดับ

1 2 3 4 5 6 7 8 10 12 13 15 16 18 19 20 22

วิธีทำ ขั้นตอนวิธี

1. เปรียบเทียบ 19 กับตัวที่ 9 ซึ่งมีค่า = 10

   $19 \neq 10$ และ 19 > 10

   $\therefore$ 19 จะต้องอยู่ในครึ่งขวาของลำดับในเซต
2. เปรียบเทียบ 19 กับตัวที่ 13 ซึ่งมีค่า = 16

   19 > 16

   $\therefore$ จะต้องอยู่ในครึ่งขวาในลักษณะเดิม

3. เปรียบเทียบ 19 กับตัวที่ 15 ซึ่งมีค่า = 19

∴ ตำแหน่งคือ 15 ▌

<u>แนวคิด</u> คำสั่งเทียม

Procedure binary search (x : int ; a_1 , a_2 ,…a_n: increasing integer)

i := 1 { i เป็นสมาชิกด้านซ้ายสุดของลำดับ }

j := n { j เป็นสมาชิกด้านขวาสุดของลำดับ }

while i < j

begin

$m := \lfloor (i + j) / 2 \rfloor$

if $x > a_m$ then i:=m+1

else j := m

end

if $x = a_i$ then location := i

else location :=0 ▌

3.3 ความซับซ้อนของขั้นตอนวิธี

การวิเคราะห์ประสิทธิภาพของขั้นตอนวิธี จะเกี่ยวข้องกับการคณนาที่ซับซ้อน (computational complexity) ของขั้นตอนวิธี ซึ่งจะมีรูปแบบของความซับซ้อนอยู่ 2 รูปแบบคือ

3.3.1 ความซับซ้อนเชิงเวลา

ความซับซ้อนเชิงเวลา (time complexity) จะเกี่ยวข้องกับ จำนวนตัวดำเนินการที่ใช้ในขั้นตอนวิธี นั้น ๆ เช่น การเปรียบเทียบเลขจำนวนเต็ม การบวกเลขจำนวนเต็ม การคูณเลขจำนวนเต็ม การหารเลขจำนวนเต็ม หรือตัวดำเนินการพื้นฐานอื่น ๆ เป็นต้น

3.3.2 ความซับซ้อนเชิงพื้นที่ว่าง

ความซับซ้อนเชิงพื้นที่ (space complexity) จะเกี่ยวข้องกับโครงสร้างข้อมูล (data structure) ที่ใช้ในการใช้งาน ขั้นตอนวิธีนั้นจะเป็นการวิเคราะห์ พื้นที่ของหน่วยความจำ (memory space) ว่าจะใช้มากน้อยเพียงไร ความซับซ้อนเชิงพื้นที่ไม่พิจารณาในที่นี้เพราะอยู่นอกเนื้อหาของรายวิชานี้

ตัวอย่างที่ 3.4 จงพิจารณาความซับซ้อนเชิงเวลาในการหาค่าสูงสุด (max) ในเซต

วิธีทำ สมมติในเซต มี n สมาชิก และไม่ได้จัดเรียงลำดับ การหา max จะใช้วิธีกำหนดตัวแรกแล้วเปรียบเทียบกับตัวถัดไปในลำดับจนกว่าจะหมด ในแต่ละการทำงานซ้ำ ๆ จะมีการใช้การเปรียบเทียบ 2 ประการคือ

1. ใช้เปรียบเทียบเพื่อตรวจการสิ้นสุดการทำงาน
2. ใช้เปรียบเทียบเพื่อปรับปรุงค่า max

$\therefore$ จะมีการเปรียบเทียบทั้งหมด = 2(n-1) ครั้ง รวมกับการเปรียบเทียบเพื่อออกจากการวนซ้ำ (loop) ครั้งสุดท้ายในการนั่นคือจะมีทั้งหมด =2(n-1)+1 เทียบกับ 2(n-1)

$\therefore$ ความซับซ้อนเชิงเวลา O(n) ▌

ตัวอย่างที่ 3.5 จงพิจารณาความซับซ้อนเชิงเวลาของการค้นหาเชิงเส้นที่แต่ละขั้น

วิธีทำ ในการค้นหา จะมีการเปรียบเทียบ 2 ส่วน

1. เพื่อตรวจสอบข้อมูลสุดท้ายหรือไม่
2. เพื่อเปรียบเทียบสมาชิกว่าใช่ค่าที่ค้นหรือไม่

สุดท้าย จะมีอีก 1 การเปรียบเทียบ คือเงื่อนไขการออกจากการวนซ้ำ และอีก 1 การเปรียบเทียบ เพื่อดูว่าการค้นหาพบหรือไม่

$\therefore$ จะมีการเปรียบเทียบ อย่างมากที่สุด 2n+2

$\therefore$ ความซับซ้อนเชิงเวลา คือ O(n) ▌

ตัวอย่างที่ 3.6 พิจารณาความซับซ้อนเชิงเวลาของการค้นหาแบบทวิภาค

วิธีทำ เพื่อความสะดวกจะให้ $n = 2^k$ หรือ $k = \lfloor \log_2 n \rfloor$ ในแต่ละการทำงานซ้ำ ๆ ของ การค้นหาแบบทวิภาค จะใช้การเปรียบเทียบออกเป็น 2 ส่วน คือส่วนที่อยู่ฝั่งซ้ายของค่ากลางและส่วนที่อยู่ด้านขวาของค่ากลาง โดยมีรูปแบบขั้นตอนการทำงานดังนี้

1. ตรวจสอบค่าว่าอยู่ฝั่งซ้ายหรือขวาในลำดับ
2. เพื่อเปรียบเทียบค่ากับสมาชิกที่อยู่ในตำแหน่งที่อ้างอิง
3. จำนวนการทำซ้ำ ๆ ทั้งหมด ที่ต้องทำ = k

$\therefore$ จะมีการเปรียบเทียบ = $2k+2 = 2\log_2 n+2$

$\therefore$ ความซับซ้อนเชิงเวลาของการค้นหาแบบทวิภาค คือ $O(\log_2 n)$

ถ้า $n = 2^k$ จำนวนการวนซ้ำจะมีอย่างมากไม่เกิน $k+1$

$\therefore$ จำนวนการเปรียบเทียบ $=2\log n+4$

$\therefore$ ความซับซ้อนเชิงเวลา = $O(\log_2 n)$ มีชื่อเรียกดังตารางที่ 3.1 ▌

ตัวอย่างที่ 3.7 พิจารณากรณีเฉลี่ยของการค้นหาเชิงเส้น ดูว่าโดยเฉลี่ยแล้วจะมีความซับซ้อนเชิงเวลาเท่าไร

วิธีทำ กรณีที่ดีที่สุด ถ้าค้น 1 ครั้ง แล้วพบใช้การเปรียบเทียบ 2+1=3 ครั้ง

ถ้าค้น 2 ครั้ง แล้วพบใช้การเปรียบเทียบ 4+1=5 ครั้ง

ถ้าค้น n ครั้ง แล้วพบใช้การเปรียบเทียบ 2n+1 ครั้ง

$\therefore$ โดยเฉลี่ย จะใช้ การเปรียบเทียบ

$$= \frac{3+5+7+\ldots+(2n+1)}{n}$$

$$= \frac{1+2+1+4+6+\ldots+n+n}{n}$$

$$= \frac{2(1+2+3+...+n)+n}{n}$$

$$= n+2$$

$$=O(n)$$ ∎

ตารางที่ 3.1 แสดงตัวอย่างความซับซ้อนของขั้นตอนวิธี

สัญลักษณ์	ชื่อเรียก
$O(1)$	Constant Complexity
$O(\log_2 n)$	Logarithmic Complexity
$O(n)$	Linear Complexity
$O(n\log_2 n)$	n log n Complexity
$O(n^b)$	Polynomial Complexity
$O(b^n)$	Exponential Complexity (where $b > 1$)
$O(n!)$	Factorial Complexity

ที่มา (Johnsonbaugh, Richard, 1984, p.28)

3.4 เลขจำนวนเต็มและการหาร

ส่วนหนึ่งของดิสครีตประกอบด้วยเลขจำนวนเต็มและคุณสมบัติ ซึ่งเป็นส่วนหนึ่งของสาขาทางคณิตศาสตร์ที่เรียกว่า ทฤษฎีจำนวน โดยมีหลักการพื้นฐาน 3 ส่วน คือ การหาร การหารร่วมมากและคูณร่วมน้อย และเลขคณิตว่าด้วยการหารเอาเศษ

3.4.1 วิธีการหาร

เมื่อเลขจำนวนเต็มหนึ่งถูกหารด้วย 2 หรือหารเลขจำนวนเต็มอื่น ๆ ที่ไม่มีค่าเป็นศูนย์แล้ว พบว่าผลลัพธ์ที่ได้อาจไม่เป็นเลขจำนวนเต็มเสมอไป ตัวอย่างเช่น 12/3 =4 เป็นเลขจำนวนเต็มจริง แต่ 11/4 = 2.75 ไม่เป็นเลขจำนวนเต็ม ดังนิยามที่ 3.2

นิยามที่ 3.2 a และ b เป็นเลขจำนวนเต็มที่ $a \neq 0$ a หาร b ลงตัวถ้ามี จำนวนเต็ม c ซึ่ง $b = ac$ จะเรียก a ว่าตัวประกอบของ b และ เรียก b ว่าพหุคูณของ a เขียนแทนด้วย $a \mid b$ ถ้า a หาร b ไม่ลงตัวแทนด้วย $a \nmid b$

ตัวอย่างที่ 3.8 จงหาว่า $3 \mid 12$ เป็นจริง

วิธีทำ เพราะ $12 = 3(4)$

$\therefore$ เป็นจริง

จงหาว่า $3 \nmid 10$ เป็นจริง

วิธีทำ เพราะ $10 = 3(C)$

$\therefore$ เป็นจริงเพราะไม่มีจำนวนเต็ม C ใดแทนลงในสมการได้

ทฤษฎีบทที่ 3.1 1. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid (b+c)$

2. ถ้า $a \mid b$ แล้ว $a \mid bc$

3. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$

นิยามที่ 3.3 เลขจำนวนเต็มบวก $p > 1$ ใด ๆ จะเรียกว่าเป็นเลขจำนวนเฉพาะ (prime) ถ้ามีเพียง 1 และ ตัวมันเอง เท่านั้นที่เป็นตัวประกอบ ถ้า p ไม่ใช่เลขจำนวนเฉพาะ p จะเป็นจำนวนประกอบ (composite number)

ทฤษฎีบทที่ 3.2 เลขจำนวนเต็มบวกทุกตัว สามารถเขียนได้เป็นผลผลิตของเลขจำนวนเฉพาะได้เพียงรูปแบบเดียว

ตัวอย่างที่ 3.9 $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$

$641 = 641$

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

$1024 = 2^{10}$ ▌

ทฤษฎีบทที่ 3.3 ถ้า n เป็นจำนวนประกอบ n จะมีตัวหารเลขจำนวนเฉพาะ ที่ $\leq \sqrt{n}$

พิสูจน์ที่ 3.3 ให้ n = ab

i<a<n และ i<b< n

$a \leq \sqrt{n}$ หรือ $b \leq \sqrt{n}$ มิฉะนั้น ab >n

$\therefore$ n จะมีตัวหารเลขจำนวนเต็มบวก ที่ $\leq \sqrt{n}$ a และ b

สามารถจะเขียนเป็นผลผลิตของเลขจำนวนเฉพาะได้

นั่นคือ n จะมีตัวหารเลขจำนวนเฉพาะ ที่ $\leq \sqrt{n}$

ตัวอย่างที่ 3.10 จงแสดงว่า 101 เป็นเลขจำนวนเฉพาะ

วิธีทำ ปกติจะต้องทดสอบ ด้วยการเอาเลขจำนวนเฉพาะที่ $<$ 101 ทั้งหมดมาหารดูแต่จากทฤษฎีบทที่ 3.3 ให้หาเลขจำนวนเฉพาะที่ไม่เกิน $\sqrt{101}$ มาหารดูก็เพียงพอที่จะบอกได้ว่า 101 เป็นเลขจำนวนเฉพาะหรือไม่ ที่ไม่เกิน $\sqrt{101}$ คือ 2,3,5,7 ซึ่งหาร101 ไม่ลงตัว

$\therefore$ 101 เป็นเลขจำนวนเฉพาะ ▌

3.4.2 ขั้นตอนวิธีการหาร

ขั้นตอนวิธีการหารโดยมากมักใช้กรณีทางหารเอาเศษ โดยมีนิยามที่น่าสนใจดังนี้

ทฤษฎีบทที่ 3.4 ให้ a เป็นเลขจำนวนเต็มและ d เป็นเลขจำนวนเต็มบวก แล้วจะมี q และ r เพียงค่าเดียว ซึ่ง a = dq + r โดยที่ $0 \leq r < d$

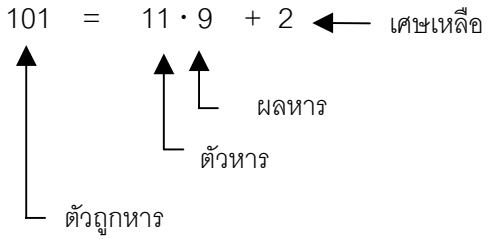
นิยามที่ 3.4 จากขั้นตอนวิธีการหาร

d จะเรียกว่า ตัวหาร (divisor) a จะเรียกว่า ตัวถูกหาร (dividend)

q จะเรียกว่า ผลหาร (quotient) r จะเรียกว่า เศษเหลือ (remainder)

ตัวอย่างที่ 3.11 จงบอกค่าของ a,d,q และ r จากขั้นตอนวิธีการหาร ของ 101 หาร 11

วิธีทำ



▌

ตัวอย่างที่ 3.12 จงหาผลหารและเศษเหลือ เมื่อ -11 ถูกหารด้วย 3

วิธีทำ $-11 = 3(-4) + 1$

$\therefore$ ผลหาร $= -4$

เศษเหลือ $= 1$

สังเกต $-11 = 3(-3) - 2$

แต่ $r = -2$ ไม่สอดคล้องกับ $0 \leq r < d$ ▌

3.4.3 หารร่วมมากและคูณร่วมน้อย

นิยามที่ 3.5 ให้ a,b เป็น เลขจำนวนเต็มที่ไม่ใช่ 0 และ จำนวนเต็มที่ใหญ่ที่สุดคือ d ซึ่ง d|a และ d|b จะเรียกว่าหารร่วมมาก (Greatest Common Divisors: GCD) ของ a และ b เขียนแทนด้วย ห.ร.ม. (a,b)

ตัวอย่างที่ 3.13 ห.ร.ม. ของ 24 กับ 36

วิธีทำ ตัวหาร ของ 24 คือ 1, 2, 3, 4, 6, 8, 12,

ตัวหาร ของ 36 คือ 1, 2, 3, 4, 6, 9, 12, 18

ตัวหารร่วมที่ใหญ่ที่สุด คือ 12

$\therefore$ ห.ร.ม. (24,36) = 12 ▌

ตัวอย่างที่ 3.14 ห.ร.ม. ของ 17 และ 22 คือเท่าไร

วิธีทำ 17 และ 22 ไม่มี ตัวประกอบหารร่วมที่ > 1

$\therefore$ ห.ร.ม. (17,22) = 1 ∎

นิยามที่ 3.6 a และ b จะเป็น จำนวนเฉพาะสัมพัทธ์ (relatively prime) ถ้า ห.ร.ม. (a,b) = 1

นิยามที่ 3.7 เลขจำนวนเต็มบวก $a_1,a_2,\ldots,a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ตรงกัน (pairwise relatively prime) ถ้า หรม. $(a_i,a_j)=1$ เมื่อ $1\le i<j\le n$

ตัวอย่างที่ 3.15 10,17,21 เป็นจำนวนเฉพาะสัมพัทธ์ตรงกัน

วิธีทำ เพราะ ห.ร.ม(10,17) = 1 , ห.ร.ม.(10,21) = 1

10,19,24 ไม่เป็นจำนวนเฉพาะสัมพัทธ์ตรงกัน

เพราะ ห.ร.ม.(10,24)= 2>1 ∎

ตัวอย่างที่ 3.16 จงหา ห.ร.ม. ของ 120 และ 500

วิธีทำ $120=2^3\cdot 3\cdot 5$

$500=2^2\cdot 5^3$

$\therefore$ ห.ร.ม.(120,500) $=2^2\cdot 3^0\cdot 5^1=20$ ∎

นิยามที่ 3.8 คูณร่วมน้อย (Least Common Multipliers: LCM) ของ a และ b จะเป็นเลขจำนวนเต็มบวกที่น้อยที่สุด d ซึ่ง a|d และ b|d เขียนแทนด้วย ค.ร.น.(a,b)

$$a=p_1^{a1}\cdot p_2^{b2}\ldots..p_n^{an}$$

$$b=p_1^{b1}\cdot p_2^{b2}\ldots..p_n^{bn}$$

$$\text{ค.ร.น.}(a,b)=P_1^{\max(a_1,b_1)}\cdot P_2^{\max(a_2,b_2)}\ldots P_n^{\max(a_n,b_n)}$$

ตัวอย่างที่ 3.17 จงหา ค.ร.น. ของ $2^3 3^5 7^2$ และ $2^4 3^3$

วิธีทำ ค.ร.น.$(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)}$

$= 2^4 3^5 7^2$ ▌

ทฤษฎีบทที่ 3.5 a,b เป็นเลขจำนวนเต็มบวก จะได้ว่า ab = ห.ร.ม.(a,b) · ค.ร.น.(a,b)

ตัวอย่างที่ 3.18 ห.ร.ม.(9,24) = 3

ค.ร.น.(9,24) = 72

9·24 = 3·72

216 = 216 ▌

3.4.4 เลขคณิตว่าด้วยการหารเอาเศษ

นิยามที่ 3.9 ให้ a เป็นเลขจำนวนเต็มและ m เป็นเลขจำนวนเต็มบวก จะเขียน a mod m เป็นเศษเหลือเมื่อ a หารด้วย m หรือ r = a mod m ถ้า a = qm+r และ $0 \leq r < m$

ตัวอย่างที่ 3.19 จงหารเอาเศษกับเลขต่อไปนี้

วิธีทำ 17 mod 5 = 2

-113 mod 9 = 2

2001 mod 101 = 82 ▌

นิยามที่ 3.10 ถ้า a และ b เป็นเลขจำนวนเต็มและ m เป็นเลขจำนวนเต็มบวกแล้ว a สมภาค (congruences) กับ b มอดุโล (modulo) m ถ้า $m|(a-b)$ เขียนแทนด้วย $a \equiv b \pmod{m}$ และ a ไม่สมภาคกับ b mod m เขียนแทนด้วย $a \not\equiv b \pmod{m}$

ตัวอย่างที่ 3.20 $17 \equiv 5 \pmod 6$

วิธีทำ เพราะ $6 \mid (17-5)$ ∎

$24 \not\equiv 14 \pmod 6$

วิธีทำ เพราะ 24-14 = 10 หารด้วย 6 ไม่ลงตัว ∎

ทฤษฎีบทที่ 3.6 ถ้า m เป็นเลขจำนวนเต็มบวก $a \equiv b \pmod m$ ก็ต่อเมื่อ มีเลขจำนวนเต็ม k ซึ่ง $a = b + km$

พิสูจน์ที่ 3.6

$a \equiv b \pmod m \rightarrow m \mid (a-b)$

$\rightarrow a - b = km$

$\rightarrow a = b + km$

$a = b + km \rightarrow km = a-b$

$\rightarrow k = m \mid (a-b)$

ทฤษฎีบทที่ 3.7 ถ้า $a \equiv b \pmod m$ และ $c \equiv d \pmod m$ แล้ว $a+b \equiv b+d \pmod m$ และ $ac \equiv bd \pmod m$

พิสูจน์ที่ 3.7

$a \equiv b \pmod m \quad b = a + sm$

$c \equiv d \pmod m \quad d = c + tm$

$b + d \equiv a + c + (s+t)m$

$a + c \equiv b + d \bmod m \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots *$

$bd = ac + m(at + cs + stm)$

$ac \equiv bd \pmod m \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots *$

ตัวอย่างที่ 3.21 ถ้า $7 \equiv 2 \pmod 5$ และ $11 \equiv 1 \pmod 5$ จงหาค่าตามทฤษฎีบทที่ 3.7

วิธีทำ $18 = 7+11 \equiv 2+1 = 3 \pmod 5$

และ $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod 5$ ▌

3.4.5 การประยุกต์ใช้สมภาค

การประยุกต์ใช้สมภาค (applications of congruences) สามารถนำมาประยุกต์สำหรับการกำหนดตำแหน่งของหน่วยความจำที่จัดเก็บแฟ้มข้อมูลของคอมพิวเตอร์ การสร้างตัวเลขสุ่มเทียม และการทำระบบการเข้ารหัสข้อมูล เป็นต้น

ตัวอย่างที่ 3.22 ฟังก์ชันสับย่อย (hashing function) ที่ใช้ในการกำหนดการค้นหาระเบียนข้อมูลของหน่วยความจำ ซึ่งมีกุญแจ (key) รหัสลับเป็น k

$$h(k) = k \bmod m$$

วิธีทำ สมมุติ ให้ระเบียนข้อมูลซึ่งมีกุญแจ = 6 , 8, 17, 3, 5, 24 และมีตำแหน่งอยู่ 5 ตำแหน่ง คือ 0, 1, 2, 3, 4

$\therefore$ แต่ละระเบียนข้อมูลจะถูกกำหนดตำแหน่งเป็น 1, 3, 2, 3, 0, 4 ตามลำดับ

ปัญหาที่มักจะเกิดจากการใช้ฟังก์ชันสับย่อยคือการชนกัน (collision) ของตำแหน่งที่ถูกครอบครองด้วยระเบียนข้อมูล 2 ระเบียนขึ้นไป เกิดจากกุญแจที่แตกต่างกันถูกกำหนดไปยังระเบียนข้อมูลตำแหน่งเดียวกัน

<u>การแก้ปัญหา</u> ปัญหาของการชนกันอาจจะแก้ไขได้โดย เลื่อนตำแหน่งไปยังตำแหน่งถัดไป หรือขยายตารางสับย่อย (hash table) หรือกำหนดฟังก์ชันสับย่อยใหม่

ตัวอย่างที่ 3.23 การสร้างตัวเลขสุ่มเทียม (pseudo random number generator)

วิธีทำ วิธีที่มักจะใช้โดยทั่วไปคือวิธีการสมภาคเชิงเส้น

$x_n+1 = (ax_n+c) \bmod m$

m = ตัวหาร $\leq \geq$

a = ตัวคูณ $2 \leq a < m$

x_0 = ตัวล่อ $0 \leq x_0 < m$

c = ตัวเพิ่ม $0 \leq c < m$

เช่น เลือก m = 9, a=7, c=4 และ $x_0 = 3$

$x_n+1 \equiv (7x_n + 4) \bmod 90$

$x_1 \equiv 25 \bmod 9 = 7$

$x_2 \equiv 53 \bmod 9 = 8$

$x_3 = 6$

$x_4 = 1$

$x_5 = 2$

$x_6 = 0$

$x_7 = 4$

$x_8 = 5$

$x_9 = 3$

ค่าที่จะมักใช้ c = 0

$m = 2^{32}-1$

$a = 7^5 = 16{,}807$ จะให้คาบยาวถึง $2^{31}-2$ ▌

ตัวอย่างที่ 3.24 รหัสลับคาเซียร์ (Casear cipher) เข้ารหัสโดย $f(p) = p + 3 \bmod 26$

ข้อความ = "MEET YOU IN THE PARK"

วิธีทำ

แปลงเป็นตัวเลข = 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

p+3 mod 16 = 15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13

∴ ข้อความที่เข้ารหัส = PHHW BRX LQ WKH SDUN

ในการถอดรหัสจะใช้ $f^{-1}(p) = (p - 3) \bmod 26$ ▌

3.5 เลขจำนวนเต็มและขั้นตอนวิธี

เนื่องจากคุณสมบัติของเลขจำนวนเต็มโดยเฉพาะการหารสามารถนำมาประยุกต์ใช้ในสาขาวิทยาการคอมพิวเตอร์ได้มากมาย ดังนั้นเมื่อทำการศึกษานิยามและทฤษฎีบทจนเป็นที่เข้าใจ รวมถึงมีความเข้าใจเรื่องการเขียนขั้นตอนวิธี จะทำให้สามารถนำความรู้ที่ได้มาประยุกต์เพื่อให้เข้าใจกลไกบางส่วนในการทำงานของคอมพิวเตอร์ทั้งโดยตรงคือการดำเนินการกับเลขจำนวนเต็มขนาดใหญ่เกินกว่าที่คอมพิวเตอร์จะแทนได้ ระบบการตรวจสอบข้อมูลในการสื่อสารข้อมูล และการเข้ารหัสข้อมูลเพื่อรักษาความปลอดภัย เป็นต้น

ทฤษฎีบทที่ 3.8 ให้ $a = bg + r$ เมื่อ a,b,q และ r เป็นเลขจำนวนเต็มแล้ว

ห.ร.ม. (a,b) = ห.ร.ม. (b,r)

พิสูจน์ที่ 3.8 สมมุติ $d \mid a$ และ $d \mid r$ → $d \mid (a - bq)$

→ d เป็นตัวหารร่วมของ b และ r

ทำนองเดียวกัน $d \mid a$ และ $d \mid r$ → $d \mid (bq + r)$

→ d เป็นตัวหารร่วมของ a และ b

∴ นั่นคือ ห.ร.ม. (a,b) = ห.ร.ม. (b,r)

3.5.1 ขั้นตอนวิธีของยูคลิด

ขั้นตอนวิธีของยูคลิด (Euclidean algorithm) เป็นการหา ห.ร.ม. ของจำนวนเต็ม 2 จำนวนใด ๆ ที่มีค่ามาก ๆ โดยใช้หลัก ขั้นตอนวิธีการหาร ซึ่งมีขั้นตอนดังนี้

$$a = q_1 b + r_1 \quad 0 \le r_1 < b$$

$$b = q_2 r_1 + r_2 \quad 0 \le r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \quad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad 0 \le r_n < r_{n-1}$$

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

ขั้นตอนวิธี ***Procedure*** gcd(a,b : positive int)

```
x=a
y=b
while y ≠ 0
begin
        r = x mod y
        x=y
        y=r
end {ห.ร.ม. (a,b) คือ x}
```

ตัวอย่างที่ 3.25 จงหา ห.ร.ม. (414,662) โดยใช้ขั้นตอนวิธีของยูคลิด

วิธีทำ
$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41 + 0$$
$\therefore$ ห.ร.ม. (414,662) = 2 ▌

3.5.2 การแทนกันของเลขจำนวนเต็ม

ในการเรียนทางด้านวิทยาการคอมพิวเตอร์มักมีการเปลี่ยนฐานของเลขไปเป็นฐาน 2 เนื่องจากคอมพิวเตอร์เป็นอุปกรณ์ดิจิทัลที่มีบิต 0 และ 1 ในการแทนข้อมูล ทฟษฎีทางด้านขั้นตอนวิธีของเลขจำนวนเต็มสามารถนำมาประยุกต์เพื่อเปลี่ยนฐานของเลขได้ดังสมการ

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$$

ฐาน b ของเลข n เขียนอยู่ในรูปเลขฐานเป็น $(a_k a_{k-1} ..... a_1 a_0)b$

ตัวอย่างที่ 3.26 จงหาเลขฐาน 8 ของ $(12345)_{10}$

วิธีทำ
$$12345 = 8 \cdot 1543 + 1$$
$$1543 = 8 \cdot 192 + 7$$
$$192 = 8 \cdot 24 + 0$$
$$24 = 8 \cdot 3 + 0$$
$$3 = 8 \cdot 0 + 3$$
$\therefore (12345)_{10} = (30071)_8$ ▌

ขั้นตอนวิธี ***Procedure*** base b expansion (n : positive int)

$q = n$

$k = 0$

while $q \neq 0$

bigin

$a_k = q \mod b$

$q = \lfloor q / b \rfloor$

$k = k + 1$

end

{ เลขฐาน b ของ n คือ $(a_{k-1}a_{k-2}...a_1a_0)_b$ } (Lamey, 2002, p.131)

3.5.3 ขั้นตอนวิธีสำหรับตัวดำเนินการของเลขจำนวนเต็ม

เนื่องจากคอมพิวเตอร์ทำงานในระบบดิจิทัล การดำเนินการกับข้อมูลจะอยู่ในรูปบิต ซึ่งในทางคณิตศาสตร์สามารถแทนได้ด้วยรหัสเลขฐาน 2 ดังนั้นขั้นตอนวิธีสำหรับดำเนินการของเลขจำนวนเต็มที่จะกล่าวจะทำกับเลขฐาน 2 ซึ่งมีการทำงานดังนี้

3.4.3.1 การบวกเลขฐาน 2 จำนวน 2 ตัว

ให้ $a = (a_{n-1}a_{n-2}...a_1a_0)_2$

$b = (b_{n-1}b_{n-2}...b_1b_0)_2$

จำนวนบิตไม่เท่ากันให้เติม 0 ข้างหน้า การบวกเริ่มจากบิตทางขวาไปซ้าย

$$a_0 + b_0 = c_0 \cdot 2 + s_0$$

$s_0 =$ ผลลัพธ์ , c_0 = ตัวทด

$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_0$$

$$a_{n-1} + b_{n-1} + c_{n-2} = c_{n-1} \cdot 2 + s_{n-1}$$

$$\therefore a+b = (s_ns_{n-1}s_{n-2}...s_1s_0)_2$$

ตัวอย่างที่ 3.27 จงบวก $a = (1110)_2$ และ $b = (1011)_2$

วิธีทำ 1110

1011

ตัวทด 11––

a+b $(11001)_2$ ▌

ขั้นตอนวิธี ***Procedure*** add (a,b; ส่วนขยายเลขฐาน 2 จำนวนเต็มบวก)

C = 0

For j = 0 to n-1

Begin

$d = \lfloor (a + b_j + c)/2 \rfloor$

$S_j = a_j + b_j + c - 2d$

c = d

end

$s_n = c$ { ส่วนขยายเลขฐาน 2 ของ sum = $(s_n s_{n-1} s_{n-2} \ldots s_1 s_0)_2$ }

3.4.3.2 การคูณกันของเลขฐาน 2 จำนวน 2 ตัว

ให้ $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$ และ $b = (b_{n-1}b_{n-2}\ldots b_1b_0)_2$

a, b จะได้จากการเอา a คูณ ด้วย b_0

a คูณ ด้วย b_0

a คูณ ด้วย b_1 เลื่อนบิตไปทางซ้าย 1

a คูณ ด้วย b_2 เลื่อนบิตไปทางซ้าย 2

⋮

a คูณ ด้วย b_{n-1} เลื่อนบิตไปทางซ้าย n-1แล้วรวมเข้าด้วยกัน

ตัวอย่างที่ 3.28 จงคูณ $a=(110)_2$ และ $b=(101)_2$

วิธีทำ

$$\begin{array}{r} 110 \\ \underline{101} \\ 110 \\ 000 \\ \underline{110} \\ (11110)_2 \end{array}$$

ขั้นตอนวิธี ***Procedure*** multiple (a,b:เลขจำนวนเต็มบวกฐาน 2)

```
For j=0 to n-1
Begin
    If b_j =1 then c_j = a shifted j places
    Else c_j = 0
End
{c_0, c_1, ..., c_n-1 เป็นส่วนย่อย}
P = 0
For j = 0 to n-1
   P = p+ c_j    {p คือค่าของ ab}
```

ตัวอย่างที่ 3.29 ความซับซ้อนของขั้นตอนวิธีพหุคูณ

วิธีทำ

1. จำนวนครั้งที่ใช้ในการเลื่อนบิต $0+1+2+\ldots+n-1 = 0(n^2)$
2. จำนวนครั้งที่ใช้ในการบวก ทั้งหมดเข้าด้วยกัน

   การบวกเลข n บิต 2 จำนวนใช้ n ครั้ง

3 จำนวนใช้ 2n ครั้ง

4 จำนวนใช้ 3n ครั้ง

n จำนวนใช้ (n-1)n ครั้ง

$\therefore$ ความซับซ้อนของการบวก = $0(n^2)$ ∎

3.6 การประยุกต์ของทฤษฎีจำนวน

ทฤษฎีจำนวนสามารถนำไปประยุกต์ใช้งานในส่วนของวิทยาการคอมพิวเตอร์ได้หลายด้าน อาทิ การดำเนินการกับตัวเลขขนาดใหญ่และการเข้ารหัสข้อมูล มีทฤษฎีสำคัญที่นำมาประยุกต์ใช้ดังนี้

ทฤษฎีบทที่ 3.9 ถ้า a,b เป็นเลขจำนวนเต็มบวกจะมีเลขจำนวนเต็ม s และ t

ซึ่ง ห.ร.ม. (a,b) = sa+tb

ตัวอย่างที่ 3.30 จงแสดงว่า ห.ร.ม.(252,198) = 18 ในการประสมเชิงเส้นของ 252 และ 198

วิธีทำ 252 = 1·198 + 54

198 = 3·54 + 36

54 = 1·36+18

36 = 2·18+0

$\therefore$ ห.ร.ม.(252,198) = 18 ∎

ทฤษฎีบทที่ 3.10 ถ้า a,b,c เป็นเลขจำนวนเต็มบวก ซึ่ง ห.ร.ม.(a,b) = 1 และ a|bc แล้ว a|c

พิสูจน์ที่ 3.10 $\because$ ห.ร.ม. (a,b) = 1 ดังนั้น sa + tb = 1

sac + tbc = c

พิจารณา a | sac และ a | tbc

$\therefore$ a | (sac+tbc) นั่นคือ a | c

ทฤษฎีบทที่ 3.11 ถ้า p เป็นเลขจำนวนเฉพาะ $p|a_1a_2....a_n$ เมื่อแต่ละ a_j เป็นเลขจำนวนเต็มแล้ว $p|a_i$ สำหรับ i บางตัว

ทฤษฎีบทที่ 3.12 ให้ m เป็นเลขจำนวนเต็มบวก a,b และ c เป็นเลขจำนวนเต็ม ถ้า $ac \equiv bc \bmod m$ และ ห.ร.ม.(c,m) = 1 แล้ว $a \equiv b \bmod n$

พิสูจน์ที่ 3.12 $ac \equiv bc \bmod m$, $m \mid (ac- bc) = c(a-b)$ ทฤษฎีบทที่ 3.10

$\therefore m \mid (a-b)$

นั่นคือ $a \equiv b \bmod m$

3.6.1 สมภาคเชิงเส้น

สมภาคเชิงเส้น (linear congruences) เป็นสมภาคที่อยู่ในรูปแบบ $ax \equiv b \bmod m$ เมื่อ x เป็นตัวแปร

ทฤษฎีบทที่ 3.13 ถ้า a และ m เป็นจำนวนเฉพาะสัมพัทธ์ และ $m > 1$ แล้ว จะมีส่วนผกผัน เพียงค่าเดียวของ a mod m แทนด้วย $\bar{a}$ ซึ่ง $a\bar{a} = 1 \bmod m$

พิสูจน์ที่ 3.13 $\because$ ห.ร.ม. (a,m) = 1 $sa + tm = 1$ $\exists s, t$

$Sa + tm \equiv 1 \bmod m$

$\because tm \equiv 0 \bmod m$ $\therefore sa \equiv 1 \bmod m$

นั่นคือ s เป็นส่วนผกผันของ a mod m

สมมติว่ามี tcm อีกตัวหนึ่งที่ทำให้ $ta \equiv 1 \bmod m$

$\therefore sa \equiv ta \equiv 1 \bmod m$

$s \equiv t \bmod m$ (ห.ร.ม.(a,m)=1)

$\because s,t < m \therefore s = t$ นั่นคือส่วนผกผัน

ตัวอย่างที่ 3.31 จงหาส่วนผกผันของ 3 mod 7

วิธีทำ ∵ ห.ร.ม.(3,7) = 1 ∴ จะสามารถหาส่วนผกผันได้

∵ $2.5 \equiv 1 \bmod 7$

∴ 5 เป็นส่วนผกผันของ 3 mod 7

ทำนองเดียวกัน $5 \pm 7, 5 \pm 14, \ldots$ ก็เป็นส่วนผกผันของ 3 ▌

ตัวอย่างที่ 3.32 จงหาค่า x ของสมภาคเชิงเส้น $3x \equiv 4 \mod 7$

วิธีทำ

$$3x \equiv 4 \bmod 7$$

$$5.3.x \equiv 5.4 \bmod 7$$

$$x \equiv 20 \equiv 6 \bmod 7$$

$$\therefore \quad x \equiv 6 \bmod 7$$ ▌

3.6.2 ทฤษฎีบทเศษเหลือของจีน

ทฤษฎีบทเศษเหลือของจีน (chinese remainder theorem) เป็นระบบสมภาคเชิงเส้นหลายชั้น เริ่มจากแนวคิดปริศนาของของนักคณิตศาสตร์ชาวจีนชื่อ ซัน ชู (Sun Tsu 's puzzle) โดยปริศนาที่ว่าคือมีสิ่งของอยู่จำนวนหนึ่ง ถ้าเอา 3 หาร จะเหลือเศษ 2 ถ้าเอา 5 หารจะเหลือเศษ 3 ถ้าเอา 7 หารจะเหลือเศษ 2 ถามว่า จำนวนสิ่งของนั้นเป็นเท่าไร

หรือ $x \equiv 2 \mod 3$

$x \equiv 3 \mod 5$

$x \equiv 2 \mod 7$

ปริศนาของ ซัน ชู นี้นำไปสู่ทฤษฎีบทเศษเหลือของจีน

ทฤษฎีบทที่ 3.14 (ทฤษฎีบทเศษเหลือของจีน) ให้ $m_1, m_2, ...m_n$ เป็นจำนวนเฉพาะสัมพัทธ์ตรงกันและเป็นเลขจำนวนเต็มบวก

$$x \equiv a_1 \mod m_1$$

$$x \equiv a_2 \mod m_2$$

$$x \equiv a_n \mod m_n$$

จะมีคำตอบเพียงค่าเดียวที่ mod m = $m_1, m_2, ...m_n$

พิสูจน์ที่ 3.14 ให้ $M_k = m/m_k \qquad k = 1,2,..,n$

$\therefore$ ห.ร.ม.$(m_k, M_k) = 1$

$\therefore$ M_k จะมี ส่วนผกผันภายใต้ mod m_k

นั่นคือ $M_k m_k \equiv 1 \mod m_k$

ให้ $x = a_1M_1y_1 + a_2M_2y_2 + ... + a_nM_ny_n$

จะได้ $x \equiv a_kM_ky_k \mod m_k$

$$\equiv a_k \mod m_k$$

$$a_kM_ky_k \equiv a_k \mod m_k$$

นั่นคือ x เป็นผลลัพธ์ด้วย

ให้ x และ y เป็นคำตอบ 2 ค่าที่ต่างกัน $(\not\equiv \mod m)$

$$x \equiv a_k \equiv y \mod m_k$$

$$x \equiv y \mod m_k$$

$$\therefore x \equiv y \mod m_1m_2.....m_k$$

พิสูจน์ $x \equiv 2 \mod 3$

$$x \equiv 3 \mod 5$$

$$x \equiv 2 \mod 7$$

และ 3,5,7 เป็นจำนวนเฉพาะสัมพัทธ์ตรงกัน

ให้ $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$

$M_2 = m/5 = 21$

$M_3 = m/7 = 15$

จากทฤษฎีบทเศษเหลือของจีนจะได้ผลลัพธ์คือ

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$$

เมื่อ y_i คือส่วนผกผันของ M_i ภายใต้ mod m_i

$\therefore$ ได้ $y_1 = 2, \quad y_2 = 1, \quad y_3 = 1$

$$\therefore x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \ (\text{mod } 105)$$

$$\therefore x \equiv 23 \ \text{mod } 105$$

3.6.3 เลขคณิตคอมพิวเตอร์กับเลขจำนวนเต็มขนาดใหญ่

ให้ $m \equiv m_1, m_2, m_3, \ldots, m_n$ ห.ร.ม.$(m_i, m_j) = 1$ $\forall_i \neq j$ เลขจำนวนเต็ม a ใด ๆ ที่ $0 \leq a < m$ สามารถ จะแทนใน n-แถว ได้เพียงค่าเดียวคือ $(a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_n)$

ตัวอย่างที่ 3.33 ต้องการแทนเลขจำนวนเต็มบวก ที่น้อยกว่า 12

วิธีทำ ให้ $m_1 = 3$, $m_2 = 4$ และ ห.ร.ม.(3,4) = 1

$\therefore$ เลขจำนวนเต็ม a สามารถแทนในรูป (a mod 3, a mod 4) ดังนี้

0 = (0,0)	4 = (1,0)	8 = (2,0)
1 = (1,1)	5 = (2,1)	9 = (0,1)
2 = (2,2)	6 = (0,2)	10 = (1,2)
3 = (0,3)	7 = (1,3)	11 = (2,3)

▌

ดังนั้น ถ้าเลขขนาดใหญ่ อาจจะแทนในแต่ละคู่แล้วแสดงการดำเนินการซึ่งกันและกัน แต่ละส่วนเสร็จแล้วจึงกู้คืนค่าที่แท้จริง โดยการวิเคราะห์ n สมภาค การแทนในแต่ละคู่จะช่วยให้ดำเนินการกับเลขจำนวนเต็มขนาดใหญ่ได้ และสามารถจะทำงานแบบขนานได้

ตัวอย่างที่ 3.34 สมมติ คอมพิวเตอร์ดำเนินการกับเลขจำนวนเต็มขนาด < 100 จะเลือกมอดุโล 99,98,97 และ 95 (เป็นจำนวนเฉพาะสัมพัทธ์แต่ละคู่)

วิธีทำ $m = 99.98.97.95 = 89,403,930$

$\therefore$ สามารถจะแทนเลขจำนวนเต็มได้ถึง 89,403,930

เช่น 123,684 = (33,8,9,89)

431,456 = (32,92,42,16)

123,684,+,413,456 = (33,8,9,89)+ (32,92,42,16)

= (65,2,51,10)

การกู้คืนจะต้องวิเคราะห์ $x \equiv 65 \bmod 99$ $x \equiv 51 \bmod 97$

$x \equiv 2 \bmod 98$ $x \equiv 10 \bmod 95$

การเลือกตัวย่อยเพื่อความสะดวกจะเลือกให้อยู่ในรูป 2^K-1 เพราะง่ายในการทำเลขคณิตแบบทวิภาค และง่ายในการหาตัวที่เป็นจำนวนเฉพาะสัมพัทธ์ (เพราะ ห.ร.ม.$(2^a-1, 2^b-1) = 2^{\text{ห.ร.ม.}(a,b)}-1$)

นั่นคือเลือก a,b ที่เป็นจำนวนเฉพาะสัมพัทธ์เท่านั้น

เช่นเลือกมอดุโลเป็น $2^{35}-1$, $2^{34}-1$, $2^{33}-1$, $2^{31}-1$, $2^{29}-1$, $2^{23}-1$

ทุกตัวจะเป็นจำนวนเฉพาะสัมพัทธ์ตรงกัน ทำให้สามารถดำเนินการทางเลขคณิตกับเลขจำนวนเต็มขนาด 2^{184} ได้ ▌

3.6.4 เลขจำนวนเฉพาะเทียม

เลขจำนวนเฉพาะเทียม (pseudoprimes) ถ้าเลขจำนวนเต็ม n สามารถแยกตัวประกอบเป็น $2^{n-1} \equiv 1 \pmod{n}$ แล้วเลขจำนวนเต็มนี้จะเรียกว่าเลขจำนวนเฉพาะเทียม

ทฤษฎีบทที่ 3.15 (ทฤษฎีบทของแฟมาต์ (Fermat's theorem)) ถ้า p เป็นเลขจำนวนเฉพาะและ a เป็นเลขจำนวนเต็ม ที่หารด้วย p ไม่ลงตัว แล้ว

$$a^{p-1} \equiv 1 \bmod p \quad \text{และ}$$

$$a^{p} \equiv a \bmod p$$

มี ตัวประกอบบางตัวที่ n m $2^{n-1} \equiv 1 \mod n$

เลขจำนวนเต็มที่มีคุณสมบัตินี้จะเรียกว่าเลขจำนวนเฉพาะเทียมหายาก

ตัวอย่างที่ 3.35 $341 = 11 \cdot 31$ และ $2^{340} \equiv 1 \mod 341$

$\therefore$ 341 เป็นเลขจำนวนเฉพาะเทียม ▌

3.6.5 การเข้ารหัสลับแบบกุญแจสาธารณะ

เทคโนโลยีของการเข้ารหัสลับมี 2 ลักษณะคือการเข้ารหัสลับแบบกุญแจส่วนตัว (private key cryptography) หมายถึงใช้กุญแจใดเข้ารหัส จะใช้กุญแจนั้นเป็นตัวถอดรหัสและการเข้ารหัสลับแบบกุญแจสาธารณะ (public key cryptography) การเข้ารหัสและถอดรหัสใช้กุญแจคนละดอก การเข้ารหัสแบบรหัสลับแบบกุญแจส่วนตัว จะมีปัญหาเรื่องการแลกเปลี่ยนกุญแจ การเข้ารหัสลับแบบกุญแจสาธารณะที่มีชื่อเสียงคืออาร์เอสเอ (RSA) ที่คิดค้นในปี 1976 โดยนักวิจัยของ เอ็มไอที 3 คน (Rosen, 1995, p.176) โดยมีพื้นฐานของมอดุโลยกกำลังของเลขจำนวนเฉพาะขนาดใหญ่ ซึ่งมีหลักในการเข้ารหัสดังนี้

หลักการทำงานของอาร์เอสเอ

1. เลือกจำนวนเฉพาะขนาดใหญ่ 2 ตัว คือ p,q

2. คำนวณ $n = pq$

3. เลือกกุญแจที่ใช้เข้ารหัส **e** โดยที่ ห.ร.ม. $(e,(p-1)(q-1)) = 1$

4. คำนวณกุญแจที่ใช้ถอดรหัส d โดยที่ $ec \equiv 1 \bmod (p-1)(q-1)$

5. การเข้ารหัส โดย $C \equiv M^e \bmod n$

6. การถอดรหัส โดย $C^d \equiv M \bmod n$

e = กุญแจที่ใช้เข้ารหัสเปิดเผยให้รู้ทั่วกันได้

d = กุญแจที่ใช้ถอดรหัสจะต้องเก็บไว้เป็นความลับ สามารถแสดงได้ว่า

ถ้าเลือก $ec \equiv 1 \bmod (p-1)(q-1)$

แล้ว $M \equiv C^d \bmod n$ เมื่อ $C \equiv M^e \bmod n$

พิสูจน์ ถ้าเลือก e ซึ่ง ห.ร.ม. $(e,(p-1)(q-1)) = 1$ แล้วจะมีส่วนผกผัน

$\therefore$ ถ้า $de \equiv 1 \bmod (p-1)(q-1)$

$\therefore$ $de \equiv 1 + k(p-1)(q-1)$ เฉพาะ k บางตัว

$$C^d = (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$$

จากทฤษฎีบทของแฟมาต์

$$M^{p-1} \equiv 1 \bmod p \text{ และ } M^{q-1} \equiv 1 \bmod q$$

$$\therefore C^d \equiv M.(M^{p-1})^{k(q-1)} \equiv M.1 \bmod p$$

และ $C^d \equiv M.(M^{q-1})^{k(p-1)} \equiv M.1 \bmod p$

และ ห.ร.ม.$(p,q) = 1$ ทฤษฎีบทเศษเหลือของจีน

$\therefore C^d \equiv M \bmod pq$

หมายเหตุ ทฤษฎีบทของแฟมาต์ จะใช้ได้ในกรณีที่ ห.ร.ม.(M,p) และ (M,q)=1 เท่านั้น แต่อย่างไรก็ตามแม้ ห.ร.ม.(M,p) และ (M,q)≠1 ก็สามารถแสดงได้เช่นกันเพราะ M จะต้องเป็นจำนวน ของ p หรือ q

ตัวอย่างที่ 3.36 จงเข้ารหัสข้อมูลคำว่า “STOP” โดยใช้ RSA ถ้ากำหนดให้ p= 43, q= 59, e = 13

ห.ร.ม.(13,42,58) = 1 และ n=p, q=43·59=25537

วิธีทำ STOP = 18 19 14 15

การเข้ารหัส $C=M^{13} \bmod 2537$

$1819^{13} \bmod 2537 = 2018$

$1415^{13} \bmod 2537 = 2182$

∴ ข้อความที่ถูกเข้ารหัสคือ 2018 2182

การถอดรหัส $ed \equiv 1 \bmod (p-1)(q-1)$

$13 \equiv 1 \bmod 2436$

$d = 937$

$\therefore M=C^{937} \bmod 2537$

$2081^{937} \bmod 2537 = 1819$

$2182^{937} \bmod 2537 = 1415$

∴ข้อความต้นฉบับคือ 18 19 14 15 = STOP ▌

3.7 สรุป

ถ้าเปรียบการเขียนแบบพิมพ์เขียวของอาคารที่ดีทำให้อาคารที่สร้างถูกต้องสมบูรณ์และแข็งแรงแล้ว การเขียนโปรแกรมภาษาคอมพิวเตอร์ให้ดีมีข้อผิดพลาดน้อย ประหยัดทรัพยากร เช่น พื้นที่หน่วยความจำ พื้นที่ดิสก์ และการใช้รอบคำสั่งของหน่วยประมวลผลกลาง จำเป็นอย่างยิ่งที่ต้องมีความรู้ความเข้าใจในขั้นตอนวิธีที่จะนำมาใช้ในการเขียนโปรแกรม การเขียนขั้นตอนวิธีที่ดีนอกจากต้องรู้ทฤษฎีของโจทย์ แล้วยังต้องอาศัยการฝึกฝนเพื่อให้เกิดทักษะด้วย ในส่วนของทฤษฎีคณิตศาสตร์มีทฤษฎีที่สำคัญและเกี่ยวข้องกับวิทยาการคอมพิวเตอร์อยู่ไม่น้อย ทฤษฎีจำนวนก็เป็นหนึ่งในนั้น ทฤษฎีจำนวนมีหลักการพื้นฐาน 3 ส่วน คือ การหาร การหารร่วมมาก การคูณร่วมน้อย และเลขคณิตว่าด้วยการหารเอาเศษ ซึ่งทั้ง 3 ส่วนถูกนำไปประยุกต์เพื่อแก้ปัญหาการแทนเลขขนาดใหญ่ในคอมพิวเตอร์ การหาเลขสุ่ม และทฤษฎีการเข้ารหัสข้อมูล โดยเฉพาะการเข้ารหัสลับข้อมูลแบบแบบกุญแจสาธารณะ

3.8 แบบฝึกหัดท้ายบท

1. จงแสดงขั้นตอนทั้งหมดที่ใช้ในการค้นหา 9 ในลำดับ 1,3,4,5,6,8,9,11 โดยใช้
   1.1 การค้นหาเชิงเส้น
   1.2 การค้นหาทวิภาค

2. ค่ามัธยฐานของตัวเลขคือจำนวนของสมาชิกที่ปรากฏมีความถี่สูงที่สุดในรายการ จงเขียนขั้นตอนวิธีในการหาค่ามัธยฐานของเลขจำนวนเต็มบวก

3. จงหาผลหารและเศษเหลือของเลขต่อไปนี้
   3.1 9 หารด้วย 7
   3.2 –111 หารด้วย 11
   3.3 789 หารด้วย 23
   3.4 1001 หารด้วย 13

4. จงหาแฟคทอเรียลจำนวนเฉพาะ (prime factorization) ของ 10!

5. จงแสดงว่า ถ้า a, b, k, และ m เป็นเลขจำนวนเต็ม ซึ่ง $k \geq 1$, $m \geq 2$ และ $a \equiv b \pmod{m}$, แล้ว $a^k \equiv b^k \pmod{m}$ เมื่อ k เป็นเลขจำนวนเต็มบวก

6. ใช้ขั้นตอนวิธีของยูคลิดเพื่อหาค่าของ ห.ร.ม. ต่อไปนี้
   6.1 ห.ร.ม.(12,18)
   6.2 ห.ร.ม. (111, 201)
   6.3 ห.ร.ม. (1001, 1331)
   6.4 ห.ร.ม. (12345, 54321)

7. จงบวกเลขฐาน 2 $(10111)_2$ กับ $(11010)_2$ โดยใช้ขั้นตอนวิธีในตัวอย่างที่ 3.27

8. จงแสดงวิธีทำในการหา ห.ร.ม. โดยใช้วิธีการประสมเชิงเส้น จากคู่ลำดับตัวเลขดังต่อไปนี้

   8.1 10,11

   8.2 21,44

   8.3 36, 48

9. จงแสดงว่า 15 เป็นส่วนผกผันของ 7 มอดุโล 26

10. เลขจำนวนเต็มใดจะมีเศษ =1 เมื่อหารด้วย 2 และจะมีเศษ = 1 เมื่อหารด้วย 3 ด้วย

เอกสารอ้างอิง

Lamey, Robert. (2002). **Logical problem solving before the flowchart with C++ and visual basic applications**. NJ: Prentice-Hall.

Rosen Kenneth H. (1995). **Discrete mathematics and its application** (3rd ed). Singapore: McGraw-Hill.