การพัฒนาขั้นตอนวิธีและวิธีสำหรับทฤษฎีจำนวน

IMPLEMENTATION OF ALGORITHMS AND METHODS FOR NUMBER THEORY

ขวัญชัย กรอนันต์ศิลป์
พัชราภรณ์ สุวรรณวัฒนกุล
สันต์สินี เพ็งพันธ์

ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต
ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2549

IMPLEMENTATION OF ALGORITHMS AND METHODS FOR NUMBER THEORY

KHWANCHAI KORNANANSIL
PATCHARAPORN SUWANWATTANAKUL
SANSINEE PENGPAN

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 2006

หัวข้อปัญหาพิเศษ	การพัฒนาขั้นตอนวิธีและวิธีสำหรับทฤษฎีจำนวน IMPLEMENTATION OF ALGORITHMS AND METHODS FOR NUMBER THEORY	
ชื่อนักศึกษา	นายชวัญชัย กรอนันต์ศิลป์	46050587
	นางสาวพัชราภรณ์ สุวรรณวัฒนกุล	46050026
	นางสาวสันต์สินี เพ็งพันธ์	46050041
ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์	
สาขาวิชา	คณิตศาสตร์ประยุกต์	
อาจารย์ที่ปรึกษา	รศ.พัชรินทร์ เหมโชติ	
	รศ.ไพรบูลย์ พันธรักษ์พงษ์	

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุมัติให้นับปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาคณิตศาสตร์ประยุกต์ ประจำปีการศึกษา 2549

คณะกรรมการสอบ		ลายมือชื่อ
ประธานกรรมการ	ผศ.ดร.ฉัฐไชย์ ลีนาวงศ์	
กรรมการ	อ.จินดา ไชยช่วย	
กรรมการและอาจารย์ที่ปรึกษา	รศ.พัชรินทร์ เหมโชติ	
กรรมการและอาจารย์ที่ปรึกษา	รศ.ไพรบูลย์ พันธรักษ์พงษ์	

(รองศาสตราจารย์ ดร.วีระ บุญจริง)

หัวหน้าภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

ลิขสิทธิ์ของภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

หัวข้อปัญหาพิเศษ	การพัฒนาขั้นตอนวิธีและวิธีสำหรับทฤษฎีจำนวน	
ชื่อนักศึกษา	นายขวัญชัย กรอนันต์ศิลป์	46050587
	นางสาวพัชราภรณ์ สุวรรณวัฒนกุล	46050026
	นางสาวสันต์สินี เพ็งพันธ์	46050041
ปริญญา	วิทยาศาสตรบัณฑิต	
ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์	
สาขาวิชา	คณิตศาสตร์ประยุกต์	
ปีการศึกษา	2549	
อาจารย์ที่ปรึกษา	รศ.พัชรินทร์ เหมโชติ	
	รศ.ไพรบูลย์ พันธรักษ์พงษ์	

บทคัดย่อ

โครงงานปัญหาพิเศษนี้เป็นโปรแกรมเพื่อใช้ในงานทางด้านทฤษฎีจำนวน ขั้นตอนวิธีและกรรมวิธีต่างๆของทฤษฎีจำนวนได้ถูกสร้างขึ้นด้วยภาษาวิชวลเบสิค เวอร์ชัน 6.0 เพื่อหาคำตอบและแสดงขั้นตอนในการคำนวณ

Special Project Title	IMPLEMENTATION OF ALGORITHMS AND METHODS FOR NUMBER THEORY	
Students	Mr.Khwanchai Kornanansil	46050587
	Miss.Patcharaporn Suwanwattanakul	46050026
	Miss.Sansinee Pengpan	45050041
Degree	Bachelor of Science	
Department	Mathematics and Computer Science, Faculty of Science	
Programme	Applied Mathematics	
Academic Year	2006	
Special Project Advisor	Assoc.Prof.Patcharin Hemchote	
	Assoc.Prof.Praiboon Pantaragphong	

ABSTRACT

The purpose of this special project is to develop software to be used in Number Theory. Various algorithm and methods from Number Theory are implemented using Visual Basic 6.0 to determine the solutions as well as to demonstrate the steps of the computation.

กิตติกรรมประกาศ

ในการทำปัญหาพิเศษเรื่องการพัฒนาโปรแกรมเพื่อการคำนวณของจำนวนเต็ม สามารถลุล่วงไปด้วยดี คณะผู้จัดทำต้องขอขอบพระคุณรองศาสตราจารย์พัชรินทร์ เหมโชติและรองศาสตราจารย์ไพรบูลย์ พันธรักษ์พงษ์ อาจารย์ที่ปรึกษาปัญหาพิเศษนี้ ที่กรุณาให้คำแนะนำและเป็นที่ปรึกษาในการแก้ปัญหาต่างๆ รวมทั้งเป็นผู้ตรวจสอบความถูกต้องของปัญหาพิเศษฉบับนี้

ขอขอบพระคุณอาจารย์ทุกท่านที่ได้ประศาสน์วิชาความรู้ทั้งทางด้านทฤษฎีและภาคปฏิบัติแก่คณะผู้จัดทำจนกระทั่งปัญหาพิเศษนี้สัมฤทธิ์ผลด้วยดีทุกประการ

ขอขอบคุณเจ้าหน้าที่ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ที่คอยให้ความสะดวกในการใช้ห้องปฏิบัติการคอมพิวเตอร์

นอกจากนี้คณะผู้จัดทำต้องขอขอบพระคุณบิดา มารดา ที่ได้ให้ความสนับสนุนทางด้านกำลังใจและทุนทรัพย์ จนทำให้การทำปัญหาพิเศษครั้งนี้สำเร็จด้วยดี รวมทั้งพี่ๆเพื่อนๆและน้องๆทุกคนที่ให้ความช่วยเหลือในด้านต่างๆเกี่ยวกับปัญหาพิเศษไว้ ณ ที่นี้

คณะผู้จัดทำ

มีนาคม 2550

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของปัญหา

จำนวนเต็มเป็นประเภทหนึ่งของจำนวนทางคณิตศาสตร์ ซึ่งแบ่งเป็นจำนวนเต็มลบ เต็มศูนย์ และเต็มบวก โดยจำนวนเต็มสามารถจะเป็นจำนวนเฉพาะหรือจำนวนประกอบก็ได้และมีทฤษฎีบทพื้นฐานต่างๆ ที่เกี่ยวข้องกับจำนวนเต็มเช่น การหารลงตัว เศษเหลือจากการหาร สมภาค ฟังก์ชันเชิงจำนวน รากปฐมฐาน เลขชี้กำลัง เศษส่วนต่อเนื่อง

การเรียนรู้เกี่ยวกับคุณสมบัติของจำนวนเต็มนั้น ถึงแม้จะดูเป็นเรื่องง่าย แต่ถ้าจำนวนเต็มจำนวนนั้นมีค่ามากก็ค่อนข้างเสียเวลาในการคำนวณเช่น การเข้ารหัส ก็ต้องใช้จำนวนเต็มซึ่งเป็นจำนวนเฉพาะที่มีค่ามากและการมีทฤษฎีบทมากมายที่เกี่ยวข้องในการศึกษา ทำให้เรื่องของจำนวนไม่เป็นที่น่าสนใจของคนทั่วไป

ดังนั้นหากสามารถพัฒนาโปรแกรมที่ช่วยแสดงวิธีการทางคณิตศาสตร์และหาคำตอบจากคุณสมบัตินั้นๆได้เร็วขึ้น จะช่วยเสริมทักษะให้กับผู้สนใจศึกษาและเป็นสิ่งจูงใจให้หลายๆ คนหันมาสนใจศึกษาเกี่ยวกับจำนวนเต็มมากขึ้น ซึ่งจะเป็นแนวทางนำไปสู่การศึกษาคณิตศาสตร์ นอกจากนี้ยังเกิดความสะดวกในการนำค่าเหล่านั้นไปประยุกต์ใช้อีกด้วย

1.2 วัตถุประสงค์ของการศึกษา

1) เพื่อสร้างโปรแกรมแสดงกรรมวิธีทางคณิตศาสตร์ในเรื่องของจำนวนเต็ม และเพื่อให้สามารถคำนวณหาคำตอบจากคุณสมบัติของจำนวนเต็มได้เร็วขึ้น
2) เพื่อเผยแพร่โปรแกรมที่พัฒนาขึ้นสู่บุคคลทั่วไปที่สนใจศึกษาในเรื่องของจำนวนเต็ม

1.3 ขอบเขตของปัญหา

1) เป็นโปรแกรมที่สามารถรับค่าตัวเลขจากผู้ใช้ได้และแสดงการคำนวณตามขั้นตอนตามบทนิยามในบางเรื่องเท่านั้น
2) ทำตารางที่เกี่ยวกับจำนวนเต็ม เช่น ตารางแสดงรากปฐมฐาน ตารางแสดงเลขชี้กำลัง ตารางแสดงอันดับ ตารางแสดงค่าฟังก์ชันเชิงจำนวน โดยจำนวนมีค่าประมาณไม่เกิน 100 และตารางเกี่ยวกับจำนวนเฉพาะ เช่น ตารางแสดงจำนวนเฉพาะ 1000 จำนวนแรก
3) โปรแกรมที่พัฒนาจะเป็นโปรแกรมสำเร็จรูปแบบผู้ใช้คนเดียว (Stand Alone) บนระบบปฏิบัติการวินโดวส์ XP

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1) โปรแกรมที่พัฒนานี้จะเป็นเครื่องมือที่ช่วยเพิ่มทักษะและความเข้าใจในวิธีการคิดเกี่ยวกับเรื่องของจำนวนเต็มแก่ผู้ใช้งานได้มากขึ้น
2) โปรแกรมที่พัฒนานี้สามารถช่วยหาคำตอบจากคุณสมบัติของจำนวนเต็มได้เร็วขึ้น

1.5 ขั้นตอนของการศึกษา

1) รวบรวมและศึกษาเนื้อหาและทฤษฎีบทพื้นฐานต่างๆเกี่ยวกับจำนวนเต็ม
2) ศึกษาเกี่ยวกับการเขียนโปรแกรม Visual Basic 6.0
3) ทำการออกแบบหน้าจอและรูปแบบของตัวโปรแกรมที่จะพัฒนา
4) ทำการเขียนโปรแกรมเพื่อแสดงการทำงานในส่วนของฟังก์ชันต่างๆตามที่ได้ออกแบบไว้
5) ทดสอบและแก้ไขโปรแกรมเพื่อให้โปรแกรมมีประสิทธิภาพ
6) ปรับแต่งรูปแบบการนำเสนอของโปรแกรมให้มีความสวยงาม
7) จัดทำเป็นรายงาน

บทที่ 2
นิยามและทฤษฎีที่เกี่ยวข้อง

2.1 การหารลงตัว (Divisibility)

2.1.1 ขั้นตอนวิธีการหาร (The Division Algorithm)

ทฤษฎีบท 2.1 สำหรับจำนวนเต็ม a , b ใดๆโดยที่ $b > 0$ จะมีจำนวนเต็ม q และ r อย่างละหนึ่งจำนวนที่สอดคล้องกับ

$$a = qb + r \quad , 0 \le r < b$$

q เรียกว่า ผลหาร (Quotient) r เรียกว่า เศษเหลือ (Remainder) ในการหาร a ด้วย b

ตัวอย่างเช่น ให้ a = 70 หารด้วย b = 30 จะได้ว่า 70 = 2(30) + 10 ดังนั้น q = 2 และ r = 10

นิยาม 2.1 ให้ a และ b เป็นจำนวนเต็ม โดยที่ $b \neq 0$ จะกล่าวว่า b หาร a ลงตัว (b divides a) เขียนแทนด้วย $b \mid a$ ถ้ามีจำนวนเต็ม q ที่ทำให้ $a = qb$

ตัวอย่างเช่น ให้ a = 60 หารด้วย b = 30 จะได้ว่า 60 = 2(30) ดังนั้น กล่าวได้ว่า 30 หาร 60 ลงตัว โดยที่ q = 2

2.1.2 ตัวหารร่วมมาก (The Greatest Common Divisor)

นิยาม 2.2 ให้ a และ b เป็นจำนวนเต็มซึ่งมีอย่างน้อยหนึ่งตัวที่ไม่เป็นศูนย์ ตัวหารร่วมมากของ a และ b แทนด้วย gcd(a , b) เป็นจำนวนเต็มบวก d ซึ่งสอดคล้องกับ

(1) $d \mid a$ และ $d \mid b$

(2) ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \le d$

ตัวอย่าง 2.1 ตัวหารที่เป็นบวกของ 35 คือ 1, 5, 7, 35

ตัวหารที่เป็นบวกของ 100 คือ 1, 2, 4, 5, 10, 20, 25, 50, 100

ดังนั้นตัวหารร่วมที่เป็นบวกของ 35 และ 100 คือ 1, 5

เนื่องจาก 5 เป็นจำนวนที่มากที่สุด จะได้ gcd(35 , 100) = 5

บทตั้ง 2.2 ถ้า $a = qb + r$ แล้ว gcd(a , b) = gcd(b , r)

ตัวอย่าง 2.2 หา gcd(1485 , 1745)

จะได้ว่า

$$1745 = 1 \cdot 1485 + 260$$
$$1485 = 5 \cdot 260 + 185$$
$$260 = 1 \cdot 185 + 75$$
$$185 = 2 \cdot 75 + 35$$
$$75 = 2 \cdot 35 + 5$$
$$35 = 7 \cdot 5 + 0$$

ดังนั้น gcd(1485 , 1745) = 5

2.1.3 สมการไดโอแฟนไทน์ (Diophantine Equation)

- สมการเชิงเส้นไดโอแฟนไทน์ คือ สมการที่มีตัวแปรไม่รู้ค่า 2 ตัว ในรูปแบบ

$$ax + by = c$$

โดยที่ a , b , c เป็นจำนวนเต็มที่ให้ และ a , b ไม่เป็นศูนย์พร้อมกัน ตัวอย่างสมการเชิงเส้นไดโอแฟนไทน์ เช่น $3x + 6y = 18$

- ผลเฉลยของสมการ $ax + by = c$ คือ คู่ของจำนวนเต็ม x_0 และ y_0 ที่สอดคล้องกับสมการ

ตัวอย่าง 2.3 จากสมการ $3x + 6y = 18$ จะได้ว่า

$3(4) + 6(1) = 18$ นั่นคือ $x_0 = 4$ และ $y_0 = 1$

$3(-6) + 6(6) = 18$ นั่นคือ $x_0 = -6$ และ $y_0 = 6$

$3(10) + 6(-2) = 18$ นั่นคือ $x_0 = 10$ และ $y_0 = -2$

ทฤษฎีบท 2.3 สมการเชิงเส้นไดโอแฟนไทน์ $ax + by = c$ มีผลเฉลย ก็ต่อเมื่อ $d \mid c$ โดยที่ $d = \gcd(a,b)$ ถ้า x_0 , y_0 เป็นผลเฉลยเฉพาะของสมการแล้ว ผลเฉลยอื่น กำหนดโดย

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

โดยที่ t เป็นจำนวนเต็มใดๆ

ตัวอย่าง 2.4 พิจารณาสมการเชิงเส้นไดโอแฟนไทน์ $33x + 14y = 115$

โดยใช้ขั้นตอนวิธีแบบยุคลิดหา gcd(33 , 14) ดังนี้

$$33 = 2 \cdot 14 + 5$$

$$14 = 2 \cdot 5 + 4$$

$$5 = 1 \cdot 4 + 1$$

$$4 = 4 \cdot 1 + 0$$

ฉะนั้น gcd(33 , 14) = 1 ซึ่ง $1 | 115$ จึงหาผลเฉลยของสมการได้

เนื่องจาก

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 \\ &= 5 - 1(14 - 2 \cdot 5) \\ &= 3 \cdot 5 - (1 \cdot 14) \\ &= 3(33 - 2 \cdot 14) - 1 \cdot 14 \\ &= 3 \cdot 33 - 7 \cdot 14 \end{aligned}$$

$$\begin{aligned} 115 = 1 \cdot 115 &= 115(3 \cdot 33 - 7 \cdot 14) \\ &= 345 \cdot 33 + (-805) \cdot 14 \end{aligned}$$

ดังนั้น $x_0 = 345$, $y_0 = -805$ เป็นผลเฉลยหนึ่งของสมการ และผลเฉลยทั้งหมดคือ

$$x = 345 + \left(\frac{14}{1}\right)t = 345 + 14t$$

$$y = -805 - \left(\frac{33}{1}\right)t = -805 - 33t$$

โดยที่ t เป็นจำนวนเต็มบางจำนวน

2.2 จำนวนเฉพาะและจำนวนประกอบ (Primes and Composites)

2.2.1 นิยามพื้นฐานของจำนวนเฉพาะและจำนวนประกอบ

นิยาม 2.3 จำนวนเต็ม $n > 1$ เรียกว่า จำนวนเฉพาะ (Prime) ถ้าจำนวนเต็มนั้นมีตัวหารเป็น 1 และ n เท่านั้นและจำนวนเต็ม $n > 1$ ซึ่งไม่เป็นจำนวนเฉพาะเรียกว่า จำนวนประกอบ (Composite) ส่วนจำนวนเต็ม 1 นั้นถือเป็นกรณีเฉพาะที่ไม่เป็นทั้งจำนวนเฉพาะและจำนวนประกอบ ตัวอย่างเช่น 11 เป็นจำนวนเฉพาะ เพราะ มี 1 และ 11 เป็นตัวหารที่เป็นบวกของ 11

นิยาม 2.4 จำนวนเต็ม a และ b เป็นจำนวนเต็มซึ่งไม่เป็นศูนย์พร้อมกันเรียกว่า จำนวนเฉพาะสัมพัทธ์ (Relatively Prime หรือ Coprime) เมื่อ gcd(a,b) = 1

ตัวอย่างเช่น gcd(20,19) = 1 ดังนั้น 20 และ 9 เป็นจำนวนเฉพาะสัมพัทธ์

2.2.2 การคัดหาจำนวนเฉพาะของเอราทอสเทนีส (Sieve of Eratosthenes)

- การคัดหาจำนวนเฉพาะของเอราทอสเทนีส เป็นวิธีการในการค้นหาจำนวนเฉพาะที่น้อยกว่าค่าที่กำหนดซึ่งถูกคิดขึ้นโดยเอราทอสเทนีส นักคณิตศาสตร์ชาวกรีก
- ถ้าจำนวนเต็ม $a > 1$ เป็นจำนวนที่หารไม่ลงตัวด้วยจำนวนเฉพาะ $p \le \sqrt{a}$ แล้ว a เป็นจำนวนเฉพาะ

ตัวอย่าง 2.5 พิจารณาจำนวนตั้งแต่ 2 ถึง 100

(1) เขียนจำนวนเต็มคี่จาก 3 ถึง 100 จะได้ว่า 3 เป็นจำนวนเต็มคี่ที่น้อยที่สุด

(2) คัดตัวเลขที่เป็นผลคูณของ 3 ออก คือ 9, 15, 21, 27, ... โดยใช้เครื่องหมาย " / " เมื่อทำเสร็จแล้วจะได้ 5 ซึ่งไม่ถูกคัดออกเป็นจำนวนเฉพาะที่มีค่าน้อยที่สุด

(3) คัดตัวเลขที่เป็นผลคูณของ 5 ออก คือ 15, 25, 35, 45, ... โดยใช้เครื่องหมาย " / " (หรือใช้เครื่องหมายอื่นแทนเพื่อความแตกต่าง) เมื่อทำเสร็จแล้วจะได้ 7 ซึ่งไม่ถูกคัดออกเป็นจำนวนเฉพาะที่น้อยที่สุด

(4) คัดตัวเลขที่เป็นผลคูณของ 7 ออก คือ 21, 35, 49, 63, ... โดยใช้เครื่องหมาย " / " (หรือใช้เครื่องหมายอื่นแทนเพื่อความแตกต่าง) และหยุดการกระทำ เพราะ $7 < 10 = \sqrt{100}$

ฉะนั้นจะได้จำนวนเฉพาะคือ 2 , 3 , 5 , 7 , 11 , 13 , 17 , 19 , 23 , 29 , 31 , 37 , 41 , 43 , 47 , 53 , 59 , 61 , 67 , 71 , 73 , 79 , 83 , 89 , 97

แสดงเป็นตารางได้ดังนี้

3		5		7		9	/	11	
13		15	//	17		19		21	//
23		25	/	27	/	29		31	
33	/	35	//	37		39	/	41	
43		45	//	47		49	/	51	/
53		55	/	57	/	59		61	
63	/	65	/	67		69	/	71	
73		75	//	77	/	79		81	/
83		85	/	87	/	89		91	/
93	/	95	/	97		99	/		

ตารางที่ 2.1 ตารางแสดงการคัดหาจำนวนเฉพาะของเอราทอสเทนีส ในช่วง 2-100

2.2.3 การแจกแจงและรูปแบบของจำนวน (Distribution and Forms)

2.2.3.1 การแจกแจงจำนวนเฉพาะและจำนวนประกอบ (Prime and Composite Distribution)

ทฤษฎีบท 2.4 ทุกๆจำนวนเต็มบวก $n > 1$ สามารถแสดงได้ในรูปผลคูณของจำนวนเฉพาะ และเขียนได้เพียงแบบเดียวเท่านั้นโดยไม่คำนึงถึงลำดับของตัวประกอบที่ได้

บทแทรก 2.5 จำนวนเต็มบวก $n > 1$ สามารถเขียนได้ในรูปแบบยกกำลังของจำนวนเฉพาะ (Canonical) ได้เพียงแบบเดียวเท่านั้น และ

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_i}$$

โดยที่ $i = 1,2,\ldots,r$ แต่ละ k_i เป็นจำนวนเต็มบวกและแต่ละ p_i เป็นจำนวนเฉพาะที่ $p_1 < p_2 < \ldots < p_r$

ตัวอย่างเช่น $360 = 2^3 \cdot 3^2 \cdot 5$

$4725 = 3^3 \cdot 5^2 \cdot 7$

- จำนวนเต็มบวกสามารถเขียนให้อยู่ในรูปแบบต่างๆได้หลายรูปแบบ ดังนี้

1) $4n$, $4n+1$, $4n+2$ และ $4n+3$ โดยที่จำนวนเต็ม $n \geq 0$

ตัวอย่าง 2.6 รูปแบบ $4n$: $4 = 4(1)$ โดยที่ $n = 1$

$8 = 4(2)$ โดยที่ $n = 2$

รูปแบบ $4n+1$: $1 = 4(0)+1$ โดยที่ $n = 0$

$5 = 4(1)+1$ โดยที่ $n = 1$

รูปแบบ $4n+2$: $2 = 4(0)+2$ โดยที่ $n = 0$

$6 = 4(1)+2$ โดยที่ $n = 1$

รูปแบบ $4n+3$: $3 = 4(0)+3$ โดยที่ $n = 0$

$7 = 4(1)+3$ โดยที่ $n = 1$

2) จำนวนเต็มบวกบางจำนวนสามารถเขียนให้อยู่ในรูปแบบ $3n+2$ โดยที่จำนวนเต็ม $n \geq 0$

ตัวอย่าง 2.7 $2 = 3(0)+2$ โดยที่ $n = 0$

$8 = 3(2)+2$ โดยที่ $n = 2$

3) ทุกๆจำนวนเต็มในรูปแบบ n^4+4 เมื่อจำนวนเต็ม $n>1$ เป็นจำนวนประกอบ

ตัวอย่าง 2.8 $20 = 2^4+4$ โดยที่ $n = 2$

$85 = 3^4+4$ โดยที่ $n = 3$

4) จำนวนเต็มบวกในรูปแบบ $3n+1$ เมื่อจำนวนเต็ม $n \geq 1$ บางจำนวนเป็นจำนวนเฉพาะ

ตัวอย่าง 2.9 $13 = 3(4)+1$ โดยที่ $n = 4$

$7 = 3(2)+1$ โดยที่ $n = 2$

5) จำนวนเฉพาะใดๆในรูปแบบ $3n+1$ สามารถจัดให้อยู่ในรูปแบบ $6m+1$ ได้ด้วย เมื่อ $n \geq 1$

ตัวอย่าง 2.10 $13 = 3(4)+1 = 6(2)+1$ โดยที่ $m = 2$

$7 = 3(2)+1 = 6(1)+1$ โดยที่ $m = 1$

6) มีจำนวนเฉพาะมากเป็นจำนวนอนันต์ ที่อยู่ในรูปแบบ n^2-2 เมื่อ $n \geq 2$

ตัวอย่าง 2.11 $2 = 2^2-2$ โดยที่ $n = 2$

$7 = 3^2-2$ โดยที่ $n = 3$

7) จำนวนเฉพาะในรูปแบบ n^2-4 คือ 5 เท่านั้น

ตัวอย่าง 2.12 $5 = 3^2-4$ โดยที่ $n = 3$

8) จำนวนเฉพาะในรูปแบบ n^3-1 คือ 7 เท่านั้น

ตัวอย่าง 2.13 $7 = 2^3 - 1$ โดยที่ n = 2

9) ฟังก์ชันพหุนาม

$$2n^2 + 29$$

$$n^2 - n + 41$$

$$n^2 - 81n + 1681$$

$$n^2 - 79n + 1601$$

$$9n^2 - 231n + 1523$$

เป็นฟังก์ชันก่อกำเนิดจำนวนเฉพาะ สำหรับ n เป็นจำนวนเต็มบวก

ตัวอย่าง 2.14 ฟังก์ชัน $2n^2 + 29$: $31 = 2(1)^2 + 29$ โดยที่ n = 1

$37 = 2(2)^2 + 29$ โดยที่ n = 2

ฟังก์ชัน $n^2 - n + 41$: $41 = 1^2 - 1 + 41$ โดยที่ n = 1

$43 = 2^2 - 2 + 41$ โดยที่ n = 2

ฟังก์ชัน $n^2 - 81n + 1681$: $1523 = 2^2 - 81(2) + 1681$ โดยที่ n = 2

$1447 = 3^2 - 81(3) + 1681$ โดยที่ n = 3

ฟังก์ชัน $n^2 - 79n + 1601$: $1447 = 2^2 - 79(2) + 1601$ โดยที่ n = 2

$1373 = 3^2 - 79(3) + 1601$ โดยที่ n = 3

ฟังก์ชัน $9n^2 - 231n + 1523$: $1301 = 9(1)^2 - 231(1) + 1523$ โดยที่ n = 1

$1097 = 9(2)^2 - 231(2) + 1523$ โดยที่ n = 2

2.2.3.2 รูปแบบของจำนวนเฉพาะ (Prime's Forms)

- มีจำนวนเฉพาะที่ต่อเนื่องกัน 2-3 จำนวนที่อยู่ในรูปแบบต่อไปนี้

1) จำนวนเฉพาะ 2 จำนวนที่อยู่ในรูปแบบ (p , p+2) เรียกว่า คู่จำนวนเฉพาะหรือ Twin Prime

ตัวอย่าง 2.15 (3 , 5) = (3 , 3 + 2) โดยที่ p = 3

(5 , 7) = (5 , 5 + 2) โดยที่ p = 5

2) จำนวนเฉพาะ 3 จำนวนที่อยู่ในรูปแบบ (p , p+2 , p+4) เรียกว่า Triple Prime

ตัวอย่าง 2.16 (3 , 5 , 7) = (3 , 3+2 , 3+4) โดยที่ p = 3

3) จำนวนเฉพาะ 3 จำนวนที่อยู่ในรูปแบบ (p , p+2 , p+6) เรียกว่า Prime-Triplet

ตัวอย่าง 2.17 (5 , 7 , 11) = (5 , 5+2 , 5+6) โดยที่ p = 5

2.3 เศษส่วนต่อเนื่อง (Continued Fractions)

2.3.1 เศษส่วนต่อเนื่องจำกัด (Finite Continued Fractions)

นิยาม 2.5 เศษส่วนต่อเนื่องจำกัด เขียนในรูปแบบ

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

เมื่อ a_0 เป็นจำนวนเต็ม และ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มบวก เขียนแทนด้วย

$$[a_0; a_1, a_2, \ldots, a_n]$$

ตัวอย่าง 2.18 การเขียน 19/51 ในรูปเศษส่วนต่อเนื่อง

ใช้ขั้นตอนวิธีแบบวิธียุคลิด 19 กับ 51

$$51 = 2 \cdot 19 + 13 \quad \text{หรือ} \quad \frac{51}{19} = 2 + \frac{13}{19}$$

$$19 = 1 \cdot 13 + 6 \quad \text{หรือ} \quad \frac{19}{13} = 1 + \frac{6}{13}$$

$$13 = 2 \cdot 6 + 1 \quad \text{หรือ} \quad \frac{13}{6} = 2 + \frac{1}{6}$$

$$6 = 1 \cdot 6 + 0 \quad \text{หรือ} \quad \frac{6}{6} = 1$$

เมื่อใช้การแทนค่าจะได้

$$\frac{19}{51} = \frac{1}{\frac{51}{19}} = \frac{1}{2 + \frac{13}{19}} = \frac{1}{2 + \frac{1}{\frac{19}{13}}} = \frac{1}{2 + \frac{1}{1 + \frac{6}{13}}} = \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{13}{6}}}} = \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}}}$$

เมื่อใช้สัญลักษณ์แทน $\frac{19}{51}$ เขียนได้เป็น $[0; 2, 1, 2, 6]$

2.3.1 การลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่องจำกัด (k^{th} Convergent of Finite Continued Fraction)

นิยาม 2.6 เศษส่วนต่อเนื่องที่ได้จาก $[a_0; a_1, a_2, \ldots, a_n]$ โดยการหยุดการกระจายหลังจากตัวหารบางส่วน a_k ในลำดับที่ k เรียกว่า **การลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่อง** และแทนด้วย C_k

$$C_k = [a_0; a_1, a_2, \ldots, a_n], \ 1 \le k \le n$$

ให้ C_0 แทนการลู่เข้าที่ศูนย์ และ เท่ากับ a_0

ตัวอย่าง 2.19 กระจาย $\frac{19}{51} = [0; 2, 1, 2, 6]$ จะได้การลู่เข้าตามลำดับ คือ

$$C_0 = 0$$

$$C_1 = [0; 2] = 0 + \frac{1}{2} = \frac{1}{2}$$

$$C_2 = [0; 2, 1] = 0 + \frac{1}{2 + \frac{1}{1}} = \frac{1}{3}$$

$$C_3 = [0; 2, 1, 2] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}} = \frac{3}{8}$$

$$C_4 = [0; 2, 1, 2, 6] = \frac{19}{51}$$

- การคำนวณการลู่เข้าของเศษส่วนต่อเนื่องจำกัด $[a_0; a_1, a_2, \ldots, a_n]$ นั้น สามารถหลีกเลี่ยงการเขียนเศษและส่วน โดยกำหนดจำนวน p_k และ q_k (k = 0, 1, 2, ..., n) ดังต่อไปนี้

$$p_0 = a_0 \qquad q_0 = 1$$

$$p_1 = a_1 a_0 + 1 \qquad q_1 = a_1$$

$$p_k = a_k a_{k-1} + p_{k-2} \qquad q_k = a_k q_{k-1} + q_{k-2} \quad \text{เมื่อ } k = 2, 3, \ldots, n$$

ทฤษฎีบท 2.6 การลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่องเชิงเดียว $[a_0; a_1, a_2, \ldots, a_n]$ มีค่า

$$C_k = \frac{p_k}{q_k}, \ 0 \le k \le n$$

ตัวอย่าง 2.20 พิจารณา $\frac{19}{51} = [0; 2, 1, 2, 6]$

$p_0 = 0$ และ $q_0 = 1$

$p_1 = 2 \cdot 0 + 1 = 1$ $q_1 = 2$

$p_2 = 1 \cdot 1 + 0 = 1$ $q_2 = 1 \cdot 2 + 1 = 3$

$p_3 = 2 \cdot 1 + 1 = 3$ $q_3 = 2 \cdot 3 + 2 = 8$

$p_4 = 6 \cdot 3 + 1 = 19$ $q_4 = 6 \cdot 8 + 3 = 51$

จะได้การลู่เข้าของ $[0; 2, 1, 2, 6]$ คือ

$$C_0 = \frac{p_0}{q_0} = 0 \,,\; C_1 = \frac{p_1}{q_1} = \frac{1}{2} \,,\; C_2 = \frac{p_2}{q_2} = \frac{1}{3} \,,$$

$$C_3 = \frac{p_3}{q_3} = \frac{3}{8} \,,\; C_4 = \frac{p_4}{q_4} = \frac{19}{51}$$

2.4 ฟังก์ชันเชิงจำนวนและฟังก์ชันฟายของออยเลอร์ (Number Theoretic Functions and Euler Phi-Function)

2.4.1 ฟังก์ชันเชิงจำนวน (Number Theoretic Funcions)

2.4.1.1 ฟังก์ชันเทาและซิกมา (Tau and Sigma Function)

นิยาม 2.7 สำหรับจำนวนเต็มบวก n กำหนดให้ $\tau(n)$ แทนจำนวนตัวหารที่เป็นบวกของ n และ $\sigma(n)$ แทนผลบวกของตัวหารเหล่านี้

ตัวอย่าง 2.20 พิจารณา $n = 12$

เพราะว่า 12 มีตัวหารที่เป็นบวก คือ 1, 2, 3, 4, 6, 12 จะได้ว่า

$$\tau(12) = 6 \text{ และ } \sigma(12) = 1+2+3+4+6+12 = 28$$

ทฤษฎีบท 2.7 ถ้า $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ เป็นการแยกตัวประกอบเป็นจำนวนเฉพาะของจำนวนเต็ม $n > 1$ แล้ว

1) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$ และ

2) $\sigma(n) = \frac{p_1^{(k_1+1)} - 1}{p_1 - 1} \frac{p_2^{(k_2+1)} - 1}{p_2 - 1} \cdots \frac{p_r^{(k_r+1)} - 1}{p_r - 1}$

โดยที่ $i = 1, 2, \ldots, r$ แต่ละ k_i เป็นจำนวนเต็มบวกและแต่ละ p_i เป็นจำนวนเฉพาะที่ $p_1 < p_2 < \ldots < p_r$

ตัวอย่าง 2.22 จำนวนเต็มบวก $180 = 2^2 \cdot 3^2 \cdot 5$

มีตัวหารบวกทั้งหมด $\tau(180) = (2+1)(2+1)\cdots(1+1) = 18$

ผลบวกของตัวหารบวกเหล่านี้คือ

$$\sigma(180) = \frac{2^3-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^2-1}{5-1} = \frac{7}{1}\cdot\frac{26}{2}\cdot\frac{24}{4} = 7\cdot 13\cdot 6 = 546$$

คุณสมบัติที่น่าสนใจ ผลคูณของตัวหารบวกของจำนวนเต็ม $n>1$ มีค่าเท่ากับ $n^{\tau(n)/2}$ เขียนเป็นสัญลักษณ์แทนด้วย $\prod_{d|n} d$

$$\prod_{d|n} d = n^{\tau(n)/2}$$

โดยที่ d แทนตัวหารบวกใดๆของ n

หมายเหตุ จะใช้สูตรนี้ได้ก็ต่อเมื่อ $\tau(n)$ เป็นจำนวนคู่ หรือ n เป็นจำนวนกำลังสองสมบูรณ์

ตัวอย่าง 2.23 ผลคูณของตัวหารบวกของจำนวนเต็ม 16 (ได้แก่ 1, 2, 4, 8, 16) คือ

$$\prod_{d|16} d = 16^{5/2} = (4^2)^{5/2} = 4^5 = 1024$$

ผลคูณของตัวหารบวกของจำนวนเต็ม 6 (ได้แก่ 1, 2, 3, 6) คือ

$$\prod_{d|6} d = 6^{4/2} = 6^2 = 36$$

2.4.1.2 ฟังก์ชันมิว หรือ Mobius (Mu Function)

นิยาม 2.8 สำหรับจำนวนเต็มบวก n ฟังก์ชัน μ กำหนดโดย

$$\mu(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้า } p^2 \mid n \text{ สำหรับบางจำนวนเฉพาะ } p \\ (-1)^r & \text{ถ้า } n = p_1p_2\cdots p_r \text{ โดยที่ } p_i \text{ เป็นจำนวนเฉพาะที่แตกต่างกัน} \end{cases}$$

ตัวอย่างเช่น $\mu(1) = 1$

$\mu(2) = -1$

$\mu(6) = \mu((2)(3)) = (-1)^2 = 1$

$\mu(8) = 0$ เพราะ $(2)^2 \mid 8$

2.4.2 ฟังก์ชันฟายของออยเลอร์ (Euler Phi-Function)

นิยาม 2.9 สำหรับ $n \geq 1$ ให้ $\phi(n)$ แทนจำนวนเต็มบวกที่ไม่รวม n ซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับ n

ตัวอย่างเช่น จำนวนที่เป็นจำนวนเฉพาะสัมพัทธ์กับ 30 คือ 1 , 7 , 11 , 13 , 17 , 19 , 23 , 29 ดังนั้น $\phi(30) = 8$

ทฤษฎีบท 2.8 ถ้า p เป็นจำนวนเฉพาะ และ $k > 0$ แล้ว

$$\phi(p^k) = p^k - p^{k-1} = p^k(1-\frac{1}{p})$$

ตัวอย่าง 2.24 $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$ นั่นคือ มีจำนวนเต็มที่น้อยกว่าและเป็นจำนวนเฉพาะสัมพัทธ์กับ 9 ดังนี้ 1, 2, 4, 5, 7, 8

ทฤษฎีบท 2.9 ถ้าจำนวนเต็ม $n > 1$ มีการแยกตัวประกอบให้อยู่ในรูปผลคูณของจำนวนเฉพาะ $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ แล้ว

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\cdots(p_r^{k_r} - p_r^{k_r-1})$$

$$= n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$$

ตัวอย่าง 2.25 หาค่า $\phi(360)$

จากการแยกตัวประกอบให้อยู่ในรูปผลคูณของจำนวนเฉพาะ จะได้

$$360 = 2^3 \cdot 3^2 \cdot 5$$

ดังนั้น $\phi(360) = 360(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})$

$$= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$$

$$= 96$$

2.5 สมภาค (Congruences)

2.5.1 คุณสมบัติพื้นฐานของสมภาค (Basic Properties of Congruences)

นิยาม 2.10 ให้ n เป็นจำนวนเต็มบวกที่ถูกตรึงค่า จำนวนเต็ม a และ b เรียกว่า สมภาคมอดุโล n เขียนแทนด้วย

$$a \equiv b \pmod{n}$$

ถ้า n หาร $a-b$ ลงตัว นั่นคือ $a-b = kn$ สำหรับจำนวนเต็ม k บางจำนวน

ตัวอย่าง 2.26 ให้ $n = 5$

$4 \equiv 14 \pmod{5}$	เนื่องจาก	$4-14 = (-2)5$
$-6 \equiv 14 \pmod{5}$	เนื่องจาก	$-6-14 = (-4)5$
$-11 \equiv -36 \pmod{5}$	เนื่องจาก	$-11+36 = (5)5$

ทฤษฎีบท 2.10 ให้ $n > 1$ ถูกตรึง และ a, b, c, d เป็นจำนวนเต็มใดๆแล้ว คุณสมบัติต่อไปนี้เป็นจริง

1) $a \equiv a \pmod{n}$
2) ถ้า $a \equiv b \pmod{n}$ แล้ว $b \equiv a \pmod{n}$
3) ถ้า $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$ แล้ว $a \equiv c \pmod{n}$
4) ถ้า $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$ แล้ว $a+c \equiv b+d \pmod{n}$ และ $ac \equiv bd \pmod{n}$
5) ถ้า $a \equiv b \pmod{n}$ แล้ว $a+c \equiv b+c \pmod{n}$ และ $ac \equiv bc \pmod{n}$
6) ถ้า $a \equiv b \pmod{n}$ แล้ว $a^k \equiv b^k \pmod{n}$ โดยที่ k เป็นจำนวนเต็มบวก

2.5.2 สมภาคเชิงเส้น (Linear Congruences)

- สมการที่อยู่ในรูปแบบ $ax \equiv b \pmod{n}$ เรียกว่า สมภาคเชิงเส้น และผลเฉลยของสมการหมายถึง จำนวนเต็ม x_0 ซึ่ง $ax_0 \equiv b \pmod{n}$ ตัวอย่างเช่น $18x \equiv 30 \pmod{42}$

ทฤษฎีบท 2.11 สมภาคเชิงเส้น $ax \equiv b \pmod{n}$ มีผลเฉลย ก็ต่อเมื่อ $d \mid b$ โดยที่ $d = \gcd(a,n)$ ถ้า $d \mid b$ แล้ว d เป็นผลเฉลยไม่สมภาค(Mutually Incongruent) ร่วมมอดุโล n

ตัวอย่าง 2.27 สมภาคเชิงเส้น $18x \equiv 30 \pmod{42}$

เนื่องจาก $\gcd(18, 42) = 6$ และ 6 หาร 30 ลงตัว

ดังนั้นจึงมี 6 ผลเฉลยที่แท้จริง ซึ่งไม่สมภาค มอดุโล 42

จาก ผลเฉลยหนึ่งพบว่า $x = 4$ ดังนั้น

$$x \equiv 4 + \frac{42}{6}t \equiv 4 + 7t \pmod{42} \quad \text{โดยให้ } t = 0, 1, 2, 3, 4, 5$$

หรือ

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}$$

ทฤษฎีบท 2.12 ทฤษฎีบทเศษเหลือของชาวจีน (Chinese Remainder Theorem)

ให้ $n_1, n_2, \ldots, n_r$ เป็นจำนวนเต็มบวกซึ่ง $\gcd(n_i, n_j)$ เมื่อ $i \neq j$ แล้วระบบของสมภาคเชิงเส้น

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

มีผลเฉลยหลายชั้น (Simultaneous Solutions) ซึ่งเป็นมอดุโลจำนวนเต็ม $n_1, n_2, \ldots, n_r$ เพียงหนึ่งเดียวเท่านั้น

ตัวอย่าง 2.28 ระบบของสมภาค

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

จะได้ $n = 3 \cdot 5 \cdot 7 = 105$ และ

$$N_1 = \frac{n}{3} = \frac{105}{3} = 35, \quad N_2 = \frac{n}{5} = \frac{105}{5} = 21, \quad N_3 = \frac{n}{7} = \frac{105}{7} = 35$$

จะได้

$$35x \equiv 1 \pmod{3}, \quad 21x \equiv 1 \pmod{5}, \quad 15x \equiv 1 \pmod{7}$$

ซึ่งสอดคล้องเมื่อ $x_1 = 2, x_2 = 1, x_3 = 1$ ตามลำดับ

ดังนั้นผลเฉลยของระบบคือ $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$

เมื่อ มอดุโล 105 จะได้ผลเฉลยเดียวคือ $x = 233 \equiv 23 \pmod{105}$

2.5.3 สมภาคไม่เชิงเส้น (Non-Linear Congruences)

- สมภาคไม่เชิงเส้น คือระบบสมภาคที่อยู่ในรูปแบบ $ax^k \equiv b \pmod{n}$ ซึ่ง x เป็นจำนวนเต็มบวกที่มีดีกรีมากกว่า 1 ตัวอย่างเช่น $x^5 \equiv 1 \pmod{11}$

2.6 รากปฐมฐานและเลขชี้กำลัง (Primitive Roots and Indices)

2.6.1 อันดับของจำนวนเต็มมอดุโล n (Order of An Integer Modulo n)

นิยาม 2.11 ให้ $n>1$ และ $\gcd(a, n) = 1$ อันดับของ a มอดุโล n คือจำนวนเต็มบวก k ที่น้อยที่สุดซึ่งทำให้ $a^k \equiv 1 \pmod{n}$

ตัวอย่าง 2.29 พิจารณากำลังของ 2 มอดุโล 7

เราได้สมภาค

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1, \ldots \pmod{7}$$

ดังนั้น จำนวนเต็ม 2 มีอันดับ 3 (mod 7)

2.6.2 รากปฐมฐาน (Primitive Roots)

นิยาม 2.12 ถ้า $\gcd(a, n) = 1$ และ a เป็นของอันดับ $\phi(n)$ มอดุโล n แล้ว a เป็นรากปฐมฐานของจำนวนเต็ม n

กล่าวอีกอย่างว่า n มี a เป็นรากปฐมฐาน ถ้า $a^{\phi(n)} \equiv 1 \pmod{n}$ แต่ $a^k \not\equiv 1 \pmod{n}$ สำหรับจำนวนเต็มบวก k ทั้งหมดที่ $k < \phi(n)$

ตัวอย่าง 2.30 พิจารณากำลังของจำนวนเต็ม มอดุโล 7 ได้ว่า $\phi(7) = 6$

ให้ a = 2, กำลังของ 2 มอดุโล 7 จะได้

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1, \ldots \pmod{7}$$

ดังนั้น 2 ไม่เป็นรากปฐมฐานของ 7 เพราะ อันดับของ 2 คือ $3 \neq \phi(7)$

ให้ a = 3, กำลังของ 3 มอดุโล 7 จะได้

$$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1, \ldots \pmod{7}$$

ดังนั้น 3 เป็นรากปฐมฐานของ 7 เพราะ อันดับของ 3 คือ $6 = \phi(7)$

บทแทรก 2.13 ถ้า n มีรากปฐมฐาน แล้วจะมีเพียง $\phi(\phi(n))$ ของทั้งหมด

ตัวอย่าง 2.31 พิจารณา $n = 7$

ดังนั้น n มีรากปฐมฐานทั้งหมด $\phi(\phi(7)) = \phi(6) = 2$ จำนวน

นั่นคือ

ให้ $a = 2$ จะได้

$$2^1 \equiv 2 \pmod 7, 2^2 \equiv 4 \pmod 7, 2^3 \equiv 1 \pmod 7$$

ให้ $a = 3$ จะได้

$$3^1 \equiv 3 \pmod 7, 3^2 \equiv 2 \pmod 7, 3^3 \equiv 6 \pmod 7,$$

$$3^4 \equiv 4 \pmod 7, 3^5 \equiv 5 \pmod 7, 3^6 \equiv 1 \pmod 7$$

ให้ $a = 4$ จะได้

$$4^1 \equiv 4 \pmod 7, 4^2 \equiv 2 \pmod 7, 4^3 \equiv 1 \pmod 7$$

ให้ $a = 5$ จะได้

$$5^1 \equiv 5 \pmod 7, 5^2 \equiv 4 \pmod 7, 5^3 \equiv 6 \pmod 7,$$

$$5^4 \equiv 2 \pmod 7, 5^5 \equiv 3 \pmod 7, 5^6 \equiv 1 \pmod 7$$

ให้ $a = 6$ จะได้

$$6^1 \equiv 6 \pmod 7, 6^2 \equiv 1 \pmod 7$$

ดังนั้น 7 มีรากปฐมฐานทั้งหมด 2 ราก คือ 3 และ 5 เนื่องจากอันดับของ 3 และ 5 คือ $6 = \phi(7)$

2.6.3 เลขชี้กำลัง (Indices)

นิยาม 2.13 ให้ r เป็นรากปฐมฐานของ n ถ้า $\gcd(a, n) = 1$ แล้ว จำนวนเต็มบวกที่น้อยที่สุด k ซึ่งทำให้ $a \equiv r^k \pmod n$ เรียกว่า เลขชี้กำลังของ a สัมพัทธ์กับ r เขียนแทนด้วย $\text{ind}_r a$ หรือ $\text{ind}\ a$ โดยที่ $1 \le \text{ind}_r a \le \phi(n)$

ตัวอย่าง 2.32 จำนวนเต็ม 2 เป็นรากปฐมฐานของ 5

จะได้ว่า $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$, $2^4 \equiv 1 \pmod 5$

ดังนั้น $\text{ind}_2 1 = 4$, $\text{ind}_2 2 = 1$, $\text{ind}_2 3 = 3$, $\text{ind}_2 4 = 2$

ทฤษฎีบท 2.14 ถ้า r เป็นรากปฐมฐานของ n และ ind a แทนเลขชี้กำลังของ a สัมพัทธ์กับ r แล้วคุณสมบัติต่อไปนี้เป็นจริง

(1) $\text{ind}\,(ab) \equiv \text{ind}\,a + \text{ind}\,b$

(2) $\text{ind}\,a^k \equiv k \cdot \text{ind}\,a \pmod{\phi(n)}$

(3) $\text{ind}\,1 \equiv 0 \pmod{\phi(n)}$, $\text{ind}\,r \equiv 1 \pmod{\phi(n)}$

ทฤษฎีบท 2.15 ให้ n เป็นจำนวนเต็มและ $\gcd(a, n) = 1$ แล้วสมภาค $x^k \equiv b \pmod{n}$ มีผลเฉลย ก็ต่อเมื่อ

$$a^{\phi(n)/d} \equiv 1 \pmod{n} \text{ เมื่อ } d = \gcd(k, \phi(n))$$

ถ้ามีผลเฉลย ดังนั้นจะมีแน่นอน d ผลเฉลยมอดุโล n

ตัวอย่าง 3.33 สมภาค $x^5 \equiv 1 \pmod{11}$

มี $\gcd(1, 11) = 1$ แล้วจะได้ว่า $d = \gcd(5, \phi(11)) = 5$ และ $a^{\phi(11)/5} \equiv 1 \pmod{11}$

ดังนั้น สมภาค $x^5 \equiv 1 \pmod{11}$ มีผลเฉลยทั้งหมด 5 ผลเฉลย

บทที่ 3
การออกแบบโปรแกรม

ในการสร้างโปรแกรม จะประกอบด้วยโปรแกรมย่อยต่างๆ ซึ่งใช้ภาษาวิชวลเบสิกทำหน้าที่ในการรับค่าข้อมูล จัดการกับข้อมูล และแสดงผลออกทางจอภาพ

3.1 ระบบฮาร์ดแวร์และซอฟท์แวร์

การออกแบบโปรแกรมมีจุดมุ่งหมายเพื่อให้สามารถนำไปใช้กับคอมพิวเตอร์ที่มีใช้อย่างแพร่หลายได้โดยสะดวก จึงออกแบบเพื่อการพัฒนาบนสภาวะแวดล้อมดังนี้

1) ให้สามารถใช้งานบนระบบปฏิบัติการวินโดว์ XP
2) ให้สามารถใช้งานแบบผู้ใช้คนเดียว ไม่ต้องการระบบอินเตอร์เน็ต
3) คอมพิวเตอร์ที่มีหน่วยประมวลผลตระกูลอินเทลหรือเทียบเท่า

3.2 รายละเอียดของการออกแบบโปรแกรม

3.2.1 โครงสร้างโปรแกรม

โปรแกรมที่พัฒนาขึ้นนี้ มีการแบ่งโปรแกรมตามเนื้อหาที่รวบรวมและศึกษาเพื่อใช้การดำเนินการ แบ่งออกได้เป็น 9 หมวด ประกอบด้วย

1) **การหารลงตัว**
2) **การหาตัวหารร่วมมาก**
   - ด้วยขั้นตอนวิธีหาตัวหารร่วม
   - ด้วยขั้นตอนวิธีแบบยุคลิด
3) **การหาผลเฉลยสมการไดโอแฟนไทน์**
4) **จำนวนเฉพาะและจำนวนประกอบ**
   - การตรวจสอบจำนวนเฉพาะ
   - จำนวนครั้งการคำนวณการตรวจสอบจำนวนเฉพาะ
   - การคัดหาจำนวนเฉพาะของเอราทอสเทนีส
   - คุณสมบัติของจำนวน
     1) จำนวนเฉพาะ
        - หาจำนวนเฉพาะที่มากกว่าค่าที่รับมา
        - หาจำนวนเฉพาะที่น้อยกว่าค่าที่รับมา
        - การเขียนในรูปแบบทั่วไปของจำนวนเฉพาะที่รับมา

- หารูปแบบ Twin Prime
- หารูปแบบ Triple Prime
- การเขียนในรูปแบบทั่วไปของจำนวนเฉพาะที่รับมา

2) จำนวนประกอบ

- การเขียนในรูปแบบยกกำลังของจำนวนเฉพาะ
- การเขียนในรูปแบบทั่วไปของจำนวนประกอบที่รับมา

5) **เศษส่วนต่อเนื่อง**

- การกระจายเศษส่วนต่อเนื่องจำกัด
- การหาการลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่องจำกัด

6) **ฟังก์ชันเชิงจำนวน**

- การหาจำนวนตัวหารที่เป็นบวกทั้งหมดของจำนวนที่รับมา (τ) และผลบวกของตัวหารที่เป็นบวกของจำนวนที่รับมา (σ)
  - ผลคูณของตัวหารที่เป็นบวกของจำนวนที่รับมา
- การหาฟังก์ชันบนจำนวนเต็มบวก (μ)
- การหาจำนวนของจำนวนทั้งหมดซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับจำนวนที่รับมา (ϕ)

7) **สมภาค**

- การแสดงเศษเหลือของการหาร a^k ด้วย n
- การหาเศษเหลือของการหาร a^b ด้วย n
- การหาผลเฉลยสมภาคเชิงเส้น
  - การหาผลเฉลยสมภาคเชิงเส้น $ax \equiv b \pmod{n}$
  - การหาผลเฉลยสมภาคเชิงเส้น โดยใช้ทฤษฎีบทเศษเหลือชาวจีน
- การหาผลเฉลยสมภาคไม่เชิงเส้น $ax^k \equiv b \pmod{n}$

8) **รากปฐมฐานและเลขชี้กำลัง**

- อันดับของ a มอดุโล n
- การหารากปฐมฐาน
- การตรวจสอบการเป็นรากปฐมฐาน
- การหาเลขชี้กำลัง

9) **ตารางต่าง ๆ**

- ตารางจำนวนเฉพาะ 1000 จำนวนแรก
- ตารางฟังก์ชันเชิงจำนวน τ , σ, μ , ϕ
- ตารางอันดับของจำนวนเต็ม

- ตารางรากปฐมฐาน
- ตารางรากปฐมฐานที่น้อยที่สุด
- ตารางเลขชี้กำลัง

3.2.2 ออกแบบจอภาพของโปรแกรม

จอภาพของโปรแกรมประกอบด้วย 2 ลักษณะคือ เมนูเลือกหัวข้อการทำงาน และจอภาพประมวลผลจำนวนเต็ม ในจอภาพประมวลผลประกอบด้วย 3 ส่วนคือ

1) ส่วนนิยามและหลักการ
   - ความหมายหรืออธิบายนิยามและหลักการ
   - ตัวอย่าง
   - วิธีคิดหรือขั้นตอนการคำนวณ
2) ส่วนการคำนวณ โดยการรับค่าข้อมูลซึ่งเป็นการกำหนดค่าด้วยตนเอง ส่วนนี้จะนำข้อมูลที่รับเข้ามา มาทำการวิเคราะห์และคำนวณค่าต่างๆ
3) ส่วนแสดงผลลัพธ์ คือ การนำข้อมูลในส่วนที่สองมาแสดงผลทางจอภาพ

3.2.2.1 **เมนูหลัก** ในส่วนของจอภาพเมนูหลักเป็นการแสดงหัวข้อที่ต้องการจะศึกษาจะแบ่งออกเป็น 7 หัวข้อ คือ

1) ทฤษฎีการหารลงตัว
2) จำนวนเฉพาะและจำนวนประกอบ
3) เศษส่วนต่อเนื่อง
4) ฟังก์ชันเชิงจำนวน
5) สมภาค
6) รากปฐมฐานและเลขชี้กำลัง
7) ตารางต่างๆ

3.2.2.2 **ทฤษฎีบทการหารลงตัว** แบ่งเป็น 3 หัวข้อย่อยคือ

1) จอภาพการหารลงตัว

- **ส่วนนิยามและหลักการ** นำค่า a มาเป็นตัวตั้งและใช้ค่า b เป็นตัวหาร จะได้ผลหารให้เป็น q และเศษเหลือจากการหารให้เป็น r

- **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a และ b ซึ่งมีค่าไม่เกิน 9 หลัก โดยที่ $b > 0$ นำมาคำนวณ โดยใช้ทฤษฎีบท 2.1 และนิยาม 2.1

• **ส่วนแสดงผลลัพธ์** มี 2 ส่วน ดังนี้

- แสดงผลหาร q และเศษเหลือจากการหาร r

- แสดงว่า b หาร a ลงตัว หรือไม่ ถ้า r มีค่าเท่ากับศูนย์แสดงว่า b หาร a ลงตัว

2) **การหาตัวหารร่วมมาก** แบ่งเป็นอีก 2 หัวข้อย่อย คือ

2.1) **จอภาพการหาตัวหารร่วมมากด้วยขั้นตอนวิธีหาตัวหารร่วม**

• **ส่วนนิยามและหลักการ**

- นำค่า a มาหาตัวหารที่เป็นบวก

- นำค่า b มาหาตัวหารที่เป็นบวก

- หาตัวหารซึ่งเป็นตัวหารร่วมของทั้ง a และ b

- เลือกเอาตัวหารร่วมที่มีค่ามากที่สุด

• **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a และ b ซึ่งมีค่าไม่เกิน 5 หลัก โดยที่อย่างน้อยมีหนึ่งตัวที่มีค่าไม่เป็นศูนย์ นำมาคำนวณโดยใช้นิยาม 2.2

• **ส่วนแสดงผลลัพธ์** มี 4 ส่วนดังนี้

- แสดงจำนวนเต็มบวกที่น้อยกว่า a และหาร a ลงตัว

- แสดงจำนวนเต็มบวกที่น้อยกว่า b และหาร b ลงตัว

- แสดงจำนวนที่หารทั้ง a และ b ลงตัว

- แสดงค่า gcd(a, b)

2.2) **จอภาพการหาตัวหารร่วมมากด้วยขั้นตอนวิธีแบบยุคลิด**

• **ส่วนนิยามและหลักการ**

- นำค่า a มาหารด้วย b จะได้ว่าเริ่มต้นจะมี q_1 และ r_1 ซึ่งทำให้ $a = q_1b + r_1$

- ถ้า $r_1 = 0$ แล้ว $b \mid a$ และ $\gcd(a, b) = b$

- ถ้า $r_1 \neq 0$ ก็ให้ทำกระบวนการหารต่อเนื่องจนกระทั่งได้เศษเหลือเป็นศูนย์ เกิดเป็นระบบสมการดังนี้

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

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

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

$$\vdots$$

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

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

r_n ซึ่งเป็นเศษเหลือสุดท้ายที่ไม่เป็นศูนย์ จะมีค่าเท่ากับ gcd(a , b)

• **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a และ b ซึ่งมีค่าไม่เกิน 9 หลัก นำมาคำนวณโดยใช้ทฤษฎีบท 2.1 นิยาม 2.2 และบทตั้ง 2.2

• **ส่วนแสดงผลลัพธ์** มี 2 ส่วนดังนี้

- แสดงขั้นตอนตามขั้นตอนวิธีแบบยุคลิด
- แสดงค่า gcd(a, b)

3) **จอภาพการหาผลเฉลยสมการไดโอแฟนไทน์**

• **ส่วนนิยามและหลักการ**

- หา gcd(a , b) = d
- ถ้า d|c แล้ว สมการมีผลเฉลย
- ถ้า x_0 และ y_0 เป็นผลเฉลยเฉพาะของสมการแล้ว ผลเฉลยทั่วไปคือ

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

เมื่อ t เป็นจำนวนเต็มใดๆ (x_0 และ y_0 หาได้โดยใช้ขั้นตอนวิธีแบบยุคลิด)

• **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a, b และ c ซึ่งไม่เกิน 3 หลัก นำมาคำนวณโดยใช้ทฤษฎีบท 2.3

• **ส่วนแสดงผลลัพธ์** มี 2 ส่วนดังนี้

- แสดงขั้นตอนการคำนวณ ได้แก่ ขั้นตอนวิธีแบบยุคลิด และ ขั้นตอนการหาผลเฉลย
- แสดงผลเฉลยของสมการไดโอแฟนไทน์ ได้แก่ ผลเฉลยเฉพาะ และ ผลเฉลยทั่วไป

3.2.2.3 **จำนวนเฉพาะและจำนวนประกอบ** แบ่งเป็น 4 หัวข้อย่อย คือ

1) **จอภาพการตรวจสอบจำนวนเฉพาะ**

• **ส่วนนิยามและหลักการ** ตรวจสอบโดยใช้วิธีนำจำนวนเฉพาะที่น้อยกว่ารากที่สองของ n เป็นตัวหาร

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 2,000,000,000 นำมาคำนวณการตรวจสอบ

• **ส่วนแสดงผลลัพธ์** แสดงผลการตรวจสอบว่าเป็นจำนวนเฉพาะ หรือ จำนวนประกอบ

2) **จอภาพจำนวนครั้งการคำนวณการตรวจสอบจำนวนเฉพาะ**

• **ส่วนนิยามและหลักการ** ซึ่งมีวิธีการคำนวณ 4 วิธีดังนี้

- ใช้จำนวนเต็มบวกที่น้อยกว่า n เป็นตัวหาร
- ใช้จำนวนเต็มบวกคี่ที่น้อยกว่า n เป็นตัวหาร
- ใช้จำนวนเต็มบวกคี่ที่น้อยกว่ารากที่สองของ n เป็นตัวหาร
- ใช้จำนวนเฉพาะที่น้อยกว่ารากที่สองของ n เป็นตัวหาร

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 5 หลัก นำมาคำนวณการตรวจสอบ

• **ส่วนแสดงผลลัพธ์** มี 2 ส่วนดังนี้

- แสดงขั้นตอนการตรวจสอบ โดยแสดงจำนวนครั้งที่มีการหารและจำนวนแรกที่หารจำนวนที่รับลงตัวในแต่ละวิธีของการตรวจสอบและแสดงจำนวนเฉพาะที่น้อยกว่ารากที่สองของจำนวนที่รับมาที่นำมาใช้ในการตรวจสอบ
- แสดงผลลัพธ์จากการตรวจสอบว่า เป็นจำนวนเฉพาะหรือจำนวนประกอบ

3) **จอภาพการคัดหาจำนวนเฉพาะของเอราทอสเทนีส**

• **ส่วนนิยามและหลักการ** วิธีการเริ่มจากการคำนวณจำนวนเต็มจาก 2 ถึง n ตามลำดับ (ซึ่งจะพิจารณาเฉพาะจำนวนเต็มคี่ เพราะว่าจำนวนเฉพาะนอกจาก 2 แล้วจะเป็นจำนวนคี่เท่านั้น ดังนั้นจึงเป็นการพิจารณาว่าจำนวนเต็มคี่เป็นจำนวนเฉพาะหรือไม่) แล้วทำอย่างเป็นระบบด้วยการคัดออกของจำนวนประกอบทั้งหมดที่เป็นผลคูณในรูป $2p, 3p, 4p, 5p, \ldots$ เมื่อ p เป็นจำนวนเฉพาะที่ $p \le \sqrt{n}$ จำนวนที่เหลือที่ไม่ถูกคัดออกจะเป็นจำนวนเฉพาะ

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งมีค่ามากกว่า 2 แต่มีค่าไม่เกิน 3 หลัก (เนื่องจากการคำนวณโดยใช้หลักที่มากกว่านี้ โปรแกรมจะทำงานช้าลง)

• **ส่วนแสดงผลลัพธ์** จะแสดงผลลัพธ์ในรูปของตารางแสดงการคัดหาจำนวนเฉพาะของเอราทอสเทนีส

4) **จอภาพคุณสมบัติของจำนวน**

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งไม่เกิน 5 หลัก นำมาคำนวณตรวจสอบประเภทของจำนวน

• **ส่วนแสดงผลลัพธ์** จะแสดงประเภทของจำนวนว่าเป็นจำนวนเฉพาะหรือจำนวนประกอบ จากนั้นจะนำเข้าสู่จอภาพย่อยแสดงรูปแบบของจำนวน

4.1) **จอภาพการแสดงรูปแบบของจำนวนเฉพาะ**

• **ส่วนการคำนวณ** จะนำค่า n ที่รับมาในจอภาพคุณสมบัติของจำนวนมาใช้ในการคำนวณ

• **ส่วนแสดงผลลัพธ์** มี 4 ส่วนดังนี้

- แสดงจำนวนเฉพาะ 3 จำนวนที่มีค่าน้อยกว่าจำนวนที่รับมา
- แสดงจำนวนเฉพาะ 3 จำนวนที่มีค่ามากกว่าจำนวนที่รับมา
- แสดงรูปแบบทั่วไปของจำนวนเฉพาะ
- แสดงประเภทของจำนวนเฉพาะ
  - Twin Prime
  - Triple Prime
  - Prime-Triplet

4.2) **จอภาพการแสดงรูปแบบของจำนวนประกอบ**

• **ส่วนการคำนวณ** จะนำค่า n ที่รับมาในจอภาพคุณสมบัติของจำนวนมาใช้ในการคำนวณ

• **ส่วนแสดงผลลัพธ์** มี 2 ส่วนดังนี้

- แสดงรูปแบบของจำนวนที่รับมาในรูปยกกำลังของจำนวนเฉพาะ โดยใช้ทฤษฎีบท 2.4 และบทแทรก 2.5
- แสดงรูปแบบทั่วไปของจำนวนประกอบ

3.2.2.4 **เศษส่วนต่อเนื่อง** แบ่งเป็น 2 หัวข้อย่อยคือ

1) **จอภาพการกระจายเศษส่วนต่อเนื่องจำกัด**

• **ส่วนนิยามและหลักการ** นำค่า a มาหารด้วย b ตามขั้นตอนวิธีการหาตัวหารร่วมมากแบบยุคลิด ทำจนกระทั่งได้เศษเหลือมีค่าเป็นศูนย์ จากนั้นนำผลหารในแต่ละขั้นมาเขียนเป็นรูปแบบการกระจายเศษส่วนต่อเนื่องจำกัด

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก a และ b ไม่เกิน 5 หลัก นำมาคำนวณโดยใช้นิยาม 2.5

• **ส่วนแสดงผลลัพธ์** จะแสดงรูปแบบของการกระจายเศษส่วนต่อเนื่องจำกัด

2) **จอภาพการลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่องจำกัด**

• **ส่วนนิยามและหลักการ**

- นำค่า $a_0, a_1, a_2, \ldots, a_6$ ที่มีการรับค่าเข้ามา นำมาคำนวณตามสูตร

$$p_0 = a_0 \qquad q_0 = 1$$

$$p_1 = a_1a_0 + 1 \qquad q_1 = a_1$$

$$p_k = a_k a_{k-1} + p_{k-2} \qquad q_k = a_k q_{k-1} + q_{k-2} \text{ เมื่อ } k = 2, 3, \ldots, n$$

- คำนวณหาค่าการลู่เข้าที่ k จากสูตร

$$C_k = \frac{p_k}{q_k}, \ 0 \le k \le n$$

• **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a_0 และรับค่าจำนวนเต็มบวก $a_1, a_2, \ldots, a_6$ โดยในการรับค่าจะต้องมีอย่างน้อย a_0 และ a_1 นำมาคำนวณ โดยใช้นิยาม 2.6 และทฤษฎีบท 2.6

• **ส่วนแสดงผลลัพธ์** จะแสดงการลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่องจำกัด

3.2.2.5 **ฟังก์ชันเชิงจำนวน** แบ่งเป็น 3 หัวข้อย่อยคือ

1) **จอภาพการหาค่าฟังก์ชันเทาและซิกมา**

• **ส่วนนิยามและหลักการ**

- นำค่า n มาแจกแจงรูปแบบให้อยู่ในรูปยกกำลังของจำนวนเฉพาะตามทฤษฎีบท 2.4 และบทแทรก 2.5

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

- คำนวณหาค่า $\tau(n)$ จากสูตร

$$\tau(n) = (k_1 + 1)(k_2 + 1)\cdots(k_r + 1)$$

- คำนวณหาค่า $\sigma(n)$ จากสูตร

$$\sigma(n) = \frac{p_1^{(k_1+1)} - 1}{p_1 - 1} \frac{p_2^{(k_2+1)} - 1}{p_2 - 1} \cdots \frac{p_r^{(k_r+1)} - 1}{p_r - 1}$$

- คำนวณหาค่าผลคูณของตัวหารที่เป็นบวกทั้งหมด

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 5 หลัก นำมาคำนวณโดยใช้นิยาม 2.7 และทฤษฎีบท 2.7

• **ส่วนแสดงผลลัพธ์** มี 4 ส่วนดังนี้

- แสดงจำนวนที่รับมาในรูปแบบยกกำลังของจำนวนเฉพาะ
- แสดงตัวหารที่เป็นบวกทั้งหมดของจำนวนที่รับมา

- แสดงค่า $\tau(n)$ และ $\sigma(n)$
- แสดงค่าผลคูณของตัวหารที่เป็นบวกทั้งหมดของจำนวนที่รับมา

2) **จอภาพการหาค่าฟังก์ชันมิว**

• **ส่วนนิยามและหลักการ**

- ถ้า $n = 1$ ให้ค่า $\mu(n) = 1$
- ถ้ามีบางจำนวนเฉพาะ p ซึ่งทำให้ $p^2 \mid n$ ดังนั้น $\mu(n) = 0$
- ถ้า $n = p_1 p_2 \cdots p_r$ โดยที่ p_i เป็นจำนวนเฉพาะที่แตกต่างกัน ดังนั้น $\mu(n) = (-1)^r$

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 5 หลัก นำมาคำนวณโดยใช้นิยาม 2.8

• **ส่วนแสดงผลลัพธ์** จะแสดงค่า $\mu(n)$ ที่ได้จากการคำนวณ และแสดงเหตุผลประกอบ

3) **จอภาพการหาฟังก์ชันฟายของออยเลอร์**

• **ส่วนนิยามและหลักการ**

- นำค่า n มาแจกแจงรูปแบบให้อยู่ในรูปยกกำลังของจำนวนเฉพาะตามทฤษฎีบท 2.4 และบทแทรก 2.5

$$n = p_1^k p_2^k \cdots p_r^k$$

- นำค่า n มาคำนวณหา $\phi(n)$ จากสูตร

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r})$$

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 5 หลัก นำมาคำนวณด้วยใช้ นิยาม 2.9 และ ทฤษฎีบท 2.9

• **ส่วนแสดงผลลัพธ์** มี 2 ส่วนดังนี้

- แสดงจำนวนเต็มบวกซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับจำนวนที่รับมา
- แสดงค่า $\phi(n)$ ที่ได้จากการคำนวณ

3.2.2.6 **สมภาค** แบ่งเป็น 4 หัวข้อย่อย คือ

1) **จอภาพการแสดงเศษเหลือของการหาร a^k ด้วย n**

• **ส่วนนิยามและหลักการ** นำค่า a มายกกำลัง k แล้วหารด้วย n ซึ่ง $k = 1, 2, \ldots, n$

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n และจำนวนเต็ม a ซึ่งมีค่าไม่เกิน 2 หลัก นำมาคำนวณโดยใช้นิยาม 2.10 และทฤษฎีบท 2.10

• **ส่วนแสดงผลลัพธ์** มี 2 ส่วนดังนี้

- แสดง gcd(a , n)
- แสดงเศษเหลือทั้งหมดที่ได้จากการหาร a^k ด้วย n

2) **จอภาพการหาเศษเหลือของการหาร a^b ด้วย n**

• **ส่วนนิยามและหลักการ** นำค่า a มายกกำลัง b แล้วหารด้วย n

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ไม่เกิน 4 หลัก จำนวนเต็ม a และจำนวนเต็มบวก b ซึ่งมีค่าไม่เกิน 5 หลัก นำมาคำนวณโดยใช้นิยาม 2.10 และทฤษฎีบท 2.10

• **ส่วนแสดงผลลัพธ์** จะเป็นการแสดงการคำนวณหาเศษเหลือบางส่วนและแสดงค่าเศษเหลือจากการหาร a^b ด้วย n

3) **การหาผลเฉลยสมภาคเชิงเส้น** แบ่งเป็นอีก 2 หัวข้อย่อย คือ

3.1) **จอภาพการหาผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod n$**

• **ส่วนนิยามและหลักการ**

- คำนวณหา gcd(a , n) ให้มีค่าเป็น d
- ตรวจสอบว่า $d \mid b$ หรือไม่
- ถ้า $d \mid b$ แสดงว่า มีผลเฉลยที่ไม่สมภาคกัน d ผลเฉลย
- ถ้า $d \nmid b$ แสดงว่า สมภาคนี้ไม่มีผลเฉลย
- ในกรณีหาผลเฉลยได้ หาผลเฉลย x จาก
- นำรูปแบบ $ax \equiv b \pmod n$ มาลดรูป โดย $\frac{ax}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ จะได้รูปแบบ $a'x \equiv b' \pmod{n'}$
- หาตัวผกผันของ a ให้เป็น y จาก $a'y \equiv 1 \pmod{n'}$
- นำค่า y มาคูณกับ b' จะได้ $x_0 \equiv yb' \pmod{n'}$
- ผลเฉลยทั้งหมดคำนวณได้จาก $x \equiv x_0 + n't$, $t = 0, 1, 2, \ldots, d-1$

• **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a, b และ n ไม่เกิน 5 หลัก นำมาคำนวณโดยใช้ทฤษฎีบท 2.11

- **ส่วนแสดงผลลัพธ์** มี 2 ส่วนดังนี้
  - แสดงค่า gcd (a, n)
  - แสดงผลเฉลยของสมภาคเชิงเส้น

3.2) **จอภาพการหาผลเฉลยของระบบสมภาคเชิงเส้น (โดยใช้ทฤษฎีบทเศษเหลือของชาวจีน)**

- **ส่วนนิยามและหลักการ**
  - หาค่า n โดยที่ $n = n_1 n_2 n_3$
  - คำนวณค่า $N_1 = \frac{n}{n_1}$, $N_2 = \frac{n}{n_2}$, $N_3 = \frac{n}{n_3}$
  - คำนวณหาค่าผกผัน จาก

    $N_1 x_1 \equiv 1 \pmod{n_1}$, $N_2 x_2 \equiv 1 \pmod{n_2}$, $N_3 x_3 \equiv 1 \pmod{n_3}$
  - หาค่า x' จาก $x' = (a_1 N_1 x_1) + (a_2 N_2 x_2) + (a_3 N_3 x_3)$
  - จะได้ค่าผลเฉลย x ว่า $x \equiv x' \pmod{n}$

- **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a_1 , a_2 , a_3 และจำนวนเต็มบวก n_1 , n_2 , n_3 ซึ่ง $\gcd(n_1, n_2, n_3) = 1$ นำมาคำนวณโดยใช้ทฤษฎีบท 2.12

- **ส่วนแสดงผลลัพธ์** จะแสดงผลเฉลยของระบบสมภาคเชิงเส้นที่ได้จากการคำนวณ

4) **จอภาพการหาผลเฉลยของสมภาคไม่เชิงเส้น**

- **ส่วนนิยามและหลักการ** มีวิธีการคำนวณ 3 วิธี

วิธีที่ 1

1.1 เริ่มคำนวณหาค่า x จากการเริ่มให้ $x = 1$ **จนถึง** n ว่า ax^k หารด้วย n แล้วเหลือเศษเท่ากับ b หรือไม่

1.2 ถ้าเศษเหลือเท่ากับ b แสดงว่าค่า x นั้นเป็นผลเฉลยหนึ่งของสมการ (อาจมีผลเฉลยได้หลายค่า)

1.3 ถ้าเศษเหลือไม่เท่ากับ b แสดงว่าค่า x นั้นไม่ใช่ผลเฉลย

วิธีที่ 2 ใช้หลักการของเลขชี้กำลังโดยปรับสมการให้มีสัมประสิทธิ์ของ x^k เป็น 1 ก่อน ซึ่งมีหลักการดังนี้

2.1 ปรับสมการให้มีสัมประสิทธิ์ของ x^k เป็น 1

(1) หาค่า phi ซึ่ง phi $= \phi(n)$

(2) คูณ a^{ph-1} ทั้ง 2 ข้างของสมการ $ax^k \equiv b \pmod{n}$

$$a \cdot a^{phi-1} \cdot x^k \equiv b \cdot a^{phi-1} \pmod{n}$$

จะได้ $$x^k \equiv b \cdot a^{phi-1} \pmod{n}$$

(3) หาผลลัพธ์ของ $b \cdot a^{phi-1} \pmod{n}$ ให้มีค่าเป็น c

ดังนั้น $$x^k \equiv c \pmod{n}$$

2.2 ตรวจสอบว่า สมภาคมีผลเฉลยหรือไม่

ให้ $d = gcd(k, phi)$ แล้วพิจารณาว่า

ถ้า $a^{phi/d} \equiv 1 \pmod{n}$ แล้วจะมีผลเฉลยทั้งหมด d ผลเฉลย

2.3 หาผลเฉลยของ $x^k \equiv c \pmod{n}$ โดยหลักการของเลขชี้กำลัง ดังนี้

(1) หารากปฐมฐานของ n ให้มีค่าเป็น r

(2) หาหรือสร้างตารางเลขชี้กำลังของ c โดยใช้รากปฐมฐาน r

(3) โดยหลักการของเลขชี้กำลังจะได้

$$k \cdot ind_r x \equiv ind_r c \pmod{\phi(n)}$$

ให้ $m = ind_r c$ และ $y = ind_r x$

จะได้สมภาคใหม่เป็น

$$ky \equiv m \pmod{phi}$$

(4) หาค่า $m = ind_r c$ จากตารางเลขชี้กำลัง

(5) หาค่า y จาก $ky \equiv m \pmod{phi}$

ควรจะได้ y ทั้งหมด d จำนวนซึ่งหาโดยใช้หลักสมภาคเชิงเส้น นั่นคือ คูณ $k^{\phi(phi)-1}$ ทั้งสองข้างของสมการ จะได้

$$y \equiv m \cdot k^{\phi(phi)-1} \pmod{phi}$$

$$\equiv c \pmod{phi}$$

คำตอบอื่นๆของ y จะได้จากสูตร

$$y_i \equiv c + t \cdot \phi(phi) \pmod{phi} \; ; \; t = 0, 1, 2, \ldots, d-1$$

(6) หาค่า x จาก $y = ind_r x$ หรือ $r^y = x \pmod{n}$ ซึ่งก็คือการคำนวณหาเศษเหลือของการหาร r^y ด้วย n สำหรับแต่ละค่า y_i ที่ได้จาก (5) เศษเหลือที่ได้จะเป็นผลเฉลยของแต่ละค่า x (สำหรับการหาผลลัพธ์ x อาจจะใช้วิธีการอ่านค่าจากตารางเลขชี้กำลัง ถ้ามี)

วิธีที่ 3 ใช้หลักการของเลขชี้กำลังโดยที่ไม่ต้องปรับสมการให้มีสัมประสิทธิ์ของ x^k เป็น 1 ก่อน ซึ่งมีหลักการดังนี้

3.1 ใช้หลักการของเลขชี้กำลังกับสมภาค $ax^k \equiv b \pmod{n}$ จะได้

$$ind_r ax^k \equiv ind_r b \pmod{\phi(n)}$$

3.2 ใช้ทฤษฎีบทของเลขชี้กำลังจะได้ว่า

$$ind_r a + ind_r x^k \equiv ind_r b \pmod{\phi(n)}$$

$$ind_r a + k \cdot ind_r x \equiv ind_r b \pmod{\phi(n)}$$

ให้ $y = ind_r x$ จะได้ว่า

$$ky \equiv ind_r b - ind_r a \pmod{\phi(n)}$$

ให้ $m = ind_r b - ind_r a$ จะได้ว่า

$$ky \equiv m \pmod{\phi(n)}$$

3.3 หาค่า $m = ind_r b - ind_r a$ จากตารางเลขชี้กำลัง

3.4 จากนั้นทำตามขั้นตอนย่อย (5) และ (6) ในขั้นตอนการหาผลเฉลยของวิธีที่ 2 ข้อ (2.3) จะได้ผลเฉลย x ของสมภาคไม่เชิงเส้น

• **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a, k, b และ n ซึ่งมีค่าไม่เกิน 5 หลัก นำค่าที่ได้มาคำนวณ

• **ส่วนแสดงผลลัพธ์** จะแสดงผลเฉลยของสมภาคไม่เชิงเส้นที่ได้จากการคำนวณ หากได้เศษเหลือไม่เท่ากับ b จะแสดงว่าสมภาคเชิงเส้นนี้ไม่มีผลเฉลย

3.2.2.7 **รากปฐมฐานและเลขชี้กำลัง** แบ่งเป็น 4 หัวข้อย่อยคือ

1) **จอภาพการหาอันดับของ a มอดุโล n**

• **ส่วนนิยามและหลักการ**

- หาค่า gcd(a , n) ให้เป็น d
- ถ้า d = 1 แสดงว่า หาอันดับได้
- ถ้า $d \neq 1$ แสดงว่า หาอันดับไม่ได้
- ถ้าหาอันดับได้ ให้คำนวณหาค่า k ตัวแรกซึ่งทำให้ $a^k \equiv 1 \pmod{n}$ โดยที่ $1 \leq k \leq n-1$

• **ส่วนการคำนวณ** รับค่าจำนวนเต็ม a และ n โดยที่ n >1 ซึ่งมีค่าไม่เกิน 4 หลัก นำมาคำนวณโดยใช้นิยาม 2.11

• **ส่วนแสดงผลลัพธ์** มี 3 ส่วนดังนี้

- แสดงค่า gcd(a, n) ถ้า gcd(a , n) = 1 จะแสดงว่า **หาอันดับได้** หาก gcd(a , n) ≠ 1 จะแสดงว่า หาอันดับไม่ได้
- แสดงค่า k ที่คำนวณได้
- สรุปค่าอันดับของ a มอดุโล n

2) **จอภาพการหารากปฐมฐาน**

• **ส่วนนิยามและหลักการ**

- หา $\phi(n)$
- คำนวณ $a^{\phi(n)} \mod n$ โดยที่ a = 2, 3, ..., n-1
- ถ้า $a^{\phi(n)} \equiv 1 \pmod{n}$ แล้ว a เป็นรากปฐมฐาน

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 3 หลัก นำมาคำนวณโดยใช้นิยาม 2.12 และบทแทรก 2.13

• **ส่วนแสดงผลลัพธ์** มี 3 ส่วนดังนี้

- แสดงค่า $\phi(n)$
- แสดงว่า หามี $a^{\phi(n)} \equiv 1 \pmod{n}$ หรือไม่ ถ้ามีแสดงว่า n **มีรากปฐมฐาน**
- แสดงจำนวนรากปฐมฐาน

3) **จอภาพการตรวจสอบการเป็นรากปฐมฐาน**

• **ส่วนนิยามและหลักการ**

- ตรวจสอบว่า gcd(a , n) = 1 หรือไม่
- หา $\phi(n)$
- คำนวณ $a^k \equiv 1 \pmod{n}$ โดย a = 2, 3, ..., n-1 **และ** $1 \le k \le \phi(n)$
- ถ้า $k = \phi(n)$ แล้ว a เป็นรากปฐมฐานของ n

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก a และ n ซึ่งมีค่าไม่เกิน 2 หลัก นำมาคำนวณโดยใช้นิยาม 2.12

• **ส่วนแสดงผลลัพธ์** มี 3 ส่วนดังนี้

- ตรวจสอบว่า gcd(a , n) = 1 หรือไม่ ถ้าไม่แสดงว่า a **ไม่เป็นรากปฐมฐานของ** n
- แสดงค่า $\phi(n)$
- แสดงว่า $a^k \equiv 1 \pmod{n}$ แล้ว $k = \phi(n)$ **หรือไม่**
- สรุปจากการตรวจสอบว่า a **เป็นรากปฐมฐานของ n หรือไม่**

4) **จอภาพการหาเลขชี้กำลัง**

• **ส่วนนิยามและหลักการ**

- หารากปฐมฐาน r ของ n โดยเลือกใช้รากปฐมฐานตัวแรก
- หาค่าจำนวนเต็มบวก k ที่น้อยที่สุดซึ่ง $a \equiv r^k \pmod{n}$

• **ส่วนการคำนวณ** รับค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 500 นำมาคำนวณโดยใช้นิยาม 2.13 และทฤษฎีบท 2.14

• **ส่วนแสดงผลลัพธ์** มี 3 ส่วนดังนี้

- แสดงรากปฐมฐานที่น้อยที่สุดของค่า n ที่รับมา หาก n ไม่มีรากปฐมฐาน ก็จะไม่มีการแสดงเลขชี้กำลัง
- แสดงการคำนวณหาเศษเหลือของการหาร r^k ด้วย n
- แสดงตารางเลขชี้กำลังที่ได้จากการคำนวณ

3.2.2.8 **ตารางต่างๆ** ประกอบด้วย 6 ตาราง**คือ**

- ตารางจำนวนเฉพาะ
- ตารางฟังก์ชันเชิงจำนวน
- ตารางอันดับของจำนวนเต็ม
- ตารางรากปฐมฐาน
- ตารางรากปฐมฐานที่น้อยที่สุด
- ตารางเลขชี้กำลัง

3.2.3 **ออกแบบจอภาพการแสดงนิยามและหลักการ** แบ่งเป็น 3 **หัวข้อย่อยคือ**

- ความหมายหรือการอธิบายนิยามหลักการ
- ตัวอย่าง
- วิธีคิด

3.2.4 **ออกแบบการตรวจสอบเงื่อนไขการป้อนค่าข้อมูล** มีการตรวจสอบเงื่อนไขในการป้อนค่าข้อมูลดังนี้

- การตรวจสอบการป้อนค่าเป็นช่องว่าง
- การตรวจสอบการป้อนค่าเป็นตัวอักษร
- การตรวจสอบการป้อนเครื่องหมาย " , "

- การตรวจสอบการป้อนจุดทศนิยม " . "
- การตรวจสอบการป้อนค่าเกินจำนวนหลักที่กำหนดไว้

บทที่ 4
ผลการพัฒนาโปรแกรม

โปรแกรมการคำนวณจำนวนเต็มนี้เขียนขึ้นด้วยภาษาวิชวลเบสิค เวอร์ชั่น 6.0 ประกอบด้วยรายละเอียด ดังนี้

4.1 การเข้าโปรแกรม ประกอบด้วย

• ปุ่มเข้าสู่โปรแกรม ปุ่มผู้พัฒนาโปรแกรม ชื่อของคณะ ชื่อภาควิชาและชื่อของสถาบัน แสดงดังรูปที่ 4.1

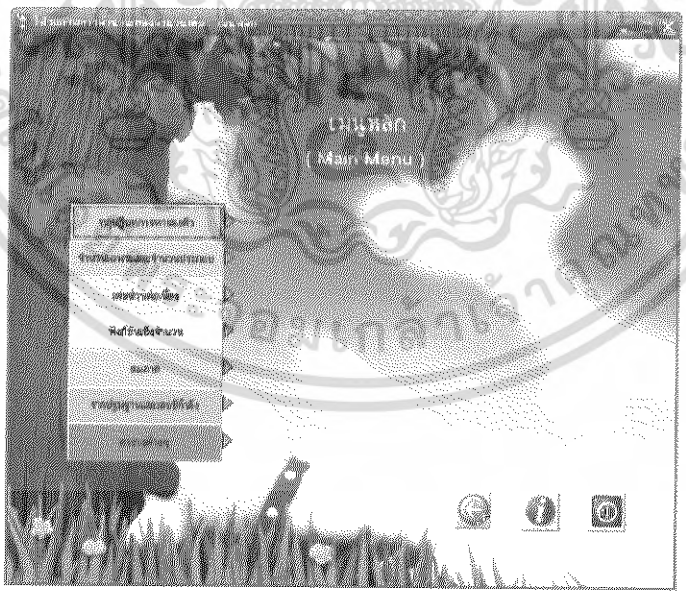
รูปที่ 4.1 จอภาพของโปรแกรมการคำนวณของจำนวนเต็ม

- เมื่อกดปุ่มผู้พัฒนาโปรแกรมจะแสดงจอภาพเกี่ยวกับผู้พัฒนาโปรแกรม แสดงดังรูปที่ 4.2

รูปที่ 4.2 จอภาพผู้พัฒนาโปรแกรมการคำนวณของจำนวนเต็ม

4.2 เมนูหลัก

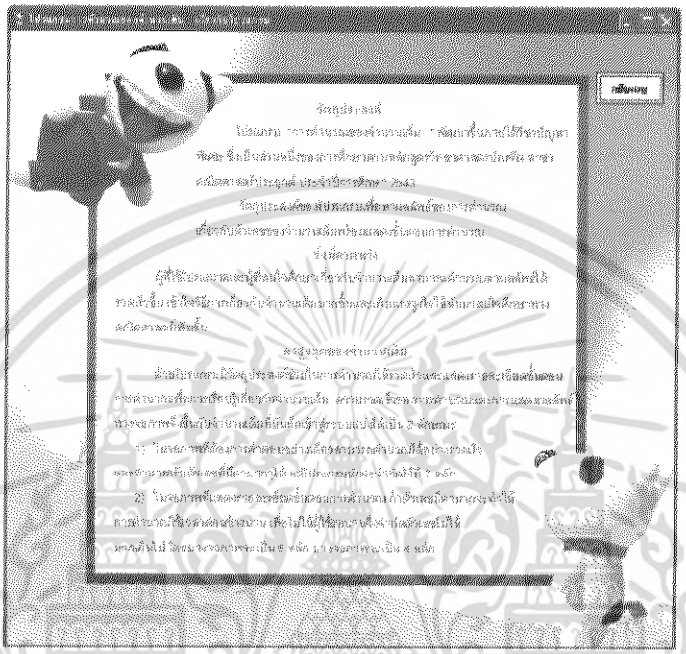
- ในจอภาพเมนูหลักจะมีปุ่มแสดงหัวข้อของจอภาพเรื่องต่างๆ ที่สามารถเชื่อมกับทุกจอภาพในโปรแกรมได้ แสดงดังรูปที่ 4.3



รูปที่ 4.3 จอภาพเมนูหลัก

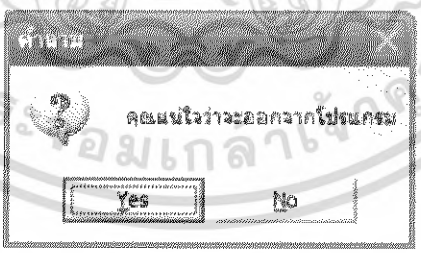
- เมื่อกดปุ่ม  จะเป็นการย้อนกลับไปยังหน้าจอแรกของโปรแกรมการคำนวณของจำนวนเต็ม

- เมื่อกดปุ่ม  จะแสดงจอภาพรายละเอียดเกี่ยวกับโปรแกรม แสดงดังรูปที่ 4.4



รูปที่ 4.4 จอภาพเกี่ยวกับโปรแกรม

- เมื่อกดปุ่ม  จะเป็นการออกจากโปรแกรม แสดงดังรูปที่ 4.5

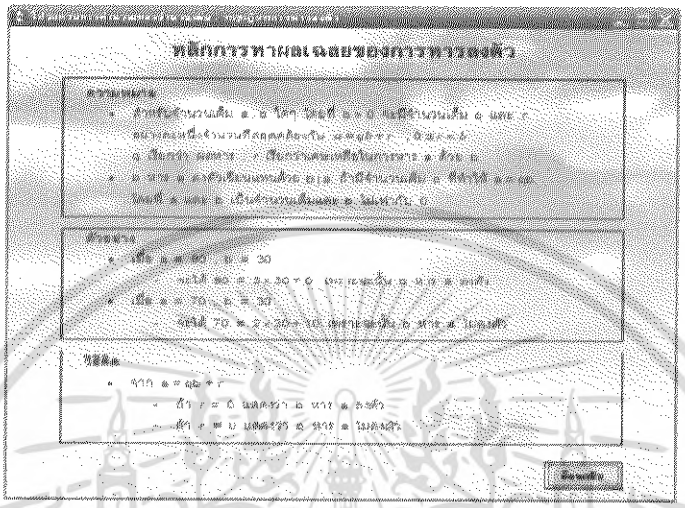


รูปที่ 4.5 จอภาพการออกจากโปรแกรม

4.3 ทฤษฎีบทการหารลงตัว

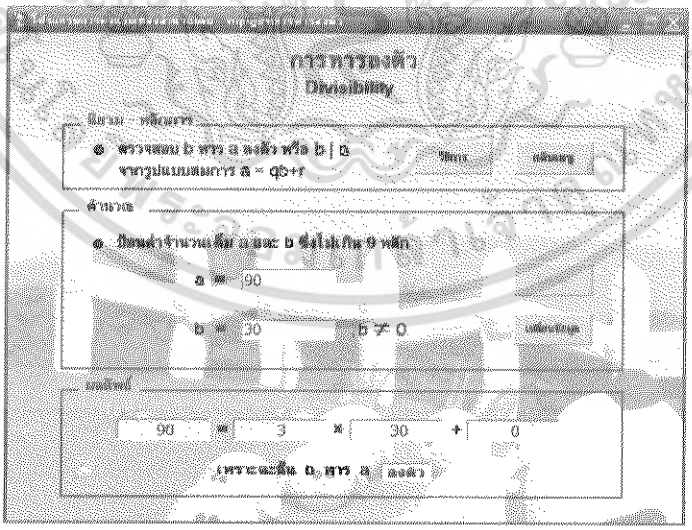
4.3.1 จอภาพการหารลงตัว

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาผลเฉลยของการหารลงตัว แสดงดังรูปที่ 4.6



รูปที่ 4.6 จอภาพนิยามและหลักการของการหารลงตัว

ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a และ b ซึ่งมีค่าไม่เกิน 9 หลัก โดยที่ $b > 0$ แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.7

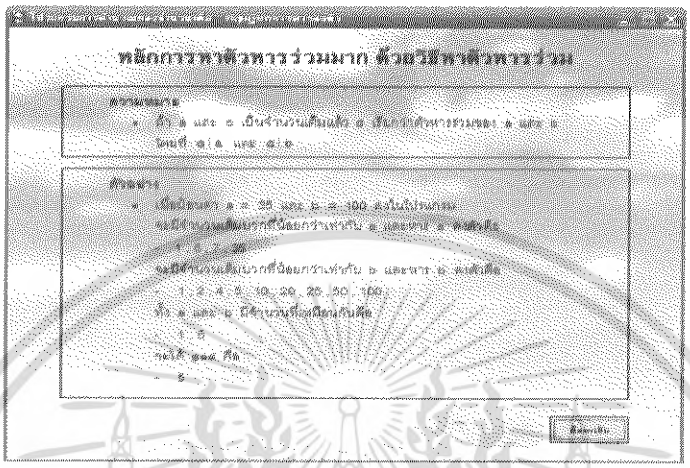


รูปที่ 4.7 จอภาพการหารลงตัว

4.3.2 จอภาพการหาตัวหารร่วมมาก

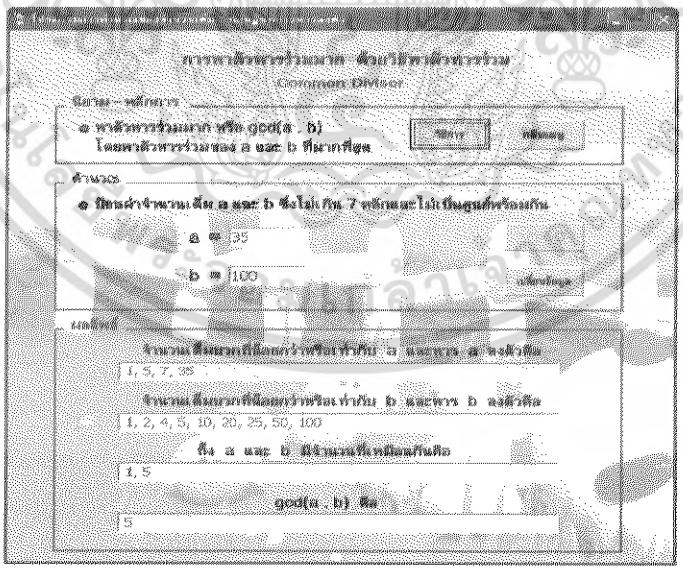
1) ด้วยวิธีหาตัวหารร่วม

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาผลเฉลยของ gcd โดยวิธีหารร่วม แสดงดังรูปที่ 4.8



รูปที่ 4.8 จอภาพนิยามและหลักการของการหาตัวหารร่วมมากด้วยวิธีหาตัวหารร่วม

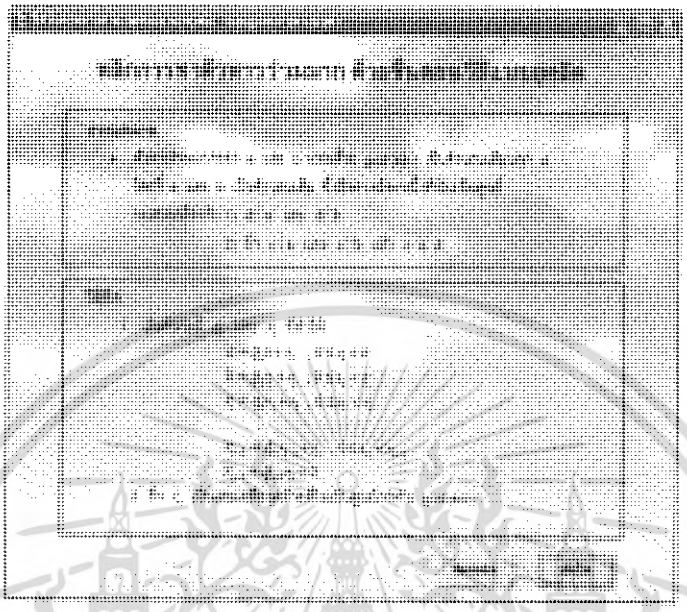
ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a และ b ซึ่งมีค่าไม่เกิน 7 หลัก โดยที่อย่างน้อยมีหนึ่งตัวที่มีค่าไม่เป็นศูนย์ แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.9



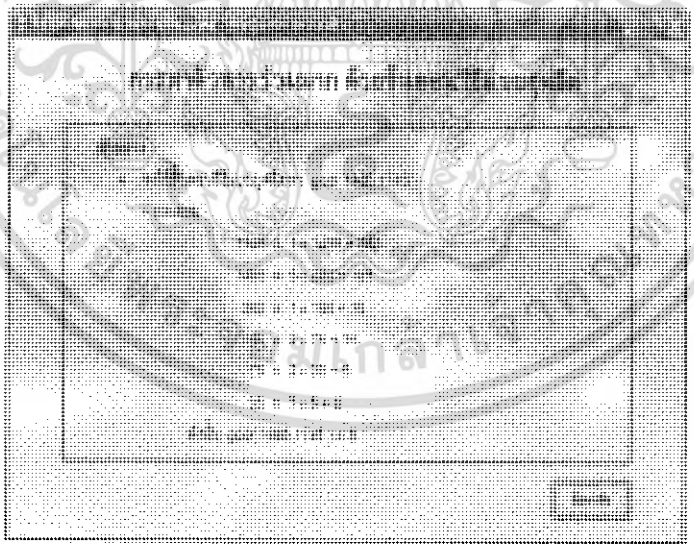
รูปที่ 4.9 จอภาพการหาตัวหารร่วมมาก ด้วยวิธีหาตัวหารร่วม

2) **ด้วยขั้นตอนวิธีแบบยุคลิด**

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหา gcd โดยวิธียุคลิด แสดงดังรูปที่ 4.10 และรูปที่ 4.11

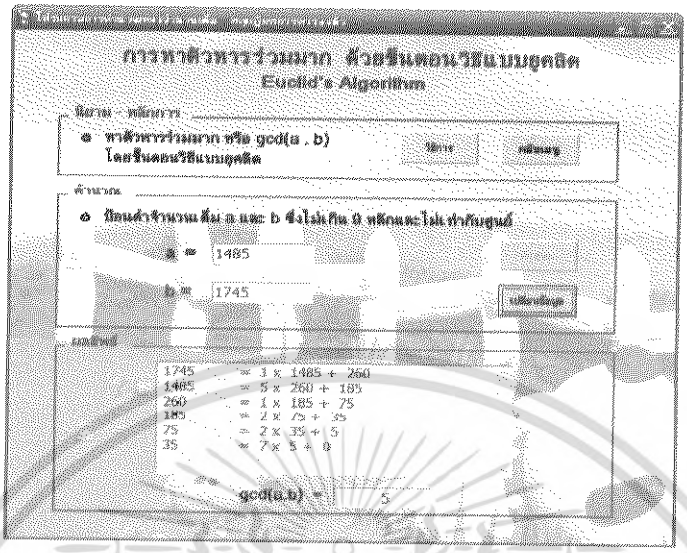


รูปที่ 4.10 จอภาพนิยามและหลักการของการหาตัวหารร่วมมาก ด้วยขั้นตอนวิธีแบบยุคลิด



รูปที่ 4.11 จอภาพนิยามและหลักการของการหาตัวหารร่วมมาก ด้วยขั้นตอนวิธีแบบยุคลิด(ต่อ)

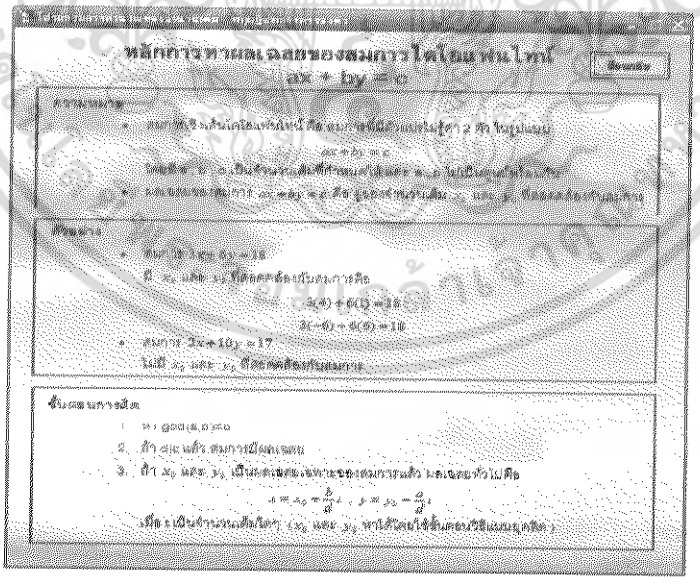
ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a และ b ซึ่งมีค่าไม่เกิน 9 หลัก แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.12



รูปที่ 4.12 จอภาพการหาตัวหารร่วมมาก ด้วยขั้นตอนวิธีแบบยุคลิด

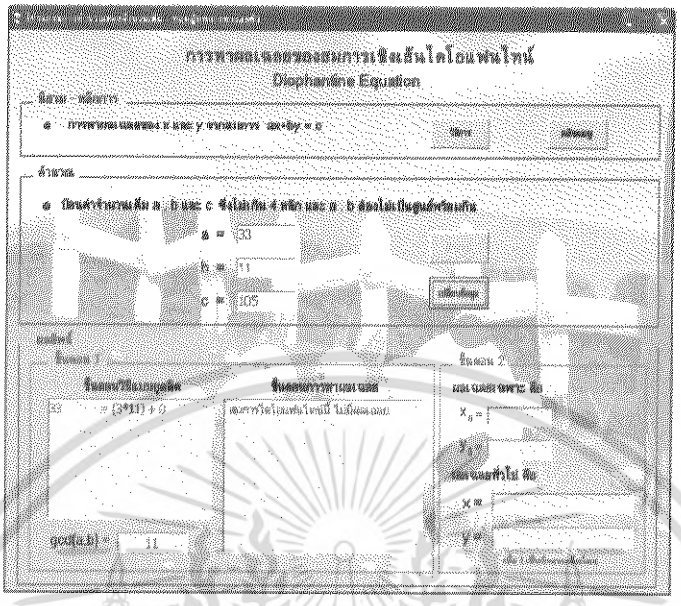
4.3.3 จอภาพการหาผลเฉลยสมการไดโอแฟนไทน์

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาผลเฉลยของสมการไดโอแฟนไทน์ แสดงดังรูปที่ 4.13

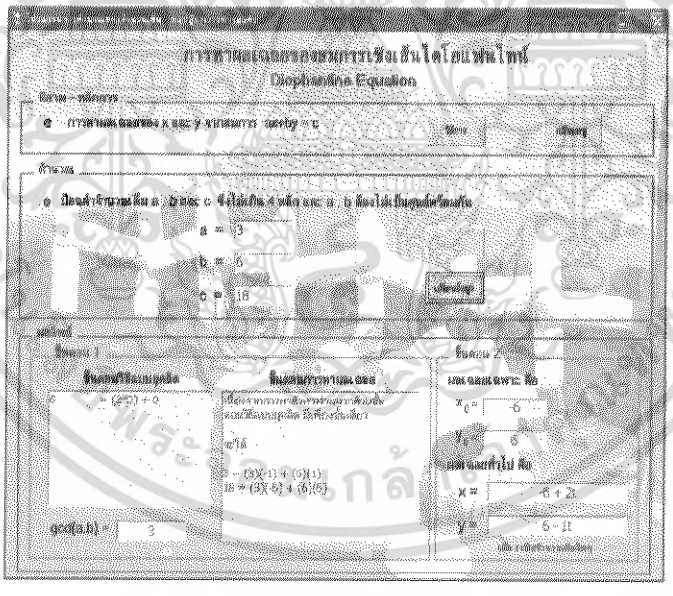


รูปที่ 4.13 จอภาพหลักการและนิยามของการหาผลเฉลยของสมการไดโอแฟนไทน์

ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม 3 จำนวน คือ ค่า a, b และ c ซึ่งมีค่าไม่เกิน 4 หลัก แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.14 และรูปที่ 4.15



รูปที่ 4.14 จอภาพการหาผลเฉลยของสมการไดโอแฟนไทน์ ในกรณีไม่มีผลเฉลย

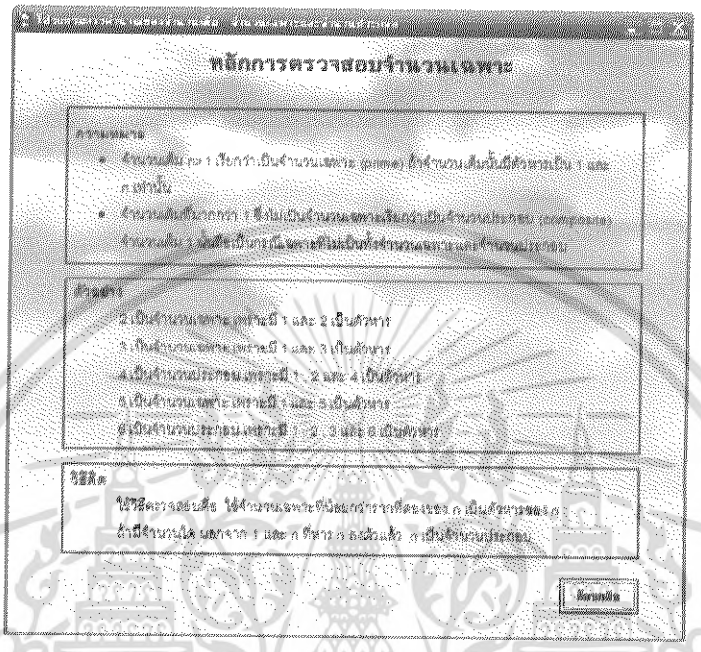


รูปที่ 4.15 จอภาพการหาผลเฉลยของสมการไดโอแฟนไทน์ ในกรณีมีผลเฉลย

4.4 จำนวนเฉพาะและจำนวนประกอบ

4.4.1 จอภาพการตรวจสอบจำนวนเฉพาะ

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการตรวจสอบจำนวนเฉพาะ แสดงดังรูปที่ 4.16

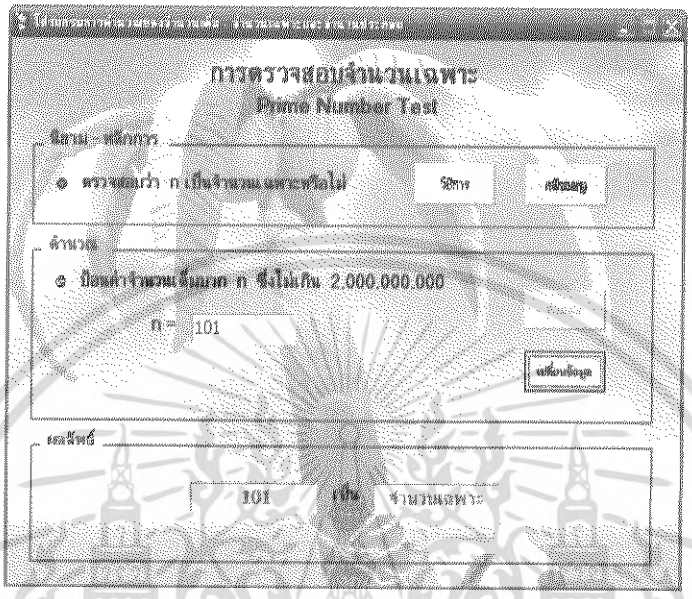


รูปที่ 4.16 จอภาพนิยามและหลักการของการตรวจสอบจำนวนเฉพาะ

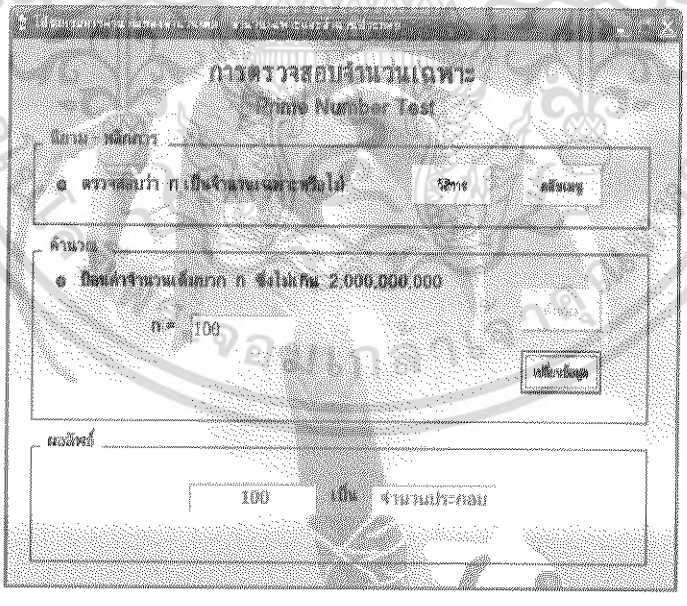
ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 5 หลัก ผลจากการตรวจสอบเกิดได้ 2 กรณี คือ

1) ตรวจสอบจำนวนเต็ม n แล้วผลที่ได้ n เป็นจำนวนเฉพาะ แสดงดังรูปที่ 4.17

2) การตรวจสอบจำนวนเต็ม n แล้วผลที่ได้ n เป็นจำนวนประกอบ แสดงดังรูปที่ 4.18



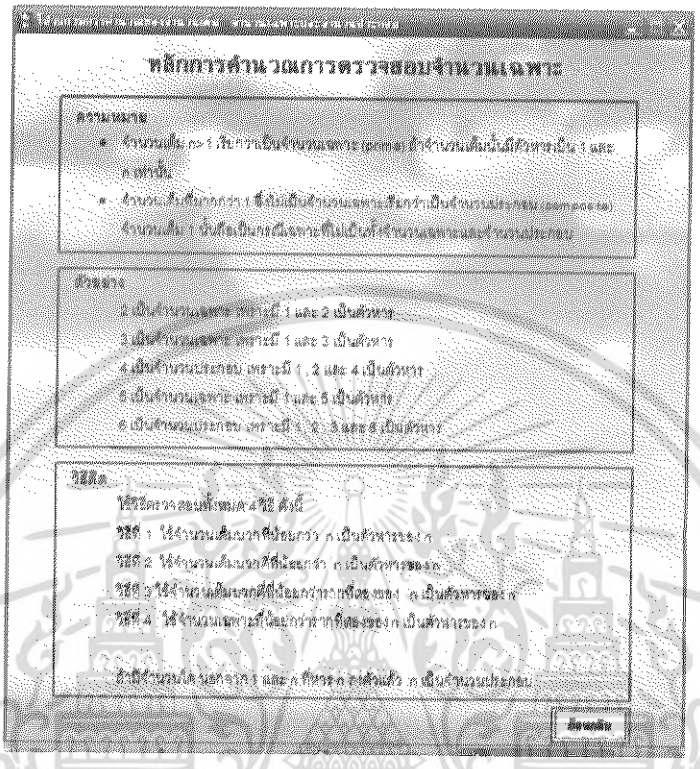
รูปที่ 4.17 จอภาพการตรวจสอบการเป็นจำนวนเฉพาะของ 101



รูปที่ 4.18 จอภาพการตรวจสอบการเป็นจำนวนเฉพาะของ 100

4.4.2 **จอภาพจำนวนครั้งการคำนวณการตรวจสอบจำนวนเฉพาะ**

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการคำนวณการตรวจสอบจำนวนเฉพาะ แสดงดังรูปที่ 4.19

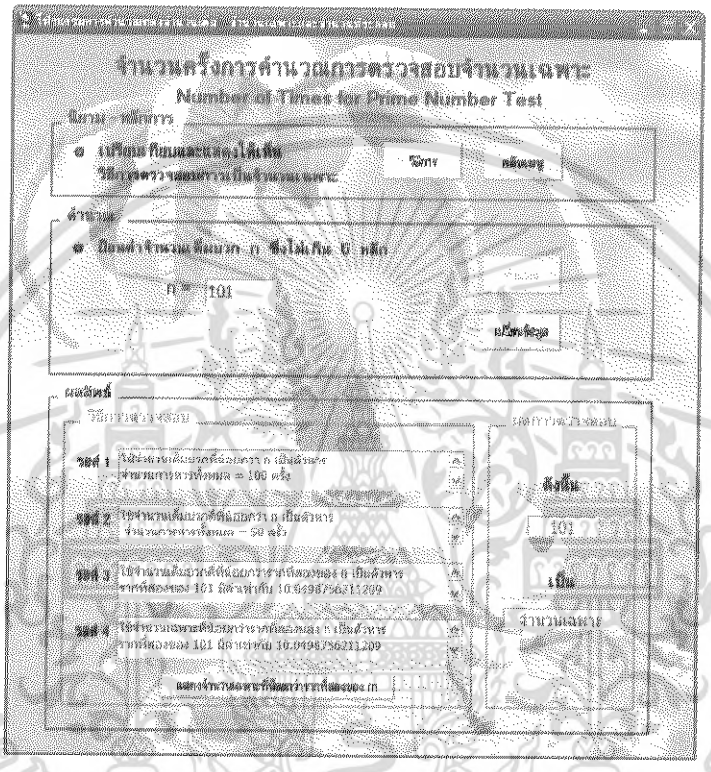


รูปที่ 4.19 จอภาพนิยามและหลักการของการคำนวณการตรวจสอบจำนวนเฉพาะ

ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 5 หลัก ผลจากการตรวจสอบเกิดได้ 2 กรณี คือ

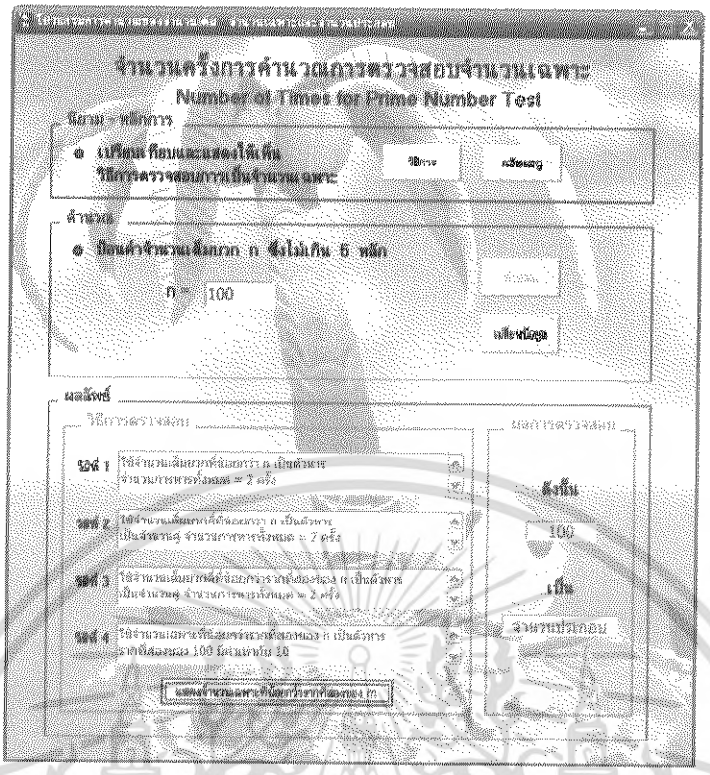
1) ตรวจสอบจำนวนเต็ม n แล้วผลที่ได้ n เป็นจำนวนเฉพาะ แสดงดังรูปที่ 4.20 และรูปที่ 4.21

2) การตรวจสอบจำนวนเต็ม n แล้วผลที่ได้ n เป็นจำนวนประกอบ แสดงดังรูป 4.22 และรูปที่ 4.23



รูปที่ 4.20 จอภาพแสดงจำนวนครั้งการคำนวณการตรวจสอบจำนวนเฉพาะของ 101

รูปที่ 4.21 จอภาพแสดงจำนวนเฉพาะที่น้อยกว่ารากที่สองของ 101



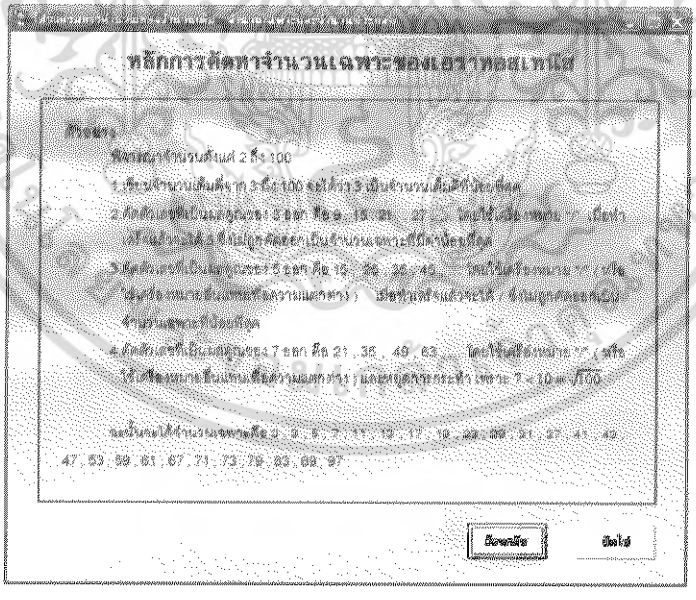
รูปที่ 4.22 จอภาพแสดงจำนวนครั้งการคำนวณการตรวจสอบจำนวนเฉพาะของ 100

รูปที่ 4.23 จอภาพแสดงจำนวนเฉพาะที่น้อยกว่ารากที่สองของ 100

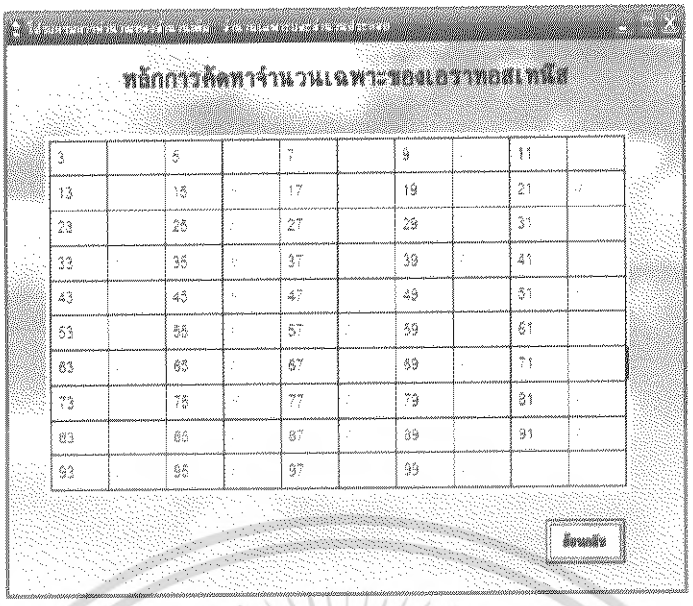
4.4.3 **จอภาพการคัดหาจำนวนเฉพาะของเอราทอสเทนีส**

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการคัดหาจำนวนเฉพาะของเอราทอสเทนีส แสดงดังรูปที่ 4.24 รูปที่ 4.25 และรูปที่ 4.26

รูปที่ 4.24 จอภาพนิยามและหลักการของการคัดหาจำนวนเฉพาะของเอราทอสเทนีส



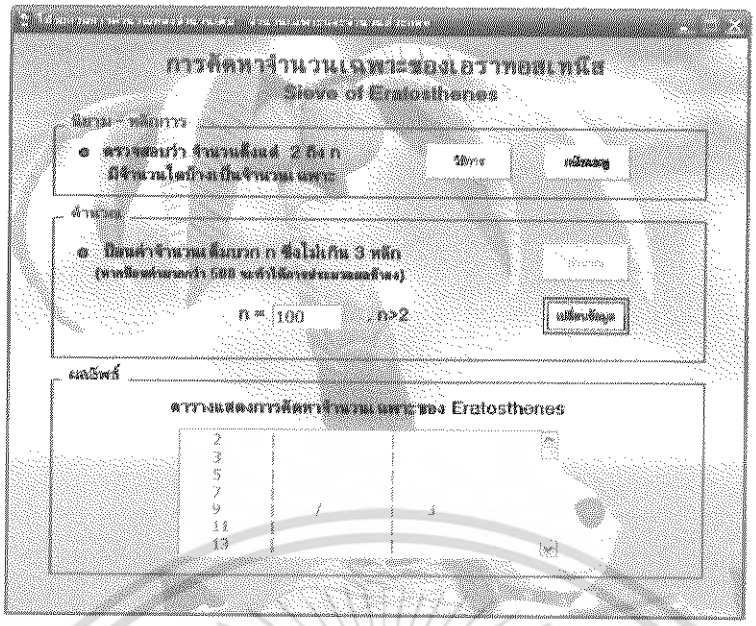
รูปที่ 4.25 จอภาพนิยามและหลักการของการคัดหาจำนวนเฉพาะของเอราทอสเทนีส(ต่อ)



รูปที่ 4.26 จอภาพนิยามและหลักการของการคัดหาจำนวนเฉพาะของเอราทอสเทนีส(ต่อ)

ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก n ซึ่งมีค่ามากกว่า 2 แต่มีค่าไม่เกิน 500 แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.27 และรูปที่ 4.28

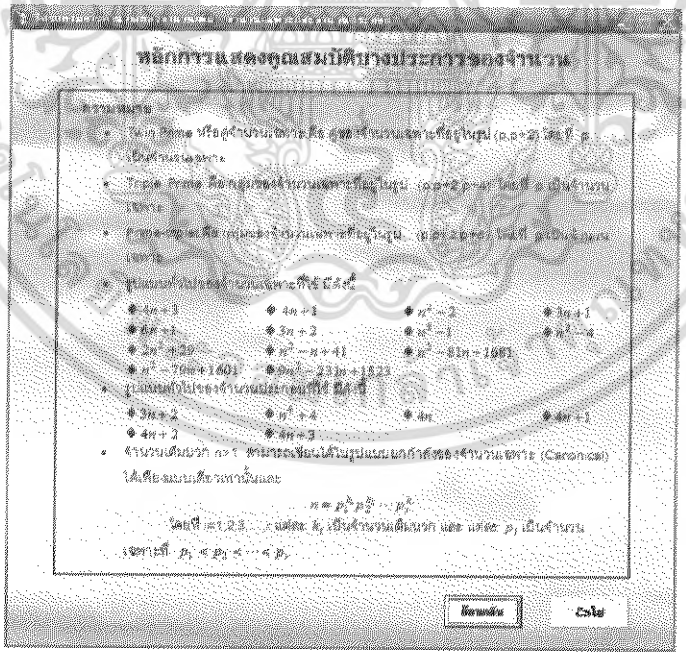
รูปที่ 4.27 จอภาพหมายเหตุของการคัดหาจำนวนเฉพาะของเอราทอสเทนีส



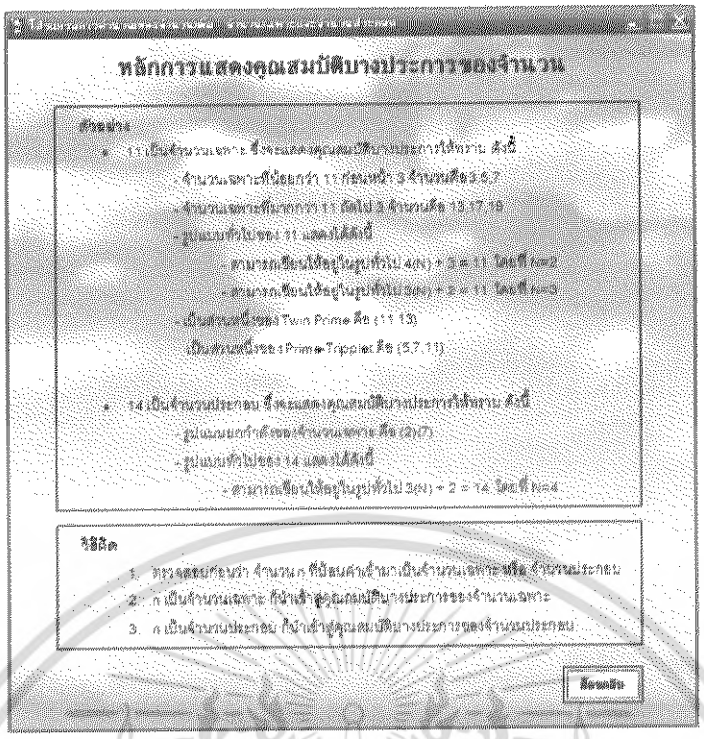
รูปที่ 4.28 จอภาพการค้นหาจำนวนเฉพาะของเอราทอสเทนีส

4.4.4 จอภาพคุณสมบัติของจำนวน

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการแสดงคุณสมบัติบางประการของจำนวน แสดงดังรูปที่ 4.29 และรูปที่ 4.30



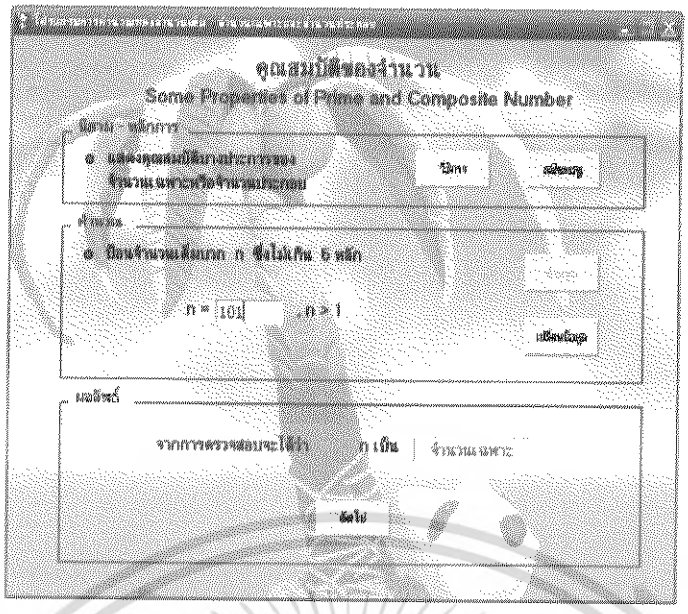
รูปที่ 4.29 จอภาพนิยามและหลักการของการแสดงคุณสมบัติของจำนวน



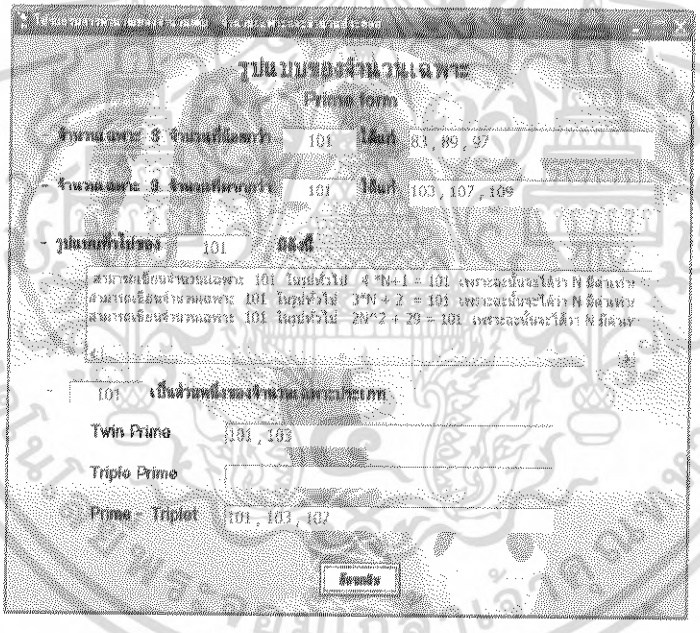
รูปที่ 4.30 จอภาพนิยามและหลักการของการแสดงคุณสมบัติของจำนวน(ต่อ)

ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม n มีค่าไม่เกิน 5 หลัก แล้วผลการตรวจสอบจำนวนเต็ม n เกิดได้ 2 กรณี คือ

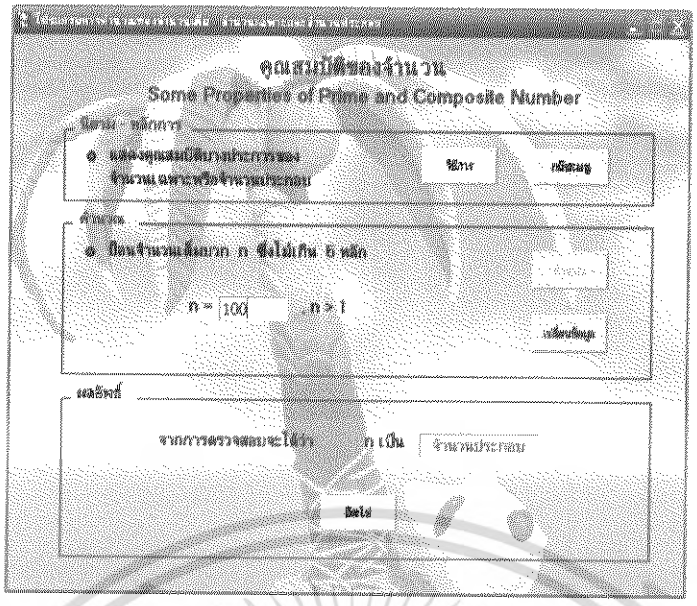
1) กรณีที่จำนวนเต็ม n เป็นจำนวนเฉพาะ แสดงดังรูปที่ 4.31 และรูปที่ 4.32
2) กรณีที่จำนวนเต็ม n เป็นจำนวนประกอบ แสดงดังรูปที่ 4.33 และรูปที่ 4.34



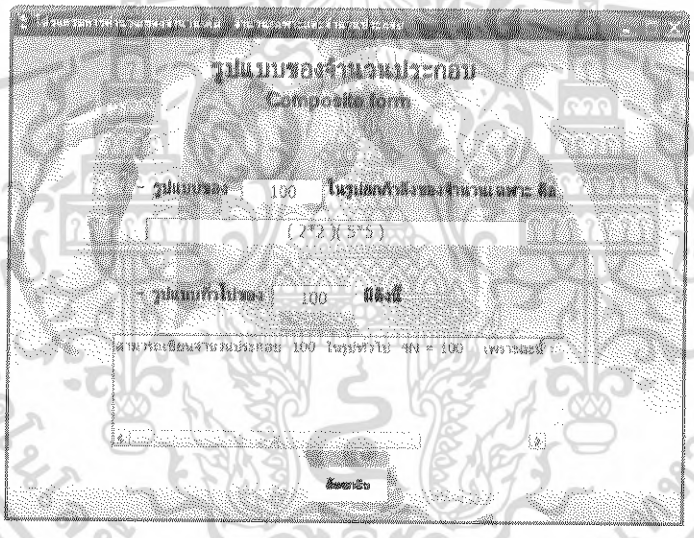
รูปที่ 4.31 จอภาพการแสดงคุณสมบัติของจำนวนในกรณีเป็นจำนวนเฉพาะ



รูปที่ 4.32 จอภาพการแสดงรูปแบบของจำนวนเฉพาะ



รูปที่ 4.33 จอภาพการแสดงคุณสมบัติของจำนวนในกรณีเป็นจำนวนประกอบ

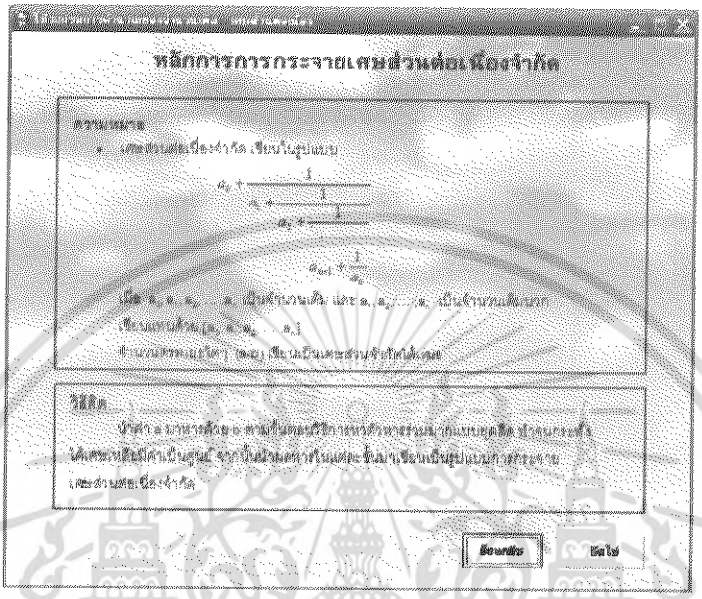


รูปที่ 4.34 จอภาพการแสดงรูปแบบของจำนวนประกอบ

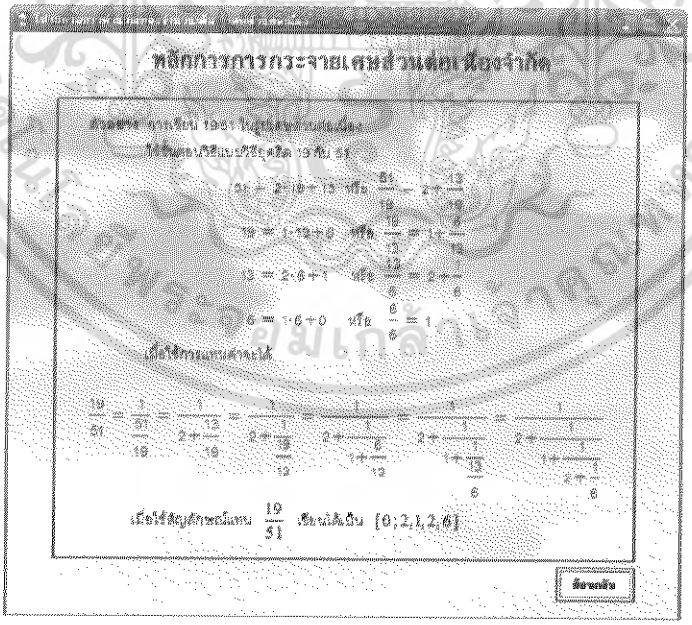
4.5 เศษส่วนต่อเนื่อง

4.5.1 จอภาพการกระจายเศษส่วนต่อเนื่องจำกัด

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการการกระจายเศษส่วนต่อเนื่องจำกัด แสดงดังรูปที่ 4.35 และรูปที่ 4.36

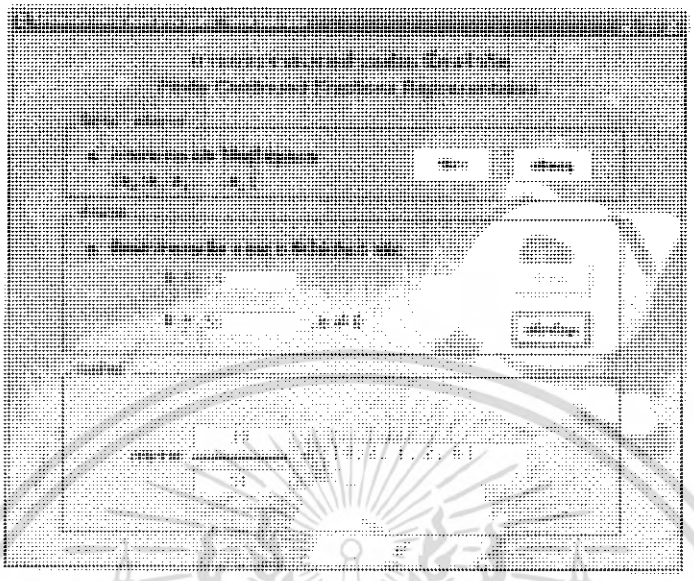


รูปที่ 4.35 จอภาพนิยามและหลักการของการกระจายเศษส่วนต่อเนื่องจำกัด



รูปที่ 4.36 จอภาพนิยามและหลักการของการกระจายเศษส่วนต่อเนื่องจำกัด(ต่อ)

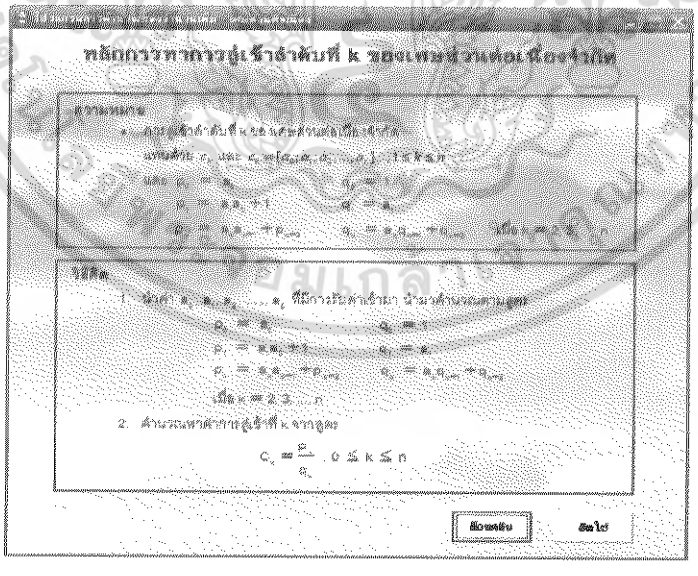
ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก a และ b ไม่เกิน 5 หลัก แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.37



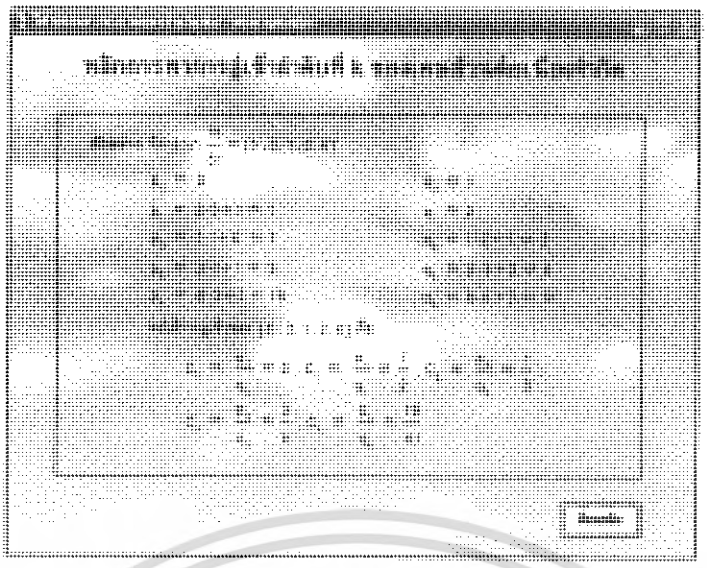
รูปที่ 4.37 จอภาพการกระจายเศษส่วนต่อเนื่องจำกัด

4.5.2 จอภาพการหาการลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่องจำกัด

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาการลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่องจำกัด แสดงดังรูปที่ 4.38 และรูปที่ 4.39

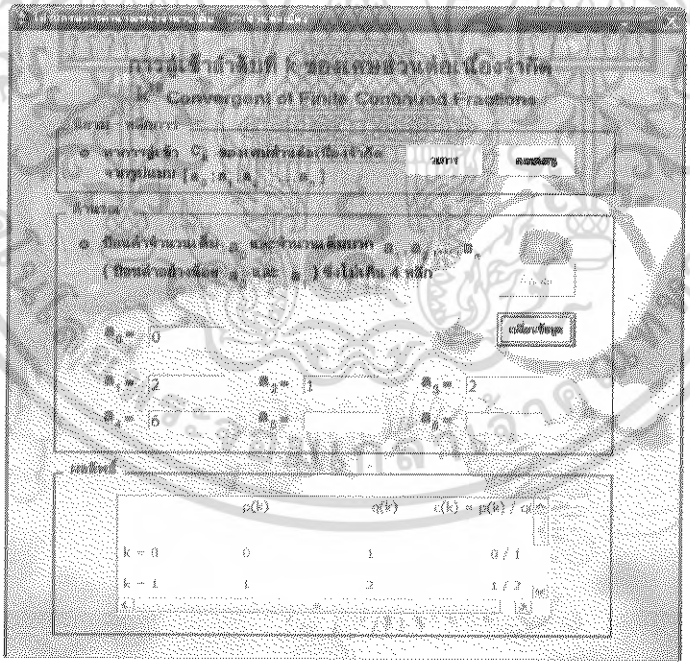


รูปที่ 4.38 จอภาพนิยามและหลักการของการลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่อง



รูปที่ 4.39 จอภาพนิยามและหลักการของการลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่อง(ต่อ)

ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a_0 และป้อนค่าจำนวนเต็มบวก $a_1, a_2, \ldots, a_6$ โดยในการรับค่าจะต้องมีอย่างน้อย a_0 และ a_1 แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.40

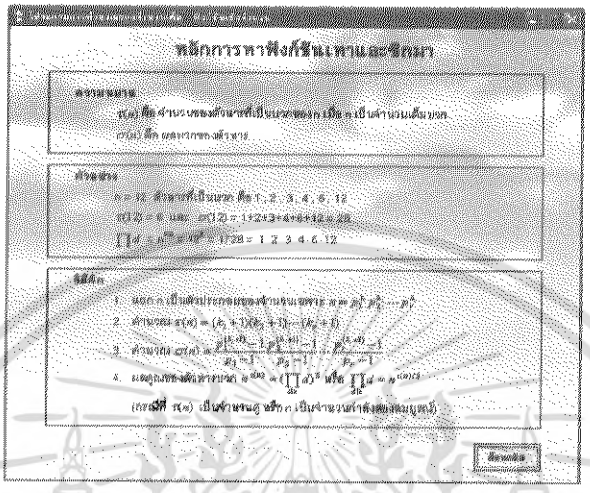


รูปที่ 4.40 จอภาพการลู่เข้าลำดับที่ k ของเศษส่วนต่อเนื่องจำกัด

4.6 ฟังก์ชันเชิงจำนวน

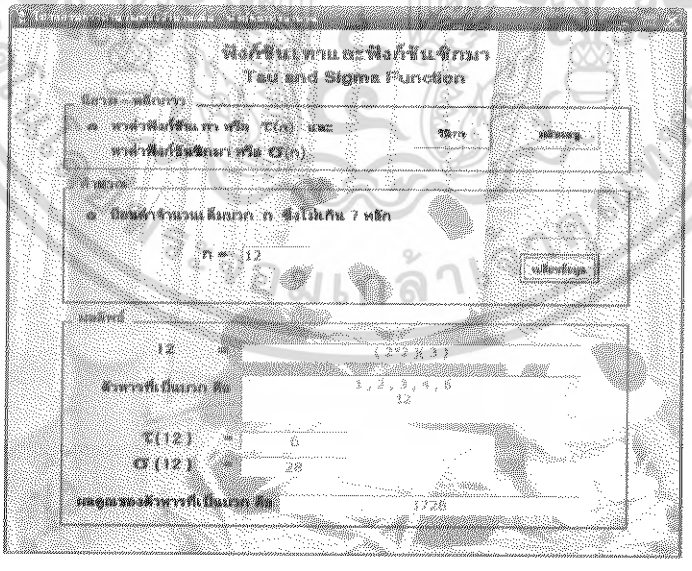
4.6.1 จอภาพการหาค่าฟังก์ชันเทา (τ) และซิกมา (σ)

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาค่าฟังก์ชันเทาและซิกมา แสดงดังรูปที่ 4.41



รูปที่ 4.41 จอภาพนิยามและหลักการของการหาค่าฟังก์ชันเทาและฟังก์ชันซิกมา

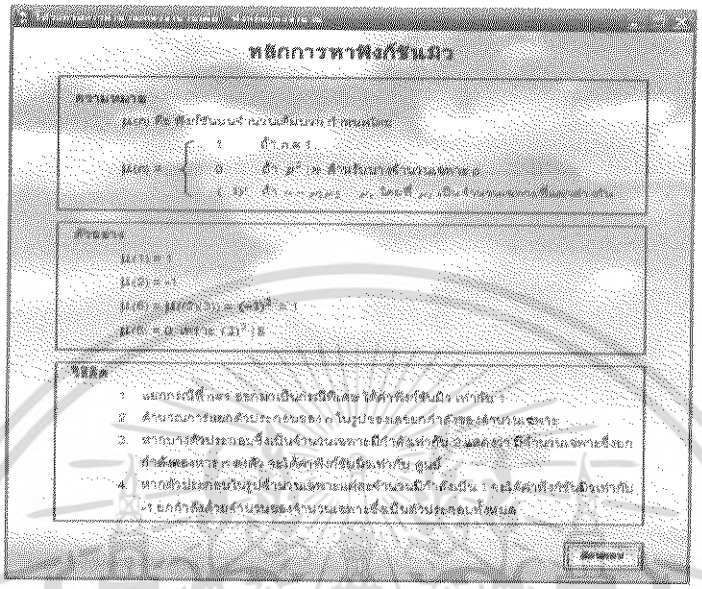
ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 7 หลักแล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.42



รูปที่ 4.42 จอภาพการหาค่าฟังก์ชันเทาและฟังก์ชันซิกมา

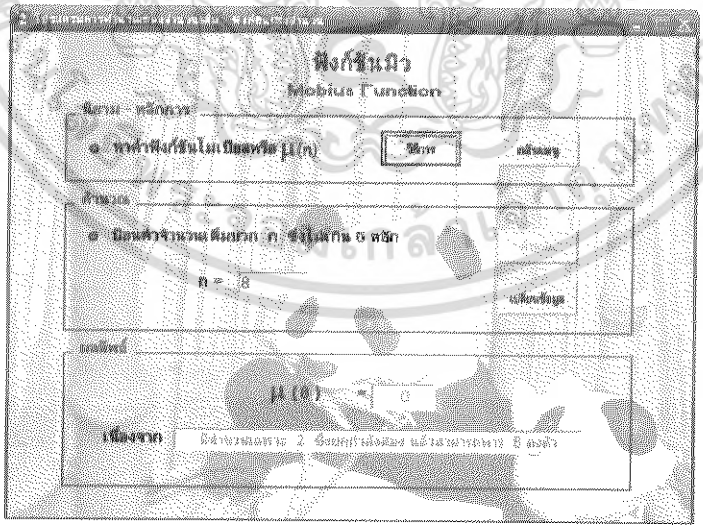
4.6.2 จอภาพการหาค่าฟังก์ชันมิว (μ)

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาค่าฟังก์ชันมิว แสดงดังรูปที่ 4.43



รูปที่ 4.43 จอภาพนิยามและหลักการของการหาค่าฟังก์ชันมิว

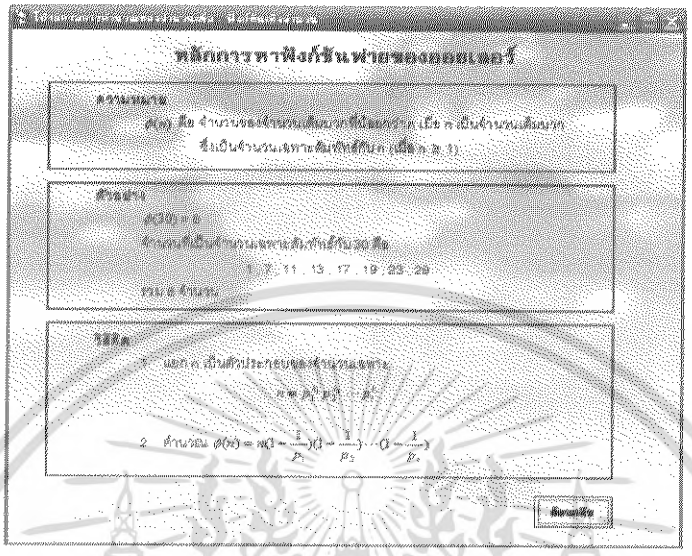
ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 6 หลักแล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.44



รูปที่ 4.44 จอภาพการหาค่าฟังก์ชันมิว

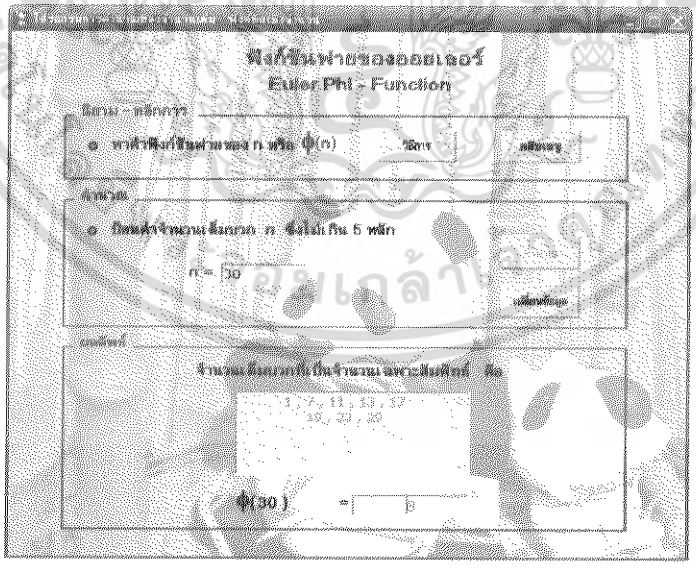
4.6.3 จอภาพการหาค่าฟังก์ชันฟายของออยเลอร์ (ϕ)

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาค่าฟังก์ชันฟายของออยเลอร์ แสดงดังรูปที่ 4.45



รูปที่ 4.45 จอภาพนิยามและหลักการของการหาค่าฟังก์ชันฟายของออยเลอร์

ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 5 หลัก แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.46

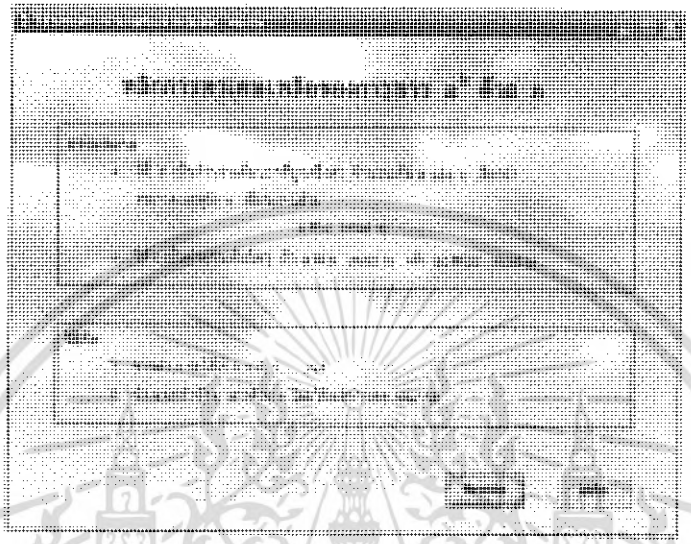


รูปที่ 4.46 จอภาพของการหาค่าฟังก์ชันฟายของออยเลอร์

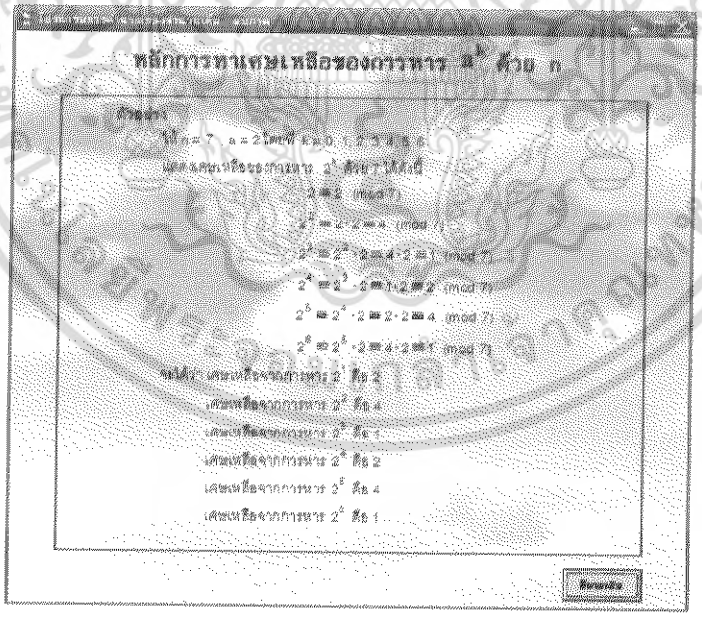
4.7 สมภาค

4.7.1 จอภาพการแสดงเศษเหลือของการหาร a^k ด้วย n

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาเศษเหลือของการหาร a^k ด้วย n แสดงดังรูปที่ 4.47 และรูปที่ 4.48

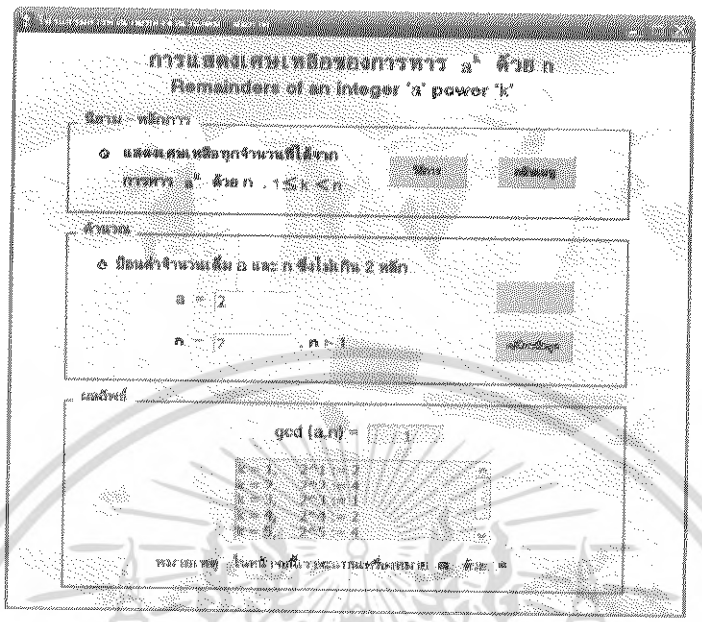


รูปที่ 4.47 จอภาพนิยามและหลักการของการหาเศษเหลือของการหาร a^k ด้วย n



รูปที่ 4.48 จอภาพนิยามและหลักการของการหาเศษเหลือของการหาร a^k ด้วย n (ต่อ)

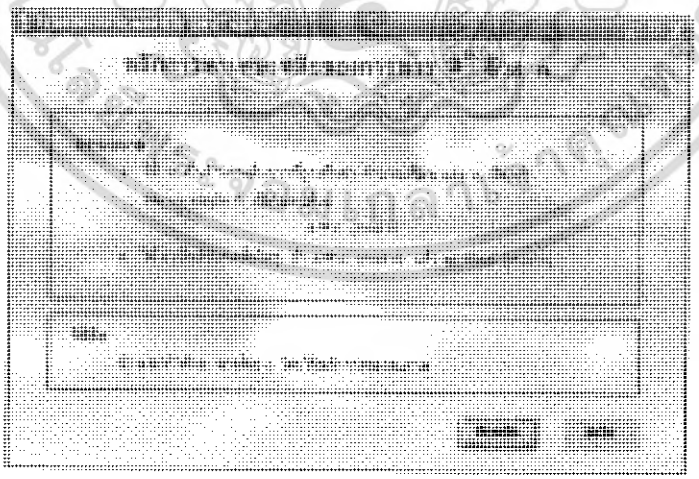
ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก n และจำนวนเต็ม a ซึ่งมีค่าไม่เกิน 2 หลัก แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.49



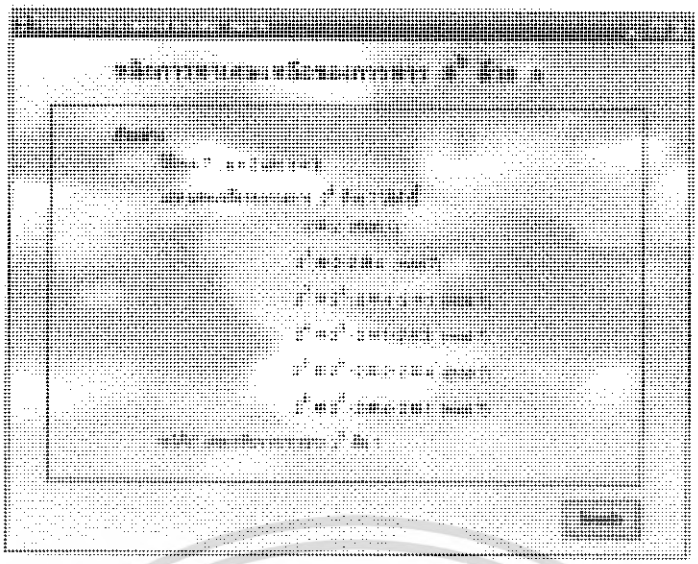
รูปที่ 4.49 จอภาพการแสดงเศษเหลือของการหาร a^k ด้วย n

4.7.2 จอภาพการหาเศษเหลือของการหาร a^b ด้วย n

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาเศษเหลือของการหาร a^b ด้วย n แสดงดังรูปที่ 4.50 และรูปที่ 4.51

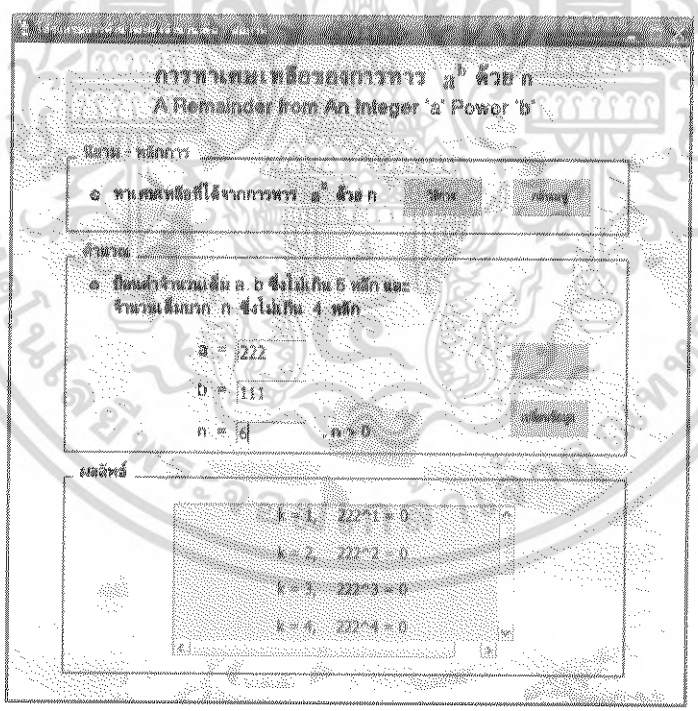


รูปที่ 4.50 จอภาพนิยามและหลักการของการหาเศษเหลือของการหาร a^b ด้วย n



รูปที่ 4.51 จอภาพนิยามและหลักการของการหาเศษเหลือของการหาร a^b ด้วย n (ต่อ)

ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a และจำนวนเต็มบวก b ซึ่งมีค่าไม่เกิน 5 หลักและป้อนค่าจำนวนเต็มบวก n ไม่เกิน 4 หลัก แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.52

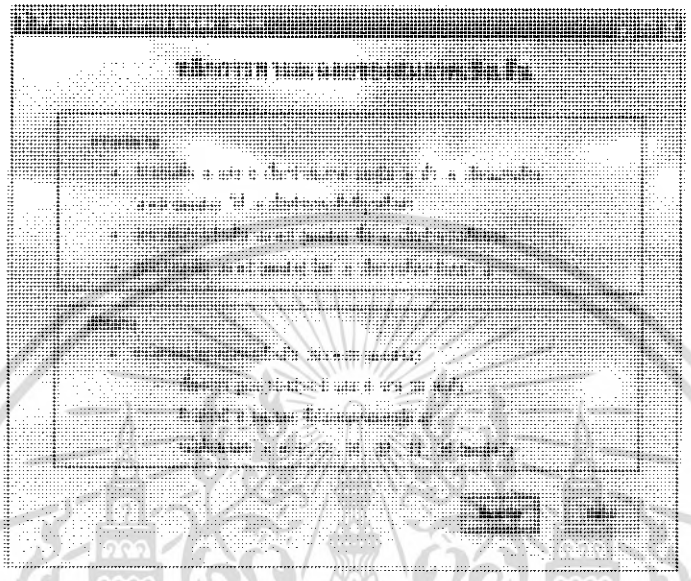


รูปที่ 4.52 จอภาพการหาเศษเหลือของการหาร a^b ด้วย n

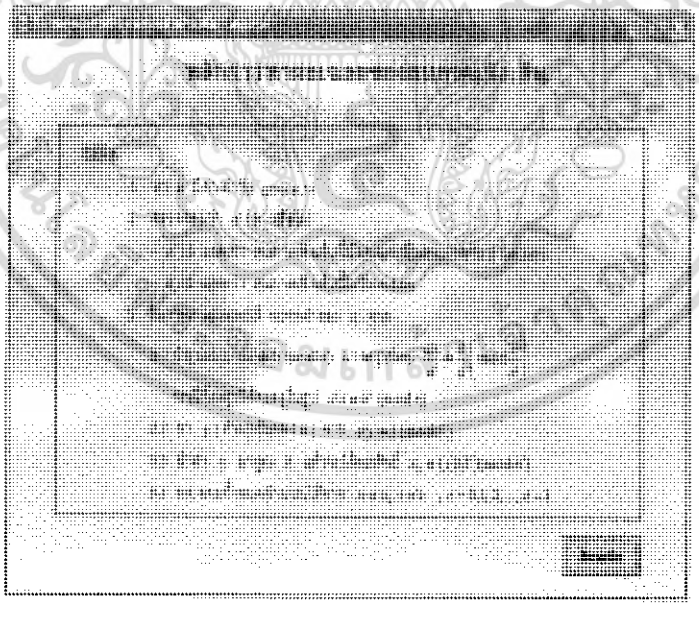
4.7.3 **จอภาพการหาผลเฉลยสมภาคเชิงเส้น**

1) **การหาผลเฉลยสมภาคเชิงเส้น** $ax \equiv b \pmod{n}$

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการของการหาผลเฉลยสมภาคเชิงเส้น แสดงดังรูปที่ 4.53 และรูปที่ 4.54

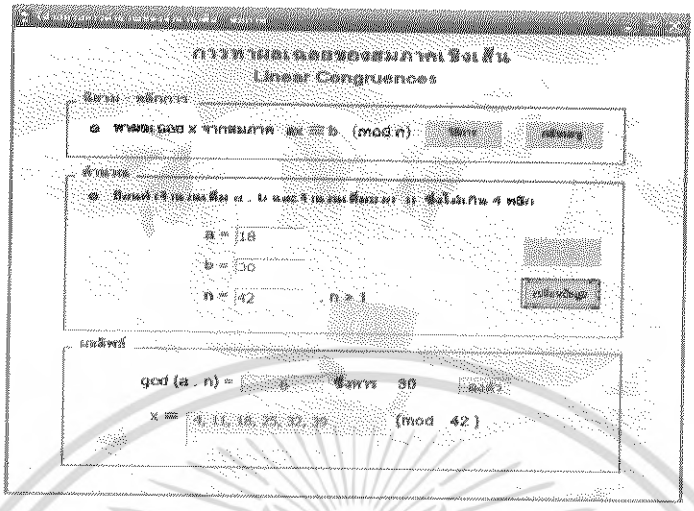


รูปที่ 4.53 **จอภาพนิยามและหลักการของการหาผลเฉลยของสมภาคเชิงเส้น**



รูปที่ 4.54 **จอภาพนิยามและหลักการของการหาผลเฉลยของสมภาคเชิงเส้น (ต่อ)**

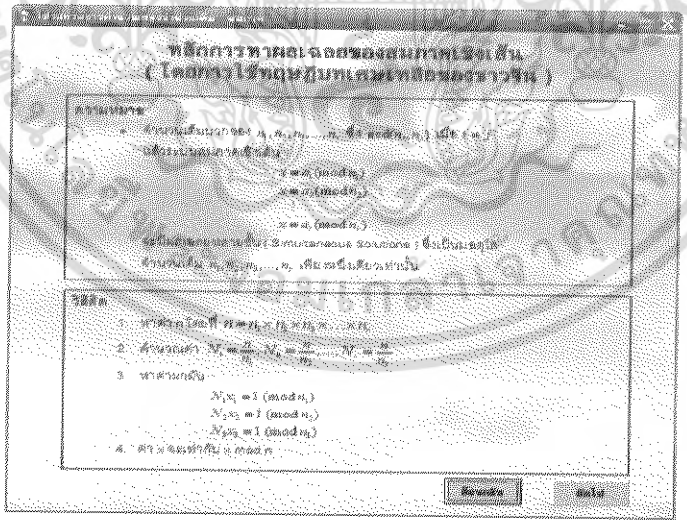
ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a, b และ n ไม่เกิน 4 หลัก แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.55



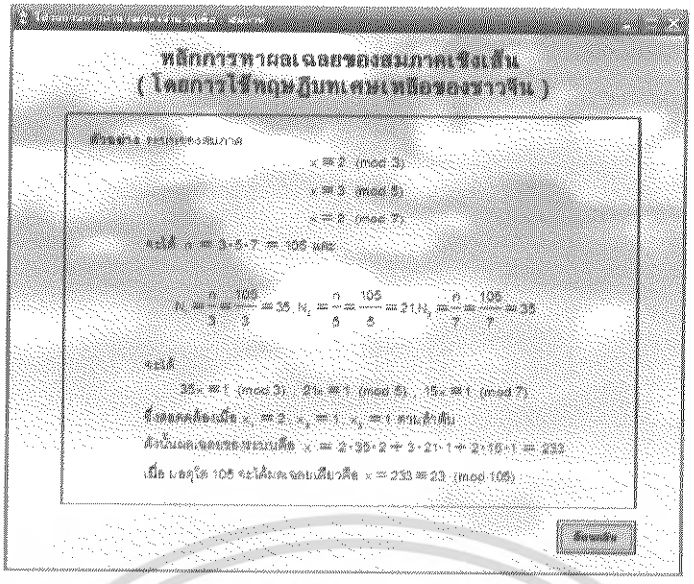
รูปที่ 4.55 จอภาพการหาผลเฉลยของสมภาคเชิงเส้น

2) **การหาผลเฉลยสมภาคเชิงเส้น โดยใช้ทฤษฎีบทเศษเหลือชาวจีน**

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการของการหาผลเฉลยสมภาคเชิงเส้น โดยใช้ทฤษฎีเศษเหลือของชาวจีน แสดงดังรูปที่ 4.56 และรูปที่ 4.57

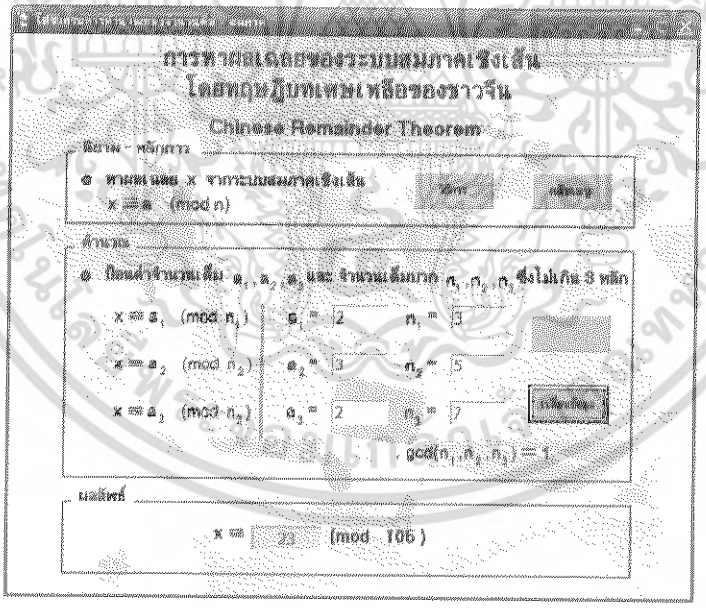


รูปที่ 4.56 จอภาพนิยามและหลักการของการหาผลเฉลยของสมภาคเชิงเส้นโดยการใช้ทฤษฎีบทเศษเหลือของชาวจีน



รูปที่ 4.57 จอภาพนิยามและหลักการของการหาผลเฉลยของสมภาคเชิงเส้นโดยการใช้ทฤษฎีบทเศษเหลือของชาวจีน (ต่อ)

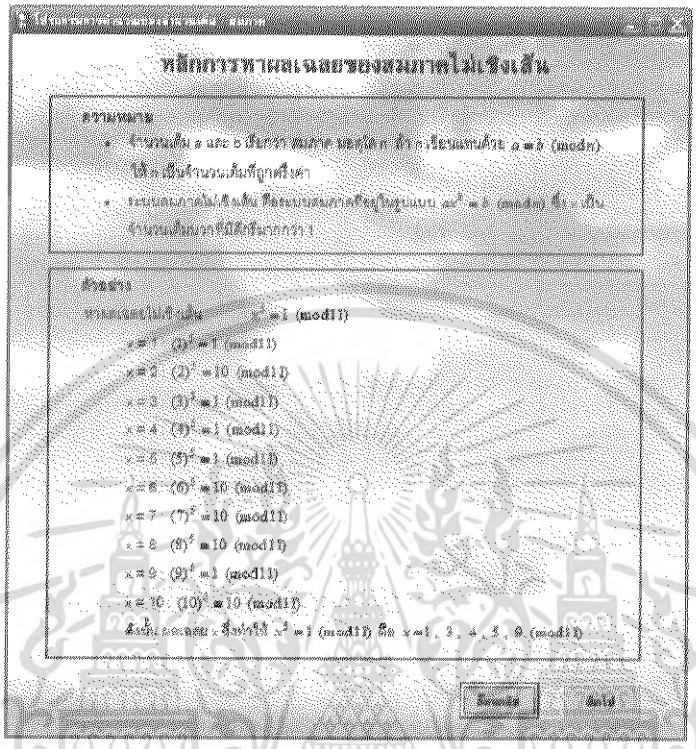
ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a_1 , a_2 , a_3 และจำนวนเต็มบวก n_1 , n_2 , n_3 ซึ่ง $\gcd(n_1,n_2,n_3) = 1$ แล้วกดปุ่มคำนวณ แสดงดังรูปที่ 4.58



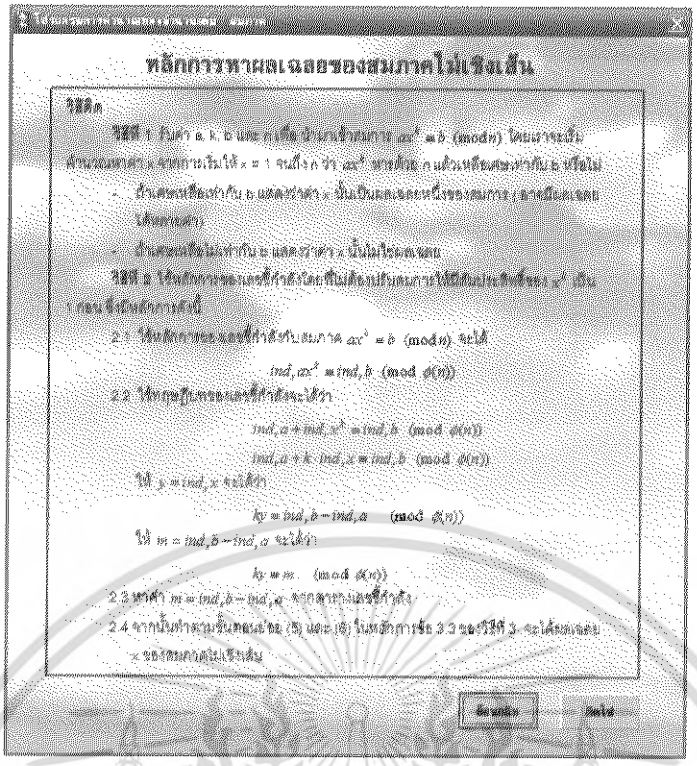
รูปที่ 4.58 จอภาพการหาผลเฉลยของสมภาคเชิงเส้นโดยการใช้ทฤษฎีบทเศษเหลือของชาวจีน

4.7.4 จอภาพการหาผลเฉลยสมภาคไม่เชิงเส้น

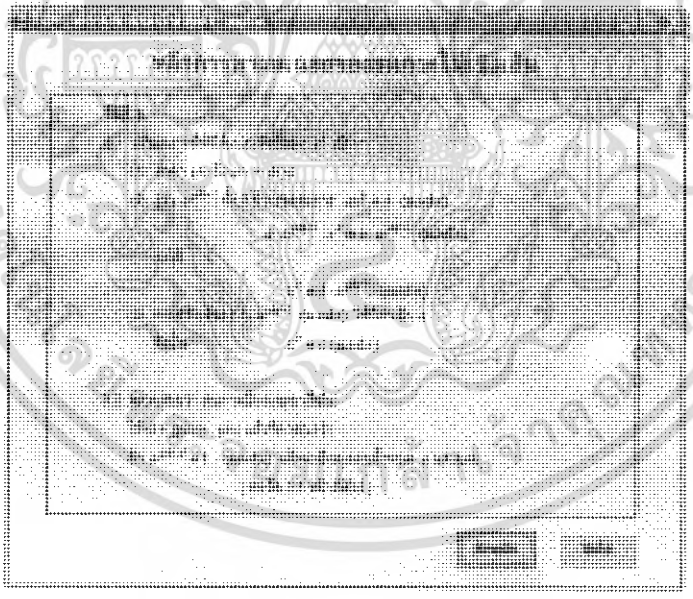
ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการของการหาผลเฉลยของสมภาคไม่เชิงเส้น แสดงดังรูปที่ 4.59 รูปที่ 4.60 รูปที่ 4.61 และรูปที่ 4.62



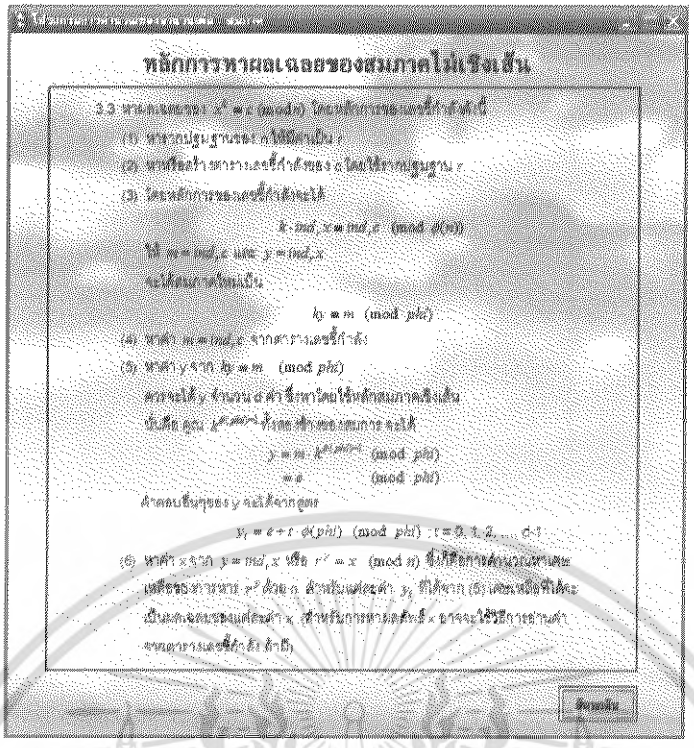
รูปที่ 4.59 จอภาพนิยามและหลักการของการหาผลเฉลยของสมภาคไม่เชิงเส้น



รูปที่ 4.60 จอภาพนิยามและหลักการของการหาผลเฉลยของสมภาคไม่เชิงเส้น (ต่อ)



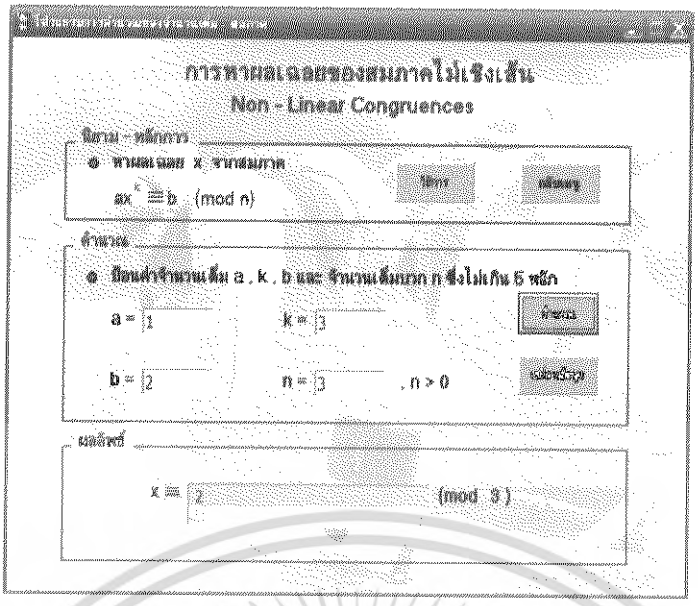
รูปที่ 4.61 จอภาพนิยามและหลักการของการหาผลเฉลยของสมภาคไม่เชิงเส้น (ต่อ)



รูปที่ 4.62 จอภาพนิยามและหลักการของการหาผลเฉลยของสมภาคไม่เชิงเส้น (ต่อ)

ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a, k, b และ n ซึ่งมีค่าไม่เกิน 5 หลัก แล้วกดปุ่มคำนวณ ผลลัพธ์จะเกิดขึ้นได้ 2 กรณี คือ

1) กรณีที่สามารถหาคำตอบได้ แสดงดังรูปที่ 4.63
2) กรณีที่ไม่สามารถหาผลเฉลยได้ แสดงดังรูปที่ 4.64



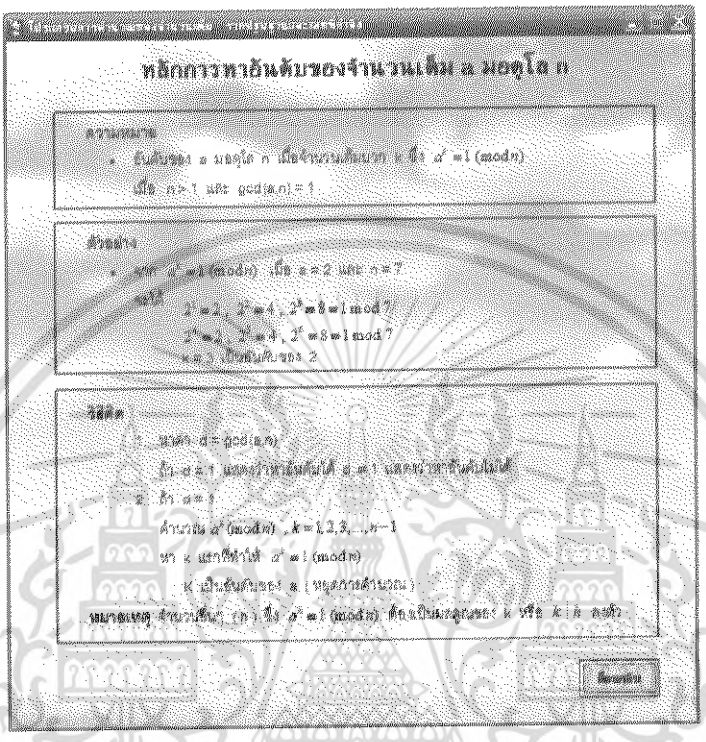
รูปที่ 4.63 จอภาพการหาผลเฉลยของสมภาคไม่เชิงเส้นกรณีหาผลเฉลยได้

รูปที่ 4.64 จอภาพการหาผลเฉลยของสมภาคไม่เชิงเส้นกรณีหาผลเฉลยไม่ได้

4.8 รากปฐมฐานและเลขชี้กำลัง

4.8.1 จอภาพการหาอันดับของ a มอดุโล n

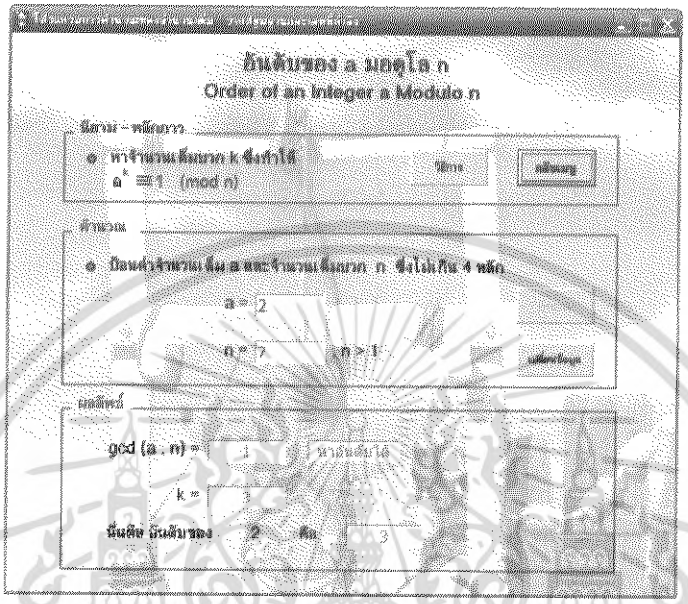
ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาอันดับของ a มอดุโล n แสดงดังรูปที่ 4.65



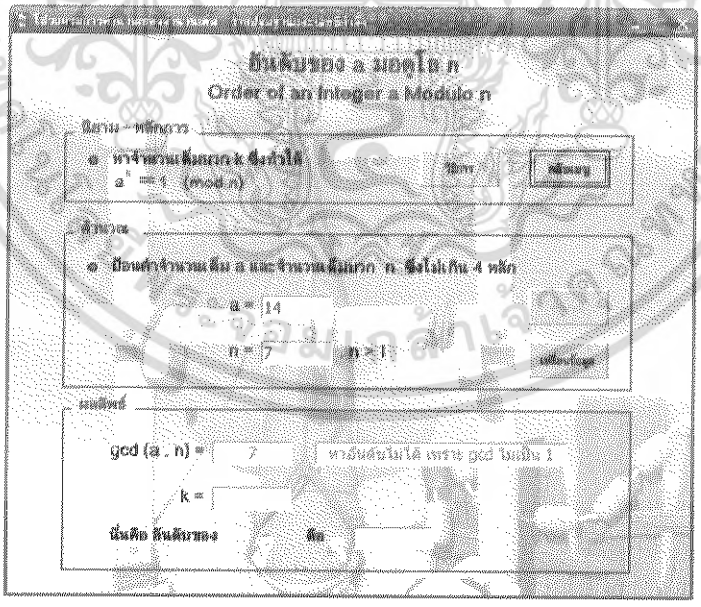
รูปที่ 4.65 จอภาพนิยามและหลักการของการหาอันดับของจำนวนเต็ม a มอดุโล n

ส่วนการคำนวณ ป้อนค่าจำนวนเต็ม a และ n โดยที่ n > 1 ซึ่งมีค่าไม่เกิน 4 หลัก แล้วกดปุ่มคำนวณผลลัพธ์จะเกิดขึ้นได้ 2 กรณี คือ

1) กรณีที่สามารถหาคำตอบได้ แสดงดังรูปที่ 4.66
2) กรณีที่ไม่สามารถหาคำตอบได้ แสดงดังรูปที่ 4.67



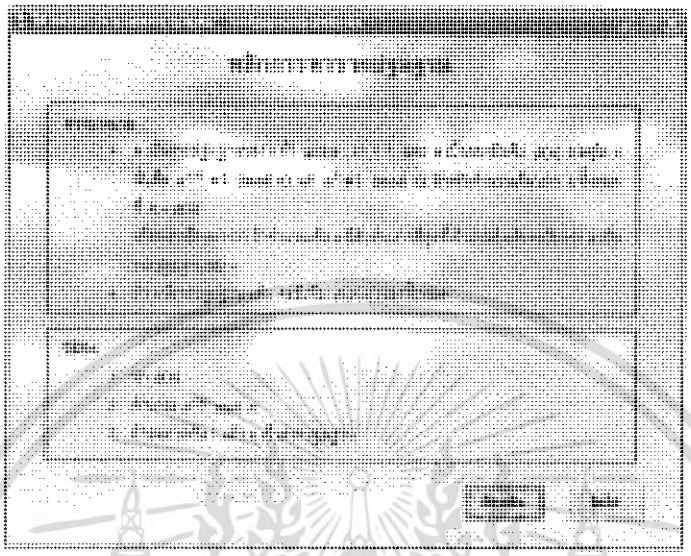
รูปที่ 4.66 จอภาพการหาอันดับของจำนวนเต็ม a มอดุโล n กรณีหาอันดับได้



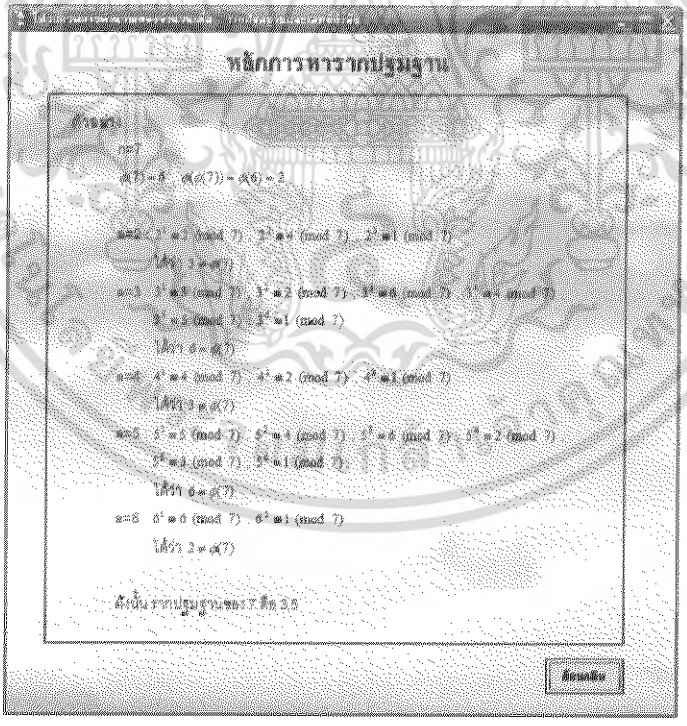
รูปที่ 4.67 จอภาพการหาอันดับของจำนวนเต็ม a มอดุโล n กรณีหาอันดับไม่ได้

4.8.2 **จอภาพการหารากปฐมฐาน**

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหารากปฐมฐาน แสดงดังรูปที่ 4.68 และรูปที่ 4.69



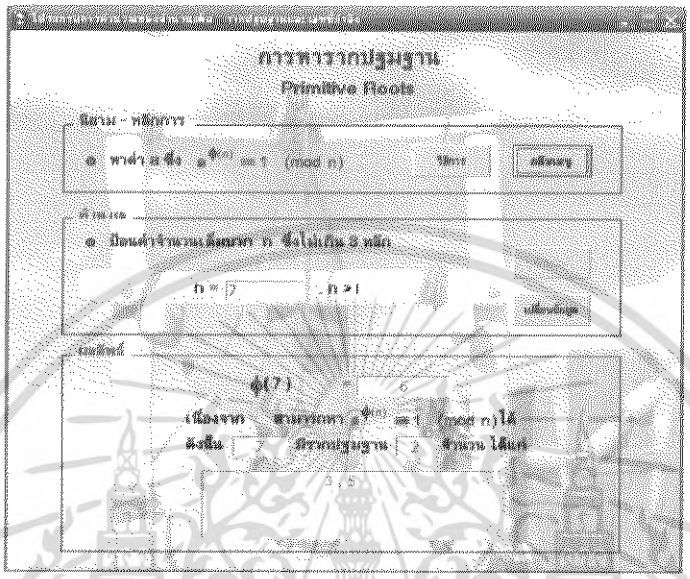
รูปที่ 4.68 จอภาพนิยามและหลักการของการหารากปฐมฐาน



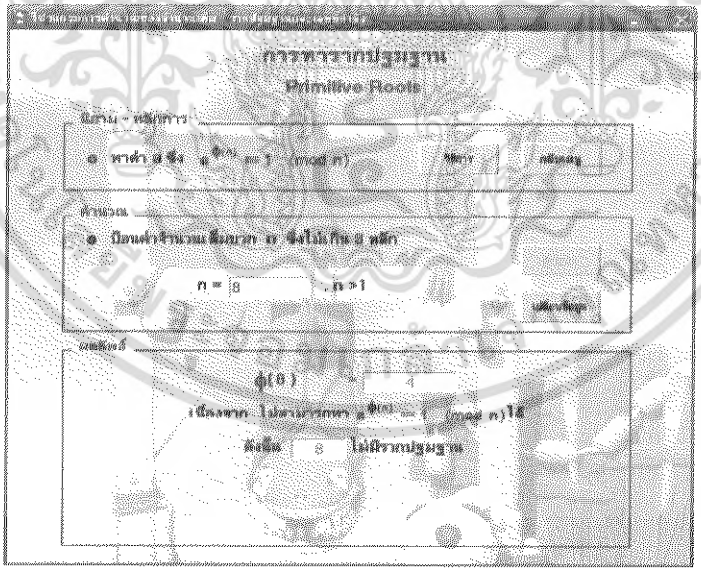
รูปที่ 4.69 จอภาพนิยามและหลักการของการหารากปฐมฐาน (ต่อ)

ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 3 หลัก แล้วกดปุ่มคำนวณผลลัพธ์จะเกิดขึ้นได้ 2 กรณี

1) กรณีที่สามารถหารากปฐมฐานได้ แสดงดังรูปที่ 4.70
2) กรณีที่ไม่สามารถหารากปฐมฐานได้ แสดงดังรูปที่ 4.71



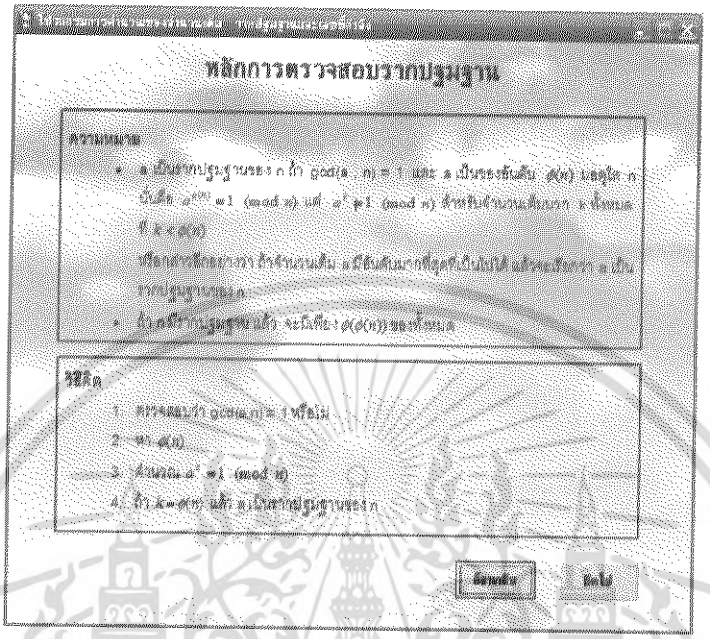
รูปที่ 4.70 จอภาพการหารากปฐมฐานกรณีหารากปฐมฐานได้



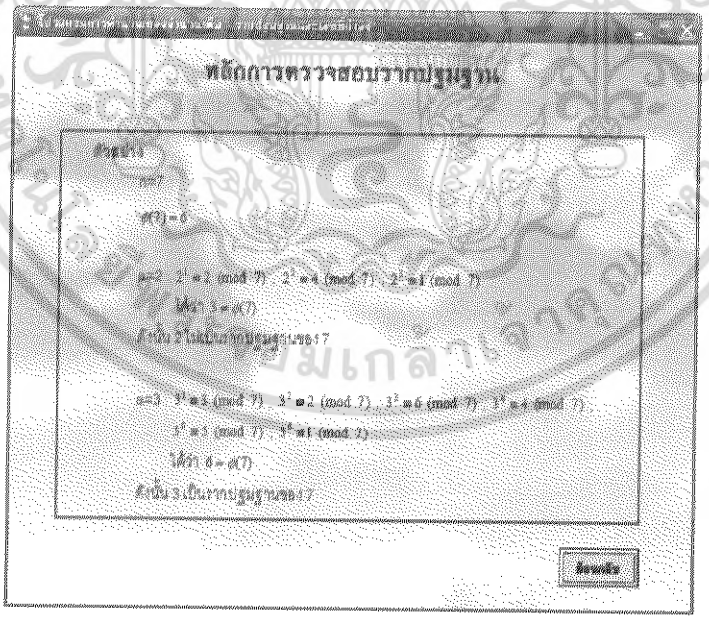
รูปที่ 4.71 จอภาพการหารากปฐมฐานกรณีหารากปฐมฐานไม่ได้

4.8.3 จอภาพการตรวจสอบการเป็นรากปฐมฐาน

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการตรวจสอบการเป็นรากปฐมฐาน แสดงดังรูปที่ 4.72 และรูปที่ 4.73



รูปที่ 4.72 จอภาพนิยามและหลักการของการตรวจสอบการเป็นรากปฐมฐาน

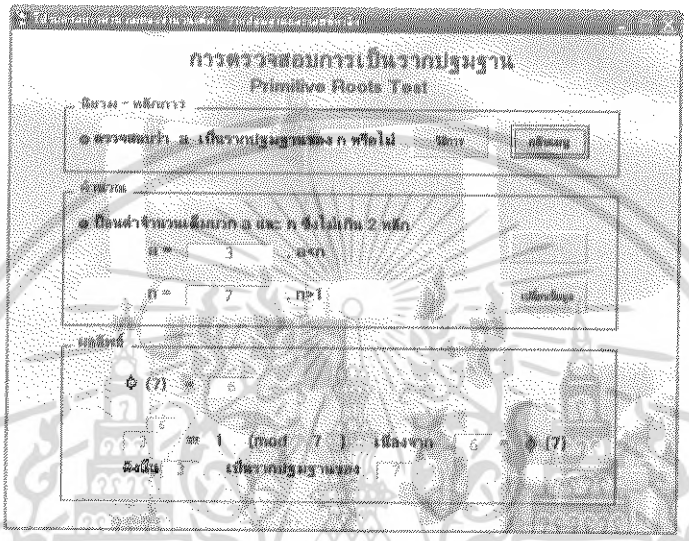


รูปที่ 4.73 จอภาพนิยามและหลักการของการตรวจสอบการเป็นรากปฐมฐาน (ต่อ)

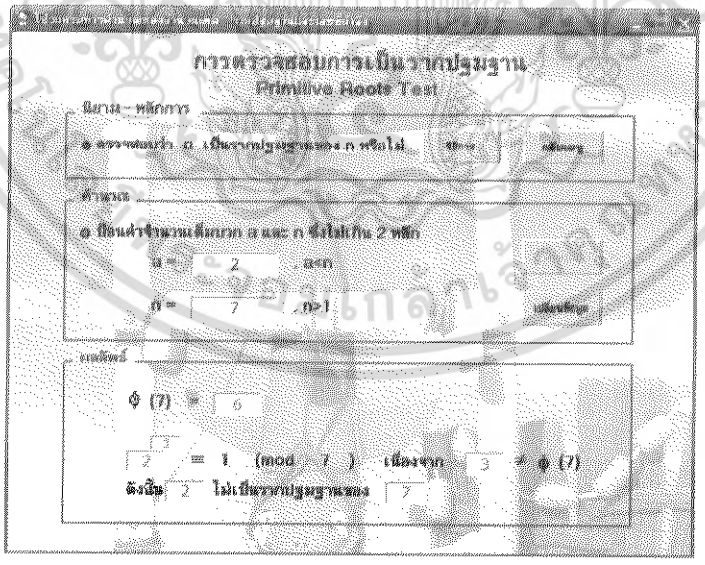
ส่วนการคำนวณ ป้อนค่าจำนวนเต็มบวก a และ n ซึ่งมีค่าไม่เกิน 2 หลัก แล้วกดปุ่มคำนวณผลลัพธ์จะเกิดขึ้นได้ 2 กรณี คือ

1) กรณีที่จำนวนเต็มบวก a เป็นรากปฐมฐานของจำนวนเต็มบวก n แสดงดังรูปที่ 4.74

2) กรณีที่จำนวนเต็มบวก a ไม่เป็นรากปฐมฐานของจำนวนเต็มบวก n แสดงดังรูปที่ 4.75



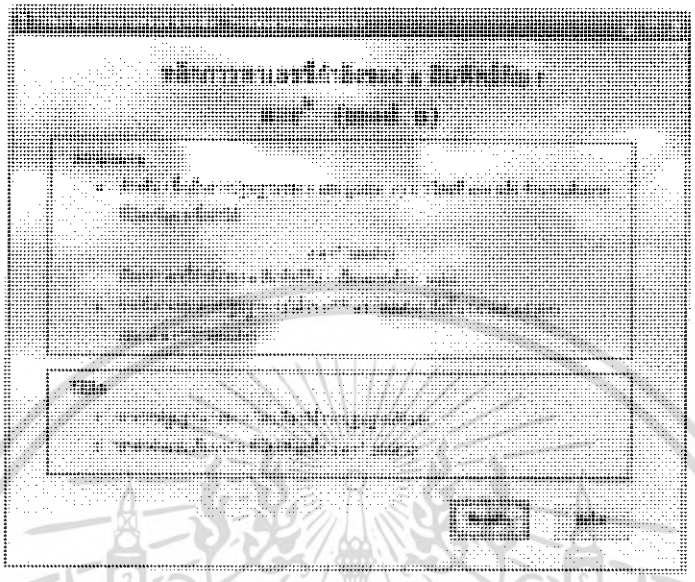
รูปที่ 4.74 จอภาพการตรวจสอบการเป็นรากปฐมฐาน กรณี a เป็นรากปฐมฐานของ n



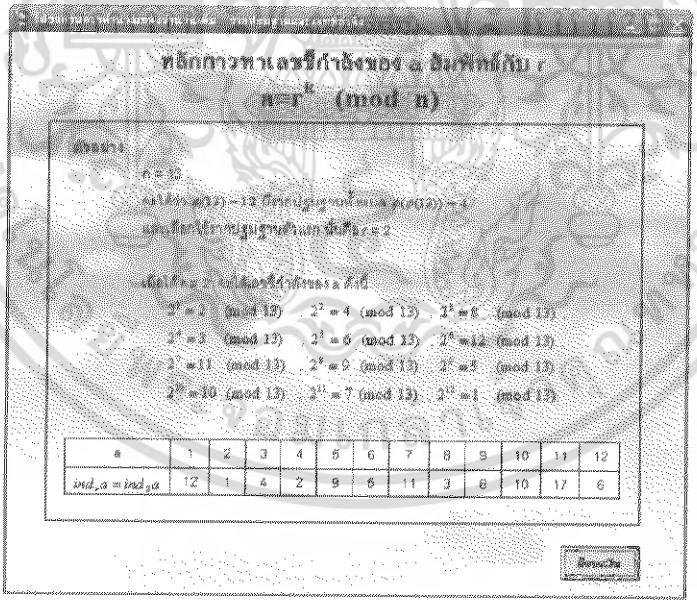
รูปที่ 4.75 จอภาพการตรวจสอบการเป็นรากปฐมฐาน กรณี a ไม่เป็นรากปฐมฐานของ n

4.8.4 การหาเลขชี้กำลังของ a สัมพัทธ์กับ r

ส่วนนิยามและหลักการ เมื่อกดปุ่มวิธีการจะแสดงจอภาพของหลักการหาเลขชี้กำลัง a สัมพัทธ์ r แสดงดังรูปที่ 4.76 และรูปที่ 4.77



รูปที่ 4.76 จอภาพนิยามและหลักการของการหาเลขชี้กำลังของ a สัมพัทธ์กับ r

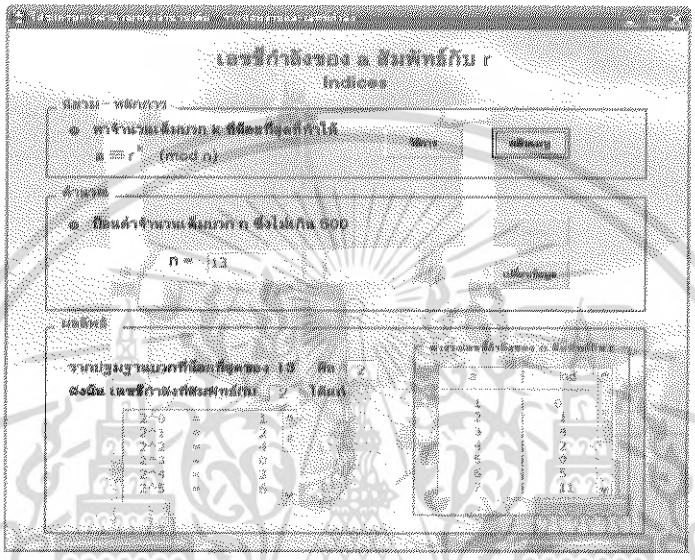


รูปที่ 4.77 จอภาพนิยามและหลักการของการหาเลขชี้กำลังของ a สัมพัทธ์กับ r (ต่อ)

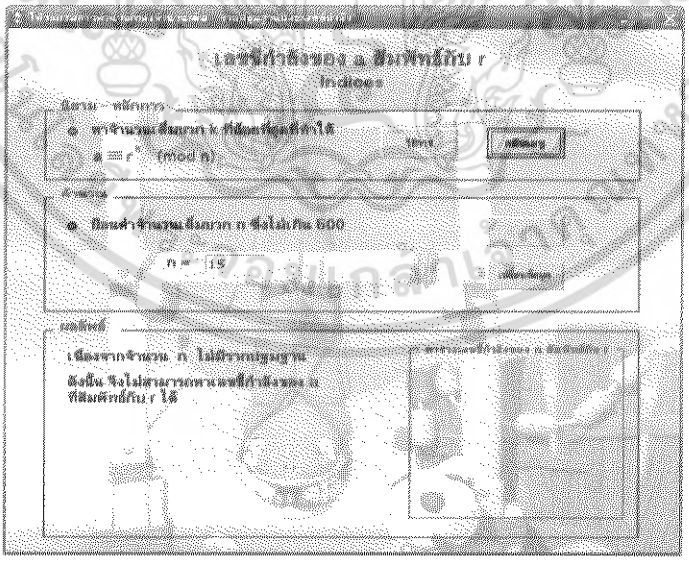
ส่วนการคำนวณ รับค่าจำนวนเต็มบวก n ซึ่งมีค่าไม่เกิน 500 แล้วกดปุ่มคำนวณ ผลลัพธ์จะเกิดขึ้นได้ 2 กรณี คือ

1) กรณีที่จำนวนเต็ม n มี รากปฐมฐานจึงสามารถหาเลขชี้กำลังของ a ที่สัมพัทธ์กับ r ได้ แสดงดังรูปที่ 4.78

2) กรณีที่จำนวนเต็ม n ไม่มีรากปฐมฐานดังนั้นจึงไม่สามารถหาเลขชี้กำลังของ a ที่สัมพัทธ์กับ r ได้ แสดงดังรูปที่ 4.79



รูปที่ 4.78 จอภาพการหาเลขชี้กำลังของ a สัมพัทธ์กับ r กรณี n มีรากปฐมฐาน



รูปที่ 4.79 จอภาพการหาเลขชี้กำลังของ a สัมพัทธ์กับ r กรณี n ไม่มีรากปฐมฐาน

4.9 ตารางต่าง ๆ ประกอบด้วย

4.9.1 จอภาพตารางจำนวนเฉพาะ แสดงดังรูปที่ 4.80

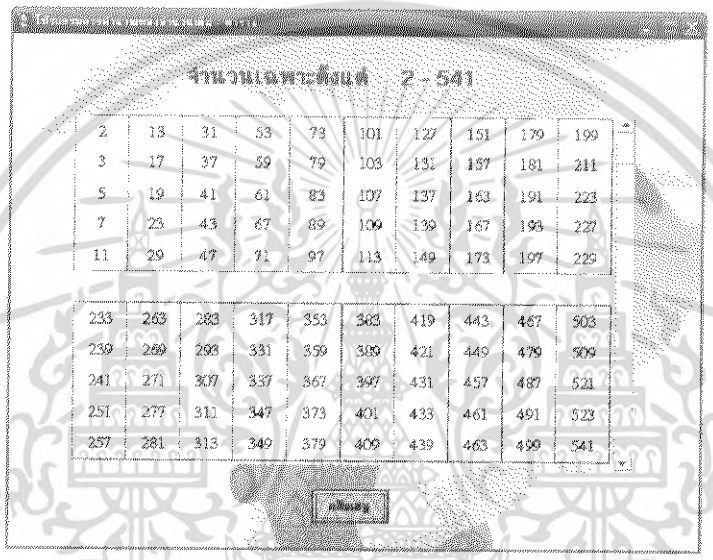
4.9.2 จอภาพตารางฟังก์ชันเชิงจำนวน แสดงดังรูปที่ 4.81

4.9.3 จอภาพตารางอันดับ แสดงดังรูปที่ 4.82

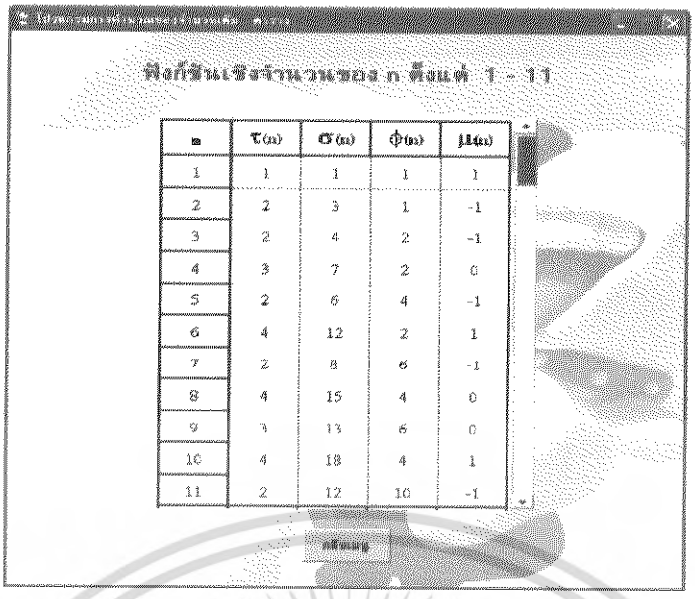
4.9.4 จอภาพตารางรากปฐมฐาน แสดงดังรูปที่ 4.83

4.9.5 จอภาพตารางรากปฐมฐานที่น้อยที่สุด แสดงดังรูปที่ 4.84

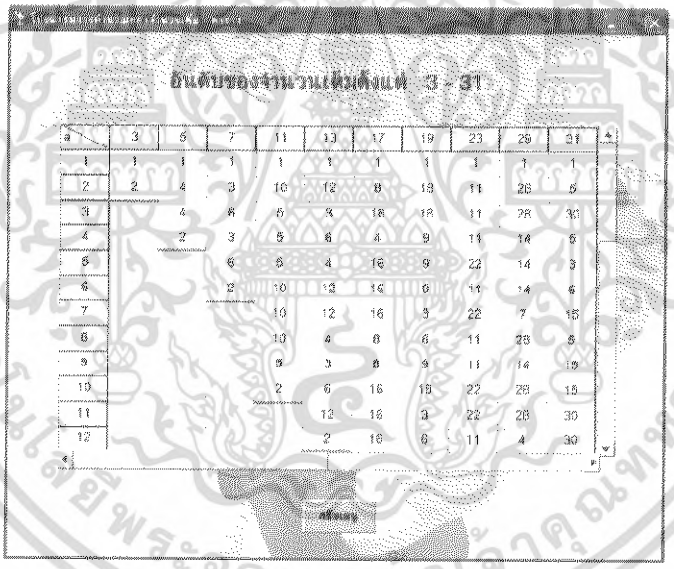
4.9.6 จอภาพตารางเลขชี้กำลัง แสดงดังรูปที่ 4.85



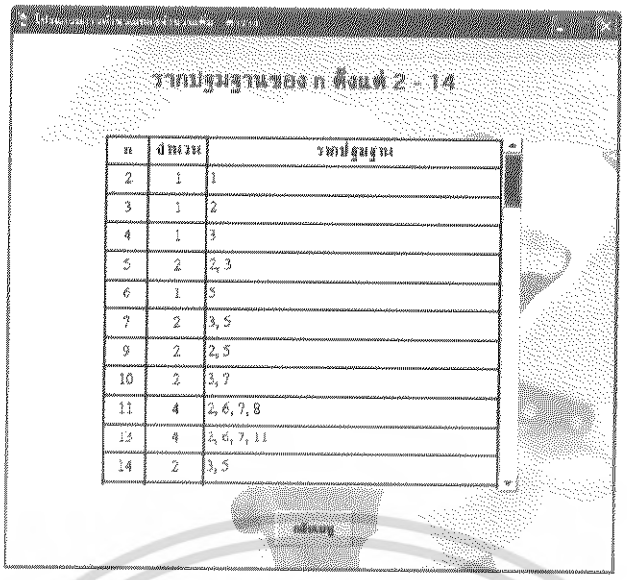
รูปที่ 4.80 **จอภาพตารางแสดงจำนวนเฉพาะ 1000 จำนวนแรก**



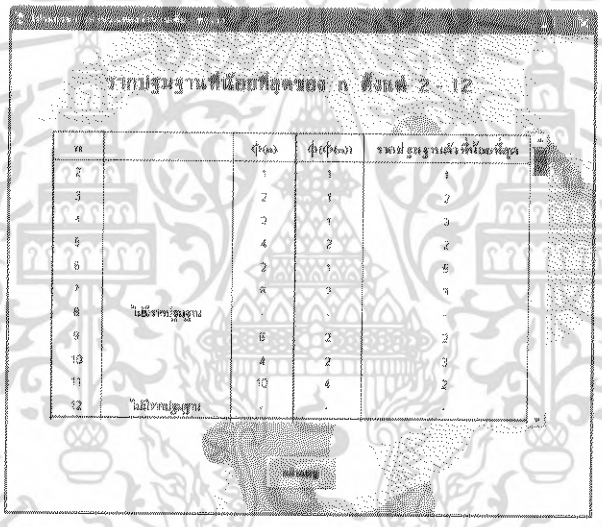
รูปที่ 4.81 จอภาพตารางฟังก์ชันเชิงจำนวน τ , σ, μ , ϕ ของจำนวนเต็มบวก n ตั้งแต่ 1-100



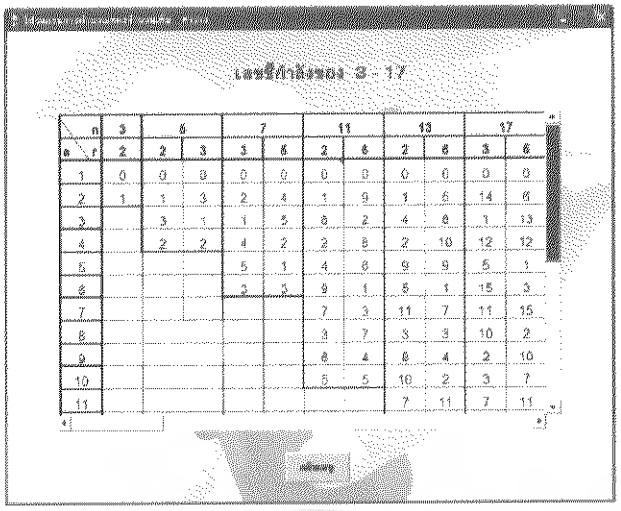
รูปที่ 4.82 จอภาพตารางอันดับของจำนวนเฉพาะ (n) น้อยกว่า 100



รูปที่ 4.83 จอภาพของตารางรากปฐมฐานของจำนวนเต็มบวก n ตั้งแต่ 2-100



รูปที่ 4.84 จอภาพตารางรากปฐมฐานที่น้อยที่สุดของจำนวนเต็มบวก n ตั้งแต่ 2-100



n	3	6		7		11		13		17	
a \ r	2	2	3	3	6	3	6	2	6	3	6
1	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	2	4	1	9	1	5	14	6
3		3	1	1	5	6	2	4	8	1	13
4		2	2	4	2	2	8	2	10	12	12
5				5	1	4	6	9	9	5	1
6				3	3	9	1	5	1	15	3
7						7	3	11	7	11	15
8						3	7	3	3	10	2
9						8	4	8	4	2	10
10						5	5	10	2	3	7
11								7	11	7	11

รูปที่ 4.85 จอภาพตารางเลขชี้กำลังของจำนวนเฉพาะ (n) < 100

บทที่ 5
การวิจารณ์หรืออภิปรายผล

5.1 บทสรุป

ในการทำปัญหาพิเศษฉบับนี้เป็นการพัฒนาโปรแกรมการคำนวณของจำนวนเต็ม ซึ่งทางคณะผู้จัดทำคาดหวังว่าจะสามารถใช้งานได้ง่ายและไม่ซับซ้อน โดยได้นำเอานิยาม ทฤษฎี และหลักการของจำนวนเต็มมาช่วยในการสร้างโปรแกรม ซึ่งช่วยให้โปรแกรมสามารถคำนวณผลลัพธ์ต่างๆได้ โดยตั้งใจที่จะทำให้ผู้ที่ไม่สนใจในเรื่องของจำนวนเต็มเพราะว่ายากต่อการคำนวณเลขจำนวนมากๆ จะได้หันมาสนใจศึกษา นอกจากนี้โปรแกรมยังสามารถแสดงกรรมวิธีในบางเรื่องได้ ซึ่งจะเป็นการเพิ่มทักษะให้กับผู้ที่มาศึกษา แต่ก่อนการใช้โปรแกรมนี้ควรศึกษาเรื่องจำนวนเต็มมาก่อนเพื่อความเข้าใจที่ง่ายขึ้นและการจัดลำดับเนื้อหาของโปรแกรมจัดตามลำดับเนื้อหาจากพื้นฐานไปยังเนื้อหาที่ซับซ้อน

การพัฒนาโปรแกรมนี้ได้เขียนขึ้นด้วยภาษาวิชวลเบสิค เวอร์ชัน 6.0 บนระบบปฏิบัติการวินโดว์ XP

5.2 ข้อจำกัดของโปรแกรมการคำนวณของจำนวนเต็ม

1) การป้อนข้อมูลเพื่อคำนวณจะจำกัดจำนวนสูงสุดไว้ในรูปของจำนวนหลัก ทั้งนี้เพื่อความเร็วในการคำนวณเพื่อให้สามารถเห็นรายละเอียดวิธีการคิด
2) โปรแกรมนี้ไม่สามารถสั่งพิมพ์ข้อมูลออกมาได้
3) โปรแกรมนี้ออกแบบการแสดงตัวอักษรกับจอภาพที่ความละเอียดขนาด 1024x768 พิกเซล

5.3 ข้อเสนอแนะ

สำหรับข้อเสนอแนะแนวทางการพัฒนาต่อไปนั้น ได้สรุปเป็นแนวทางไว้ดังนี้

1) ควรพัฒนาโปรแกรมให้ครอบคลุมเนื้อหาอื่นๆ ของจำนวนเต็ม เช่น ส่วนกลับกำลังสอง จำนวนเต็มในรูปผลบวกกำลังสอง
2) ควรเพิ่มตัวอย่างการประยุกต์ใช้เลขจำนวนเต็ม เช่น การหาวันของสัปดาห์ การหาวันเกิด การเข้ารหัส

บรรณานุกรม

Gareth A.Jones and J.Mary Jone. 1998. Elementary Number Theory. London : Springer – Verlag London Limited 1998.

รศ.พัชรินทร์ เหมโชติและรศ.ไพรบูลย์ พันธรักษ์พงษ์. 2549. **ทฤษฎีจำนวนและการประยุกต์** 1.กรุงเทพมหานคร : ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

สัจจะ จรัสรุ่งรวีวร. 2544. **คู่มือการเขียนโปรแกรมและใช้งาน** Visual Basic 6.0. กรุงเทพมหานคร : อินโฟเพรส.

ฉัททวุฒิ พีชผล,พิชิต สันติกุลานนท์,พร้อมเลิศ หล่อวิจิตร. 2544. **คู่มือเรียน** Visual Basic 6 **(ฉบับปรับปรุงใหม่)**. กรุงเทพมหานคร : โปรวิชัน.