การศึกษาขั้นตอนวิธีการหาผลบวกกำลังสองสองเทอมของจำนวนเต็ม

ALGORITHM FOR REPRESENTATION OF INTEGER AS SUMS OF TWO SQUARES

ศรัญยา มืดขุนทด

อรอนงค์ อ่อนสกุล

อุไรวรรณ สมบูรณ์

ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาคณิตศาสตร์ประยุกต์

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2557

การศึกษาขั้นตอนวิธีการหาผลบวกกำลังสองสองเทอมของจำนวนเต็ม

ALGORITHM FOR REPRESENTATION OF INTEGER AS SUMS OF TWO SQUARES

ศรัญยา มีดขุนทด

อรอนงค์ อ่อนสกุล

อุไรวรรณ สมบูรณ์

ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาคณิตศาสตร์ประยุกต์

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2557

ALGORITHM FOR REPRESENTATION OF INTEGER AS SUMS OF TWO SQUARES

SARANYA MUEDKHUNTOD

ONANONG ONSAKUN

URAIWAN SOMBOON

A SPECIAL PROBLEM SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIRMENT FOR THE DEGREE OF BACHELOR OF SCIENCE

IN APPLIED MATHEMATICS

DEPARTMENT OF MATHEMATICS

FACULTY OF SCIENCE

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

ACADEMIC YEAR 2014

หัวข้อปัญหาพิเศษ	การศึกษาขั้นตอนวิธีการหาผลบวกกำลังสองสองเทอมของจำนวนเต็ม Algorithm for Representation of Integers as Sums of Two Squares	
ชื่อนักศึกษา	นางสาวศรัญยา มืดขุนทด	54050081
	นางสาวอรอนงค์ อ่อนสกุล	54050109
	นางสาวอุไรวรรณ สมบูรณ์	54050114
ปริญญา	วิทยาศาสตรบัณฑิต (คณิตศาสตร์ประยุกต์)	
ภาควิชา	คณิตศาสตร์	
ปีการศึกษา	2557	
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ไพรบูลย์ พันธรักษ์พงษ์	
	รองศาสตราจารย์ พัชรินทร์ เหมโชติ	

คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุมัติให้ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาคณิตศาสตร์ประยุกต์ ประจำปีการศึกษา 2557

คณะกรรมการสอบ	ลายมือชื่อ
ดร.กัญญ์ณณัฏฐ์ แจ่มศรี ประธานกรรมการ	
ดร.งามเฉิด ด่านพัฒนามงคล กรรมการ	
รศ.ไพรบูลย์ พันธรักษ์พงษ์ กรรมการและอาจารย์ที่ปรึกษา	
รศ.พัชรินทร์ เหมโชติ กรรมการและอาจารย์ที่ปรึกษา	

หัวข้อปัญหาพิเศษ	การศึกษาขั้นตอนวิธีการหาผลบวกกำลังสองสองเทอมของจำนวนเต็ม
ชื่อนักศึกษา	นางสาวศรัญยา มืดขุนทด 54050081
	นางสาวอรอนงค์ อ่อนสกุล 54050109
	นางสาวอุไรวรรณ สมบูรณ์ 54050114
ปริญญา	วิทยาศาสตรบัณฑิต (คณิตศาสตร์ประยุกต์)
ภาควิชา	คณิตศาสตร์
ปีการศึกษา	2557
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ไพรบูลย์ พันธรักษ์พงษ์
	รองศาสตราจารย์ พัชรินทร์ เหมโชติ

บทคัดย่อ

ปัญหาพิเศษนี้เป็นการศึกษาการแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอม จากงานวิจัยที่ศึกษาไว้แล้ว สำหรับ $p=a^2+b^2$ เมื่อ a และ b เป็นจำนวนเต็ม เขียนเป็นผลบวกกำลังสอง 2 เทอมได้ก็ต่อเมื่อ p เป็นจำนวนเฉพาะ รูปแบบ $4k+1$ แล้ว $0<a<\sqrt{p}$ และ $0<b<\sqrt{p}$

ในงานวิจัยนี้พบว่าสำหรับจำนวนเฉพาะ p ที่มีรูปแบบ $4k+1$ และ $a>b$ จะได้ $\sqrt{p/2}<a<\sqrt{p}$ และ $b=\sqrt{p-a^2}$ และสำหรับจำนวนเต็มบวก n ใดๆ ที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้เป็น $n=a^2+b^2$ แล้ว $\sqrt{n/2}\le a\le\sqrt{n}$ และคำนวณ $b=\sqrt{n-a^2}$ การคำนวณค่า a เริ่มจาก $\sqrt{n}$ จะจะพบค่า a ได้เร็วกว่าเริ่มจาก $\sqrt{n/2}$ ในงานวิจัยนี้ได้ศึกษาและออกแบบขั้นตอนวิธีสำหรับตรวจสอบ จำนวนเต็มบวก n ที่สามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ ซึ่งขึ้นกับรูปแบบของจำนวนเฉพาะที่เป็นตัวประกอบ

คำสำคัญ: จำนวนเฉพาะ การแทนจำนวนเต็ม ผลบวกกำลังสอง 2 เทอม

Title	Algorithm for Representation of Integers as Sums of Two Squares
Students	Ms.Saranya Muedkhuntod 54050081
	Ms.Onanong Onsakun 54050109
	Ms.Uriwan Somboon 54050114
Degree	Bachelor of Science (Applied Mathematics)
Department	Mathematics
Academic Year	2014
Advisor	Assoc.Prof.Praiboon Pantaragphong
	Assoc.Prof.Patcharin Hemchote

Abstract

The special problem is to study the representation of integer as sums of two squares. From the related research, for $p=a^2+b^2$ where a and b are integers, p can be representation as sums of two squares if and only if p has the form $4k+1$ and $0<a<\sqrt{p}$ and $0<b<\sqrt{p}$.

In this research it is found that the prime number p in the form $4k+1$ and $a>b$ can obtain $\sqrt{p/2}<a<\sqrt{p}$ and $b=\sqrt{p-a^2}$. For any integer n that can be a representation of integer as sums of two squares, $n=a^2+b^2$, $\sqrt{n/2}\le a\le\sqrt{n}$ and $b=\sqrt{n-a^2}$. The calculation of a, starting with $\sqrt{n}$ is faster than starting with $\sqrt{n/2}$. The research also studies and designs an algorithm for testing that an integer n can be a representation of integer as sums of two squares which depends on the prime factor of n

Keywords: prime number, representation of integer, sum of two squares

กิตติกรรมประกาศ

ปัญหาพิเศษเล่มนี้สำเร็จลุล่วงเป็นอย่างดีก็ด้วยความกรุณาจาก รศ.ไพรบูลย์ พันธรักษ์พงษ์ และ รศ.พัชรินทร์ เหมโชติ อาจารย์ที่ปรึกษาปัญหาพิเศษ ที่ได้ให้คำปรึกษา แนะนำ และช่วยเหลือเติมเต็มในส่วนที่ขาดหายไป คอยให้กำลังใจ และแก้ไขในส่วนที่บกพร่อง จนเป็นผลให้ปัญหาพิเศษฉบับนี้สำเร็จได้ด้วยดี

ขอกราบขอบพระคุณคณาจารย์ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกท่านที่ได้ให้ความรู้และคำแนะนำ และขอขอบคุณรุ่นพี่และเพื่อนๆ ในภาควิชาคณิตศาสตร์ที่คอยช่วยเหลือ และให้คำแนะนำในเรื่องต่างๆ

สุดท้ายนี้ขอขอบพระคุณ คุณพ่อและคุณแม่ของคณะผู้จัดทำ ที่คอยเคี่ยวเข็ญ และสนับสนุนการศึกษา และคอยเป็นกำลังใจจนทำให้ประสบความสำเร็จในวันนี้ได้

นางสาวศรัญยา มีดขุนทด

นางสาวอรอนงค์ อ่อนสกุล

นางสาวอุไรวรรณ สมบูรณ์

สารบัญ

หน้า

สารบัญตาราง

บทที่ 1

บทนำ

ในส่วนบทนำของปัญหาพิเศษเล่มนี้ คณะผู้จัดทำได้กล่าวถึงความเป็นมาและความสำคัญ วัตถุประสงค์ของงานวิจัย ขอบเขตของงานวิจัย ขั้นตอนในการดำเนินการและประโยชน์ที่คาดว่าจะได้รับ ซึ่งมีรายละเอียดดังต่อไปนี้

1.1 ที่มาและความสำคัญของปัญหา

มีการศึกษาถึง การแทนผลบวกกำลังสอง 2 เทอม เพื่อหาวิธีพิจารณาว่าจำนวนเต็มใดๆ เป็นจำนวนเฉพาะหรือไม่ (จำนวนเฉพาะมีประโยชน์มากในปัจจุบันในด้านทฤษฎีการเข้ารหัสลับ) สำหรับจำนวนเต็ม มีบางจำนวนที่สามารถเขียนเป็นผลบวกกำลังสอง 2 เทอม เช่น $13=3^2+2^2$ จำนวนประกอบบางจำนวนเขียนได้แบบเดียว บางจำนวนเขียนได้ 2 แบบ เช่น $68=8^2+2^2$ และ $65=8^2+1^2=7^2+4^2$ มีการศึกษาไว้แล้วว่า จำนวนเฉพาะรูปแบบใดเขียนแทนเป็นรูปผลบวกกำลังสอง 2 เทอมได้ จำนวนประกอบรูปแบบใดที่เขียนแทนได้ สำหรับจำนวนเฉพาะ ในรูปแบบ $p=a^2+b^2$ สามารถหาขอบเขตของจำนวนเต็ม a และ b ได้ แต่ยังไม่ทราบว่าจะหาวิธีใดจึงจะหาได้เร็ว

ปัจจุบันแม้จะมีคอมพิวเตอร์ช่วยในการหาว่าจำนวนเต็มใดสามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ แต่ขั้นตอนวิธีในการเขียนโปรแกรมเพื่อหาผลเฉลยจะขึ้นกับความรู้ทางคณิตศาสตร์

ปัญหาพิเศษนี้จึงสนใจศึกษาวิธีการและขั้นตอนวิธีในการตรวจสอบว่าจำนวนเต็มใดที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ และเขียนโปรแกรมคอมพิวเตอร์แจกแจง ลักษณะของจำนวนที่เขียนได้เพื่อวิเคราะห์หาคุณลักษณะเฉพาะ และศึกษาจำนวนรูปแบบที่เขียนได้ของจำนวนเต็ม

1.2 วัตถุประสงค์ของการทำปัญหาพิเศษ

1. พิจารณาหาการแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม
2. ออกแบบขั้นตอนวิธีการตรวจสอบการแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม
3. พิจารณาหาจำนวนครั้งการคำนวณการแทนด้วยผลบวกกำลังสอง 2 เทอมของจำนวนเต็มตั้งแต่ $1-1000000$
4. พิจารณาหาจำนวนรูปแบบในการแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม

1.3 ขอบเขตของปัญหา

1. ศึกษาวิธีการการพิจารณาผลบวกกำลังสอง 2 เทอมของจำนวนเต็มที่สามารถเขียนแทนได้
2. ศึกษาจำนวนรูปแบบการแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม โดยพิจารณาเพียง 4 กรณี จากทั้งหมด 6 กรณี
3. ศึกษาขั้นตอนวิธีการตรวจสอบจำนวนเต็มที่สามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอม
4. ศึกษาและวิเคราะห์หาขอบเขตการคำนวณหาจำนวนเต็ม a,b ที่ทำให้ $n=a^2+b^2$ โดยศึกษาจากจำนวนเต็มตั้งแต่ $1-1000000$ โดยเขียนโปรแกรมเพื่อช่วยในการคำนวณ

1.4 ขั้นตอนในการดำเนินงาน

1. ศึกษาการแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม
2. ออกแบบขั้นตอนวิธีการตรวจสอบการแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม
3. เขียนโปรแกรมเพื่อหาและแจกแจงจำนวนเต็มที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้
4. วิเคราะห์หาขอบเขตและคุณลักษณะเฉพาะของจำนวนเต็ม a,b ที่ทำให้ $n=a^2+b^2$
5. พิจารณาหาจำนวนรูปแบบของจำนวนเต็ม n ที่แทนด้วยผลบวกกำลังสอง 2 เทอม
6. รวบรวมและจัดทำรายงานโครงงานปัญหาพิเศษ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. เข้าใจในขั้นตอนวิธีตรวจสอบการแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม
2. ได้ขั้นตอนวิธี ที่มีประสิทธิภาพในการตรวจสอบว่าจำนวนเต็ม n ใดเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้
3. ได้รู้และเข้าใจในการหาขอบเขตบนและขอบเขตล่างของจำนวนเต็ม a,b ที่ทำให้ $n=a^2+b^2$ โดยในการคำนวณหาจำนวนเต็ม n ที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอม จะมีจำนวนครั้งในการคำนวณที่น้อยลงกว่าเดิม
4. ได้แนวทางในการคำนวณหาจำนวนเต็ม a,b ว่าควรเริ่มคำนวณจากขอบเขตบนหรือขอบเขตล่างจะพบค่า a,b ได้รวดเร็วกว่า
5. นำไปสู่การเกิดองค์ความรู้ใหม่

1.6 ระยะเวลาการดำเนินงาน

ระยะเวลาการเวลาการดำเนินงานตามแผนงานแสดงไว้ในตารางที่ 1.1

ตาราง 1.1 แสดงระยะเวลาการดำเนินงานตามแผน

กิจกรรม	ระยะเวลาในการดำเนินงาน									
	ปี 2557					ปี 2558				
	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.
1) ศึกษาข้อมูล และเตรียมการทำปัญหาพิเศษ										
2) ศึกษาและออกแบบขั้นตอนวิธีการตรวจสอบและหาจำนวนเต็มที่แทนด้วยผลบวกกำลังสอง 2 เทอม										
3) ออกแบบโปรแกรมเพื่อช่วยในการคำนวณ										
4) นำเสนอความก้าวหน้าของปัญหาพิเศษ										
5) ศึกษาจำนวนครั้งในการคำนวณหาจำนวนเต็ม a,b										
6) ศึกษาจำนวนรูปแบบและข้อสังเกตของผลบวกกำลังสอง 2 เทอมของจำนวนเต็ม										
7) รวบรวมข้อมูลทำรูปเล่ม ปัญหาพิเศษ										
8) นำเสนอปัญหาพิเศษ										

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในส่วนของทฤษฎีและงานวิจัยที่เกี่ยวข้องของปัญหาพิเศษฉบับนี้ ทางคณะผู้จัดทำจะกล่าวถึงความรู้พื้นฐานทางคณิตศาสตร์ที่มีความสำคัญต่อการทำปัญหาพิเศษนี้ โดยแบ่งเนื้อหาออกเป็น 3 เรื่องที่สำคัญ คือ ทฤษฎีบทการหารลงตัว สมภาค จำนวนเฉพาะและการแจกแจง และการแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอมซึ่งมีรายละเอียดดังต่อไปนี้

2.1 ทฤษฎีบทการหารลงตัว (Divisibility)

ทฤษฎีบท 2.1 ขั้นตอนวิธีการหาร
สำหรับจำนวนเต็ม a,b ใดๆ โดยที่ $b>0$ จะมีจำนวนเต็ม q และ r อย่างละหนึ่งจำนวน ที่สอดคล้องกับ $a=qb+r$, $0\le r<b$
q เรียกว่า ผลหาร (quotient) , r เรียกว่าเศษเหลือ (remainder) ในการหาร a ด้วย b

พิสูจน์ ดูในภาคผนวก □

บทแทรก 2.2 สำหรับจำนวนเต็ม a,b ใดๆ โดยที่ $b\neq 0$ จะมีจำนวนเต็ม q และ r อย่างละหนึ่งจำนวน ซึ่ง $a=qb+r$, $0\le r<|b|$

พิสูจน์ ดูในภาคผนวก □

ตัวอย่าง 2.1 จงหา q,r โดยที่ $0\le r<|b|$ ที่ทำให้ $a=qb+r$ เมื่อกำหนด

1) $a=162,b=-5$

จะได้ $162=(-32)(-5)+2$ โดยที่ $q=-32$ และ $r=2$

2) $a=-59,b=-3$

จะได้ $-59=(20)(-3)+1$ โดยที่ $q=20$ และ $r=1$

3) $a=132,b=4$

จะได้ $132=(33)(4)+0$ โดยที่ $q=33$ และ $r=0$

ในการหารจำนวนเต็มด้วยจำนวนเต็ม เราพบว่า เศษที่เกิดจากการหารอาจเป็นศูนย์ได้ จากตัวอย่างที่ 2.1 ข้อ 3) 132 หารด้วย 4 จะได้ว่า $132=(33)(4)+0$ ดังนั้น เศษของการหารคือ 0 เราจะเรียกการหารจำนวนเต็มด้วยจำนวนเต็มแล้วเหลือเศษศูนย์ว่า การหารลงตัว (divisibility) ซึ่งมีนิยามดังนี้

นิยาม 2.1 ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a\neq 0$ จะกล่าวว่า a หาร b ลงตัว (a divisides b) เขียนแทนด้วย $a\mid b$ ถ้ามีจำนวนเต็ม k ที่ทำให้ $b=ak$

และสำหรับกรณีที่ a หาร b ไม่ลงตัว เขียนแทนด้วย $a\nmid b$ โดยจากนิยามที่ 2.1 a เรียกว่า ตัวหาร (divisor) หรือตัวประกอบ (factor) ตัวหนึ่งของ b และ b เรียกว่าพหุคูณ (multiple) ของ a

ถ้า a หาร b ลงตัวแล้ว จะได้ $-a$ หาร b ลงตัวด้วย เนื่องจากเมื่อ $b=ak=(-a)(-k)$

ตัวอย่าง 2.2

1) $13\mid 182$ เพราะมีจำนวนเต็ม 14 ที่ทำให้ $182=(13)(14)$
2) $-5\mid 30$ เพราะมีจำนวนเต็ม -6 ที่ทำให้ $30=(-5)(-6)$
3) $17\mid(-289)$ เพราะมีจำนวนเต็ม -17 ที่ทำให้ $-289=(17)(-17)$
4) $135\mid 0$ เพราะมีจำนวนเต็ม 0 ที่ทำให้ $0=(135)(0)$
5) $4\nmid 15$ เพราะไม่มีจำนวนเต็ม q ใดๆ เลยที่ทำให้ $15=4q$

2.2 สมภาค (Congruences)

เศษเหลือการหาร หรือสมภาค

นิยาม 2.2 ให้ n เป็นจำนวนเต็มบวกที่ถูกตรึงค่า
จำนวนเต็ม a และ b เรียกว่า สมภาค มอดุโล n เขียนแทนด้วย

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

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

ตัวอย่าง 2.3 จากนิยามเมื่อ $n=5$

$4\equiv 14\pmod 5$ เนื่องจาก $4-14=(-2)5$

$-6\equiv 14\pmod 5$ เนื่องจาก $-6-14=(-4)5$

เมื่อ $a \nmid b(\mathrm{mod}\, n)$ กล่าวว่า a ไม่สมภาคกับ b มอดุโล n ซึ่งเขียนแทนด้วย $a \not\equiv b(\mathrm{mod}\, n)$

เช่น $12 \not\equiv 20(\mathrm{mod}\, 5)$ เนื่องจาก 5 หาร $12-20=-8$ ไม่ลงตัว

ทฤษฎีบท 2.3 สำหรับจำนวนเต็ม a และ b
$a \equiv b(\mathrm{mod}\, n)$ ก็ต่อเมื่อ a และ b มีเศษเหลือที่ไม่เป็นลบเหมือนกันเมื่อหารด้วย n

พิสูจน์ ดูในภาคผนวก □

ตัวอย่าง 2.4 เนื่องจากจำนวนเต็ม -56 และ -11 เขียนแสดงได้ในรูปแบบ

$$-56=(-7)9+7 \qquad -11=(-2)9+7$$

มีเศษเหลือเดียวกันคือ 7 จากทฤษฎีบท 2.2 บอกให้รู้ว่า $-56 \equiv -11(\mathrm{mod}\, 9)$

นอกจากนั้น $-31 \equiv 11(\mathrm{mod}\, 7)$ จะได้ว่า -31 และ 11 มีเศษเหลือเดียวกันเมื่อหารด้วย 7

เนื่องจาก $-31=(-5)7+4 \qquad 11=(1)7+4$

ทฤษฎีบท 2.4 ให้ $n>1$ ถูกตรึง และ a,b,c,d เป็นจำนวนเต็มใดๆแล้ว
คุณสมบัติต่อไปนี้เป็นจริง

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

พิสูจน์ ดูในภาคผนวก □

2.3 จำนวนเฉพาะ (Prime)

2.3.1 ทฤษฎีบทหลักมูลเลขคณิต (The Fundamental of Arithmetic)

นิยาม 2.3 จำนวนเต็ม $p>1$ เรียกว่าจำนวนเฉพาะ (prime) ถ้าจำนวนเต็มนั้นมีตัวหารเป็น 1 และ p เท่านั้น จำนวนเต็มที่มากกว่า 1 ซึ่งไม่เป็นจำนวนเฉพาะเรียกว่าจำนวนประกอบ (composite)

ตัวอย่าง 2.5 จงพิจารณาจำนวนต่อไปนี้ จำนวนใดบ้างเป็นจำนวนเฉพาะ และถ้าจำนวนใดไม่เป็นจำนวนเฉพาะแล้วจงแยกตัวประกอบให้อยู่ในรูปผลคูณของจำนวนเฉพาะ

$21, 37, 53, 69, 91, 111, 323, 301$

เนื่องจาก

$21=3\cdot 7$ และ $21=1\cdot 21$		ดังนั้น 21 ไม่เป็นจำนวนเฉพาะ
$37=1\cdot 37$	มีแบบเดียว	ดังนั้น 37 เป็นจำนวนเฉพาะ
$53=1\cdot 53$	มีแบบเดียว	ดังนั้น 53 เป็นจำนวนเฉพาะ
$69=3\cdot 23$ และ $69=1\cdot 69$		ดังนั้น 69 ไม่เป็นจำนวนเฉพาะ
$91=7\cdot 13$	มีแบบเดียว	ดังนั้น 91 ไม่เป็นจำนวนเฉพาะ
$111=3\cdot 37$	มีแบบเดียว	ดังนั้น 111 ไม่เป็นจำนวนเฉพาะ
$323=17\cdot 19$	มีแบบเดียว	ดังนั้น 323 ไม่เป็นจำนวนเฉพาะ
$301=7\cdot 43$	มีแบบเดียว	ดังนั้น 301 ไม่เป็นจำนวนเฉพาะ

ทฤษฎีบท 2.5 ทฤษฎีหลักมูลเลขคณิต

ทุกๆ จำนวนเต็มบวก $n>1$ สามารถแสดงได้ในรูปผลคูณของจำนวนเฉพาะ และเขียนได้เพียงแบบเดียวเท่านั้น โดยไม่คำนึงถึงลำดับของตัวประกอบที่ได้

พิสูจน์ ดูในภาคผนวก □

บทแทรก 2.6 จำนวนเต็มบวก $n>1$

สามารถเขียนได้ในรูปแบบยกกำลังของจำนวนเฉพาะ (Canonical) ได้เพียงแบบเดียวเท่านั้น และ $n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$

โดยที่ $i=1,2,\ldots,r$ แต่ละ k_i เป็นจำนวนเต็มบวก และ

แต่ละ p_i เป็นจำนวนเฉพาะ ที่ $p_1<p_2<\ldots<p_r$

ตัวอย่าง 2.6 จำนวนเต็มต่อไปนี้สามารถเขียนในรูปแบบยกกำลังของจำนวนเฉพาะได้ดังนี้

$$476280 = 2^3 \times 3^5 \times 5 \times 7^2$$

$$113190 = 2 \times 3^2 \times 5 \times 7^3 \times 11$$

2.3.2 การคัดหาจำนวนเฉพาะของ Eratosthenes

นักคณิตศาสตร์ชาวกรีก ชื่อ เอราโตสเทเนส (Eratosthenes) เป็นผู้คิดวิธีการหาจำนวนเฉพาะจากจำนวนนับตั้งแต่ 1 ถึง n ด้วยวิธีการตัดจำนวนนับที่ไม่เป็นจำนวนเฉพาะทิ้ง เราเรียกวิธีนี้ว่า The Sieve of Eratosthenes หรือ ตะแกรงของเอราโตสเทเนส

ทฤษฎีบท 2.7 ถ้า n เป็นจำนวนเต็มบวกที่มากกว่า 1 และ $n=ab$ แล้ว $a \le \sqrt{n}$ หรือ $b \le \sqrt{n}$

พิสูจน์ สมมติว่า $a > \sqrt{n}$ และ $b > \sqrt{n}$

จาก $n=ab$

จะได้ $n > \sqrt{n}\sqrt{n}$

$n > n$

ซึ่งเกิดการขัดแย้ง

ดังนั้นสรุปได้ว่า $a \le \sqrt{n}$ หรือ $b \le \sqrt{n}$ □

การพิจารณาจำนวนเฉพาะตั้งแต่ $2-n$

ขั้นตอนวิธีการของ Sieve of Eratosthenes มีดังต่อไปนี้

1) เขียนจำนวนเต็มทั้งหมดตั้งแต่ 2 ถึง n
2) ตัดจำนวนที่ 2 หารลงตัวออกให้หมดยกเว้น 2
3) จำนวนที่ถัดจาก 2 และไม่โดนตัดทิ้งคือ 3 ซึ่งเป็นจำนวนเฉพาะจากนั้นให้ตัดจำนวนที่ 3 หารลงตัวออกให้หมดยกเว้น 3
4) จำนวนที่ถัดจาก 3 และไม่โดนตัดทิ้งคือ 5 ซึ่งเป็นจำนวนเฉพาะจากนั้นให้ตัดจำนวนที่ 5 หารลงตัวออกให้หมดยกเว้น 5
5) จำนวนที่ถัดจาก 5 และไม่โดนตัดทิ้งคือ 7 ซึ่งเป็นจำนวนเฉพาะจากนั้นให้ตัดจำนวนที่ 7 หารลงตัวออกให้หมดยกเว้น 7
6) ทำเช่นนี้เรื่อยไปจนถึงจำนวน $\sqrt{n}$
7) จำนวนที่เหลือทั้งหมดเป็นจำนวนเฉพาะ

การพิจารณาว่าจำนวนเต็มใดเป็นจำนวนเฉพาะ

ขั้นตอนวิธีมีดังต่อไปนี้

1. จำนวนเต็มที่ต้องการพิจารณา n โดย $n>1$
2. หาร n ด้วยจำนวนเฉพาะที่น้อยกว่า $\sqrt{n}$
3. ถ้ามีจำนวนเฉพาะที่หาร n ลงตัวจะได้ว่า n ไม่เป็นจำนวนเฉพาะ แต่ถ้าไม่มีจำนวนเฉพาะใดหารลงตัว จะได้ว่า n เป็นจำนวนเฉพาะ

ตัวอย่าง 2.7 จงพิจารณาว่า $n = 509$ เป็นจำนวนเฉพาะหรือจำนวนประกอบ

เนื่องจาก $\sqrt{509} = 22.5610$ ซึ่ง $22 < \sqrt{509} < 23$

จึงพิจารณาโดยใช้จำนวนเฉพาะที่ไม่เกิน 22 เท่านั้นเป็นตัวหาร ได้แก่ 2, 3, 5, 7, 11, 16, 17, 19 เมื่อนำแต่ละจำนวนไปหาร 509 พบว่าไม่มีจำนวนใดหาร 509 ลงตัว สรุปได้ว่า 509 เป็นจำนวนเฉพาะ

2.4 การแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอม

ทฤษฎีบท 2.8 ไม่มีจำนวนเฉพาะ p ในรูปแบบ $4k+3$ ที่เขียนแทนด้วยผลบวกของกำลังสอง 2 เทอม

พิสูจน์ จะพิสูจน์ว่าไม่มี $p=4k+3$ ที่เป็น $p=a^2+b^2$

ให้ a,b จำนวนเต็มใดๆ

a จะมีรูปแบบเป็น $4k+0, 4k+1, 4k+2$ และ $4k+3$ สำหรับบางจำนวนเต็ม k

เมื่อ มอดุโล a ด้วย 4 จะได้ว่า $a \equiv 0,1,2,3 \pmod 4$

พิจารณารูปแบบของ a^2 โดยทฤษฎีบท 2.4 ข้อ 4 จะได้ว่า

เมื่อ $a \equiv 0 \pmod 4$ จะได้ $a^2 \equiv 0 \cdot 0 \equiv 0 \pmod 4$,

$a \equiv 1 \pmod 4$ จะได้ $a^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4$,

$a \equiv 2 \pmod 4$ จะได้ $a^2 \equiv 2 \cdot 2 \equiv 0 \pmod 4$,

$a \equiv 3 \pmod 4$ จะได้ $a^2 \equiv 3 \cdot 3 \equiv 1 \pmod 4$

ดังนั้น $a^2 \equiv 0,1 \pmod 4$

ทำนองเดียวกัน จะได้ $b^2 \equiv 0,1 \pmod 4$

พิจารณาเมื่อ a^2+b^2 โดยทฤษฎีบท 2.4 ข้อ 4 จะได้ว่า

เมื่อ $a \equiv 0, b \equiv 0 \pmod 4$ จะได้ $a^2+b^2 \equiv 0+0 \equiv 0 \pmod 4$,

$a \equiv 0, b \equiv 1 \pmod 4$ จะได้ $a^2+b^2 \equiv 0+1 \equiv 1 \pmod 4$,

$a \equiv 1, b \equiv 0 \pmod 4$ จะได้ $a^2+b^2 \equiv 1+0 \equiv 1 \pmod 4$,

$a \equiv 1, b \equiv 1 \pmod 4$ จะได้ $a^2+b^2 \equiv 1+1 \equiv 2 \pmod 4$

ดังนั้น $a^2+b^2 \equiv 0,1,2 \pmod 4$

นั่นคือถ้า p มีรูปแบบ $4k+3$ หรือ $p \equiv 3 \pmod 4$ สมการ $p = a^2 + b^2$ เมื่อ a, b เป็นจำนวนเต็มใดๆ จึงเป็นไปไม่ได้

สรุปได้ว่าไม่มีจำนวนเฉพาะ p ในรูปแบบ $4k+3$ ที่แทนด้วยผลบวกของกำลังสอง 2 เทอม □

ทฤษฎีบท 2.9 ทฤษฎีบทวิลสัน (Wilson's Theorem)
ถ้า p เป็นจำนวนเฉพาะ แล้ว $p \mid (p-1)!+1$

พิสูจน์ ดูในภาคผนวก □

ทฤษฎีบท 2.10 (แฟร์มา) จำนวนเฉพาะคี่ p เขียนแทนด้วยผลบวกของกำลังสอง 2 เทอมของจำนวนเต็มได้ ก็ต่อเมื่อ $p \equiv 1 \pmod 4$

พิสูจน์ สมมติว่า p สามารถเขียนได้เป็นผลบวกกำลังสอง 2 เทอมให้เป็น $p = a^2 + b^2$

เพราะว่า p เป็นจำนวนเฉพาะจะได้ $p \nmid a$ และ $p \nmid b$

ถ้า $p \mid a$ แล้ว $p \mid b^2$ และ $p \mid b$ ให้ $a = kp$ และ $b = rp$ สำหรับจำนวนเต็ม k, r บางจำนวน และ $p = a^2 + b^2 = (kp)^2 + (rp)^2 = p^2(k^2 + r^2)$ แสดงว่า $p^2 \mid p$ ซึ่งนำไปสู่ข้อขัดแย้ง+

โดยทฤษฎีบทของสมภาคเชิงเส้น มีจำนวนเต็ม c สำหรับ $bc \equiv 1 \pmod p$

ด้วยมอดุโล p ความสัมพันธ์ $(ac)^2 + (bc)^2 = pc^2$ เปลี่ยนเป็นสมภาคได้

$$(ac)^2 \equiv -1 \pmod p$$

ทำให้ -1 เป็นส่วนตกค้างกำลังสองของ p

โดยนิยามสัญลักษณ์เลอจองด์จะได้ว่า สำหรับ $x^2 \equiv -1 \pmod p$ เมื่อ $p \equiv 1 \pmod 4$ เท่านั้น

ในทางกลับกัน สมมติว่า $p \equiv 1 \pmod 4$ เพราะว่า -1 เป็นส่วนตกค้างกำลังสองของ p สามารถหาจำนวนเต็ม a ที่สอดคล้องกับ $a^2 \equiv -1 \pmod 4$

จากทฤษฎีบทวิลสัน $a = [(p-1)/2]!$ เป็นจำนวนเต็มหนึ่ง

ขณะนี้ $\gcd(a,p)=1$ เพื่อที่สมภาค $ax \equiv y \pmod{p}$

มีผลเฉลย x_0, y_0 ซึ่งเป็นข้อสรุปตามบทตั้งของ Thue เป็นจริง จึงได้ผลเป็น

$$-x_0^2 \equiv a^2 x_0^2 \equiv (ax_0)^2 \equiv y_0^2 \pmod{p}$$

หรือ $$x_0^2 + y_0^2 \equiv 0 \pmod{p}$$

หรือกล่าวได้ว่า $x_0^2 + y_0^2 \equiv kp$ สำหรับจำนวนเต็ม $k \geq 1$

ขณะที่ $0 < |x_0| < \sqrt{p}$ และ $0 < |y_0| < \sqrt{p}$ จึงได้ $0 < x_0^2 + y_0^2 < 2p$

มีความหมายว่า $k=1$ ผลตามมาได้ $x_0^2 + y_0^2 = p$ □

ตัวอย่าง 2.8 จำนวนเฉพาะที่มีรูปแบบ $4k+1$ $p = 5, 17, 29, 37, 41$

$5 = 2^2 + 1^2$ $17 = 4^2 + 1^2$ $29 = 5^2 + 2^2$

$37 = 6^2 + 1^2$ $41 = 5^2 + 4^2$

บทแทรก 2.11 จำนวนเฉพาะ p ใดๆ ที่มีรูปแบบ $4k+1$
เขียนเป็นผลบวกกำลังสอง 2 เทอมได้เพียงรูปแบบเดียว (ไม่คำนึงลำดับ)

พิสูจน์ จะแสดงว่ามีแบบเดียว สมมติให้ $p = a^2 + b^2 = c^2 + d^2$

เมื่อ a, b, c, d เป็นจำนวนเต็มบวก

จะได้ว่า $(ad - bc)(ad + bc) = a^2 d^2 - b^2 c^2 = p(d^2 - b^2) \equiv 0 \pmod{p}$

ฉะนั้น $p \mid ad - bc$ หรือ $p \mid ad + bc$

เพราะว่า a, b, c, d ทุกจำนวนน้อยกว่า $\sqrt{p}$ ความสัมพันธ์นี้ได้

$$ad - bc = 0 \text{ หรือ } ad + bc = p$$

กรณีที่ 1 สมมติ $ad + bc = p$ แล้ว

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

$$= (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2$$

ดังนั้น $ac-bd=0$ นั่นคือ $ac=bd$

เพราะว่า $a|bd$ และ $\gcd(a,b)=1$ ทำให้ได้ $a|d$ นั่นคือ $d=ka$ สำหรับบางจำนวน k

จาก $ac=bd=b(ak)$

จะได้ $c=bk$

$$p=c^2+d^2=k^2(a^2+b^2)$$

ทำให้ได้ว่า $k=1$ และได้ว่า $a=d$ และ $b=c$

กรณีที่ 2 สมมติว่า $ad-bc=0$ นั่นคือ $ad=bc$ ด้วยการพิจารณาในทำนองเดียวกันกับวิธีที่ 1

จะได้ว่า $a=c$ และ $b=d$

จึงสรุปได้ว่าการแทนจำนวนเฉพาะ p ด้วยผลบวกกำลังสอง 2 เทอมได้แบบเดียวเท่านั้น □

บทตั้ง 2.12 ถ้า n และ m เขียนเป็นผลบวกของกำลังสอง 2 เทอม แล้ว ผลคูณ mn เขียนเป็นผลบวกของกำลังสอง 2 เทอม

พิสูจน์ ให้ $m=a^2+b^2$ และ $n=c^2+d^2$ สำหรับจำนวนเต็ม a,b,c,d

แล้ว $mn=(a^2+b^2)(c^2+d^2)=a^2c^2+a^2d^2+b^2c^2+b^2d^2$

$$=a^2c^2+a^2d^2+2abcd+b^2c^2+b^2d^2-2abcd$$

$$=(ac+bd)^2+(ad-bc)^2 \quad (1)$$

ดังนั้น mn เขียนเป็นผลบวกกำลังสอง 2 เทอม ได้

บทตั้งไม่ได้สรุปว่ามีกี่แบบ จากวิธีพิสูจน์เมื่อจัดกลุ่มใหม่ แล้วผลคูณจะได้ดังนี้

$$mn=(a^2+b^2)(c^2+d^2)=a^2c^2+a^2d^2+b^2c^2+b^2d^2$$

$$=a^2c^2+a^2d^2-2abcd+b^2c^2+b^2d^2+2abcd$$

$$=(ac-bd)^2+(ad+bc)^2 \quad (2)$$

ในกรณีที่สลับตำแหน่งใน n เป็น $n=d^2+c^2$ จะได้สูตร (1) หรือ (2) ขึ้นกับการจัดกลุ่ม □

ตัวอย่าง2.9 ผลคูณของสองจำนวนที่มีรูปผลบวกกำลังสอง 2 เทอม

1) จำนวนเต็ม $85=5\cdot17$ จำนวนเฉพาะคี่ $5=2^2+1^2$ และ $17=4^2+1^2$

$$\begin{aligned}85=5\cdot17&=\left(2^2+1^2\right)\left(4^2+1^2\right)\\&=\left(2\cdot4+1\cdot1\right)^2+\left(2\cdot1-1\cdot4\right)^2 \quad \text{(ใช้สูตร (1) ตามบทตั้ง)}\\&=9^2+2^2\end{aligned}$$

$$\begin{aligned}85=5\cdot17&=\left(2^2+1^2\right)\left(4^2+1^2\right)\\&=\left(2\cdot4-1\cdot1\right)^2+\left(2\cdot1+1\cdot4\right)^2 \quad \text{(ใช้สูตร (2) ตามบทตั้ง)}\\&=7^2+6^2\end{aligned}$$

2) จำนวนเต็ม $493=17\cdot29$ จำนวนเฉพาะคี่ $17=4^2+1^2$ และ $29=5^2+2^2$

$$\begin{aligned}493=17\cdot29&=\left(4^2+1^2\right)\left(5^2+2^2\right)\\&=\left(4\cdot5+1\cdot2\right)^2+\left(4\cdot2-1\cdot5\right)^2 \quad \text{(ใช้สูตร (1) ตามบทตั้ง)}\\&=22^2+3^2\end{aligned}$$

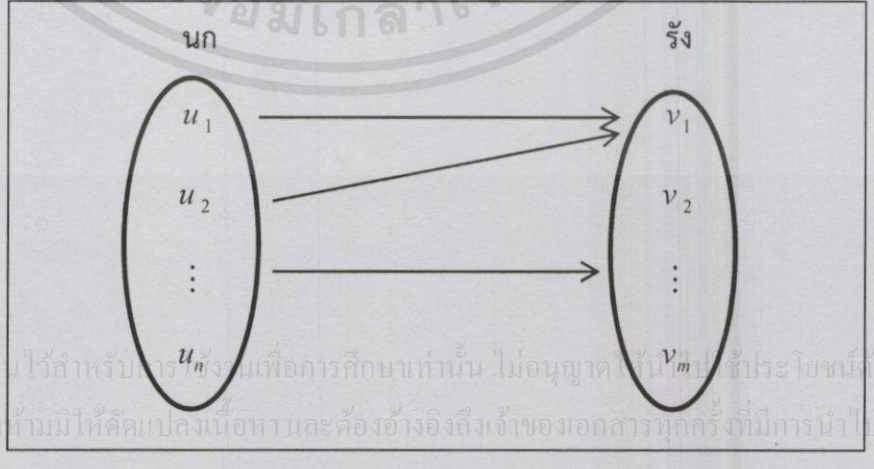
$$\begin{aligned}493=17\cdot29&=\left(4^2+1^2\right)\left(5^2+2^2\right)\\&=\left(4\cdot5-1\cdot2\right)^2+\left(4\cdot2+1\cdot5\right)^2 \quad \text{(ใช้สูตร (2) ตามบทตั้ง)}\\&=18^2+13^2\end{aligned}$$

ทฤษฎีบท 2.13 หลักการรังนกพิราบ (Pigeonhole principle)

ให้ $m,n\in\mathbb{Z}^+$

ถ้ามีนกพิราบอย่างน้อย n ตัว บินเข้ารัง m รัง และถ้า $n>m$

แล้วจะมีรังอย่างน้อย 1 รัง ที่มีนกพิราบอย่างน้อย 2 ตัว



จะมีบางรังที่มีนกมากกว่า 1 ตัว

$$\exists v_1 = f(u_1)$$

$$\exists v_1 = f(u_2)$$

$$u_1 \neq u_2 \rightarrow f(u_1) = f(u_2)$$

กล่าวได้ว่า หากมีนกพิราบอยู่ n ตัว แล้วต้องการนำนกพิราบเหล่านี้ไปใส่ในรังนกพิราบที่มีอยู่ m รัง โดยที่ $n > m$ แล้ว จะได้ว่าจะมีรังนกอย่างน้อย 1 รังที่จะมีนกพิราบอยู่มากกว่า 1 ตัว

ตัวอย่าง 2.10 สมมติว่าในกล่องใบหนึ่งมีถึงเท่าสีขาวอยู่ 12 ข้าง และสีดำอยู่ 10 ข้าง จงหาจำนวนครั้งในการหยิบน้อยที่สุดที่จะรับประกันได้เลยว่าจะได้ถุงเท้าสีเดียวกันหนึ่งคู่

จะได้ว่า มีรังนกสีขาวและสีดำ 2 รัง $(m = 2)$

จากหลักรังนกพิราบจะได้ว่าต้องหา $n > m$ ที่น้อยที่สุดนั่นก็คือ $n = 3$ จะเห็นว่าถ้าเราหยิบถุงเท้ามาแล้วสองข้าง $(n = 2)$ อย่างแย่ที่สุดเราก็จะมีถุงเท้าสีขาวและสีดำอย่างละข้างเมื่อหยิบอีกหนึ่งข้าก็ต้องได้ครบคู่

บทตั้ง 2.14 บทตั้งของ Thue (Thue's lemma)
ให้ p เป็นจำนวนเฉพาะและ $\gcd(a,p) = 1$ แล้วสมภาค $ax \equiv y \pmod{p}$
มีผลเฉลย x_0, y_0 ซึ่ง $0 < |x_0| < \sqrt{p}$ และ $0 < |y_0| < \sqrt{p}$

พิสูจน์ ให้ $k = \lfloor \sqrt{p} + 1 \rfloor$ และพิจารณาเซตของจำนวนเต็ม

$$S = \{ax - y \mid 0 \leq x \leq k-1, 0 \leq y \leq k-1\}$$

เพราะว่า $ax - y$ เกิดจาก $k^2 > p$ บางค่าที่เป็นไปได้

หลักการรังนกพิราบรับประกันว่ามีอย่างน้อย 2 สมาชิกของ S ต้องสมภาคมอดุโล p

ให้เป็น $ax_1 - y_1$ และ $ax_2 - y_2$ เมื่อ $x_1 \neq x_2$ หรือ $y_1 \neq y_2$ แล้วสามารถเขียน

$$a(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}$$

ให้ $x_0 = x_1 - x_2$ และ $y_0 = y_1 - y_2$

ผลตามมาได้ x_0 และ y_0 ให้ผลเฉลยสมภาค $ax \equiv y(\text{mod } p)$

เพราะว่า $\gcd(a, p) = 1$ ถ้า x_0 หรือ y_0 ไม่เป็นศูนย์แล้ว

แสดงว่า อีกจำนวนต้องเป็นศูนย์ ซึ่งขัดแย้งกับสมมติฐาน

ฉะนั้น $0 < x_0 \le k-1 < \sqrt{p}$ และ $0 < y_0 \le k-1 < \sqrt{p}$ □

จำนวนอิสระกำลังสอง

จำนวนอิสระกำลังสอง (square-free หรือ quadratfrei) เป็นจำนวนที่หารไม่ลงตัวด้วยจำนวนที่เขียนรูปกำลังสอง หรือกล่าวอีกอย่างว่า ไม่มีตัวประกอบจำนวนเฉพาะซ้ำ ดังนั้น ชัดเจนว่าจำนวนเฉพาะทุกจำนวนเป็นอิสระกำลังสอง

ยกตัวอย่าง จำนวนอิสระกำลังสอง มีดังนี้

$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 33, 34, 35, 37, 38, 39, \ldots$

18 ไม่เป็นจำนวนอิสระกำลังสองเพราะหารลงตัวด้วย $9 = 3^2$

จำนวนเต็มที่ไม่เป็นอิสระกำลังสอง เป็นจำนวนที่มีจำนวนรูปกำลังสองอย่างน้อยหนึ่งจำนวนเป็นตัวประกอบ หรือหารลงตัว เช่น $4, 8, 9, 12, 16, 18, 20, 24, 25$

ทฤษฎีบท 2.15 ให้ n เป็นจำนวนเต็มบวก $n = N^2 m$ เมื่อ m เป็นจำนวนอิสระกำลังสอง แล้ว n แทนได้ด้วยผลบวกของกำลังสอง 2 เทอม ก็ต่อเมื่อ m ไม่มีตัวประกอบเป็นจำนวนเฉพาะในรูป $4k+3$

พิสูจน์ สมมติให้ m ไม่มีตัวประกอบที่เป็นจำนวนเฉพาะในรูปแบบ $4k+3$

ถ้า $m = 1$ แล้ว $n = N^2 + 0^2$

กรณี $m > 1$ ให้ $m = p_1 p_2 \ldots p_r$ มีตัวประกอบในรูปผลคูณของจำนวนเฉพาะที่ต่างกัน

แต่ละจำนวนเฉพาะ p_i เป็น 2 หรือเป็นรูปแบบ $4k+1$ เขียนเป็นผลบวกของกำลังสอง 2 เทอมได้ โดยเอกลักษณ์

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 (ad - bc)^2$$

แสดงว่าผลคูณของจำนวนเต็ม 2 จำนวน (และโดยอุปนัย จำนวนจำกัดใดๆ) แต่ละจำนวนแทนได้ด้วยผลบวกกำลังสอง 2 เทอม

ดังนั้น จะมีจำนวนเต็ม x และ y สอดคล้องกับ $m = x^2 + y^2$ และจะได้

$$n = N^2 m = N^2(x^2 + y^2) = (Nx)^2 + (Ny)^2$$

เป็นผลบวกของกำลังสอง 2 เทอม

ในทางตรงกันข้าม สมมติว่า n เขียนแทนด้วยผลบวกกำลังสอง 2 เทอม

$$n = a^2 + b^2 = N^2 m$$

และให้ p เป็นตัวหารที่เป็นจำนวนเฉพาะคี่ใดๆ ของ m (เพื่อให้เป็นกรณีทั่วไป สมมติให้ $m > 1$)

ถ้า $d = \gcd(a,b)$ แล้ว $a = rd, b = sd$ เมื่อ $\gcd(r,s) = 1$ จะได้

$$d^2(r^2 + s^2) = N^2 m$$

จาก m เป็นอิสระกำลังสอง ดังนั้น $d^2 \mid N^2$ และได้

$$r + s = \left(\frac{N^2}{d^2}\right) m = tp \quad \text{สำหรับบางจำนวนเต็ม } t$$

ซึ่งนำไปสู่ $r^2 + s^2 \equiv 0 \pmod{p}$

ขณะนี้ด้วยเงื่อนไข $\gcd(r,s) = 1$ ได้ว่าหนึ่งจำนวนจาก r หรือ s เป็นจำนวนเฉพาะสัมพัทธ์กับ p ให้เป็น r และ r' สอดคล้องกับ $rr' \equiv 1 \pmod{p}$

เมื่อ $r^2 + s^2 \equiv 0 \pmod{p}$ เป็นพหุคูณ โดย $(r')^2$ ได้

$$(sr')^2 + 1 \equiv 0 \pmod{p}$$

เพราะว่า -1 เป็นส่วนตกค้างกำลังสองของ p โดยทฤษฎีคุณสมบัติของเลอจองด์

จะได้ว่า $p \equiv 1 \pmod{4}$

จึงได้ว่าไม่มีจำนวนเฉพาะที่อยู่ในรูปแบบ $4k + 3$ หาร m ลงตัว □

บทแทรก 2.16 จำนวนเต็มบวก n เขียนแทนได้ด้วยผลบวกของกำลังสอง 2 เทอมก็ต่อเมื่อ แต่ละตัวประกอบที่เป็นจำนวนเฉพาะรูปแบบ $4k+3$ มีกำลังเป็นจำนวนคู่

ตัวอย่าง 2.11 พิจารณาการเขียนเป็นผลบวกของกำลังสอง 2 เทอม ของจำนวนต่อไปนี้

1) $459=3^3\cdot 17$ เนื่องจาก จำนวนเฉพาะ 3 มีรูปแบบเป็น $4k+3$ มีกำลังเป็นจำนวนคี่ ดังนั้น 459 ไม่สามารถเขียนเป็นผลบวกของกำลังสอง 2 เทอมได้

2) $153=3^2\cdot 17$ สามารถเขียนเป็นผลบวกของกำลังสอง 2 เทอมได้

เนื่องจาก จำนวนเฉพาะ 3 มีรูปแบบเป็น $4k+3$ มีกำลังเป็นจำนวนคู่ จึงเขียนได้ จำนวนเฉพาะ 17 มีรูปแบบเป็น $4k+1$ ดังนั้น 153 จึงเขียนได้และสามารถเขียนได้เพียงรูปแบบเดียวเท่านั้น โดยขึ้นอยู่กับจำนวนเฉพาะรูปแบบ $4k+1$

ดังนั้น $153=3^2\left(4^2+1^2\right)=12^2+3^2$

พิจารณาตามบทตั้ง 2.12

$$\begin{aligned}153=17\cdot 9&=\left(4^2+1^2\right)\left(3^2+0^2\right)\\&=\left(4\cdot 0+1\cdot 3\right)^2+\left(4\cdot 3-1\cdot 0\right)^2\\&=3^2+12^2\end{aligned}$$

$$\begin{aligned}153=17\cdot 9&=\left(4^2+1^2\right)\left(3^2+0^2\right)\\&=\left(4\cdot 3-1\cdot 0\right)^2+\left(4\cdot 0+1\cdot 3\right)^2\\&=12^2+3^2\end{aligned}$$

กรณีนี้เป็นจำนวนเดียวกันและมีรูปแบบเดียว

3) $54145=5\cdot 7^2\cdot 13\cdot 17$ สามารถเขียนเป็นผลบวกกำลังสอง 2 เทอมได้

เนื่องจาก จำนวนเฉพาะที่มีรูปแบบ $4k+3$ มีกำลังเป็นจำนวนคู่ จำนวนที่มีผลต่อรูปแบบมีทั้งหมด 3 จำนวน ซึ่งเป็นจำนวนเฉพาะที่มีรูปแบบ $4k+1$

จาก $54145=7^2\cdot 5\cdot 13\cdot 17=7^2\left(2^2+1^2\right)\left(3^2+2^2\right)\left(4^2+1^2\right)$

ขั้นที่ 1 พิจารณาทีละคู่ 1 คู่ ได้ 2 แบบ

$$\left(2^2+1^2\right)\left(3^2+2^2\right)=\left(12+2\right)^2+\left(3-8\right)^2=14^2+5^2$$

และ $\left(2^2+1^2\right)\left(3^2+2^2\right)=(12-2)^2+(3+8)^2=10^2+11^2$

ขั้นที่ 2 นำผลขั้นที่ 1 มาพิจารณากับพจน์ใหม่

จากแบบที่ 1 $\left(2^2+1^2\right)\left(14^2+5^2\right)=(28+5)^2+(10-14)^2=33^2+4^2$

และ $\left(2^2+1^2\right)\left(14^2+5^2\right)=(28-5)^2+(10+14)^2=23^2+24^2$

จากแบบที่ 2 $\left(2^2+1^2\right)\left(11^2+10^2\right)=(22+10)^2+(20-11)^2=32^2+9^2$

และ $\left(2^2+1^2\right)\left(11^2+10^2\right)=(22-10)^2+(20+11)^2=12^2+31^2$

ขั้นที่ 3 นำผลขั้นที่ 2 มาพิจารณากับพจน์ใหม่ โดยคูณกับ 7^2 จะได้

$54145=7^2\left(33^2+4^2\right)=231^2+28^2,\ 54145=7^2\left(24^2+23^2\right)=168^2+161^2$

$54145=7^2\left(32^2+9^2\right)=224^2+63^2,\ 54145=7^2\left(31^2+12^2\right)=217^2+84^2$

บทที่ 3

ขั้นตอนวิธีการหาผลบวกกำลังสอง 2 เทอม

ในส่วนวิธีการดำเนินงานวิจัยของปัญหาพิเศษฉบับนี้ ทางคณะผู้จัดทำ ได้ทำการศึกษาและได้รวบรวมเนื้อหาที่มีความสำคัญ สามารถนำมาใช้ในการสร้างทฤษฎีบทใหม่ขึ้นมา โดยเนื้อหาที่นำมาใช้ ได้แก่ นิยาม ทฤษฎีบท บทแทรก บทตั้ง ข้อสังเกต คุณสมบัติ และตัวอย่าง ซึ่งมีรายละเอียดดังต่อไปนี้

3.1 วิธีพิจารณาผลบวกกำลังสอง 2 เทอม

3.1.1 การพิจารณาผลบวกกำลังสอง 2 เทอม ของจำนวนเฉพาะ p ที่มีรูปแบบ $4k+1$

โดยทฤษฎีบทแฟร์มา ในหัวข้อ 2.4 กล่าวไว้เพียงว่า สำหรับจำนวนเฉพาะ p ที่มีรูปแบบ $4k+1$ สามารถเขียนเป็นผลบวกกำลังสอง 2 เทอมได้เพียงรูปแบบเดียวเท่านั้น แต่ไม่ได้กล่าวว่ารูปแบบเดียวที่เขียนได้เขียนได้อย่างไร มีขั้นตอนในการหาอย่างไร ในหัวข้อนี้จะแสดงวิธีการหา จำนวนเต็ม a และ b ที่ทำให้ $p=a^2+b^2$

ทฤษฎีบท 3.1 สำหรับจำนวนเฉพาะ p ซึ่งมีรูปแบบ $4k+1$ และ $p=a^2+b^2$ ถ้า $a>b$ แล้ว $\sqrt{p/2}<a<\sqrt{p}$

พิสูจน์ ให้ $p=a^2+b^2$ และให้ $a>b$

จากบทตั้งของ Thue จะได้ว่าจำนวนเต็ม a,b มีค่าระหว่าง $0<a<\sqrt{p}$ และ $0<b<\sqrt{p}$

กรณีที่ $b=0$ จะได้ว่า $a=\sqrt{p}$

และ สำหรับจำนวนเต็ม $b>0$ จะได้ว่า a เป็นจำนวนเต็มที่น้อยกว่า $\sqrt{p}$

ซึ่งถ้าค่าของ a ลดลง ค่าของ b จะเพิ่มขึ้น

และลดลงได้เพียง a และ b เท่ากัน เพราะว่า $\left(\sqrt{p/2}\right)^2+\left(\sqrt{p/2}\right)^2=p$

ดังนั้นจำนวนเต็ม a มีค่า $\sqrt{p/2}<a<\sqrt{p}$

และหาจำนวนเต็ม b จาก $b^2=p-a^2$ จะได้ $b=\sqrt{p-a^2}$ □

3.1.2 การพิจารณาผลบวกกำลังสอง 2 เทอม ของจำนวนเต็ม n

ทฤษฎีบท 3.2 สำหรับจำนวนประกอบ n ที่เขียนแทนด้วย $n=a^2+b^2$ และ $n=4k+1$ ถ้า $a>b$ แล้ว $\sqrt{n/2}\le a\le\sqrt{n}$

พิสูจน์ ให้ $n=a^2+b^2$ และให้ $a>b$

จากบทตั้งของ Thue จะได้ว่าจำนวนเต็ม a,b มีค่าระหว่าง $0\le a\le\sqrt{n}$ และ $0\le b\le\sqrt{n}$

กรณีที่ $b=0$ จะได้ว่า $a=\sqrt{n}$

และ สำหรับจำนวนเต็ม $b>0$ จะได้ว่า a เป็นจำนวนเต็มที่น้อยกว่า $\sqrt{n}$

ซึ่งถ้าค่าของ a ลดลง ค่าของ b จะเพิ่มขึ้น

และลดลงได้เพียง a และ b เท่ากัน เพราะว่า $\left(\sqrt{n/2}\right)^2+\left(\sqrt{n/2}\right)^2=n$

ดังนั้นจำนวนเต็ม a มีค่า $\sqrt{n/2}\le a\le\sqrt{n}$

และหาจำนวนเต็ม b จาก $b^2=n-a^2$ จะได้ $b=\sqrt{n-a^2}$ □

จากทฤษฎีบทข้างต้นจะรู้เพียงขอบบน และขอบล่างของ a แนวทางในการหา a จะทดลองคำนวณหา a และ b ที่สอดคล้อง เป็นไปได้ 2 วิธี ดังต่อไปนี้

วิธีที่ 1 เริ่มแทนค่าจากขอบบน

ให้ a เป็นจำนวนเต็มที่มากที่สุดที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$ คำนวณค่า $b_0=n-a^2$

และพิจารณาถ้า b_0 เป็นจำนวนรูปกำลังสองให้คำนวณ $b=\sqrt{b_0}$

ถ้าไม่ใช่ให้ลดค่าของ a ลง 1 จนถึงให้ a ที่เป็นจำนวนเต็มที่น้อยที่สุดที่มากกว่าหรือเท่ากับ $\sqrt{n/2}$ โดยในแต่ละค่าของ a ให้พิจารณาด้วยวิธีการเดียวกันจนกว่าจะพบค่า a และ b ที่สอดคล้อง

สำหรับ n ที่เป็นจำนวนประกอบอาจมีมากกว่า 1 ชุด

ถ้า n เป็นจำนวนเฉพาะจะมีเพียงชุดเดียว

วิธีที่ 2 เริ่มแทนค่าจากขอบล่าง

ให้ a เป็นจำนวนเต็มที่น้อยที่สุดที่มากกว่าหรือเท่ากับ $\sqrt{n/2}$ คำนวณค่าโดยวิธีเดียวกันกับวิธีที่ 1 ถ้าไม่ใช่ให้เพิ่มค่าของ a ขึ้นอีก 1 จนถึง a ที่เป็นจำนวนเต็มที่มากที่สุดที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$ โดยในแต่ละค่าของ a ให้พิจารณาด้วยวิธีการเดียวกัน จนกว่าจะพบค่า a และ b ที่สอดคล้อง

ตัวอย่าง 3.1 การพิจารณาผลบวกของกำลังสอง 2 เทอม ของจำนวนเฉพาะ $p=181$

หาจำนวนเต็ม a และ b ที่สอดคล้องกับ $181=a^2+b^2$

จำนวนเต็ม a ตั้งแต่ $a=10>\sqrt{181/2}$

ถึง $a=13<\sqrt{181}$

ดังนั้น จำนวนเต็ม a มีค่าอยู่ระหว่าง $10\le a\le 13$

วิธีที่ 1 คำนวณค่า a โดยเริ่มจากขอบบน และลดค่าของ a ลงครั้งละ 1

ครั้งที่ 1 เลือก $a=13$ หา b โดย $b^2=p-a^2=181-169=12$

เนื่องจาก $p-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 2 เลือก $a=12$ หา b โดย $b^2=p-a^2=181-144=37$

เนื่องจาก $p-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 3 เลือก $a=11$ หา b โดย $b^2=p-a^2=181-121=60$

เนื่องจาก $p-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 4 เลือก $a=10$ หา b โดย $b^2=p-a^2=181-100=81=9^2$

เนื่องจาก $p-a^2$ เป็นจำนวนกำลังสอง จะได้ $b=9$

ดังนั้น ผลบวกของกำลังสอง 2 เทอม ของจำนวนเฉพาะ $p=181$ คือ 10^2+9^2

จากวิธีที่ 1 จะหาค่า a ได้ ต้องคำนวณทั้งหมด 4 ครั้ง

วิธีที่ 2 คำนวณค่า a โดยเริ่มจากขอบล่าง และเพิ่มค่าของ a ขึ้นครั้งละ 1

ครั้งที่ 1 เลือก $a=10$ หา b โดย $b^2=p-a^2=181-100=81=9^2$

เนื่องจาก $p-a^2$ เป็นจำนวนกำลังสอง จะได้ $b=9$

สามารถที่จะหยุดการคำนวณได้ทันทีเมื่อคำนวณหาค่า a ที่ทำให้ $p-a^2$ เป็นจำนวนกำลังสอง เนื่องจาก มีบทแทรกที่ว่า จำนวนเฉพาะ p ใดๆ ที่อยู่ในรูป $4k+1$ เขียนเป็นผลบวกกำลังสอง 2 เทอมได้เพียงรูปแบบเดียว (ไม่คำนึงลำดับ)

ดังนั้น ผลบวกของกำลังสอง 2 เทอม ของจำนวนเฉพาะ $p=181$ คือ 10^2+9^2

จากวิธีที่ 2 จะหาค่า a ได้ ต้องคำนวณทั้งหมด 1 ครั้ง

ตัวอย่าง 3.2 การพิจารณาผลบวกของกำลังสอง 2 เทอม ของจำนวนประกอบ $n=85$

หาจำนวนเต็ม a และ b ที่สอดคล้องกับ $85=a^2+b^2$

จำนวนเต็ม a ตั้งแต่ $a=7\geq\sqrt{85/2}$

ถึง $a=9\leq\sqrt{85}$

ดังนั้น จำนวนเต็ม a มีค่าอยู่ระหว่าง $7\leq a\leq 9$

วิธีที่ 1 คำนวณค่า a โดยเริ่มจากขอบบน และลดค่าของ a ลงครั้งละ 1

ครั้งที่ 1 เลือก $a=9$ หา b โดย $b^2=n-a^2=85-81=4=2^2$

เนื่องจาก $n-a^2$ เป็นจำนวนกำลังสอง จะได้ $b=2$ และ $85=9^2+2^2$

ครั้งที่ 2 เลือก $a=8$ หา b โดย $b^2=n-a^2=85-64=21$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 3 เลือก $a=7$ หา b โดย $b^2=n-a^2=85-49=63=6^2$

เนื่องจาก $n-a^2$ เป็นจำนวนกำลังสอง จะได้ $b=6$ และ $85=7^2+6^2$

ดังนั้น ผลบวกของกำลังสอง 2 เทอม ของจำนวนประกอบ $n=85$

คือ 9^2+2^2 และ 7^2+6^2

วิธีที่ 2 คำนวณค่า a โดยเริ่มจากขอบล่าง และเพิ่มค่าของ a ขึ้นครั้งละ 1

ครั้งที่ 1 เลือก $a=7$ หา b โดย $b^2=n-a^2=85-49=63=6^2$

เนื่องจาก $n-a^2$ เป็นจำนวนกำลังสอง จะได้ $b=6$ และ $85=7^2+6^2$

ครั้งที่ 2 เลือก $a=8$ หา b โดย $b^2=n-a^2=85-64=21$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 3 เลือก $a=9$ หา b โดย $b^2=n-a^2=85-81=4=2^2$

เนื่องจาก $n-a^2$ เป็นจำนวนกำลังสอง จะได้ $b=2$ และ $85=9^2+2^2$

ดังนั้น ผลบวกของกำลังสอง 2 เทอม ของจำนวนประกอบ $n=85$ คือ 7^2+6^2 และ 9^2+2^2

จากตัวอย่าง 3.1 และ 3.2 ยังไม่สามารถสรุปได้ว่าเริ่มจากขอบบน หรือ เริ่มจากขอบล่าง ที่จะสามารถคำนวณหาค่า a ที่ทำให้ $p-a^2$ หรือ $n-a^2$ เป็นรูปกำลังสองได้เร็วกว่า

จึงได้มีการศึกษาคุณลักษณะจำนวนเต็ม a,b โดยเริ่มจากขอบบน เปรียบเทียบกับเริ่มจากขอบล่าง ว่าหาค่า a ด้วยวิธีใดมีโอกาสพบค่า a ได้เร็วกว่า
โดยรายละเอียดจะแสดงไว้ในบทที่ 4 ของปัญหาพิเศษเล่มนี้

3.2 รูปแบบของจำนวนเฉพาะ

จำนวนเต็ม n ใดๆ มีรูปแบบเป็น $4k+0, 4k+1, 4k+2$ หรือ $4k+3$ สำหรับบางจำนวนเต็ม k

จำนวนเต็ม n ที่มีรูปแบบ $4k+0$ มีความหมายในเชิงสมภาคว่า $n \equiv 0 (\mathrm{mod}\, 4)$ และถ้า n ที่มีรูปแบบ $4k+1, 4k+2, 4k+3$ จะหมายถึง

$n \equiv 1 (\mathrm{mod}\, 4)$, $n \equiv 2 (\mathrm{mod}\, 4)$ และ $n \equiv 3 (\mathrm{mod}\, 4)$ ตามลำดับ

สำหรับ จำนวนเฉพาะคี่ จะมีรูปแบบเป็น $4k+1$ หรือ $4k+3$ สำหรับบางจำนวนเต็ม k เพราะว่า ถ้าเป็นรูปแบบ $4k+0 = 2(2k)$ หรือ $4k+2 = 2(2n+1)$ จะเป็นจำนวนคู่ เพราะว่า 2 หารลงตัว ดังนั้น ถ้า p เป็นจำนวนเฉพาะคี่ แล้ว $p \equiv 1 (\mathrm{mod}\, 4)$ หรือ $p \equiv 3 (\mathrm{mod}\, 4)$

จำนวนเฉพาะ เช่น $2, 3, 5, 7, 11, 13, 17, \ldots$

จำนวนเฉพาะคู่ มีจำนวนเดียว คือ 2

จำนวนเฉพาะคี่รูปแบบ $4k+1$ เช่น $5, 13, 17, 29, \ldots$

จำนวนเฉพาะคี่รูปแบบ $4k+3$ เช่น $3, 7, 11, 19, \ldots$

สมบัติ 3.1 ถ้า m และ n เป็นจำนวนเต็มบวกใดๆ ที่มีรูปแบบเป็น $4k+1$ แล้วผลคูณของ mn จะมีรูปแบบเป็น $4k+1$

พิสูจน์ วิธีที่ 1 ให้ $m = 4k_1 + 1$ และ $n = 4k_2 + 1$
คูณสองจำนวนนี้จะได้

$$\begin{aligned} mn &= (4k_1+1)(4k_2+1) \\ &= 16k_1k_2 + 4k_1 + 4k_2 + 1 \\ &= 4(4k_1k_2 + k_1 + k_2) + 1 \quad \text{เมื่อ } k = (4k_1k_2 + k_1 + k_2) \end{aligned}$$

ดังนั้น mn อยู่ในรูป $4k+1$ ข

วิธีที่ 2 พิสูจน์โดยใช้สมภาคมอดุโล

เนื่องจาก m มีรูปแบบ $4k+1$ มีความหมายเชิงสมภาคว่า $m \equiv 1 (\mathrm{mod}\, 4)$

และ n มีรูปแบบ $4k+1$ มีความหมายเชิงสมภาคว่า $n \equiv 1 (\mathrm{mod}\, 4)$

โดยทฤษฎีบท 2.4 ข้อ 4 จะได้ $mn \equiv 1 \cdot 1 \equiv 1 (\mathrm{mod}\, 4)$ □

สมบัติ 3.2 ถ้า m และ n เป็นจำนวนเต็มบวกใดๆที่มีรูปแบบเป็น $4k+3$ แล้วผลคูณของ mn จะมีรูปแบบเป็น $4k+1$

พิสูจน์ วิธีที่1 ให้ $m=4k_1+3$ และ $n=4k_2+3$

$$\begin{aligned} mn &= (4k_1+3)(4k_2+3) \\ &= 16k_1k_2+12k_1+12k_2+9 \\ &= 16k_1k_2+12k_1+12k_2+8+1 \\ &= 4(4k_1k_2+3k_1+3k_2+2)+1 \quad \text{เมื่อ } k=4(4k_1k_2+3k_1+3k_2+2) \end{aligned}$$

ดังนั้น mn อยู่ในรูป $4k+1$

วิธีที่ 2 พิสูจน์โดยใช้สมภาคมอดุโล

เนื่องจาก m มีรูปแบบ $4k+3$ มีความหมายเชิงสมภาคว่า $m\equiv 3\pmod 4$

และ n มีรูปแบบ $4k+3$ มีความหมายเชิงสมภาคว่า $n\equiv 3\pmod 4$

โดยทฤษฎีบท 2.4 ข้อ 4 จะได้ $mn\equiv 3\cdot 3\equiv 9\equiv 1\pmod 4$ □

สมบัติ 3.3 ถ้า m,n เป็นจำนวนเต็มบวกใดๆ m เป็นมีรูปแบบเป็น $4k+1$ และ n มีรูปแบบเป็น $4k+3$ แล้ว ผลคูณ mn จะมีรูปแบบเป็น $4k+3$

พิสูจน์ วิธีที่ 1 ให้ $m=4k_1+3$, $n=4k_2+3$

$$\begin{aligned} mn &= (4k_1+1)(4k_2+3) \\ &= 16k_1k_2+12k_1+4k_2+3 \\ &= 4(4k_1k_2+3k_1+k_2)+3 \quad \text{เมื่อ } k=(4k_1k_2+3k_1+k_2) \end{aligned}$$

ดังนั้น mn อยู่ในรูป $4k+3$

วิธีที่ 2 พิสูจน์โดยใช้สมภาคมอดุโล

เนื่องจาก m มีรูปแบบ $4k+1$ มีความหมายเชิงสมภาคว่า $m\equiv 1\pmod 4$

และ n มีรูปแบบ $4k+3$ มีความหมายเชิงสมภาคว่า $n\equiv 3\pmod 4$

โดยทฤษฎีบท 2.4 ข้อ 4 จะได้ $mn\equiv 1\cdot 3\equiv 3\pmod 4$ □

3.3 พิจารณาการเขียนแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม

จำนวนเต็ม n ที่เขียนเป็นผลบวกของกำลังสอง 2 เทอมได้ อาจมีมากกว่า 1 รูปแบบขึ้นกับจำนวนประกอบ จำนวนเต็ม n สามารถแยกตัวประกอบในรูปแบบนี้ได้เสมอ

$$n = 2^g p_1^{f_1} \ldots p_r^{f_r} q_1^{h_1} \ldots q_s^{h_s} \quad = 2^g \prod_{k=1}^{r} p_k^{f_k} \prod_{j=1}^{s} q_j^{f_j}$$

โดยที่ $g, f_1, \ldots, f_r, h_1, \ldots, h_s$ เป็นจำนวนเต็มบวก

$p_1^{f_1} \ldots p_r^{f_r}$ มีรูปแบบ $4k+1$ หรือ $p_k \equiv 1 \pmod 4$ สำหรับ $k = 1, \ldots, r$

$q_1^{h_1} \ldots q_s^{h_s}$ มีรูปแบบ $4k+3$ หรือ $q_j \equiv -3 \equiv 1 \pmod 4$ สำหรับ $j = 1, \ldots, s$

และ n จะเขียนเป็นผลบวกกำลังสอง 2 เทอมได้ขึ้นกับ เลขยกกำลังของ q_j ต้องเป็นจำนวนคู่เสมอ

การพิจารณาจำนวนรูปแบบจากจำนวนเต็ม n ที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ จะแยกได้เป็น 6 กรณีดังนี้

1. $n = 2^g$ เมื่อ g เป็นจำนวนเต็มบวก
2. $n = q^h$ เมื่อ q มีรูปแบบ $4k+3$ และ h เป็นจำนวนเต็มคู่
3. $n = p_1 \ldots p_r$ เมื่อ p มีรูปแบบ $4k+1$
4. $n = p^f$ เมื่อ p มีรูปแบบ $4k+1$ และ f เป็นจำนวนเต็มบวก
5. $n = p_1^{f_1} \ldots p_r^{f_r}$ เมื่อ p มีรูปแบบ $4k+1$ และ $f_1, \cdots, f_r$ เป็นจำนวนเต็มบวก
6. $n = 2^g p_1^{f_1} \cdots p_r^{f_r} q_1^{h_1} \cdots q_s^{h_s}$ เมื่อ p มีรูปแบบ $4k+1$ และ q มีรูปแบบ $4k+3$ ซึ่งเป็นรูปแบบทั่วไป

ซึ่งในการพิจารณาว่าจำนวนเต็ม n เขียนแทนด้วยผลบวกกำลังสอง 2 เทอม ไม่สามารถพิจารณาที่รูปแบบของจำนวนเต็ม n ได้ เนื่องจาก สมบัติในหัวข้อ 3.2 กล่าวไว้ว่าจำนวนเต็มที่มีรูปแบบ $4k+1$ คูณกับจำนวนเต็มที่มีรูปแบบ $4k+1$ ผลคูณยังเป็นจำนวนเต็มที่มีรูปแบบ $4k+1$ และเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้เสมอ ส่วนจำนวนเต็มที่มีรูปแบบ $4k+3$ คูณกับจำนวนเต็มที่มีรูปแบบ $4k+3$ แต่ผลคูณกลับเป็นจำนวนเต็มที่มีรูปแบบ $4k+1$ ซึ่งไม่สามารถเขียนแทนด้วยผลบวกกำลังสองเทอมได้ แต่จำนวนเต็มที่มีตัวประกอบเป็น $n = 2^g$ เมื่อ g เป็นจำนวนเต็มบวก หรือมีตัวประกอบเป็นจำนวนเฉพาะในรูป $4k+3$ ที่มีซ้ำเป็นจำนวนคู่ จะสามารถเขียนแทนด้วยผลบวกกำลังสองได้แน่นอนเพียงรูปแบบเดียว แสดงรายละเอียดไว้ดังต่อไปนี้

3.3.1 พิจารณาในกรณีที่ 1 $n = 2^g$ เมื่อ g เป็นจำนวนเต็มบวก

ทฤษฎีบท 3.3 $n = 2^g$ เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้
เมื่อ g เป็นจำนวนเต็มบวก จำนวนรูปแบบมีเพียงรูปแบบเดียวเท่านั้น
$n = \left(2^{(g-1)/2}\right)^2 + \left(2^{(g-1)/2}\right)^2$ หรือ $n = \left(2^{g/2}\right)^2 + 0^2$

พิสูจน์ 1) จะแสดงว่า $n = 2^g$ เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้

เมื่อ $2^1 = 1^2 + 1^2$

$2^2 = 2^2 + 0^2$

$2^3 = 2^2 \cdot 2 = 2^2 + 2^2$

พิจารณาที่ 2^k เมื่อ k เป็นจำนวนเต็มบวกคู่

จะได้ $2^k = \left(2^{k/2}\right)^2 + 0^2$ เขียนได้

และ พิจารณาว่า 2^{k+1} เขียนได้

จะได้ว่า $2^{k+1} = 2 \cdot 2^k$

$= 2^k + 2^k$

$= \left(2^{k/2}\right)^2 + \left(2^{k/2}\right)^2$

$\therefore 2^{k+1}$ เขียนเป็นผลบวกกำลังสอง 2 เทอมได้

ดังนั้น $n = 2^g$ เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ เมื่อ g เป็นจำนวนเต็มบวก

2) จะแสดงว่า $n = 2^g$ เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้เพียงแบบเดียว

ให้ $n = 2^g$

สมมติรูปแบบที่ 1 คือ $n = a^2 + b^2$ $(*)$

และรูปแบบที่ 2 คือ $n = c^2 + d^2$ $(**)$

สำหรับจำนวนเต็มบวก a, b, c, d

จะได้ว่า a, b, c, d มีค่ามากกว่า 0 และน้อยกว่าหรือเท่ากับ $\sqrt{n}$

พิจารณา ad และ bc

คูณ d^2 ใน $(*)$ จะได้ $nd^2 = a^2d^2 + b^2d^2$ (I)

คูณ b^2 ใน $(**)$ จะได้ $nb^2 = b^2c^2 + b^2d^2$ (II)

$(\mathrm{I})-(\mathrm{II})$; $a^2d^2 - b^2c^2 = nd^2 - nb^2$

$$(ad)^2 - (bc)^2 = n(d^2 - b^2)$$

$$(ad-bc)(ad+bc) \equiv 0 \pmod{n}$$

จะได้ว่า $ad-bc \equiv 0 \pmod{n}$ หรือ $ad+bc \equiv 0 \pmod{n}$

ในทำนองเดียวกันข้างต้น จะได้

$$ad-bc=0 \quad \text{หรือ} \quad ad+bc=n$$

พิจารณาผลคูณของสองรูปแบบ ดังนี้

$$\begin{aligned} n^2 &= (a^2+b^2)(c^2+d^2) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= n^2 + (ac-bd)^2 \end{aligned}$$

และดังนั้น $ac-bd=0$ และผลที่ตามมาคือ

$$ad=bc \quad \text{หรือ} \quad ac=bd$$

สมมติว่า $ad=bc$ จะได้ $a \mid bc$ และ $\gcd(a,b)=1$ ทำให้ได้ $a \mid c$ นั่นคือ $c=ka$

ด้วยเงื่อนไข $ad=bc=b(ka)$ แล้วได้ว่า $d=bk$ แต่

$$n = c^2 + d^2 = k^2(a^2+b^2)$$

ทำให้ได้ว่า $k=1$ และได้ว่า $a=c$ และ $b=d$

ในทำนองเดียวกันด้วยเงื่อนไข $ac=bd$ ได้ว่า $a=d$ หรือ $b=c$

จึงสรุปได้ว่าการแทนจำนวนเต็ม $n=2^g$ เขียนผลบวกกำลังสอง 2 เทอมได้แบบเดียวเท่านั้น

จาก 1) และ 2) สามารถสรุปได้ว่า $n=2^g$ เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ 1 รูปแบบ

ตัวอย่าง 3.3 พิจารณาจำนวนเต็มที่อยู่ในรูป 2^g เมื่อ g เป็นจำนวนเต็มบวก

- $n=2^1$ เขียนได้ 1 แบบ คือ 1^2+1^2
- $n=2^2$ เขียนได้ 1 แบบ คือ 2^2+0^2

$$2^2 = (1+1)^2(1+1)^2$$

แบบที่ 1 $= (1-1)^2 + (1+1)^2 = 0^2 + 2^2$

แบบที่ 2 $=(1+1)^2+(1-1)^2=2^2+0^2$

เนื่องจาก 0^2+2^2 และ 2^2+0^2 เกิดจากการสลับที่ ดังนั้นจึงคิดเป็นแบบเดียวเท่านั้น

- $n=2^3$ เขียนได้ 1 แบบ คือ 2^2+2^2

$$2^3=2\cdot 2^2=(1+1)^2(2+0)^2$$

แบบที่ 1 $=(2-0)^2+(2+0)^2=2^2+2^2$

แบบที่ 2 $=(2+0)^2+(2-0)^2=2^2+2^2$

เนื่องจากมี 2^2+2^2 ซ้ำกัน ดังนั้นจึงคิดเป็นแบบเดียวเท่านั้น

- $n=2^4$ เขียนได้ 1 แบบ คือ 4^2+0^2

$$2^4=2^2\cdot 2^2=(2+0)^2(2+0)^2$$

แบบที่ 1 $=(4-0)^2+(0+0)^2=4^2+0^2$

แบบที่ 2 $=(4+0)^2+(0-0)^2=4^2+0^2$

เนื่องจากมี 4^2+0^2 ซ้ำกัน ดังนั้นจึงคิดเป็นแบบเดียวเท่านั้น

จำนวนอื่นๆ $2^5,2^6,\ldots,2^g$ คิดได้ในทำนองเดียวกัน

ดังนั้นสรุปได้ว่า $n=2^g$ เขียนได้ 1 แบบ เมื่อ g เป็นจำนวนเต็มบวก

3.3.2 พิจารณาในกรณีที่ 2 $n=q^h$ เมื่อ q มีรูปแบบ $4k+3$ และ h เป็นจำนวนเต็มคู่

ทฤษฎีบท 3.4 $n=q^h$ เมื่อ h เป็นจำนวนเต็มบวกคู่ จำนวนรูปแบบมีเพียงรูปแบบเดียว เท่านั้นคือ $n=\left(q^{h/2}\right)^2+0^2$

พิสูจน์ 1) จะแสดงว่า $n=q^h$ เมื่อ h เป็นจำนวนเต็มบวกคู่ และ q มีรูปแบบ $4k+3$

เมื่อ $q^2=q^2+0^2$

$$q^4=\left(q^2\right)^2+0^2$$

พิจารณาที่ q^k เมื่อ k เป็นจำนวนเต็มบวกคู่

จะได้ $q^k=\left(q^{k/2}\right)^2+0^2$

เมื่อ q^k เขียนได้ จะพิจารณาว่า q^{k+2} เขียนได้

$$\begin{aligned} q^{k+2} &= q^k\cdot q^2 \\ &= \left(\left(q^{k/2}\right)^2+0^2\right)\cdot q^2 \\ &= \left(q^{k/2}\right)^2\cdot q^2+0^2\cdot q^2 \\ &= \left(q^{\frac{k}{2}+1}\right)^2+0^2 \end{aligned}$$

$\therefore q^{k+2}$ เขียนเป็นผลบวกกำลังสอง 2 เทอมได้

ดังนั้น $n=q^h$ เมื่อ h เป็นจำนวนเต็มบวกคู่ เขียนเป็นผลบวกกำลังสอง 2 เทอมได้

2) จะแสดงว่า $n=q^h$ เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้เพียงแบบเดียว

ให้ $n=q^h$

สมมติรูปแบบที่ 1 คือ $n=a^2+b^2$ (*)

และรูปแบบที่ 2 คือ $n=c^2+d^2$ (**)

สำหรับจำนวนเต็มบวก a,b,c,d

จะได้ว่า a,b,c,d มีค่ามากกว่า 0 และน้อยกว่าหรือเท่ากับ $\sqrt{n}$

พิจารณา ad และ bc

คูณ d^2 ใน $(*)$ จะได้ $nd^2 = a^2d^2 + b^2d^2$ (I)

คูณ b^2 ใน $(**)$ จะได้ $nb^2 = b^2c^2 + b^2d^2$ (II)

$(\mathrm{I})-(\mathrm{II})$; $a^2d^2 - b^2c^2 = nd^2 - nb^2$

$$(ad)^2 - (bc)^2 = n(d^2 - b^2)$$

$$(ad-bc)(ad+bc) \equiv 0 \pmod{n}$$

จะได้ว่า $ad-bc \equiv 0 \pmod{n}$ หรือ $ad+bc \equiv 0 \pmod{n}$

ในทำนองเดียวกันข้างต้น จะได้

$$ad-bc=0 \text{ หรือ } ad+bc=n$$

พิจารณาผลคูณของสองรูปแบบ ดังนี้

$$\begin{aligned} n^2 &= (a^2+b^2)(c^2+d^2) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= n^2 + (ac-bd)^2 \end{aligned}$$

และดังนั้น $ac-bd=0$ และผลที่ตามมาคือ

$$ad=bc \text{ หรือ } ac=bd$$

สมมติว่า $ad=bc$ จะได้ $a \mid bc$ และ $\gcd(a,b)=1$ ทำให้ได้ $a \mid c$ นั่นคือ $c=ka$

ด้วยเงื่อนไข $ad=bc=b(ka)$ แล้วได้ว่า $d=bk$ แต่

$$n=c^2+d^2=k^2(a^2+b^2)$$

ทำให้ได้ว่า $k=1$ และได้ว่า $a=c$ และ $b=d$

ในทำนองเดียวกันด้วยเงื่อนไข $ac=bd$ ได้ว่า $a=d$ หรือ $b=c$

จึงสรุปได้ว่าการแทนจำนวนเต็ม $n=q^h$ เขียนผลบวกกำลังสอง 2 เทอมได้แบบเดียวเท่านั้น

จาก 1) และ 2) สรุปได้ว่า $n=q^h$ เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ 1 รูปแบบ □

ตัวอย่าง 3.4 พิจารณา $n=3^6=729$ เมื่อ 3 เป็นจำนวนเฉพาะที่มีรูปแบบ $4k+3$

หาจำนวนเต็ม a และ b ที่สอดคล้องกับ $729=a^2+b^2$

จำนวนเต็ม a ตั้งแต่ $a=27 \le \sqrt{729}$ ลดลงถึง $a=20 \ge \sqrt{\frac{729}{2}}$

จำนวนเต็ม a มีค่าอยู่ระหว่าง $20 \le a \le 27$

ใช้วิธีที่ 1 คำนวณค่า a โดยเริ่มจากขอบบน และลดค่าของ a ลงครั้งละ 1

ครั้งที่ 1 เลือก $a=27$ หา b โดย $b^2=n-a^2=729-729=0$

เนื่องจาก $n-a^2$ เป็นจำนวนกำลังสอง จะได้ $b=0$ และ $729=27^2+0^2$

ครั้งที่ 2 เลือก $a=26$ หา b โดย $b^2=n-a^2=729-676=53$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 3 เลือก $a=25$ หา b โดย $b^2=n-a^2=729-625=104$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 4 เลือก $a=24$ หา b โดย $b^2=n-a^2=729-576=153$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 5 เลือก $a=23$ หา b โดย $b^2=n-a^2=729-529=200$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 6 เลือก $a=22$ หา b โดย $b^2=n-a^2=729-484=245$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 7 เลือก $a=21$ หา b โดย $b^2=n-a^2=729-441=288$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ครั้งที่ 8 เลือก $a=20$ หา b โดย $b^2=n-a^2=729-400=329$

เนื่องจาก $n-a^2$ ไม่เป็นจำนวนกำลังสอง จึงใช้ไม่ได้

ดังนั้น ผลบวกของกำลังสอง 2 เทอม ของจำนวนประกอบ $n=3^6=729$ คือ

$$\left(3^{6/2}\right)^2+0^2=\left(3^3\right)^2+0^2=27^2+0^2$$

จากตัวอย่างนี้จะสังเกตได้ว่า เพียงครั้งที่ 1 ก็สามารถหาค่า a,b ที่ทำให้ n เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้

ตัวอย่าง 3.5 จงหาผลบวกกำลังสอง 2 เทอมของจำนวนประกอบ $n=14641$

แยกตัวประกอบได้เป็น $14641=11\times11\times11\times11$

จะได้ $14641=11^4=\left(11^{4/2}\right)^2+0^2=\left(11^2\right)^2+0^2=121^2+0^2$

ดังนั้น ผลบวกกำลังสอง 2 เทอมของจำนวนประกอบ $n=14641$ คือ 121^2+0^2

3.4 ขั้นตอนวิธีพิจารณาการเขียนแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอม

สำหรับจำนวนเต็ม n ใดๆ การพิจารณาว่าสามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้หรือไม่ โดยพิจารณาหาว่ามีตัวประกอบที่เป็นจำนวนเฉพาะรูป $4k+3$ หรือไม่ และถ้ามีต้องมีซ้ำเป็นจำนวนคู่ มีขั้นตอนดังนี้

1. รับจำนวนเต็มบวก n
2. ตรวจสอบว่าจำนวนเต็ม n อยู่ในรูป $4k+3$ หรือไม่
   ถ้า n อยู่ในรูป $4k+3$ จำนวนเต็มนี้จะไม่สามารถเขียนเป็นผลบวกกำลังสอง 2 เทอมได้
   ถ้า n ไม่อยู่ในรูป $4k+3$ ไม่ใช่จะพิจารณาขั้นต่อไป
   (ซึ่ง n อาจจะมีรูปแบบ $4k+0,\ 4k+1,\ 4k+2$)
3. จะพิจารณาที่ตัวประกอบของ n ที่มีรูปแบบ $4k+1$ จึงขจัดตัวประกอบในรูป 2^g เนื่องจาก 2^g เมื่อ g เป็นจำนวนเต็มบวกเขียนได้เสมอและมีเพียงรูปแบบเดียว โดยจะทำการหาร n ด้วย 2 จนได้ผลลัพธ์เป็นจำนวนเต็มคี่ m
   (ซึ่ง m จะมีรูป $4k+1$ แต่ยังไม่สามารถสรุปได้ว่าเขียนได้หรือไม่ได้ซึ่งกล่าวไว้ในหัวข้อ 3.3)
4. ได้จำนวนเต็มคี่ m จากขั้นที่ 3 มาตรวจสอบว่ามีจำนวนเฉพาะในรูป $4k+3$ หารลงตัวหรือไม่ โดยพิจารณาจากจำนวนเฉพาะรูป $4k+3$ ที่น้อยกว่าหรือเท่ากับ $\sqrt{m}$
   โดยนำมาหารจำนวนเต็มคี่ m ออกจนเหลือเป็นจำนวนเต็มคี่ s
   (ที่ไม่มีตัวประกอบเป็นจำนวนเฉพาะ $4k+3$) พร้อมพิจารณาเลขชี้กำลังของแต่จำนวนเฉพาะ $4k+3$ ถ้าเป็นจำนวนคี่แสดงว่าไม่สามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ ถ้าเป็นจำนวนคู่จะเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ (ในหัวข้อ 3.3)
5. ได้จำนวนเต็ม s ที่มีรูปแบบ $4k+1$ และเกิดจากตัวประกอบที่เป็นจำนวนเฉพาะรูป $4k+1$ ซึ่งสามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้แน่นอน

ตัวอย่าง 3.6 จงแสดงว่าจำนวนเต็ม $n=127296$
สามารถเขียนเป็นผลบวกกำลังสอง 2 เทอมได้หรือไม่

ขั้นที่ 1 จำนวนเต็ม $n=127296$

ขั้นที่ 2 $127296 \equiv 0 \pmod 4$ จำนวนเต็มไม่อยู่ในรูป $4k+3$

ขั้นที่ 3 นำ 2 ไปหารเรื่อยๆ จนเลขที่ได้เป็นจำนวนคี่ (m)

$2)\underline{127296}$

$2)\underline{63648}$

$2)\underline{31824}$

$2)\underline{15912}$

$2)\underline{7956}$

$2)\underline{3978}$

จะได้ $m = \underline{\underline{1989}}$

ตัวประกอบของ $127296 = 2^6 \cdot 1989$

ขั้นที่ 4 จำนวนเฉพาะที่มีรูปแบบ $4k+3$ ที่น้อยกว่าหรือเท่ากับ $\sqrt{1989} \approx 44$ คือ $3, 7, 11, 19, 23, 31, 43$

พิจารณาหารด้วย 3

$1989 \div 3 = 663$ หารด้วย 3 ครั้งที่ 1

$663 \div 3 = 221$ หารด้วย 3 ครั้งที่ 2

$221 \div 3$ ไม่ลงตัว

พิจารณาหารด้วย 7

$221 \div 7$ ไม่ลงตัว

พิจารณาหารด้วย 11

$221 \div 11 =$ ไม่ลงตัว

และ $19, 23, 31, 43$ ก็หาร 221 ไม่ลงตัว

จะได้ว่า 1989 มีจำนวนเฉพาะ 3 เพียงจำนวนเดียวที่หารลงตัว และมีกำลังเป็นจำนวนคู่คือ 2 และได้จำนวนเต็มคี่ $s = 221$ ตัวประกอบของ $1989 = 3^2 \cdot 221$

ขั้นที่ 5 จำนวนเต็มคี่ $s = 221 = 17 \times 13$ (มีตัวประกอบเป็นจำนวนเฉพาะในรูป $4k+1$) เป็นตัวประกอบที่สามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้แน่นอน

3.5 จำนวนรูปแบบของการแทนจำนวนเต็ม n ด้วยผลบวกกำลังสอง 2 เทอม

จากหัวข้อ 3.3 กล่าวไว้ว่า จำนวนเต็ม n สามารถแยกตัวประกอบในรูปแบบนี้ได้เสมอ

$$n = 2^g p_1^{f_1} \ldots p_r^{f_r} q_1^{h_1} \ldots q_s^{h_s} \quad = 2^g \prod_{k=1}^{r} p_k^{f_k} \prod_{j=1}^{s} q_j^{f_j}$$

และจำนวนรูปแบบของจำนวนเต็ม n ที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ จะแยกได้เป็น 6 กรณีดังนี้

1. $n = 2^g$ เมื่อ g เป็นจำนวนเต็มบวก
2. $n = q^h$ เมื่อ q มีรูปแบบ $4k+3$ และ h เป็นจำนวนเต็มคู่
3. $n = p_1 \ldots p_r$ เมื่อ p มีรูปแบบ $4k+1$
4. $n = p^f$ เมื่อ p มีรูปแบบ $4k+1$ และ f เป็นจำนวนเต็มบวก
5. $n = p_1^{f_1} \ldots p_r^{f_r}$ เมื่อ p มีรูปแบบ $4k+1$ และ $f_1, \cdots, f_r$ เป็นจำนวนเต็มบวก
6. $n = 2^g p_1^{f_1} \cdots p_r^{f_r} q_1^{h_1} \cdots q_s^{h_s}$ เมื่อ p มีรูปแบบ $4k+1$ และ q มีรูปแบบ $4k+3$ ซึ่งเป็นรูปแบบทั่วไป

ปัญหาพิเศษนี้จะศึกษาเพียง กรณีที่ 1, 2, 3 และ 4 ดังนี้
กรณีที่ 1 $n = 2^g$ เมื่อ g เป็นจำนวนเต็มบวก เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้และเขียนได้เพียงรูปแบบเดียวเท่านั้น

กรณีที่ 2 $n = q^h$ เมื่อ q มีรูปแบบ $4k+3$ และ h เป็นจำนวนเต็มคู่ เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้และเขียนได้เพียงรูปแบบเดียวเท่านั้น

ซึ่งกรณีที่ 1 และ กรณีที่ 2 รายละเอียดได้กล่าวไปแล้วในหัวข้อที่ 3.3
ดังนั้น จึงจะกล่าวถึงรายละเอียด ในกรณีที่ 3 และ 4 ต่อไป

3.5.1 พิจารณาในกรณีที่ 3 $n = p_1 \ldots p_r$ เมื่อ p มีรูปแบบ $4k+1$

ทฤษฎีบท 3.5 $n = p_1 \ldots p_r$ เมื่อ $p_1, \ldots, p_r$ มีรูปแบบ $4k+1$
จำนวนรูปแบบมี 2^{r-1} รูปแบบ

พิสูจน์ ให้ $p_1 = a_1^2 + b_1^2, p_2 = a_2^2 + b_2^2, \ldots, p_r = a_r^2 + b_r^2$

เมื่อ $p_1, \ldots, p_r$ มีรูปแบบ $4k+1$ และ $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_r$ เป็นจำนวนเต็มบวก

p_1 เขียนแทนได้ 1 รูปแบบโดยไม่คำนึงถึงลำดับ (บทแทรก 2.10)

กรณีที่ 1 ให้ $r=2$ จะได้ $n=p_1p_2$ จากบทตั้ง 2.11 จะได้ว่า

รูปแบบที่ 1 $p_1p_2=\left(a_1^2+b_1^2\right)\left(a_2^2+b_2^2\right)=\left(a_1a_2+b_1b_2\right)^2+\left(a_1b_2-a_2b_1\right)^2$

รูปแบบที่ 2 $p_1p_2=\left(a_1^2+b_1^2\right)\left(b_2^2+a_2^2\right)=\left(a_1b_2+a_2b_1\right)^2+\left(a_1a_2-b_1b_2\right)^2$

รูปแบบที่ 3 $p_1p_2=\left(b_1^2+a_1^2\right)\left(a_2^2+b_2^2\right)=\left(a_2b_1+a_1b_2\right)^2+\left(b_1b_2-a_1a_2\right)^2$

รูปแบบที่ 4 $p_1p_2=\left(b_1^2+a_1^2\right)\left(b_2^2+a_2^2\right)=\left(b_1b_2+a_1a_2\right)^2+\left(a_2b_1-a_1b_2\right)^2$

จากกรณีที่ 1 จะเห็นว่า รูปแบบที่ 1 และ 4 เป็นรูปแบบเดียวกัน

เพราะว่า $\left(a_2b_1-a_1b_2\right)^2=\left(a_1b_2-a_2b_1\right)^2$

และรูปแบบที่ 2 และ 3 เป็นรูปแบบเดียวกัน เพราะว่า $\left(a_1a_2-b_1b_2\right)^2=\left(b_1b_2-a_1a_2\right)^2$

นั่นคือ $n=p_1p_2$ มีจำนวนรูปแบบที่ต่างกันจำนวน 2 รูปแบบ

และมีจำนวนรูปแบบที่ซ้ำกัน 2 รูปแบบ

ถ้าพิจารณาโดยหลักการนับ p_1 เขียนแทนได้ 2 รูปแบบ และ p_2 เขียนแทนได้ 2 รูปแบบ

ฉะนั้น p_1p_2 จะเขียนแทนได้ 4 รูปแบบ และใน 4 รูปแบบจะมีรูปแบบที่ต่างกันอยู่ 2 รูปแบบ

กรณีที่ 2 ให้ $r=3$ จะได้ $n=p_1p_2p_3$ จัดรูป $n=\left(p_1p_2\right)p_3$

จาก p_1p_2 จะเขียนแทนได้ 4 รูปแบบ มีจำนวนรูปแบบที่ต่างกัน 2 รูปแบบ

และมีจำนวนรูปแบบที่ซ้ำกัน 2 รูปแบบ

และ p_3 เขียนแทนได้ 2 รูปแบบ

ดังนั้น $n=\left(p_1p_2\right)p_3$ จะเขียนแทนได้ทั้งหมด 8 รูปแบบ

จำนวนรูปแบบซ้ำกัน $(2)(2)=4=2^2$ รูปแบบ

จำนวนรูปแบบที่ต่างกัน $(2)(2)=4=2^2$ รูปแบบ

กรณีที่ 3 ให้ $r=4$ จะได้ $n=p_1p_2p_3p_4$ จัดรูป $n=\left(p_1p_2p_3\right)p_4$

จาก $n=p_1p_2p_3$ จะเขียนแทนได้ $8=2^3$ รูปแบบ

มีจำนวนรูปแบบซ้ำกัน $(2)(2)=4=2^2$ รูปแบบ

และจำนวนรูปแบบที่ต่างกัน $(2)(2)=4=2^2$ รูปแบบ

จะได้ว่า $n=(p_1p_2p_3)p_4$ มีรูปแบบที่เขียนแทนได้ทั้งหมด $16=2^4$ รูปแบบ

มีจำนวนรูปแบบซ้ำกัน $(2^2)(2)=2^3$ รูปแบบ

และจำนวนรูปแบบที่ต่างกัน $(2^2)(2)=2^3$ รูปแบบ

กรณีทั่วไป $n=p_1p_2...p_r$

จาก $n=p_1p_2...p_{r-1}$ จะเขียนแทนได้ 2^{r-1} รูปแบบ

มีจำนวนรูปแบบซ้ำกัน 2^{r-2} รูปแบบ

และจำนวนรูปแบบที่ต่างกัน 2^{r-2} รูปแบบ

จะได้ว่า $n=(p_1p_2...p_{r-1})p_r$ มีรูปแบบที่เขียนแทนได้ทั้งหมด 2^r รูปแบบ

มีจำนวนรูปแบบซ้ำกัน 2^{r-1} รูปแบบ

และจำนวนรูปแบบที่ต่างกัน 2^{r-1} รูปแบบ

แน่นอนว่า $2^{r-1}+2^{r-1}=2^{r-1}(1+1)=2^r$

ดังนั้นสรุปได้ว่า $p_1,\ldots,p_r$ เมื่อ $p_1,\ldots,p_r$ มีรูปแบบ $4k+1$
จะเขียนแทนด้วยผลบวกกำลังสองสองเทอมรูปแบบที่ต่างกันได้ 2^{r-1} รูปแบบ □

ตัวอย่าง 3.7 ให้จำนวนประกอบ $n=1105$

แยกตัวประกอบจะได้ $n=5\cdot13\cdot17$

มีจำนวนเฉพาะรูปแบบ $4k+1$ สามจำนวนคูณกัน

จะได้ว่า จำนวนรูปแบบของ $n=1105$ คือ $2^{3-1}=2^2=4$ รูปแบบ

พิจารณาผลบวกกำลังสอง 2 เทอมของจำนวนประกอบ $n=1105$

หาจำนวนเต็ม a และ b ที่สอดคล้องกับ $1105=a^2+b^2$

จำนวนเฉพาะคี่ $5=2^2+1^2$, $13=3^2+2^2$ และ $17=4^2+1^2$

ขั้นที่ 1 พิจารณาทีละคู่ 1 คู่ ได้ 2 แบบ

$$13\cdot 17=\left(3^2+2^2\right)\left(4^2+1^2\right)=(12+2)^2+(3-8)^2=14^2+5^2$$

และ $$=(12-2)^2+(3+8)^2=10^2+11^2$$

ขั้นที่ 2 นำผลขั้นที่ 1 มาพิจารณากับพจน์ใหม่

จากแบบที่ 1 $$\left(2^2+1^2\right)\left(14^2+5^2\right)=(28+5)^2+(10-14)^2=33^2+4^2$$

และ $$=(28-5)^2+(10+14)^2=23^2+24^2$$

จากแบบที่ 2 $$\left(2^2+1^2\right)\left(11^2+10^2\right)=(22+10)^2+(20-11)^2=32^2+9^2$$

และ $$=(22-10)^2+(20+11)^2=12^2+31^2$$

ดังนั้น ผลบวกของกำลังสอง 2 เทอม ของจำนวนประกอบ $n=1105$ คือ

33^2+4^2, 23^2+24^2, 32^2+9^2 และ 12^2+31^2 มีทั้งหมด 4 รูปแบบ

ตัวอย่าง 3.8 พิจารณาจำนวนรูปแบบของจำนวนเต็ม n ต่อไปนี้

- $n=5\times 13$ เขียนได้ $2^{2-1}=2$ แบบ คือ $8^2+1^2, 7^2+4^2$
- $n=5\times 13\times 17$ เขียนได้ $2^{3-1}=4$ แบบ คือ

  $33^2+4^2, 32^2+9^2, 31^2+12^2, 24^2+23^2$

- $n=5\times 13\times 17\times 29$ เขียนได้ $2^{4-1}=8$ แบบ คือ

  $179^2+2^2, 178^2+19^2, 173^2+46^2, 166^2+67^2,$
  $163^2+74^2, 157^2+86^2, 142^2+109^2, 131^2+122^2$

- $n=5\times 13\times 17\times 29\times 37$ เขียนได้ $2^{5-1}=16$ แบบ คือ

  $1087^2+64^2, 1084^2+103^2, 1076^2+167^2, 1072^2+191^2,$
  $1063^2+236^2, 1052^2+281^2, 1049^2+292^2, 1028^2+359^2,$
  $992^2+449^2, 961^2+512^2, 929^2+568^2, 908^2+601^2,$
  $904^2+607^2, 863^2+664^2, 856^2+673^2, 796^2+743^2$

3.5.2 พิจารณาในกรณีที่ 4 $n=p^f$ เมื่อ p มีรูปแบบ $4k+1$ และ f เป็นจำนวนเต็มบวก

ทฤษฎีบท 3.6 ให้ $p^f = p^s \cdot p^t$ เมื่อ s,t เป็นจำนวนเต็มบวก
จำนวนรูปแบบของ p^f แทนด้วย $N(p^f)$ รูปแบบ
จำนวนรูปแบบของการแทนด้วยผลบวกกำลังสอง 2 เทอมของ p^f ขึ้นกับ s และ t ดังนี้
ถ้า s หรือ t เป็นจำนวนคู่ $N(p^f) = N(p^s)+N(p^t)-1$
แต่ ถ้า s และ t เป็นจำนวนคี่ $N(p^f) = N(p^s)+N(p^t)$

พิสูจน์ ให้ $p^1 = a^2+b^2$ และ a,b,s,t เป็นจำนวนเต็มบวก

จาก $n(p^1)=1$ เสมอ (มีทฤษฎีบทได้กล่าวไว้)

กรณีที่ 1 ให้ $f=2$ จะได้

$p^2 = p^s \cdot p^t = p^1 \cdot p^1$ เนื่องจาก $s,t=1$ เป็นจำนวนคี่

นั่นคือ $N(p^2)= N(p^1)+N(p^1)=1+1=2$ รูปแบบ

กรณีที่ 2 ให้ $f=3$ จะได้

$p^3 = p^s \cdot p^t = p^1 \cdot p^2$ เนื่องจาก $s=1,t=2$ มีจำนวนหนึ่งเป็นจำนวนคู่

นั่นคือ $N(p^3) = N(p^1)+N(p^2)-1=1+2-1=2$ รูปแบบ

กรณีที่ 3 ให้ $f=4$ จะได้

$p^4 = p^s \cdot p^t = p^1 \cdot p^3$ เนื่องจาก $s=1,t=3$ เป็นจำนวนคี่

นั่นคือ $N(p^4) = N(p^1)+N(p^3)=1+2=3$ รูปแบบ

$p^4 = p^s \cdot p^t = p^2 \cdot p^2$ เนื่องจาก $s=2,t=2$ เป็นจำนวนคู่

นั่นคือ $N(p^4) = N(p^1)+N(p^3)-1=2+2-1=3$ รูปแบบ

พิจารณากรณีทั่วไป p^f เมื่อ f เป็นจำนวนเต็มบวก จะได้

$p^f = p^1 \cdot p^{f-1}$ เนื่องจาก $s=1,t=f-1$

ถ้า $f-1$ เป็นจำนวนคู่ นั่นคือ $N(p^f)=N(p^1)+N(p^{f-1})-1$ รูปแบบ

หรือ $N(p^f)=1+N(p^{f-1})-1=N(p^{f-1})$ รูปแบบ

และ ถ้า $f-1$ เป็นจำนวนคี่ นั่นคือ $N(p^f)=N(p^1)+N(p^{f-1})$ รูปแบบ

หรือ $N(p^f)=N(p^{f-1})+1$ รูปแบบ

$p^f=p^2\cdot p^{f-2}$ เนื่องจาก $s=2,t=f-2$ มีจำนวนหนึ่งเป็นจำนวนคู่

นั่นคือ $N(p^f)=N(p^2)+N(p^{f-2})-1=2+N(p^{f-2})-1=N(p^{f-2})+1$ รูปแบบ

และในกรณี s เป็นจำนวนเต็มบวกใดๆนอกเหนือจากนี้ ก็แสดงได้ในทำนองเดียวกัน และจำนวนรูปแบบของ p^f ไม่ว่า s,t เป็นจำนวนเต็มบวกใดๆ จำนวนรูปแบบก็จะเท่ากันเสมอ

ดังนั้นสรุปได้ตาม ทฤษฎีบทที่ 3.6 □

ทฤษฎีบท 3.7 $n=p^f$ เมื่อ p มีรูปแบบ $4k+1$ และ f เป็นจำนวนเต็มบวก จำนวนรูปแบบ มี $\left\lfloor\frac{f}{2}\right\rfloor+1$ รูปแบบ

พิสูจน์ ให้ p เป็นจำนวนเฉพาะ ที่มีรูปแบบ $4k+1$ และ f เป็นจำนวนเต็มบวก

จากนิยามแบร็กเก็ตฟังก์ชัน $k=\left\lfloor\frac{f}{2}\right\rfloor$ จะได้ว่า k เป็นจำนวนเต็มที่มากที่สุดที่น้อยกว่า $\frac{f}{2}$

กรณีที่ 1 เมื่อ $f=1$ p^1 มีจำนวนรูปแบบคือ $\left\lfloor\frac{1}{2}\right\rfloor+1=0+1=1$ รูปแบบ

กรณีที่ 2 เมื่อ $f=2$ p^2 มีจำนวนรูปแบบคือ $\left\lfloor\frac{2}{2}\right\rfloor+1=1+1=2$ รูปแบบ

กรณีที่ 3 เมื่อ $f=3$ p^3 มีจำนวนรูปแบบคือ $\left\lfloor\frac{3}{2}\right\rfloor+1=1+1=2$ รูปแบบ

กรณีที่ 4 เมื่อ $f=4$ p^4 มีจำนวนรูปแบบคือ $\left\lfloor\frac{4}{2}\right\rfloor+1=2+1=3$ รูปแบบ

กรณีทั่วไป เมื่อ f เป็นจำนวนคู่จะมี m เป็นจำนวนเต็ม ที่ $f=2m$ จะได้

$$k=\left\lfloor\frac{f}{2}\right\rfloor=\left\lfloor\frac{2m}{2}\right\rfloor=m$$

ดังนั้น $p^f=\left\lfloor\frac{f}{2}\right\rfloor+1=\left\lfloor\frac{2m}{2}\right\rfloor+1=m+1$

เมื่อ $f-1$ เป็นจำนวนคี่ จะมี m เป็นจำนวนเต็ม ที่ $(f-1)=2m-1$ จะได้

$$k=\left\lfloor\frac{(f-1)}{2}\right\rfloor=\left\lfloor\frac{2m-1}{2}\right\rfloor=m-1$$

ดังนั้น $p^f=\left\lfloor\frac{f}{2}\right\rfloor+1=\left\lfloor\frac{2m-1}{2}\right\rfloor+1=(m-1)+1=m$

เมื่อ $f+1$ เป็นจำนวนคี่ จะมี n เป็นจำนวนเต็ม ที่ $f+1=2m+1$ จะได้

$$k=\left\lfloor\frac{f}{2}\right\rfloor=\left\lfloor\frac{2m+1}{2}\right\rfloor=m$$

ดังนั้น $p^f=\left\lfloor\frac{f}{2}\right\rfloor+1=\left\lfloor\frac{2m+1}{2}\right\rfloor+1=\left\lfloor\frac{2m}{2}+\frac{1}{2}\right\rfloor=m+1$

ดังนั้น สามารถสรุปได้ว่า $n=p^f$ เมื่อ p มีรูปแบบ $4k+1$ มี $\left\lfloor\frac{k}{2}\right\rfloor+1$ รูปแบบ □

ตัวอย่าง 3.9 จงหาผลบวกกำลังสอง 2 เทอมของจำนวนต่อไปนี้เมื่อ $41=5^2+4^2$

- $n=41^2$ เขียนได้ 2 แบบ คือ $41^2+0^2, 40^2+9^2$

$$41^2=41\cdot 41=\left(5^2+4^2\right)\left(5^2+4^2\right)$$

$$41^2=(25-16)^2+(20+20)^2=9^2+40^2$$

และ $$41^2=(25+16)^2+(20-20)^2=41^2+0^2$$

- $n=41^3$ เขียนได้ 2 แบบ คือ $236^2+115^2, 205^2+164^2$

$41^3=41\cdot 41^2$ ซึ่ง 41^2 เขียนได้ 2 แบบ

จากแบบที่ 1 $41^3=(5^2+4^2)(41^2+0^2)$

$41^3=(205-0)^2+(0+164)^2=205^2+164^2$

และ $41^3=(205+0)^2+(0-164)^2=205^2+(-164)^2=205^2+164^2$

จากแบบที่ 2 $41^3=(5^2+4^2)(40^2+9^2)$

$41^3=(200-36)^2+(45+160)^2=164^2+205^2$

และ $41^3=(200+36)^2+(45-160)^2=236^2+(-115)^2=236^2+115^2$

ข้อสังเกต การนับ a^2 และ $(-a)^2$ จะเหมือนกัน

จากความเป็นจริงจะเห็นได้ว่าสามารถเขียนได้ทั้งหมด 4 แบบ แต่เนื่องจากว่า $205^2+164^2, 205^2+(-164)^2, 164^2+205^2$ รูปแบบของการแทนได้มาจากการเปลี่ยนเครื่องหมายของ 164 หรือสลับที่ จึงถือว่าแทนผลบวกกำลังสอง 2 เทอมได้เพียงแบบเดียวเท่านั้น

- $n=41^4$ เขียนได้ 3 แบบ คือ $1681^2+0^2, 1640^2+369^2, 1519^2+720^2$

  $41^3=41\cdot 41^3$ ซึ่ง 41^3 เขียนได้ 2 แบบ

  จากแบบที่ 1 $41^4=(5^2+4^2)(236^2+115^2)$

  $41^4=(1180-460)^2+(575+944)^2=720^2+1519^2$

  และ $41^4=(1180+460)^2+(575-944)^2=1640^2+369^2$

  จากแบบที่ 2 $41^4=(5^2+4^2)(205^2+164^2)$

  $41^4=(1025-656)^2+(820+820)^2=369^2+1640^2$

  และ $41^4=(1025+656)^2+(820-820)^2=1681^2+0^2$

  จากความเป็นจริงจะเห็นได้ว่าสามารถเขียนได้ทั้งหมด 4 แบบ แต่เนื่องจากว่า มีสองจำนวนที่เกิดจากการสลับที่ซึ่งกันและกัน จึงคิดเป็นเพียง 1 รูปแบบเท่านั้น

  ดังนั้น 41^4 สามารถเขียนได้เพียง 3 แบบ

- $n = 41^5$ เขียนได้ 3 แบบ คือ $10475^2 + 2476^2, 9676^2 + 4715^2,$ $8405^2 + 6724^2$
- $n = 41^6$ เขียนได้ 4 แบบ คือ $68921^2 + 0^2, 67240^2 + 15129^2,$ $62279^2 + 29520^2, 54280^2 + 42471^2$
- $n = 41^7$ เขียนได้ 4 แบบ คือ $441284^2 + 4765^2, 429475^2 + 101516^2,$ $396716^2 + 193315^2, 344605^2 + 275684^2$

และ $n = 41^8, 41^9, ..., 41^f$ ก็สามารถหาคำตอบได้โดยวิธีเดียวกัน

บทที่ 4

จำนวนครั้งการคำนวณการแทนด้วยผลบวกกำลังสอง 2 เทอม

จากการศึกษาบทความที่เกี่ยวข้องและวิธีการดำเนินงานวิจัย ในบทที่ 3 ที่ผ่านมาได้ศึกษาขั้นตอนการแทนด้วยผลบวกกำลังสอง 2 เทอมของจำนวนเต็ม และใช้โปรแกรมคอมพิวเตอร์เพื่อช่วยในการพิจารณาจำนวนครั้งการคำนวณของจำนวนเต็ม a,b และหาการแทนด้วยผลบวกกำลังสอง 2 เทอมของจำนวนเต็ม n เราได้ข้อสรุปและข้อสังเกต โดยมีรายละเอียดดังนี้

4.1 โปรแกรมที่ใช้หาจำนวนเต็มที่แทนด้วยผลบวกกำลังสอง 2 เทอม

จากบทที่ 3 สามารถหาค่า a,b ของจำนวนเต็ม n ที่เขียนแทนด้วยบวกกำลังสอง 2 เทอมได้ถึง 2 วิธี แต่จากการทดลองสุ่มหาการแทนด้วยผลบวกกำลังสอง 2 เทอม ค่า a,b ของจำนวนเต็มที่สามารถเขียนแทนได้ทั้งจำนวนเฉพาะและจำนวนประกอบ ซึ่งยังไม่สามารถสรุปได้ว่าการเริ่มจากขอบบนหรือการเริ่มจากขอบล่าง วิธีใดที่จะคำนวณหาค่า a,b ได้รวดเร็วกว่า

ดังนั้น ในหัวข้อนี้เราจะหาค่า a,b ของจำนวนเต็ม n ที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ โดยใช้โปรแกรมคอมพิวเตอร์ภาษา Java ช่วยในการคำนวณ

4.1.1 โปรแกรมที่ใช้คำนวณหาจำนวนเต็ม a,b

สำหรับโปรแกรมที่ใช้ในการคำนวณนี้จะแยกเป็น 2 เมท็อด คือ เมท็อดคำนวณค่าสำหรับจำนวนเฉพาะ และเมท็อดคำนวณค่าสำหรับจำนวนประกอบ

1. เมท็อดคำนวณค่าสำหรับจำนวนเฉพาะ

```
public static void sumof2squarePXFile() throws IOException {
    long  n, m1, m2,  i, j, k, a, b;
    long  median;
   boolean sqr = false;
    char  ch;
    int   cntPrime = 0, cntNearUpper=0;
   String ofilestr="_sum_squareP.txt";
    System.out.println("List of all Sum of two Squares of primes a to b");
    System.out.print("From number  a : ");  a = sc.nextLong();
    System.out.print("To   number  b : ");  b = sc.nextLong();
    if (b-a < 4000)
        ofile = new PrintWriter ("con:");
```

```
        else {
            System.out.println("Output write to file "+ofilestr);
            ofile = new PrintWriter (ofilestr);
            ofile.printf("Prime Number : From-To :   %d - %d %n", a, b );
            }
        ofile.printf("  Prime     Upper  Low    Median %n");
        for(k=a; k<=b ; k++) {
            if (!isPrime(k))  continue;
            if ( k%4==3)  continue;
            cntPrime=cntPrime+1;
            m1 = (long) (Math.sqrt(k/2)+0.5);  m2 = (long) Math.sqrt(k);
            median = (m1+m2)/2;
            ofile.printf("%8d, U-L:%5d,%5d :%5d %n", k, m2,m1, median );
            for ( i=m2; i>=m1; i-- ) {
                j=(long) Math.sqrt(k-i*i);
                if (k==(i*i+j*j)  && (j<=i)) {
                    if (i>median) { ch='*'; cntNearUpper++; }
                    else ch=' ';
                    ofile.printf("%10c %c :  %5d^2 : %4d^2 :", ' ',ch, i,  j );
                    ofile.printf(" sq:% 10d,%10d%n", i*i, j*j );
                    sqr=true;
                    }
                }
            }
        ofile.printf("Amount of prime number : %5d %n", cntPrime );
        ofile.printf("Amount of near upper   : %5d %n", cntNearUpper);
        ofile.close();
}
```

2. เมท็อดคำนวณค่าสำหรับจำนวนประกอบ

```
public static void sumof2squareNXFile() throws IOException {
    long  n, m1, m2,  i, j, k, a, b;
    long  median;
    boolean sqr=false;
    char  ch;
    boolean prnNewGrp;
    int   cntN=0, cntCase=0, cntNearUpper=0;
    ofilestr="_sum_squareN.txt";
    System.out.println("List of all Sum of two Squares of composite a to b");
    System.out.print("From number  a : ");   a = sc.nextLong();
    System.out.print("To   number  b : ");   b = sc.nextLong();
    if (b-a < 4000)
       ofile = new PrintWriter ("con:");
    else {
       System.out.println("Output write to file "+ofilestr);
       ofile = new PrintWriter (ofilestr);
       ofile.printf("Composite Number : From-To :   %d - %d %n", a, b );
    }
    ofile.printf("      N      Upper   Low    Median %n");
    for(k=a; k<=b ; k++) {
       if (isPrime(k))  continue;
       if ( k%4==3)  continue;
       m1 = (long) (Math.sqrt(k/2)+0.5);     m2 = (long) Math.sqrt(k);
       median = (m1+m2)/2;
       prnNewGrp=true;
```

```
            for ( i=m2; i>=m1; i-- ) {
                    j=(long) Math.sqrt(k-i*i);
                    if (k==(i*i+j*j)  && (j<=i)) {
                       if (prnNewGrp) {
                            ofile.printf("%8d, U-L:%5d,%5d :%5d %n", k, m2,m1, median );
                            prnNewGrp=false;
                            cntN =cntN+1;
                       }
                       cntCase =cntCase+1;
                       if (i>median) { ch='*'; cntNearUpper++; }
                       else ch=' ';
                       ofile.printf("%10c %c :  %5d^2 : %4d^2 : ", ' ',ch, i,  j );
                       ofile.printf(" sq:% 10d,%10d  %n", i*i, j*j );
                       sqr=true;
                    }
               }
            }
            ofile.printf("Amount of N     : %5d %n", cntN );
            ofile.printf("Amount of cases : %5d %n", cntCase );
            ofile.printf("Amount of near upper : %5d %n", cntNearUpper);
            ofile.close()
}
```

3.เมท็อด main

ตัวอย่างเมท็อด main ที่ใช้ในการเรียกใช้ เมท็อดคำนวณในข้อที่ 1 และข้อที่ 2

```
public static void main(String[] args) throws IOException  {
    sumof2squarePXFile();
}
```

4.2 การหาค่า a, b ของจำนวนเต็มที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอม

การพิจารณาหาค่าของ a, b หาได้โดยคำนวณเริ่มจากขอบบน และคำนวณเริ่มจากขอบล่าง ซึ่งวิธีการกล่าวไว้ในหัวข้อ 3.1

4.2.1 จำนวนครั้งการหาค่า a ของจำนวนเฉพาะ

ในหัวข้อนี้จะพิจารณาหาค่า a ของจำนวนเฉพาะ โดยเปรียบเทียบจำนวนครั้งในการคำนวณระหว่างคำนวณเริ่มจากของบน และคำนวณเริ่มจากขอบล่าง

รายละเอียดส่วนหัวของตาราง 4.1 เป็นดังนี้

คอลัมน์ที่ 1 จำนวนเต็ม คือ จำนวนที่เฉพาะที่สามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอม ได้ ซึ่งก็คือเป็นจำนวนเฉพาะที่มีรูปแบบ $4k+1$
คอลัมน์ที่ 2 ขอบบนเป็นจำนวนเต็มที่มากที่สุดที่น้อยกว่า $\sqrt{p}$
คอลัมน์ที่ 3 ขอบล่างเป็นจำนวนเต็มที่น้อยที่สุดที่มากกว่า $\sqrt{p/2}$
คอลัมน์ที่ 4 ระยะห่างระหว่างขอบ คำนวณได้จาก ขอบบน – ขอบล่าง $+1$
คอลัมน์ที่ 5 ค่า a คือค่าที่สามารถคำนวณหาค่า b ที่เป็นรูปกำลังสองได้และทำให้ $p = a^2 + b^2$ ซึ่งจำนวนเฉพาะสามารถหาค่า a, b ที่สอดคล้องได้เพียงแบบเดียว
คอลัมน์ที่ 6 เริ่มจากขอบบน หมายถึง จำนวนครั้งที่พบค่า a โดยวิธีเริ่มคำนวณจากขอบบน
คอลัมน์ที่ 7 เริ่มจากขอบล่าง หมายถึง จำนวนครั้งที่พบค่า a โดยวิธีเริ่มคำนวณจากขอบล่าง

ตารางที่ 4.1 ตัวอย่างจำนวนครั้งคำนวณหาค่าของ a ของจำนวนเฉพาะ จาก 3000 ถึง 3209

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
3001	54	39	16	51	4	13
3037	55	39	17	54	2	16
3041	55	39	17	55	1	17
3049	55	40	16	45	11	6
3061	55	40	16	55	1	16
3089	55	40	16	55	1	16
3109	55	40	16	47	9	8
3121	55	40	16	40	16	1
3137	56	40	17	56	1	17
3169	56	40	17	55	2	16
3181	56	40	17	45	12	6
3209	56	41	16	53	4	13

จากตัวอย่างในตาราง 4.1 จะเห็นได้ว่า บางจำนวนเมื่อคำนวณหาค่า a จะมีจำนวนครั้งในการคำนวณโดยคำนวณเริ่มจากขอบบนมีจำนวนครั้งน้อยกว่าคำนวณเริ่มจากขอบล่าง เช่น 3041 จะได้ว่าจำนวนครั้งในการคำนวณโดยเริ่มจากขอบบน คำนวณทั้งหมด 1 ครั้ง ส่วนการคำนวณโดยเริ่มจากขอบล่างจะคำนวณทั้งหมด 17 ครั้ง นั่นคือ 3041 เมื่อคำนวณโดยเริ่มจากขอบบนจะพบค่า a ได้เร็วกว่า และมีบางจำนวนเมื่อคำนวณหาค่า a จะมีจำนวนครั้งในการคำนวณโดยคำนวณเริ่มจากขอบล่างมีจำนวนครั้งน้อยกว่าคำนวณเริ่มจากขอบบน เช่น 3121 ซึ่งจากตารางจะเห็นได้ชัดว่าเมื่อคำนวณโดยเริ่มจากขอบล่างจะพบค่า a ได้เร็วกว่า แต่ก็ยังไม่สามารถสรุปได้ว่าเริ่มจากขอบบนหรือขอบล่างจึงจะพบค่า a ได้เร็วกว่า

จากการศึกษาการแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอม และพิจารณาการคำนวณหาค่า a ของจำนวนเฉพาะตั้งแต่ $1-1000000$ เพื่อให้ได้ข้อสรุปสำหรับการหาค่า a,b ที่ทำให้จำนวนเต็มเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ ดังตารางที่ 4.2

ตารางที่ 4.2 การเปรียบเทียบการหาจำนวนที่แทนด้วยผลบวกกำลังสอง 2 เทอม โดยเริ่มจากขอบล่าง และเริ่มจากขอบบน ของจำนวนเฉพาะ $1-1000000$

จำนวนเต็ม	จำนวนเต็มที่แทนด้วย a^2+b^2 ได้	จำนวนเต็มที่พบค่า a ได้เร็ว เมื่อเริ่มจากขอบบน	จำนวนเต็มที่พบค่า a ได้เร็ว เมื่อเริ่มจากขอบล่าง
1-100000	4784	3337	1447
100001-200000	4194	2928	1266
200001-300000	4003	2799	1204
300001-400000	3920	2732	1188
400001-500000	3831	2672	1159
500001-600000	3791	2618	1173
600001-700000	3726	2627	1099
700001-800000	3667	2556	1111
800001-900000	3669	2563	1106
900001-1000000	3591	2508	1083
รวม	39176	27340	11836

จากตารางที่ 4.2 สรุปได้ว่าจำนวนเฉพาะตั้งแต่ $1-1000000$ จำนวนที่สามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ทั้งหมด 39176 จำนวน และพบว่ามีจำนวนที่พบค่า a ได้เร็วโดยคำนวณเริ่มจากขอบบนมีทั้งหมด 27340 จำนวน คิดเป็น 69.79% และจำนวนที่พบค่า a ได้เร็วโดยคำนวณเริ่มจากขอบล่างด้วยมีทั้งหมด 11836 จำนวน คิดเป็น 30.21% ของจำนวนที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ทั้งหมด

4.2.1 จำนวนครั้งการหาค่า a ของจำนวนประกอบ

ในหัวข้อนี้จะพิจารณาหาค่า a ของจำนวนประกอบ โดยเปรียบเทียบจำนวนครั้งในการคำนวณระหว่างคำนวณเริ่มจากของบน และคำนวณเริ่มจากขอบล่าง

รายละเอียดส่วนหัวของตาราง 4.2 เป็นดังนี้

คอลัมน์ที่ 1 จำนวนเต็ม คือ จำนวนที่ประกอบที่สามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ ซึ่งก็คือเป็นจำนวนประกอบทที่มีรูปแบบ ตามหัวข้อ 3.3

คอลัมน์ที่ 2 ขอบบนเป็นจำนวนเต็มที่มากที่สุดที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$

คอลัมน์ที่ 3 ขอบล่างเป็นจำนวนเต็มที่น้อยที่สุดที่มากกว่าหรือเท่ากับ $\sqrt{n/2}$

คอลัมน์ที่ 4 ระยะห่างระหว่างขอบ คำนวณได้จาก ขอบบน – ขอบล่าง $+1$

คอลัมน์ที่ 5 ค่า a คือค่าที่สามารถคำนวณหาค่า b ที่เป็นรูปกำลังสองได้และทำให้ $n=a^2+b^2$ ซึ่งจำนวนประกอบสามารถหาค่า a,b ที่สอดคล้องได้หลายรูปแบบโดยขึ้นกับตัวประกอบ

คอลัมน์ที่ 6 เริ่มจากขอบบน หมายถึง จำนวนครั้งที่พบค่า a โดยวิธีเริ่มคำนวณจากขอบบน

คอลัมน์ที่ 7 เริ่มจากขอบล่าง หมายถึง จำนวนครั้งที่พบค่า a โดยวิธีเริ่มคำนวณจากขอบล่าง

ตารางที่ 4.3 ตัวอย่างจำนวนครั้งคำนวณหาค่าของ a ของจำนวนประกอบ จาก 2000 ถึง 2036

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
2000	44	32	13	40	5	9
2000	44	32	13	44	1	13
2005	44	32	13	39	6	8
2005	44	32	13	41	4	10
2009	44	32	13	35	10	4
2017	44	32	13	44	1	13
2018	44	32	13	43	2	12
2020	44	32	13	38	7	7
2020	44	32	13	42	3	11
2025	45	32	14	36	10	5
2025	45	32	14	45	1	14
2026	45	32	14	45	1	14
2034	45	32	14	45	1	14
2036	45	32	14	44	2	13

จากตาราง 4.3 จะพบว่าบางรูปแบบของจำนวนเต็ม จะมีจำนวนครั้งในการคำนวณหาค่า a โดยคำนวณเริ่มจากขอบบนจะน้อยกว่า แต่บางรูปแบบจำนวนครั้งในการคำนวณเริ่มจากขอบล่างจะน้อยกว่า แต่ก็ยังไม่สามารถสรุปได้ว่าเริ่มจากขอบบนหรือขอบล่างจึงจะพบค่า a ได้เร็วกว่า จากการศึกษาการแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอม และพิจารณาการคำนวณหาค่า a ของจำนวนประกอบตั้งแต่ $1-1000000$ ได้ดังตาราง 4.4

ตารางที่ 4.4 การเปรียบเทียบการหาจำนวนที่แทนด้วยผลบวกกำลังสอง 2 เทอม โดยเริ่มจากขอบบน และเริ่มจากขอบล่าง ของจำนวนประกอบ $1-1000000$

จำนวนเต็ม	จำนวนเต็มที่แทนด้วย a^2+b^2 ได้	จำนวนรูปแบบทั้งหมด	จำนวนรูปแบบที่พบค่า a ได้เร็วเมื่อเริ่มจากขอบบน	จำนวนรูปแบบที่พบค่า a ได้เร็วเมื่อเริ่มจากขอบล่าง
1-100000	19243	34759	24225	10534
100001-200000	18228	35184	24539	10645
200001-300000	17914	35347	24647	10700
300001-400000	17708	35431	24717	10714
400001-500000	17553	35500	24771	10729
500001-600000	17447	35535	24813	10722
600001-700000	17362	35597	24804	10793
700001-800000	17318	35650	24879	10771
800001-900000	17210	35652	24863	10789
900001-1000000	17181	35715	24910	10805
รวม	177164	354370	247168	107202

จากตารางที่ 4.4 พบว่าจำนวนประกอบตั้งแต่ $1-1000000$ มีจำนวนที่สามารถเขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ทั้งหมด 177164 จำนวน ประกอบด้วยทั้งหมด 354370 รูปแบบ จะได้ว่ามีจำนวนรูปแบบที่พบค่า a ได้เร็วโดยคำนวณเริ่มจากขอบบนมีทั้งหมด 247168 จำนวน คิดเป็น 69.75% และจำนวนที่พบค่า a ได้เร็วด้วยโดยคำนวณเริ่มจากขอบล่าง มีทั้งหมด 107202 จำนวน คิดเป็น 30.25% ของจำนวนรูปแบบที่เขียนแทนด้วยผลบวกกำลังสอง 2 เทอมได้ทั้งหมด

ดังนั้นจากการศึกษาดังตารางที่ 4.2 และตารางที่ 4.4 สรุปได้ว่าสามารถหาค่าของจำนวนเต็ม a,b ของจำนวนเต็มที่แทนด้วยผลบวกกำลังสอง 2 เทอมได้โดยคำนวณเริ่มจากขอบบน จะมีโอกาสพบค่า a ได้รวดเร็วกว่าคำนวณเริ่มจากขอบล่าง

4.3 ข้อสังเกตเกี่ยวกับการคำนวณหาค่า a

ให้ n เป็นจำนวนเต็มที่เป็นผลคูณของจำนวนเฉพาะ 2 จำนวน

ข้อสังเกตที่ 4.1 จำนวนเฉพาะ 2 จำนวนที่พบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบบน แล้วค่า a ของจำนวนเต็ม n จะยังคงพบค่าได้เร็วโดยเริ่มคำนวณจากขอบบนหรือไม่

ข้อสังเกตที่ 4.2 จำนวนเฉพาะ 2 จำนวนพบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบล่าง แล้วค่า a ของจำนวนเต็ม n จะยังคงพบได้เร็วโดยเริ่มคำนวณจากขอบล่างหรือไม่

ข้อสังเกตที่ 4.3 จำนวนเฉพาะ 2 จำนวน มีหนึ่งจำนวนที่พบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบบน และอีกหนึ่งจำนวนพบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบล่างแล้วค่า a ของจำนวนเต็ม n จะพบได้เร็วโดยเริ่มคำนวณจากขอบบน หรือ เริ่มคำนวณจากขอบล่าง

จากข้อสังเกตที่ 4.1 จะแสดงในตัวอย่างที่ 4.1 และ 4.2

ตัวอย่าง 4.1 $p_1 = 29, p_2 = 37$ พบค่า a ได้เร็วโดยเริ่มคำนวณจากขอบบน

$$p_1 \times p_2 = 29 \times 37 = 1073$$

1073 ขอบบนคือ 32 ขอบล่างคือ 24 ความกว้างระหว่างช่วง 9

ผลบวกกำลังสอง 2 เทอม คือ $32^2 + 7^2$ และ $28^2 + 17^2$

จะได้ $a = 32$ พบค่า a โดยคำนวณ 1 ครั้งโดยเริ่มคำนวณจากขอบบน

$a = 28$ พบค่า a โดยคำนวณ 6 ครั้งโดยเริ่มคำนวณจากขอบบน

ตัวอย่าง 4.2 $p_1 = 101, p_2 = 109$ พบค่า a ได้เร็วโดยเริ่มคำนวณจากขอบบน

$$p_1 \times p_2 = 101 \times 109 = 11009$$

11009 ขอบบนคือ 104 ขอบล่างคือ 75 ความกว้างระหว่างช่วง 30

ผลบวกกำลังสอง 2 เทอม คือ $103^2 + 20^2$ และ $97^2 + 40^2$

$a = 103$ พบค่า a โดยคำนวณ 2 ครั้ง โดยเริ่มคำนวณจากขอบบน

$a = 97$ พบค่า a โดยคำนวณ 8 ครั้งโดยเริ่มคำนวณจากขอบบน

จากตัวอย่างข้างต้นจะเห็นได้ว่าไม่สามารถสรุปได้ว่าจะพบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบบน หรือ เริ่มคำนวณจากขอบล่าง

จากข้อสังเกตที่ 4.2 จะแสดงในตัวอย่างที่ 4.3 และ 4.4

ตัวอย่าง 4.3 ถ้าให้ $p_1 = 41, p_2 = 61$ พบค่า a ได้เร็วโดยเริ่มคำนวณจากขอบล่าง

$$p_1 \times p_2 = 41 \times 61 = 2501$$

2501 ขอบบนคือ 50 ขอบล่างคือ 36 ความกว้างระหว่างช่วง 15

ผลบวกกำลังสอง 2 เทอม คือ $50^2 + 1^2$ และ $49^2 + 10^2$

จะได้ $a = 50$ พบค่า a โดยคำนวณ 15 ครั้งโดยเริ่มคำนวณจากขอบล่าง

$a = 49$ พบค่า a โดยคำนวณ 14 ครั้งโดยเริ่มคำนวณจากขอบเขตล่าง

ตัวอย่าง 4.4 $p_1 = 181, p_2 = 313$ พบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบล่าง

$$p_1 \times p_2 = 181 \times 313 = 56653$$

56653 ขอบบนคือ 238 ขอบล่างคือ 169 ความกว้างระหว่างช่วง 70

ผลบวกกำลังสอง 2 เทอม คือ $238^2 + 3^2$ และ $237^2 + 22^2$

$a = 238$ พบค่า a โดยคำนวณ 70 ครั้ง โดยเริ่มคำนวณจากขอบล่าง

$a = 237$ พบค่า a โดยคำนวณ 69 ครั้ง โดยเริ่มคำนวณจากขอบล่าง

จากตัวอย่างข้างต้น ถ้าจำนวนเฉพาะสองจำนวนพบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบล่างทั้งคู่ จากการทดลองจะได้ว่าจำนวนเต็ม n นั้นกลับพบค่า a ได้เร็วโดยเริ่มคำนวณจากขอบบน

จากข้อสังเกตที่ 4.3 จะแสดงรายละเอียดในตัวอย่างที่ 4.5 และ 4.6

ตัวอย่าง 4.5 $p_1 = 37$ พบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบบน

$p_2 = 61$ พบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบล่าง

$p_1 \times p_2 = 37 \times 61 = 2257$

2257 ขอบบนคือ 47 ขอบล่างคือ 34 ความกว้างระหว่างช่วง 14

ผลบวกกำลังสอง 2 เทอม คือ $41^2 + 24^2$ และ $36^2 + 31^2$

$a = 41$ พบค่า a โดยคำนวณ 7 ครั้ง โดยเริ่มคำนวณจากขอบบน

$a = 36$ พบค่า a โดยคำนวณ 3 ครั้ง โดยเริ่มคำนวณจากขอบล่าง

ตัวอย่าง 4.6 $p_1 = 137$ พบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบบน

$p_2 = 773$ พบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบล่าง

$p_1 \times p_2 = 137 \times 773 = 105901$

105901 ขอบบนคือ 325 ขอบล่างคือ 231 ความกว้างระหว่างช่วง 95

ผลบวกกำลังสอง 2 เทอม คือ $310^2 + 99^2$ และ $275^2 + 174^2$

$a = 310$ พบค่า a โดยคำนวณ 16 ครั้ง โดยเริ่มคำนวณจากขอบบน

$a = 275$ พบค่า a โดยคำนวณ 45 ครั้ง โดยเริ่มคำนวณจากขอบล่าง

จากตัวอย่างข้างต้นจะเห็นได้ว่าไม่สามารถสรุปได้ว่าจะพบค่า a ได้เร็ว โดยเริ่มคำนวณจากขอบบน หรือ เริ่มคำนวณจากขอบล่าง

บทที่ 5

สรุปผลการดำเนินงานและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

1. สำหรับจำนวนเฉพาะที่สามารถเขียนแทนได้ในรูป $p=a^2+b^2$ สามารถหาค่า a ได้โดย สำหรับ $a>b$ จะได้ $\sqrt{p/2}<a<\sqrt{p}$ และหาค่า b ได้จาก $b=\sqrt{p-a^2}$
2. การเขียนแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอมของจำนวนประกอบในรูป $n=a^2+b^2$ โดยถ้ามีตัวประกอบเป็นจำนวนเฉพาะรูปแบบ $4k+3$ และมีซ้ำเป็นจำนวนคู่ จะสามารถเขียนแทนได้ แต่ถ้ามีตัวประกอบรูป $4k+3$ และมีซ้ำเป็นจำนวนคี่ จะไม่สามารถเขียนแทนได้
3. สำหรับจำนวนประกอบที่สามารถเขียนแทนได้ในรูป $n=a^2+b^2$ สามารถหาค่า a ได้โดย สำหรับ $a>b$ จะได้ $\sqrt{n/2}<a<\sqrt{n}$ และหาค่า b ได้จาก $b=\sqrt{n-a^2}$ และสำหรับจำนวนประกอบที่เขียนแทนได้อาจมีมากกว่า 1 รูปแบบขึ้นกับตัวประกอบ
4. ขั้นตอนในการพิจารณาจำนวนเต็มที่สามารถเขียนเป็นผลบวกกำลังสอง 2 เทอมได้
5. จำนวนรูปแบบของการแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอม
6. จำนวนครั้งการคำนวณหาค่า a ของการแทนจำนวนเต็มด้วยผลบวกกำลังสอง 2 เทอมในรูป a^2+b^2 สำหรับจำนวนเฉพาะ การคำนวณหาค่า a โดยเริ่มจากขอบบนได้รวดเร็วคิดเป็น 69.79% สำหรับจำนวนประกอบ การคำนวณหาค่า a โดยเริ่มจากขอบบนได้รวดเร็วคิดเป็น 69.75%

5.2 ข้อเสนอแนะ

1. การหารูปแบบการแทนด้วยผลบวกกำลังสอง 2 เทอมในปัญหาพิเศษนี้ยังไม่เพียงพอซึ่งยังมีรูปแบบอื่นอีก ควรศึกษาเพิ่มเติมจาก 4 กรณีนี้ซึ่งยังเหลืออีก 2 กรณี
2. จากการที่ศึกษาจำนวนเต็มตั้งแต่ $1-1000000$ โดยร้อยละในการคำนวณหาค่า a,b โดยเริ่มจากขอบเขตบนของทั้งจำนวนเฉพาะและจำนวนประกอบมากพอที่จะสามารถเป็นแนวทางในการเลือกวิธีที่ใช้คำนวณหาค่า a ได้

เอกสารอ้างอิง

[1] รศ.ไพรบูลย์ พันธรักษ์พงษ์ และรศ.พัชรินทร์ เหมโชติ. ทฤษฎีจำนวน 1. พิมพ์ครั้งที่ 3. กรุงเทพฯ: ห้างหุ้นส่วนจำกัดมีนเซอวิสซัพพลาย, 2556

[2] รศ.ไพรบูลย์ พันธรักษ์พงษ์ และรศ.พัชรินทร์ เหมโชติ. ทฤษฎีจำนวน 2. พิมพ์ครั้งที่ 3. กรุงเทพฯ: ห้างหุ้นส่วนจำกัดมีนเซอวิสซัพพลาย, 2557

[3] David M. Burton. Elementary Number Theory. Seventh Edition. Singapore: McGraw – Hill, 2011.

ภาคผนวก

ภาคผนวก ก

พิสูจน์ทฤษฎีบท

ทฤษฎีบท 2.1 ขั้นตอนวิธีการหาร

สำหรับจำนวนเต็ม a,b ใดๆ โดยที่ $b>0$ จะมีจำนวนเต็ม q และ r อย่างละหนึ่งจำนวน ที่สอดคล้องกับ $a=qb+r$, $0\le r<b$

q เรียกว่า ผลหาร (quotient) , r เรียกว่าเศษเหลือ (remainder) ในการหาร a ด้วย b

พิสูจน์ ให้ a,b เป็นจำนวนเต็ม สิ่งที่สนใจอยู่ในรูปแบบ $a=xb+r$ หรือ $r=a-xb$

พิจารณาเซตของจำนวนเต็มที่มาเป็นลบ

$$S=\{a-xb \mid x\in\mathbb{Z}, a-xb\ge 0\}$$

จงแสดงว่าเซต S เป็นเซตที่ไม่ว่าง

การพิสูจน์เพียงพอที่จะแสดงว่ามีจำนวนเต็ม x ซึ่ง $ax-b$ ไม่เป็นลบ เนื่องจาก $b\ge 1$ ดังนั้น

$$|a|b\ge|a|$$

บวก a ทั้งสองข้างได้ $a+|a|b\ge a+|a|$

เพราะว่า $a+|a|b=a-\left(-|a|\right)b$ และ $a+|a|\ge 0$ ดังนั้น $a-\left(-|a|\right)b\ge 0$

ถ้าให้ $x=-|a|$ แล้วจะได้ $a-xb\in S$

ดังนั้น S เป็นเซตของจำนวนเต็มบวกที่ไม่เป็นเซตว่าง

และโดยคุณสมบัติการเป็นอันดับที่ดี S มีสมาชิกตัวที่น้อยที่สุด

จะแสดงว่า $r<b$ ให้ r เป็นสมาชิกตัวที่น้อยที่สุดของ S ฉะนั้น $r\ge 0$

โดยนิยามจะมีจำนวนเต็ม q ที่สอดคล้องกับ $r=a-qb$

สมมติว่า $r\ge b$ และพิจารณา

$$r-b=a-qb-b=a-(q+1)b\ge 0$$

เพราะว่า $q+1$ เป็นจำนวนเต็มจะได้ว่า

$$r-b \in S \quad \text{และ} \quad r-b \geq 0$$

แต่ที่ขัดแย้งกันคือเพราะว่า r เป็นสมาชิกตัวที่เล็กที่สุดของ S และ $b \geq 1$

แสดงว่า $r-b<r$

นั่นคือ $r-b<0$ หรือ $r<b$

ต่อไปจะแสดงว่า r และ q มีได้อย่างละ 1 จำนวนเท่านั้น

สมมติว่า a เขียนได้ 2 รูปแบบคือ

$a=qb+r$ เมื่อ $0 \leq r<b$

และ $a=q'b+r'$ เมื่อ $0 \leq r'<b$

ดังนั้น $qb+r=q'b+r'$

และ $r'-r=b(q-q')$

จากความจริงที่ว่า ค่าสัมบูรณ์ของผลคูณ เท่ากับ ผลคูณของค่าสัมบูรณ์

จะได้ว่า $|r'-r|=|b||q-q'|=b|q-q'|$ (เพราะว่า $b \geq 1$)

จาก $-b<-r \leq 0$ และ $0 \leq r'<b$

จะได้ $-b<r'-r<b$ หรือ $|r'-r|<b$

ดังนั้น $b|q-q'|<b$ เมื่อ $0 \leq |q-q'|<1$

เพราะว่า $|q-q'|$ เป็นจำนวนเต็มที่ไม่เป็นลบ จึงเป็นได้อย่างเดียวเท่านั้นคือ

$$|q-q'|=0$$

นั่นคือ $q=q'$ และผลที่ตามมาคือ $r=r'$ □

บทแทรก 2.2 สำหรับจำนวนเต็ม a,b ใดๆ โดยที่ $b \neq 0$ จะมีจำนวนเต็ม q และ r อย่างละหนึ่งจำนวน ซึ่ง $a = qb + r \quad , 0 \leq r < |b|$

พิสูจน์ เพราะว่า $b \neq 0$ จะได้ว่า $|b| > 0$

ดังนั้น โดยทฤษฎีบท 2.1 จะมีจำนวนเต็ม q' และ r อย่างละหนึ่งจำนวนที่

$$a = |b|q' + r \qquad 0 \leq r < |b|$$

ถ้า $b > 0$ จะได้ $\quad a = bq' + r \qquad 0 \leq r < |b|$

ถ้า $b < 0$ จะได้ $\quad a = -bq' + r$

$$= b(-q') + r \qquad 0 \leq r < |b|$$

ให้ $q = -q'$ จะได้ $\quad a = bq + r \qquad 0 \leq r < |b|$ □

ทฤษฎีบท 2.3 สำหรับจำนวนเต็ม a และ b $a \equiv b \pmod{n}$ ก็ต่อเมื่อ a และ b มีเศษเหลือที่ไม่เป็นลบเหมือนกันเมื่อหารด้วย n

พิสูจน์ ให้ $a \equiv b \pmod{n}$

จะได้ $a = b + kn$ โดยที่ k เป็นจำนวนเต็มบางจำนวน

การหาร b ด้วย n นั้น มีเศษเหลือคือ r นั่นคือ $b = qn + r$ เมื่อ $0 \leq r < n$

ฉะนั้น $\quad a = b + kn = (qn + r) + kn = (q + k)n + r$

ซึ่งแสดงให้เห็นว่า a มีเศษเหลือเดียวกันกับ b

ในทางกลับกัน สมมติให้ $a = q_1 n + r$ และ $b = q_2 n + r$

เมื่อเศษเหลือเหมือนกันคือ r $(0 \leq r < n)$ แล้ว

$$a - b = (q_1 + r) - (q_2 + r) = (q_1 - q_2)n$$

ฉะนั้น $n|(a-b)$ ซึ่งเมื่อเป็นสมภาคจะเขียนได้คือ $a \equiv b \pmod{n}$ □

ทฤษฎีบท 2.4 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

พิสูจน์

1) สำหรับจำนวนเต็ม a ใดๆ $a-a=0\cdot n$ จะได้ $a\equiv a\pmod{n}$

2) ถ้า $a\equiv b\pmod{n}$ แล้ว $a-b=kn$ สำหรับจำนวนเต็ม k บางจำนวน

เพราะฉะนั้น $b-a=-(kn)=(-k)n$

เนื่องจาก $-k$ เป็นจำนวนเต็ม จะได้ $b\equiv a\pmod{n}$

3) สมมติ $a\equiv b\pmod{n}$ และ $b\equiv c\pmod{n}$ แล้ว

จะมีจำนวนเต็ม h และ k ที่สอดคล้อง $a-b=hn$ และ $b-c=kn$

ซึ่งจะได้ $a-c=(a-b)+(b-c)=hn+kn=(h+k)n$

นั่นคือ $a\equiv c\pmod{n}$

4) ถ้า $a\equiv b\pmod{n}$ และ $c\equiv d\pmod{n}$

จะได้ $a-b=k_1n$ และ $c-d=k_2n$ สำหรับจำนวนเต็ม k_1 และ k_2 บางจำนวน

และ $(a+c)-(b+d)=(a-b)+(c-d)$

$=k_1n+k_2n=(k_1+k_2)n$

จากนิยามของสมภาคจะได้

$$a+c \equiv b+d \pmod{n}$$

ส่วนการพิสูจน์ $ac \equiv bd \pmod{n}$ ทำได้ดังนี้

$$ac = (b-k_1 n)(d-k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

เนื่องจาก $bk_2 + dk_1 + k_1 k_2 n$ เป็นจำนวนเต็มจะได้ว่า $ac-bd$ หารลงตัวด้วย n

เพราะฉะนั้น $ac \equiv bd \pmod{n}$

5) การพิสูจน์ครอบคลุมโดยข้อ 4 เนื่องจาก $c \equiv c \pmod{n}$

6) ใช้อุปนัยเชิงคณิตศาสตร์

เมื่อ $k=1$ ข้อความเป็นจริง

สมมติว่าเป็นจริงสำหรับบาง k ที่ถูกตรึง

จากข้อ 5 เมื่อ $a \equiv b \pmod{n}$ และ $a^k \equiv b^k \pmod{n}$

แล้วจะได้ $aa^k \equiv bb^k \pmod{n}$ หรือ $a^{k+1} \equiv b^{k+1} \pmod{n}$

นั่นคือข้อความเป็นจริงสำหรับ $k+1$

ซึ่งสรุปได้ว่าข้อความเป็นจริงสำหรับทุกจำนวนเต็มบวก k □

ทฤษฎีบท 2.5 ทฤษฎีหลักมูลเลขคณิต

ทุกๆ จำนวนเต็มบวก $n>1$ สามารถแสดงได้ในรูปผลคูณของจำนวนเฉพาะ และเขียนได้เพียงแบบเดียวเท่านั้น โดยไม่คำนึงถึงลำดับของตัวประกอบที่ได้

พิสูจน์ จำนวนเต็ม n เป็นจำนวนเฉพาะหรือจำนวนประกอบ
กรณีที่ n เป็นจำนวนเฉพาะไม่มีอะไรที่ต้องพิสูจน์
กรณีที่ n เป็นจำนวนประกอบแล้วจะมีจำนวนเต็ม d ที่สอดคล้องกับ $d \mid n$
และ $1<d<n$

สำหรับทุกจำนวนเต็ม d เลือก p_1 เป็นจำนวนที่น้อยที่สุดแล้ว p_1 ต้องเป็นจำนวนเฉพาะ มิฉะนั้นจะมีตัวหาร q ที่ $1<q<p_1$

แต่ $q \mid p_1$ และ $p_1 \mid n$ จะได้ $q \mid n$ ซึ่งเกิดข้อขัดแย้งกับที่ p_1 เป็นตัวหารที่เป็นบวกที่น้อยที่สุดของ n ซึ่งไม่เท่ากับ 1 ฉะนั้น

$$n = p_1 n_1 \qquad \text{เมื่อ } p_1 \text{ เป็นจำนวนเฉพาะและ } 1 < n_1 < n$$

ถ้า n_1 เป็นจำนวนเฉพาะแล้วจะเขียนแสดงได้ แต่ถ้าไม่เป็นตามนี้จะทำซ้ำสำหรับจำนวนเฉพาะ p_2 ซึ่ง $n_1 = p_2 n_2$

$$n = p_1 p_2 n_2 \qquad \text{โดยที่ } 1 < n_2 < n_1$$

ถ้า n_2 ไม่เป็นจำนวนเฉพาะ ให้ $n_2 = p_3 n_3$ ซึ่ง p_3 เป็นจำนวนเฉพาะ

$$n = p_1 p_2 p_3 n_3 \qquad \text{โดยที่ } 1 < n_3 < n_2$$

ลำดับลดลง

$$n > n_1 > n_2 > \ldots > 1$$

ซึ่งต้องเป็นจำนวนจำกัดของขั้น n_{k-1} เป็นจำนวนเฉพาะ ให้เป็น p_k ฉะนั้น

$$n = p_1 p_2 p_3 \ldots p_k$$

สำหรับการพิสูจน์ส่วนที่สองคือเขียนเป็นผลคูณจำนวนเฉพาะได้เพียงแบบเดียว สมมติว่า

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s \qquad \text{โดยที่ } r \le s$$

เมื่อ p_i และ q_j เป็นจำนวนเฉพาะ และ

$$p_1 \le p_2 \le \ldots \le p_r \text{ และ } q_1 \le q_2 \le \ldots \le q_s$$

เนื่องจาก $p_1 \mid q_1 q_2 \ldots q_s$ (โดยบทแทรกที่ว่า ถ้า $p, q_1, q_2, \ldots, q_n$ เป็นจำนวนเฉพาะและ $p \mid q_1 q_2 \ldots q_n$ แล้ว $p = q_k$ สำหรับบาง k โดยที่ $1 \le k \le n$)

ดังนั้น จะได้ว่า $p_1 = q_k$ สำหรับบาง k

แต่ $p_1 \ge q_k$ และด้วยเหตุผลทำนองเดียวกันจะได้ $q_1 \ge p_1$ ฉะนั้น $p_1 = q_1$ ละเว้นการเขียนตัวประกอบร่วมจึงได้

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s$$

และเมื่อทำกระบวนการซ้ำจะได้ $p_2 = q_2$ และ

$$p_3 p_4 \ldots p_r = q_3 q_4 \ldots q_s$$

และทำต่อไปเรื่อยๆ

ถ้า $r < s$ แล้วจะได้ $1 = q_{r+1} q_{r+2} \ldots q_s$

ซึ่งเป็นไปไม่ได้ เนื่องจากแต่ละ $q_j > 1$ ฉะนั้น $r = s$

และ $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_s$

จึงสรุปได้ว่าสองรูปที่เขียนได้เป็นแบบเดียวกัน □

ทฤษฎีบท 2.9 ทฤษฎีบทวิลสัน (Wilson's Theorem)

ถ้า p เป็นจำนวนเฉพาะ แล้ว $p|(p-1)!+1$

พิสูจน์ กรณี $p=2$ และ $p=3$ เห็นได้ชัดเจน ให้ $p>3$

สมมติว่า a เป็นจำนวนหนึ่งของจำนวนเต็มบวก $1,2,3,...,p-1$

และพิจารณาสมภาคเชิงเส้น $ax \equiv 1 (\mathrm{mod}\, p)$ จะได้ $\gcd(a,p)=1$

โดยทฤษฎีบทของสมภาคเชิงเส้น สมภาคมีผลเฉลยเพียงผลเฉลยเดียวมอดุโล p

ฉะนั้นจะมีจำนวนเต็ม a' เพียงจำนวนเดียวซึ่ง $1 \le a' \le p-1$

ที่สอดคล้องกับ $aa' \equiv 1 (\mathrm{mod}\, p)$

เนื่องจาก p เป็นจำนวนเฉพาะ $a=a'$ ก็ต่อเมื่อ $a=1$ หรือ $a=p-1$

ฉะนั้น $a^2 \equiv 1 (\mathrm{mod}\, p)$

สมมูลกับ $(a-1)\cdot(a+1) \equiv 0 (\mathrm{mod}\, p)$

ฉะนั้นจะได้ $a-1 \equiv 0 (\mathrm{mod}\, p)$ ซึ่งเป็นกรณี $a=1$

หรือ $a+1 \equiv 0 (\mathrm{mod}\, p)$ ซึ่งเป็นกรณี $a=p-1$

หรือถ้าละเว้น 1 และ $p-1$ จำนวนเต็มที่ยังเหลืออยู่คือ $2,3,...,p-2$ ซึ่งจะจัดเป็นคู่ของ a และ a' โดยที่ $a \ne a'$ ซึ่ง $aa' \equiv 1 (\mathrm{mod}\, p)$ จะได้ทั้งหมด $\frac{p-3}{2}$ สมภาค เมื่อคูณสมภาคทั้งหมดเข้าด้วยกัน และจัดตัวประกอบใหม่ จะได้

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

หรือ $(p-2)! \equiv 1 (\mathrm{mod}\, p)$

เมื่อคูณด้วย $p-1$ จะได้

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}$$ □

ภาคผนวก ข

จำนวนครั้งการคำนวณหาค่า a ของจำนวนเฉพาะ

ตารางที่ ข1 จำนวนครั้งคำนวณหาค่าของ a ของจำนวนเฉพาะ จาก 3000 ถึง 4800

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
3001	54	39	16	51	4	13
3037	55	39	17	54	2	16
3041	55	39	17	55	1	17
3049	55	40	16	45	11	6
3061	55	40	16	55	1	16
3089	55	40	16	55	1	16
3109	55	40	16	47	9	8
3121	55	40	16	40	16	1
3137	56	40	17	56	1	17
3169	56	40	17	55	2	16
3181	56	40	17	45	12	6
3209	56	41	16	53	4	13
3217	56	41	16	56	1	16
3221	56	41	16	55	2	15
3229	56	41	16	50	7	10
3253	57	41	17	57	1	17
3257	57	41	17	56	2	16
3301	57	41	17	49	9	9
3313	57	41	17	57	1	17
3329	57	41	17	52	6	12
3361	57	41	17	56	2	16
3373	58	42	17	58	1	17
3389	58	42	17	58	1	17
3413	58	42	17	58	1	17
3433	58	42	17	52	7	11

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
3449	58	42	17	43	16	2
3457	58	42	17	44	15	3
3461	58	42	17	50	9	9
3469	58	42	17	45	14	4
3517	59	42	18	59	1	18
3529	59	42	18	48	12	7
3533	59	43	17	58	2	16
3541	59	43	17	54	6	12
3557	59	43	17	49	11	7
3581	59	43	17	59	1	17
3593	59	43	17	53	7	11
3613	60	43	18	43	18	1
3617	60	43	18	44	17	2
3637	60	43	18	46	15	4
3673	60	43	18	48	13	6
3677	60	43	18	59	2	17
3697	60	43	18	49	12	7
3701	60	44	17	55	6	12
3709	60	44	17	53	8	10
3733	61	44	18	57	5	14
3761	61	44	18	56	6	13
3769	61	44	18	60	2	17
3793	61	44	18	52	10	9
3797	61	44	18	46	16	3
3821	61	44	18	61	1	18
3833	61	44	18	53	9	10
3853	62	44	19	62	1	19
3877	62	45	18	54	9	10
3881	62	45	18	59	4	15
3889	62	45	18	60	3	16

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
3917	62	45	18	61	2	17
3929	62	45	18	52	11	8
3989	63	45	19	58	6	14
4001	63	45	19	49	15	5
4013	63	45	19	62	2	18
4021	63	45	19	50	14	6
4049	63	45	19	55	9	11
4057	63	46	18	59	5	14
4073	63	46	18	52	12	7
4093	63	46	18	58	6	13
4129	64	46	19	60	5	15
4133	64	46	19	62	3	17
4153	64	46	19	48	17	3
4157	64	46	19	59	6	14
4177	64	46	19	64	1	19
4201	64	46	19	51	14	6
4217	64	46	19	64	1	19
4229	65	46	19	65	1	20
4241	65	47	19	65	1	19
4253	65	47	19	53	13	7
4261	65	47	19	65	1	19
4273	65	47	19	57	9	11
4289	65	47	19	65	1	19
4297	65	47	19	61	5	15
4337	65	47	19	49	17	3
4349	65	47	19	50	16	4
4373	66	47	20	62	5	16
4397	66	47	20	61	6	15
4409	66	47	20	53	14	7
4421	66	48	19	65	2	18

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
4441	66	48	19	60	7	13
4457	66	48	19	64	3	17
4481	66	48	19	65	2	18
4489	67	48	20	67	1	20
4493	67	48	20	67	1	20
4513	67	48	20	48	20	1
4517	67	48	20	49	19	2
4549	67	48	20	65	3	18
3561	67	48	20	60	8	13
4597	67	48	20	54	14	7
4621	67	49	19	61	7	13
4637	68	49	20	59	10	11
4649	68	49	20	68	1	20
4657	68	49	20	56	13	8
4673	68	49	20	58	11	10
4721	68	49	20	64	5	16
4729	68	49	20	52	17	4
4733	68	49	20	58	11	10
4789	69	49	21	55	15	7
4793	69	49	21	68	2	20

ตารางที่ ข2 จำนวนครั้งคำนวณหาค่าของ a ของจำนวนเฉพาะจาก 50000 ถึง 51800

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
50021	223	159	65	214	10	56
50033	223	159	65	172	52	14
50053	223	159	65	223	1	65
50069	223	159	65	215	9	57
50077	223	159	65	219	5	61
50093	223	159	65	173	51	15
50101	223	159	65	185	39	27
50129	223	159	65	223	1	65
50153	223	159	65	208	16	50
50177	223	159	65	224	0	66
50221	223	159	65	186	38	28
50261	223	159	65	190	34	32
50273	223	159	65	212	12	54
50321	223	159	65	215	9	57
50329	223	159	65	165	59	7
50333	223	159	65	218	6	60
50341	223	159	65	210	14	52
50377	223	159	65	216	8	58
50417	223	159	65	199	25	41
50441	223	159	65	221	3	63
50461	223	159	65	219	5	61
50497	223	159	65	184	40	26
50513	223	159	65	223	1	65
50549	223	159	65	218	6	60
50581	224	160	65	215	10	56
50593	224	160	65	207	18	48
50741	225	160	66	190	36	31
50753	225	160	66	223	3	64

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
50773	225	160	66	218	8	59
50777	225	160	66	221	5	62
50789	225	160	66	175	51	16
50821	225	160	66	225	1	66
50833	225	160	66	208	18	49
50849	225	160	66	215	11	56
50857	225	160	66	176	50	17
50873	225	160	66	212	14	53
50893	225	160	66	162	64	3
50909	225	160	66	197	29	38
50929	225	160	66	177	49	18
50957	225	160	66	221	5	62
50969	225	160	66	188	38	29
50989	225	160	66	210	16	51
50993	225	160	66	167	59	8
51001	225	160	66	220	6	61
51061	225	160	66	169	57	10
51109	226	160	67	225	2	66
51133	226	160	67	222	5	63
51137	226	160	67	224	3	65
51157	226	160	67	226	1	67
51169	226	160	67	180	47	21
51193	226	160	67	172	55	13
51197	226	161	66	226	1	66
51217	226	161	66	201	26	41
51229	226	161	66	190	37	30
51241	226	161	66	205	22	45
51257	226	161	66	181	46	21
51329	226	161	66	223	4	63
51341	226	161	66	221	6	61

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
51349	226	161	66	182	45	22
51361	226	161	66	175	52	15
51413	226	161	66	202	25	42
51421	226	161	66	214	13	54
51437	226	161	66	226	1	66
51449	226	161	66	200	27	40
51461	226	161	66	206	21	46
51473	226	161	66	188	39	28
51481	226	161	66	195	32	35
51517	226	161	66	226	1	66
51521	226	161	66	161	66	1
51577	227	161	67	211	17	51
51581	227	161	67	166	62	6
51593	227	161	67	227	1	67
51613	227	161	67	203	25	43
51637	227	161	67	201	27	41
51673	227	161	67	227	1	67
51713	227	161	67	217	11	57
51721	227	161	67	180	48	20
51749	227	161	67	218	10	58
51769	227	161	67	213	15	53
51797	227	161	67	194	34	34

ตารางที่ ข3 จำนวนครั้งคำนวณหาค่าของ a ของจำนวนเฉพาะจาก 900000 ถึง 902053

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
900001	948	671	278	924	25	254
900037	948	671	278	874	75	204
900061	948	671	278	750	199	80
900089	948	671	278	908	41	238
900121	948	671	278	936	13	266
900149	948	671	278	743	206	73
900157	948	671	278	891	58	221
900161	948	671	278	944	5	274
900169	948	671	278	725	224	55
900217	948	671	278	939	10	269
900233	948	671	278	757	192	87
900241	948	671	278	940	9	270
900253	948	671	278	802	147	132
900293	948	671	278	938	11	268
900329	948	671	278	923	26	253
900349	948	671	278	795	154	125
900397	948	671	278	726	223	56
900409	948	671	278	947	2	277
900461	948	671	278	910	39	240
900481	948	671	278	884	65	214
900553	948	671	278	948	1	278
900569	948	671	278	925	24	255
900577	948	671	278	849	100	179
900589	948	671	278	942	7	272
900593	948	671	278	847	102	177

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
900649	949	671	279	845	105	175
900673	949	671	279	903	47	233
900689	949	671	279	920	30	250
900701	949	671	279	949	1	279
900737	949	671	279	904	46	234
900761	949	671	279	940	10	270
900773	949	671	279	737	213	67
900797	949	671	279	949	1	279
900817	949	671	279	824	126	154
900821	949	671	279	905	45	235
900869	949	671	279	938	12	268
900917	949	671	279	934	16	264
900929	949	671	279	775	175	105
900937	949	671	279	944	6	274
900973	949	671	279	717	233	47
900997	949	671	279	894	56	224
901009	949	671	279	872	78	202
901013	949	671	279	887	63	217
901093	949	671	279	753	197	83
901097	949	671	279	859	91	189
901133	949	671	279	893	57	223
901141	949	671	279	921	29	251
901169	949	671	279	913	37	243
901177	949	671	279	949	1	279
901193	949	671	279	908	42	238
901213	949	671	279	923	27	253

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
901249	949	671	279	807	143	137
901253	949	671	279	703	247	33
901273	949	671	279	837	113	167
901309	949	671	279	822	128	152
901333	949	671	279	793	157	123
901429	949	671	279	850	100	180
901441	949	671	279	804	146	134
901457	949	671	279	929	21	259
901489	949	671	279	945	5	275
901501	949	671	279	949	1	279
901513	949	671	279	948	2	278
901517	949	671	279	874	76	204
901529	949	671	279	835	115	165
901613	949	671	279	922	28	252
901657	949	671	279	856	94	186
901709	949	671	279	947	3	277
901717	949	671	279	814	136	144
901741	949	671	279	915	35	245
901781	949	671	279	935	15	265
901841	949	672	278	820	130	149
901861	949	672	278	945	5	274
901909	949	672	278	678	272	7
901937	949	672	278	679	271	8
901973	949	672	278	722	228	51
901993	949	672	278	947	3	276
901997	949	672	278	926	24	255

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
902009	949	672	278	860	90	189
902017	949	672	278	936	14	265
902029	949	672	278	789	161	118
902053	949	672	278	838	112	167

ภาคผนวก ค

จำนวนครั้งการคำนวณหาค่า a ของจำนวนประกอบ

ตารางที่ ค1 จำนวนครั้งคำนวณหาค่าของ a ของจำนวนประกอบ จาก 2000 ถึง 2500

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
2000	44	32	13	40	5	9
2000	44	32	13	44	1	13
2005	44	32	13	39	6	8
2005	44	32	13	41	4	10
2009	44	32	13	35	10	4
2017	44	32	13	44	1	13
2018	44	32	13	43	2	12
2020	44	32	13	38	7	7
2020	44	32	13	42	3	11
2025	45	32	14	36	10	5
2025	45	32	14	45	1	14
2026	45	32	14	45	1	14
2034	45	32	14	45	1	14
2036	45	32	14	44	2	13
2041	45	32	14	40	6	9
2041	45	32	14	45	1	14
2042	45	32	14	41	5	10
2045	45	32	14	37	9	6
2045	45	32	14	43	3	12
2048	45	32	14	32	14	1
2050	45	33	13	33	13	1
2050	45	33	13	39	7	7
2050	45	33	13	45	1	13
2056	45	33	13	34	12	2
2057	45	33	13	44	2	12

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
2066	45	33	13	35	11	3
2074	45	33	13	43	3	11
2074	45	33	13	45	1	13
2080	45	33	13	36	10	4
2080	45	33	13	44	2	12
2084	45	33	13	40	6	8
2088	45	33	13	42	4	10
2097	45	33	13	39	7	7
2098	45	33	13	37	9	5
2105	45	33	13	43	3	11
2105	45	33	13	44	2	12
2106	45	33	13	45	1	13
2116	46	33	14	46	1	14
2117	46	33	14	34	13	2
2117	46	33	14	46	1	14
2120	46	33	14	38	9	6
2120	46	33	14	46	1	14
2122	46	33	14	41	6	9
2125	46	33	14	35	12	3
2125	46	33	14	42	5	10
2125	46	33	14	45	2	13
2125	46	33	14	46	1	14
2132	46	33	14	44	3	12
2132	46	33	14	46	1	14
2138	46	33	14	43	4	11
2146	46	33	14	39	8	7
2146	46	33	14	45	2	13
2152	46	33	14	46	1	14
2164	46	33	14	42	5	10
2165	46	33	14	41	6	9

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
2165	46	33	14	46	1	14
2169	46	33	14	45	2	13
2173	46	33	14	38	9	6
2173	46	33	14	43	4	11
2176	46	33	14	40	7	8
2178	46	33	14	33	14	1
2180	46	34	13	34	13	1
2180	46	34	13	46	1	13
2186	46	34	13	35	12	2
2192	46	34	13	44	3	11
2194	46	34	13	45	2	12
2196	46	34	13	36	11	3
2197	46	34	13	39	8	6
2197	46	34	13	46	1	13
2205	46	34	13	42	5	9
2209	47	34	14	47	1	14
2210	47	34	14	37	11	4
2210	47	34	14	41	7	8
2210	47	34	14	43	5	10
2210	47	34	14	47	1	14
2216	47	34	14	46	2	13
2218	47	34	14	47	1	14
2225	47	34	14	40	8	7
2225	47	34	14	44	4	11
2225	47	34	14	47	1	14
2228	47	34	14	38	10	5
2234	47	34	14	47	1	14
2245	47	34	14	34	14	1
2245	47	34	14	47	1	14
2248	47	34	14	42	6	9

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
2249	47	34	14	35	13	2
2249	47	34	14	43	5	10
2250	47	34	14	39	9	6
2250	47	34	14	45	3	12
2257	47	34	14	36	12	3
2257	47	34	14	41	7	8
2258	47	34	14	47	1	14
2260	47	34	14	44	4	11
2260	47	34	14	46	2	13
2269	47	34	14	37	11	4
2273	47	34	14	47	1	14
2276	47	34	14	40	8	7
2285	47	34	14	38	10	5
2285	47	34	14	46	2	13
2290	47	34	14	43	5	10
2290	47	34	14	47	1	14
2304	48	34	15	48	1	15
2305	48	34	15	39	10	6
2305	48	34	15	48	1	15
2306	48	34	15	41	8	8
2308	48	34	15	48	1	15
2312	48	34	15	34	15	1
2312	48	34	15	46	3	13
2313	48	34	15	48	1	15
2314	48	35	14	35	14	1
2314	48	35	14	45	4	11
2320	48	35	14	36	13	2
2320	48	35	14	48	1	14
2329	48	35	14	40	9	6
2329	48	35	14	48	1	14

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
2330	48	35	14	37	12	3
2330	48	35	14	47	2	13
2336	48	35	14	44	5	10
2340	48	35	14	42	7	8
2340	48	35	14	48	1	14
2344	48	35	14	38	11	4
2349	48	35	14	45	4	11
2353	48	35	14	47	2	13
2353	48	35	14	48	1	14
2362	48	35	14	39	10	5
2368	□□□35	35	14	48	1	14
2372	48	35	14	46	3	12
2378	48	35	14	43	6	9
2378	48	35	14	47	2	13
2384	48	35	14	42	7	8
2385	48	35	14	36	13	2
2385	48	35	14	48	1	14
2386	48	35	14	45	4	11
2401	49	35	15	49	1	15
2402	49	35	15	49	1	15
2404	49	35	15	48	2	14
2405	49	35	15	38	12	4
2405	49	35	15	46	4	12
2405	49	35	15	47	3	13
2405	49	35	15	49	1	15
2410	49	35	15	41	9	7
2410	49	35	15	49	1	15
2420	49	35	15	44	6	10
2421	49	35	15	39	11	5
2425	49	35	15	43	7	9

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
2425	49	35	15	45	5	11
2425	49	35	15	48	2	14
2426	49	35	15	49	1	15
2434	49	35	15	47	3	13
2440	49	35	15	42	8	8
2440	49	35	15	46	4	12
2448	49	35	15	48	2	14
2450	49	35	15	35	15	1
2450	49	35	15	49	1	15
2452	49	36	14	36	14	1
2458	49	36	14	37	13	2
2465	49	36	14	41	9	6
2465	49	36	14	44	6	9
2465	49	36	14	47	3	12
2465	49	36	14	49	1	14
2466	49	36	14	45	5	10
2468	49	36	14	38	12	3
2474	49	36	14	43	7	8
2482	49	36	14	39	11	4
2482	49	36	14	49	1	14
2493	49	36	14	42	8	7
2498	49	36	14	47	3	12
2500	50	36	15	42	9	7
2500	50	36	15	48	3	13
2500	50	36	15	50	1	15

ตารางที่ ค2 จำนวนครั้งคำนวณหาค่าของ a ของจำนวนประกอบ จาก 50000 ถึง 50200

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
50000	223	159	65	164	60	6
50000	223	159	65	200	24	42
50000	223	159	65	220	4	62
50005	223	159	65	199	25	41
50005	223	159	65	201	23	43
50005	223	159	65	206	18	48
50005	223	159	65	217	7	59
50013	223	159	65	222	2	64
50018	223	159	65	193	31	35
50018	223	159	65	223	1	65
50020	223	159	65	176	48	18
50020	223	159	65	198	26	40
50020	223	159	65	202	22	44
50020	223	159	65	216	8	58
50021	223	159	65	214	10	56
50024	223	159	65	182	42	24
50024	223	159	65	190	34	32
50024	223	159	65	218	6	60
50026	223	159	65	165	59	7
50029	223	159	65	210	14	52
50033	223	159	65	172	52	14
50045	223	159	65	197	27	39
50045	223	159	65	203	21	45
50053	223	159	65	223	1	65
50056	223	159	65	166	58	8
50066	223	159	65	221	3	63

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
50068	223	159	65	222	2	64
50069	223	159	65	215	9	57
50074	223	159	65	207	17	49
50077	223	159	65	219	5	61
50080	223	159	65	196	28	38
50080	223	159	65	204	20	46
50081	223	159	65	209	15	51
50081	223	159	65	220	4	62
50089	223	159	65	180	44	22
50089	223	159	65	192	32	34
50090	223	159	65	167	57	9
50090	223	159	65	223	1	65
50093	223	159	65	173	51	15
50098	223	159	65	177	47	19
50098	223	159	65	187	37	29
50101	223	159	65	185	39	27
50114	223	159	65	217	7	59
50121	223	159	65	189	35	31
50125	223	159	65	195	29	37
50125	223	159	65	205	19	47
50125	223	159	65	218	6	60
50125	223	159	65	222	2	64
50128	223	159	65	168	56	10
50128	223	159	65	212	12	54
50129	223	159	65	223	1	65
50130	223	159	65	183	41	25

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
50130	223	159	65	213	11	55
50137	223	159	65	216	8	58
50137	223	159	65	221	3	63
50146	223	159	65	211	13	53
50152	223	159	65	214	10	56
50153	223	159	65	208	16	50
50157	223	159	65	174	50	16
50164	223	159	65	220	4	62
50170	223	159	65	169	55	11
50170	223	159	65	191	33	33
50170	223	159	65	219	5	61
50170	223	159	65	223	1	65
50176	224	159	66	224	1	66
50177	224	159	66	224	1	66
50180	224	159	66	178	47	20
50180	224	159	66	194	31	36
50180	224	159	66	206	19	48
50180	224	159	66	224	1	66
50184	224	159	66	210	15	52
50184	224	159	66	222	3	64
50185	224	159	66	181	44	23
50185	224	159	66	224	1	66
50192	224	159	66	224	1	66
50194	224	159	66	215	10	57

ตารางที่ ค3 จำนวนครั้งคำนวณหาค่าของ a ของจำนวนประกอบ จาก 900000 ถึง 900250

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
900002	948	671	278	841	108	171
900005	948	671	278	863	86	193
900005	948	671	278	833	116	163
900008	948	671	278	938	11	268
900010	948	671	278	901	48	231
900010	948	671	278	899	50	229
900017	948	671	278	871	78	201
900017	948	671	278	856	93	186
900029	948	671	278	805	144	135
900029	948	671	278	773	176	103
900040	948	671	278	902	47	232
900040	948	671	278	898	51	228
900058	948	671	278	947	2	277
900065	948	671	278	943	6	273
900065	948	671	278	916	33	246
900065	948	671	278	881	68	211
900065	948	671	278	692	257	22
900073	948	671	278	948	1	278
900073	948	671	278	933	16	263
900073	948	671	278	768	181	98
900073	948	671	278	712	237	42
900081	948	671	278	945	4	275
900081	948	671	278	840	109	170
900090	948	671	278	903	46	233

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
900090	948	671	278	897	52	227
900090	948	671	278	879	70	209
900090	948	671	278	813	136	143
900098	948	671	278	883	66	213
900098	948	671	278	857	92	187
900100	948	671	278	946	3	276
900100	948	671	278	888	61	218
900100	948	671	278	800	149	130
900112	948	671	278	816	133	146
900112	948	671	278	704	245	34
900113	948	671	278	868	81	198
900113	948	671	278	823	126	153
900122	948	671	278	941	8	271
900122	948	671	278	719	230	49
900133	948	671	278	942	7	272
900133	948	671	278	927	22	257
900133	948	671	278	913	36	243
900133	948	671	278	778	171	108
900136	948	671	278	810	139	140
900136	948	671	278	730	219	60
900146	948	671	278	935	14	265
900146	948	671	278	925	24	255
900146	948	671	278	911	38	241
900146	948	671	278	739	210	69
900148	948	671	278	948	1	278
900153	948	671	278	693	256	23

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
900154	948	671	278	827	122	157
900160	948	671	278	904	45	234
900160	948	671	278	896	53	226
900160	948	671	278	864	85	194
900160	948	671	278	832	117	162
900170	948	671	278	937	12	267
900170	948	671	278	839	110	169
900173	948	671	278	947	2	277
900173	948	671	278	877	72	207
900189	948	671	278	885	64	215
900189	948	671	278	858	91	188
900202	948	671	278	819	130	149
900224	948	671	278	920	29	250
900224	948	671	278	760	189	90
900225	948	671	278	948	1	278
900225	948	671	278	921	28	251
900225	948	671	278	735	214	65
900226	948	671	278	915	34	245
900234	948	671	278	747	202	77
900244	948	671	278	930	19	260
900245	948	671	278	946	3	276
900245	948	671	278	934	15	264
900245	948	671	278	713	236	43
900245	948	671	278	694	255	24
900250	948	671	278	945	4	275
900250	948	671	278	931	18	261

จำนวนเต็ม	ขอบบน	ขอบล่าง	ระยะห่างระหว่างขอบ	ค่า a	เริ่มจากขอบบน	เริ่มจากขอบล่าง
900250	948	671	278	905	44	235
900250	948	671	278	895	54	225
900250	948	671	278	807	142	137
900250	948	671	278	789	160	119
900250	948	671	278	771	178	101