ทฤษฎีจำนวน

Number Theory

คณะครุศาสตร์

มหาวิทยาลัยราชภัฏสวนสุนันทา

2566

MAI1305

ทฤษฎีจำนวน

Number Theory

ผู้ช่วยศาสตราจารย์ ดร.ธนัชยศ จำปาหวาย
สาขาวิชาคณิตศาสตร์ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา
เอกสารประกอบการสอนวิชาทฤษฎีจำนวน ประจำปีการศึกษา 2/2566

สารบัญ

บทที่ 1
ความรู้พื้นฐาน

การนับจำนวนเป็นสิ่งที่อยู่คู่กับมนุษยชาติมาช้านาน การพยายามทำความเข้าใจเกี่ยวกับจำนวนของมนุษย์จึงเกิดขึ้นเพื่อนำไปใช้ประโยชน์ในด้านต่าง ๆ จนเกิดเป็นการศึกษาสมบัติของจำนวนเหล่านั้นเรื่อยมา อันเป็นที่มาของสาขาหนึ่งทางคณิตศาสตร์ คือ “ทฤษฎีจำนวน” (number theory) การมองเห็นวิวัฒนาการของวิชาทฤษฎีจำนวนนับเป็นพื้นฐานความรู้เพื่อให้รู้จักวิชานี้ ซึ่งจะกล่าวถึงเป็นส่วนแรก ก่อนจะกล่าวถึงเซตเบื้องต้น การพิสูจน์เบื้องต้น และสมบัติจำนวนเต็ม เนื่องจากในขอบข่ายการศึกษาทฤษฎีจำนวน จะจำกัดเฉพาะจำนวนเต็มเท่านั้น และการเข้าใจสมบัติที่เกี่ยวกับจำนวนเต็มจะเป็นเครื่องมือสำคัญในการพิสูจน์สมบัติต่าง ๆ ที่เกี่ยวข้องต่อไป

1.1 วิวัฒนาการของวิชาทฤษฎีจำนวน

ทฤษฎีจำนวน เป็นสาขาวิชาหนึ่งในคณิตศาสตร์ซึ่งศึกษาเกี่ยวกับสมบัติของจำนวนโดยเน้นที่สมบัติของจำนวนเต็มและจำนวนนับ (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2552. หน้า1) เนื่องจากจำนวนนับเป็นจำนวนชนิดแรก ๆ ที่มนุษย์รู้จัก จึงไม่น่าแปลกใจที่มนุษย์สนใจศึกษาจำนวนเหล่านี้ในแง่มุมต่าง ๆ อย่างกว้างขวาง และมีผู้ยกย่องไว้ว่า "วิชาทฤษฎีจำนวนเปรียบเสมือนราชินี แห่งคณิตศาสตร์ (Number theory is the queen of mathematics)" ตามคำกล่าวของนักคณิตศาสตร์ผู้มีชื่อเสียงนามว่า คาร์ล ฟรีดริช เกาส์ (Carl Fridrich Gauss 1777–1855)

ทฤษฎีจำนวนมีความเก่าแก่ย้อนกลับไปกว่า 2,500 ปีซึ่งนับว่าเป็นศาสตร์ที่มีความเก่าแก่ที่สุดก็ว่าได้ ผู้บุกเบิกวิชานี้ คือ พีทาโกรัส (Pythagoras 569–500 ปีก่อนคริสต์ศักราช) โดยเขาพยายามอธิบายจักรวาลและสรรพสิ่งรอบตัวว่าคือจำนวน จนก่อกำเนิดเป็นสำนักคิดอันรวบรวมผู้คนที่เชื่อเหมือนพีทาโกรัสไว้ด้วยกัน โดยมีปรัชญาสำคัญว่า "ทุกสิ่งทุกอย่างคือจำนวน" จากการรวมเป็นสำนักคิดนี้เองทำให้ค้นพบสมบัติพิเศษเกี่ยวกับจำนวนมากมาย เช่น **จำนวนมิตรภาพ (amicable numbers)** ซึ่งผลบวกของตัวหารแท้ของจำนวนหนึ่งจะเท่ากับผลบวกของตัวหารแท้อีกจำนวนหนึ่ง ในสมัยของพีทาโกรัสพบจำนวนมิตรภาพคู่แรกคือ 284 และ 220 ตัวหารแท้ของ 284 คือ 1, 2, 4, 71 และ 142 จะได้ว่า

$$1 + 2 + 4 + 71 + 142 = 220$$

ตัวหารแท้ของ 220 คือ 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 และ 110 จะได้ว่า

$$1+2+4+5+10+11+20+22+44+55+110=284$$

การบุกเบิกเรื่องจำนวนมิตรภาพข้างต้นเป็นฐานให้เกิดการค้นพบจำนวนมิตรภาพอื่น ๆ อีกมากมายตามมา ดังตัวอย่างตามตารางต่อไปนี้

ปีที่ค้นพบ	ผู้คนพบ	จำนวนมิตรภาพ
ค.ศ. 1636	Pierre De Fermat (1601–1665)	17,296 และ 18,416
ค.ศ. 1686	Rene Descartes (1596–1650)	9,363,584 และ 9,437,056
ค.ศ. 1830	Adrien Marie Legendre (1752–1833)	2,172,649,216 และ 8,520,191
ค.ศ. 1866	Nicolo Painini ชาวอิตาลีอายุ 16 ปี	1,184 และ 1,210

ตารางที่ 1 แสดงตัวอย่างจำนวนมิตรภาพและผู้คนพบ

กระทั่งในปัจจุบันคอมพิวเตอร์สามารถคำนวณจำนวนมิตรภาพได้มากกว่า 1,000 ล้านคู่ (เมษายน ค.ศ.2016) ซึ่งเห็นได้ชัดว่ารากฐานของการคำนวณจำนวนดังกล่าวนี้มีมากกว่าสองพันปีแล้ว

จำนวนสมบูรณ์ (perfect number) ถูกค้นพบในยุคของพีทาโกรัสเป็นจำนวนที่มีความมหัศจรรย์อีกจำนวน เหตุที่เรียกเช่นนี้ เพราะเป็นจำนวนที่เท่ากับผลบวกของตัวหารแท้ของจำนวนนั้น เช่น 6 มีตัวหารแท้ คือ 1 2 และ 3 ผลบวกเท่ากับ 6 ก่อนที่จะเกิดการค้นพบจำนวนสมบูรณ์อีกสองจำนวนต่อมา คือ 28 และ 496 กระทั่งในปี ค.ศ. 2016 ได้พบทั้งหมด 49 จำนวน

ยุคสำคัญของการศึกษาทฤษฎีจำนวนสมัยต่อมาเกิดขึ้นราว 300 ปีก่อนคริสตกาล เมื่อยุคลิด แห่งอเล็กซานเดรีย (Euclic of Alexandria 450–380 ปีก่อนคริสต์ศักราช) ได้ตีพิมพ์หนังสืออิลิเมนต์ จำนวน 13 เล่ม โดยมีหนังสือ 3 เล่มในชุดนั้นกล่าวถึงเรื่องราวเกี่ยวกับทฤษฎีจำนวน ได้แก่ จำนวนคู่ จำนวนคี่ และจำนวนเฉพาะ ขั้นตอนวิธีแบบยุคลิด ตัวหารร่วมมาก ตัวคูณรวมน้อย และทฤษฎีบทที่ว่าจำนวนเฉพาะมีจำนวนเป็นอนันต์

สมัยกรีกยังมีนักคณิตศาสตร์อีกคนที่สำคัญคือ ดีโอฟานโตสแห่งอเล็กซานเดรีย (Diophantus of Alexandria) ซึ่งมีชีวิตอยู่ในช่วง 250 ปีก่อนคริสตกาล ได้ตีพิมพ์หนังสือ 13 เล่ม เนื้อหาในหนังสือชุดนี้ได้เรียบเรียงวิธีการแก้สมการทางพีชคณิตและปัญหาต่าง ๆ ผลงานสำคัญของดีโอฟานโตส คือ สมการที่มีคำตอบเป็นจำนวนเต็มเรียกว่า **สมการไดโอแฟนไทน์ (Diophantine equation)** ตัวอย่างเช่นสมการพีทาโกรัส $x^2+y^2=z^2$ อันกลายเป็นรากฐานของการศึกษาทฤษฎีจำนวนในปัจจุบัน

แม้การศึกษาทฤษฎีจำนวนจะมีมาตั้งแต่สมัยกรีก หากการสิ้นสุดอารยธรรมกรีกโรมันต่อด้วยการเข้าสู่ยุคกลางของยุโรปทำให้เกิดการชะงักงันทางการศึกษาดังกล่าว เนื่องจากองค์ความรู้จาก คริสตศาสนาได้กลายเป็นศูนย์กลางในการอธิบายสรรพสิ่งรอบตัวแทน จนกระทั่งเข้าสู่ยุคฟื้นฟูศิลปวิทยาการ (Renaissance) ราวคริสตศตวรรษที่ 14–17 ได้มีการฟื้นฟูวิทยาการสมัยกรีกโรมันขึ้นมาอีกครั้ง ช่วงเวลานี้เองที่เป็นจุดเริ่มต้นของทฤษฎีจำนวนสมัยปัจจุบัน เริ่มโดยนักคณิตศาสตร์ชาวฝรั่งเศสชื่อว่า ปิแยร์ เดอ แฟร์มาต์ (Pierre de Fermat 1601–1665) เขาได้ทำการศึกษางานของดีโอฟานโตสและเป็นคนที่ได้พบสมบัติของจำนวนเต็มอีกมากมาย โดยเฉพาะการคาดการณ์ว่าสมการ $x^n+y^n=z^n$ ไม่มีคำตอบเป็นจำนวนเต็มที่ไม่ใช่ศูนย์เมื่อ n เป็นจำนวนเต็มที่มากกว่า 2 แม้ขณะนั้นเขาสามารถพิสูจน์ได้เพียงกรณีที่ $n=3$ เท่านั้น หากต่อมา

นักคณิตศาสตร์รุ่นหลังได้พยายามพิสูจน์ต่อจนสำเร็จ และตั้งชื่อว่า “ทฤษฎีบทสุดท้ายของแฟร์มาต์” เพื่อเป็นเกียรติพร้อมยกย่อง แฟร์มาต์ว่าเป็นบิดาของทฤษฎีจำนวนสมัยใหม่

ทฤษฎีจำนวนของแฟร์มาต์ได้ส่งอิทธิพลต่อนักทฤษฎีจำนวนคนสำคัญอีกคน คือ เกาส์ ซึ่งได้ตีพิมพ์หนังสือ Disquistiones Arithmeticae ในปี 1801 เนื้อหาเกี่ยวกับการพิสูจน์อย่างเป็นระบบก่อนพัฒนาต่อมาเป็นสมบัติของจำนวนเฉพาะอันเป็นการวางรากฐานเกี่ยวกับทฤษฎีจำนวนไว้อย่างมั่นคง

จากการศึกษาวิชาทฤษฎีจำนวนหลายพันปีเห็นได้ว่า มีหัวข้อเกี่ยวกับจำนวนให้ขบคิดมากมาย หัวข้อในการศึกษาบางประการต้องใช้เวลานานกว่าจะได้รับการแก้ไข บางครั้งต้องผ่านการพิสูจน์ซ้ำแล้วซ้ำเล่า หากพิจารณาว่าประเด็นใดเป็นสิ่งที่นักคณิตศาสตร์ให้ความสนใจอย่างยิ่งคงไม่พ้นเรื่องจำนวนเฉพาะ เหตุผลประการแรก คือการตรวจสอบว่าจำนวนใดเป็นจำนวนเฉพาะไม่ใช่เรื่องง่ายดายนัก ถ้าจำนวนนั้นเป็นจำนวนขนาดใหญ่ เช่น 10,006,721 แต่ปัญหานี้ในปัจจุบันเราสามารถตรวจสอบโดยใช้คอมพิวเตอร์พบว่า 10,006,721 เป็นจำนวนเฉพาะตัวที่ 664,999 เหตุผลอีกประการหนึ่ง คือมีสูตรทั่วไปในการหาจำนวนเฉพาะตัวที่ n หรือไม่ หลายศตวรรษมาแล้วเชื่อว่า $n^2 + n + 41$ เป็นจำนวนเฉพาะ สูตรนี้เป็นจริงเพียง 40 จำนวนเรียงติดกันคือ $n = 0, 1, 2, ..., 39$ ทั้งนี้ ข้อเสนอของแฟร์มาต์ในการหาจำนวนเฉพาะคือ $F_n = 2^{2^n} + 1$ เป็นจำนวนเฉพาะสำหรับทุกจำนวนเต็ม $n \geq 0$ ต่อมาพบว่า $n = 5$ ไม่เป็นจำนวนเฉพาะเนื่องจาก 641 เป็นตัวประกอบของ F_5 พบโดยออยเลอร์ (Leonhard Euler ค.ศ. 1707–1783) เรียก F_n ว่า**จำนวนแฟร์มาต์ (Fermat number)** ในกรณีที่เป็นจำนวนเฉพาะเรียกว่า **จำนวนเฉพาะแฟร์มาต์ (Fermat prime)**

ปัญหาเกี่ยวกับจำนวนเฉพาะที่สนใจเรื่องหนึ่งก็คือ **จำนวนเฉพาะคู่แฝด (twin prime)** คือ จำนวนเต็ม p และ $p + 2$ เป็นจำนวนเฉพาะทั้งคู่ เช่น 5 และ 7, 11 และ 13, 17 และ 19, 29 และ 31 เป็นต้น มีจำนวนเฉพาะคู่แฝดไม่จำกัดจำนวนใช่หรือไม่ โดยใช้เครื่องคอมพิวเตอร์ตรวจสอบพบว่ามีจำนวนเฉพาะคู่แฝดที่น้อยกว่า 30,000,000 มีทั้งหมด 152,892 คู่

ทั้งหมดนี้เป็นเพียงจุดสนใจส่วนหนึ่งในวิชาทฤษฎีจำนวนเท่านั้น ยังมีสิ่งที่น่าสนใจอีกมากมายและยังคงมีปัญหาที่ยังไม่สามารถหาคำตอบได้ (unsolved problem) ให้ได้ขบคิด สิ่งนี้เป็นความ ท้าท้ายและอาจก่อให้เกิดองค์ความรู้ใหม่ ๆ ตามมาได้

1.2 เซตเบื้องต้น

เซต (Set) เป็นคำอนิยาม หมายถึงคำที่ต้องยอมรับกันในเบื้องต้นว่าไม่สามารถให้ความหมายที่รัดกุมได้ คำว่าเซตจึงหมายถึงกลุ่มของสิ่งของต่าง ๆ เมื่อกล่าวถึงกลุ่มใดแล้วจะสามารถบอกได้แน่นอนว่าสิ่งใดอยู่ในกลุ่ม และสิ่งใดอยู่นอกกลุ่ม เรียกสิ่งต่าง ๆ ที่อยู่ในเซตว่า **สมาชิก (element)** (P. Glendinning. 2012. หน้า 48) ถ้า a เป็นสมาชิกของเซต A เขียนแทนด้วย $a \in A$ และถ้า a ไม่เป็นสมาชิกของเซต A เขียนแทนด้วย $a \notin A$ เช่น $A = \{1, 2, 3\}$ จะได้ว่า $1 \in A$ แต่ $4 \notin A$ เป็นต้น

การเขียนเซตประกอบด้วย 2 วิธีคือ วิธีแจกแจงสมาชิก และวิธีบอกเงื่อนไขของสมาชิก

1. **วิธีแจกแจงสมาชิก (Tubular form)** การเขียนเซตแบบแจกแจงสมาชิก คือการเขียน

เซตโดยเขียนสมาชิกลงในเครื่องหมายวงเล็บปีกกา $\{\}$ และใช้เครื่องหมายจุลภาค $(,)$ คั่นระหว่างสมาชิกแต่ละตัว ตัวอย่างเช่น $\{1,2,3\}, \{4,5,6\}$ และ $\{a,b,c\}$ เป็นต้น

2. **วิธีบอกเงื่อนไขของสมาชิก (Set builder form)** การเขียนเซตแบบบอกเงื่อนไขประกอบด้วย 2 ส่วน ส่วนแรกหมายถึงสมาชิก และส่วนที่สองคือเงื่อนไขของสมาชิก โดยมีเครื่องหมายทวิภาค $(:)$ คั่นระหว่างสองส่วนนั้น อ่านว่า "โดยที่"

$$A = \{ \text{ สมาชิก } : \text{ เงื่อนไขของสมาชิก } \}$$

ตัวอย่างเช่น $A = \{x : x \text{ เป็นจำนวนเต็มบวกที่น้อยกว่า } 5\}$ หมายถึง เซต A คือเซตของ x โดยที่ x เป็นจำนวนเต็มบวกที่น้อยกว่า 5 และเขียนแจกแจงสมาชิกได้เป็น $A = \{1,2,3,4,5\}$

สำหรับเซต A ที่มีสมาชิกทุกตัวอยู่ในเซต B จะกล่าวว่า A เป็น **สับเซต (subset)** ของ B เขียนแทนด้วย $A \subseteq B$

ในเบื้องต้นเพื่อให้ง่ายต่อการนำไปใช้ กำหนดสัญลักษณ์ดังนี้

$\mathbb{C}$	แทนเซตของจำนวนเชิงซ้อน	$\mathbb{Z}$	แทนเซตของจำนวนเต็ม
$\mathbb{R}$	แทนเซตของจำนวนจริง	$\mathbb{N}$	แทนเซตของจำนวนนับ

สำหรับเซตที่ไม่มีสมาชิกเขียนแทนด้วย $\varnothing$ เรียกว่า **เซตว่าง (empty set)** และ **เอกภพสัมพัทธ์ (universe)** คือเซตที่ถูกกำหนดขึ้นโดยมีข้อตกลงว่า จะกล่าวถึงสิ่งที่เป็นสมาชิกของเซตนี้เท่านั้น และนิยมใช้ $\mathcal{U}$ แทนเอกภพสัมพัทธ์ เมื่อให้ A และ B เป็นเซตในเอกภพสัมพัทธ์ $\mathcal{U}$ นิยามการดำเนินการบนเซตดังต่อไปนี้

ยูเนียน (union)	$A \cup B = \{x \in \mathcal{U} : x \in A \text{ หรือ } x \in B\}$
อินเตอร์เซกชัน (intersection)	$A \cap B = \{x \in \mathcal{U} : x \in A \text{ และ } x \in B\}$
ผลต่าง (difference)	$A - B = \{x \in \mathcal{U} : x \in A \text{ และ } x \notin B\}$
ส่วนเติมเต็ม (complement)	$A^c = \{x \in \mathcal{U} : x \notin A\}$

ในกรณีที่ทราบจำนวนสมาชิกของเซต A เขียน $|A|$ แทนจำนวนสมาชิกของ A และได้ว่า

$$|A \cup B| = |A| + |B| - |A \cap B|$$
$$|A| = |\mathcal{U}| - |A^c|$$

เมื่อ A และ B เป็นเซตที่ทราบจำนวนสมาชิกแน่ชัด เป็นเซตในเอกภพสัมพัทธ์ $\mathcal{U}$

1.3 การพิสูจน์เบื้องต้น

ในหัวข้อนี้เราจะกล่าวถึงพื้นฐานทางตรรกศาสตร์และระเบียบวิธีการพิสูจน์เบื้องต้นเพื่อนำไปใช้เป็นเครื่องมือในการศึกษาทฤษฎีจำนวนในบทต่อ ๆ ไป เริ่มต้นด้วยประโยคหรือข้อความที่

น่าสนใจทางคณิตศาสตร์เป็นข้อความที่เราตัดสินใจได้ว่า ต้องเป็นจริงหรือเป็นเท็จอย่างใดอย่างหนึ่งเท่านั้น จะเป็นทั้งสองอย่างไม่ได้ กล่าวคือถ้าข้อความใดไม่เป็นจริงแล้วข้อความนั้นต้องเป็นเท็จ ในนัยกลับกัน ถ้าข้อความใดไม่เป็นเท็จแล้วข้อความนั้นต้องเป็นจริง (พัฒนี อุดมกะวานิช. 2559. หน้า 2) เรียกข้อความหรือประโยคเหล่านั้นว่า **ประพจน์ (proposition)** และมีตัวเชื่อมประพจน์ 4 ชนิดคือ

1. และ เขียนแทนด้วย $\wedge$
2. หรือ เขียนแทนด้วย $\vee$
3. ถ้า...แล้ว เขียนแทนด้วย $\rightarrow$
4. ก็ต่อเมื่อ เขียนแทนด้วย $\leftrightarrow$

สรุปค่าความจริงในแต่ละกรณีตามตารางดังต่อไปนี้ เมื่อ p และ q เป็นประพจน์ และ T แทนค่าความจริงเป็นจริง F แทนค่าความจริงเป็นเท็จ

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	T	F
F	T	F	T	F	F
F	F	F	F	T	T

ตารางที่ 2 แสดงค่าความจริงของประพจน์ที่ถูกเชื่อมทั้ง 4 แบบ

ต่อไปจะกล่าวถึง **นิเสธของประพจน์ (negation of proposition)** หมายถึงประพจน์ที่มีค่าความจริงตรงข้ามกับประพจน์นั้น ให้ p เป็นประพจน์ แล้วนิเสธของประพจน์ของ p เขียนแทนด้วย $\sim p$ แสดงค่าความจริงได้ดังตารางต่อไปนี้

p	$\sim p$
T	F
F	T

ตารางที่ 3 แสดงค่าความจริงของ $\sim p$

สองประพจน์มีความหมายเดียวกันในทางตรรกศาสตร์จะเรียกว่า **สมมูลกันเชิงตรรกศาสตร์ (logically equivalent)** หรือกล่าวคือ ประพจน์ p **สมมูล (equivalence)** กับ q เขียนแทนด้วย $p \equiv q$ ก็ต่อเมื่อประพจน์ทั้งสองมีค่าความจริงตรงกันทุกกรณี ตัวอย่างเช่น $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ และ $p \rightarrow q \equiv \sim q \rightarrow \sim p$ เรียกว่า**กฎแย้งสลับที่ (contrapositive law)**

ประพจน์ที่มีรูปแบบที่มีค่าความจริงเป็นจริงเสมอเรียกว่า **สัจนิรันดร์ (tautology)** และเรียกนิเสธของสัจนิรันดร์ว่า **ข้อความขัดแย้ง (contradiction)** ตัวอย่างเช่น $\sim p \vee p$ และ $p \rightarrow p \vee q$ เป็นสัจนิรันดร์ และ $\sim p \wedge p$ เป็นข้อความขัดแย้ง

ให้ p แทนประพจน์ $x > 2$ เมื่อ $x \in \{1, 2, 3, 4\}$ พิจารณาค่าความจริงดังตาราง

x	$p:\ x > 2$	ค่าความจริง
1	$1 > 2$	F
2	$2 > 2$	F
3	$3 > 2$	T
4	$4 > 2$	T

จากตารางจะเห็นได้ว่าค่าความจริงของประพจน์ p เปลี่ยนไปตามค่า x นิยมใช้ $p(x)$ แทนประพจน์ p และเรียก $\{1,2,3,4\}$ ว่า**เอกภพสัมพัทธ์** (universe) นิยมเขียนแทนด้วย $\mathcal{U}$ เมื่อกล่าวว่า

" มี x ใน $\mathcal{U}$ ที่สอดคล้อง $p(x)$ "

ประพจน์นี้มีค่าความจริงเป็นจริงเพราะว่ามี $x = 3$ ซึ่งทำให้ $p(3)$ มีค่าความจริงเป็นจริง เขียนแทนคำว่า "มี" ด้วย $\exists$ ดังนั้นเขียนประพจน์ดังกล่าวได้เป็น $\exists x \in \mathcal{U}, p(x)$ ในทำนองเดียวกัน ถ้ากล่าวว่า

" ทุก ๆ x ใน $\mathcal{U}$ ที่สอดคล้อง $p(x)$ "

ประพจน์นี้จะมีค่าความจริงเป็นเท็จเพราะว่ามี $x = 1$ ที่ทำให้ $p(1)$ มีค่าความจริงเป็นเท็จ เขียนแทนคำว่า "ทุก ๆ" ด้วย $\forall$ ดังนั้นเขียนประพจน์ดังกล่าวได้เป็น $\forall x \in \mathcal{U}, p(x)$ เรียก 2 สัญลักษณ์ดังกล่าวว่า **ตัวบ่งปริมาณ** (quantifier)

หลายครั้งมักจะพบประพจน์ที่ซับซ้อนมากขึ้นเช่น "มีจำนวนเต็มจำนวนหนึ่งซึ่งบวกกับทุกจำนวนเต็มแล้วเท่ากับศูนย์" เขียนสัญลักษณ์ได้เป็น

$$\exists x \in \mathbb{Z} \forall y \in \mathbb{Z},\ x + y = 0$$

ประพจน์ลักษณะนี้กล่าวได้ว่ามีตัวบ่งปริมาณ 2 ตัว

ต่อมาจะกล่าวถึงการหานิเสธของประพจน์ที่มีตัวบ่งปริมาณ เช่น "ไม่มีจำนวนเต็ม x ที่สอดคล้อง $x^2 + x + 1 = 0$" เขียนเป็นสัญลักษณ์คือ

$$\sim \exists x \in \mathbb{Z},\ x^2 + x + 1 = 0$$

หมายถึง "ทุกจำนวนเต็ม x จะสอดคล้อง $x^2 + x + 1 \neq 0$" เขียนเป็นสัญลักษณ์คือ

$$\forall x \in \mathbb{Z},\ x^2 + x + 1 \neq 0$$

สรุปได้ดังนี้ ให้ $\mathcal{U}$ เป็นเอกภพสัมพัทธ์ของประพจน์ $p(x)$ นิเสธของตัวบ่งปริมาณนิยามโดย

นิสเธของ $\forall x \in \mathcal{U},\ p(x)$ คือ $\sim \forall x \in \mathcal{U},\ p(x) \equiv \exists x \in \mathcal{U},\ \sim p(x)$

นิสเธของ $\exists x \in \mathcal{U},\ p(x)$ คือ $\sim \exists x \in \mathcal{U},\ p(x) \equiv \forall x \in \mathcal{U},\ \sim p(x)$

ในหัวข้อนี้ผู้เขียนจะมีการนำเสนอวิธีการพิสูจน์ไว้ทั้งหมด 6 วิธี ประกอบไปด้วย

1. การพิสูจน์ข้อความแบบมีเงื่อนไข
2. การพิสูจน์โดยการแจกแจงกรณี
3. การพิสูจน์ข้อความแบบผันกลับได้
4. การพิสูจน์โดยวิธีขัดแย้ง
5. การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว
6. การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์

1. การพิสูจน์ข้อความแบบมีเงื่อนไข

การพิสูจน์ข้อความที่อยู่ในรูปแบบมีเงื่อนไข $p \to q$ เรียกวิธีการพิสูจน์แบบนี้ว่า **การพิสูจน์ข้อความแบบมีเงื่อนไข** (proof of conditional statements) เราต้องการแสดงว่าข้อความ $p \to q$ เป็นจริงทุก ๆ กรณีหรือเป็นสัจนิรันดร์ นั่นคือแสดงว่าถ้า p เป็นจริง แล้ว q เป็นจริงเสมอ เขียนเป็นโครงพิสูจน์ได้ดังนี้

สมมติ	p	เป็นจริง
	$\vdots$	
ดังนั้น	q	เป็นจริง (ข้อสรุป) $\square$

เราจะเรียกวิธีนี้ว่า**การพิสูจน์โดยวิธีตรง** (direct proof) นิยมใช้เครื่องหมาย $\square$ วางไว้บรรทัดสุดท้ายเพื่อบอกว่าจบการพิสูจน์ ในส่วนที่ว่างเว้นไว้คือส่วนที่จะเติมรายละเอียดให้สมบูรณ์อาจจะได้จากนิยาม ทฤษฎีบทที่พิสูจน์มาก่อนหน้า หรือสัจพจน์ เพื่อให้นำไปสู่ข้อสรุปอย่างเป็นเหตุเป็นผลกัน เมื่อพิสูจน์โดยวิธีตรงไม่ได้เราจะใช้สมมูลที่ว่า $p \to q \equiv \sim q \to \sim p$ เราเรียกว่า **การพิสูจน์โดยวิธีการแย้งสลับที่** (contrapositive proof) มีโครงการพิสูจน์ดังนี้

สมมติ	$\sim q$	เป็นจริง
	$\vdots$	
ดังนั้น	$\sim p$	เป็นจริง $\square$

ก่อนจะให้ตัวอย่างการพิสูจน์เราจะให้บทนิยามที่ต้องใช้การพิสูจน์ก่อนคือ

บทนิยาม 1.3.1 จำนวนคู่ (even number) คือจำนวนเต็มที่หารด้วยสองลงตัว หรือเราจะกล่าวว่า a เป็นจำนวนคู่ถ้ามีจำนวนเต็ม k ซึ่ง $a = 2k$ และ**จำนวนคี่** (odd number) คือจำนวนเต็มที่ไม่ใช่จำนวนคู่ หรือเราจะกล่าวว่า a เป็นจำนวนคี่ถ้ามีจำนวนเต็ม k ซึ่ง $a = 2k + 1$

ตัวอย่าง 1.3.2 จงพิสูจน์ว่า " ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่ "

ตัวอย่าง 1.3.3 จงพิสูจน์ว่า " ถ้า n^2 เป็นจำนวนคู่ แล้ว n เป็นจำนวนคู่ "

2. การพิสูจน์โดยการแจกแจงกรณี

การพิสูจน์ข้อความในรูปแบบ $(p \vee q) \to r$ เนื่องจาก

$$(p \vee q) \to r \equiv (p \to r) \wedge (q \to r)$$

ต้องพิสูจน์ว่าทั้ง 2 กรณีเป็นจริงคือ

กรณีที่ 1 $p \to r$

สมมติ	p	เป็นจริง
	$\vdots$	
ดังนั้น	r	เป็นจริง

กรณีที่ 2 $q \to r$

สมมติ	q	เป็นจริง
	$\vdots$	
ดังนั้น	r	เป็นจริง $\square$

เราเรียกว่า**การพิสูจน์โดยแจกแจงกรณี** (proof by cases)

ตัวอย่าง 1.3.4 จงพิสูจน์ว่า "ถ้า a เป็นจำนวนคู่ หรือ a เป็นจำนวนคี่ แล้ว $a^2 + a$ เป็นจำนวนคู่"

ตัวอย่าง 1.3.5 จงพิสูจน์ว่า ถ้า n เป็นจำนวนเต็ม แล้ว $n^2 + 3n + 4$ เป็นจำนวนคู่

ตัวอย่าง 1.3.6 ให้ a เป็นจำนวนเต็ม จงพิสูจน์ว่า ถ้า $a^2 + 1$ เป็นจำนวนคี่ แล้ว a เป็นจำนวนคู่

3. การพิสูจน์ข้อความแบบผันกลับได้

ในตัวอย่าง 1.3.2 ได้พิสูจน์ว่า "ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่" ในตัวอย่าง 1.3.2 เมื่อ n เป็นจำนวนคู่ จะนำไปสู่ข้อสรุป n^2 เป็นจำนวนคู่ เมื่อตั้งคำถามต่อไปว่าในทางกลับกัน ข้อความนี้จะเป็นจริงหรือไม่ นั่นคือต้องพิสูจน์ว่า "ถ้า n^2 เป็นจำนวนคู่ แล้ว n เป็นจำนวนคู่" ซึ่งได้พิสูจน์ไว้แล้วในตัวอย่าง 1.3.3 ทำให้ได้ว่าผลสามารถสรุปเหตุได้ด้วย อันหมายถึงการพิสูจน์ว่า

"n เป็นจำนวนคู่ **ก็ต่อเมื่อ** n^2 เป็นจำนวนคู่"

นั่นคือการพิสูจน์ในรูปแบบ $p \leftrightarrow q$ ซึ่งทำ 2 ขั้นตอนดังนี้

1. $p \to q$ เรียกว่าขั้น sufficient part (p เป็นเงื่อนไขที่เพียงพอสำหรับ q)
2. $q \to p$ เรียกว่าขั้น necessily part (p เป็นเงื่อนไขที่จำเป็นสำหรับ q)

เรียกว่า **การพิสูจน์ข้อความแบบผันกลับได้ (proof of biconditional statements)**

ตัวอย่าง 1.3.7 จงพิสูจน์ "จำนวนเต็ม a ใด ๆ a เป็นจำนวนคี่ ก็ต่อเมื่อ $a+3$ เป็นจำนวนคู่"

4. การพิสูจน์โดยวิธีขัดแย้ง

เมื่อพิสูจน์โดยวิธีต่าง ๆ ที่ผ่านมาแล้วไม่สามารถทำได้ สามารถทำได้อีกทางหนึ่งคือ เมื่อต้องการพิสูจน์ข้อความ p เป็นจริงโดยการสมมติว่า $\sim p$ เป็นจริง แล้วนำไปสู่ข้อความขัดแย้ง c การพิสูจน์แบบนี้ได้จากสัจนิรันดร์ $(\sim p \to c) \to p$ เรียกวิธีนี้ว่า **การพิสูจน์โดยวิธีขัดแย้ง** (proof by contradiction) มีโครงการพิสูจน์ดังนี้

สมมติ	$\sim p$ เป็นจริง	
	$\vdots$	
ดังนั้น	เกิดข้อขัดแย้ง	$\square$

ตัวอย่าง 1.3.8 จงพิสูจน์ข้อความ

"ไม่ว่า x จะเป็นจำนวนจริงใดก็ตามที่ไม่ใช่ศูนย์ จะได้ว่า $x^{-1} \neq 0$"

โดยวิธีขัดแย้ง

ตัวอย่าง 1.3.9 จงพิสูจน์ข้อความ "ถ้า x, y เป็นจำนวนเต็ม แล้ว $x^2 - 4y \neq 2$" โดยวิธีขัดแย้ง

5. การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว

การพิสูจน์ข้อความ $\exists! x \in \mathcal{U},\, p(x)$ อ่านว่า มี x ใน $\mathcal{U}$ เพียงตัวเดียวเท่านั้นที่สอดคล้อง $p(x)$ ข้อความนี้สมมูลกับ

$$(\exists x \in \mathcal{U},\, p(x)) \wedge (\forall x, y \in \mathcal{U},\, p(x) \wedge p(y) \to x = y)$$

ดังนั้นการพิสูจน์ $\exists! x \in \mathcal{U},\, p(x)$ แบ่งการพิสูจน์ออกเป็น 2 ส่วนคือ

1. **ขั้นที่ 1** มีอย่างน้อยหนึ่งตัว (existence)
   $\exists x \in \mathcal{U},\, p(x)$
2. **ขั้นที่ 2** มีเพียงตัวเดียว (uniqueness)
   $\forall x, y \in \mathcal{U},\, p(x) \wedge p(y) \to x = y$

เรียกการพิสูจน์แบบนี้ว่า **การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว** (uniqueness proofs)

ตัวอย่าง 1.3.10 จงพิสูจน์ว่า "มีจำนวนจริง x เพียงตัวเดียวเท่านั้นซึ่ง $2^x = 1$"

ตัวอย่าง 1.3.11 จงพิสูจน์ว่า "ทุก ๆ จำนวนจริง x จะมีจำนวนจริง y เพียงตัวเดียวซึ่ง $x + y = 1$"

6. การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์

ต่อไปจะกล่าวถึงการพิสูจน์ข้อความที่มีเอกภพสัมพัทธ์เป็นจำนวนนับในรูปแบบ

$$\forall n \in \mathbb{N},\, P(n)$$

เมื่อ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็ม การพิสูจน์ทำได้ 2 ขั้นตอนดังนี้

1. **ขั้นฐาน (Basic step)** : $P(1)$ เป็นจริง
2. **ขั้นอุปนัย (Inductive step)** : ถ้า $P(k)$ เป็นจริง แล้ว $P(k+1)$ เป็นจริง ทุก ๆ $k \in \mathbb{N}$

เรียกการพิสูจน์นี้ว่า **การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์ (proof by mathematical induction)**

ตัวอย่าง 1.3.12 จงแสดงว่า $1+2+3+4+\cdots+n = \dfrac{n(n+1)}{2}$ สำหรับทุกจำนวนนับ n

ตัวอย่าง 1.3.13 จงแสดงว่า $1+3+5+\cdots+(2n-1)=n^2$ สำหรับทุกจำนวนนับ n

ตัวอย่าง 1.3.14 จงแสดงว่า $\forall n \in \mathbb{N},\ 2^n < 2^{n+1}$

ต่อไปกล่าวถึงการพิสูจน์อุปนัยเชิงคณิตศาสตร์ที่ขั้นฐานเริ่มต้นที่ $n_0 \in \mathbb{Z}$ ข้อความในรูปแบบ

$$\forall n \in \mathbb{Z}, n \geq n_0,\ P(n)$$

เมื่อ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็ม ถ้า

1. **ขั้นฐาน** : $P(n_0)$ เป็นจริง
2. **ขั้นอุปนัย** : สำหรับจำนวนเต็ม k ซึ่ง $k \geq n_0$ ถ้า $P(k)$ เป็นจริง แล้ว $P(k+1)$ เป็นจริง

สรุปได้ว่า $\forall n \in \mathbb{Z},\ n \geq n_0,\ P(n)$ เป็นจริง หรือ $P(n)$ เป็นจริงสำหรับจำนวนนับ ซึ่ง $n \geq n_0$

ตัวอย่าง 1.3.15 จงหาจำนวนนับเริ่มต้นที่ทำให้ข้อความนี้เป็นจริงพร้อมทั้งพิสูจน์ $2^n \geq n^2$

ในกรณีข้อความเกี่ยวกับจำนวนนับไม่สามารถพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์ที่กล่าวมาข้างต้น อาจจะใช้รูปแบบการพิสูจน์ได้ดังต่อไปนี้ ให้ $P(n)$ แทนข้อความเกี่ยวกับจำนวนนับ ถ้า

1. **ขั้นฐาน** : $P(1)$ เป็นจริง
2. **ขั้นอุปนัย** : ถ้า $P(k)$ เป็นจริงสำหรับทุกจำนวนนับ k ที่ $k < m$ แล้ว $P(m)$ เป็นจริง

สรุปได้ว่า $\forall n \in \mathbb{N},\, P(n)$ เป็นจริง หรือ $P(n)$ เป็นจริงสำหรับทุกจำนวนนับ n

ตัวอย่าง 1.3.16 ลำดับลูคัส (Lucus sequence) นิยามโดย $a_1 = 1,\ a_2 = 3$ และ

$$a_n = a_{n-1} + a_{n-2} \qquad \text{สำหรับ } n = 3, 4, 5, ...$$

จงพิสูจน์ว่า $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับทุกจำนวนนับ n

แบบฝึกหัด 1.3

1. จงพิสูจน์ข้อความต่อไปนี้

   1.1 ถ้า x เป็นจำนวนคู่ แล้ว $3x$ เป็นจำนวนคู่

   1.2 ถ้า m และ n เป็นจำนวนคู่ แล้ว $3n + 5m$ เป็นจำนวนคู่

   1.3 ถ้า n เป็นจำนวนเต็ม แล้ว $7n^2 + n + 2$ เป็นจำนวนคู่

   1.4 ถ้า n เป็นจำนวนเต็ม แล้ว $n^2 + n + 1$ เป็นจำนวนคี่

   1.5 สำหรับจำนวนเต็ม a ใดๆ a เป็นจำนวนคู่ ก็ต่อเมื่อ $a^2 + 1$ เป็นจำนวนคี่

   1.6 สำหรับจำนวนเต็ม a ใด ๆ a เป็นจำนวนคี่ ก็ต่อเมื่อ $a^2 + 3$ เป็นจำนวนคู่

   1.7 $\sqrt{3}$ เป็นจำนวนอตรรกยะ

   1.8 ทุกๆจำนวนจริง x จะมีจำนวนจริง y เพียงตัวเดียวเท่านั้นซึ่ง $x + y = 5$

   1.9 ทุก ๆ จำนวนจริง x จะมีจำนวนจริง y เพียงตัวเดียวเท่านั้นซึ่ง $x + y = 0$

2. จงพิสูจน์ข้อความต่อไปนี้ โดยใช้หลักอุปนัยเชิงคณิตศาสตร์

   2.1 $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$ สำหรับทุกจำนวนนับ n

   2.2 $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$ สำหรับทุกจำนวนนับ n

   2.3 $2 + 4 + 6 + \cdots + (2n) = n^2 + n$ สำหรับทุกจำนวนนับ n

   2.4 $2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2$ สำหรับทุกจำนวนนับ n

   2.5 $1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + ... + n \cdot 2^n = (n-1)2^{n+1} + 2$ สำหรับทุกจำนวนนับ n

   2.6 $1 \cdot 3 + 2 \cdot 5 + 3 \cdot 7 + \cdots + (3n-2) \cdot (3n+1) = n(3n^2 + 3n - 2)$ สำหรับทุก ๆ $n \in \mathbb{N}$

   2.7 $1(1!) + 2(2!) + 3(3!) + \cdots + n(n!) = (n+1)! - 1$ สำหรับทุกจำนวนนับ n

   2.8 $\forall n \in \mathbb{N},\ 2^n > n$

   2.9 $\forall n \in \mathbb{N},\ 2^n \leq 2^{n+1} - 2^{n-1} - 1$

3. จงหาจำนวนนับเริ่มต้นที่ทำให้ข้อความนี้เป็นจริงพร้อมทั้งพิสูจน์

   3.1 $2^{n-1} \leq n!$

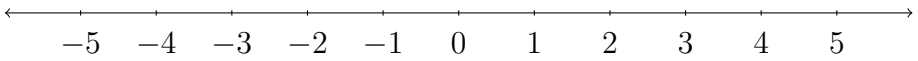
   3.2 $4^n > n^4$

   3.3 $(2n)! < 2^{2n}(n!)^2$

   3.4 $n^2 < (\frac{3}{2})^n$

1.4 สมบัติจำนวนเต็ม

ในหัวข้อนี้เราจะกล่าวถึงระบบจำนวนเต็ม และศึกษาสมบัติที่เกิดจากสัจพจน์ของจำนวนเต็ม เมื่อ $\mathbb{Z}$ แทนเซตจำนวนเต็ม ดังนั้น $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ และแสดงได้ดังแผนภาพ



รูปที่ 1 แผนภาพแสดงจำนวนเต็มบนเส้นจำนวน

สัจพจน์จำนวนเต็ม สมมติว่ามีเซต $\mathbb{Z}$ ซึ่งเรียกว่า **เซตของจำนวนเต็ม** และมีตัวดำเนินการ $+$ และ $\cdot$ ซึ่งเรียกว่า**การบวก (addition)** และ**การคูณ (multiplication)** ตามลำดับ โดยมีสมบัติดังนี้

(A1) **สมบัติปิด** (closer laws)
สำหรับการบวก : ทุก ๆ $x, y \in \mathbb{Z}$ จะได้ว่า $x + y \in \mathbb{Z}$
สำหรับการคูณ : ทุก ๆ $x, y \in \mathbb{Z}$ จะได้ว่า $x \cdot y \in \mathbb{Z}$

(A2) **สมบัติสลับที่** (commutative laws)
สำหรับการบวก : ทุก ๆ $x, y \in \mathbb{Z}$ จะได้ว่า $x + y = y + x$
สำหรับการคูณ : ทุก ๆ $x, y \in \mathbb{Z}$ จะได้ว่า $x \cdot y = y \cdot x$

(A3) **สมบัติการเปลี่ยนหมู่** (associative laws)
สำหรับการบวก : ทุก ๆ $x, y, z \in \mathbb{Z}$ จะได้ว่า $(x + y) + z = x + (y + z)$
สำหรับการคูณ : ทุก ๆ $x, y, z \in \mathbb{Z}$ จะได้ว่า $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(A4) **สมบัติการมีเอกลักษณ์** (existence of identities)
สำหรับการบวก : มี $0 \in \mathbb{Z}$ ซึ่ง $x + 0 = x = 0 + x$ ทุก ๆ $x \in \mathbb{Z}$
เรียก 0 ว่าเอกลักษณ์การบวก (additive identity)
สำหรับการคูณ : มี $1 \in \mathbb{Z}$ ซึ่ง $x \cdot 1 = x = 1 \cdot x$ ทุก ๆ $x \in \mathbb{Z}$
เรียก 1 ว่าเอกลักษณ์การคูณ (multiplicative identity)

(A5) **สมบัติการมีตัวผกผัน** (existence of inverse)
สำหรับการบวก : สำหรับ $x \in \mathbb{Z}$ จะมี $-x \in \mathbb{Z}$ ซึ่ง $x + (-x) = 0 = (-x) + x$
เรียก $-x$ ว่าตัวผกผันการบวกของ x

(A6) **สมบัติการแจกแจง** (distributive laws)
สำหรับ $x, y, z \in \mathbb{Z}$ จะได้ว่า

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{และ} \quad (y + z) \cdot x = y \cdot x + z \cdot x$$

นิยมเขียน xy แทน $x \cdot y$ และ $x - y$ แทน $x + (-y)$

ข้อสังเกต 1.4.1 จาก A5 จะเห็นว่า x เป็นตัวผกผันการบวกของ $-x$ ดังนั้น $x = -(-x)$

ทฤษฎีบท 1.4.2 ให้ a, b, c เป็นจำนวนเต็ม แล้ว

1. $a0 = 0 = 0a$
2. $(-a)b = a(-b) = -(ab)$
3. $(-a)(-b) = ab$
4. ถ้า $a + b = a + c$ แล้ว $b = c$

ทฤษฎีบท 1.4.3 ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. $(-1)a = a(-1) = -a$
2. $-(a+b) = -a - b$
3. $a(b-c) = ab - ac$

(A7) **กฎไตรวิภาค (Trichotomy Law)**
มีสับเซต $\mathbb{N}$ ของ $\mathbb{Z}$ คือ $\mathbb{N} = \{1, 2, 3, ...\}$ ที่มีสมบัติ

1. $0 \notin \mathbb{N}$
2. ถ้า $a, b \in \mathbb{N}$ แล้ว $a + b \in \mathbb{N}$ และ $ab \in \mathbb{N}$
3. ถ้า $x \in \mathbb{Z}$ แล้ว $x \in \mathbb{N}$ หรือ $x = 0$ หรือ $-x \in \mathbb{N}$

บทนิยาม 1.4.4 ให้ $a, b \in \mathbb{Z}$ เราจะกล่าวว่า

a **มากกว่า (greater than)** b เขียนแทนด้วย $a > b$ ก็ต่อเมื่อ $a - b \in \mathbb{N}$

a **น้อยกว่า (less than)** b เขียนแทนด้วย $a < b$ ก็ต่อเมื่อ $b > a$

ทฤษฎีบท 1.4.5 ให้ $a, b, c, y \in \mathbb{Z}$ แล้ว

1. ถ้า $a > b$ แล้ว $a + c > b + c$
2. ถ้า $a > b$ และ $b > c$ แล้ว $a > c$

ทฤษฎีบท 1.4.6 ให้ $a, b, c, x, y \in \mathbb{Z}$ แล้ว

1. ถ้า $a > b$ และ $x > y$ แล้ว $a + x > b + y$
2. ถ้า $a > b$ และ $x > 0$ แล้ว $ax > bx$
3. ถ้า $a > b$ และ $x < 0$ แล้ว $ax < bx$

ทฤษฎีบท 1.4.7 สำหรับจำนวนเต็ม a, b ใด ๆ ถ้า $ab = 0$ แล้ว $a = 0$ หรือ $b = 0$

บทแทรก 1.4.8 สำหรับจำนวนเต็ม a, b, c ใด ๆ ถ้า $ab = ac$ และ $a \neq 0$ แล้ว $b = c$

(A8) **หลักการจัดอันดับดี** (Well Ordering Principle)
ให้ $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ จะได้ว่า S มีสมาชิกตัวเล็กสุด หรือ มี $m \in S$ ซึ่ง $m \leq s$ ทุก ๆ $s \in S$

ทฤษฎีบท 1.4.9 หลักการของอาร์คีมีดีส (Archimedean Principle)
สำหรับจำนวนเต็มบวก a และ b ใด ๆ จะมีจำนวนเต็มบวก n ซึ่ง $na \geq b$

แบบฝึกหัด 1.4

1. ให้ $a, b, c, d \in \mathbb{Z}$ จงพิสูจน์ว่า

   1.1 $(a-b)+(c-d) = (a+c)-(b+d)$

   1.2 $(a-b)-(c-d) = (a+d)-(b+c)$

   1.3 $(a-b)(c-d) = (ac+bd)-(ad+bc)$

   1.4 $a-b = c-d$ ก็ต่อเมื่อ $a+d = b+c$

   1.5 $(a-b)c = ac-bc$

2. ให้ $a, b, c, x, y \in \mathbb{Z}$ จงพิสูจน์ว่า

   2.1 $a < b$ ก็ต่อเมื่อ $a+c < b+c$

   2.2 $a-x < a-y$ ก็ต่อเมื่อ $x > y$

   2.3 ถ้า $a < 0$ แล้ว $ax > ay$ ก็ต่อเมื่อ $x < y$

   2.4 ถ้า $c > 0$ และ $ac < bc$ แล้ว $a < b$

   2.5 $a-b = c-d$ ก็ต่อเมื่อ $a+d = b+c$

   2.6 ถ้า $x+x = 0$ แล้ว $x = 0$

   2.7 ถ้า $a^3 < b^3$ แล้ว $a < b$

3. จงพิสูจน์ว่า $a^3 = b^3$ แล้ว $a = b$

4. จงพิสูจน์ว่า $a^2 - ab + b^2 > 0$ เมื่อ $a, b \in \mathbb{Z}$

บทที่ 2

การหารลงตัว

2.1 ขั้นตอนวิธีการหาร

ทฤษฎีบท 2.1.1 ขั้นตอนวิธีการหาร (The Division Algorithm)
ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ แล้วมีจำนวนเต็ม q และ r เพียงคู่เดียวที่ทำให้

$$b = aq + r \qquad \text{โดยที่} \qquad 0 \leq r < |a| \qquad (*)$$

เรียก q ว่า**ผลหาร (quotient)** และ r ว่า**เศษเหลือ (remainder)**

ตัวอย่าง 2.1.2 จงเขียนการหารต่อไปนี้โดยใช้ขั้นตอนการหาร

1. 11 หาร 111
2. 9 หาร -108
3. -12 หาร 1205
4. -5 หาร -183

ข้อสังเกต 2.1.3 ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ จากขั้นตอนวิธีการหารอาจนิยามเศษ r เป็นจำนวนเต็มลบได้ โดยที่ q และ r จะขาดสมบัติความเป็นหนึ่งเดียว กล่าวคือ

$$b = aq + r \qquad \text{โดยที่} \qquad 0 \leq |r| < |a|$$

เช่น 3 หาร 2 ได้เศษเท่ากับ 2 หรือ -1 โดยการพิจารณารูปได้ 2 กรณีดังนั้น

$$2 = 3(0) + 2 \qquad \text{และ} \qquad 2 = 3(1) - 1$$

ตัวอย่าง 2.1.4 จงเขียนรูปแบบทั้งหมดของจำนวนเต็ม a เมื่อกำหนดให้

1. 2 หาร a
2. 3 หาร a
3. 4 หาร a
4. 5 หาร a

ตัวอย่าง 2.1.5 จงแสดงว่า**กำลังสอง**ของจำนวนเต็มใด ๆ จะอยู่ในรูป

$$3k \qquad \text{หรือ} \qquad 3k + 1$$

สำหรับบางจำนวนเต็ม k

ตัวอย่าง 2.1.6 จงแสดงว่า**กำลังสาม**ของจำนวนเต็มใด ๆ จะอยู่ในรูป

$$9k \quad \text{หรือ} \quad 9k+1 \quad \text{หรือ} \quad 9k+8$$

สำหรับบางจำนวนเต็ม k

ตัวอย่าง 2.1.7 จงหาจำนวนนับตั้งแต่ 1 ถึง 200 ทั้งหมดที่หารด้วย 6 เศษเหลือคือ 2 และเมื่อหารด้วย 14 เศษเหลือคือ 10

ทฤษฎีบท 2.1.8 ให้ a, b และ c เป็นจำนวนเต็มโดยที่ $a \neq 0$ ถ้า

$$\begin{array}{lllll} a & \text{หาร} & b & \text{เศษเหลือเท่ากับ} & r \\ a & \text{หาร} & c & \text{เศษเหลือเท่ากับ} & s \end{array}$$

แล้ว

(ก) เศษเหลือจากการหาร $b+c$ ด้วย a เท่ากับเศษเหลือที่ได้จากการหาร $r+s$ ด้วย a

(ข) เศษเหลือจากการหาร bc ด้วย a เท่ากับเศษเหลือที่ได้จากการหาร rs ด้วย a

ตัวอย่าง 2.1.9 ให้ m และ n เป็นจำนวนเต็มบวก ถ้า

$$\begin{array}{lllll} 5 & \text{หาร} & m & \text{เศษเหลือเท่ากับ} & 4 \\ 5 & \text{หาร} & n & \text{เศษเหลือเท่ากับ} & 2 \end{array}$$

แล้ว 5 หารจำนวนต่อไปนี้ เศษเหลือเท่าใด

1. $m+n$
2. mn
3. m^2
4. $m(n+2)$
5. $n^2(n+m)$
6. $5m+3n$
7. $m-n$
8. $n-m$

ทฤษฎีบท 2.1.10 ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ และ n เป็นจำนวนนับ ถ้า a หาร b เศษเหลือเท่ากับ r แล้ว

เศษเหลือจากการหาร b^n ด้วย a เท่ากับเศษเหลือที่ได้จากการหาร r^n ด้วย a

ตัวอย่าง 2.1.11 จงหาเศษเหลือที่เกิดจากการหารต่อไปนี้

1. 2 หาร 5^{100}
2. 2 หาร $3^{1999} + 5^{2000}$
3. 3 หาร $2^{999} \cdot 5^{898}$
4. 7 หาร 100^{2558}

ตัวอย่าง 2.1.12 จงหาเศษเหลือที่เกิดจากการหารต่อไปนี้

1. 31 หาร 2^{2018}
2. 13 หาร 444^{444}

ต่อไปนี้เป็นการประยุกต์การหาเศษเหลือ เพื่อจะใช้ในการหาหลักหน่วย (เลขท้าย) และหลักสิบของเลขยกกำลัง เมื่อพิจารณา 1,025 ด้วย 10 เศษเหลือเท่ากับ 5 สังเกตเห็นว่าเศษเหลือที่ได้จากการหารจำนวนเต็มด้วย 10 จะได้ตรงกับหลักหน่วยของจำนวนนั้นเสมอ ทำนองเดียวกันเมื่อหาร 1,025 ด้วย 100 จะได้เศษเหลือเท่ากับ 25 ซึ่งเท่ากับสองหลักสุดท้ายของจำนวนนั้น โดยอาศัยหลักการดังกล่าวจึงสรุปได้ว่า

1. หลักหน่วย (เลขท้าย) ของจำนวนเต็มบวก a คือเศษเหลือจากการหาร a ด้วย 10
2. สองหลักสุดท้าย ของจำนวนเต็มบวก a คือเศษเหลือจากการหาร a ด้วย 100

ตัวอย่าง 2.1.13 จงหาหลักหน่วยของจำนวนต่อไปนี้

1. 2^{1000}
2. 3^{1999}
3. 6^{666}
4. 7^{888}
5. $55^{555} + 44^{444}$
6. $(3^{100} + 5^{100})^{100}$

ตัวอย่าง 2.1.14 จงหาสองหลักสุดท้ายของจำนวนต่อไปนี้

1. 7^{2558}

2. 2^{100}

3. 3^{100}

4. 6^{666}

แบบฝึกหัด 2.1

1. มีจำนวนนับตั้งแต่ 1 ถึง 100 รวมทั้งหมดกี่จำนวนซึ่งเมื่อหารด้วย 6 เศษเหลือคือ 2 และหารด้วย 14 เศษเหลือคือ 1

2. จงแสดงว่ากำลังสี่ของจำนวนเต็มใด ๆ จะอยู่ในรูป $5k$ หรือ $5k+1$ สำหรับบางจำนวนเต็ม k

3. ให้ a, b และ c เป็นจำนวนเต็มบวก ถ้า

$$\begin{array}{lllll} 9 & \text{หาร} & a & \text{เศษเหลือเท่ากับ} & 3 \\ 9 & \text{หาร} & b & \text{เศษเหลือเท่ากับ} & 5 \\ 9 & \text{หาร} & c & \text{เศษเหลือเท่ากับ} & 7 \end{array}$$

แล้ว 9 หารจำนวนต่อไปนี้ เศษเหลือเท่าใด

3.1 $a+b+c$ 3.3 abc 3.5 $2a+5(b+c)$ 3.7 $(a+b-c)^3$

3.2 $a(b+c)$ 3.4 $3a^2+2b^2$ 3.6 $ab+ac$ 3.8 $5a+b+3c$

4. จงหาเศษเหลือที่เกิดจากการหาร

4.1 2 หาร 2549^{2013} 4.3 2 หาร $3^{2548}+5^{1001}$ 4.5 7 หาร 344^{44344}

4.2 3 หาร 5^{555} 4.4 3 หาร 728^{9855} 4.6 11 หาร 999^{999}

5. จงหาหลักหน่วยของจำนวนต่อไปนี้

5.1 2^{2013} 5.3 $3^{2548}+5^{1001}$ 5.5 8888^{7777}

5.2 2549^{2013} 5.4 113^{2002} 5.6 12345678^{98765}

6. จงหาสองหลักสุดท้ายของจำนวนต่อไปนี้

6.1 2^{55} 6.2 3^{500} 6.3 66^{66}

2.2 การหารลงตัว

การหารจำนวนเต็มด้วยจำนวนเต็มที่ไม่ใช่ศูนย์ ในกรณีที่เศษเหลือมีค่าเท่ากับศูนย์จะเรียกว่า **การหารลงตัว** (divisibility) เขียนเป็นนิยามได้ดังต่อไปนี้

บทนิยาม 2.2.1 ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ จะกล่าวว่า a **หาร** b **ลงตัว** แทนด้วยสัญลักษณ์ $a \mid b$ นิยามโดย

$$a \mid b \quad \text{ก็ต่อเมื่อ} \quad \text{มีจำนวนเต็ม} \quad c \quad \text{ที่ทำให้} \quad b = ac$$

เรียก a ว่า**ตัวหาร** (divisor) หรือ **ตัวประกอบ** (factor) ของ b หรือเรียก b ว่าเป็น**พหุคูณ** (multiple) ของ a ถ้า a **หาร** b **ไม่ลงตัว** เขียนแทนด้วย $a \nmid b$

ข้อสังเกต 2.2.2 สำหรับจำนวนเต็ม a ใด ๆ

1. $1 \mid a$
2. $a \mid 0$ เมื่อ $a \neq 0$
3. $a \mid a$ เมื่อ $a \neq 0$

เนื่องจาก $a = 1(a)$, $0 = 0(a)$ และ $a = 1(a)$

ตัวอย่าง 2.2.3 จงให้เหตุผลเกี่ยวกับการหารต่อไปนี้ตามนิยามการหารลงตัว

1. $13 \mid 182$ เพราะว่า
2. $-5 \mid 30$ เพราะว่า
3. $15 \mid (-225)$ เพราะว่า
4. $-12 \mid (-108)$ เพราะว่า
5. $7 \nmid 17$ เพราะว่า

ตัวอย่าง 2.2.4 จงหาจำนวนเต็มบวก a ทั้งหมดที่สอดคล้องเงื่อนไข

1. $a \mid 10$
2. $(a-1) \mid 48$
3. $a \mid 75$ และ $a \mid 125$
4. $6 \mid a$ และ $8 \mid a$

ตัวอย่าง 2.2.5 จงแสดงว่าไม่มีจำนวนเต็ม a ใด ๆ ซึ่ง $2 \mid a$ และ $2 \mid (a+1)$

ตัวอย่าง 2.2.6 สำหรับจำนวนเต็ม a, p และ q ใด ๆ จงแสดงว่า

$$\text{ถ้า} \quad a \mid (2p-3q) \quad \text{และ} \quad a \mid (4p-5q) \quad \text{แล้ว} \quad a \mid q$$

ตัวอย่าง 2.2.7 สำหรับจำนวนเต็ม k ใด ๆ ซึ่ง

$$d \mid (24k+29) \quad \text{และ} \quad d \mid (3k+2)$$

จงหาจำนวนเต็มบวก d ซึ่งมากกว่า 1

ตัวอย่าง 2.2.8 ถ้า d เป็นจำนวนเต็มบวกที่มากกว่า 1 และจำนวน $3456, 2561$ และ 1308 หารด้วย d มีเศษเหลือเท่ากันคือ r แล้ว $d + r$ เท่ากับเท่าใด

โดยขั้นตอนวิธีการหาร ทำให้สามารถจำแนกจำนวนเต็มออกเป็นกลุ่ม ๆ ตามเศษเหลือที่ได้จากการหารด้วยจำนวนเต็มที่ไม่ใช่ศูนย์ a ตัวอย่างเช่น $a = 2$ เศษเหลือที่ได้จากการหารจำนวนเต็ม a ด้วย 2 มีสองแบบคือ $r = 0$ และ $r = 1$ ดังนั้นจำนวนเต็มใด ๆ จะอยู่ในรูป $2q$ เรียกว่า**จำนวนคู่** และ $2q + 1$ เรียกว่า**จำนวนคี่** สำหรับบางจำนวนเต็ม q เมื่อ $a = 3$ เศษเหลือที่ได้จากการหารจำนวนเต็มด้วย 3 มีสองแบบคือ $r = 0$, $r = 1$ และ $r = 2$ ทำให้ได้ว่าจำนวนเต็มใด ๆ จะอยู่ในรูป $3q$, $3q + 1$ และ $3q + 2$ สำหรับบางจำนวนเต็ม q

กล่าวได้ว่าขั้นตอนวิธีการหารมีประโยชน์ในการพิสูจน์หรือแก้ปัญหาในระบบจำนวนเต็มโดยแบ่งกรณีตามเศษเหลือที่ได้จากการหารด้วย a ได้ a กรณี นั่นคือจำนวนเต็มใด ๆ จะอยู่ในรูปดั้งนี้

$$aq, aq + 1, aq + 2, ..., aq + (a - 1)$$

เมื่อเลือก a ที่เหมาะสมกับปัญหาที่สนใจจะทำให้แก้ปัญหาได้สะดวกยิ่งขึ้น

ตัวอย่าง 2.2.9 จงแสดงว่า $2 \mid (a^2 + a)$ เมื่อ a เป็นจำนวนเต็ม

ตัวอย่าง 2.2.10 จงแสดงว่า $3 \mid (a^3 - a)$ เมื่อ a เป็นจำนวนเต็ม

ตัวอย่าง 2.2.11 จงแสดงว่า $3 \mid a(a^2 + 2)$ เมื่อ a เป็นจำนวนเต็ม

ตัวอย่าง 2.2.12 จงแสดงว่า $8 \mid (a^2 - 1)$ เมื่อ a เป็นจำนวนเต็มคี่

ตัวอย่าง 2.2.13 จงแสดงว่า $16 \mid (n^4 + 4n^2 + 11)$ เมื่อ n เป็นจำนวนเต็มคี่

ต่อไปจะกล่าวถึงสมบัติต่าง ๆ ของการหารลงตัว ซึ่งผลที่ได้จะนำไปใช้พิสูจน์ทฤษฎีบทต่าง ๆ และแก้ปัญหาเกี่ยวกับจำนวนเต็มในบทต่อ ๆ ไป

ทฤษฎีบท 2.2.14 ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$
2. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = \pm b$
3. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$

ทฤษฎีบท 2.2.15 ให้ a, b, c และ d เป็นจำนวนเต็ม แล้ว

1. ถ้า $a \mid b$ และ $c \mid d$ แล้ว $ac \mid bd$
2. ถ้า $a \mid b$ แล้ว $a^n \mid b^n$ ทุก ๆ จำนวนนับ n

ทฤษฎีบท 2.2.16 ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. ถ้า $a \mid b$ แล้ว $a \mid bx$ ทุก ๆ จำนวนเต็ม x
2. ถ้า $a \mid b$ แล้ว $a \mid b^n$ ทุก ๆ จำนวนนับ n

ทฤษฎีบท 2.2.17 ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (b + c)$
2. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid bc$
3. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bx + cy)$ ทุก ๆ จำนวนเต็ม x และ y

ตัวอย่าง 2.2.18 ให้ a, b และ c เป็นจำนวนเต็ม จงพิจารณาข้อความต่อไปนี้ ถ้าเป็นจริงจงพิสูจน์ ถ้าเป็นเท็จจงยกตัวอย่างค้าน

1. ถ้า $a \mid (b+c)$ แล้ว $a \mid b$ หรือ $a \mid c$

2. ถ้า $a \mid bc$ แล้ว $a \mid b$ หรือ $a \mid c$

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

4. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a^2 \mid bc$

5. ถ้า $a \mid b^2$ แล้ว $a \mid b$

ทฤษฎีบท 2.2.19 ให้ a, b และ c เป็นจำนวนเต็ม

$$\text{ถ้า} \quad a \mid (b+c) \quad \text{และ} \quad a \mid b \quad \text{แล้ว} \quad a \mid c$$

บทแทรก 2.2.20 ให้ a, c และ k เป็นจำนวนเต็ม ถ้า $a \mid (ak+c)$ แล้ว $a \mid c$

ตัวอย่าง 2.2.21 จงหาจำนวนเต็มบวก a ทั้งหมดที่สอดคล้องเงื่อนไข โดยใช้บทแทรก 2.2.20

1. $a \mid (a+10)$
2. $a \mid (a^2-a+20)$
3. $a \mid (10-a)(10+a)$
4. $a^2 \mid ((a^2+3)^2+7)$

ตัวอย่าง 2.2.22 จงหาจำนวนเต็มบวก a ทั้งหมดที่สอดคล้องเงื่อนไข โดยใช้บทแทรก 2.2.20

1. $a \mid (a+2)^2$

2. $(a+1) \mid (a^2+1)$

3. $(a-1) \mid (a+1)^3$

4. $(a-3) \mid (a^3-3)$

ตัวอย่าง 2.2.23 ให้ $abcd$ เป็นเลขฐานสิบสี่หลัก จงแสดงว่า

$$9 \mid abcd \text{ ก็ต่อเมื่อ } 9 \mid (a+b+c+d)$$

จากตัวอย่าง 2.2.23 ทำให้ขยายแนวคิดเพื่อตรวจสอบการหารลงตัวของจำนวนในระบบฐานสิบได้ดังนี้ (พิสูจน์จะเว้นไว้เป็นแบบฝึกหัด) ให้ $a_1, a_2, ..., a_n \in \{0, 1, 2, ..., 9\}$ (เลขโดด) และ $a_1a_2...a_n$ เป็นเลขฐานสิบ n หลัก โดยที่ $a_1 \neq 0$

1. $2 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $2 \mid a_n$
2. $3 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $3 \mid (a_1 + a_2 + ... + a_n)$
3. $4 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $4 \mid a_{n-1}a_n$
4. $5 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $5 \mid a_n$
5. $6 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $3 \mid (a_1 + a_2 + ... + a_n)$ และ $2 \mid a_n$
6. $7 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $7 \mid (a_1a_2...a_{n-1} - 2a_n)$
7. $8 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $8 \mid a_{n-2}a_{n-1}a_n$
8. $9 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $9 \mid (a_1 + a_2 + ... + a_n)$
9. $10 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $10 \mid a_n$
10. $11 \mid a_1a_2...a_n$ ก็ต่อเมื่อ $11 \mid (a_n - a_{n-1} + a_{n-2} - a_{n-3} + ... \pm a_1)$

ตัวอย่าง 2.2.24 จงตรวจสอบการหารลงตัวของจำนวนต่อไปนี้

1. จำนวนต่อไปนี้หารด้วย 3 ลงตัว หรือไม่

   1.1 $1,236$

   1.2 $22,481$

   1.3 $7,773,339$

2. จำนวนต่อไปนี้หารด้วย 4 ลงตัว หรือไม่

   2.1 $1,236$

   2.2 $57,230$

   2.3 $88,032,332$

3. จำนวนต่อไปนี้หารด้วย 8 ลงตัว หรือไม่

   3.1 $9,248$

   3.2 $21,482$

4. จำนวนต่อไปนี้หารด้วย 9 ลงตัว หรือไม่

   4.1 $1,233$

   4.2 $31,482$

   4.3 $210,135$

5. จำนวนต่อไปนี้หารด้วย 11 ลงตัว หรือไม่

   5.1 $1,034$

   5.2 $100,236$

   5.3 $2,347,896,701$

ตัวอย่าง 2.2.25 กำหนดให้ $a, b \in \{0, 1, 2, ..., 9\}$ และ $1a5$, $6b9$ เป็นจำนวนสามหลัก ถ้า $6b9 - 1a5 = 454$ และ $6b9$ หารด้วย 9 ลงตัว แล้ว $a + b$ เท่ากับเท่าใด

ตัวอย่าง 2.2.26 ถ้า a, b, c และ d เป็นเลขโดดที่แตกต่างกันที่ทำให้จำนวนเต็ม 4 หลัก $dcba$ เท่ากับ 9 เท่าของ $abcd$ แล้ว b มีค่าเท่ากับเท่าใด

ตัวอย่าง 2.2.27 มีเลขโดด $3, 4, 6$ และ 7 นำมาจัดเรียงสร้างจำนวน 4 หลักโดยที่แต่ละหลักไม่ซ้ำกันจะมีจำนวน 4 หลักทั้งหมดกี่จำนวนที่หารด้วย 44 ลงตัว

สำหรับเงื่อนไขในหลักของจำนวนเต็มบวกหารด้วย 7 ลงตัว

$$7 \mid a_1a_2...a_n \qquad \text{ก็ต่อเมื่อ} \qquad 7 \mid (a_1a_2...a_{n-1} - 2a_n)$$

ตัวอย่างเช่น 7 หาร 142365

ทฤษฎีบท 2.2.28 (ธนัชยศ จำปาหวาย. 2564.)
เงื่อนไขในหลักของจำนวนเต็มบวกที่หารด้วย 7 ลงตัว คือผลบวกของผลคูณระหว่างเลขโดดในหลักหน่วย หลักสิบ หลักร้อย หลักพัน หลักหมื่น หลักแสน หลักล้าน หลักสิบล้าน หลักร้อยล้าน หลักพันล้าน หลักหมื่นล้าน หลักแสนล้าน ... ของจำนวนนั้นกับ 1,3,2,-1,-3,-2,1,3,2,-1,-3,-2,... ตามลำดับจนครบทุกหลัก ต้องหารด้วย 7 ลงตัว

ตัวอย่าง 2.2.29 จงตรวจสอบจำนวนเต็มต่อไปนี้ว่าหาร 7 ลงตัวหรือไม่

1. 142365
2. 23674112
3. 1122330014
4. 6498142571

ตัวอย่าง 2.2.30 จงหาจำนวนเต็มสามหลัก aba ทั้งหมดที่หารด้วย 7 ลงตัว

แบบฝึกหัด 2.2

1. จงพิสูจน์ข้อความต่อไปนี้ โดยใช้ขั้นตอนวิธีการหาร

   1.1 $3 \mid a(2a^2+7)$ สำหรับจำนวนเต็ม a

   1.2 $3 \mid a(a^2+2)$ เมื่อ a เป็นจำนวนเต็ม

   1.3 $4 \mid (n^2-1)$ สำหรับจำนวนเต็มคี่ n

   1.4 $6 \mid n(n+1)(n+2)$ สำหรับจำนวนเต็ม n

   1.5 $6 \mid n(n+1)(2n+1)$ สำหรับจำนวนเต็ม n

   1.6 $32 \mid (a^2+3)(a^2+7)$ สำหรับจำนวนเต็มคี่ a

   1.7 $30 \mid (n^5-n)$ สำหรับจำนวนเต็ม n

2. กำหนดให้ a, b, c, d เป็นจำนวนเต็ม จงพิจารณาข้อความต่อไปนี้ ถ้าเป็นจริงจงพิสูจน์ ถ้าเป็นเท็จจงยกตัวอย่างค้าน

   2.1 ถ้า $a \mid b^2$ แล้ว $a \mid b$

   2.2 ถ้า $a^2 \mid b^3$ แล้ว $a \mid b$

   2.3 ถ้า $a \mid b$ แล้ว $ac \mid bc$ เมื่อ $c \neq 0$

   2.4 ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a^2 \mid bc$

   2.5 ถ้า $a \mid b$ และ $c \mid d$ แล้ว $(a+c) \mid (b+d)$

   2.6 ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (b^2-c^2)$

3. จงหาจำนวนเต็มบวก a ทั้งหมดที่สอดคล้องเงื่อนไขต่อไปนี้

   3.1 $a \mid 625^2$ 3.3 $a \mid (a+6)^2$ 3.5 $(a-1) \mid (a+1)^3$

   3.2 $(a-1) \mid (2a+11)$ 3.4 $(2a+1) \mid (2a-1)^3$ 3.6 $(a-3) \mid (a^3-3)$

4. กำหนดให้ $a, b \in \{0, 1, 2, ..., 9\}$ จงหาคู่อันดับ (a, b) ทั้งหมดที่สอดคล้องเงื่อนไขต่อไปนี้

   4.1 $2 \mid a23b$ 4.5 $6 \mid 999a7b$ 4.9 $9 \mid 369a785b$

   4.2 $3 \mid 1a23b1$ 4.6 $7 \mid a27635b$ 4.10 $9 \mid ab125481$

   4.3 $3 \mid a791b112$ 4.7 $8 \mid 45ab32ab$ 4.11 $11 \mid 1a23571b$

   4.4 $4 \mid 45a13ab$ 4.8 $9 \mid 1234a5b6$ 4.12 $11 \mid a4557798b$

5. จงหาจำนวนเต็มสี่หลัก $abba$ ทั้งหมดที่หารด้วย 7 ลงตัว

6. จำนวนเต็มบวก n ที่มีค่าน้อยสุดซึ่งทำให้ $45 \mid (n \cdot 2^{2547} + 7^{2547})$ มีค่าเท่าใด

7. กำหนดให้ x และ y เป็นจำนวนนับ แล้ว $xy - 2547x - 2004y = 0$ มีกี่คำตอบ

2.3 การพิสูจน์การหารลงตัวโดยใช้หลักอุปนัยเชิงคณิตศาสตร์

เมื่อต้องการพิสูจน์ข้อความ $3 \mid (5^n - 2^n)$ สำหรับ $n \in \mathbb{N}$ จะเห็นได้ว่า $5^n - 2^n$ อยู่ในรูปเลขยกกำลัง ถ้าจะใช้ขั้นตอนวิธีการหารแบ่ง n ออกเป็นกรณีตามเศษเหลือจะไม่สามารถพิสูจน์ข้อความนี้ได้ อีกทางหนึ่งที่ทำได้คือใช้หลักอุปนัยเชิงคณิตศาสตร์พิสูจน์ข้อความดังกล่าวได้ ซึ่งทำได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.3.1 จงแสดงว่า $3 \mid (5^n - 2^n)$ เมื่อ n เป็นจำนวนเต็มบวก

ตัวอย่าง 2.3.2 จงแสดงว่า $5 \mid (3^{3n+1} + 2^{n+1})$ เมื่อ n เป็นจำนวนเต็มบวก

ตัวอย่าง 2.3.3 จงแสดงว่า $8 \mid (5^{2n} + 7)$ เมื่อ n เป็นจำนวนเต็มบวก

ตัวอย่าง 2.3.4 จงแสดงว่า $(3!)^n \mid (3n)!$ สำหรับจำนวนนับ n

แบบฝึกหัด 2.3

จงพิสูจน์ข้อความต่อไปนี้ โดยใช้หลักอุปนัยเชิงคณิตศาสตร์

1. $12 \mid (n^4 - n^2)$ สำหรับจำนวนนับ n
2. $5 \mid (n^5 - n)$ สำหรับจำนวนนับ n
3. $3 \mid (5^n - 2^n)$ เมื่อ n เป็นจำนวนเต็มบวก
4. $5 \mid (3^{3n+1} + 2^{n+1})$ เมื่อ n เป็นจำนวนเต็มบวก
5. $8 \mid (5^{2n} + 7)$ เมื่อ n เป็นจำนวนเต็มบวก
6. $5 \mid (2^{2n-1} + 3^{2n-1})$ สำหรับจำนวนนับ n
7. $7 \mid (3^{2n+1} + 2^{n+2})$ สำหรับจำนวนนับ n
8. $7 \mid (2^{3n} + 6)$ สำหรับจำนวนนับ n
9. $8 \mid (7 \cdot 3^{2n} - 7)$ สำหรับจำนวนนับ n
10. $11 \mid (8 \cdot 10^{2n} + 6 \cdot 10^{2n-1} + 9)$ สำหรับ $n \in \mathbb{N}$
11. $15 \mid (2^{4n} - 1)$ สำหรับจำนวนนับ n
12. $21 \mid (4^{n+1} + 5^{2n-1})$ สำหรับจำนวนนับ n

บทที่ 3

ตัวหารร่วมมาก

แม้เรื่องตัวหารร่วมมาก (ห.ร.ม.) และตัวคูณร่วมน้อย (ค.ร.น.) เป็นเรื่องที่มีการเรียนมาตั้งแต่ระดับชั้นประถมศึกษา อีกทั้งยังมีโจทย์ประยุกต์มากมายที่หลายคนคงได้พบ แต่ในบทนี้จะศึกษาในแง่บทนิยามและทฤษฎีบทที่สำคัญ ซึ่งจะนำไปประยุกต์ใช้ในการแก้ปัญหาเกี่ยวกับจำนวนเต็ม อันเป็นพื้นฐานในการศึกษาคณิตศาสตร์ในระดับสูงต่อไป

3.1 ตัวหารร่วมมาก

บทนิยาม 3.1.1 ให้ a, b และ d เป็นจำนวนเต็ม

d เป็น**ตัวหารร่วม (common divisor)** ของ a และ b ถ้า $d \mid a$ และ $d \mid b$

ข้อสังเกต 3.1.2 ให้ A แทนเซตของตัวหารของ a และ B แทนเซตของตัวหารของ b แล้ว

$A \cap B$ คือเซตของตัวหารร่วมของ a และ b

1. เนื่องจาก $1 \mid a$ และ $1 \mid b$ ดังนั้น $A \cap B \neq \varnothing$
2. ถ้า $a = 0$ แล้ว A เป็นเซตอนันต์ เพราะจำนวนเต็มที่ไม่ใช่ศูนย์ทุกจำนวนเป็นตัวหารของ 0
3. ถ้า $a = b = 0$ แล้ว $A \cap B$ เป็นเซตอนันต์ เหตุผลเดียวกับข้อ 2
4. ถ้า $a \neq 0$ และ $b \neq 0$ แล้ว $A \cap B$ เป็นเซตจำกัด
5. A เป็นเซตของตัวหารของ $-a$ ทำนองเดียวกัน B เป็นเซตของตัวหารของ $-b$

ตัวอย่าง 3.1.3 จงหาเซตของตัวร่วมของสองจำนวนต่อไปนี้

1. 125 และ -215
2. 252 และ 225

สำหรับจำนวนเต็ม a และ b ที่ไม่เป็นศูนย์พร้อมกัน จะได้ว่าเซตของตัวหารร่วมเป็นเซตจำกัด ทำให้สามารถหาสมาชิกตัวมากสุดได้ ซึ่งจะเรียกว่าตัวหารร่วมมากของ a และ b ดังนิยามดังนี้

บทนิยาม 3.1.4 ให้ a และ b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์พร้อมกัน จำนวนเต็ม d เป็น**ตัวหารร่วมมาก (greatest common divisior)** หรือ **ห.ร.ม. (g.c.d.)** ของ a และ b เขียนแทนด้วย $\gcd(a,b)$ ก็ต่อเมื่อ

(ก) $d \mid a$ และ $d \mid b$

(ข) ทุกจำนวนเต็ม c ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \leq d$

บทนิยาม 3.1.5 จำนวนเต็ม a และ b เป็น**จำนวนเฉพาะสัมพัทธ์ (relatively prime)** ถ้า $\gcd(a,b) = 1$

ข้อสังเกต 3.1.6 a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกัน จะได้ว่า

1. $\gcd(a,b) > 0$
2. $\gcd(a,b) = \gcd(b,a) = \gcd(|a|,|b|) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b)$
3. ถ้า $a \neq 0$ แล้ว $\gcd(a,0) = |a|$
4. ถ้า $a \mid b$ แล้ว $\gcd(a,b) = |a|$

ตัวอย่าง 3.1.7 จงหาตัวหารร่วมมากของจำนวนแต่ละคู่ต่อไปนี้

1. 125 และ -215
2. 252 และ 225

ตัวอย่าง 3.1.8 กำหนดให้ a เป็น ห.ร.ม. ของ 403 และ 465 และ b เป็น ห.ร.ม. ของ 431 และ 465 แล้ว $a-b$ มีค่าเท่าใด

ตัวอย่าง 3.1.9 จงหาตัวหารร่วมมากของจำนวนแต่ละคู่ต่อไปนี้

1. 36^3 และ 100^2

2. $10!$ และ 225^2

ตัวอย่าง 3.1.10 ถ้า n เป็นจำนวนเต็มบวกที่มากที่สุด ซึ่งหาร 90 เศษเหลือคือ 6 และหาร 150 เศษเหลือคือ 3 แล้ว n หาร 41 เศษเหลือเท่าใด

ตัวอย่าง 3.1.11 ให้ a เป็นจำนวนเต็มบวกซึ่ง $3 \mid a$ และ $5 \mid a$ ถ้า a กับ 7 เป็นจำนวนเฉพาะสัมพัทธ์กัน แล้ว ห.ร.ม. ของ a กับ 105 เท่ากับข้อใดต่อไปนี้

ตัวอย่าง 3.1.12 สำหรับจำนวนเต็ม a, b ใด ๆ ให้ $S = \{1, 2, 3, ..., 400\}$ ให้

$$G = \{x \in S : \gcd(x, 40) = 5\}$$

แล้วจำนวนสมาชิกของเซต G เท่ากับเท่าใด

ตัวอย่าง 3.1.13 จำนวนเต็มตั้งแต่ 0 ถึง 100 ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ 15 มีทั้งหมดกี่จำนวน

ตัวอย่าง 3.1.14 มีลูกแก้ว 2 กอง กองหนึ่งเป็นลูกแก้วสีแดงจำนวน 143 ลูก อีกกองหนึ่งเป็นสีเหลืองจำนวน 338 ลูก ต้องการแบ่งลูกแก้วทั้งสองกองนี้ออกเป็นกองเล็ก ๆ โดยที่จำนวนลูกแก้วกองละเท่า ๆ กันและมีจำนวนของลูกแก้วในกองเล็ก ๆ เหล่านั้นมากที่สุด ถ้าลูกแก้วสีแดงแบ่งได้ x กอง และสีเหลืองแบ่งได้ y กอง แล้ว $x + y$ มีค่าเท่ากับเท่าใด

ต่อไปจะกล่าวถึงสมบัติเกี่ยวกับตัวหารร่วมมากซึ่งมีมากมาย แต่ในหัวข้อนี้จะนำเสนอที่เป็นเบื้องต้น และทฤษฎีบทที่จะใช้ในการพิสูจน์สมบัติอื่น ๆ ของสมบัติจำนวนเต็มในบทต่อไป

ทฤษฎีบท 3.1.15 สมบัติเชิงเส้น (Linearily)
ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ และ $d = \gcd(a, b)$ แล้ว

$$\text{จะมี } x, y \in \mathbb{Z} \qquad \text{ที่ทำให้} \qquad d = ax + by$$

บทแทรก 3.1.16 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ และ $d = \gcd(a, b)$ จะได้ว่า

$$\text{สำหรับจำนวนเต็ม } c \text{ ใด ๆ ถ้า } \quad c \mid a \quad \text{และ} \quad c \mid b \quad \text{แล้ว} \quad c \mid d$$

ทฤษฎีบท 3.1.17 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ แล้ว

$$\gcd(a,b) = 1 \quad \text{ก็ต่อเมื่อ} \quad \text{มี} \quad x, y \in \mathbb{Z} \quad \text{ที่ทำให้} \quad 1 = ax + by$$

ทฤษฎีบท 3.1.18 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ ซึ่ง $\gcd(a,b) = 1$ จะได้ว่า

$$\gcd(a, b^n) = 1 \text{ สำหรับจำนวนนับ } n \text{ ใด ๆ}$$

ทฤษฎีบท 3.1.19 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ และ m เป็นจำนวนเต็มบวก แล้ว

$$\gcd(ma, mb) = m \cdot \gcd(a,b)$$

ตัวอย่าง 3.1.20 จงหาตัวหารร่วมมากของจำนวนเต่อไปนี้ โดยใช้ทฤษฎีบท 3.1.19

1. 75 และ 100

2. 6^5 และ 10^3

3. 9900 และ 11880

ทฤษฎีบท 3.1.21 ให้ $a, b \in \mathbb{Z}$ โดยที่ $d = \gcd(a, b)$ แล้ว $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

ทฤษฎีบท 3.1.22 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ และ x เป็นจำนวนเต็ม แล้ว

$$\gcd(a, b) = \gcd(a + bx, b) = \gcd(a, b + ax)$$

ตัวอย่าง 3.1.23 จงหาตัวหารร่วมมากของจำนวนเต่อไปนี้ โดยใช้ทฤษฎีบท 3.1.22

1. 75 และ 100

2. 43008 และ 7680

ทฤษฎีบท 3.1.24 ให้ a, b, c, m เป็นจำนวนเต็ม จะได้ว่า

1. ถ้า $\gcd(a, m) = \gcd(b, m) = 1$ แล้ว $\gcd(ab, m) = 1$
2. ถ้า $\gcd(a, m) = 1$ และ $b \mid a$ แล้ว $\gcd(b, m) = 1$
3. ถ้า $a \mid bc$ และ $\gcd(a, b) = 1$ แล้ว $a \mid c$
4. ถ้า $a \mid c$ และ $b \mid c$ โดยที่ $\gcd(a, b) = 1$ แล้ว $ab \mid c$

ตัวอย่าง 3.1.25 มีจำนวนเต็มตั้งแต่ 1 ถึง 1000 ที่หารด้วย 3 และ 5 ลงตัว ทั้งหมดกี่จำนวน

ตัวอย่าง 3.1.26 จงแสดงว่า สำหรับจำนวนเต็ม a, b, c ใด ๆ

$$\text{ถ้า } ab \mid c \text{ และ } \gcd(a,b) = 1 \quad \text{แล้ว} \quad a \mid c \text{ และ } b \mid c$$

ตัวอย่าง 3.1.27 จงแสดงว่า สำหรับจำนวนเต็ม a, b, c ใด ๆ

$$\text{ถ้า} \quad \gcd(a,b) = c \quad \text{แล้ว} \quad \gcd(a^2, b^2) = c^2$$

ทฤษฎีบท 3.1.28 วิธีแบบยุคลิด
ให้ a, b, q, r เป็นจำนวนเต็ม โดยที่ $a > 0$ และ $b = aq + r$ เมื่อ $0 \leq r < a$ แล้ว

$$\gcd(a, b) = \gcd(a, r)$$

ตัวอย่าง 3.1.29 จงหาตัวหารร่วมมากของจำนวนแต่ละคู่ต่อไปนี้ โดยวิธีแบบยุคลิด

1. 252 และ 198

2. 2004 และ 1106

ตัวอย่าง 3.1.30 กำหนดให้ $a \in \mathbb{Z}$ จงพิสูจน์ข้อความต่อไปนี้

1. $\gcd(2a+1, 9a+4) = 1$

2. $\gcd(5a+2, 7a+3) = 1$

3. $\gcd(3a, 3a+2) = 1$ เมื่อ a เป็นจำนวนเต็มคี่

ตัวอย่าง 3.1.31 จงแสดงว่า สำหรับจำนวนเต็มบวก n ใด ๆ

$$\gcd(n^3 + 2n, n^4 + 3n^2 + 1) = 1$$

บทนิยาม 3.1.32 ให้ $a_1, a_2, ..., a_n$ เป็นจำนวนเต็มที่ไม่ใช่ศูนย์พร้อมกัน แล้ว

จำนวนเต็มบวก d จะเป็น**ตัวหารร่วม**ของ $a_1, a_2, ..., a_n$ ก็ต่อเมื่อ $d \mid a_1, d \mid a_2, ..., d \mid a_n$

และ d จะเป็น**ตัวหารร่วมมาก**ของ $a_1, a_2, ..., a_n$ เขียนแทนด้วย $\gcd(a_1, a_2, ..., a_n)$ ก็ต่อเมื่อ

(1) d เป็นตัวหารร่วมของ $a_1, a_2, ..., a_n$ และ

(2) สำหรับจำนวนเต็มบวก c ถ้า c เป็นตัวหารร่วมของ $a_1, a_2, ..., a_n$ แล้ว $d \leq c$

ทฤษฎีบท 3.1.33 สำหรับจำนวนเต็ม $a_1, a_2, ..., a_n$ ที่ไม่ใช่ศูนย์พร้อมกัน แล้ว

1. $\gcd(\gcd(a_1, a_2), a_3, ..., a_n) = \gcd(a_1, a_2, ..., a_n)$
2. $\gcd(\gcd(a_1, a_2, ..., a_{n-1}), a_n) = \gcd(a_1, a_2, ..., a_n)$

ตัวอย่าง 3.1.34 จงหาตัวหารร่วมมากต่อไปนี้

1. $\gcd(4, 6, 18)$

2. $\gcd(12, 18, 24)$

3. $\gcd(350, 49, 140, 105)$

4. $\gcd(50, 125, 145, 500)$

ทฤษฎีบท 3.1.35 สำหรับจำนวนเต็ม $a_1, a_2, ., , , a_n$ ที่ไม่ใช่ศูนย์พร้อมกัน และ $d = \gcd(a_1, a_2, ., , , a_n)$ แล้ว

1. จะมี $x_1, x_2, ..., x_n \in \mathbb{Z}$ ที่ทำให้ $d = a_1x_1x + a_2x_2 + ... + a_nx_n$
2. สำหรับจำนวนเต็ม c ใด ๆ ถ้า $c \mid a_1, c \mid a_2, ..., c \mid a_n$ แล้ว $c \mid d$

บทนิยาม 3.1.36 ถ้า $\gcd(a_1, a_2, ., , , a_n) = 1$ เราจะกล่าวว่า $a_1, a_2, ., , , a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ ถ้าทุก ๆ คู่เป็นจำนวนเฉพาะสัมพัทธ์กันเราจะกล่าวว่าเป็น**จำนวนเฉพาะสัมพัทธ์ทุกคู่** (pairwise relatively prime)

ตัวอย่าง 3.1.37 จงตรวจสอบจำนวนต่อไปนี้ว่าเป็นเฉพาะสัมพัทธ์

1. $4, 6, 9$

2. $3, 21, 15$

3. $12, 17, 25$

ทฤษฎีบท 3.1.38 สำหรับจำนวนเต็ม $a_1, a_2, ., , , a_n$ ที่ไม่ใช่ศูนย์พร้อมกัน
จะได้ว่า $\gcd(a_1, a_2, ., , , a_n) = 1$ ก็ต่อเมื่อ

มีจำนวนเต็ม $x_1, x_2, ..., x_n$ ที่ทำให้ $1 = a_1x_1x + a_2x_2 + ... + a_nx_n$

แบบฝึกหัด 3.1

1. จงหาจำนวนเต็มทั้งหมดตั้งแต่ 1 ถึง 200 ที่สอดคล้องเงื่อนไขต่อไปนี้

   1.1 หารด้วย 8 ลงตัว

   1.2 หารด้วย 7 ได้เศษเหลือเท่ากับ 2

   1.3 หารด้วย 3 หรือ 5 ลงตัว

   1.4 เป็นจำนวนเฉพาะสัมพัทธ์กับ 18

   1.5 ห.ร.ม. กับ 30 เท่ากับ 5

   1.6 หารด้วย 7 ลงตัว แต่หารด้วย 5 ไม่ลงตัว

2. จงหา $\gcd(a,b)$ เมื่อกำหนดให้

   2.1 $a = 127$ และ $b = 125$

   2.2 $a = 289$ และ $b = -96$

   2.3 $a = -339$ และ $b = -1234$

   2.4 $a = 9987$ และ $b = 2351$

   2.5 $a = 1123$ และ $b = 5547$

   2.6 $a = 3054$ และ $b = 12378$

3. จงแสดงว่า ถ้า $\gcd(a,4) = 2$ และ $\gcd(b,4) = 2$ แล้ว $\gcd(a+b,4) = 2$ เมื่อ $a, b \in \mathbb{Z}$

4. จงแสดงว่า ถ้า $a, b \in \mathbb{Z}$ ซึ่ง $\gcd(a,b) = 1$ แล้ว $\gcd(a+b, a-b) = 1$ หรือ 2

5. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มคู่ที่ไม่ใช่ศูนย์ทั้งคู่ แล้ว $\gcd(a,b) = 2\gcd\left(\frac{a}{2}, \frac{b}{2}\right)$

6. จงแสดงว่า ถ้า a เป็นจำนวนเต็มคู่ และ b เป็นจำนวนเต็มคี่ แล้ว $\gcd(a,b) = \gcd\left(\frac{a}{2}, b\right)$

7. จงแสดงว่า ถ้า $a, b, c \in \mathbb{Z}$ ซึ่ง $c \mid ab$ แล้ว $c \mid d_1 d_2$ เมื่อ $d_1 = \gcd(a,c)$ และ $d_2 = \gcd(b,c)$

8. จงแสดงว่า ถ้า $a, b \in \mathbb{Z}$ ซึ่ง $\gcd(a,b) = 1$ แล้ว $\gcd(a^n, b^n) = 1$ ทุก $n \in \mathbb{N}$

9. จงแสดงว่า $\gcd(3n+4, 2n+3) = 1$ สำหรับทุก ๆ จำนวนเต็ม n

10. จงแสดงว่า ไม่มีจำนวนเต็ม x, y ที่สอดคล้องกับ $x + y = 100$ และ $\gcd(x,y) = 3$

11. จงแสดงว่า มี $x, y \in \mathbb{Z}$ จำนวนอนันต์ที่สอดคล้องกับ $x + y = 100$ และ $\gcd(x,y) = 5$

12. จงพิสูจน์ว่า ถ้ามีจำนวนเต็ม x, y ที่ทำให้ $\gcd(a,b) = ax + by$ แล้ว $\gcd(x,y) = 1$ เมื่อ $a, b \in \mathbb{Z}$

13. ให้ $a, b, c \in \mathbb{Z}$ และ $d = \gcd(a,b)$ จงพิสูจน์ว่า $a \mid bc$ ก็ต่อเมื่อ $\frac{a}{d} \mid c$

14. ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ จงพิสูจน์ว่าถ้า $\gcd(a, b^n) = 1$ แล้ว $\gcd(a,b) = 1$ สำหรับจำนวนนับ n ใด ๆ

3.2 ขั้นตอนวิธีแบบยุคลิด

ทฤษฎีบท 3.2.1 ขั้นตอนวิธีแบบยุคลิด (Euclidean Algorithm)
ให้ a และ b เป็นจำนวนเต็มโดยที่ $a > 0$ จะได้ว่ามีจำนวนเต็ม

$$q_i \quad \text{เมื่อ} \quad i = 1, 2, 3, .., n+1 \qquad \text{และ} \qquad r_j \quad \text{เมื่อ} \quad j = 1, 2, 3, .., n \quad \text{ที่ทำให้}$$

$$\begin{aligned}
b &= aq_1 + r_1 && \text{เมื่อ} \quad 0 < r_1 < a \\
a &= r_1q_2 + r_2 && \text{เมื่อ} \quad 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3 && \text{เมื่อ} \quad 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n && \text{เมื่อ} \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

และ $\gcd(a, b) = r_n$

โดยทฤษฎีบท 3.1.28 จะได้ว่า

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

โดยขั้นตอนวิธีแบบยุคลิด ทำให้หาจำนวนเต็ม x, y ซึ่ง $\gcd(a,b) = ax + by$ ทำได้โดยกำจัดเศษ $r_{n-1}, ..., r_2, r_1$ เริ่มจากสมการ

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

แล้วแทนค่า r_{n-1} ด้วยค่าในสมการขั้นตอนวิธีแบบยุคลิดจะได้ว่า

$$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2} = r_{n-2}(1 + q_n q_{n-1}) + r_{n-3}(-q_n)$$

เห็นได้ว่าสมการที่ได้แสดงการเขียน r_n ในรูปผลบวก r_{n-2} และ r_{n-3} จากนั้นทำขั้นตอนเช่นนี้ไปเรื่อย ๆ ซึ่งกำจัดเศษ $r_{n-1}, ..., r_2, r_1$ ตามลำดับ ในที่สุดจะแสดงการเขียน r_n ในรูปผลบวกของ a และ b ซึ่ง r_n คือ ห.ร.ม. ของ a และ b นั่นคือวิธีการที่ทำให้ทราบค่าของ x, y ซึ่ง

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

ตัวอย่าง 3.2.2 จงหา $d = \gcd(305, 168)$ และหาจำนวนเต็ม x, y ซึ่งทำให้ $d = 305x + 168y$

ตัวอย่าง 3.2.3 จงหา $d = \gcd(5767, 4453)$ และหาจำนวนเต็ม x, y ซึ่งทำให้

$$d = 5767x + 4453y$$

ตัวอย่าง 3.2.4 จงหาจำนวนเต็ม x และ y ที่สอดคล้องสมการ $243x + 198y = 9$

ต่อไปจะเป็นวิธีการหาจำนวน x, y ที่สอดคล้องสมการ $\gcd(a,b) = ax+by$ โดยใช้การดำเนินการบนแถวตามขั้นตอนดังนี้

1. เลือกตัวมากสุดระหว่าง a และ b เป็นแถวที่ 1 เรียกว่า R_1 โดยเขียนไว้ท้ายสุดของแถว และอีกจำนวนเป็นแถวที่ 2 เรียกว่า R_2 โดยเขียนไว้ท้ายสุดของแถวเช่นกัน โดยเขียนกั้นด้วย | ระหว่างสมการกับเมตริกซ์ สมมติว่า $b > a$ เขียนได้ดังนี้

$$\begin{array}{rcrcr|rrrr} b &=& b(1) &+& a(0) & b & 1 & 0 & R_1 \\ a &=& b(0) &+& a(1) & a & 0 & 1 & R_2 \end{array}$$

2. แถวที่ 3 เรียกว่า R_3 จะเกิดจาก $R_3 = R_1 - q_1R_2$ เมื่อ $b = aq_1 + r_1$ โดยที่ $0 \le r_1 < a$

$$\begin{array}{rcrcr|rrrr} b &=& b(1) &+& a(0) & b & 1 & 0 & R_1 \\ a &=& b(0) &+& a(1) & a & 0 & 1 & R_2 \\ r_1 &=& b(1) &+& a(-q_1) & r_1 & 1 & -q_1 & R_3 = R_1 - q_1R_2 \end{array}$$

3. แถวที่ 4 เรียกว่า R_4 จะเกิดจาก $R_4 = R_2 - q_2R_3$ เมื่อ $b = r_1q_2 + r_2$ โดยที่ $0 \le r_2 < r_1$ ทำเช่นนี้ไปเรื่อย ๆ จนแถวสุดท้ายเป็น $\gcd(a,b)$ อยู่ซ้ายมือ ตามขั้นตอนวิธีการหารแบบยุคลิด แล้วจะได้ $\gcd(a,b) = ax + by$ นั่นเอง

จากตัวอย่าง 3.2.4 พิจารณา $27x + 22y = 1$ ทำได้โดยวิธีการดำเนินบนแถวดังนี้

$$\begin{array}{rcrcr|rrrr} 27 &=& 27(1) &+& 22(0) & 27 & 1 & 0 & R_1 \\ 22 &=& 27(0) &+& 22(1) & 22 & 0 & 1 & R_2 \\ 5 &=& 27(1) &+& 22(-1) & 5 & 1 & -1 & R_3 = R_1 - R_2 \\ 2 &=& 27(-4) &+& 22(5) & 2 & -4 & 5 & R_4 = R_2 - 4R_3 \\ 1 &=& 27(9) &+& 22(-11) & 1 & 9 & -11 & R_5 = R_3 - 2R_4 \end{array}$$

ดังนั้น $x = 9$ และ $y = -11$

ตัวอย่าง 3.2.5 จงหาจำนวนเต็ม x และ y ที่สอดคล้องสมการ $71x - 50y = 1$

ตัวอย่าง 3.2.6 ให้ a, b และ c เป็นจำนวนเต็ม ถ้า c เป็น ห.ร.ม. ของ -864 และ -354 ซึ่ง

$$c = a(-864) + b(-354)$$

แล้ว $c + b$ เท่ากับเท่าใด

ตัวอย่าง 3.2.7 จงหา $d = \gcd(12378, 3054)$ และหาจำนวนเต็ม x, y ซึ่งทำให้

$$d = 12378x + 3054y$$

แบบฝึกหัด 3.2

1. ให้ n เป็นจำนวนเต็มบวก ซึ่ง ห.ร.ม. ของ n และ 42 เท่ากับ 6 ถ้า

$$42 = nq_0 + r_0 \qquad \text{เมื่อ} \quad 0 < r_0 < n$$
$$n = 2r_0 + r_1 \qquad \text{เมื่อ} \quad 0 < r_1 < r_0$$

   โดยที่ q_0, r_0, r_1 เป็นจำนวนเต็ม จงหา n

2. ให้ a และ b เป็นจำนวนเต็ม ซึ่ง a เป็น ห.ร.ม. ของ b และ 216 ถ้า q_1, q_2 เป็นจำนวนเต็มบวก โดยที่

$$216 = bq_1 + 106$$
$$b = 106q_2 + 4$$

   จงหา $a + b$

3. จงหา $d = \gcd(a, b)$ และจำนวนเต็ม x และ y ซึ่ง $d = ax + by$ เมื่อกำหนดให้

   3.1 $a = 127$ และ $b = 125$

   3.2 $a = 289$ และ $b = -96$

   3.3 $a = -339$ และ $b = 1234$

   3.4 $a = 9987$ และ $b = 2351$

   3.5 $a = -1123$ และ $b = 5547$

   3.6 $a = 3054$ และ $b = 12378$

   3.7 $a = 37129$ และ $b = 14659$

   3.8 $a = 1769$ และ $b = 2378$

   3.9 $a = 2106$ และ $b = 8318$

   3.10 $a = 4125$ และ $b = 3218$

4. จงหาจำนวนเต็ม x และ y ที่สอดคล้องกับ

   4.1 $43x + 64y = 1$

   4.2 $93x - 81y = 3$

   4.3 $73x + 51y = 1$

5. ให้ m, n เป็นจำนวนเต็ม ซึ่ง $\gcd(28, 42) = 28m + 42n$ จงหาค่าของ $m + n$

3.3 ตัวคูณร่วมน้อย

บทนิยาม 3.3.1 ให้ a, b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์ และ m เป็นจำนวนเต็มบวก

m เป็น**ตัวคูณร่วม (common multiple)** ของ a และ b ถ้า $a \mid m$ และ $b \mid m$

ข้อสังเกต 3.3.2 ให้ A แทนเซตของจำนวนเต็มที่หารด้วย a ลงตัว และ B แทนเซตของจำนวนเต็มที่หารด้วย b ลงตัว แล้ว

$A \cap B$ คือเซตของตัวคูณร่วมของ a และ b

1. เนื่องจาก $a \mid a$ และ $b \mid b$ ดังนั้น $A \cap B \neq \varnothing$
2. ถ้า $a = 1$ แล้ว A เป็นเซตของจำนวนเต็มบวก
3. A และ B เป็นเซตอนันต์

ตัวอย่าง 3.3.3 จงหาตัวคูณร่วมของ

1. 2 และ 3
2. 6 และ 9

บทนิยาม 3.3.4 ให้ a และ b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์ จำนวนเต็มบวก m จะเป็น**ตัวคูณร่วมน้อย (least common multiple)** หรือ **ค.ร.น. (l.c.m.)** ของ a และ b เขียนแทนด้วย $\ell\mathrm{cm}(a, b)$ ก็ต่อเมื่อ

(ก) $a \mid m$ และ $b \mid m$

(ข) ทุกจำนวนเต็มบวก c ถ้า $a \mid c$ และ $b \mid c$ แล้ว $m \leq c$

ตัวอย่าง 3.3.5 จงหาตัวคูณร่วมน้อยของจำนวนแต่ละคู่ต่อไปนี้

1. 15 และ 21
2. 125 และ -55
3. 588 และ 1050
4. 12^4 และ $10!$

ตัวอย่าง 3.3.6 ให้ a และ b เป็นจำนวนเต็มบวก ซึ่ง $a < b$ สอดคล้องเงื่อนไข

(1) 5 หาร a ลงตัว และ 3 หาร b ลงตัว

(2) a และ b เป็นจำนวนเฉพาะสัมพัทธ์กัน

(3) ค.ร.น. ของ a และ b เท่ากับ 165

จงหาจำนวน a และ b

ตัวอย่าง 3.3.7 กำหนดให้ x และ y เป็นจำนวนเต็มบวก โดยที่ $x < y$ สอดคล้องเงื่อนไข

(1) ห.ร.ม. ของ x และ y เท่ากับ 9

(2) ค.ร.น. ของ x และ y เท่ากับ 28215

(3) จำนวนเฉพาะที่แตกต่างกันทั้งหมดที่หาร x ลงตัวมี 3 จำนวน

ค่าของ $y - x$ เท่ากับเท่าใด

ทฤษฎีบท 3.3.8 ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ จะได้ว่า

$$\gcd(a, b) \cdot \ell\mathrm{cm}(a, b) = |ab|$$

ทฤษฎีบท 3.3.9 ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ และ $m = \ell\mathrm{cm}(a, b)$ จะได้ว่า

สำหรับจำนวนเต็ม c ใด ๆ ถ้า $a \mid c$ และ $b \mid c$ แล้ว $m \mid c$

ทฤษฎีบท 3.3.10 ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ และ $k \in \mathbb{N}$ จะได้ว่า

$$\ell\mathrm{cm}(ka, kb) = k \cdot \ell\mathrm{cm}(a, b)$$

ตัวอย่าง 3.3.11 ให้ a เป็นจำนวนคู่บวก และ b เป็นจำนวนคี่บวก จงตรวจสอบข้อความต่อไปนี้ว่าเป็นจริงหรือเท็จ พร้อมให้เหตุผลประกอบ

1. a และ b เป็นจำนวนเฉพาะสัมพัทธ์

2. ห.ร.ม. ของ a และ b เท่ากับ ห.ร.ม. ของ a และ $2b$

3. ค.ร.น. ของ a และ b เท่ากับ ค.ร.น. ของ a และ $2b$

ตัวอย่าง 3.3.12 ให้ a และ b เป็นจำนวนเต็มบวก จงตรวจสอบข้อความ

$$\text{ถ้า } \ a \mid b \ \text{ แล้ว } \ \ell\mathsf{cm}(a,b) = b$$

เป็นจริงหรือเท็จ พร้อมให้เหตุผลประกอบ

บทนิยาม 3.3.13 ให้ $a_1, a_2, ..., a_n$ เป็นจำนวนเต็มที่ไม่ใช่ศูนย์พร้อมกัน แล้ว

จำนวนเต็มบวก m จะเป็น**ตัวคูณร่วม**ของ $a_1, a_2, ..., a_n$ ก็ต่อเมื่อ $a_1 \mid m, a_2 \mid m, ..., a_n \mid m$

และ m จะเป็น**ตัวคูณร่วมน้อย**ของ $a_1, a_2, ..., a_n$ เขียนแทนด้วย $\ell\mathsf{cm}(a_1, a_2, ., , , a_n)$ ก็ต่อเมื่อ

(1) m เป็นตัวคูณร่วมของ $a_1, a_2, ..., a_n$ และ

(2) สำหรับจำนวนเต็มบวก c ถ้า c เป็นตัวคูณร่วมของ $a_1, a_2, ..., a_n$ แล้ว $m \leq c$

ตัวอย่าง 3.3.14 จงหาตัวคูณร่วมของ $9, 6$ และ 15

ตัวอย่าง 3.3.15 ถ้า x เป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่ง $9, 12$ และ 15 หาร x ลงตัว แต่ 11 หาร x เศษเหลือเท่ากับ 7 แล้ว x มีค่าเท่าใด

ทฤษฎีบท 3.3.16 สำหรับจำนวนเต็ม $a_1, a_2, ., , , a_n$ ที่ไม่ใช่ศูนย์พร้อมกัน แล้ว

1. $\ell\mathsf{cm}(\ell\mathsf{cm}(a_1, a_2), a_3, ..., a_n) = \ell\mathsf{cm}(a_1, a_2, ..., a_n)$
2. $\ell\mathsf{cm}(\ell\mathsf{cm}(a_1, a_2, ..., a_{n-1}), a_n) = \ell\mathsf{cm}(a_1, a_2, ..., a_n)$

ตัวอย่าง 3.3.17 จงหาตัวคูณร่วมน้อยของจำนวนต่อไปนี้

1. $\ell\mathsf{cm}(4, 6, 18)$

2. $\ell\mathsf{cm}(6, 10, 15)$

3. $\ell\mathsf{cm}(35, 49, 42, 63)$

4. $\ell\mathsf{cm}(50, 125, 150, 500)$

ทฤษฎีบท 3.3.18 สำหรับจำนวนเต็ม $a_1, a_2, ., , , a_n$ ที่ไม่ใช่ศูนย์พร้อมกัน และ $m = \ell\mathsf{cm}(a_1, a_2, ., , , a_n)$ แล้ว สำหรับจำนวนเต็ม c ใด ๆ ถ้า $c \mid a_1, c \mid a_2, ..., c \mid a_n$ แล้ว $m \mid c$

แบบฝึกหัด 3.3

1. จงหา $\ell\mathsf{cm}(a,b)$ เมื่อกำหนดให้

   1.1 $a=36$ และ $b=96$

   1.2 $a=280$ และ $b=-96$

   1.3 $a=-125$ และ $b=-325$

   1.4 $a=990$ และ $b=1020$

   1.5 $a=1024$ และ $b=2350$

   1.6 $a=5005$ และ $b=6590$

2. ถ้า a เป็นจำนวนเต็มบวกซึ่ง ค.ร.น. ของ a และ 63 เท่ากับ $7a$ และ ห.ร.ม. ของ a และ 63 เท่ากับ c จงหา a และ c

3. กำหนดให้ a,b,c และ d เป็นจำนวนเต็ม พิจารณาข้อความต่อไปนี้ ถ้าเป็นจริงจงพิสูจน์ ถ้าเป็นเท็จจงยกตัวอย่างค้าน

   3.1 $\ell\mathsf{cm}(a^2,b^2)=(\ell\mathsf{cm}(a,b))^2$

   3.2 ถ้า $a\,|\,b$ แล้ว $\ell\mathsf{cm}(a,b)=|b|$

   3.3 ถ้า $a\mid c$ และ $b\mid c$ และ $\ell\mathsf{cm}(a,b)=|ab|$ แล้ว $ab\mid c$

   3.4 $\ell\mathsf{cm}(ca,b)=c\cdot\ell\mathsf{cm}(a,b)$

   3.5 $\ell\mathsf{cm}(a+c,b+c)=\ell\mathsf{cm}(a,b)$

   3.6 ถ้า $\mathsf{gcd}(a,b)=d$ และ $\ell\mathsf{cm}(a,b)=c$ แล้ว $dc=ab$ เมื่อ $a,b,c,d\in\mathbb{Z}^+$

4. ให้ $a,b,c\in\mathbb{Z}$ จงแสดงว่า $\ell\mathsf{cm}(a,b)\mid c$ ก็ต่อเมื่อ $a\mid c$ และ $b\mid c$

5. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มบวก แล้ว $\mathsf{gcd}(a,b)=\mathsf{gcd}(a+b,\ell\mathsf{cm}(a,b))$

6. ให้ a,b,c เป็นจำนวนเต็มที่ไม่ใช่ศูนย์ และ $c>0$ จงพิสูจน์ว่า

$$\ell\mathsf{cm}(a,b)=m \qquad \text{ก็ต่อเมื่อ} \qquad \ell\mathsf{cm}(ca,cb)=cm$$

7. ให้ x และ y เป็นจำนวนเต็มบวก ซึ่ง $80<x<y$ และ $x=pq$ เมื่อ p,q เป็นจำนวนเฉพาะซึ่ง $p\neq q$ ถ้า x และ y เป็นจำนวนเฉพาะสัมพัทธ์กัน และ ค.ร.น. ของ x และ y เท่ากับ $15,015$ จงหา y ทั้งหมดที่สอดคล้องเงื่อนไขที่กำหนดให้

บทที่ 4

จำนวนเฉพาะ

ในบทนี้จะศึกษาสมบัติบางประการของจำนวนเฉพาะ ตลอดจนข้อพิสูจน์ต่าง ๆ ที่เกี่ยวข้อง รวมถึงข้อคาดการณ์เกี่ยวกับจำนวนเฉพาะ การตรวจสอบ และค้นหาจำนวนเฉพาะ

4.1 นิยามและสมบัติบางประการของจำนวนเฉพาะ

บทนิยาม 4.1.1 จำนวนเต็ม p ที่มากกว่า 1 เรียกว่า **จำนวนเฉพาะ (prime)** ก็ต่อเมื่อ

$$p \quad \text{มีตัวหารคือ} \quad \pm 1 \quad \text{และ} \quad \pm p \quad \text{เท่านั้น}$$

จำนวนเต็มที่มากกว่า 1 ที่ไม่ใช่จำนวนเฉพาะเรียกว่า **จำนวนประกอบ (composite number)**

ตัวอย่าง 4.1.2 จงยกตัวอย่างจำนวนเฉพาะและจำนวนประกอบ ที่ไม่เกิน 50

ข้อสังเกต 4.1.3 จากบทนิยาม 4.1.1 จะได้ว่า

1. 2 เป็นจำนวนเฉพาะที่เป็นจำนวนคู่เพียงตัวเดียวเท่านั้น
2. p เป็นจำนวนเฉพาะ ก็ต่อเมื่อ $d \nmid p$ ทุก ๆ จำนวนเต็ม d ซึ่ง $1 < d < p$
3. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ ถ้า $a \mid p$ แล้ว $a = \pm 1$ หรือ $a = \pm p$
4. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ จะได้ว่า $p \mid a$ ก็ต่อเมื่อ $\gcd(a, p) = p$
5. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ จะได้ว่า $p \nmid a$ ก็ต่อเมื่อ $\gcd(a, p) = 1$
6. ให้ p และ q เป็นจำนวนเฉพาะ ถ้า $p \mid q$ แล้ว $p = q$
7. a เป็นจำนวนประกอบ ก็ต่อเมื่อ มีจำนวนเต็ม d ซึ่ง $1 < d < a$ ที่ทำให้ $d \mid a$
8. a เป็นจำนวนประกอบ ก็ต่อเมื่อ มีจำนวนเต็ม b, c ซึ่ง $1 < b \leq c < a$ ที่ทำให้ $a = bc$

ตัวอย่าง 4.1.4 มีจำนวนเฉพาะ p ที่ทำให้ $2^p - 1$ ไม่เป็นจำนวนเฉพาะ

ตัวอย่าง 4.1.5 จงแสดงว่า ถ้า n จำนวนประกอบ แล้ว $2^n - 1$ เป็นจำนวนประกอบ

ทฤษฎีบท 4.1.6 ทุกจำนวนเต็ม a ที่มากกว่า 1 จะมีจำนวนเฉพาะ p ที่ $p \mid a$

ทฤษฎีบท 4.1.7 (**ยุคลิด**) มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์

ตัวอย่าง 4.1.8 ให้ $n \in \mathbb{N}$ จงแสดงว่ามีจำนวนประกอบเรียงต่อกัน n จำนวน

ทฤษฎีบท 4.1.9 ทฤษฎีบทนำของยุคลิด
ให้ p เป็นจำนวนเฉพาะ และ $a, b \in \mathbb{Z}$ จะได้ว่า

$$\text{ถ้า} \quad p \mid ab \quad \text{แล้ว} \quad p \mid a \quad \text{หรือ} \quad p \mid b$$

ตัวอย่าง 4.1.10 จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องเงื่อนไข $p \mid (p+1)250$

ทฤษฎีบท 4.1.11 ให้ p เป็นจำนวนเฉพาะ และ $a, b, a_1, a_2, ..., a_n \in \mathbb{Z}$ เมื่อ $n \in \mathbb{N}$ จะได้ว่า

$$\text{ถ้า} \quad p \mid (a_1 a_2 ... a_n) \quad \text{แล้ว} \quad p \mid a_i \quad \text{สำหรับบางจำนวน } i \in \{1, 2, ..., n\}$$

บทแทรก 4.1.12 ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ เมื่อ $n \in \mathbb{N}$ แล้ว

$$\text{สำหรับจำนวนนับ } n \text{ ถ้า} \quad p \mid a^n \quad \text{แล้ว} \quad p \mid a$$

ตัวอย่าง 4.1.13 จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องกับเงื่อนไขต่อไปนี้

1. $p \mid 590^{15}$
2. $p \mid 10920^{99}$
3. $p \mid (630+p)^4$
4. $p \mid (150-3p)^{251}$
5. $p \mid (1225-10p)^{p+1}$
6. $p \mid (7700^3-p^2)^p$

ตัวอย่าง 4.1.14 กำหนดให้

$$A = \{p : p \text{ เป็นจำนวนเฉพาะ ที่ } p \mid (980-p)^3\}$$

แล้วผลบวกของสมาชิกทั้งหมดของ A มีค่าเท่าใด

ตัวอย่าง 4.1.15 จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องกับเงื่อนไข $p \mid 100!$

ตัวอย่าง 4.1.16 จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องกับเงื่อนไข $(p+1) \mid (p^2+2p+195)^2$

ตัวอย่าง 4.1.17 จงพิสูจน์ว่า สำหรับจำนวนเต็มบวก n จะได้ว่า

$n!+1$ และ $(n+1)!+1$ เป็นจำนวนเฉพาะสัมพัทธ์

แบบฝึกหัด 4.1

1. จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้อง

   1.1 $p \mid 231^3$

   1.2 $p \mid (p-455)^4$

   1.3 $p \mid (627+2p)^{11}$

   1.4 $p \mid (p+1530)^3$

   1.5 $(p+1) \mid (p-3382)^5$

   1.6 $(p-1) \mid (p^2-p+3333)$

2. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะ แล้ว $p \mid (2^p-2)$

3. ถ้า p และ q เป็นจำนวนเฉพาะซึ่ง $p \geq q > 4$ จงแสดงว่า $24 \mid (p^2-q^2)$

4. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ ซึ่ง $p \mid a^n$ แล้ว $p^n \mid a^n$

5. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะซึ่ง $p > 2$ แล้ว $4 \mid (p^2-1)$

6. จงหาจำนวนเฉพาะ p ทั้งหมดที่ทำให้ $p \mid (2^p-1)$

7. จงหาจำนวนเฉพาะ p ทั้งหมดที่ทำให้ $p \mid (2^p+1)$

8. จงหาจำนวนเฉพาะทั้งหมดที่หาร $100!$ ลงตัว

9. จงแสดงว่า p เป็นจำนวนเฉพาะที่ $p > 4$ แล้ว p^2+2 เป็นจำนวนประกอบ

10. จงตรวจสอบจำนวนเต็มที่อยู่ในรูป 8^n+1 เมื่อ $n \in \mathbb{N}$ เป็นจำนวนประกอบเมื่อใด ข้อเสนอแนะ $(2^n+1) \mid (2^{3n}+1)$

11. จงแสดงว่า ถ้า 2^n-1 เป็นจำนวนเฉพาะ แล้ว n เป็นจำนวนเฉพาะ

12. สำหรับจำนวนนับ n ถ้า n^3+1 เป็นจำนวนเฉพาะ จงแสดงว่า $n=1$

13. จงพิสูจน์ว่า $24 \mid (p^2-1)$ ทุกจำนวนเฉพาะ p ที่มากกว่า 3

14. ถ้า p เป็นจำนวนเฉพาะ จงแสดงว่าไม่มีจำนวนเต็ม a และ b ใด ๆ ซึ่ง $a^2 = pb^2$

4.2 ทฤษฎีบทหลักมูลเลขคณิต

ทฤษฎีบทต่อไปนี้มีบทบาทสำคัญต่อการนำไปใช้ ซึ่งเป็นเครื่องมือที่เกี่ยวข้องกับจำนวนเต็มในการศึกษาทฤษฎีบทต่าง ๆ ซึ่งยุคลิดได้เขียนไว้ในหนังสือ Euclid's Element เล่มที่ 9

ทฤษฎีบท 4.2.1 ทฤษฎีบทหลักมูลเลขคณิต (The Fundamental Theorem of Arithmematic)
จำนวนเต็มที่มากกว่า 1 ใด ๆ สามารถเขียนในรูปผลคูณของจำนวนเฉพาะได้ และถ้าไม่คิดลำดับเป็นสำคัญแล้วการเขียนนี้ทำได้เพียงวิธีเดียวเท่านั้น
หรือกล่าวได้ว่า จำนวนเต็ม $n > 1$ สามารถเขียนในรูป

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k}$$

โดยที่ $p_1, p_2, p_3, ..., p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < ... < p_k$ และ $a_i \in \mathbb{N}$ สำหรับทุก $i = 1, 2, 3, ..., k$ และเขียน n ในรูปดังกล่าวได้เพียงแบบเดียวเท่านั้น
เรียกการเขียน n รูปแบบนี้ว่า **รูปแบบบัญญัติ** (canonical form) ของ n

ตัวอย่าง 4.2.2 จงเขียนจำนวนที่เขียนในรูปแบบบัญญัติ

1. 48
2. 150^2
3. 1225
4. 4725
5. 1000^3
6. 15750
7. 846876
8. $50!$

ตัวอย่าง 4.2.3 ในการเขียน $50!$ ในรูปของจำนวนเต็มจะมีศูนย์ลงท้ายเรียงต่อเนื่องกันกี่ตัว

โดยทฤษฎีบท 4.2.1 ถ้า $n > 1$ และ $m > 1$ และเขียนรูปแบบบัญญัติได้ดังนี้

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k} \qquad \text{และ} \qquad m = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdots p_k^{b_k}$$

เมื่อแต่ละจำนวนเต็ม $a_i \geq 0$ และ $b_i \geq 0$ โดยที่ไม่เป็นศูนย์พร้อมกัน จะได้ว่า

$$\gcd(n, m) = p_1^{c_1} \cdot p_2^{c_2} \cdot p_3^{c_3} \cdots p_k^{c_k}$$
$$\ell\text{cm}(n, m) = p_1^{d_1} \cdot p_2^{d_2} \cdot p_3^{d_3} \cdots p_k^{d_k}$$

โดยที่ d_i และ c_i คือ ค่าต่ำสุดและสูงสุด ของ a_i และ b_i ตามลำดับ สำหรับทุก ๆ $i \in \{1, 2, 3, ..., k\}$

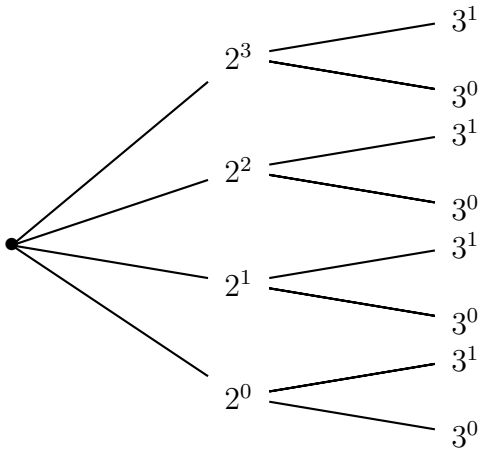
ตัวอย่าง 4.2.4 จงหาตัวหารร่วมมากและตัวคูณร่วมน้อยของจำนวนต่อไปนี้

1. 150 และ 100

2. 308 และ 1,176

3. 31,752 และ 4,725

พิจารณาการหาตัวหารทั้งหมดของ 24 เมื่อเขียนในรูปแบบบัญญัติจะได้ $24 = 2^3 \cdot 3$ เขียนแผนภาพต้นไม้ได้ดังนี้



จากแผนภาพจะได้ว่าตัวหารของ 24 คือ $1, 2, 3, 4, 6, 8, 12, 24$

ตัวอย่าง 4.2.5 จงหาตัวหารทั้งหมดของ 7,425

ทฤษฎีบท 4.2.6 ให้ $n \in \mathbb{Z}$ ซึ่ง $n > 1$ มีรูปแบบบัญญัติคือ

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k}$$

เมื่อ $a_i \in \mathbb{N}$ ทุก ๆ i แล้วจำนวนตัวประกอบทั้งหมดของ n มีทั้งหมด

$$(a_1 + 1)(a_2 + 1)(a_3 + 1) \cdots (a_k + 1)$$

ตัวอย่าง 4.2.7 จงหาจำนวนตัวหารทั้งหมดของ

1. 1,225

2. 100^3

3. 4,725

4. $650^3 \cdot 36^4$

5. $5265^3 \cdot 24255^2$

บทตั้ง 4.2.8 ผลคูณของจำนวนเต็มที่อยู่ในรูป $4k+1$ ตั้งแต่สองจำนวนขึ้นไปจะเป็นจำนวนเต็มที่อยู่ในรูป $4k+1$

ทฤษฎีบท 4.2.9 จำนวนเฉพาะที่อยู่ในรูป $4k+3$ มีอยู่เป็นจำนวนอนันต์

แบบฝึกหัด 4.2

1. จงเขียนจำนวนต่อไปนี้ในรูปแบบบัญญัติ

   1.1 $1,250$ 1.3 $2,5025$ 1.5 $150!$

   1.2 $1,000$ 1.4 $65,304$ 1.6 $88,442$

2. จงหาตัวหารร่วมมากและตัวคูณร่วมน้อยของจำนวนต่อไปนี้

   2.1 250 และ 150 2.2 330 และ $1,175$ 2.3 $10,240$ และ $4,725$

3. จงหาตัวหารทั้งหมดของจำนวนต่อไปนี้

   3.1 150 3.3 600 3.5 $15!$

   3.2 542 3.4 720 3.6 $31,752$

4. จงหาจำนวนของตัวหารทั้งหมดของ

   4.1 85 4.4 4095^5 4.7 $3528^5 \cdot 228^4$

   4.2 125 4.5 $10,395$ 4.8 $(10!)^4$

   4.3 $2,025$ 4.6 $30!$ 4.9 $(5!)(10!) \cdot 7425^7$

5. มีจำนวนเฉพาะที่อยู่ในรูป $6k+5$ เป็นจำนวนอนันต์

6. ถ้า n เป็นจำนวนเต็มคี่ แล้ว $3 \mid (2^n+1)$

7. จงแสดงว่า จำนวนเฉพาะที่เขียนในรูป $8n+5$ มีจำนวนอนันต์

8. ในการเขียนจำนวน $1000!$ ในรูปของจำนวนเต็มจะมีศูนย์ลงท้ายเรียงต่อเนื่องกันกี่ตัว

9. ในการเขียนจำนวน $(125)^{14} \cdot 44^{15} \cdot 45^{16}$ ในรูปของจำนวนเต็มจะมีศูนย์ลงท้ายเรียงต่อเนื่องกันกี่ตัว

10. จงหาจำนวนเต็ม k ที่มากที่สุดที่ $7^k \mid 100!$

11. มีจำนวนนับที่ไม่ใช่จำนวนเฉพาะกี่จำนวนที่หาร 77,760,000 ลงตัว

4.3 การค้นหาจำนวนเฉพาะ

วิธีหนึ่งในการตรวจสอบว่า n เป็นจำนวนเฉพาะหรือไม่ คือการหาจำนวนเต็มบวกที่มากกว่า 1 แต่น้อยกว่า n ถ้าไม่มีจำนวนใดที่หาร n ลงตัว แสดงว่าจำนวน n เป็นจำนวนเฉพาะ แต่วิธีดังกล่าวจะใช้ได้ดีเมื่อ n มีค่าไม่มากนัก ทฤษฎีบทต่อไปนี้จะเป็นอีกวิธีในการตรวจสอบจำนวนเฉพาะอย่างมีประสิทธิภาพมากกว่าวิธีดังที่กล่าวมา

ทฤษฎีบท 4.3.1 ถ้า a เป็นจำนวนประกอบ แล้วจะมีจำนวนเฉพาะ p ซึ่ง

$$p \leq \sqrt{a} \qquad \text{และ} \qquad p \mid a$$

ตัวอย่าง 4.3.2 จงตรวจสอบจำนวนต่อไปนี้ว่าเป็นจำนวนเฉพาะหรือไม่

1. 101
2. 113
3. 313
4. 401
5. 719
6. 1001

ต่อไปจะกล่าวถึงการหาจำนวนเฉพาะทุกตัวที่น้อยกว่าหรือเท่ากับ n เมื่อกำหนดจำนวนเต็ม n โดยใช้กฎแย้งสลับที่ของทฤษฎีบท 4.3.1 จะได้ว่า

ถ้าทุกจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{a}$ และ $p \nmid a$ แล้ว a เป็นจำนวนเฉพาะ

วิธีการนี้เรียกว่า **ตะแกรงเอราโตสเทเนส (The sieve of Eratosthesnes)** ซึ่งทำได้ดังนี้

(1) $p_1 = 2, p_2 = 3, p_3 = 5, ..., p_k$ เป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$

(2) เขียนจำนวนเต็มตั้งแต่ 2 ถึง n

(3) วงกลม p_1 แล้วกำจัดจำนวนทุกตัวในข้อ (2) ที่หารด้วย p_1 ลงตัว

(4) ทำข้อ (3) ซ้ำไปเรื่อยจาก $p_2, p_3, ..., p_k$

จำนวนเต็มที่เหลือจะเป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่า n

ตัวอย่าง 4.3.3 จงตรวจสอบจำนวนเฉพาะที่ไม่เกิน 50

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

ตัวอย่าง 4.3.4 จงหาจำนวนเฉพาะที่ไม่เกิน 50 ที่สามารถเขียนในรูป $3k + 1$ ได้

ต่อไปเป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่า 1,000

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	419	421	431	433	439
443	449	457	461	463	467	479	487	491	499	503	509
521	523	541	547	557	563	569	571	577	587	593	599
601	607	613	617	619	631	641	643	647	653	659	661
673	677	683	691	701	709	719	727	733	739	743	751
757	761	769	773	787	797	809	811	821	823	827	829
839	853	859	863	877	881	883	887	907	911	919	929
937	941	947	953	967	971	977	983	911	997		

ตัวอย่าง 4.3.5 จงตรวจสอบว่า 2,093 เป็นจำนวนเฉพาะหรือไม่

ตัวอย่าง 4.3.6 จงตรวจสอบว่า 30,031 เป็นจำนวนเฉพาะหรือไม่

ตัวอย่าง 4.3.7 จงหาจำนวนเฉพาะทั้งหมดที่หาร $150!$ ลงตัว

ในปี ค.ศ. 1940 แฟร์มาต์ได้ศึกษาจำนวนเต็มที่อยู่ในรูปตามนิยามต่อไปนี้

บทนิยาม 4.3.8 จำนวนแฟร์มาต์ (Fermat Numbers) คือจำนวนที่อยู่ในรูป

$$F_n = 2^{2^n} + 1 \qquad \text{เมื่อ } n \geq 0$$

ตัวอย่างเช่น

$$F_0 = 3 \qquad F_1 = 5 \qquad F_2 = 17 \qquad F_3 = 257 \qquad F_4 = 65537$$

ทั้ง 5 จำนวนล้วนเป็นจำนวนเฉพาะแฟร์มาต์คาดเดาว่าจำนวนต่อ ๆ น่าจะเป็นจำนวนเฉพาะ ต่อมาในปี ค.ศ. 1732 ออยเลอร์พบว่า $F_5 = 4294967297 = 641 \cdot 6700417$ ทำให้คำกล่าวของแฟร์มาต์เป็นเท็จ ดังนั้นถ้า F_n เป็นจำนวนเฉพาะ จะเรียก F_n ว่า **จำนวนเฉพาะแฟร์มาต์ (Fermat prime)** และในปี ค.ศ. 1878 ลูคัส นักคณิตศาสตร์ชาวฝรั่งเศสได้พิสูจน์ว่า

$$F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 274177 \cdot 67280421310721$$

ดังนั้น F_6 เป็นจำนวนประกอบ จากการศึกษาพบว่าจำนวนแฟร์มาต์ F_n เป็นจำนวนประกอบสำหรับ $5 \leq n \leq 50$ อย่างไรก็ตามยังไม่มีผู้ใดพิสูจน์ได้ว่าจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ที่สามารถเขียนในรูป $2^{2^n} + 1$ หรือไม่ และก็ยังไม่มีผู้ใดพบจำนวนเฉพาะของแฟร์มาต์ตัวอื่น ๆ

ทฤษฎีบท 4.3.9 สำหรับ $m > n$ แล้ว $\gcd(F_m, F_n) = 1$

มาริน แมร์เซน บาทหลวงชาวฝรั่งเศส นักคณิตศาสตร์คนหนึ่งที่สนใจในการสร้างลำดับของจำนวนเฉพาะโดยสนใจจำนวนเต็มที่อยู่ในรูปแบบดังนิยามต่อไปนี้

บทนิยาม 4.3.10 จำนวนมาร์เซน (Mersenne Numbers) คือจำนวนที่อยู่ในรูป

$$M_n = 2^n - 1 \qquad \text{เมื่อ } n \in \mathbb{N}$$

ตัวอย่างเช่น

$$M_1 = 1 \qquad M_2 = 3 \qquad M_3 = 7 \qquad M_4 = 15 \qquad M_5 = 31$$

ถ้า M_n เป็นจำนวนเฉพาะ เราจะเรียก M_n ว่า **จำนวนเฉพาะแมร์เซน (Mersenne prime)**

ทฤษฎีบท 4.3.11 ถ้า M_n เป็นจำนวนเฉพาะ แล้ว n เป็นจำนวนเฉพาะ

จากทฤษฎีบทดังกล่าวจะได้ว่าจำนวน M_p เป็นจำนวนเฉพาะของแมร์เซนได้ ก็ต่อเมื่อ มีจำนวนเฉพาะ p ที่ทำให้ M_p เป็นจำนวนเฉพาะเช่น

$$M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127,\ M_{13} = 8191$$

แมร์เซนได้ตั้งข้อคาดการณ์ไว้ว่า M_p เป็นจำนวนเฉพาะเมื่อ $p =$ 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 และ 257 เท่านั้น และเป็นจำนวนประกอบสำหรับจำนวนเฉพาะ p อื่น ๆ ที่น้อยกว่า 257 ใน ค.ศ. 1876 ลูคัส ได้พิสูจน์ว่า M_{67} เป็นจำนวนประกอบแต่ไม่สามารถแยกตัวประกอบออกมาได้ ในปี ค.ศ. 1903 โคล ได้คำนวณออกมาเป็นผลคูณดังนี้

$$2^{67} - 1 = (193707721)(761838257287)$$

ในปี ค.ศ.2001 พบว่า $M_{13466917}$ เป็นจำนวนเฉพาะแมร์เซนที่มีค่ามากสุด ปัญหาที่น่าสนใจคือ จำนวนเฉพาะ $M_p = 2^p - 1$ มีอยู่จำนวนอนันต์หรือไม่ ซึ่งปัญหานี้ยังไม่มีใครตอบคำถามได้

แบบฝึกหัด 4.3

1. จงตรวจสอบว่าจำนวนต่อไปนี้เป็นจำนวนเฉพาะหรือไม่

1.1 1003	1.3 1117	1.5 5139	1.7 8009
1.2 1007	1.4 2111	1.6 10001	1.8 77777

2. $2^{19}-1$ เป็นจำนวนเฉพาะหรือไม่
3. $25!+1$ เป็นจำนวนเฉพาะหรือไม่
4. $4^{545}+545^4$ เป็นจำนวนเฉพาะหรือไม่
5. จงตรวจสอบว่า M_{13}, M_{19} และ M_{23} เป็นจำนวนเฉพาะหรือไม่
6. จงหาจำนวนเฉพาะที่เขียนในรูป $3k+3$ มา 20 จำนวน
7. จงหาจำนวนเฉพาะที่เขียนในรูป $6k+5$ มา 20 จำนวน
8. จงหาจำนวนเฉพาะที่เขียนในรูป k^2+k+41 มา 20 จำนวน
9. จงหาจำนวนเฉพาะที่เขียนในรูป $k^2-79k+160$ มา 20 จำนวน
10. มีจำนวนเต็ม n ซึ่ง $6<n<20$ จำนวนใดบ้างที่ทำให้ n^2+1 เป็นจำนวนเฉพาะบ้าง
11. จงแสดงว่า จำนวนเฉพาะที่เขียนในรูป $8n+5$ มีจำนวนอนันต์
12. จงแสดงว่า ถ้า p และ p^2+8 เป็นจำนวนเฉพาะ แล้ว p^3+4 เป็นจำนวนเฉพาะ
13. จงแสดงว่า ถ้า p, $p+2$ และ $p+4$ เป็นจำนวนเฉพาะทุกตัว แล้ว $p=3$
14. จงแสดงว่า ถ้า p และ $p+2$ เป็นจำนวนเฉพาะทั้งคู่ (จำนวนเฉพาะคู่แฝด) และ $p(p+2)+2$ เป็นจำนวนเฉพาะ แล้ว $p=3$
15. จงแสดงว่า ถ้า p และ $p+2$ เป็นจำนวนเฉพาะคู่แฝดที่ $p>3$ แล้วผลบวกของจำนวนเฉพาะคู่แฝดนี้หารด้วย 12 ลงตัว
16. สำหรับ $n\geq 1$ จงแสดงว่า $\gcd(F_n,n)=1$
17. จงแสดงว่า จำนวนเต็มที่เขียนในรูป F_n+4 เป็นจำนวนประกอบ
18. จงพิสูจน์ว่า ถ้า p และ $2p+1$ เป็นจำนวนเฉพาะ แล้ว $(2p+1)\mid M_p$ หรือ $(2p+1)\mid(M_p+2)$

บทที่ 5

สมภาค

ใน ค.ศ. 1801 คาร์ส ฟรีดริค เกาส์ (Carl Friedrich Gauss ค.ศ.1777–1855) นักคณิตศาสตร์ชาวเยอรมัน ได้เสนอแนวคิดที่เรียกว่า สมภาค (congruence) ซึ่งแนวคิดดังกล่าวปรากฏในหนังสือของเขาชื่อ Disquisitones Arithmeticae ในขณะที่เขามีอายุเพียง 24 ปี จนกลายเป็นเครื่องมือสำคัญเกี่ยวกับทฤษฎีจำนวน

5.1 นิยามและสมบัติของสมภาค

บทนิยาม 5.1.1 ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก
จะกล่าวว่า a และ b **สมภาคกัน (congruent) มอดุโล (modulo)** m หรือ a สมภาคกับ b มอดุโล m เขียนแทนด้วย $a \equiv b \pmod{m}$ นิยามโดย

$$a \equiv b \pmod{m} \qquad \text{ก็ต่อเมื่อ} \qquad m \mid (b-a)$$

a ไม่สมภาคกับ b มอดุโล m เขียนแทนด้วย $a \not\equiv b \pmod{m}$

ข้อสังเกต 5.1.2 ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จะได้ว่า

1. $a \not\equiv b \pmod{m}$ ก็ต่อเมื่อ $m \nmid (b-a)$
2. $a \equiv b \pmod{1}$
3. $a \equiv a \pmod{m}$

ตัวอย่าง 5.1.3 จงให้เหตุผลเกี่ยวกับการสมภาคต่อไปนี้

1. $2 \equiv 5 \pmod{3}$ เพราะว่า
2. $-3 \equiv 7 \pmod{5}$ เพราะว่า
3. $-15 \equiv -3 \pmod{6}$ เพราะว่า
4. $5 \not\equiv 7 \pmod{3}$ เพราะว่า

ทฤษฎีบท 5.1.4 ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก แล้ว

$a \equiv b \pmod{m}$ ก็ต่อเมื่อ a และ b มีเศษเหลือจากการหารด้วย m เท่ากัน

ตัวอย่าง 5.1.5 จงให้เหตุผลสมภาคต่อไปนี้

1. $123 \equiv 192 \pmod{3}$ เพราะว่า
2. $-124 \not\equiv 77 \pmod{5}$ เพราะว่า
3. $687 \equiv 176 \pmod{7}$ เพราะว่า
4. $557 \equiv 718 \pmod{3}$ เพราะว่า

ทฤษฎีบท 5.1.6 ให้ a, b, c เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก แล้ว

1. $a \equiv a \pmod{m}$ สมบัติสะท้อน (Reflexive law)
2. ถ้า $a \equiv b \pmod{m}$ แล้ว $b \equiv a \pmod{m}$ สมบัติสมมาตร (Symmetric law)
3. ถ้า $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$ แล้ว $a \equiv c \pmod{m}$

   สมบัติถ่ายทอด (Transitive law)

ทฤษฎีบท 5.1.7 ให้ a, b, c, d เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ แล้ว

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$

ทฤษฎีบท 5.1.8 ให้ a, b, c เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก ถ้า $a \equiv b \pmod{m}$ แล้ว

1. ถ้า $a \equiv b \pmod{m}$ แล้ว $a + c \equiv b + c \pmod{m}$
2. ถ้า $a \equiv b \pmod{m}$ แล้ว $ac \equiv bc \pmod{m}$

ตัวอย่าง 5.1.9 ให้ a, b, c, d, x, y เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จงแสดงว่า

ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ แล้ว $ax + cy \equiv bx + dy \pmod{m}$

ทฤษฎีบท 5.1.10 ให้ a, b เป็นจำนวนเต็ม และ m, k เป็นจำนวนเต็มบวก แล้ว

$$\text{ถ้า} \quad a \equiv b \pmod{m} \quad \text{แล้ว} \quad a^k \equiv b^k \pmod{m}$$

ตัวอย่าง 5.1.11 จงแสดงว่า 41 หาร $2^{20} - 1$ ลงตัว

ตัวอย่าง 5.1.12 จงหาเศษที่เกิดจากการหาร

1. 8 หาร 3^{10}

2. 23 หาร 2^{13}

3. 51 หาร 7^{20}

ตัวอย่าง 5.1.13 จงหาเศษที่เกิดจากการหาร

1. 51 หาร 3^{10}
2. 51 หาร 21^{10}

ตัวอย่าง 5.1.14 จงหาเลขโดดหลักสุดท้ายของ 3^{4000}

ตัวอย่าง 5.1.15 จงแสดงว่า $4^n \equiv 1 + 3n \pmod 9$ ทุกจำนวนเต็มบวก n

ทฤษฎีบท 5.1.16 ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จะได้ว่า

$$\text{ถ้า } a \equiv b \pmod{m} \text{ แล้ว } \gcd(a, m) = \gcd(b, m)$$

ทฤษฎีบท 5.1.17 ให้ $a, b, n \in \mathbb{Z}$ และ m เป็นจำนวนเต็มบวก ซึ่ง $d = \gcd(m, n)$ จะได้ว่า

$$an \equiv bn \pmod{m} \quad \text{ก็ต่อเมื่อ} \quad a \equiv b \left(\mod \frac{m}{d}\right)$$

บทแทรก 5.1.18 ให้ a, b, p เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จะได้ว่า

1. ถ้า $an \equiv bn \pmod{m}$ และ $\gcd(m, n) = 1$ แล้ว $a \equiv b \pmod{m}$
2. ถ้า $an \equiv bn \pmod{p}$ และ p เป็นจำนวนเฉพาะที่ $p \nmid n$ แล้ว $a \equiv b \pmod{p}$

ทฤษฎีบท 5.1.19 ให้ a, b เป็นจำนวนเต็ม และ m_1, m_2 เป็นจำนวนเต็มบวก จะได้ว่า

1. ถ้า $a \equiv b \pmod{m_1}$ และ $a \equiv b \pmod{m_2}$ แล้ว $a \equiv b \pmod{\ell\text{cm}(m_1, m_2)}$
2. ถ้า $a \equiv b \pmod{m_1}$ และ $a \equiv b \pmod{m_2}$ และ $\gcd(m_1, m_2) = 1$ แล้ว $a \equiv b \pmod{m_1 m_2}$

ตัวอย่าง 5.1.20 จงหาเลขโดดหลักสุดท้ายของ 3^{4000}

ตัวอย่าง 5.1.21 จงหาเลขโดดสองหลักสุดท้ายของ 3^{4000}

ทฤษฎีบท 5.1.22 ให้ a, b เป็นจำนวนเต็ม และ $m_1, m_2, ..., m_k$ เป็นจำนวนเต็มบวก จะได้ว่า

1. ถ้า $a \equiv b \pmod{m_i}$ $i = 1, 2, ..., k$ แล้ว $a \equiv b \pmod{\ell\text{cm}(m_1, m_2, ..., m_k)}$
2. ถ้า $a \equiv b \pmod{m_1}$ และ $m_1, m_2, ..., m_k$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แล้ว $a \equiv b \pmod{m_1 m_2 \cdots m_k}$

ทฤษฎีบท 5.1.23 ทุก ๆ จำนวนเต็ม a จะมีจำนวนเต็ม r เพียงตัวเดียวที่ $0 \leq r < m$ เมื่อ m เป็นจำนวนเต็มบวก และ

$$a \equiv r \pmod{m}$$

บทนิยาม 5.1.24 ถ้า $a \equiv b \pmod{m}$ จะเรียก b ว่าเป็น**ส่วนตกค้าง (residue)** ของ a มอดุโล m เซตของ

$$\{a_1, a_2, ..., a_m\}$$

จะเป็น**ระบบส่วนตกค้างบริบูรณ์ (complete residue system)** มอดุโล m ก็ต่อเมื่อ ทุก ๆ จำนวนเต็ม a จะมี a_i เพียงตัวเดียวที่ทำให้ $a \equiv a_i \pmod{m}$ ชั้นสมมูลของ a_i คือ

$$\{a : a \in \mathbb{Z}, a \equiv a_i \pmod{m}\}$$

จะเรียกว่า **ชั้นส่วนตกค้าง (residue class)** ของ a_i มอดุโล m

ตัวอย่าง 5.1.25 จงหาส่วนตกค้างของ 5 มอดุโล 7 ทั้งหมดที่เป็นไปได้

ตัวอย่าง 5.1.26 จงหาระบบส่วนตกค้างบริบูรณ์มอดุโล 3

ข้อสังเกต 5.1.27 จากการสังเกตจะได้ว่า

1. ถ้า $\{a_1, a_2, ..., a_m\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m
   ก็ต่อเมื่อ ทุก ๆ $i \neq j \quad a_i \not\equiv a_j \pmod{m}$
2. ถ้า $\{a_1, a_2, ..., a_m\}$ และ $\{b_1, b_2, ..., b_m\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m
   แล้วจะได้ว่าทุก ๆ a_i จะมี b_j เพียงตัวเดียวที่ทำให้ $a_i \equiv b_j \pmod{m}$

ตัวอย่าง 5.1.28 จงตรวจสอบว่าจงหาเซตต่อไปนี้ระบบส่วนตกค้างบริบูรณ์มอดุโล 5 หรือไม่

1. $\{-1, 5, 6, 7, 8\}$

2. $\{-11, -3, 18, 16, 22\}$

3. $\{8, -2, 6, 12, 1\}$

บทนิยาม 5.1.29 เราจะเรียกเป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m

$$\{0, 1, 2, ..., m-1\}$$

ว่า**ระบบส่วนตกค้างบริบูรณ์ที่ไม่เป็นค่าลบน้อยสุด** (least non–negative complete residue system) มอดุโล m

ตัวอย่างเช่น $\{0, 1, 2, 3, 4, 5, 6\}$ เป็นระบบส่วนตกค้างบริบูรณ์ที่ไม่เป็นค่าลบน้อยสุด มอดุโล 7

ทฤษฎีบท 5.1.30 $\{a_1, a_2, ..., a_m\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m และ $\gcd(c, m) = 1$
จะได้ว่า $\{ca_1, ca_2, ..., ca_m\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m

แบบฝึกหัด 5.1

1. จงหาเลขโดดหลักสุดท้ายของ 3^{400}
2. จงหาเศษเหลือที่เกิดจากการหาร 97^{104} ด้วย 105
3. จงหาเศษเหลือที่เกิดจากการหาร 10^{49} ด้วย 7
4. จงหาเศษเหลือที่เกิดจากการหาร $36^{36} + 41^{41}$ ด้วย 77
5. จงหาเศษเหลือที่เกิดจากการหาร $1^5 + 2^5 + 3^5 + \cdots + 99^5$ ด้วย 4
6. จงแสดงการหารลงตัวต่อไปนี้ โดยใช้สมภาค

   6.1 $44 \mid (19^{19} + 69^{19})$

   6.2 $13 \mid (2^{70} + 3^{70})$

   6.3 $7 \mid (9^{50} - 4)$

   6.4 $13 \mid (5^{36} - 1)$

   6.5 $19 \mid (17^{75} + 8)$

   6.6 $11 \cdot 31 \cdot 61 \mid (20^{15} - 1)$

7. จงแสดงว่า $42 \mid (n^7 - n)$ ทุกจำนวนเต็มบวก n
8. จงแสดงว่า $19 \nmid (4n^2 + 4)$ ทุกจำนวนเต็ม n
9. จงแสดงว่า สำหรับจำนวนเต็มบวก n ใด ๆ $11 \mid (2^{4n+3} + 5^{n+2})$ โดยใช้สมภาค
10. จงแสดงว่า สำหรับจำนวนเต็ม n ใด ๆ ถ้า $\gcd(n, 7) = 1$ แล้ว $7 \mid (n^2 - 1)$
11. จงแสดงว่า สำหรับจำนวนเต็มบวกคี่ n ใด $1 + 2 + 3 + \cdots + (n-1) \equiv 0 \pmod{n}$
12. ให้ a, b, m เป็นจำนวนเต็ม จงพิสูจน์ว่า ถ้า $a \equiv b \pmod{m}$ แล้ว $\gcd(a, m) = \gcd(b, m)$
13. จงพิสูจน์ว่า ถ้า $a \equiv 2 \pmod{4}$ จะไม่มีจำนวนเต็ม b และ $m > 1$ ที่ $a = b^m$
14. จงหาเศษเหลือที่เกิดจากการหาร $2^{1000000}$ ด้วย 17
15. จงหาเศษเหลือที่เกิดจากการหาร $10^{10} + 10^{10^2} + 10^{10^3} + \cdots + 10^{10^{10}}$ ด้วย 7
16. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะคี่ แล้ว $2(p-3)! \equiv -1 \pmod{p}$
17. จงแสดงว่า $11^{320} - 1$ หารด้วย 17 ลงตัว
18. จงแสดงว่า $36^{36} + 41^{41}$ หารด้วย 77 ลงตัว
19. จงแสดงว่า $19^{19} + 69^{19}$ หารด้วย 44 ลงตัว
20. จงแสดงว่า $2^{70} + 3^{70}$ หารด้วย 13 ลงตัว
21. จงแสดงว่า 97^{104} หารด้วย 105 เศษเหลือเป็น 1
22. จงแสดงว่า $20^{15} - 1$ หารด้วย $11 \cdot 31 \cdot 61$ ลงตัว

23. จงแสดงว่า $561 \mid (2^{561} - 2)$ และ $561 \mid (2^{561} - 3)$
24. จงแสดงว่า $1835^{1910} + 1986^{2061} \equiv 0 \pmod 7$
25. จงแสดงว่า $2222^{5555} + 5555^{2222} \equiv 0 \pmod 7$
26. จงหาเลขโดดสามหลักสุดท้ายของ 13^{398}
27. จงหาเลขโดดสามหลักสุดท้ายของ 7^{999}
28. จงหาเลขโดดสองหลักสุดท้ายของ 9^{9^9}
29. จงหาเลขโดดสามหลักสุดท้ายของ F_{13}
30. จงหาเลขโดดสามหลักสุดท้ายของ 13^{398}
31. จงพิจารณาว่า $2^{117} - 2$ หารด้วย 117 ลงตัวหรือไม่
32. จงแสดงว่า $13 \mid (2^{4n+1} - 5 \cdot 3^{n+1})$ ทุก ๆ $n \in \mathbb{N}$ โดยใช้สมภาค
33. จงแสดงว่า $7^{4n} \equiv 1 + 2400n \pmod{1000}$ ทุก ๆ $n \in \mathbb{N}$ โดยใช้อุปนัยเชิงคณิตศาสตร์

5.2 สมการสมภาคเชิงเส้น

พิจารณาจำนวนเต็ม x ที่สอดคล้องสมการสมภาค

$$6x \equiv 4 \pmod{8}$$

จะได้ว่า $6x = 4 + 8k$ เมื่อ $k \in \mathbb{Z}$ นั่นคือ

$$x = \frac{4+8k}{6} = \frac{2+4k}{3}$$

มีเขียนคำตอบบางส่วน ดังตารางต่อไปนี้

k	x
−11	−14
−5	−6
1	2
7	10
13	18

k	x
−8	−10
−2	−2
4	6
10	14
16	22

สำหรับคำตอบในระบบส่วนตกค้างบริบูรณ์มอดุโล 8 จะได้คำตอบคือ $x = 2, 6$ ซึ่งเรียกว่า **คำตอบที่ไม่สมภาคกันในมอดุโล 8**

ให้ a, b เป็นจำนวนเต็ม และ m จำนวนเต็มบวก แล้ว

$$ax \equiv b \pmod{m}$$

เรียกว่า **สมการสมภาคเชิงเส้น (linear congruence equation)** ในหัวข้อนี้สนใจคำตอบของสมการที่ไม่สมภาคกันในมอดุโล m มีวิธีการหาผลเฉลยดังทฤษฎีบทต่อไปนี้

ตัวอย่าง 5.2.1 คำตอบของสมการ $7x \equiv 5 \pmod{11}$ ที่ไม่สมภาคกันในมอดุโล 11

ทฤษฎีบท 5.2.2 ให้ a, b เป็นจำนวนเต็ม และ m จำนวนเต็มบวก และ gcd$(a, m) = d$ จะได้ว่า

สมการสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ มีคำตอบ $x \in \mathbb{Z}$ ก็ต่อเมื่อ $d \mid b$

ถ้า $d \mid b$ จะมีคำตอบอยู่ d คำตอบที่ไม่สมภาคกันในมอดุโล m และคำตอบนั่นคือ

$$x \equiv x_0 + t\frac{m}{d} \pmod{m} \qquad \text{เมื่อ} \quad t = 0, 1, 2, ..., d-1$$

โดยที่ x_0 คือคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right)$

จากทฤษฎีบท 5.2.2 พบว่า

1. ถ้า $d \nmid b$ สมการสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ ไม่มีคำตอบ
2. ถ้า $d \mid b$ สมการสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ มีอยู่ d คำตอบที่ไม่สมภาคกันในมอดุโล m
3. ถ้า $d = 1$ แล้วสมการ $ax \equiv b \pmod{m}$ มีเพียงคำตอบเดียวที่ไม่สมภาคกันในมอดุโล m หรือกล่าวได้อีกนัยว่า ถ้า x_1 และ x_2 เป็นคำตอบของสมการ $ax \equiv b \pmod{m}$ แล้ว $x_1 \equiv x_2 \pmod{m}$
4. ถ้า x_0 เป็นคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv 1 \pmod{\frac{m}{d}}$ แล้ว $x_1 = \frac{b}{d}x_0$ จะเป็นคำตอบของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

ตัวอย่าง 5.2.3 จงหาคำตอบของสมการสมภาคเชิงเส้นต่อไปนี้

1. $9x \equiv 21 \pmod{30}$

2. $14x \equiv 15 \pmod{28}$

3. $18x \equiv 30 \pmod{42}$

ตัวอย่าง 5.2.4 จงหาคำตอบของสมการสมภาคเชิงเส้นต่อไปนี้

1. $6x \equiv 21 \pmod{39}$

2. $39x \equiv 65 \pmod{52}$

ตัวอย่าง 5.2.5 จงหาคำตอบที่ไม่สมภาคกัน ของสมการสมภาคเชิงเส้น $91x \equiv 98 \pmod{119}$

ตัวอย่าง 5.2.6 โรงงานผลิตเสื้อยืดแห่งหนึ่งพบว่าเมื่อแบ่งจำนวนเสื้อยืดคอกลมออกเป็น 102 กอง จะเหลือเสื้อยืดคอกลมจำนวน 12 ตัว ถ้าจำนวนเสื้อยืดคอกลมมีจำนวนเป็น 36 เท่าของเสื้อยืดคอวี พบว่าจำนวนเสื้อยืดคอวีมีมากกว่า 80 ตัว แต่ไม่เกิน 100 ตัว จงหาจำนวนเสื้อยืดคอวีและคอกลม

ตัวอย่าง 5.2.7 ณ โรงเรียนแห่งหนึ่ง ครูประจำชั้นให้ แก้ว และกล้า ซึ่งเป็นนักเรียนในห้อง นับเหรียญที่ได้จากการบริจาคเพื่อช่วยเหลือผู้ประสบภัยน้ำท่วมของเพื่อน ๆ ในชั้นเรียน จากการนับพบว่า เมื่อแบ่งเหรียญบาทออกเป็น 35 กอง จะเหลือ 14 เหรียญ

- แก้วกล่าวว่า "จำนวนเหรียญบาท เป็น 15 เท่าของจำนวนเหรียญสิบ"
- กล้ากล่าวว่า "จำนวนเหรียญบาท เป็น 21 เท่าของจำนวนเหรียญสิบ"

ครูประจำชั้นจะตรวจสอบได้อย่างไรว่านักเรียนคนใดกล่าวถูกต้อง

แบบฝึกหัด 5.2

1. จงเซตคำตอบของ x ที่สอดคล้อง

   1.1 $20x \equiv 45 \pmod 5$

   1.2 $20x \equiv 30 \pmod 4$

   1.3 $15x \equiv 25 \pmod{35}$

   1.4 $15x \equiv 24 \pmod{35}$

   1.5 $15x \equiv 0 \pmod{35}$

   1.6 $39x \equiv 65 \pmod{52}$

   1.7 $20x \equiv 4 \pmod{30}$

   1.8 $335x \equiv 254 \pmod{400}$

2. จงหาคำตอบทั้งหมดของสมการสมภาค

   2.1 $20x \equiv 4 \pmod{30}$

   2.2 $20x \equiv 3 \pmod 4$

   2.3 $353x \equiv 254 \pmod{400}$

3. ถ้า p เป็นจำนวนเฉพาะ จงพิสูจน์ว่า สำหรับทุกจำนวนเต็ม x ใดๆ

   $$x^2 \equiv x \pmod p \qquad \text{ก็ต่อเมื่อ} \qquad x \equiv 0 \pmod p \quad \text{หรือ} \quad x \equiv 1 \pmod p$$

4. จงหาจำนวนเต็มบวกที่น้อยที่สุดที่สอดคล้องสมการ $49x \equiv 23 \pmod{55}$

5.3 ทฤษฎีบทเศษเหลือของจีน

คำถามหนึ่งที่มักได้ยินบ่อยครั้งในเรื่องการหารคือ มีจำนวนเต็มอะไรเมื่อหารด้วย 4 เศษเหลือเป็น 3 และหารด้วย 5 เศษเหลือเป็น 4 คำถามนี้คือจำนวนเต็ม x ที่สอดคล้องระบบสมการสมภาค

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

นั่นคือต้องหา x ที่สอดคล้อง $x = 3 + 4t$ และ $x = 4 + 5s$ เมื่อ $t, s \in \mathbb{Z}$ เมื่อพิจารณาแล้วจะได้ $x = 79$ เมื่อ $t = 19$ และ $s = 15$ ให้ z เป็นคำตอบของระบบสมการจะได้ว่า

$$z \equiv 79 \pmod 4 \qquad \text{และ} \qquad z \equiv 79 \pmod 5$$

เนื่องจาก $\gcd(4, 5) = 1$ ดังนั้น $z \equiv 79 \pmod{20}$ คำตอบของระบบสมการนี้คือ

$$79 + 20k, \qquad k \in \mathbb{Z}$$

จากตัวอย่างที่กล่าวมาเริ่มต้นหา $x = 79$ ที่สอดคล้องระบบสมการโดยการแทนค่า t และ s จนกว่าจะได้ค่า x ที่เท่ากันคือ 79 ซึ่งมีความยุ่งยาก ในหัวข้อนี้จะนำเสนอวิธีการในหาคำตอบของระบบสมการสมภาค เริ่มต้นพิจารณาระบบสมการสมภาค

$$\begin{aligned} nx &\equiv 1 \pmod m \\ mx &\equiv 1 \pmod n \end{aligned}$$

ให้ $m, n \in \mathbb{N}$ และ $\gcd(m, n) = 1$ ขั้นแรกให้ x_1 และ x_2 เป็นคำของระบบสมการ $nx \equiv 1 \pmod m$ และ $mx \equiv 1 \pmod n$ ตามลำดับ สำหรับทุก ๆ จำนวนเต็ม a, b จะได้ว่า

$$\begin{aligned} nx_1a &\equiv a \pmod m \\ mx_2b &\equiv b \pmod n \end{aligned}$$

นั่นคือ x_1a และ x_2b เป็นคำตอบของระบบสมการ

$$\begin{aligned} nx &\equiv a \pmod m \\ mx &\equiv b \pmod n \end{aligned}$$

ให้ $x_0 = nx_1a + mx_2b$ จะได้ว่า

$$\begin{aligned} x_0 = nx_1a + mx_2b \equiv nx_1a + 0 \equiv a \pmod m \\ x_0 = nx_1a + mx_2b \equiv 0 + mx_2b \equiv b \pmod n \end{aligned}$$

นี้คือการแสดงว่า $x_0 = nx_1a + mx_2b$ เป็นคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod n \end{aligned}$$

พิสูจน์เบื้องต้นทำให้ได้ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 5.3.1 ให้ $m, n \in \mathbb{N}$ และ $\gcd(m, n) = 1$ จะได้ว่าระบบสมการ

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

มีคำตอบของระบบสมการเพียงคำตอบเดียวในมอดุโล mn กล่าวคือ จะมี $x_0 \in \mathbb{Z}$ ซึ่ง $x_0 \equiv a \pmod{m}$ และ $x_0 \equiv b \pmod{n}$ และถ้า x_1 และ x_2 เป็นคำตอบของระบบแล้ว $x_1 \equiv x_2 \pmod{mn}$

เมื่อย้อนกลับไปหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

เห็นได้ว่า $\gcd(4, 5) = 1$ ให้ $a = 3, b = 4, m = 4, n = 5$ พิจารณาระบบสมการ

$$\begin{aligned} 5x &\equiv 1 \pmod{4} \\ 4x &\equiv 1 \pmod{5} \end{aligned}$$

จะได้ว่า $x_1 = 1$ และ $x_2 = 4$ เป็นคำของระบบสมการ $5x \equiv 1 \pmod{4}$ และ $4x \equiv 1 \pmod{5}$ ตามลำดับ แล้ว

$$x_0 = nx_1a + mx_2b = 5(1)(3) + 4(4)(4) = 79$$

ดังนั้นคำตอบของระบบสมการนี้คือ $x \equiv 79 \pmod{20}$ นั่นคือ

$$79 + 20t, \qquad t \in \mathbb{Z}$$

ตัวอย่าง 5.3.2 จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv 5 \pmod{9} \end{aligned}$$

ตัวอย่าง 5.3.3 จงหาจำนวนเต็มเมื่อหารด้วย 6 เศษเหลือเท่ากับ 3 และหารด้วย 11 เศษเหลือเท่ากับ 5

ตัวอย่าง 5.3.4 จงหาคำตอบของระบบสมการ

$$\begin{aligned} 2x &\equiv 1 \pmod 5 \\ 3x &\equiv 5 \pmod{11} \end{aligned}$$

ต่อไปจะพิจารณาในระบบสมการที่มากกว่า 2 สมการ เช่นจงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \end{aligned}$$

เมื่อ $\gcd(m_1, m_2) = \gcd(m_1, m_3) = \gcd(m_2, m_3) = 1$
ให้ $x_0 = m_2m_3x_1a_1 + m_1m_3x_2a_2 + m_1m_2x_3a_3$ สำหรับจำนวนเต็ม x_1, x_2, x_3 ใด ๆ จะได้ว่า

$$\begin{aligned} x_0 &\equiv m_2m_3x_1a_1 + 0 + 0 \pmod{m_1} \\ x_0 &\equiv 0 + m_1m_3x_2a_2 + 0 \pmod{m_2} \\ x_0 &\equiv 0 + 0 + m_1m_2x_3a_3 \pmod{m_3} \end{aligned}$$

ในการหาคำตอบของระบบสมการข้างต้นเลือก x_1, x_2, x_3 ที่สอดคล้องสมการ

$$\begin{aligned} m_2m_3x &\equiv a_1 \pmod{m_1} \\ m_1m_3x &\equiv a_2 \pmod{m_2} \\ m_1m_2x &\equiv a_3 \pmod{m_3} \end{aligned}$$

ถ้า x_1, x_2 เป็นคำตอบของระบบสมการ จะได้ว่า $x_1 \equiv x_2 \pmod{m_1m_2m_3}$

ตัวอย่าง 5.3.5 จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 5 \pmod{4} \\ x &\equiv 4 \pmod{7} \end{aligned}$$

ทฤษฎีบทต่อไปนี้จะกล่าวถึงการหาคำตอบของระบบสมการสมภาคที่ประกอบด้วย k สมการซึ่งมีแนวคิดคล้ายกับกรณี 2 และ 3 สมการ ซึ่งจะเรียกว่า **ทฤษฎีบทเศษเหลือของจีน (Chinese Remainder Theorem)** เขียนโดยย่อว่า CRT เหตุที่เรียกเช่นนี้ก็เพราะว่าชาวจีนได้ใช้ความรู้ที่คล้ายทฤษฎีบทดังกล่าวตั้งแต่คริสตศวรรษที่ 1 และหลังจากนั้นชาวจีนได้นำไปเผยแพร่ในยุโรป โดยเขียนเป็นภาษาจีนในการนำไปเผยแพร่ครั้งแรก

ทฤษฎีบท 5.3.6 ทฤษฎีบทเศษเหลือของจีน (Chinese Remainder Theorem)
ให้ $m_1, m_2, ..., m_k$ เป็นจำนวนเต็มบวกซึ่ง $\gcd(m_i, m_j) = 1$ สำหรับ $i \neq j$
จะได้ว่าระบบสมการสมภาค

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

มีคำตอบของระบบสมการเพียงคำตอบเดียวในมอดุโล $m = m_1m_2m_3...m_k$ กล่าวคือจะมี $x_0 \in \mathbb{Z}$ ซึ่ง $x_0 \equiv a_i \pmod{m_i}$ ทุก $i = 1, 2, ..., k$ ถ้า x_1 และ x_2 เป็นคำตอบของสมการ $x_1 \equiv x_2 \pmod{m}$

ตัวอย่าง 5.3.7 จงหาจำนวนเต็มเมื่อหารด้วย 5 เศษเหลือเท่ากับ 4 หารด้วย 6 เศษเหลือเท่ากับ 5 และหารด้วย 7 เศษเหลือเท่ากับ 6

ตัวอย่าง 5.3.8 จงหาคำตอบของสมการสมภาค $17x \equiv 9 \pmod{276}$

ทฤษฎีบทต่อไปนี้จะเป็นเครื่องมือในการหาคำตอบของระบบสมการสมภาคในกรณีทั่วไป โดยเริ่มต้นจากระบบสมการที่มี 2 สมการดังนี้

ทฤษฎีบท 5.3.9 ให้ m_1, m_2 เป็นจำนวนเต็มบวกและ $a_1, a_2 \in \mathbb{Z}$ จะได้ระบบสมการสมภาค

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

มีคำตอบ ก็ต่อเมื่อ $\gcd(m_1, m_2) \mid (a_1 - a_2)$
และถ้ามีคำตอบแล้ว จะมีคำตอบเพียงคำตอบเดียวในมอดุโล $m = \ell\text{cm}(m_1, m_2)$

ตัวอย่าง 5.3.10 จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 11 \pmod{16} \\ x &\equiv 5 \pmod{20} \end{aligned}$$

ตัวอย่าง 5.3.11 จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 13 \pmod{15} \\ x &\equiv 7 \pmod{21} \end{aligned}$$

ทฤษฎีบท 5.3.12 ให้ $m_1, m_2, ..., m_k$ เป็นจำนวนเต็มบวกและ $a_1, a_2, ..., a_k \in \mathbb{Z}$ จะได้ว่าระบบสมการสมภาค

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

มีคำตอบ ก็ต่อเมื่อ $\gcd(m_i, m_j) \mid (a_i - a_j)$ สำหรับทุก $i, j \in \{1, 2, ..., k\}$ และถ้ามีคำตอบแล้ว จะมีคำตอบเพียงคำตอบเดียวในมอดุโล $\ell\text{cm}(m_1, m_2, ..., m_k)$

ตัวอย่าง 5.3.13 จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 11 \pmod{15} \\ x &\equiv 15 \pmod{20} \\ x &\equiv 2 \pmod{25} \end{aligned}$$

ตัวอย่าง 5.3.14 จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 5 \pmod{6} \\ x &\equiv 17 \pmod{21} \\ x &\equiv 3 \pmod{28} \end{aligned}$$

แบบฝึกหัด 5.3

1. จงหาคำตอบของระบบสมการสมภาคต่อไปนี้

   1.1
   $$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

   1.2
   $$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

2. จงหาคำตอบของระบบสมการ
   $$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

3. จงหาคำตอบของระบบสมการสมภาคต่อไปนี้

   3.1
   $$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 11 \pmod 9 \end{aligned}$$

   3.2
   $$\begin{aligned} x &\equiv 2 \pmod{15} \\ x &\equiv 8 \pmod{21} \end{aligned}$$

4. จงหาจำนวนเต็มบวก x ที่สอดคล้องสมการสมภาค $\begin{cases} x \equiv 16 \pmod{45} \\ x \equiv 7 \pmod{18} \\ x \equiv 1 \pmod{20} \end{cases}$

5. จงหาคำตอบของ $25x \equiv 37 \pmod{445}$

6. จงหาจำนวนเต็มบวกที่มีค่าน้อยสุดที่เมื่อหารด้วย 5, 6, 7 แล้วเศษเหลือเท่ากับ 1, 2, 3 ตามลำดับ

7. จงหาจำนวนเต็มทั้งหมดที่อยู่ระหว่าง 1,000 ถึง 2,000 ที่เมื่อหารด้วย 5, 7, 11 แล้วได้เศษเหลือ 1, 3, 5 ตามลำดับ

8. อายุของชายคนหนึ่งเมื่อหารด้วย 3 เศษเหลือคือ 2 เมื่อหารด้วย 4 เศษเหลือคือ 1 และเมื่อหารด้วย 5 เศษเหลือคือ 1 จงหาอายุของชายคนนี้

9. จงหาจำนวนเต็มบวกทั้งหมดที่หารด้วย 3, 4, 5 แล้วเศษเหลือเท่ากับ 1 หรือ 2

10. จงหาจำนวนเต็มบวกที่น้อยที่สุดเมื่อหารด้วย $12, 15$ และ 21 เศษเหลือ $10, 7$ และ 13 ตามลำดับ

5.4 ระบบส่วนตกค้างลดทอน

บทนิยาม 5.4.1 ระบบส่วนตกค้างลดทอน (reduced residue system) มอดุโล m คือเซตของจำนวนเต็มในระบบส่วนตกค้างบริบูรณ์ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ m

(ก) ระบบส่วนตกค้างลดทอนมอดุโล m ที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{0, 1, 2, ..., m-1\}$ คือ

$$\{k : 0 \leq k < m \text{ และ } \gcd(k, m) = 1\}$$

เรียกว่า **ระบบส่วนตกค้างลดทอนที่ไม่เป็นลบค่าน้อยสุด (least non–negative reduced residue system)** มอดุโล m

(ข) $\phi(m)$ แทนจำนวนสมาชิกของระบบส่วนตกค้างลดทอนมอดุโล m

ข้อสังเกต 5.4.2 จากนิยามข้างต้นจะได้ว่า

1. เซตของจำนวนเต็ม r_i เป็นระบบส่วนตกค้างลดทอนมอดุโล m ก็ต่อเมื่อ
   (1) $\gcd(r_i, m) = 1$ ทุก ๆ r_i
   (2) ถ้า $i \neq j$ แล้ว $r_i \not\equiv r_j \pmod{m}$
   (3) ถ้า $x \in \mathbb{Z}$ ที่ $\gcd(x, m) = 1$ แล้วมี r_i ที่ $x \equiv r_i \pmod{m}$
2. ระบบส่วนตกค้างลดทอนมอดุโล m ทุกระบบมีจำนวนสมาชิกเท่ากัน
3. $\phi(p) = p - 1$ เมื่อ p เป็นจำนวนเฉพาะ

ตัวอย่าง 5.4.3 จงยกตัวอย่างระบบส่วนตกค้างลดทอนมอดุโล 5 และ 8 มาอย่างน้อย 2 ระบบ

ต่อไปจะเป็นตัวอย่างของ $\phi(m)$

m	ระบบส่วนตกค้างลดทอนมอดุโล m	$\phi(m)$
1	$\{1\}$	1
2	$\{1\}$	1
3	$\{1,2\}$	2
4	$\{1,3\}$	2
5	$\{1,2,3,4\}$	4
6	$\{1,5\}$	2
7	$\{1,2,3,4,5,6\}$	6
8	$\{1,3,5,7\}$	4
9	$\{1,2,4,5,7,8\}$	6
10	$\{1,3,7,9\}$	4
20	$\{1,3,7,9,11,13,17,19\}$	8
50	$\{k \in \mathbb{Z} : 0 \leq k < 50, \gcd(k,50) = 1\}$	20
100	$\{k \in \mathbb{Z} : 0 \leq k < 100, \gcd(k,100) = 1\}$	40
1000	$\{k \in \mathbb{Z} : 0 \leq k < 1000, \gcd(k,1000) = 1\}$	400

วิธีการหาค่าของ $\phi(m)$ จะแสดงในหัวข้อ 6.4 บทที่ 6

ทฤษฎีบท 5.4.4 ถ้า $\{a_1, a_2, ..., a_{\phi(m)}\}$ เป็นเซตของจำนวนเต็มซึ่งทุก ๆ i, $\gcd(a_i, m) = 1$ และทุก ๆ $i \neq j$, $a_i \not\equiv a_j \pmod{m}$ แล้ว $\{a_1, a_2, ..., a_{\phi(m)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล m

ทฤษฎีบท 5.4.5 ให้ $\gcd(a, m) = 1$ และ $\{r_1, r_2, ..., r_{\phi(m)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล m จะได้ว่า

$$\{ar_1, ar_2, ..., ar_{\phi(m)}\}$$

เป็นระบบส่วนตกค้างลดทอนมอดุโล m

ทฤษฎีบท 5.4.6 ทฤษฎีบทของออยเลอร์ (Euler's Theorem)
ถ้า $a \in \mathbb{Z}$ และ $m \in \mathbb{N}$ ซึ่ง $\gcd(a, m) = 1$ แล้ว

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

ตัวอย่าง 5.4.7 100 หาร 3^{256} มีเศษเหลือเท่าใด

ตัวอย่าง 5.4.8 จงหาเลขโดดสามหลักสุดท้ายของ 7^{10000}

บทแทรก 5.4.9 ทฤษฎีบทของแฟร์มาต์ (Fermat's Little Theorem)
ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ โดยที่ $p \nmid a$ แล้ว

$$a^{p-1} \equiv 1 \pmod{p}$$

บทแทรก 5.4.10 ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ แล้ว

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

ตัวอย่าง 5.4.11 จงหาเศษเหลือที่เกิดจากการหาร 3^{1000} ด้วย 17

ตัวอย่าง 5.4.12 จงหาค่า a ที่ทำให้ $102^{1999} + 103^{1999} \equiv a \pmod{1999}$ เมื่อ $0 \leq a < 1999$

ทฤษฎีบท 5.4.13 ให้ p และ q เป็นจำนวนเฉพาะที่แตกต่างกัน และ $a \in \mathbb{Z}$

ถ้า $a^q \equiv a \pmod{p}$ และ $a^p \equiv a \pmod{q}$ แล้ว $a^{pq} \equiv a \pmod{pq}$

ตัวอย่าง 5.4.14 จงแสดงว่า $2^{340} \equiv 1 \pmod{341}$

ทฤษฎีบท 5.4.15 ให้ p เป็นจำนวนเฉพาะ จะได้

$$x^2 \equiv 1 \pmod{p} \qquad \text{ก็ต่อเมื่อ} \qquad x \equiv 1 \text{ หรือ } -1 \pmod{p}$$

ทฤษฎีบท 5.4.16 ทฤษฎีบทของวิลสัน (Wilson's Theorem)
ให้ p เป็นจำนวนเฉพาะ จะได้

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

ตัวอย่าง 5.4.17 จงหาเศษเหลือที่เกิดจากการหาร $15!$ ด้วย 17

ตัวอย่าง 5.4.18 จงแสดงว่า $18! \equiv -1 \pmod{437}$

ตัวอย่าง 5.4.19 จงหาเศษเหลือที่เกิดจากการหาร $2(26)!$ ด้วย 29

แบบฝึกหัด 5.4

1. ให้ a และ m เป็นจำนวนเต็มบวกที่ $\gcd(a,m)=1$ จงพิสูจน์ว่าสำหรับจำนวนเต็มบวก b

$$\{b, b+a, b+2a, ..., b+(m-1)a\}$$

เป็นระบบส่วนตกค้างบริบรูณ์มอดุโล m

2. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะคี่ แล้ว $2(p-3)! \equiv -1 \pmod{p}$
3. จงแสดงว่า $19^{19}+69^{19}$ หารด้วย 44 ลงตัว
4. จงแสดงว่า 97^{104} หารด้วย 105 เศษเหลือเป็น 1
5. จงแสดงว่า $2222^{5555}+5555^{2222} \equiv 0 \pmod{7}$
6. จงหาเลขโดดสามหลักสุดท้ายของ 13^{398}
7. จงหาเลขโดดสามหลักสุดท้ายของ 7^{999}
8. จงหาเศษเหลือที่เกิดจากการหาร 61^{1000} ด้วย 23 โดยใช้ทฤษฎีของแฟร์มาต
9. จงหาเลขสามตัวสุดท้ายของจำนวนเต็ม 3^{2016} เมื่อเขียนในระบบฐานสิบ
10. เศษเหลือที่เกิดจากการหาร $18!$ ด้วย 23 คือจำนวนใด
11. จงแสดงว่า $44 \mid (19^{19}+69^{19})$
12. จงหาเศษเหลือที่เกิดจากการหาร $30!+29!+28!+27!$ ด้วย 31

บทที่ 6

ฟังก์ชันเลขคณิต

บทที่ผ่านมาได้กล่าวถึงสัญลักษณ์ $\phi(m)$ ว่าหมายถึงจำนวนสมาชิกของระบบส่วนตกค้างลดทอนมอดุโล m เรียกว่าฟังก์ชันฟีออยเลอร์ (Euler phi function) เป็นตัวอย่างหนึ่งของฟังก์ชันในทฤษฎีจำนวน ในบทนี้จะกล่าวถึงฟังก์ชันอื่น ๆ โดยเฉพาะฟังก์ชันที่มีโดเมนเป็นจำนวนเต็มบวกและเรจน์เป็นสับเซตของจำนวนเชิงซ้อนเรียกว่า **ฟังก์ชันเลขคณิต (arithematic function)** ซึ่งจะมีบทบาทสำคัญและประยุกต์ใช้ในการศึกษาทฤษฎีจำนวน

สำหรับเซต A และ B ผลคูณคาร์ทีเซียน $A \times B = \{(a,b) : a \in A \text{ และ } b \in B\}$ เรียก $f \subseteq A \times B$ ว่าฟังก์ชันก็ต่อเมื่อ ทุก ๆ $(x_1, y_1), (x_2, y_2) \in f$ ถ้า $x_1 = x_2$ แล้ว $y_1 = y_2$ กำหนดให้

$$\text{โดเมนของ } f \text{ คือ } \{x \in A : (x,y) \in f\} \text{ และ เรจน์ของ } f \text{ คือ } \{y \in B : (x,y) \in f\}$$

ถ้า $f \subseteq A \times B$ เป็นฟังก์ชันจาก A ไป B เขียนแทนด้วย $f : A \to B$ ก็ต่อเมื่อ f เป็นฟังก์ชัน และโดเมนของ f คือ A และสำหรับ $(x,y) \in f$ เขียนแทนด้วย $y = f(x)$

6.1 ฟังก์ชันเชิงการคูณ

บทนิยาม 6.1.1 ฟังก์ชันที่มีโดเมนเป็นเซตของจำนวนเต็มบวก และเรจน์เป็นสับเซตของจำนวน–เชิงซ้อน เรียกว่า **ฟังก์ชันเลขคณิต**

ตัวอย่างฟังก์ชันเลขคณิต

1. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 2n$
2. $f : \mathbb{N} \to \mathbb{C}$ กำหนดโดย $f(n) = n + i$
3. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) =$ จำนวนตัวประกอบที่เป็นจำนวนเฉพาะของ n

ตัวอย่างฟังก์ชันที่ไม่เป็นฟังก์ชันเลขคณิต

1. $f : \mathbb{Z} \to \mathbb{Z}$ กำหนดโดย $f(n) = 2n$
2. $f : \mathbb{C} \to \mathbb{R}$ กำหนดโดย $f(x) = |x|$
3. $f : \mathbb{Z} \to \mathbb{R}$ กำหนดโดย $f(n) = n^2$

ตัวอย่าง 6.1.2 ให้ $\lambda : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย

$$\lambda(n) = \begin{cases} 1 & \text{เมื่อ } n = 1 \\ (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k} & \text{เมื่อ } n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \text{ (รูปแบบบัญญัติ)} \end{cases}$$

เรียกว่า ฟังก์ชันลีอูวิลล์ (Liouville's λ–function) จงหา $\lambda(2), \lambda(6)$ และ $\lambda(12)$

ตัวอย่าง 6.1.3 ให้ $\Lambda : \mathbb{N} \to \mathbb{R}$ กำหนดโดย

$$\Lambda(n) = \begin{cases} \log p & \text{ถ้า } n = p^a \text{ เมื่อ } p \text{ เป็นจำนวนเฉพาะ และ } a \in \mathbb{N} \\ 0 & \text{ถ้า } n \text{ เป็นอย่างอื่น} \end{cases}$$

เรียกว่า ฟังก์ชันมานเกอลท์ (Mangoldt's function) จงหา $\Lambda(2), \Lambda(6)$ และ $\Lambda(9)$

ตัวอย่าง 6.1.4 ให้ $\mu : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย

$$\mu(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้ามีจำนวนเฉพาะ } p \text{ ซึ่ง } p^2 \mid n \\ (-1)^k & \text{ถ้า } n = p_1 p_2 \cdots p_k \text{ เมื่อ } p_i \text{ เป็นจำนวนเฉพาะที่แตกต่างกัน} \end{cases}$$

เรียกว่า ฟังก์ชันเมอบิอุส (Mobius function) จงหา $\mu(2), \mu(6), \mu(9)$ และ $\mu(105)$

บทนิยาม 6.1.5 ฟังก์ชันเลขคณิต f จะเรียกว่า **ฟังก์ชันเชิงการคูณ** (multiplicative function) ก็ต่อเมื่อ

$$f(mn) = f(n)f(m) \qquad \text{สำหรับทุกจำนวนเต็ม } n, m \text{ และ } \gcd(m, n) = 1$$

และเรียกว่า **ฟังก์ชันเชิงการคูณแบบบริบูรณ์** (completely multiplicative function) ก็ต่อเมื่อ

$$f(mn) = f(n)f(m) \qquad \text{สำหรับทุกจำนวนเต็ม } n, m$$

ตัวอย่าง 6.1.6 จงตรวจสอบฟังก์ชันเลขคณิตต่อไปนี้ว่าเป็นฟังก์ชันเชิงการคูณ และ/หรือ ฟังก์ชันเชิงการคูณแบบบริบูรณ์

1. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 0$

2. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 1$

3. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = n$

4. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = n^2$

5. $f : \mathbb{N} \to \mathbb{C}$ กำหนดโดย $f(n) = n + i$

บทนิยาม 6.1.7 ฟังก์ชันเลขคณิต f จะเรียกว่า **ฟังก์ชันเชิงการบวก (additive function)** ก็ต่อเมื่อ

$$f(mn) = f(n) + f(m) \qquad \text{สำหรับทุกจำนวนเต็ม } n, m \text{ และ } \gcd(m, n) = 1$$

และเรียกว่า **ฟังก์ชันเชิงการบวกแบบบริบูรณ์ (completely additive function)** ก็ต่อเมื่อ

$$f(mn) = f(n) + f(m) \qquad \text{สำหรับทุกจำนวนเต็ม } n, m$$

ตัวอย่าง 6.1.8 จงตรวจสอบฟังก์ชันเลขคณิตต่อไปนี้ว่าเป็นฟังก์ชันเชิงการบวก และ/หรือ ฟังก์ชันเชิงการบวกแบบบริบูรณ์

1. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 0$

2. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 1$

3. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = n$

4. $f : \mathbb{N} \to \mathbb{R}$ กำหนดโดย $f(n) = \ell n(n)$

5. $f : \mathbb{N} \to \mathbb{R}$ กำหนดโดย $f(n) = e^n$

ทฤษฎีบท 6.1.9 ให้ f เป็นฟังก์ชันเลขคณิต โดยที่ $f(1) = 1$ และ $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ ในรูปแบบบัญญัติ แล้ว

$$f \text{ เป็นฟังก์ชันเชิงการคูณ} \qquad \text{ก็ต่อเมื่อ} \qquad f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) ... f(p_k^{\alpha_k})$$

ทฤษฎีบท 6.1.10 ให้ f เป็นฟังก์ชันเลขคณิต โดยที่ $f(1) = 1$ และ $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ ในรูปแบบบัญญัติ จะได้ว่า f เป็นฟังก์ชันเชิงการคูณแบบบริบูรณ์ ก็ต่อเมื่อ

$$f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}) = f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} ... f(p_k)^{\alpha_k}$$

บทแทรก 6.1.11 ให้ f เป็นฟังก์ชันเชิงการคูณ โดยที่ $f(1) = 1$ และ $n \in \mathbb{N}$ จะได้ว่า f เป็นฟังก์ชันเชิงการคูณแบบบริบูรณ์ ก็ต่อเมื่อ

$$f(p^m) = (f(p))^m \text{ เมื่อ } p \text{ เป็นจำนวนเฉพาะที่ } p \mid n \text{ และ } m \in \mathbb{N}$$

ต่อไปจะกล่าวถึงสัญลักษณ์แทนการบวกของฟังก์ชันเลขคณิต f คือ

$$\sum_{d|n} f(d) \quad \text{หมายถึง ผลบวกของ } f(d) \text{ เมื่อ } d \text{ เป็นตัวหารที่เป็นบวกของ } n$$

ตัวอย่างเช่น $\sum_{d|3} f(d) = f(1) + f(3)$ และ $\sum_{d|6} f(d) = f(1) + f(2) + f(3) + f(6)$ เป็นต้น

ตัวอย่าง 6.1.12 ให้ฟังก์ชันเลขคณิต $f(n) = n^2$ จงหาของ

1. $\sum_{d|4} f(d)$

2. $\sum_{d|6} f(d)$

3. $\sum_{d|12} f(d)$

สัญลักษณ์แทนการคูณของฟังก์ชันเลขคณิต f คือ

$$\prod_{i=1}^{k} f(i) = f(1)f(2)f(3)\cdots f(k)$$

ตัวอย่างเช่น $\prod_{i=1}^{3} f(i) = f(1)f(2)f(3)$ และ $\prod_{n=1}^{5} n = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5!$ เป็นต้น

แบบฝึกหัด 6.1

1. จงตรวจสอบฟังก์ชันต่อไปนี้ เป็นฟังก์ชันเชิงการคูณหรือไม่

   1.1 $f:\mathbb{N}\to\mathbb{Z}$ โดย $f(n)=3n$

   1.2 $f:\mathbb{N}\to\mathbb{Z}$ โดย $f(n)=n^2$

   1.3 $f:\mathbb{N}\to\mathbb{R}$ โดย $f(n)=n^{-1}$

   1.4 $f:\mathbb{N}\to\mathbb{C}$ โดย $f(n)=n+ni$

2. จงตรวจสอบฟังก์ชันต่อไปนี้ เป็นฟังก์ชันเชิงการบวกหรือไม่

   2.1 $f:\mathbb{N}\to\mathbb{Z}$ โดย $f(n)=5$

   2.2 $f:\mathbb{N}\to\mathbb{Z}$ โดย $f(n)=\gcd(n,n+2)$

   2.3 $f:\mathbb{N}\to\mathbb{R}$ โดย $f(n)=\cos n$

   2.4 $f:\mathbb{N}\to\mathbb{C}$ โดย $f(n)=e^{in}$

3. จงพิสูจน์ว่า ถ้า f และ g เป็นฟังก์ชันเชิงการคูณ แล้ว fg เป็นฟังก์ชันเชิงการคูณ

4. ให้ f และ g เป็นฟังก์ชันเชิงการคูณ จงพิสูจน์ว่า $f=g$ ก็ต่อเมื่อ $f(p^a)=g(p^a)$ สำหรับทุกจำนวนเฉพาะ p และทุกจำนวนนับ d

5. จงหาค่าของ

   5.1 $\displaystyle\sum_{d\mid 6} d$

   5.2 $\displaystyle\sum_{d\mid 12} d^2$

   5.3 $\displaystyle\sum_{d\mid 16} (d+1)$

   5.4 $\displaystyle\sum_{d\mid 36} 2d$

   5.5 $\displaystyle\sum_{d\mid 125} (d+1)(d-1)$

   5.6 $\displaystyle\sum_{d\mid 1000} 1$

6. ให้ M เป็นฟังก์ชันเชิงการคูณซึ่ง $M(p^n)=[M(p)]^n$ ทุก ๆ จำนวนเฉพาะ p และจำนวนนับ n ถ้า

   $$M(1)=1,\quad M(2)=3,\quad M(3)=5 \quad \text{และ} \quad M(5)=7$$

   จงหาค่าของ $M(3600)$

6.2 ฟังก์ชันเทา

บทนิยาม 6.2.1 ให้ $n \in \mathbb{N}$ กำหนดให้

$$\tau(n) = \text{จำนวนตัวหารที่เป็นบวกของ } n$$

เรียกฟังก์ชันนี้ว่า **ฟังก์ชันเทา (tau function)**

ข้อสังเกต 6.2.2 ให้ $n \in \mathbb{N}$ จากบทนิยามจะได้ว่า

1. τ เป็นฟังก์ชันเลขคณิต
2. $\tau(1) = 1$
3. $\tau(n) = \sum_{d|n} 1$

ตัวอย่าง 6.2.3 จงหาค่าของ

1. $\tau(12)$
2. $\tau(23)$
3. $\tau(308)$
4. $\tau(625)$

ทฤษฎีบท 6.2.4 ถ้า p เป็นจำนวนเฉพาะ $a \in \mathbb{N}$ แล้ว

1. $\tau(p) = 2$
2. $\tau(p^a) = a + 1$

ทฤษฎีบท 6.2.5 ให้ $n \in \mathbb{N}$ และ $n > 1$ ถ้า $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ ในรูปแบบบัญญัติ แล้ว

$$\tau(n) = \prod_{i=1}^{k}(\alpha_i + 1) = (a_1 + 1)(a_2 + 2) \cdots (a_k + 1)$$

ตัวอย่าง 6.2.6 จงหาค่าของ

1. $\tau(500)$
2. $\tau(720)$
3. $\tau(1000)$
4. $\tau(8820)$

ทฤษฎีบท 6.2.7 ฟังก์ชันเทาเป็นฟังก์ชันเชิงการคูณ

ต่อไปเป็นตัวอย่างของค่าฟังก์ชันเทา

n	$\tau(n)$
1	1
2	2
3	2
4	3
5	2
6	4
7	2
8	4
9	3
10	4

n	$\tau(n)$
11	2
12	6
13	2
14	4
15	4
16	6
17	2
18	6
19	2
20	6

n	$\tau(n)$
21	4
22	4
23	2
24	8
25	3
26	4
27	4
28	6
29	2
30	8

n	$\tau(n)$
31	2
32	6
33	4
34	4
35	4
36	9
37	2
38	4
39	4
40	8

n	$\tau(n)$
41	2
42	8
43	2
44	6
45	6
46	4
47	2
48	10
49	3
50	6

ตารางที่ 5 แสดงค่าฟังก์ชันเทาตั้งแต่ 1 ถึง 50

ตัวอย่าง 6.2.8 ถ้า $2^k - 1$ เป็นจำนวนเฉพาะ และ $n = 2^{k-1}(2^k - 1)$ จงหาค่าของ $\tau(n)$

แบบฝึกหัด 6.2

1. จงหาค่าของ

   1.1 $\tau(25)$ 1.4 $\tau(125)$ 1.7 $\tau(2560)$

   1.2 $\tau(99)$ 1.5 $\tau(525)$ 1.8 $\tau(3125)$

   1.3 $\tau(100)$ 1.6 $\tau(676)$ 1.9 $\tau(9938)$

2. จงตรวจสอบว่า $\tau(n) = \tau(n+1) + \tau(n+2) + \tau(n+3)$ เป็นจริงสำหรับ $n = 3655$ และ $n = 4503$ หรือไม่

3. จงหาค่าของ $\sum_{d|72} \tau(d)$

4. มีจำนวนนับที่ไม่ใช่จำนวนเฉพาะกี่จำนวนที่หาร $4^5 \cdot 3^{11} \cdot 10^7$ ลงตัว

5. จงตรวจสอบข้อความ

   ถ้า $\tau(a) = 2$ แล้ว a เป็นจำนวนเฉพาะ

   เป็นจริงหรือเท็จ ถ้าจริงจงพิสูจน์ถ้าเป็นเท็จจงยกตัวอย่างค้าน

6.3 ฟังก์ชันซิกมา

บทนิยาม 6.3.1 ให้ $n, k \in \mathbb{N}$ กำหนดให้

$$\sigma(n) = \text{ผลบวกของตัวหารที่เป็นบวกทั้งหมดของ } n$$

เรียกฟังก์ชันนี้ว่า **ฟังก์ชันซิกมา (sigma function)** และนิยาม

$$\sigma_k(n) = \text{ผลบวกของกำลัง } k \text{ ของตัวหารที่เป็นบวกทั้งหมดของ } n$$

ข้อสังเกต 6.3.2 ให้ $n, k \in \mathbb{N}$ จากบทนิยามจะได้ว่า

1. σ และ σ_k เป็นฟังก์ชันเลขคณิต ทุก ๆ $k \in \mathbb{N}$
2. $\sigma = \sigma_1$
3. $\sigma(1) = 1$ และ $\sigma_k(1) = 1$
4. $\sigma(n) = \sum_{d|n} d$ และ $\sigma_k(n) = \sum_{d|n} d^k$

ตัวอย่าง 6.3.3 จงหาค่าของ

1. $\sigma(6)$ และ $\sigma_2(6)$

2. $\sigma(7)$ และ $\sigma_3(7)$

3. $\sigma(81)$ และ $\sigma_2(81)$

ทฤษฎีบท 6.3.4 ถ้า p เป็นจำนวนเฉพาะ แล้ว

$$\sigma(p) = 1 + p \qquad \text{และ} \qquad \sigma_k(p) = 1 + p^k$$

ทฤษฎีบท 6.3.5 ถ้า p เป็นจำนวนเฉพาะ และ $a \in \mathbb{N}$ แล้ว

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1} \qquad \text{และ} \qquad \sigma_k(p^a) = \frac{(p^k)^{a+1} - 1}{p^k - 1}$$

ตัวอย่าง 6.3.6 จงหาค่าของ

1. $\sigma(16)$

2. $\sigma_2(343)$

3. $\sigma(729)$

บทตั้ง 6.3.7 ให้ n_1, n_2 เป็นจำนวนเต็มซึ่ง $\gcd(n_1, n_2) = 1$ จะได้ว่าทุก ๆ จำนวนเต็มบวก d ซึ่ง $d \mid n_1 n_2$ ก็ต่อเมื่อ มีจำนวนเต็มบวก d_1 และ d_2 ที่ $d = d_1 d_2$ และ $d_1 \mid n_1$, $d_2 \mid n_2$ นอกจากนี้ ถ้า $d_1 \mid n_1$, $d_2 \mid n_2$ และ $d_1' \mid n_1$, $d_2' \mid n_2$ โดยที่ $d_1 d_2 = d_1' d_2'$ แล้ว $d_1 = d_1'$ และ $d_2 = d_2'$

ทฤษฎีบท 6.3.8 ฟังก์ชันซิกมาเป็นฟังก์ชันเชิงการคูณ

ตัวอย่าง 6.3.9 จงหาค่าของ

1. $\sigma(600)$

2. $\sigma_2(200)$

3. $\sigma(3250)$

ทฤษฎีบท 6.3.10 ถ้า $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ รูปแบบบัญญัติ แล้ว

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \qquad \text{และ} \qquad \sigma_k(n) = \prod_{i=1}^{k} \frac{(p_i^k)^{\alpha_i+1} - 1}{p_i^k - 1}$$

ต่อไปเป็นตัวอย่างของค่าฟังก์ชันซิกมา

n	$\sigma(n)$
1	1
2	3
3	4
4	7
5	6
6	12
7	8
8	15
9	13
10	18

n	$\sigma(n)$
11	12
12	28
13	14
14	24
15	24
16	31
17	18
18	39
19	20
20	42

n	$\sigma(n)$
21	32
22	36
23	24
24	60
25	31
26	42
27	45
28	56
29	30
30	72

n	$\sigma(n)$
31	32
32	63
33	48
34	54
35	48
36	91
37	38
38	60
39	56
40	90

n	$\sigma(n)$
41	42
42	96
43	44
44	84
45	78
46	72
47	48
48	124
49	57
50	93

ตารางที่ 6 แสดงค่าฟังก์ชันซิกมาตั้งแต่ 1 ถึง 50

ตัวอย่าง 6.3.11 ถ้า $2^k - 1$ เป็นจำนวนเฉพาะ และ $n = 2^{k-1}(2^k - 1)$ จงหาค่าของ $\sigma(n)$

บทนิยาม 6.3.12 เรียกจำนวนนับ n ว่า **จำนวนสมบูรณ์ (perfect number)** ถ้า $\sigma(n) = 2n$

จากตัวอย่าง 6.3.11 ทำให้ได้ตัวอย่างจำนวนสมบูรณ์ดังตาราง

k	$2^k - 1$	จำนวนสมบูรณ์ $n = 2^{k-1}(2^k - 1)$
2	3	6
3	7	28
5	31	496
7	127	8,128
13	8191	335,500,336
17	131071	8,589,869,056

ตารางที่ 7 แสดงจำนวนสมบูรณ์ 6 จำนวนแรก

แบบฝึกหัด 6.3

1. จงหาค่าของ

   1.1 $\sigma_2(20)$ 1.4 $\sigma(1000)$ 1.7 $\sigma(6000)$

   1.2 $\sigma_3(72)$ 1.5 $\sigma(1500)$ 1.8 $\sigma(5545)$

   1.3 $\sigma(900)$ 1.6 $\sigma(3333)$ 1.9 $\sigma(10101)$

2. ให้ $n \in \mathbb{N}$ จงพิสูจน์ว่า $\sigma(n) = n + 1$ ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

3. สำหรับจำนวนนับ n ใด ๆ จงพิสูจน์ว่า $\sigma(n^2) \leq \sigma^2(n)$

4. จงหาจำนวนเต็ม m มีสมบัติว่า

   $$5 \leq m \leq 20 \qquad \text{และ} \qquad \sigma(m+1) = \sigma(m)$$

   และหาค่าของ $\displaystyle\sum_{d|m} \sigma_2(d)$

5. ให้ p เป็นจำนวนเฉพาะโดยที่ $5 \nmid p$ ถ้า

   $$\sigma(5p) = 2\sigma(p^2) - 2$$

   จงหาค่าของ $\tau(p^3 + 3^p)$

6. สำหรับจำนวนนับ n ใด ๆ จงแสดงว่า $\sigma(n) = 1$ ก็ต่อเมื่อ $n = 1$

6.4 ฟังก์ชันฟีออยเลอร์

บทนิยาม 6.4.1 ให้ $n \in \mathbb{N}$ นิยาม

$$\phi(n) = \text{จำนวนของจำนวนเต็มบวก } k \leq n \text{ และ } \gcd(k,n) = 1$$

เรียกว่า **ฟังก์ชันฟีออยเลอร์** (Euler phi function) หรือ **ฟังก์ชันฟี** (phi function)

ข้อสังเกต 6.4.2 ให้ $n \in \mathbb{N}$ จากบทนิยามจะได้ว่า

1. ϕ เป็นฟังก์ชันเลขคณิต
2. $\phi(1) = 1$

ตัวอย่าง $\phi(n)$ เมื่อ $2 \leq n \leq 10$

n	จำนวนเต็มบวก $k \leq n$ ซึ่ง $\gcd(k,n) = 1$	$\phi(n)$
2	1	1
3	1,2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	4
9	1,2,4,5,7,8	6
10	1,3,7,9	4

ตารางที่ 8 แสดงค่าฟังก์ชันฟีออยเลอร์ตั้งแต่ 2 ถึง 10

ตัวอย่าง 6.4.3 จงหาค่าของ

1. $\phi(15)$
2. $\phi(17)$
3. $\phi(25)$
4. $\phi(36)$

ทฤษฎีบท 6.4.4 ถ้า p เป็นจำนวนเฉพาะ แล้ว $\phi(p) = p - 1$

ตัวอย่าง 6.4.5 จงหาค่าของ

1. $\phi(37)$
2. $\phi(101)$
3. $\phi(1277)$

ตัวอย่าง 6.4.6 จงหาค่าของ $\phi(625)$

ทฤษฎีบท 6.4.7 ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{N}$ แล้ว

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

ตัวอย่าง 6.4.8 จงหาค่าของ

1. $\phi(64)$
2. $\phi(97)$
3. $\phi(343)$
4. $\phi(625)$
5. $\phi(729)$
6. $\phi(1225)$

ทฤษฎีบท 6.4.9 ฟังก์ชันฟีออยเลอร์เป็นฟังก์ชันเชิงการคูณ

บทแทรก 6.4.10 ให้ $m_1, m_2, ..., m_k \in \mathbb{N}$ และ $\gcd(m_i, m_j) = 1$ ทุก ๆ $i \neq j$ แล้ว

$$\phi(m_1, m_2...m_k) = \phi(m_1)\phi(m_2)...\phi(m_k)$$

ตัวอย่าง 6.4.11 จงหาค่าของ

1. $\phi(72)$

2. $\phi(500)$

3. $\phi(1000)$

บทแทรก 6.4.12 ถ้า $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ เป็นการเขียน n ในรูปแบบบัญญัติ แล้ว

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

ตัวอย่าง 6.4.13 จงหาค่าของ

1. $\phi(225)$

2. $\phi(360)$

3. $\phi(900)$

4. $\phi(66924)$

ตัวอย่าง 6.4.14 จงหาค่าของ $\sum_{d|n} \phi(d)$ เมื่อ

1. $n = 12$

2. $n = 20$

ทฤษฎีบท 6.4.15 ให้ $n \in \mathbb{N}$ แล้ว

$$\sum_{d|n} \phi(d) = n$$

แบบฝึกหัด 6.4

1. จงหาค่าของ

   1.1 $\phi(18)$ 1.4 $\phi(289)$ 1.7 $\phi(2000)$

   1.2 $\phi(150)$ 1.5 $\phi(256)$ 1.8 $\phi(2016)$

   1.3 $\phi(350)$ 1.6 $\phi(520)$ 1.9 $\phi(49000)$

2. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $\phi(2n) = \phi(n)$

3. จงแสดงว่า ถ้า n เป็นจำนวนเต็มคี่ แล้ว $\phi(2n) = \phi(n)$

4. จงแสดงว่า ถ้า n เป็นจำนวนเต็มคู่ แล้ว $\phi(2n) = 2\phi(n)$

5. จงพิสูจน์ว่า ถ้า n และ $n+2$ เป็นจำนวนเฉพาะคู่แฝด แล้ว $\phi(n+2) = \phi(n) + 2$

6. จงหาจำนวนเต็มบวก k ที่ทำให้ $\phi(2^k \cdot 7^3) = 4704$

7. ให้จำนวนเต็มบวก $n = 2^p \cdot 3^q \cdot 5^r$ อยู่ในรูปแบบบัญญัติ โดยที่ $p > q > r$ ถ้า $\tau(n) = 120$ และ $27 \mid n$ เมื่อเขียน n ในระบบเลขฐานสิบจะลงท้ายด้วยศูนย์ทั้งหมด 3 จำนวน จงหาค่าของ $\phi(pqr)$

8. ถ้า $\displaystyle\sum_{d|n} \phi(d) = 500$ จงหาค่าของ $\phi(n^3)$

9. กำหนดให้ $\displaystyle X = \sum_{n=1}^{100} \left(\sum_{d|n} \phi(d) \right)$ จงหาค่าของ $\phi(X)$

10. ให้ p เป็นจำนวนเฉพาะ โดยที่ $\gcd(3, p) = 1$ และ $\phi(3p) = 380$ จงหา p

11. จงหาค่าของ $\phi(2561^2 - 2018^2)$

6.5 ฟังก์ชันจำนวนเต็มค่ามากสุด

บทนิยาม 6.5.1 สำหรับจำนวนจริง x ใด ๆ

$$[x] \text{ คือจำนวนเต็มค่ามากสุดที่มีค่าน้อยกว่าหรือเท่ากับ } x$$

เรียก $[x]$ ว่า **ฟังก์ชันจำนวนเต็มค่ามากสุด** (the greatest integer function)

ตัวอย่างเช่น $[1.5] = 1$, $[-2.14] = -3$, $[\sqrt{3}] = 1$, $[\frac{15}{7}] = 2$ และ $[3] = 3$

ข้อสังเกต 6.5.2 สำหรับจำนวนจริง x จะได้ว่า

1. $[x] \leq x \leq [x] + 1$
2. $0 \leq x - [x] \leq 1$

ทุกจำนวนจริง x ใด ๆ จะมีจำนวนเต็ม n ที่ $n \leq x < n + 1$ ทำให้ได้

$$x = n + (x - n) \qquad \text{โดยที่} \qquad 0 \leq x - n < 1$$

นั่นคือ $x = n + k$ เมื่อ k เป็นจำนวนจริงที่ $0 \leq k < 1$ ซึ่งในกรณีนี้ $[x] = k$ นั่นเอง

ทฤษฎีบท 6.5.3 สำหรับจำนวนจริง x ใด ๆ จะได้ว่า

1. ถ้า $x \geq 0$ แล้ว $[x] = \sum_{1 \leq i \leq x} 1$
2. $[x] + [-x] = \begin{cases} 0 & \text{ถ้า } x \in \mathbb{Z} \\ -1 & \text{ถ้า } x \notin \mathbb{Z} \end{cases}$
3. $[x + m] = [x] + m$ เมื่อ m เป็นจำนวนเต็ม

ทฤษฎีบท 6.5.4 สำหรับจำนวนจริง x ใด ๆ จะได้ว่า

1. $\left[\frac{x}{m}\right] = \left[\frac{[x]}{m}\right]$ เมื่อ m เป็นจำนวนเต็มบวก
2. $-[-x]$ คือจำนวนเต็มค่าน้อยสุดที่มากกว่าหรือเท่ากับ x
3. ถ้า n และ m เป็นจำนวนเต็มบวก จำนวนของจำนวนเต็มจากเซตของ $\{1, 2, ..., n\}$ ที่หาร n ลงตัวด้วย m คือ $\left[\frac{n}{m}\right]$

สำหรับจำนวนเต็ม a และ b โดยขั้นตอนการหารจะได้ว่ามีจำนวนเต็ม q และ r ซึ่ง $b = aq + r$ เมื่อ $0 \leq r < a$ ทำให้ได้ว่า

$$\frac{b}{a} = q + \frac{r}{a} \qquad \text{โดยที่} \qquad 0 \leq \frac{r}{a} < 1$$

นั่นคือ

$$q = \left[\frac{b}{a}\right] \qquad \text{และ} \qquad r = b - aq = b - a\left[\frac{b}{a}\right]$$

ตัวอย่าง 6.5.5 จงหาเศษเหลือที่เกิดจากการหาร -934 ด้วย 248

ต่อไปจะใช้ฟังก์ชันจำนวนเต็มค่ามากสุดช่วยในการเขียนรูปแบบบัญญัติของจำนวนที่อยู่ในรูปแฟคทอเรียล กำหนดให้ $A = \{1, 2, 3, ..., n\}$ และ $a \in \mathbb{N}$ ให้

$$X_a = \{x \in A : a \text{ หาร } x \text{ ลงตัว }\}$$

แล้วจะได้ว่า $|X_a| = \left[\frac{n}{a}\right]$ จงหาจำนวนเต็ม k มากสุดที่ทำให้ 2^k หาร $100!$ ลงตัว นั่นคือ $100!$ เขียนรูปแบบบัญญัติคือ

$$100! = 2^k \cdot 3^{a_1} \cdot 5^{a_2} \cdot 7^{a_3} \cdots 97$$

พิจารณา $100! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots 97 \cdot 98 \cdot 99 \cdot 100$ พบว่าถ้า $A = \{1, 2, 3, ..., 100\}$ จะได้ว่า

$$X_{2^1} = \{x \in A : 2^1 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^1}| = \left[\frac{100}{2^1}\right] = 50$$

$$X_{2^2} = \{x \in A : 2^2 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^2}| = \left[\frac{100}{2^2}\right] = 25$$

$$X_{2^3} = \{x \in A : 2^3 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^3}| = \left[\frac{100}{2^3}\right] = 12$$

$$X_{2^4} = \{x \in A : 2^4 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^4}| = \left[\frac{100}{2^4}\right] = 6$$

$$X_{2^5} = \{x \in A : 2^5 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^5}| = \left[\frac{100}{2^5}\right] = 3$$

$$X_{2^6} = \{x \in A : 2^6 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^6}| = \left[\frac{100}{2^6}\right] = 1$$

ดังนั้น $k = 50 + 25 + 12 + 6 + 3 + 1 = 97$ นั่นคือ

$$k = \sum_{i=1}^{6} |X_{2^i}| = \sum_{i=1}^{6} \left[\frac{100}{2^i}\right]$$

จะใช้สัญลักษณ์ $e_p(n)$ แทน $\displaystyle\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$ ในตัวอย่างนี้คือ $k = e_2(100)$ จากการสังเกตนี้ทำให้ได้ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 6.5.6 ให้ p เป็นจำนวนเฉพาะ และ n เป็นจำนวนเต็มบวก จะได้ว่ากำลังสูงสุดของ p ที่หาร $n!$ ลงตัวคือ

$$e_p(n) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right]$$

ตัวอย่าง 6.5.7 จงหาจำนวนเต็ม k มากสุดที่ทำให้ 3^k หาร $500!$ ลงตัว

ตัวอย่าง 6.5.8 จงหาจำนวนเต็ม k มากสุดที่ทำให้ 18^k หาร $100!$ ลงตัว

ตัวอย่าง 6.5.9 จงเขียนรูปแบบบัญญัติของ $10!$

ตัวอย่าง 6.5.10 จงหาจำนวนที่ลงท้ายด้วยศูนย์ทั้งหมดของ $1000!$

ทฤษฎีบท 6.5.11 สำหรับจำนวนจริง x และ y จะได้ว่า $[x] + [y] \leq [x + y]$

ทฤษฎีบท 6.5.12 ให้ n และ r เป็นจำนวนเต็มบวก ซึ่ง $1 \leq r \leq n$ จะได้ว่า

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} \qquad \text{เป็นจำนวนเต็ม}$$

บทแทรก 6.5.13 ผลคูณของจำนวนเต็มบวก r จำนวนที่เรียงติดกัน จะหารด้วย $r!$ ลงตัว

ตัวอย่าง 6.5.14 จงแสดงว่า 24 หาร $2016 \cdot 2017 \cdot 2018 \cdot 2019 \cdot 2020$ ลงตัว

แบบฝึกหัด 6.5

1. จงหาค่าของ

   1.1 $[-2\sqrt{31}+1]+[\sqrt{31}]$

   1.2 $\left[\frac{235}{24}+\frac{24}{235}\right]$

   1.3 $\left[\sqrt{1+2+...+10}\right]$

   1.4 $\left[1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{100}\right]$

2. จงเขียนรูปแบบบัญญัติของจำนวนต่อไปนี้

   2.1 $18!$ 2.2 $25!$ 2.3 $30!$ 2.4 $60!$

3. ให้ F และ f เป็นฟังก์ชันเลขคณิตโดยที่ $F(n)=\sum_{d|n} f(d)$ จงพิสูจน์ว่า

   สำหรับจำนวนเต็มบวก m

$$\sum_{i=1}^{m} F(k)=\sum_{k=1}^{m} f(k)\left[\frac{m}{k}\right]$$

4. จงหากำลังสูงสุดของ 7 ที่หาร $1000!$ ลงตัว

5. ถ้าเขียน $500!$ ในรูปเลขฐานสิบจะมีจำนวนที่ลงท้ายด้วยศูนย์ต่อเนื่องกันกี่จำนวน

6. จงหาจำนวน $n!$ ที่เขียนในรูปเลขฐานสิบจะมีจำนวนที่ลงท้ายด้วยศูนย์ต่อเนื่องกัน 37 จำนวน

7. จงหาจำนวนเต็มบวก n ที่น้อยที่สุดที่ทำให้ 105^n หาร $5000!$ ลงตัว

8. จงหาจำนวนเต็มบวก k ที่มีค่ามากสุด ที่ทำให้ 77^k หาร $5000!$ ลงตัว

บทที่ 7

สมการไดโอแฟนไทน์

สมการไดโอแฟนไทน์ (Diophatine equations) เป็นชื่อที่ตั้งเป็นเกียรติแก่นักคณิตศาสตร์ชาวกรีกชื่อ ดีโอฟานโตส (Diophantos) ซึ่งอาศัยอยู่ในเมืองอะเล็กซานเดรียและเชื่อกันว่าเขามีชีวิตอยู่ในช่วง ค.ศ. 250 ถึง ค.ศ. 300 ไม่มีใครทราบประวัติของเขามากนัก ผลงานเขียนที่มีชื่อเสียงมากคือหนังสือ "เลขคณิต" ทั้งหมด 13 เล่ม ทำให้ได้รับการยกย่องว่าเป็น "บิดาของพีชคณิต"

สมการไดโอแฟนไทน์คือสมการที่สนใจคำตอบเป็นจำนวนเต็มเท่านั้น อาจเป็นสมการดีกรีหนึ่ง หรือมากกว่านั้น อาจมีตัวแปรเดียวหรือหลายตัวแปร หรืออาจเป็นระบบสมการที่กำหนดตัวแปรมากกว่าจำนวนสมการ

7.1 สมการเชิงเส้นดีกรีหนึ่ง

ในหัวข้อนี้เราสนใจหาเงื่อนไขที่เพียงพอที่จะแสดงว่าสมการ

$$ax + by = c \qquad \text{เมื่อ } a, b, c \in \mathbb{Z}$$

ถ้า $a = 0$ หรือ $b = 0$ สามารถหาคำตอบได้โดยง่าย เช่น $ax = c$ สมการนี้มีคำตอบก็ต่อเมื่อ $a \mid c$ และคำตอบคือ $x = \frac{c}{a}$ ทำให้สนใจกรณีที่ $a \neq 0$ และ $b \neq 0$

ทฤษฎีบท 7.1.1 ให้ $a, b, c \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ แล้ว

$$\text{สมการ} \quad ax + by = c \quad \text{มีคำตอบ } x, y \in \mathbb{Z} \qquad \text{ก็ต่อเมื่อ} \qquad \gcd(a, b) \mid c$$

ตัวอย่าง 7.1.2 จงตรวจสอบสมการไดโอแฟนไทน์ต่อไปนี้ว่ามีคำตอบหรือไม่

1. $2x + 3y = 5$
2. $42x + 21y = 15$
3. $50x + 15y = 20$
4. $45x + 18y = 100$

ทฤษฎีบท 7.1.3 ให้ $a, b, c \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ ถ้าสมการ $ax+by = c$ มีคำตอบเป็น $x = x_0$ และ $y = y_0$ เรียกคำตอบนี้ว่า**คำตอบเฉพาะราย (particular solution)** และ $d = \gcd(a, b)$ แล้วทุก ๆ คำตอบของสมการ $ax + by = c$ เขียนในรูป

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 - \frac{a}{d}t \qquad \text{เมื่อ } t \in \mathbb{Z}$$

บทแทรก 7.1.4 ให้ $a, b, c \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ ถ้า x_0, y_0 เป็นคำตอบเฉพาะรายของสมการ $ax + by = c$ และ $\gcd(a, b) = 1$ แล้วทุก ๆ คำตอบของสมการสามารถเขียนในรูป

$$x = x_0 + bt, \qquad y = y_0 - at \qquad \text{เมื่อ } t \in \mathbb{Z}$$

ตัวอย่าง 7.1.5 จงหาคำตอบของสมการไดโอแฟนไทน์ $4x + 5y = 13$

สรุปขั้นตอนการหาคำตอบของสมการไดโอแฟนไทน์ $ax + by = c$

1. หา $d = \gcd(a, b)$
2. ตรวจสอบว่า $d \mid c$ หรือ $d \nmid c$
3. ถ้า $d \nmid c$ แล้วสมการ $ax + by = c$ ไม่มีคำตอบในระบบจำนวนเต็ม
4. ถ้า $d \mid c$ แล้วสมการ $ax + by = c$ มีคำตอบในระบบจำนวนเต็ม
   หาคำตอบเฉพาะราย โดยเลือกได้ 2 วิธี ดังนี้
   (ก) ขั้นตอนวิธีแบบยุคลิด จาก $d = ax_1 + by_1$ และ $c = dk$ เลือก $x_0 = kx_1$ และ $y_0 = ky_1$
   (ข) สมการสมภาค $ax \equiv c \pmod{b}$ หรือ $by \equiv c \pmod{a}$
   หา x_0 เป็นคำตอบของ $ax \equiv c \pmod{b}$ แล้วหา y_0 จากสมการ $ax_0 + by_0 = c$
   หา y_0 เป็นคำตอบของ $by \equiv c \pmod{a}$ แล้วหา x_0 จากสมการ $ax_0 + by_0 = c$
5. สร้างคำตอบทั้งหมด

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 - \frac{a}{d}t \qquad \text{เมื่อ } t \in \mathbb{Z}$$

ตัวอย่าง 7.1.6 จงตรวจสอบสมการไดโอแฟนไทน์ต่อไปนี้ว่ามีคำตอบหรือไม่ ถ้ามีจงหาคำตอบ

1. $4x + 2y = 11$

2. $10x + 6y = 16$

3. $6x + 21y = 4$

4. $12x - 5y = 8$

ตัวอย่าง 7.1.7 จงหาคำตอบคำตอบเฉพาะรายของสมการไดโอแฟนไทน์ โดยใช้สมการสมภาค

1. $56x + 72y = 40$

2. $12x - 18y = -60$

3. $101x + 65y = 111$

จากตัวอย่าง 7.1.7 ข้อ 3 การหาคำตอบเฉพาะราย x_0, y_0 มีความยุ่งยากเมื่อหาโดยแก้สมการสมภาค ในกรณีหลีกเลี่ยงได้โดยใช้ขั้นตอนวิธีแบบยุคลิด

$$\begin{array}{rcrcr|rrrl}
101 & = & 101(1) & + & 65(0) & 101 & 1 & 0 & R_1 \\
65 & = & 101(0) & + & 65(1) & 65 & 0 & 1 & R_2 \\
36 & = & 101(1) & + & 65(-1) & 36 & 1 & -1 & R_3 = R_1 - R_2 \\
29 & = & 101(-1) & + & 65(2) & 29 & -1 & 2 & R_4 = R_2 - R_3 \\
7 & = & 101(2) & + & 65(-3) & 7 & 2 & -3 & R_5 = R_3 - R_4 \\
1 & = & 101(-9) & + & 65(14) & 1 & -9 & 14 & R_6 = R_3 - 4R_4
\end{array}$$

จะได้ว่า $x_0 = -9$ และ $y_0 = 14$

ตัวอย่าง 7.1.8 จงหาคำตอบเฉพาะรายของสมการไดโอแฟนไทน์ โดยใช้ขั้นตอนวิธีแบบยุคลิด

1. $80x - 62y = 90$

2. $112x + 97y = 100$

ตัวอย่าง 7.1.9 เด็กชายเอ ได้เงินค่าขนมจากพ่อจำนวน 200 บาท ถ้าเราทราบเพียงว่าพ่อของเด็กชายเอให้เป็นธนบัตร 2 ชนิดคือธนบัตรชนิด 20 บาท และธนบัตรชนิด 50 บาทเท่านั้น จงหาจำนวนธนบัตรที่เด็กชายเอได้รับทั้งหมด

ตัวอย่าง 7.1.10 นายมีเงินอยู่ 100 ต้องการจะซื้อน้ำอัดลมชนิดกระป๋องราคากระป๋องละ 15 บาท และซื้อขนมคบเคี้ยวชนิดห่อ ๆ ละ 20 บาท ถ้านายต้องซื้อของทั้ง 2 ชนิดนี้เท่านั้นให้เงินหมดพอดี นายสามารถทำได้หรือไม่ ถ้าทำได้ทำได้ทั้งหมดกี่แบบ

ต่อไปจะพิจารณาสมการไดโอแฟนไทน์ดีกรีหนึ่งที่มีตัวแปรมากกว่า 2 ตัวขึ้นไป การตรวจสอบว่ามีคำตอบในระบบจำนวนเต็มหรือไม่ ทำได้คล้ายคลึงกับทฤษฎีบท 7.1.1

ทฤษฎีบท 7.1.11 ให้ $d = \gcd(a_1, a_2, ..., a_k)$ แล้ว

สมการ $a_1x_1 + a_2x_2 + ... + a_kx_k = c$ มีคำตอบ $x_1, x_2, ..., x_k \in \mathbb{Z}$ ก็ต่อเมื่อ $d \mid c$

พิจารณาการหาคำตอบของสมการไดโอแฟนไทน์

$$ax + by + cz = m$$

ให้ $d = \gcd(a, b, c)$ และ $d_0 = \gcd(a, b)$ ถ้า $d \mid m$ สมการนี้มีคำตอบในระบบจำนวนเต็ม โดยทฤษฎีบท 7.1.11 พิจารณาสมการ

$$ax + by = m - cz$$

ดังนั้น $d_0 \mid (m - cz)$ นั่นคือ

$$cz \equiv m \pmod{d_0}$$

ให้ z_0 เป็นคำตอบของสมการ $cz \equiv m \pmod{d_0}$ เนื่องจาก $\gcd(a, b, c) = \gcd(\gcd(a, b), c) = d$ และ $d \mid m$ ดังนั้น

$$z = z_0 + \frac{d_0}{d}t \qquad \text{เมื่อ} \qquad t \in \mathbb{Z}$$

เมื่อแทน z ลงในสมการไดโอแฟนไทน์ $ax + by + cz = m$ ทำให้ได้สมการไดโอแฟนไทน์ 2 ตัวแปร แล้วดำเนินการหาคำตอบของสมการด้วยวิธีเดิมที่กล่าวมาแล้ว

ตัวอย่าง 7.1.12 จงหาคำตอบของสมการไดโอแฟนไทน์ $3x - 6y + 9z = 63$

ตัวอย่าง 7.1.13 จงหาคำตอบของสมการไดโอแฟนไทน์ $3x - 6y + 2z = 11$

ตัวอย่าง 7.1.14 จงหาคำตอบของสมการไดโอแฟนไทน์ $15x + 12y + 30z = 24$

ตัวอย่าง 7.1.15 จงหาคำตอบของสมการไดโอแฟนไทน์ $14x + 6y + 30z + 90w = 200$

ตัวอย่าง 7.1.16 มานะมีธนบัตร 1 ใบมูลค่า 50 บาท ต้องการแลกเหรียญ 3 ชนิดคือ เหรียญ 2 บาท เหรียญ 5 บาท และเหรียญ 10 บาท ถามว่ามานะจะได้เหรียญทั้งหมดกี่แบบโดยต้องมีเหรียญแต่ละชนิดอย่างน้อย 1 เหรียญ

ตัวอย่าง 7.1.17 จงหาสมการไดโอแฟนไทน์มาอย่างน้อยหนึ่งสมการที่มีคำตอบเป็น

$$\begin{aligned} x &= 12 + 4s - 7t \\ y &= 5 - 2s \qquad\qquad \text{เมื่อ } t, s \in \mathbb{Z} \\ z &= t \end{aligned}$$

แบบฝึกหัด 7.1

1. จงตรวจสอบสมการไดโอแฟนไทน์ต่อไปนี้ว่ามีคำตอบในระบบจำนวนเต็มหรือไม่ ถ้ามีจงหาคำตอบ

   1.1 $172x + 20y = 1000$
   1.2 $4x - 82y = -6$
   1.3 $999x - 49y = 500$
   1.4 $247x + 589y = 817$

2. จงหาคำตอบคำตอบเฉพาะรายของสมการไดโอแฟนไทน์ โดยใช้สมการสมภาค

   2.1 $393x + 23y = 120$
   2.2 $44x - 200y = -600$
   2.3 $99x - 699y = 333$
   2.4 $123x + 51y = 303$
   2.5 $69x - 96y = 300$
   2.6 $125x - 315y = 1200$

3. จงหาคำตอบคำตอบเฉพาะรายของสมการไดโอแฟนไทน์ โดยใช้ขั้นตอนวิธีแบบยุคลิด

   3.1 $172x + 20y = 1000$
   3.2 $97x - 751y = 881$
   3.3 $919x + 213y = 251$
   3.4 $2520x + 154y = 14$
   3.5 $1004x + 2016y = 5000$
   3.6 $111x - 1111y = 11111$

4. จงหาคำตอบคำตอบของสมการไดโอแฟนไทน์

   4.1 $10x + 16y - 4z = 48$
   4.2 $15x + 12y + 30z = 24$
   4.3 $7x + 8y + 9z = 1000$
   4.4 $2x + 3y + 4z = 5$

5. จงพิสูจน์ว่า สมการ $ax + by = a + c$ มีคำตอบ ก็ต่อเมื่อ สมการ $ax + by = c$ มีคำตอบ

6. เด็กชายเอมีเงิน 990 บาท ต้องการแลกธนบัตรใบละ 20 และ 50 บาท จงหาจำนวนวิธีแลกธนบัตรที่เป็นไปได้ทั้งหมด

7. นาย AppMan นำปากกา 2 ชนิดมาขายให้กับเพื่อนในห้องเรียนวิชา Number Theory ที่สอนโดยอาจารย์หน้าตาดีท่านหนึ่ง โดยชนิดที่ 1 ขายแท่งละ 15 บาท ชนิดที่ 2 ขายแท่งละ 25 บาท ถ้าพบว่านาย AppMan ขายปากกาได้เงินทั้งหมด 105 บาท จงหาความเป็นไปได้ทั้งหมดที่นาย AppMan จะขายปากกาแต่ละชนิดจำนวนเท่าใดบ้าง

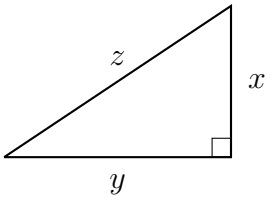
8. เด็กชาย M มี แบงค์ชนิด 20 บาทอย่างน้อย 10 ใบ ชนิด 50 บาท อย่างน้อย 5 ใบ และแบงค์ 100 บาท อย่างน้อย 5 ใบ ถ้าเด็กหญิง W ทราบว่าเด็กชาย M นำเงินมาด้วยมีมูลค่า 1000 บาท ถามว่าเด็กหญิง W จะเดาจำนวนแบงค์แต่ละชนิดที่เด็กชาย M มีได้กี่แบบมีแบบใดบ้าง

7.2 สมการพีทาโกรัส

ในหัวข้อนี้จะพิจารณาสมการพีทาโกรัส

$$x^2 + y^2 = z^2$$

เพื่อศึกษาวิธีการหาคำตอบที่เป็นจำนวนเต็มบวกทั้งหมด ซึ่งเรียกว่าสมการไดโอแฟนไทน์ดีกรีสอง 3 ตัวแปร หรือกล่าวอีกนัยคือการหาความยาวด้านทั้งสามของสามเหลี่ยมมุมฉาก



รูปที่ 3 สามเหลี่ยมมุมฉากแสดงความยาวแต่ละด้าน

ให้ x_0, y_0, z_0 เป็นคำตอบของสมการ $x^2 + y^2 = z^2$ เราเขียนแทนด้วย $\{x_0, y_0, z_0\}$ ตัวอย่างเช่น $\{3, 4, 5\}$ และ $\{5, 12, 13\}$ เป็นต้น

บทนิยาม 7.2.1 ให้ x, y, z เป็นจำนวนเต็มบวกซึ่ง $x < z$ และ $y < z$
สามสิ่งอันดับพีทาโกรัส (Pythagorean Triple) คือ $\{x, y, z\}$ ที่สอดคล้องสมการ

$$x^2 + y^2 = z^2$$

ตัวอย่างสามสิ่งอันดับพีทาโกรัส เช่น $\{3, 4, 5\}$, $\{4, 3, 5\}$, $\{7, 24, 25\}$ เป็นต้น

ตัวอย่าง 7.2.2 จงตรวจสอบจำนวนต่อไปนี้ว่าเป็นสามสิ่งอันดับพีทาโกรัสหรือไม่

1. $\{15, 8, 17\}$
2. $\{21, 20, 29\}$
3. $\{12, 84, 87\}$
4. $\{39, 80, 89\}$

พีทาโกรัสได้ให้คำตอบของสมการ $x^2 + y^2 = z^2$ ไว้ว่า

$$x = k, \quad y = \frac{k^2 - 1}{2} \quad \text{และ} \quad z = \frac{k^2 + 1}{2} \quad \text{เมื่อ } k \text{ เป็นจำนวนคี่ที่มากกว่า 1}$$

ซึ่งจะเห็นว่า

ดังนั้น $\left\{k, \frac{k^2 - 1}{2}, \frac{k^2 + 1}{2}\right\}$ เป็นสามสิ่งอันดับพีทาโกรัส เมื่อ k เป็นจำนวนคี่ที่มากกว่า 1

ตัวอย่างสามสิ่งอันดับพีทาโกรัสจากคำตอบของพีทาโกรัสแสดงดังตารางต่อไปนี้

$x = k$	$y = \frac{k^2 - 1}{2}$	$z = \frac{k^2 + 1}{2}$
3	4	5
5	12	13
7	24	25
9	40	41
11	60	61
13	84	85
15	112	113
17	144	145
19	180	181
21	220	221

$x = k$	$y = \frac{k^2 - 1}{2}$	$z = \frac{k^2 + 1}{2}$
23	264	265
25	312	313
27	364	365
29	420	421
31	480	481
33	544	545
35	612	613
37	684	685
39	760	761
41	840	841

ตารางที่ 9 แสดงตัวอย่างสามสิ่งอันดับพีทาโกรัสที่ได้จากคำตอบของพีทาโกรัส

ทฤษฎีบท 7.2.3 ถ้า $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัส และ $k \in \mathbb{N}$ แล้ว

$$\{ka, kb, kc\} \qquad \text{เป็นสามสิ่งอันดับพีทาโกรัส}$$

ตัวอย่าง 7.2.4 จงหาสามสิ่งอันดับพีทาโกรัสที่ได้จาก $\{3, 4, 5\}$ อีกอย่างน้อย 3 ชุด

ทฤษฎีบท 7.2.5 ถ้า $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัส และ $d = \gcd(a, b, c)$ แล้ว

$$\left\{\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right\} \quad \text{เป็นสามสิ่งอันดับพีทาโกรัส}$$

มากกว่านั้นจะได้ด้วยว่า $\gcd\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) = 1$

ทฤษฎีบท 7.2.6 ถ้า $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัส และ $\gcd(a, b, c) = 1$ แล้ว

$$\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$$

บทนิยาม 7.2.7 เรียกสามสิ่งอันดับพีทาโกรัส $\{a, b, c\}$ ว่า **สามสิ่งอันดับพีทาโกรัสปฐมฐาน (Primitive Pythagorean Triple)** ถ้า $\gcd(a, b, c) = 1$

ตัวอย่าง 7.2.8 จงตรวจสอบสามสิ่งอันดับพีทาโกรัสต่อไปนี้ว่าเป็นสามสิ่งอันดับพีทาโกรัสปฐมฐานหรือไม่

1. $\{3, 4, 5\}$
2. $\{8, 15, 17\}$
3. $\{10, 24, 26\}$
4. $\{45, 200, 205\}$

ทฤษฎีบท 7.2.9 ถ้า $\{a, b, c\}$ สามสิ่งอันดับพีทาโกรัสปฐมฐาน จะได้ว่า $a \not\equiv b \pmod 2$

หมายเหตุ $a \not\equiv b \pmod 2$ หมายความว่า a, b เป็นจำนวนคู่พร้อมกันไม่ได้ และเป็นจำนวนคี่พร้อมกันไม่ได้ นั่นคือถ้าตัวหนึ่งเป็นจำนวนคู่อีกตัวหนึ่งจะเป็นจำนวนคี่

จากทฤษฎีบท 7.2.9 เราอาจสมมติว่า a เป็นจำนวนคู่ และ b เป็นจำนวนคี่ ไม่ถือว่า $\{a, b, c\}$ และ $\{b, a, c\}$ เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐานที่แตกต่างกัน และได้ข้อสรุปอีกอย่างว่า a, b, c เป็นจำนวนเฉพาะพร้อมกันไม่ได้ด้วย

ทฤษฎีบท 7.2.10 $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน ก็ต่อเมื่อ มีจำนวนเต็ม u, v ซึ่ง $u > v > 0$, $\gcd(u, v) = 1$ และ $u \not\equiv v \pmod 2$ ที่ทำให้

$$a = u^2 - v^2, \qquad b = 2uv \qquad \text{และ} \qquad c = u^2 + v^2$$

จากทฤษฎีบท 7.2.10 ทำให้ทราบว่าสามารถหาสามสิ่งอันดับพีทาโกรัสปฐมฐานได้ไม่จำกัดจำนวน ดังแสดงตัวอย่างตามตารางต่อไปนี้

u	v	a	b	c
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61
7	2	45	28	53
7	4	33	56	65

u	v	a	b	c
7	6	13	84	85
8	1	63	16	65
8	3	55	48	73
8	5	39	80	89
8	7	15	112	113
9	1	80	36	85
9	4	65	72	97
9	5	56	90	106
9	7	32	126	130
9	8	17	144	145

u	v	a	b	c
10	1	99	20	101
10	3	91	60	109
10	7	51	140	149
10	9	19	180	181
11	2	117	44	125
11	4	105	88	137
11	6	85	132	157
11	8	57	176	185
11	10	21	220	221
12	1	143	24	145

ตารางที่ 10 แสดงตัวอย่างสามสิ่งอันดับพีทาโกรัสปฐมฐาน

ตัวอย่าง 7.2.11 จงหาสามสิ่งอันดับพีทาโกรัสปฐมฐาน โดยใช้ทฤษฎีบท 7.2.10 เมื่อ

1. $u = 15$
2. $u = 23$

ต่อไปจะกล่าวถึงวิธีการหาสามสิ่งอันดับพีทาโกรัสปฐมฐาน $\{a,b,c\}$ เมื่อกำหนด a หรือ b โดยอาศัยทฤษฎีบท 7.2.10 จะเห็นว่า $b=2uv$ เป็นจำนวนคู่ ดังนั้น $a=u^2-v^2=(u-v)(u+v)$ เป็นจำนวนคี่ จึงพิจารณาเป็น 2 กรณีคือจำนวนนั้นเป็นจำนวนคี่และเป็นจำนวคู่

กรณี x เป็นจำนวนเต็มคี่

1. แยกตัวประกอบของ x ออกเป็นผลคูณของสองจำนวน
2. เขียนตัวประกอบมากสุดในรูป $\quad u+v$
   เขียนตัวประกอบน้อยสุดในรูป $\quad u-v$
3. แก้สมการใน ข้อ 2. เพื่อหา u และ v
4. หา $\{a,b,c\}$ จาก $a=u^2-v^2, \quad b=2uv \quad$ และ $\quad c=u^2+v^2$

ตัวอย่าง 7.2.12 กำหนดให้จำนวนต่อไปนี้เป็นจำนวนหนึ่งในสามสิ่งอันดับพีทาโกรัสปฐมฐาน จงหาสามสิ่งอันดับพีทาโกรัสปฐมฐานที่เป็นไปได้ทั้งหมด

1. 35

2. 43

3. 51

ตัวอย่าง 7.2.13 กำหนดให้จำนวนต่อไปนี้เป็นจำนวนหนึ่งในสามสิ่งอันดับพีทาโกรัสปฐมฐาน จงหาอีกสองจำนวน

1. 63

2. 105

ในกรณี x เป็นจำนวนคู่ จะได้ $x = 2uv$ และ u, v ไม่เป็นจำนวนคี่พร้อมกัน ดังนั้นมีจำนวนหนึ่งเป็นจำนวนคู่ทำให้ได้ $4 \mid x$ ถ้า $4 \nmid x$ สรุปได้ว่า x ไม่เป็นหนึ่งในจำนวนของสามสิ่งอันดับพีทาโกรัสปฐมฐาน

กรณี x เป็นจำนวนเต็มคู่

1. ถ้า $4 \nmid x$ แสดงว่า x ไม่เป็นหนึ่งในจำนวนของสามสิ่งอันดับพีทาโกรัสปฐมฐาน
2. ถ้า $4 \mid x$ แล้ว $x = 2uv$ โดยที่ $\gcd(u, v) = 1$ และ $u > v > 0$ ดังนั้นมี u หรือ v เป็นจำนวนคู่ และอีกจำนวนหนึ่งเป็นจำนวนคี่
3. หา u และ v ที่สอดคล้อง ข้อ 2.
4. หา $\{a, b, c\}$ จาก $a = u^2 - v^2, \quad b = 2uv \quad$ และ $\quad c = u^2 + v^2$

ตัวอย่าง 7.2.14 กำหนดให้จำนวนต่อไปนี้เป็นจำนวนหนึ่งในสามสิ่งอันดับพีทาโกรัสปฐมฐาน จงหาสามสิ่งอันดับพีทาโกรัสปฐมฐานที่เป็นไปได้ทั้งหมด

1. 8

2. 24

3. 48

4. 42

ตัวอย่าง 7.2.15 กำหนดให้จำนวนต่อไปนี้เป็นจำนวนหนึ่งในสามสิ่งอันดับพีทาโกรัส จงหาสามสิ่งอันดับพีทาโกรัสทั้งหมดที่เป็นไปได้

1. 28

2. 42

3. 100

บทตั้ง 7.2.16 ให้ x เป็นจำนวนเต็ม จะได้ว่า

1. เศษเหลือที่เกิดจากการหาร x ด้วย 3 เท่ากับ 0 หรือ 1 เท่านั้น
2. เศษเหลือที่เกิดจากการหาร x ด้วย 5 เท่ากับ 0 หรือ 1 หรือ 4 เท่านั้น

ทฤษฎีบท 7.2.17 ถ้า $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัส จะได้ว่า

1. $3 \mid a$ หรือ $3 \mid b$
2. $5 \mid a$ หรือ $5 \mid b$ หรือ $5 \mid c$

ทฤษฎีบท 7.2.18 ให้ $\{a, b, c\}$ และ $\{x, y, z\}$ เป็นสามสิ่งอันดับพีทาโกรัส จะได้ว่า

$\{|by - ax|, bx + ay, cz\}$ เป็นสามสิ่งอันดับพีทาโกรัส

บทแทรก 7.2.19 ให้ $\{a, b, c\}$ จะได้ว่า $\{|b^2 - a^2|, 2ab, c^2\}$ เป็นสามสิ่งอันดับพีทาโกรัส

ตัวอย่าง 7.2.20 จงหาสามจำนวนของปีทาโกรัส ที่เกิดจากสามจำนวนของปีทาโกรัส

1. $\{3, 4, 5\}$ และ $\{3, 4, 5\}$
2. $\{3, 4, 5\}$ และ $\{5, 12, 13\}$
3. $\{3, 4, 5\}$ และ $\{8, 15, 17\}$
4. $\{8, 15, 17\}$ และ $\{7, 24, 25\}$

แบบฝึกหัด 7.2

1. จงหาสามสิ่งอันดับพีทาโกรัสปฐมฐานที่เกิดจาก u, v

   1.1 $u = 9, v = 2$ 1.3 $u = 10, v = 1$ 1.5 $u = 11, v = 2$

   1.2 $u = 9, v = 4$ 1.4 $u = 10, v = 9$ 1.6 $u = 13, v = 4$

2. จงหา u, v จากสามสิ่งอันดับพีทาโกรัสที่กำหนดให้

   2.1 $\{24, 7, 25\}$ 2.3 $\{36, 77, 85\}$

   2.2 $\{48, 51, 78\}$ 2.4 $\{140, 51, 149\}$

3. ให้ $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน ที่เกิดจาก u, v จงหาจำนวนที่เหลือ

   3.1 $a = 24, b = 13$ 3.4 $v = 4, c = 97$

   3.2 $u = 7, a = 56$ 3.5 $u = 8, c = 89$

   3.3 $u = 9, v = 17$ 3.6 $u = 7, c = 15$

4. จงหาสามสิ่งอันดับพีทาโกรัสปฐมฐาน $\{a, b, c\}$ ทุกชุดที่สอดคล้องกับ

   4.1 $a = 12$ 4.4 $b = 23$

   4.2 $a = 24$ 4.5 $a = 20$

   4.3 $b = 9$ 4.6 $c = 125$

5. จงหาสามสิ่งอันดับพีทาโกรัส $\{a, b, c\}$ ทุกชุดที่สอดคล้องกับ

   5.1 $a = 16$ 5.3 $b = 35$

   5.2 $a = 20$ 5.4 $c = 85$

6. จงหาคำตอบของ $x^2 + y^2 = z^2$ เมื่อ $0 < z < 30$

7. จงหาสามสิ่งอันดับพีทาโกรัสที่เกิดสามสิ่งอันดับพีทาโกรัสที่กำหนดให้

   7.1 $\{3, 4, 5\}$ และ $\{21, 20, 29\}$ 7.2 $\{5, 12, 13\}$ และ $\{9, 40, 41\}$

8. ให้ $n \in \mathbb{N}$ จงแสดงว่า $\{2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1\}$ เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน พร้อมทั้งหาสามสิ่งอันดับพีทาโกรัสจากสูตรดังกล่าวมาอย่างน้อย 5 ชุด

9. ถ้า $\{a, a + 1, a + 2\}$ เป็นสามสิ่งอันดับพีทาโกรัส จงหา a

7.3 สมการไดโอแฟนไทน์กำลังสอง

ในหัวข้อนี้จะพิจารณาการหาคำตอบของสมการไดโอแฟนไทน์กำลังสองรูปแบบอื่น ๆ

ทฤษฎีบท 7.3.1 ให้ c เป็นจำนวนเต็ม สมการ $x^2 - y^2 = c$ มีคำตอบเป็นจำนวนเต็ม ก็ต่อเมื่อ c เป็นจำนวนเต็มคี่ หรือ $4 \mid c$

ตัวอย่าง 7.3.2 จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 - y^2 = 15$

ตัวอย่าง 7.3.3 จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 - y^2 = 24$

ทฤษฎีบท 7.3.4 ให้ $c \in \mathbb{Z}$ แล้วมีจำนวนเต็ม x, y, z ซึ่ง $x^2 + y^2 - z^2 = c$

ตัวอย่าง 7.3.5 จงหาคำตอบของสมการไดโอแฟนไทน์

$$x^2 + y^2 - z^2 = 8$$

มาอย่างน้อย 5 ชุดคำตอบ

ตัวอย่าง 7.3.6 จงหาคำตอบของสมการไดโอแฟนไทน์

$$x^2 + y^2 - z^2 = 5$$

มาอย่างน้อย 5 ชุดคำตอบ

ตัวอย่าง 7.3.7 จงพิสูจน์ว่า ไม่มีจำนวนเต็ม x, y ที่เป็นคำตอบของสมการ $3x^2 + 8 = y^2$

ตัวอย่าง 7.3.8 จงหาจำนวนเต็มบวก x, y ทุกคู่ที่เป็นคำตอบของสมการ $x^2 - xy + y = 3$

ตัวอย่าง 7.3.9 จงหาจำนวนเต็มบวก a, b, c ที่เป็นคำตอบของสมการ

$$a^3 - b^3 - c^3 = 3abc$$
$$a^2 = 2(b + c)$$

แบบฝึกหัด 7.3

1. สมการ $x^4 - y^4 = z^2$ ไม่มีคำตอบเป็นจำนวนนับ
2. จงหาจำนวนเต็มบวก a, b, c, d ที่แตกต่างกัน ซึ่ง $a^2 + b^2 = c^2 + d^2 = 493097 = 577 \cdot 761$
3. จงแสดงว่า มีจำนวนเฉพาะ p ซึ่ง $p \equiv 1 \pmod 8$ เป็นจำนวนไม่จำกัด
4. จงแสดงว่า มีจำนวนเฉพาะ p ซึ่ง $p \equiv 5 \pmod 8$ เป็นจำนวนไม่จำกัด
5. จงแสดงว่า ถ้า $4 \mid (x^2 + y^2 + z^2)$ แล้ว x, y, z เป็นจำนวนเต็มคู่
6. จงหาจำนวนเต็มบวก x, y ทุกคู่ที่ทำให้ $x^2 = y^2 + 120$
7. จงหาจำนวนเต็มบวก x, y ทุกคู่ที่ทำให้ $x^3 = y^3 + 721$
8. จงหาจำนวนเต็มบวก x, y ทุกคู่ที่ทำให้ $15x^2 - 7y^2 = 9$
9. จงตรวจสอบว่าสมการ $a^2 + b^2 + c^2 = a^2b^2$ มีคำตอบเป็นจำนวนเต็มบวกหรือไม่

บรรณานุกรม

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. (2552). **ทฤษฎีจำนวน**. กรุงเทพฯ : มูลนิธิ สอวน.

อัจฉรา หาญชูวงศ์. (2542). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

Ivan Niven, Herbert S. Zuckerman and Hugh L. Montgomery. (1991). **An introduction to Theory of Numbers**. New York : John Wiley & Sons, Inc.

ประวัติผู้เขียน

ผู้ช่วยศาสตรจารย์ ดร.ธนัชยศ จำปาหวาย

- ปัจจุบันดำรงตำแหน่ง ผู้ช่วยศาสตรจารย์ประจำสาขาวิชาคณิตศาสตร์ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา
- ปริญญาเอก วิทยาศาสตร์ดุษฎีบัณฑิต (คณิตศาสาตร์), จุฬาลงกรณ์มหาวิทยาลัย, 2557
  Ph.D. (Mathematics), Chulalongkorn University, 2014
- ปริญญาโท วิทยาศาสตร์มหาบัณฑิต (คณิตศาสาตร์), จุฬาลงกรณ์มหาวิทยาลัย, 2552
  M.Sc. (Mathematics), Chulalongkorn University, 2009
- ปริญญาตรี วิทยาศาสตร์บัณฑิต (คณิตศาสาตร์, เกียติรนิยมอันดับสอง),
  จุฬาลงกรณ์มหาวิทยาลัย, 2549
  B.Sc. (Mathematics, 2^{nd} class honours),Chulalongkorn University, 2006

Email: thanatyod_ja@ssru.ac.th Office: 1144
Facebook: www.facebook.com/Jampawai Block: www.eledu.ssru.ac.th/thanatyod_ja

ผลงานทางวิชาการ

1. พีชคณิตนามธรรม. (2565). www.mebmarket.com
2. หลักการคณิตศาสตร์สำหรับครู. (2565). www.mebmarket.com
3. ทฤษฎีจำนวน. (2565). www.mebmarket.com
4. หนังสือความจริงที่ต้องพิสูจน์. (2560). มหาวิทยาลัยราชภัฏสวนสุนันทา

บัญชีสัญลักษณ์

สัญลักษณ์	ความหมาย
$a \in A$	a เป็นสมาชิกของเซต A
$A \subseteq B$	A เป็นสับเซตของ B
$\mathbb{C}$	เซตของจำนวนเชิงซ้อน
$\mathbb{R}$	เซตของจำนวนจริง
$\mathbb{Z}$	เซตของจำนวนเต็ม
$\mathbb{N}$	เซตของจำนวนนับ
$\varnothing$	เซตว่าง
$A \cup B$	ยูเนียนของเซต A กับ B
$A \cap B$	อินเตอร์เซกชันของเซต A กับ B
$A - B$	ผลต่างของเซต A กับ B
$A \times B$	ผลคูณคาร์ทีเซียนของ A และ B
A^c	ส่วนเติมเต็มของเซต A
$\lvert A \rvert$	จำนวนสมาชิกของเซต A
$a \mid b$	a หาร b ลงตัว
$a \nmid b$	a หาร b ไม่ลงตัว
$\mathsf{gcd}(a, b)$	ตัวหารร่วมมากของ a และ b
$\ell\mathsf{cm}(a, b)$	ตัวคูณร่วมน้อยของ a และ b
F_n	จำนวนแฟร์มาต์ $F_n = 2^{2^n} + 1$ เมื่อ $n \in \mathbb{Z}$ ซึ่ง $n \geq 0$
M_n	จำนวนมาร์เซน $M_n = 2^n - 1$ เมื่อ $n \in \mathbb{N}$
$f : A \to B$	ฟังก์ชันจาก A ไป B
$\tau(n)$	จำนวนตัวหารที่เป็นบวกของ n
$\sigma(n)$	ผลบวกของตัวหารที่เป็นบวกทั้งหมดของ n
$\sigma_k(n)$	ผลบวกของกำลัง k ของตัวหารที่เป็นบวกทั้งหมดของ n
$\phi(n)$	จำนวนของจำนวนเต็มบวก $k \leq n$ และ $\mathsf{gcd}(k, n) = 1$
$[x]$	คือจำนวนเต็มค่ามากสุดที่มีค่าน้อยกว่าหรือเท่ากับ x
$\{x, y, z\}$	สามสิ่งอันดับพีทาโกรัส $x^2 + y^2 = z^2$