

ANCIENT EGYPTIAN HIEROGLYPHS									
1	10	100	1000	10000	100000	1000000	10000000	MAN	WOMAN
GOD	GODDESS	WATER	TOWN	DESERT	Dual	Plural	1	2	3
4	5	6	7	8	9	10	11	12	13

โครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.

ทฤษฎีจำนวน

(ความรู้เบื้องต้น การหารลงตัว จำนวนเฉพาะ ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ
ฟังก์ชันเลขคณิต คอนกรูเอนซ์ สมการไดโอแฟนไทน์)

$$6 \times 2,697 = 16,182$$

1	2	6	9	7
2	4	12	18	14
3	6	18	27	21
4	8	24	36	28
5	10	30	45	35
6	12	36	54	42
7	14	42	63	49
8	16	48	72	56
9	18	54	81	63

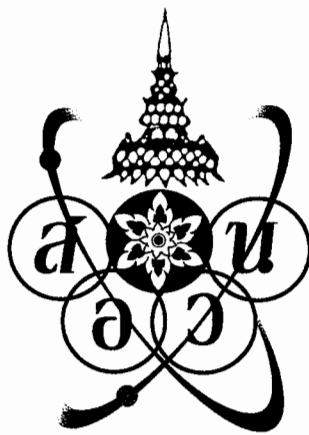
6	12 ⁺ 3	36 ⁺ 5	54 ⁺ 4	2
---	-------------------	-------------------	-------------------	---

+ (1)
1 6 1 8 2

Tens-carry (1)

The model shows six rotating rods suitable for a six-digit multiplicand. As the rods cannot be exchanged, only four different digits can be chosen in each position.

โครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.



**มูลนิธิส่งเสริมโอลิมปิกวิชาการและพัฒนามาตรฐานวิทยาศาสตร์ศึกษา
ในพระอุปถัมภ์สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา
กรมหลวงนราธิวาสราชนครินทร์ (สอวน.)**

ความเป็นมา

ประเทศไทยส่งนักเรียนเข้าแข่งขันคณิตศาสตร์โอลิมปิกระหว่างประเทศครั้งแรกในปี พ.ศ. 2532 ที่ประเทศเยอรมนี โดยความร่วมมือระหว่างสมาคมวิทยาศาสตร์แห่งประเทศไทยในพระบรมราชูปถัมภ์ และสมาคมคณิตศาสตร์แห่งประเทศไทย ในพระบรมราชูปถัมภ์ สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา (พระยศในขณะนั้น) ได้พระราชทานเงินส่วนพระองค์ จำนวนหนึ่งเพื่อเป็นค่าใช้จ่าย

การคัดเลือกนักเรียนเพื่อไปแข่งขันคณิตศาสตร์โอลิมปิกระหว่างประเทศ ครั้งที่ 30 สมาคมคณิตศาสตร์แห่งประเทศไทยฯ ได้จัดคณาจารย์มหาวิทยาลัยจำนวนหนึ่งมาช่วยฝึกอบรมรวมเป็นเวลาประมาณสองเดือน เพื่อให้นักเรียนได้เรียนรู้เนื้อหาเพิ่มเติมครอบคลุมหลักสูตรที่จะใช้แข่งขัน ซึ่งอยู่ในระดับชั้นปีที่ 1-2 ของมหาวิทยาลัย จากผลสำเร็จในปีแรก ทำให้รัฐบาลเห็นความสำคัญจึงได้จัดสรรงบประมาณให้กับโครงการนี้ผ่านสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ตั้งแต่ปี พ.ศ. 2533 เป็นต้นมา สมทบกับเงินพระราชทานเป็นรายปีจากสมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ เพื่อสนับสนุนการส่งนักเรียนไทยไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศ 5 สาขา จนถึงปัจจุบันรวม 14 ปี นักเรียนไทยได้ทำชื่อเสียงได้เหรียญทองรวม 17 เหรียญ เหรียญเงิน 53 เหรียญ เหรียญทองแดง 93 เหรียญ และเกียรติคุณประกาศอีก 35 ราย รวมทั้งสิ้น 198 รางวัล จากจำนวนนักเรียนที่ส่งไปแข่งขัน 276 คน (72%)

อย่างไรก็ตาม จากการที่ประเทศไทยดำเนินการจัดส่งนักเรียนเข้าร่วมการแข่งขันคณิตศาสตร์ วิทยาศาสตร์ โอลิมปิกระหว่างประเทศ ตั้งแต่ พ.ศ.2532 จนถึงปัจจุบัน ทำให้เห็นว่ามาตรฐานการศึกษาด้านคณิตศาสตร์และวิทยาศาสตร์ของไทยยังต่ำกว่ามาตรฐานสากล การเตรียมตัวของนักเรียนยังใช้เวลานานเกินไป

เพื่อให้การส่งเสริมและสนับสนุน โครงการจัดส่งผู้แทนประเทศไทยไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศมีประสิทธิภาพยิ่งขึ้นสมเด็จพระเจ้า พี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ จึงมีพระดำริให้จัดตั้งมูลนิธิ สอวน. และได้รับอนุมัติจากกระทรวงมหาดไทยเมื่อวันที่ 12 ตุลาคม 2542 โดยมีวัตถุประสงค์หลัก 2 ประการ

วัตถุประสงค์

1. ส่งเสริมให้นักเรียนในระดับมัธยมศึกษาตอนปลายทั่วประเทศที่มีความสามารถทางวิทยาศาสตร์และคณิตศาสตร์ มีโอกาสได้รับการพัฒนาศักยภาพทางด้านคณิตศาสตร์ คอมพิวเตอร์ เคมี ฟิสิกส์ และชีววิทยา ตามความถนัดทั้งด้านทฤษฎีและทักษะด้านปฏิบัติ ให้สามารถวิเคราะห์และแก้ปัญหาที่ซับซ้อนได้ โดยจัดให้มีศูนย์อบรมทั่วประเทศเป็นการเพิ่มเวลาฝึกอบรม เพื่อช่วยให้นักเรียนมีความพร้อมที่จะเข้ารับการคัดเลือกไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศให้ได้ผลดียิ่งขึ้น ตามพระดำริของสมเด็จพระเจ้าพี่นางเธอเจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ องค์ประธานมูลนิธิ สอวน.
2. เพื่อนำประสบการณ์ที่ได้จากการแข่งขันโอลิมปิกวิชาการระหว่างประเทศมาพัฒนามาตรฐานคณิตศาสตร์และวิทยาศาสตร์ศึกษาของไทยให้สูงขึ้นเทียบเท่าระดับสากล

โครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.

มูลนิธิส่งเสริมโอลิมปิกวิชาการและพัฒนามาตรฐานวิทยาศาสตร์ศึกษา ในพระอุปถัมภ์สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ (สอวน.) ได้ร่วมมือกับคณาจารย์มหาวิทยาลัยของรัฐ 20 แห่ง และกระทรวงศึกษาธิการ ดำเนินการจัดตั้งศูนย์ สอวน. ในภูมิภาค 12 ศูนย์ และในกรุงเทพฯ 1 ศูนย์ (5 โรงเรียน) เพื่อพัฒนาศักยภาพทางปัญญาของนักเรียนที่มีความพร้อมในด้านวิทยาศาสตร์ คณิตศาสตร์และคอมพิวเตอร์จากทั่วประเทศ เพื่อให้นักเรียนได้มีความรู้ความสามารถเทียบเท่ามาตรฐานสากล และพร้อมที่จะสอบคัดเลือกเป็นผู้แทนประเทศไทยไปร่วมการแข่งขันโอลิมปิกวิชาการระหว่างประเทศในสาขาวิชาต่างๆ ได้ และเพื่อขยายผลจากประสบการณ์ที่ได้เข้าแข่งขัน โอลิมปิกวิชาการระหว่างประเทศมาพัฒนามาตรฐานวิทยาศาสตร์และคณิตศาสตร์ของไทยให้สูงขึ้นเทียบเท่าสากล

ในการอบรมนักเรียนของศูนย์ สอวน. มูลนิธิ สอวน. ได้พิจารณาเห็นว่าตำราที่มีความสมบูรณ์ของเนื้อหาตามหลักสูตรของ สอวน. จะช่วยพัฒนาศักยภาพของนักเรียนในศูนย์ สอวน. ให้สูงขึ้นได้ นอกจากนั้นตำราเรียนในวิชาวิทยาศาสตร์และคณิตศาสตร์ในระดับมัธยมศึกษาตอนปลายที่มีความสมบูรณ์ถูกต้องยังขาดแคลน นักเรียนและครูสามารถนำตำราที่พัฒนาขึ้นมานี้ไปใช้เป็นหนังสืออ้างอิงประกอบการเรียนการสอนได้อีกด้วย มูลนิธิ สอวน. จึงได้มี “โครงการจัดทำตำราส่งเสริมพัฒนาศักยภาพของนักเรียนด้านวิทยาศาสตร์ คณิตศาสตร์และคอมพิวเตอร์” ขึ้น เพื่อผลิตตำราคณิตศาสตร์ คอมพิวเตอร์ เคมี ชีววิทยาและฟิสิกส์ที่มีเนื้อหาหลักสูตรตามมาตรฐานสากล โดยมีวัตถุประสงค์

1. เพื่อเป็นที่ระลึกในมหามงคลสมัยที่สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ ทรงเจริญพระชนมายุ 80 พรรษา ซึ่งพระองค์ทรงมีพระมหากรุณาธิคุณต่อโครงการจัดตั้งผู้แทนประเทศไทยไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศและทรงสนับสนุนการดำเนินงานเพื่อพัฒนามาตรฐานการศึกษาวิทยาศาสตร์และคณิตศาสตร์ของไทยอย่างหาที่สุดมิได้

2. เพื่อผลิตหนังสือคณิตศาสตร์ คอมพิวเตอร์ เคมี ชีววิทยาและฟิสิกส์ระดับมัธยมศึกษาตอนปลายถึงระดับชั้นปีที่ 1 ของคณะวิทยาศาสตร์ในมหาวิทยาลัยให้มีคุณภาพเทียบเท่าสากล เรียบเรียงโดยคณาจารย์จากมหาวิทยาลัยของรัฐที่มีประสบการณ์สูง และที่มีส่วนรวมในการฝึกอบรมนักเรียนในค่าย สอวน. ค่าย สสวท. และควบคุมนักเรียนไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศ เนื้อหาในหนังสือเน้นกระบวนการคิดแบบวิทยาศาสตร์ เพื่อฝึกฝนให้นักเรียนสามารถคิดวิเคราะห์และแก้ปัญหาที่ซับซ้อนทั้งในเชิงทฤษฎีและประยุกต์ได้โดยจัดพิมพ์บนกระดาษอาร์ตอย่างดีและมีภาพสีประกอบคำบรรยาย

โครงการตำราวิทยาศาสตร์และคณิตศาสตร์ของมูลนิธิ สอวน. มีเป้าหมายในการผลิตตำราคณิตศาสตร์ รวม 5 เล่ม คอมพิวเตอร์ 3 เล่ม เคมี 3 เล่ม ชีววิทยา 5 เล่ม และฟิสิกส์ 3 เล่ม โดยหนังสือชุดแรกจะนำขึ้นทูลเกล้าถวายในวันที่ 6 มิถุนายน 2547 ซึ่งเป็นวันประชุมสามัญประจำปี พ.ศ. 2547 ของคณะกรรมการบริหาร และสมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ เสด็จเป็นองค์ประธานที่ประชุม ส่วนที่เหลือคาดว่าจะจัดพิมพ์ให้แล้วเสร็จภายในปี พ.ศ. 2547 นี้ นอกจากนั้นคณะกรรมการโครงการผลิตตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน. มีเป้าหมายจะผลิตตำราที่มีคุณภาพสูงนี้ในระดับมัธยมศึกษาต้นโดยคณาจารย์จากมหาวิทยาลัย เพื่อวางรากฐานวิทยาศาสตร์และคณิตศาสตร์พื้นฐานและเพื่อสร้างแรงบันดาลใจและความสนใจทางด้านวิทยาศาสตร์ คณิตศาสตร์แก่เยาวชนอีกด้วย หากได้รับความอนุเคราะห์ช่วยเหลือด้านงบประมาณจากภาครัฐและเอกชน

คณะจัดทำหนังสือคณิตศาสตร์ วิทยาศาสตร์หวังว่าโครงการตำราคณิตศาสตร์ วิทยาศาสตร์ของมูลนิธิ สอวน. จะมีส่วนร่วมในการปฏิรูปการเรียนรู้และยกระดับมาตรฐานวิทยาศาสตร์และคณิตศาสตร์ของไทยให้เทียบเท่ากับระดับสากลเพื่อสนองพระดำริของสมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์

*คำขอบคุณ : คณะกรรมการดำเนินงานโครงการตำราฯ ขอขอบคุณพิพิธภัณฑ ARITHMEUM, Bonn ที่อนุญาต

ให้ประธานคณะกรรมการฯ เข้าถ่ายภาพในพิพิธภัณฑ เพื่อนำมาเผยแพร่

คณะกรรมการโครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอน.

คณะกรรมการที่ปรึกษา

1. ศาสตราจารย์ นายแพทย์ จรัส สุวรรณเวลา
2. รองศาสตราจารย์ ดร.กำจัด มงคลกุล
3. ดร. คุณหญิงกษมา วรวรรณ ณ อยุธยา
4. รองศาสตราจารย์ ดร. คุณหญิงสุมณฑา พรหมบุญ
5. นายเชาว์ อรรถมานะ (อดีต)
6. นายสมนึก พิมลเสถียร
7. นายสุนทร อรุณานนท์ชัย
8. รองศาสตราจารย์บุญรักษา สุนทรธรรม

รองประธานมูลนิธิ สอน.
กรรมการมูลนิธิฯ
กรรมการมูลนิธิฯ
กรรมการมูลนิธิฯ
กรรมการมูลนิธิฯ
กรรมการมูลนิธิฯ
กรรมการมูลนิธิฯ
กรรมการมูลนิธิฯ

คณะกรรมการดำเนินงานโครงการตำราฯ

1. ศาสตราจารย์ศักดิ์ ศิริพันธุ์ (ราชบัณฑิต) เลขาธิการมูลนิธิ สอน.
2. รองศาสตราจารย์เย็นใจ สมวิเชียร
3. รองศาสตราจารย์ ดร. ณรงค์ ปิ่นนัม
4. รองศาสตราจารย์ยืน ภู่วรรณ
5. รองศาสตราจารย์ ดร. พินิติ รตะนานุกูล
6. ผู้ช่วยศาสตราจารย์ ดร. วุทธิพันธุ์ ปรัชญพฤทธิ์
7. ศาสตราจารย์อักษร ศรีปลั่ง
8. รองศาสตราจารย์ ดร. อุษณีย์ ยศยิ่งยวด

ประธาน
รองประธาน
กรรมการ (วิชาคณิตศาสตร์)
กรรมการ (วิชาคอมพิวเตอร์)
กรรมการ (วิชาเคมี)
กรรมการ (วิชาฟิสิกส์)
กรรมการ (วิชาชีววิทยา ประเภทพืช)
กรรมการ (วิชาชีววิทยา ประเภทสัตว์)

คณะผู้เขียนวิชาคณิตศาสตร์

1. รองศาสตราจารย์ ดร. ณรงค์ ปิ่นนัม
2. ศาสตราจารย์ กิตติคุณยุพิน พิพิธกุล
3. ผู้ช่วยศาสตราจารย์ ดร. อุษณีย์ ธีรวัฒน์
4. ผู้ช่วยศาสตราจารย์ ดร. นิตติยา ปภาพจน์
5. รองศาสตราจารย์ ดร. ณวีวรรณ รัตนประเสริฐ
6. รองศาสตราจารย์ ดร. วิเชียร เลหาโกศล
7. ดร. ภัทธิตรา เรืองสินทรัพย์
8. นายวัชรพล พิมพ์เสริฐ

ประธานคณะกรรมการ
อนุกรรมการ
อนุกรรมการ
อนุกรรมการ
อนุกรรมการ
อนุกรรมการ
อนุกรรมการ
อนุกรรมการ

คำนำ

ตำราทฤษฎีจำนวนเล่มนี้ ผู้เขียนได้เขียนขึ้นมาโดยมีวัตถุประสงค์ 5 ประการ คือ

1. เพื่อรวบรวมความรู้พื้นฐานที่จำเป็นในการศึกษาทฤษฎีจำนวนเบื้องต้น
2. เพื่อให้ง่ายต่อการอ่านของนักเรียน นิสิต นักศึกษาและง่ายต่อผู้สอนที่จะนำตำราเล่มนี้ไป เพื่อใช้ในการสอน
3. เพื่อให้เหมาะสมสำหรับผู้สนใจในวงกว้าง ทั้งทางด้านคณิตศาสตร์บริสุทธิ์และคณิตศาสตร์ประยุกต์
4. เพื่อให้ผู้เรียนได้มีโอกาสพัฒนาทักษะทางการพิสูจน์จากตัวอย่างง่าย ๆ
5. เพื่อให้ผู้เรียนได้มีโอกาสฝึกการแก้ปัญหาโจทย์ทางด้าน “การแก้ปัญหาทางทฤษฎีจำนวน” โดยมีการบรรจุแบบฝึกหัดในหลายระดับเรียงตามความยากง่าย

เพื่อให้ตำราเล่มนี้บรรลุตามวัตถุประสงค์ที่ได้ตั้งไว้ ผู้เขียนได้เริ่มต้นกล่าวถึงประวัติความเป็นมาของการศึกษาทฤษฎีจำนวนโดยเริ่มจากปีทาโกรัส (Pythagoras 569-500 ปีก่อนคริสต์ศักราช) ซึ่งนับเป็นเวลากว่า 2500 ปีแล้ว ทฤษฎีจำนวนนับว่าเป็นศาสตร์ในสาขาคณิตศาสตร์เก่าแก่ที่สุดและได้ถูกพัฒนาขึ้นมาเรื่อยๆ โดยนักคณิตศาสตร์แต่ละยุค แต่ละสมัย โดยนักคณิตศาสตร์รุ่นต่อๆ มา พยายามที่จะตอบปัญหาที่นักคณิตศาสตร์รุ่นก่อนๆ ยังไม่สามารถหาคำตอบได้ ความพยายามในการหาคำตอบของปัญหาทำให้เกิดเทคนิคและแนวคิดใหม่ๆ อย่างไรก็ตามผู้อ่านจะได้พบว่าการพัฒนาเทคนิคและแนวคิดที่ได้รับการพัฒนาขึ้นมาก็ยังไม่เพียงพอที่จะตอบปัญหาได้ทุกๆ ปัญหาซึ่งผู้อ่านก็จะได้พบ “ข้อคาดเดา (Conjecture)” มากมายในการศึกษาทฤษฎีจำนวน

เนื้อหาทางด้านทฤษฎีจำนวนได้รับการนำไปประยุกต์ใช้ในด้านต่างๆ มากมายเช่น ทฤษฎีรหัส (Coding Theory), การพัฒนาของขั้นตอนวิธีในการสั่งงานของคอมพิวเตอร์, การกำหนดแถบรหัสสินค้า (Bar code) การกำหนดการออกชุดของเลขรหัสของบัตรเครดิตต่างๆ ตลอดจนใช้เป็นกฎเกณฑ์ในการออกบัตรประจำตัวประชาชนของบางประเทศ

ตำราทฤษฎีจำนวนเล่มนี้ได้รับรู้เนื้อหาที่เพียงพอในการใช้เป็นแนวทางในการสอนวิชาทฤษฎีจำนวนในทุกๆ ระดับ ตั้งแต่ระดับมัธยมศึกษาสำหรับนักเรียนที่มีความสามารถพิเศษ จนถึงระดับนิสิต-นักศึกษาในระดับปริญญาตรี ทั้งในส่วนเนื้อหาสาระที่กำหนดไว้เป็นขั้นตอนและวิวัฒนาการ เพื่อให้ผู้อ่านได้เห็นความพยายามของนักคณิตศาสตร์ในอดีต นอกจากนั้นเพื่อให้สอดคล้องกับยุคโลกาภิวัตน์ ผู้เขียนยังได้รับรู้ข้อมูลข่าวสารที่ทันสมัยผ่านทาง website เช่น www.yahoo.com หรือ www.google.com โจนดระหนักถึงวิวัฒนาการที่รวดเร็วทางด้านคณิตศาสตร์และตระหนักถึงความทันสมัยของเนื้อหาวิชา ซึ่งเป็นที่ทราบดีว่าเมื่อตำราเล่มนี้ได้ถูกพิมพ์เผยแพร่และผู้อ่านทุกๆ ท่านเมื่อได้อ่านตำราเล่มนี้แล้วอาจพบว่าตำราเล่มนี้ขาดความทันสมัยในเนื้อหาสาระบางส่วน ดังนั้นเพื่อให้ตำราเล่มนี้ยังคงมีความทันสมัยในด้านเนื้อหาสาระ ผู้เขียนสนับสนุนให้ผู้อ่านได้ติดตามข้อมูลข่าวสารที่ทันสมัยได้จาก website ที่กำหนดข้างต้น

แบบฝึกหัดท้ายหัวข้อของแต่ละบทมีความสำคัญในการทำความเข้าใจในเนื้อหาที่ได้เรียนในแต่ละหัวข้อและแบบฝึกหัดท้ายบทก็มีความสำคัญในการตรวจสอบความเข้าใจในหัวข้อต่างๆ ในบทนั้นๆ แบบฝึกหัดมีความหลากหลายทั้งง่ายและยาก ผู้เขียนขอให้ผู้อ่านทุกท่านใช้ความพยายามในการทำแบบฝึกหัดเพื่อพัฒนาทางด้านความคิดและเป็นพื้นฐานที่ดีในการศึกษาคณิตศาสตร์ต่อไป

ISBN 974-92235-1-9

สงวนลิขสิทธิ์

จัดพิมพ์โดย มุลนิธิ สอวน.

พิมพ์ครั้งที่ 2 พ.ศ. 2548 (2005)

ออกแบบปก หน้ารองปกและหน้านำบทที่ 1 โดย ศาสตราจารย์ศักดิ์ดา ศิริพันธ์

ศิลปกรรม: นายปรีชา นัตระเนตร

พิมพ์ที่ บริษัทด้านสุทธาการพิมพ์ จำกัด

แยกสี่ / เพลท เอ็นอาร์ ฟิล์ม

ที่ปรึกษา

อาจารย์ไอศุรีย์ สุดประเสริฐ

วท.ม. (คณิตศาสตร์) จุฬาลงกรณ์มหาวิทยาลัย

ผู้เขียน

รองศาสตราจารย์ ดร. ณรงค์ ปิ่นนัม

Ph.D. (Mathematics) University of The Philippines

ผู้ช่วยศาสตราจารย์ ดร. นิตติยา ปากาพจน์

กศ.ก. (คณิตศาสตร์ศึกษา) มหาวิทยาลัยศรีนครินทรวิโรฒ

สารบัญ

บทที่ 1 ความรู้เบื้องต้น

1.1	บทนำ	1
1.2	ระบบจำนวนเต็ม	6
1.3	หลักอุปนัยเชิงคณิตศาสตร์	11
1.4	ข้อแนะนำบางประการเกี่ยวกับจำนวนเต็ม	16
	โจทย์ปัญหาเสริมเรื่อง ความรู้เบื้องต้น	20
	แบบฝึกหัดเรื่องความรู้เบื้องต้น	27

บทที่ 2 การหารลงตัว

2.1	ขั้นตอนวิธีการหาร	29
2.2	นิยามการหารลงตัว	32
2.3	สมบัติเบื้องต้นของการหารลงตัว	34
2.4	ตัวหารร่วมมาก	36
2.5	ขั้นตอนวิธีแบบยุคลิด	41
2.6	ตัวคูณร่วมน้อย	44
	โจทย์ปัญหาเสริมเรื่อง การหารลงตัว	48
	แบบฝึกหัดเรื่องการหารลงตัว	45

บทที่ 3 จำนวนเฉพาะ

3.1	นิยามของจำนวนเฉพาะ	57
3.2	ทฤษฎีบทหลักมูลของเลขคณิต	61
3.3	การค้นหาจำนวนเฉพาะ	65
	โจทย์ปัญหาเสริมเรื่อง จำนวนเฉพาะ	68
	แบบฝึกหัดเรื่องจำนวนเฉพาะ	71

บทที่ 4 ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ

4.1	ทฤษฎีบทสำคัญของจำนวนเฉพาะ	73
4.2	ข้อคาดเดาที่เกี่ยวข้องกับจำนวนเฉพาะ	79
4.3	จำนวนเฉพาะแฟร์มาต์	82
4.4	จำนวนเฉพาะเมอร์เซน	84
	โจทย์ปัญหาเสริมเรื่อง ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ	88
	แบบฝึกหัดเรื่องข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ	91

บทที่ 5 ฟังก์ชันเลขคณิต

5.1	ฟังก์ชันแยกคุณ	94
5.2	ฟังก์ชัน τ	98
5.3	ฟังก์ชัน σ และ σ_k	101
5.4	ฟังก์ชัน ϕ	106
5.5	ฟังก์ชัน μ	111
5.6	ฟังก์ชันจำนวนเต็มค่ามากที่สุด	115
	โจทย์ปัญหาเสริมเรื่อง ฟังก์ชันเลขคณิต	121
	แบบฝึกหัดเรื่องฟังก์ชันเลขคณิต	125

บทที่ 6 คอนกรูเอนซ์

6.1	นิยามและสมบัติของคอนกรูเอนซ์	128
6.2	สมการคอนกรูเอนซ์	136
6.3	ทฤษฎีบทของแฟร์มาต์และออยเลอร์	154
	โจทย์ปัญหาเสริมเรื่อง คอนกรูเอนซ์	161
	แบบฝึกหัดเรื่องคอนกรูเอนซ์	165

บทที่ 7 สมการไดโอแฟนไทน์

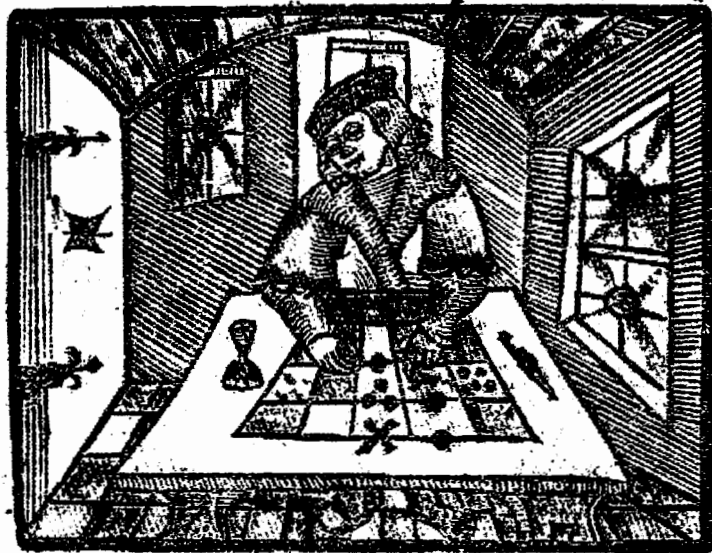
7.1	บทนำ	169
7.2	สมการเชิงเส้นดีกรีหนึ่ง	170
7.3	สมการของปีทาโกรัส	178
7.4	สมการ $x^4 + y^4 = z^2$ และ $x^4 + y^4 = z^4$	184
7.5	สมการไดโอแฟนไทน์กำลังสอง	186
	โจทย์ปัญหาเสริมเรื่อง สมการไดโอแฟนไทน์	193
	แบบฝึกหัดเรื่องสมการไดโอแฟนไทน์	195

บรรณานุกรม	197
------------	-----

ดัชนี	199
-------	-----

บัญชีสัญลักษณ์	201
----------------	-----

Rechnung auff der linihen
 gemache durch Adam Riesen vonn Staffels-
 steyn/ in massen man es pflege zu lern in allen
 rechnenschulen grundlich begriffen anno 1518.
 vleysiglich vberlesen/ vnd zum andern mal
 in trugk vorfertiger.



¶ Gedruckt zu Wessforde zum
 Schwarzen Horn.
 1525.

บทที่ 1

ความรู้เบื้องต้น

1.1 บทนำ

วิชาทฤษฎีจำนวน (เลขคณิตชั้นสูง) เป็นวิชาที่ศึกษาเกี่ยวกับสมบัติของจำนวนโดยเฉพาะอย่างยิ่งสมบัติของจำนวนเต็มและจำนวนนับ เนื่องจากจำนวนนับเป็นจำนวนชนิดแรกที่มนุษย์รู้จัก สมบัติต่าง ๆ ของจำนวนนับจึงเป็นสิ่งที่สนใจของมนุษย์ตลอดเวลาอันยาวนาน มีแง่มุมต่าง ๆ ที่มนุษย์ได้ศึกษาค้นคว้าไว้มากมายหลายแง่มุมและอาจกล่าวได้ว่าไม่มีวันที่จะจบสิ้นตราบที่มนุษย์ยังมีความคิด จินตนาการ และมีความยากู้อากเห็นในความมหัศจรรย์ของจำนวนเหล่านั้นอยู่ (สมใจ จิตพิทักษ์. 2545 : คำนำ) ซึ่งคำกล่าวนี้อาจสอดคล้องกับนักคณิตศาสตร์หลายท่านและอาจกล่าวว่าวิชาทฤษฎีจำนวนเป็นวิชาที่มีความสำคัญอย่างยิ่งวิชาหนึ่งจนได้รับการยกย่องจาก คาร์ล ฟรีดริช เกาส์ (Carl Friedrich Gauss ค.ศ. 1777 – 1855) ที่กล่าวว่า “ทฤษฎีจำนวนเปรียบเสมือนเป็นราชินีแห่งคณิตศาสตร์ (Number Theory is the queen of mathematics)” ธรรมชาติของวิชาทฤษฎีจำนวนนั้นง่ายต่อการเรียนรู้เพราะอาศัยความรู้เพียงน้อยนิดแต่พัฒนาความคิดได้หลากหลายและลึกซึ้ง และเป็นตัวแบบที่เปิดโอกาสให้ผู้เรียนได้ค้นพบความสำเร็จในการแก้ปัญหาด้วยตนเอง โดยเฉพาะอย่างยิ่งผู้เรียนที่มีความคิดสร้างสรรค์จะได้มีโอกาสแสดงความสามารถของตนเองออกมาในลักษณะการแก้ปัญหาต่าง ๆ ที่หลากหลายในวิชาทฤษฎีจำนวน

ทฤษฎีจำนวนเป็นสาขาหนึ่งที่เก่าแก่ที่สุดทางคณิตศาสตร์ เพราะถูกพัฒนามาตั้งแต่สมัยกรีกโบราณเมื่อประมาณ 2500 ปีมาแล้ว โดยพิจารณาจากหลักฐานที่ปรากฏในอดีต นักคณิตศาสตร์มีความเห็นว่าน่าจะเริ่มจากยุคของพีทาโกรัส (Pythagoras 569 – 500 ปีก่อนคริสต์ศักราช) และปัจจุบันยังได้รับการศึกษาค้นคว้าอีกมากมายจากทั้งนักคณิตศาสตร์มืออาชีพและมือสมัครเล่น ด้วยเหตุผลที่ว่าปัญหาทางทฤษฎีจำนวนนั้นชวนคิดและท้าทายความสามารถ มีความง่ายที่จะทำความเข้าใจประกอบกับปัญหาแต่ละปัญหาคูเหมือนว่ามีโอกาสหาคำตอบได้ นอกจากนี้ยังมีข้อคาดเดา (conjecture) และปัญหาที่ยังไม่สามารถหาคำตอบได้ (unsolved problems) อีกมากมายน่าสนใจจะศึกษา

โดยทั่วไปเป็นที่ยอมรับกันว่า พีทาโกรัส และศิษย์เป็นผู้ริเริ่มในการพัฒนาจำนวน พีทาโกรัสและศิษย์มีความเชื่อว่าทฤษฎีจำนวนจะอธิบายสิ่งต่าง ๆ ในจักรวาลคือจำนวน แนวคิดของคณกลุ่มนี้ยึดปรัชญาว่า “ทุกสิ่งทุกอย่างคือจำนวน”

การศึกษาจำนวนในสมัยของปีทาโกรัส ได้นำความมหัศจรรย์ของจำนวนไปผูกพันกับความเชื่อโชคลางโหราศาสตร์และราศี เช่น จำนวนมิตรภาพ (*amicable numbers*) คู่แรก ที่เชื่อว่าพบในสมัยของปีทาโกรัส คือ 284 และ 220 สองจำนวนนี้มีสมบัติพิเศษ คือตัวหารแท้ของจำนวนหนึ่งมีผลบวกเท่ากับตัวหารแท้ของอีกจำนวนหนึ่ง กล่าวคือ ตัวหารแท้ของ 284 ได้แก่ 1, 2, 4, 71 และ 142 มีผลบวกเป็น 220 ตัวหารแท้ของ 220 ได้แก่ 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 และ 110 มีผลบวกเป็น 284 ผู้ที่เชื่อโชคลางจะจารึกตัวเลขลงในเครื่องรางของขลัง โดยเชื่อว่าคนใดได้ห้อยของขลังที่จารึกตัวเลขดังกล่าวจะเป็นมิตรแท้ต่อกัน ในปี ค.ศ. 1636 ปีแยร์ เดอ แฟร์มาต์ (Pierre De Fermat ค.ศ. 1601 – 1665) พบจำนวนมิตรภาพคู่ที่สองคือ 17,296 และ 18,416 ต่อมาในปี ค.ศ. 1638 เรอเน เดส์การ์ตส์ (René Descartes ค.ศ. 1596 – 1650) พบจำนวนมิตรภาพคู่ที่สามคือ 9,363,584 และ 9,437,056 จากนั้นในปี ค.ศ. 1747 เลออนฮาร์ด ออยเลอร์ (Leonhard Euler ค.ศ. 1707 – 1783) ได้เสนอจำนวนมิตรภาพถึง 64 คู่ แต่จากการตรวจสอบโดยนักคณิตศาสตร์รุ่นหลัง ปรากฏว่ามี 2 คู่ในจำนวน 64 คู่ ไม่ใช่จำนวนมิตรภาพ แต่ค้นพบหลังจากออยเลอร์ประกาศเกือบ 200 ปี ในปี ค.ศ. 1830 อาเดรียง มารี เลอจองด์ (Adrien Marie Legendre ค.ศ. 1752 – 1833) ได้พบคู่ใหม่อีก 1 คู่ คือ 2,172,649,216 และ 8,520,191 ในปี ค.ศ. 1866 เด็กชายนิโคโล ปาินี (Nicolo Painini) ชาวอิตาลีอายุ 16 ปี พบจำนวนมิตรภาพที่น้อยกว่าของแฟร์มาต์ คือ 1,184 และ 1,210 ต่อมาในปี ค.ศ. 1981 ฮิลตัน เซน (Hilton Chen) และเดล วูดส์ (Dale Woods) ได้พบจำนวนมิตรภาพที่มีขนาด อีกคู่หนึ่งโดยแต่ละจำนวนประกอบด้วย 50 หลัก คือ

$$21,741,269,040,875,890,083,566,772,572,567,935,979,368,836,363,843$$

และ

$$22,261,723,990,815,556,829,012,769,686,652,975,057,619,942,956,477$$

และในปัจจุบันโดยการใช้คอมพิวเตอร์ในการค้นหาจำนวนมิตรภาพ เราพบว่ามีทั้งหมด 6,262,871 คู่ (ข้อมูล ณ ปี ค.ศ. 2004)

อีกหนึ่งตัวอย่างที่เกี่ยวกับความเชื่อถือในความมหัศจรรย์ของจำนวน คือ จำนวนสมบูรณ์ (*perfect number*) เป็นจำนวนที่มีสมบัติพิเศษ คือจำนวนนั้นมีค่าเท่ากับผลบวกของตัวหารแท้ทั้งหมดของจำนวนนั้น เช่น 6 เป็นจำนวนสมบูรณ์ เพราะมี 1, 2, 3 เป็นตัวหารแท้ และ $6 = 1 + 2 + 3$ ในสมัยนั้นเชื่อว่าพระเจ้าสร้างโลกและสร้างเสร็จภายใน 6 วัน ซึ่งเป็นจำนวนสมบูรณ์ จนถึงปี ค.ศ. 1952 มีการพบจำนวนสมบูรณ์รวม 12 จำนวน ทุกจำนวนเป็นจำนวนคู่ สามจำนวนแรกคือ 6, 28 และ 496 ต่อมาในปี ค.ศ. 2004 ได้มีการค้นพบจำนวนสมบูรณ์รวมทั้งสิ้น 40 จำนวน ซึ่งรายละเอียดของการค้นพบศึกษาได้ในบทที่ 4

การศึกษาเกี่ยวกับทฤษฎีจำนวนมีหลักฐานเด่นชัดในสมัยของกรีกประมาณ 300 ปีก่อน คริสต์ศักราช ปรากฏในหนังสืออีลิเมนต์ซึ่งเรียบเรียงโดย ยูคลิด แห่งอะเล็กซานเดรีย (Euclid of Alexandria ประมาณ 450 – 380 ก่อน คริสต์ศักราช) มี 13 เล่ม เล่มที่ 7, 8 และ 9 มีเรื่องราวเกี่ยวกับทฤษฎีจำนวน เนื้อหาที่รู้จักกันดีในปัจจุบัน ได้แก่ จำนวนเต็มคู่ จำนวนเต็มคี่ จำนวนเฉพาะ ทฤษฎีบทขั้นตอนวิธีแบบยูคลิด ตัวหารร่วมมาก ตัวคูณร่วมน้อย และทฤษฎีบทที่ว่าจำนวนเฉพาะมีจำนวนอนันต์ เป็นต้น (สมวงษ์ แปลงประสพโชค. 2537 : 3)

ความเฟื่องฟูของทฤษฎีจำนวนหลังจากยุคของยูคลิดได้หยุดชะงักไป จนกระทั่งปี ค.ศ. 250 มีนักคณิตศาสตร์ชาวกรีกชื่อ ดีโอฟานโตสแห่งอะเล็กซานเดรีย (Diophantos of Alexandria) ได้ตีพิมพ์หนังสือจำนวน 13 เล่ม โดยดีโอฟานโตสสามารถแก้สมการทางพีชคณิตที่มีตัวไม่ทราบค่าสองตัวหรือสามตัวได้และปัญหาของดีโอฟานโตสหลาย ๆ ปัญหากลายเป็นจุดเริ่มต้นของทฤษฎีจำนวน โดยเฉพาะอย่างยิ่งดีโอฟานโตสสนใจสมการพีชคณิตที่มีคำตอบเป็นจำนวนเต็ม ปัจจุบันเราเรียกสมการพีชคณิตที่มีคำตอบเป็นจำนวนเต็มนี้ว่า สมการไดโอแฟนไทน์ (*Diophantine equation*) ตัวอย่างหนึ่งของสมการไดโอแฟนไทน์คือสมการสามจำนวนของปีทาโกรัส $x^2 + y^2 = z^2$ เป็นต้น

เมื่อสิ้นยุคของดีโอฟานโตสแล้วการพัฒนาทฤษฎีจำนวนมีเพียงเล็กน้อย มีหลักฐานแสดงถึงการพัฒนาทฤษฎีจำนวนในดินแดนแถบตะวันออกไกลในช่วงปี ค.ศ. 500 – 1200 โดยเฉพาะอย่างยิ่งในประเทศอินเดีย จนกระทั่งศตวรรษที่ 17 ทฤษฎีจำนวนได้กลับมาเจริญอีกครั้งในแถบยุโรปตะวันตกโดยมีนักคณิตศาสตร์ชาวฝรั่งเศสที่มีชื่อเสียงมากคือ แฟร์มาต์ ซึ่งต่อมาได้รับการยกย่องให้เป็นบิดาของทฤษฎีจำนวนสมัยใหม่ แฟร์มาต์ได้ศึกษางานของดีโอฟานโตสและเป็นคนแรกที่ค้นพบสมบัติของจำนวนเต็มมากมาย

เมื่อหมดยุคของแฟร์มาต์ไม่นาน ก็มีนักคณิตศาสตร์ที่มีชื่อเสียงทางด้านทฤษฎีจำนวนเกิดขึ้นอีกหลายคน อาทิ ออยเลอร์ ชาวสวิส, โชแซฟ ลุยส์ ลากรองจ์ (Joseph Louis Lagrange ค.ศ. 1736 – 1813) ชาวฝรั่งเศส, ปีเตอร์ กุสตาฟ เลอเจิน เลอจองด์ ชาวฝรั่งเศส, เกาส์ ชาวเยอรมัน, ดีริชเลต์ (Peter Gustav Lejeune Dirichlet ค.ศ. 1805 – 1859) ชาวเยอรมัน ตำราทฤษฎีจำนวนเล่มแรกได้ตีพิมพ์ขึ้นโดยเลอจองด์ในปี ค.ศ. 1798 และอีกสามปีถัดมา เกาส์ก็ได้ตีพิมพ์หนังสือชื่อ *Disquisitiones Arithmeticae* ซึ่งเป็นหนังสือเกี่ยวกับทฤษฎีจำนวนที่ได้ทำการพิสูจน์ทฤษฎีบทต่าง ๆ ไว้อย่างเป็นระบบ จากหนังสือเล่มนี้ของเกาส์ก่อให้เกิดประโยชน์ต่อคณิตศาสตร์ในสาขาอื่นเป็นอย่างมาก และตัวเกาส์เองก็ถือว่าหนังสือทฤษฎีจำนวนเล่มนี้เป็นผลงานอันยิ่งใหญ่ที่สุดของตน

จากประวัติของทฤษฎีจำนวนที่กล่าวมาทั้งหมดทำให้เราทราบถึงพัฒนาการตลอดจนนักคณิตศาสตร์ที่ยิ่งใหญ่และมีชื่อเสียงในด้านทฤษฎีจำนวน นักคณิตศาสตร์หลายท่านถือว่าทฤษฎีจำนวนเป็นรากฐานที่จะนำไปสู่การศึกษาคณิตศาสตร์สมัยใหม่หลายสาขาวิชา และในการศึกษาทฤษฎีจำนวนนั้น เราสามารถมองเห็นวิวัฒนาการต่าง ๆ เกี่ยวกับความพยายามของมนุษย์ที่จะตอบปัญหาต่าง ๆ ที่ยังไม่มีผู้ใดตอบได้ในอดีตดังตัวอย่างของปัญหาต่อไปนี้

ปัญหาเกี่ยวกับจำนวนเฉพาะ คือ จำนวนเฉพาะตัวที่ n คือจำนวนอะไร ตัวอย่างเช่น จำนวนเฉพาะตัวที่ 10 คือ 29 จำนวนเฉพาะตัวที่ 100 คือ 541 จำนวนเฉพาะตัวที่ 664,999 คือ 10,006,721 สูตรทั่วไปในการหาจำนวนเฉพาะตัวที่ n สำหรับ n ทุกจำนวน ยังไม่เป็นที่ทราบกัน อีกปัญหาหนึ่งเกี่ยวกับจำนวนเฉพาะคือ มีสูตรใดบ้างที่ให้แค่จำนวนเฉพาะ เมื่อหลายศตวรรษมาแล้วมีความเชื่อกันว่า ถ้า n เป็นจำนวนเต็มบวกแล้ว $n^2 + n + 41$ เป็นจำนวนเฉพาะ สูตรนี้เป็นจริงสำหรับ $n = 0, 1, 2, \dots, 39$ ซึ่งให้จำนวนเฉพาะติดต่อกัน 40 จำนวน แต่ไม่เป็นจริงสำหรับ $n = 40$ และ $n = 41$ (ทั้งสองกรณีมี 41 เป็นตัวประกอบร่วม) สูตรอีกสูตรหนึ่งที่ให้จำนวนเฉพาะติดต่อกันถึง 80 จำนวนคือ $n^2 - 79n + 1601$

เราสามารถพิสูจน์ต่อไปได้ว่าไม่มีพหุนามใด ๆ ที่ให้แค่จำนวนเฉพาะ แฟร์มาต์ได้เสนอว่า $F_n = 2^{2^n} + 1$ เป็นจำนวนเฉพาะ สำหรับทุก ๆ จำนวนเต็ม $n \geq 0$ เขาได้ตรวจสอบข้อเสนอของเขาสำหรับ $n = 0, 1, 2, 3, 4$ และพบว่า F_n คือ 3, 5, 17, 257, 65537 ตามลำดับ ซึ่งเป็นจำนวนเฉพาะ สำหรับ $n = 5$ จะได้ $F_5 = 4,294,967,297$ แฟร์มาต์ไม่ได้ตรวจสอบข้อเสนอของเขา จนกระทั่งในปี ค.ศ. 1732 ออยเลอร์ได้พิสูจน์ว่า $641 \mid F_5$ ดังนั้น F_5 ไม่เป็นจำนวนเฉพาะ ยังไม่เป็นที่ทราบกันว่าเมื่อ $n > 4$ มี F_n ตัวใดเป็นจำนวนเฉพาะอีกบ้าง จำนวนที่อยู่ในรูป $2^{2^n} + 1$ มีชื่อเรียกว่า จำนวนแฟร์มาต์ (Fermat number) ในกรณีที่มันเป็นจำนวนเฉพาะเรียกว่า จำนวนเฉพาะแฟร์มาต์ (Fermat prime)

ปัญหาเกี่ยวกับจำนวนเฉพาะอีกปัญหาหนึ่งคือ มีจำนวนเฉพาะกี่จำนวนที่น้อยกว่าหรือเท่ากับจำนวนเต็มบวก n ที่กำหนดให้ ต่อมาเกาส์ได้เสนอว่าคำตอบที่ใกล้เคียงคือ

$$\frac{n}{1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}}$$

อัตราส่วนของจำนวนนี้กับจำนวนของจำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ n จะเข้าใกล้ 1 เมื่อ n มีค่ามาก ๆ ทฤษฎีบทนี้มีชื่อรู้จักกันโดยทั่วไปว่า “ทฤษฎีบทของจำนวนเฉพาะ (Prime number theorem)” ทฤษฎีบทนี้อาตามาร์ (J. S. Hadamard ค.ศ. 1865 – 1963) และ ปูแซง (C. V. Poussin ค.ศ. 1866 – 1962) พิสูจน์ได้ในปี ค.ศ. 1896 โดยใช้สมบัติของฟังก์ชันซีตา (zeta function) ในวิชาทฤษฎีฟังก์ชันเชิงซ้อน (Complex Function Theory) ต่อมาในปี ค.ศ. 1949 อาเทิล เซลเบิร์ก (Atle Selberg) และ พอล เออดอส (Paul Erdős ค.ศ. 1913 – 1996) พิสูจน์ได้อีกทางหนึ่งโดยใช้ทฤษฎีบททางเลขคณิตซึ่งก็ยากและซับซ้อนมาก

ถ้าให้จำนวนใด ๆ มา เราจะบอกได้อย่างไรว่าจำนวนนั้นเป็นจำนวนเฉพาะหรือไม่ ในปัจจุบันยังไม่มีสูตรทั่วไปที่จะตอบคำถามนี้ บางครั้งเราอาจลองผิดลองถูก หาดั้วประกอบของจำนวนดังกล่าว แล้วสรุปว่าเป็นจำนวนประกอบ แต่ถ้ามีเลข 20 หลัก ตัวอย่างเช่น

$$32,598,158,477,190,044,731$$

ถ้าถามว่า ตัวเลข 20 หลักดังกล่าวนี้เป็นจำนวนเฉพาะหรือไม่ จะทดสอบได้อย่างไร มีวิธีการทางทฤษฎีบทบางวิธีที่จะตอบคำถามนี้ แต่ใช้ได้ไม่สะดวกอย่างยิ่งในทางปฏิบัติ ตัวอย่างเช่น มีทฤษฎีบทที่ว่าจำนวนเต็มบวก n เป็นจำนวนเฉพาะก็ต่อเมื่อ $n \mid [(n-1)! + 1]$

ตัวอย่างเช่น $5 \mid [4! + 1]$ ดังนั้น 5 เป็นจำนวนเฉพาะ

$6 \nmid [5! + 1]$ ดังนั้น 6 ไม่เป็นจำนวนเฉพาะ

ทฤษฎีบทเหล่านี้น่าสนใจแต่ก็ใช้ประโยชน์อะไรได้ไม่มากนัก เช่น ในการตรวจสอบเลข 20 หลักข้างต้นว่าเป็นจำนวนเฉพาะหรือไม่

มีปัญหาลหลายปัญหาที่อยู่ในแวดวงของจำนวนเฉพาะ เช่น จำนวนเฉพาะคู่แฝด (twin prime) มีได้ไม่จำกัดจำนวนหรือไม่ จำนวนเฉพาะคู่แฝดคือคู่ของจำนวนเต็มบวก p และ $p + 2$ ซึ่งต่างเป็นจำนวนเฉพาะ ตัวอย่างเช่น 5 และ 7, 11 และ 13, 17 และ 19, 29 และ 31, 10,006,427 และ 10,006,429 เป็นต้น (สมใจ จิตพิทักษ์. 2545 : 3 – 4) จากการใช้เครื่องคอมพิวเตอร์พบว่า มีจำนวนเฉพาะคู่แฝดที่น้อยกว่า 30,000,000 อยู่ทั้งหมด 152,892 คู่ และจำนวนเฉพาะคู่แฝดที่อยู่ระหว่าง 999,999,990,000 และ 1,000,000,000,000 มี 15 คู่ และระหว่าง 1,000,000,000,000 และ 1,000,000,010,000 มี 20 คู่ คู่หนึ่งในจำนวนนี้คือ 1,000,000,000,061 และ 1,000,000,000,063 ในปี ค.ศ. 1989 มีผู้ค้นพบจำนวนเฉพาะคู่หนึ่งคือ $1706595 \cdot 2^{11235} \pm 1$ โดยที่แต่ละจำนวนประกอบด้วยเลขโดด 3,389 หลัก

จำนวนเฉพาะที่อยู่ในรูป $2^p - 1$ โดยที่ p เป็นจำนวนเฉพาะมีได้ไม่จำกัดจำนวนหรือไม่ ตั้งแต่ก่อนคริสตกาลจนถึง ค.ศ. 2004 จำนวนเฉพาะในรูปดังกล่าวเพิ่งทราบเพียง 40 จำนวนเท่านั้น จำนวนเฉพาะในรูป $2^p - 1$ มีชื่อเรียกว่า จำนวนเฉพาะแมร์เซน (Mersenne prime) ที่กล่าวมานี้เป็นเพียงแง่มุมหนึ่งของจุดสนใจในวิชาทฤษฎีจำนวนเท่านั้น

ตัวอย่างต่อไปเป็นตัวอย่างของปัญหาการบวกซึ่งเกี่ยวข้องกับจำนวนเฉพาะ คือ ข้อคาดเดาของโกลด์บาค (Goldbach's conjectures) ซึ่งคริสเตียน โกลด์บาค (Cristian Goldbach ค.ศ. 1690 – 1764) ได้เสนอในปี ค.ศ. 1742 ว่า จำนวนคู่ทุก ๆ จำนวนที่มากกว่า 4 สามารถเขียนเป็นผลบวกของจำนวนเฉพาะคือ 2 จำนวนได้ และจำนวนคี่ทุกจำนวนที่มากกว่า 7 สามารถเขียนเป็นผลบวกของจำนวนเฉพาะคี่ทุกจำนวนได้ ตัวอย่างเช่น

$$6 = 3 + 3, 8 = 5 + 3, 12 = 7 + 5, 20 = 13 + 7 = 17 + 3$$

ปีพิง (N. Pipping) ได้ตรวจสอบข้อเสนอนี้สำหรับจำนวนเต็มคู่จนถึง 100,000 ต่อมามีการตรวจสอบว่าเป็นจริง สำหรับจำนวนเต็มคู่ทุกจำนวนที่น้อยกว่า 10^{10} แต่การพิสูจน์ว่าข้อเสนอนี้เป็นจริงสำหรับจำนวนเต็มคู่ทุก ๆ

จำนวนที่มากกว่า 4 ยังไม่มีผู้ใดทราบ ในปี ค.ศ. 1922 ฮาร์ดี้ (G. H. Hardy ค.ศ. 1877 – 1947) ได้กล่าวถึงข้อคาดเดาของโกลด์บาคว่า บางทีมันอาจยากจนไม่สามารถหาคำตอบได้ แต่ถ้าข้อคาดเดานี้เป็นจริงแล้วจะกล่าวได้ว่าทุก ๆ จำนวนเต็มคี่ที่มากกว่า 7 สามารถเขียนได้ในรูปผลบวกของจำนวนเฉพาะคี่ 3 จำนวนได้ ต่อมาในปี ค.ศ. 1937 นักคณิตศาสตร์ชาวรัสเซียชื่อ วินogradอฟ (I. M. Vinogradov) ได้พิสูจน์ว่าจะมีจำนวนเต็มบวก K ที่ทำให้ทุก ๆ จำนวนเต็มคี่ N ซึ่ง $N > K$ แล้ว N สามารถเขียนได้ในรูปผลบวกของจำนวนเฉพาะคี่ 3 จำนวนได้ แต่เขาก็ไม่สามารถบอกได้ว่า K ควรจะมีขนาดเท่าใด แต่ในปี ค.ศ. 1956 บอโรซดิน (Borozdkin) พิสูจน์ว่า $K < 3^{15}$ จนมาถึง ค.ศ. 1988 มีการตรวจสอบโดยใช้คอมพิวเตอร์พบว่า $K < 10^{400,000}$

หัวข้อสำคัญที่อยู่ในจุดสนใจอีกเรื่องหนึ่งนอกเหนือจากปัญหาเกี่ยวกับจำนวนเฉพาะหรือปัญหาเกี่ยวกับการบวก ซึ่งเป็นปัญหาที่ยอมรับว่าเป็นปัญหาที่ยากที่สุดปัญหาหนึ่งคือ “*ทฤษฎีบทสุดท้ายของแฟร์มาต์ (Fermat's last theorem)*” ในปี ค.ศ. 1637 แฟร์มาต์ได้เขียนเป็นบทสรุปในบันทึกส่วนตัวของเขาว่า เขาได้ค้นพบบทพิสูจน์ของทฤษฎีบทที่ว่า “สมการ $x^n + y^n = z^n$ ไม่มีคำตอบ x, y, z ที่เป็นจำนวนเต็มบวก สำหรับทุก ๆ ค่าของจำนวนเต็มบวก n ที่ $n \geq 3$ ” แต่เขาไม่ได้แสดงบทพิสูจน์ไว้โดยอ้างว่าเนื้อที่ที่เหลือในบันทึกนั้นไม่พอที่จะเขียนบทพิสูจน์ แต่แฟร์มาต์ได้พิสูจน์เพียงว่าทฤษฎีบทของเขาเป็นจริงกรณี $n = 4$ ในปี ค.ศ. 1770 ออยเลอร์พิสูจน์ว่าทฤษฎีบทนี้เป็นจริงสำหรับ $n = 3$ ซึ่งการพิสูจน์ของเขายังมีส่วนบกพร่องอยู่แต่นักคณิตศาสตร์รุ่นต่อมาได้แก้ไขให้ถูกต้องสมบูรณ์สำหรับ $n = 5$ ดิริชเลต์และเลอจองด์ พิสูจน์ได้ในปี ค.ศ. 1825 กรณี $n = 6$ ใช้ผลจากกรณี $n = 3$ สำหรับกรณี $n = 7$ กาเบรียล เลม (Gabriel Lamé ค.ศ. 1795 – 1870) พิสูจน์ได้ในปี ค.ศ. 1839 ต่อมาในปี ค.ศ. 1857 คุมเมอร์ (E. E. Kummer ค.ศ. 1810 – 1893) นักคณิตศาสตร์ชาวเยอรมัน พิสูจน์ได้ว่าทฤษฎีบทนี้เป็นจริงสำหรับ n ที่น้อยกว่า 100 เป็นเวลากว่า 300 ปีที่แฟร์มาต์ได้เสนอทฤษฎีบทของเขา จนกระทั่งได้มีการตรวจสอบสำหรับ n ที่มีค่ามาก ๆ แต่การพิสูจน์ “ทฤษฎีบท” นี้ว่าเป็นจริงสำหรับทุก ๆ $n \geq 3$ ยังไม่เป็นที่ทราบกัน จนกระทั่งในปี ค.ศ. 1993 เมื่อแอนดรู ไวลส์ (Andrew Wiles ค.ศ. 1953 -) นักคณิตศาสตร์ชาวอังกฤษ ได้ประกาศต่อสาธารณชนว่าเขาสามารถพิสูจน์ทฤษฎีบทสุดท้ายของแฟร์มาต์ได้ โดยการจัดบรรยายอย่างต่อเนื่องในวันที่ 21 – 23 ของเดือนมิถุนายน ค.ศ. 1993 ที่ Newton Institute ในเมืองเคมบริดจ์ ประเทศอังกฤษ ไวลส์ได้ตรวจสอบบทพิสูจน์พร้อมกับคณะทำงานจนกระทั่งเดือนธันวาคมในปีเดียวกัน เขาพบข้อบกพร่องของบทพิสูจน์บางประการ เขาและเทย์เลอร์ (R. Taylor) จึงต้องเติมในส่วนที่บกพร่องให้ชัดเจนและถูกต้อง และที่ผลงานของเขาก็สำเร็จลุล่วงได้ในช่วงเดือนกันยายนปี ค.ศ. 1994 (ณรงค์ ปันนัม, 2545 : 1 – 2)

ถึงตอนนี้อาจมีคำถามว่า เราจะศึกษาวิชานี้ไปเพื่ออะไรและมีประโยชน์ด้านใดบ้าง ก่อนจะตอบคำถามนี้ได้จะต้องศึกษารายละเอียดของวิชานี้เสียก่อน เพราะว่าทฤษฎีจำนวนไม่ใช่เพียงแต่ศึกษาเฉพาะสมบัติและการพิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนนับและจำนวนเต็มเท่านั้น ส่วนหนึ่งของวิชาทฤษฎีจำนวนที่ไม่ค่อยได้ปรากฏในหนังสือก็คือ การแก้ปัญหาคณิต (Puzzles) ต่าง ๆ เกี่ยวกับตัวเลข เช่น Games with digits, Magic square, Number puzzles เป็นต้น ซึ่งปัญหาลักษณะนี้จะสามารถพัฒนาความคิดความสามารถในการแก้ปัญหาย่างสร้างสรรค์ได้เป็นอย่างดี

1.2 ระบบจำนวนเต็ม

ในการศึกษาทฤษฎีจำนวนเบื้องต้นนั้น เราจะมุ่งเน้นการศึกษาสมบัติของจำนวนนับและจำนวนเต็ม ตลอดจนการพิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนนับและจำนวนเต็ม นอกจากนี้เรายังมุ่งเน้นให้ผู้เรียนได้เห็นวิวัฒนาการและความสวยงามของระบบจำนวนดังกล่าว และยังให้ผู้เรียนได้นำความรู้ที่ได้รับจากการศึกษาทฤษฎีจำนวนเพื่อเป็นพื้นฐานในการเรียนคณิตศาสตร์ขั้นสูงต่อไป

เพื่อให้บรรลุถึงวัตถุประสงค์ดังกล่าวข้างต้น เนื้อหาในบทนี้จะประกอบด้วยสมบัติพื้นฐานของจำนวนเต็มบางส่วนที่เพียงพอในการนำไปอ้างอิงเมื่อมีการพิสูจน์ทฤษฎีบท และเพื่อทำให้การพิสูจน์ทฤษฎีบทต่าง ๆ เป็นไปตามวิธีการทางคณิตศาสตร์

ในหัวข้อนี้จะกล่าวถึง ระบบจำนวนเต็ม ซึ่งเป็นระบบที่เราสามารถศึกษาสมบัติได้มากมาย และเอกภพสัมพัทธ์ที่เราจะอ้างถึงคือ เซตของจำนวนเต็ม $\mathbb{Z}$ โดยที่

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

ระบบจำนวนเต็มคือระบบที่ประกอบด้วยเซตของจำนวนเต็ม $\mathbb{Z}$ พร้อมด้วยการดำเนินการ “+” และ “ $\cdot$ ” ที่สอดคล้องกับสัจพจน์ที่แบ่งได้ 3 กลุ่ม ดังนี้

กลุ่มที่ 1 สมบัติทางพีชคณิต (algebraic property)

กลุ่มที่ 2 สมบัติไตรวิภาค (trichotomy law)

กลุ่มที่ 3 หลักการจัดอันดับดี (well ordering principle)

นั่นคือ ระบบจำนวนเต็มเป็นระบบเชิงสัจพจน์ระบบหนึ่งซึ่งประกอบด้วย เซตของจำนวนเต็ม $\mathbb{Z}$ และการดำเนินการ + และ $\cdot$ ที่สอดคล้องสมบัติ P_1 ถึง P_8 ที่จะได้กล่าวต่อไป เราสามารถนำสัจพจน์ P_1 ถึง P_8 ข้อใดหรือหลายข้อใดไปอ้างในการพิสูจน์ข้อเท็จจริงต่าง ๆ ที่เกี่ยวข้องกับระบบจำนวนเต็ม ข้อเท็จจริงที่ได้จากการนำสัจพจน์เหล่านี้ไปอ้าง เราเรียกว่า **ทฤษฎีบท** ทฤษฎีบทบางทฤษฎีบทอาจเป็นผลสืบเนื่องโดยตรงจากสัจพจน์หรืออาจเป็นผลสืบเนื่องมาจากสัจพจน์กับทฤษฎีบทที่ได้ผ่านการพิสูจน์มาแล้วก็ได้ และทฤษฎีบทบางทฤษฎีบทอาจเป็นผลสืบเนื่องมาจากสัจพจน์ ทฤษฎีบทที่ได้ผ่านการพิสูจน์มาแล้วและบทนิยามที่ตั้งขึ้นมาใหม่นั้น จะต้องไม่มีความขัดแย้งกันในระบบ

สมบัติทางพีชคณิต (Algebraic properties)

P_1 : สมบัติการปิด (closure laws)

สำหรับการบวก : ทุก ๆ $a, b \in \mathbb{Z}$ จะมี $c \in \mathbb{Z}$ เพียงตัวเดียวเท่านั้น
ที่ทำให้ $a + b = c$

สำหรับการคูณ : ทุก ๆ $a, b \in \mathbb{Z}$ จะมี $c \in \mathbb{Z}$ เพียงตัวเดียวเท่านั้น
ที่ทำให้ $a \cdot b = c$

P_2 : สมบัติการเปลี่ยนกลุ่ม (associative laws)

สำหรับการบวก : ถ้า $a, b, c \in \mathbb{Z}$ แล้ว $(a + b) + c = a + (b + c)$

สำหรับการคูณ : ถ้า $a, b, c \in \mathbb{Z}$ แล้ว $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

- P_3 : สมบัติการมีเอกลักษณ์ (*existence of identities*)
 สำหรับการบวก : มี $0 \in \mathbb{Z}$ ซึ่ง $0 + a = a + 0 = a$ สำหรับทุก $a \in \mathbb{Z}$
 สำหรับการคูณ : มี $1 \in \mathbb{Z}$ ซึ่ง $1 \cdot a = a \cdot 1 = a$ สำหรับทุก $a \in \mathbb{Z}$
- P_4 : สมบัติการมีอินเวอร์สการบวก (*existence of additive inverse*)
 สำหรับแต่ละ $a \in \mathbb{Z}$ จะมี $-a \in \mathbb{Z}$ ซึ่ง $(-a) + a = a + (-a) = 0$
- P_5 : สมบัติการสลับที่ (*commutative laws*)
 สำหรับการบวก : ถ้า $a, b \in \mathbb{Z}$ แล้ว $a + b = b + a$
 สำหรับการคูณ : ถ้า $a, b \in \mathbb{Z}$ แล้ว $a \cdot b = b \cdot a$
- P_6 : สมบัติการกระจาย (*distributive law*)
 ถ้า $a, b, c \in \mathbb{Z}$ แล้ว

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{และ} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

ข้อตกลง เราจะใช้สัญลักษณ์ $\langle \mathbb{Z}, +, \cdot \rangle$ แทนระบบจำนวนเต็ม และเราจะเขียน ab แทน $a \cdot b$
 และ $a - b$ แทน $a + (-b)$

จากระบบจำนวนเต็มพร้อมด้วยสมบัติ 6 ข้อที่กล่าวข้างต้น เราอาจนำไปพิสูจน์หรือให้เหตุผลต่อความจริงดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 1.2.1 ข้อความต่อไปนี้เป็นจริง

1. ในระบบจำนวนเต็มจะมี 0 เพียงตัวเดียวเท่านั้นที่เป็นสมาชิกเอกลักษณ์ของการบวก
2. ในระบบจำนวนเต็มจะมี 1 เพียงตัวเดียวเท่านั้นที่เป็นสมาชิกเอกลักษณ์ของการคูณ
3. สำหรับจำนวนเต็ม a ใด ๆ $a0 = 0a = 0$
4. ถ้า $a, b, c \in \mathbb{Z}$ และ $a + b = a + c$ แล้ว $b = c$

- บทพิสูจน์**
1. สมมติว่ามี $x \in \mathbb{Z}$ ซึ่ง $a + x = a$ สำหรับจำนวนเต็ม a ใด ๆ
 ดังนั้น $0 = 0 + x = x$ นั่นคือ $0 = x$
 2. สมมติว่ามี $x \in \mathbb{Z}$ ซึ่ง $ax = a$ สำหรับจำนวนเต็ม a ใด ๆ
 ดังนั้น $1 = 1x = x$ นั่นคือ $1 = x$
 3. ให้ $a \in \mathbb{Z}$ จะได้ว่า $a0 = a(0 + 0) = a0 + a0$ ดังนั้น $a0 = 0$
 และในทำนองเดียวกัน จะได้ว่า $0a = (0 + 0)a = 0a + 0a$
 นั่นคือ $0a = 0$
 4. สมมติว่า $a + b = a + c$ และให้ x แทนอินเวอร์สการบวกของ a
 จะได้ว่า $b = 0 + b = (x + a) + b = x + (a + b) = x + (a + c)$
 ดังนั้น $b = (x + a) + c = 0 + c = c$

ทฤษฎีบท 1.2.2 ข้อความต่อไปนี้จริง

1. สำหรับจำนวนเต็ม a ใด ๆ a จะมีสมาชิกอินเวอร์สของการบวกเพียงตัวเดียวเท่านั้น
2. สำหรับจำนวนเต็ม a ใด ๆ อินเวอร์สการบวกของ $-a$ คือ a
3. สำหรับจำนวนเต็ม a, b ใด ๆ จะได้ $(-a)b = a(-b) = -(ab)$
และ $(-a)(-b) = ab$

บทพิสูจน์ 1. สมมติว่ามี $b \in \mathbb{Z}$ ซึ่ง $a + b = b + a = 0$ สำหรับจำนวนเต็ม a ใด ๆ

$$\begin{aligned} \text{ดังนั้น } b &= b + 0 = b + [a + (-a)] \\ &= (b + a) + (-a) = 0 + (-a) = -a \end{aligned}$$

นั่นคือ $b = -a$

2. ให้ $a \in \mathbb{Z}$ จะได้ว่า $(-a) + [-(-a)] = (-a) + a = 0$

$$\text{ดังนั้น } -(-a) = a$$

นั่นคือ อินเวอร์สการบวกของ $-a$ คือ a

3. ให้ $a, b \in \mathbb{Z}$ จะได้ว่า

$$\begin{aligned} ab + (-a)b &= [a + (-a)]b = 0b \\ &= a0 = a[b + (-b)] = ab + a(-b) \end{aligned}$$

$$\text{นั่นคือ } (-a)b = a(-b)$$

พิสูจน์ในทำนองเดียวกันจะได้ว่า $(-a)b = -(ab)$

$$\text{ต่อไปพิจารณา } (-a)(-b) + [-(-a)(-b)] = 0(-b) = ab + (-a)b$$

$$\text{เนื่องจาก } -(-a)(-b) = (-a)b$$

$$\text{ดังนั้น } (-a)(-b) = ab$$

สมบัติไตรวิภาค (Trichotomy law)

P_7 : สมบัติไตรวิภาค

มีสับเซต N ของ $\mathbb{Z}$ คือ $N = \{1, 2, 3, \dots\}$ ที่มีสมบัติว่า

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

สมบัติไตรวิภาคนี้มีประโยชน์ในการกำหนดนิยามเพื่อเปรียบเทียบสมาชิก 2 ตัวใด ๆ ใน $\mathbb{Z}$ ในแง่ “มากกว่า” หรือ “น้อยกว่า” กล่าวคือ

บทนิยาม 1.2.3 ให้ $a, b \in \mathbb{Z}$ เรากล่าวว่า

a มากกว่า b เขียนแทนด้วย $a > b$ ก็ต่อเมื่อ $a - b \in N$ และ

a น้อยกว่า b เขียนแทนด้วย $a < b$ ก็ต่อเมื่อ $b > a$

ทฤษฎีบท 1.2.4 ให้ $a, b, c, x, y \in \mathbb{Z}$ จะได้ว่า

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

บทพิสูจน์ 1. เพราะว่า $(a + c) - (b + c) = a - b \in \mathbb{N}$ ดังนั้น $a + c > b + c$
 สำหรับการพิสูจน์ในข้ออื่น ๆ สามารถกระทำได้โดยการใช้สมบัติไตรวิภาคของระบบจำนวนเต็ม
 จึงขอละไว้เพื่อเป็นแบบฝึกหัด ■

ทฤษฎีบท 1.2.5 ให้ $a, b, c, x, y \in \mathbb{Z}$ จะได้ว่า

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

บทพิสูจน์ ขอให้ผู้เรียนพิสูจน์เป็นแบบฝึกหัด ■

ทฤษฎีบทต่อไปจะแสดงว่าระบบจำนวนเต็มจะมีเซตที่สอดคล้องกับสัจพจน์ P_7 เพียงเซตเดียวเท่านั้น คือ $\mathbb{N} = \{1, 2, 3, \dots\}$ นั่นคือ จากบทนิยามการเปรียบเทียบสมาชิกใน $\mathbb{Z}$ ในแง่ “มากกว่า” หรือ “น้อยกว่า” ซึ่งเราสามารถเปรียบเทียบได้เพียงแบบเดียวเท่านั้น

ทฤษฎีบท 1.2.6 $\mathbb{Z}$ มีเพียงสับเซตเดียวเท่านั้นคือ $\mathbb{N}$ ที่สอดคล้องกับสมบัติไตรวิภาค

บทพิสูจน์ สมมติว่า $S \subseteq \mathbb{Z}$ ที่สอดคล้องกับสมบัติไตรวิภาค จะได้ว่า $1 \in S$ หรือ $-1 \in S$

ถ้า $-1 \in S$ จะได้ว่า $(-1)(-1) = 1 \in S$ และ $1 + (-1) = 0 \in S$ ซึ่งเป็นไปไม่ได้ขัดแย้งกับ $0 \notin S$ ดังนั้น $1 \in S$

ให้ $n \in \mathbb{N}$ จะได้ว่า $n = 1 + 1 + 1 + \dots + 1$ (n ตัว)

ดังนั้น $n \in S$ แสดงว่า $\mathbb{N} \subseteq S$ นั่นคือ $S = \mathbb{N}$ หรือ $S \setminus \mathbb{N} \neq \emptyset$

สมมติว่า $S \setminus \mathbb{N} \neq \emptyset$ จะได้ว่ามี $x \in S$ แต่ $x \notin \mathbb{N}$

ดังนั้น $x \neq 0$ นั่นคือ $-x \in \mathbb{N}$ จาก $x \in S$ และ $-x \in \mathbb{N} \subseteq S$

แสดงว่า $x + (-x) = 0 \in S$ ซึ่งเป็นไปไม่ได้จึงเกิดข้อขัดแย้ง ดังนั้น $S = \mathbb{N}$ ■

ทฤษฎีบท 1.2.7 ให้ $a, b \in \mathbb{Z}$

ถ้า $ab = 0$ แล้ว $a = 0$ หรือ $b = 0$

บทพิสูจน์ ถ้า $a \neq 0$ และ $b \neq 0$ จากสมบัติไตรวิภาคจะได้ว่า $a \in \mathbb{N}$ หรือ $-a \in \mathbb{N}$
และ $b \in \mathbb{N}$ หรือ $-b \in \mathbb{N}$ ดังนั้น $ab \in \mathbb{N}$ หรือ $-(ab) \in \mathbb{N}$
นั่นคือ $ab \neq 0$ ■

บทแทรก 1.2.8 ให้ $a, b, c \in \mathbb{Z}$

ถ้า $ab = ac$ และ $a \neq 0$ แล้ว $b = c$

บทพิสูจน์ สมมติว่า $ab = ac$ และ $a \neq 0$ จะได้ว่า $ab - ac = a(b - c) = 0$
ดังนั้น $b - c = 0$ นั่นคือ $b = c$ ■

จากทฤษฎีบท 1.2.7 และบทแทรก 1.2.8 ข้างต้น เราพบว่า สมบัติการตัดออกสำหรับการคูณ หรือ สมบัติการไม่มีตัวหารศูนย์แท้ (no proper zero divisor) ในระบบจำนวนเต็ม เป็นผลสืบเนื่องมาจากสัจพจน์ P_1 ถึง P_6

หลักการจัดอันดับดี

เพื่อให้การศึกษาสมบัติของจำนวนเต็มมีประสิทธิภาพมากขึ้นและเพื่อการพิสูจน์ข้อความต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มมีความสมเหตุสมผลมากขึ้น เราจึงขอกำหนดว่าเซตของจำนวนเต็มบวกมีสมบัติหลักการจัดอันดับดี กล่าวคือ

หลักการจัดอันดับดี (Well ordering principle)

P_8 : ให้ $S \subseteq \mathbb{N}$ และ $S \neq \emptyset$ จะได้ว่า

มี $x \in S$ ซึ่ง $x \leq a$ สำหรับทุก $a \in S$

สมบัติของการจัดอันดับดีในระบบจำนวนเต็ม นำไปสู่ทฤษฎีบทที่น่าสนใจ ซึ่งสามารถนำไปประยุกต์ใช้ในการพิสูจน์ทฤษฎีบทต่าง ๆ ที่จะได้กล่าวถึงในบทต่อ ๆ ไป

ทฤษฎีบท 1.2.9 ไม่มีจำนวนเต็มใดอยู่ระหว่าง 0 และ 1

บทพิสูจน์ ให้ $T = \{a \in \mathbb{Z} \mid 0 < a < 1\}$ และสมมติว่า $T \neq \emptyset$

จากหลักการจัดอันดับดี จะได้ว่ามี $m \in T$ ซึ่ง $m \leq x$ สำหรับทุก $x \in T$

ดังนั้น $0 < m < 1$ นั่นคือ $0 < m^2 < m$ แสดงว่า $m^2 \in T$

จึงเกิดข้อขัดแย้งในการเลือก m ที่เป็นจำนวนเต็มบวกที่น้อยที่สุดใน T

นั่นคือ $T = \emptyset$ ■

ทฤษฎีบท 1.2.10 สมบัติของอาร์คิมิดีส (Archimedean property)

สำหรับจำนวนเต็มบวก a และ b จะมีจำนวนเต็มบวก n ซึ่ง $na \geq b$

บทพิสูจน์ สมมติว่าข้อความในทฤษฎีบทไม่จริง

นั่นคือ มีจำนวนเต็มบวก a, b และทุก n จำนวนเต็มบวก n , $na < b$

ให้ $S = \{b - na \mid n \in \mathbb{N}\}$ จากสมมติฐานจะเห็นว่า $S \subseteq \mathbb{N}$ และ $S \neq \emptyset$

จากหลักการจับอันดับดี จะมี $k \in \mathbb{N}$ ซึ่ง $m = b - ka$ ที่ m เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S

จาก $b - (k+1)a \in S$ และ $[b - (k+1)a] - [b - ka] = -a < 0$

ดังนั้น $b - (k+1)a < b - ka$

จึงเกิดข้อขัดแย้งในการเลือก $m = b - ka$ ที่เป็นสมาชิกที่น้อยที่สุดใน S ■

หลักการจับลำดับดียังนำไปสู่ทฤษฎีบทที่สำคัญที่ใช้เพื่อพิสูจน์ข้อความต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มบวก เรียกทฤษฎีบทนี้ว่า “หลักอุปนัยเชิงคณิตศาสตร์” (Principle of Mathematical Induction)

ทฤษฎีบท 1.2.11 ให้ $S \subseteq \mathbb{N}$ จะได้ว่า $\mathbb{N} = S$ ก็ต่อเมื่อ

(1) $1 \in S$ และ

(2) ถ้า $n \in S$ แล้ว $n+1 \in S$

บทพิสูจน์ ให้ $S = \mathbb{N}$ เห็นได้ชัดว่า (1) และ (2) เป็นจริง

สมมติว่า (1) และ (2) เป็นจริง และ $\mathbb{N} \setminus S \neq \emptyset$ โดยหลักการจับอันดับดี จะมี $m \in \mathbb{N} \setminus S$ ซึ่ง

m เป็นจำนวนเต็มบวกที่น้อยที่สุดใน $\mathbb{N} \setminus S$ เพราะว่า $m-1 < m$

ดังนั้น $m-1 \notin \mathbb{N} \setminus S$

จาก $1 \in S$ แสดงว่า $m > 1$ ดังนั้น $m-1 \in \mathbb{N}$

จากการเลือก m เราพบว่า $m-1 \in S$ และจาก (2) จะได้ว่า

$m = (m-1) + 1 \in S$ ซึ่งเป็นไปไม่ได้เกิดข้อขัดแย้งที่ว่า $m \notin S$

ดังนั้น $\mathbb{N} = S$ ■

1.3 หลักอุปนัยเชิงคณิตศาสตร์

ในการพิสูจน์หรือการให้เหตุผลทางทฤษฎีจำนวนนั้น หลักการพื้นฐานที่สำคัญมีอยู่ 2 ประการ คือ

1. ทุกสับเซตของ $\mathbb{N}$ จะมีสมาชิกตัวน้อยที่สุด ซึ่งหลักการนี้ได้กล่าวไว้แล้วในหลักการจับอันดับดีข้างต้น
2. หลักอุปนัยเชิงคณิตศาสตร์ เป็นหลักการที่ใช้สำหรับพิสูจน์ประพจน์ต่าง ๆ ที่เป็นจริงสำหรับทุก ๆ ค่าของ n ที่เป็นจำนวนเต็มบวกซึ่งมีรายละเอียดดังนี้

ทฤษฎีบท 1.3.1 หลักอุปนัยเชิงคณิตศาสตร์ที่ 1 (*1st Principle of Mathematical Induction*)

ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก n ถ้า

(1) $P(1)$ เป็นจริง

และ (2) ถ้า $P(k)$ เป็นจริงแล้ว $P(k+1)$ เป็นจริง
สำหรับจำนวนเต็มบวก k ใด ๆ

จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

บทพิสูจน์ ให้ $P(n)$ แทนข้อความที่สอดคล้องกับเงื่อนไข (1) และ (2)

ให้ $S = \{n \in \mathbb{N} \mid P(n) \text{ เป็นจริง}\}$

จาก (1) จะได้ว่า $1 \in S$ และจาก (2) จะได้ว่า ถ้า $k \in S$ แล้ว $k+1 \in S$

ดังนั้นโดยทฤษฎีบท 1.2.11 จะได้ว่า S เป็นเซตของจำนวนเต็มบวก

นั่นคือ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ■

ตัวอย่าง 1 จงพิสูจน์ว่า $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

บทพิสูจน์ ให้ $P(n)$ แทน $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$

เราจะต้องพิสูจน์ว่า $P(n)$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

(1) $P(1)$ เป็นจริง เพราะว่า $1 = \frac{1(1+1)}{2}$

(2) ถ้ายอมรับ $P(k)$ เป็นจริง แล้วจะต้องแสดงว่า $P(k+1)$ เป็นจริง

สมมติว่า $P(k)$ เป็นจริง นั่นคือ $1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$

ดังนั้น จากสมบัติการเท่ากันของการบวก นำ $k+1$ บวกเข้าทั้งสองข้าง

$$\begin{aligned} \text{จะได้ว่า } 1 + 2 + 3 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)[(k+1)+1]}{2} \end{aligned}$$

นั่นคือ $P(k+1)$ เป็นจริง

ดังนั้น $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ สำหรับทุก $n \in \mathbb{N}$ □

ตัวอย่าง 2 พิจารณา

$$\begin{aligned} 1 + 3 &= 4 = 2^2 \\ 1 + 3 + 5 &= 9 = 3^2 \\ 1 + 3 + 5 + 7 &= 16 = 4^2 \\ 1 + 3 + 5 + 7 + 9 &= 25 = 5^2 \\ &\vdots \end{aligned}$$

จงพิสูจน์ว่า $1 + 3 + 5 + \cdots + (2n-1) = n^2$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

บทพิสูจน์ ให้ $P(n)$ แทนข้อความ $1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2$

เราจะต้องพิสูจน์ว่า $P(n)$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

(1) $P(1)$ เป็นจริง เพราะว่า $1 = 1^2$

(2) ถ้ายอมรับ $P(k)$ เป็นจริงแล้วจะต้องแสดงว่า $P(k + 1)$ เป็นจริง

สมมติว่า $P(k)$ เป็นจริง นั่นคือ $1 + 3 + 5 + \cdots + (2k - 1) = k^2$

ดังนั้นจากสมบัติการเท่ากันของการบวก นำ $2k + 1$ บวกเข้าทั้งสองข้าง
จะได้ว่า

$$\begin{aligned} 1 + 3 + 5 + 7 + \cdots + (2k - 1) + (2k + 1) &= k^2 + (2k + 1) \\ &= (k + 1)^2 \end{aligned}$$

นั่นคือ $P(k + 1)$ เป็นจริง

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

การพิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ อาจนำไปใช้พิสูจน์ข้อความที่เกี่ยวกับจำนวนเต็ม n ใด ๆ ที่ $n \geq a$ เมื่อ $a \in \mathbb{Z}$ ซึ่งมีรายละเอียดดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 1.3.2 ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็ม n และ $a \in \mathbb{Z}$

(1) $P(a)$ เป็นจริง

และ (2) สำหรับจำนวนเต็ม k ซึ่ง $k \geq a$

ถ้า $P(k)$ เป็นจริง แล้ว $P(k + 1)$ เป็นจริง

จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็ม n ที่ $n \geq a$

บทพิสูจน์ เนื่องจาก $n \geq a$ ดังนั้น $n = a, a + 1, a + 2, a + 3, \dots$

ถ้าให้ $m = n - a + 1$ จะได้ $m = 1, 2, 3, 4, \dots$

และจะได้ $P(n)$ คือประโยคเดียวกับ $P(m + a - 1)$

ในการพิสูจน์ว่าข้อความ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็ม n ที่ $n \geq a$

เป็นการเพียงพอที่เราจะพิสูจน์ว่าข้อความ $P(m + a - 1)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก m

ให้ $Q(m)$ แทน $P(m + a - 1)$

จะได้ว่า $Q(1)$ แทน $P(1 + a - 1)$ ซึ่งก็คือ $P(a)$

$Q(k)$ แทน $P(k + a - 1)$

และ $Q(k + 1)$ แทน $P(k + 1 + a - 1)$

(1) $Q(1)$ เป็นจริงเพราะ $P(a)$ เป็นจริงตามที่กำหนดให้ข้อ (1)

(2) ถ้า $Q(k)$ เป็นจริงจะได้ $P(k + a - 1)$ เป็นจริงโดยที่ $k \geq 1$

จะได้ $k + a - 1 \geq a$ เมื่อ $P(k + a - 1)$ เป็นจริง

จากที่กำหนดให้ ข้อ (2) จะได้ $P(k + 1 + a - 1)$ เป็นจริง

นั่นคือ $Q(k + 1)$ เป็นจริง

จาก (1) และ (2) สรุปว่า $Q(m)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก m
 ดังนั้น $P(m + a - 1)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก m ที่ $m \geq 1$
 แต่ $n = m + a - 1$ เมื่อ $m \geq 1$ จะได้ว่า $n \geq a$
 จึงได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็ม n ที่ $n \geq a$ ■

ตัวอย่าง 3 จงพิสูจน์ว่า $3^n > n^3$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 4$

บทพิสูจน์ ให้ $P(n)$ แทนข้อความ $3^n > n^3$

- (1) $P(4)$ เป็นจริง เพราะว่า $3^4 > 4^3$
 (2) ถ้ายอมรับ $P(k)$ เป็นจริงเมื่อ $k \geq 4$ แล้วจะต้องแสดงว่า $P(k + 1)$ เป็นจริง
 สมมติว่า $P(k)$ เป็นจริง นั่นคือ $3^k > k^3$ เป็นจริง
 จากสมบัติของจำนวนเต็ม นำ 3 คูณทั้งสองข้าง จะได้ว่า

$$3^{k+1} > k^3 + k^3 + k^3 > k^3 + 3k^2 + 3k + 1$$

 ดังนั้น $3^{k+1} > (k + 1)^3$
 นั่นคือ $P(k + 1)$ เป็นจริง
 ดังนั้น $3^n > n^3$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 4$ □

ปัญหา 4 ให้ $n! = n(n - 1)(n - 2) \cdots (3)(2)(1)$

จงพิสูจน์ว่า $n! > 2^n$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 4$

ทฤษฎีบท 1.3.3 หลักอุปนัยเชิงคณิตศาสตร์ที่ 2 (*2nd Principle of Mathematical Induction*)

ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก n ถ้า

- (1) $P(1)$ เป็นจริง
 และ (2) ถ้า $P(k)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก k ที่
 $k < m$ แล้ว $P(m)$ เป็นจริง
 จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

บทพิสูจน์ ให้ $S = \{n \in \mathbb{N} \mid P(n) \text{ เป็นเท็จ}\}$

สมมติว่า $S \neq \emptyset$ โดยหลักการจัดอันดับดี จะมี $m \in S$ ซึ่ง m เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S
 ดังนั้น $P(m)$ เป็นเท็จ
 เนื่องจาก $P(1)$ เป็นจริง ดังนั้น $m > 1$
 แสดงว่า $P(k)$ เป็นจริงสำหรับทุกจำนวนจริงบวก k ที่ $k < m$
 โดยสมมติฐานข้อ (2) จะได้ว่า $P(m)$ เป็นจริงซึ่งผลที่ได้ ขัดแย้งกับ $m \in S$
 ดังนั้นที่สมมติว่า $S \neq \emptyset$ เป็นเท็จ แสดงว่า $S = \emptyset$
 นั่นคือ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ■

- หมายเหตุ (1) โดยทั่วไปนิยมเรียกการพิสูจน์หลักอุปนัยเชิงคณิตศาสตร์ที่ 2 นี้ว่าหลักอุปนัยอย่างเข้ม (Strong Induction)
- (2) เราสามารถแสดงได้ว่าการพิสูจน์โดยใช้ทฤษฎีบท 1.3.3 อาจนำไปใช้พิสูจน์ข้อความที่เกี่ยวกับจำนวนเต็ม n ใด ๆ ที่ $n \geq a$ เมื่อ $a \in \mathbb{Z}$ ซึ่งมีรายละเอียดดังนี้

หลักอุปนัยอย่างเข้ม (Strong Induction)

ให้ $P(n)$ เป็นข้อความที่เกี่ยวข้องกับจำนวนเต็ม n และ $a \in \mathbb{Z}$ ซึ่ง

- (1) $P(a)$ เป็นจริง
- (2) ถ้า $P(a), P(a+1), P(a+2), \dots, P(m-1)$ เป็นจริง แล้ว $P(m)$ เป็นจริง

จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็ม n ที่ $n \geq a$

ตัวอย่าง 4 พิจารณาลำดับ 1, 3, 4, 7, 11, 18, 29, 47, 76, ...

ลำดับนี้เรียกว่า ลำดับลูคัส (Lucas sequence)

โดยที่ $a_1 = 1, a_2 = 3$ และ

$$a_n = a_{n-1} + a_{n-2} \quad \text{สำหรับทุกจำนวนเต็มบวก } n \text{ ที่ } n \geq 3$$

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

บทพิสูจน์ ให้ $P(n)$ แทน $a_n < \left(\frac{7}{4}\right)^n$

(1) $n = 1$ จะได้ $a_1 = 1 < \left(\frac{7}{4}\right)^1$ ดังนั้น $P(1)$ เป็นจริง

$n = 2$ จะได้ $a_2 = 3 < \left(\frac{7}{4}\right)^2$ ดังนั้น $P(2)$ เป็นจริง

(2) สมมติว่า $P(k)$ เป็นจริงสำหรับทุก $k < m$ เมื่อ $m \geq 3$

ดังนั้น $a_{m-1} < \left(\frac{7}{4}\right)^{m-1}$ และ $a_{m-2} < \left(\frac{7}{4}\right)^{m-2}$

แต่ $a_m = a_{m-1} + a_{m-2} < \left(\frac{7}{4}\right)^{m-1} + \left(\frac{7}{4}\right)^{m-2} = \left(\frac{7}{4}\right)^{m-2} \left(\frac{7}{4} + 1\right)$

ดังนั้น $a_m < \left(\frac{7}{4}\right)^{m-2} \left(\frac{11}{4}\right) < \left(\frac{7}{4}\right)^{m-2} \left(\frac{7}{4}\right)^2 < \left(\frac{7}{4}\right)^m$ เป็นจริง

นั่นคือ $P(m)$ เป็นจริง

โดยหลักอุปนัยเชิงคณิตศาสตร์ที่ 2 สรุปได้ว่า

$$a_n < \left(\frac{7}{4}\right)^n \quad \text{เป็นจริงสำหรับทุกจำนวนเต็มบวก } n$$

□

ตัวอย่าง 5 จงพิสูจน์ว่า ทุก ๆ จำนวนเต็มบวก n จะมี t และ m เพียงคู่เดียวเท่านั้นที่ทำให้

$$n = 2^t \cdot m$$

โดยที่ $t \in \{0, 1, 2, \dots\}$ และ m เป็นจำนวนเต็มคี่

บทพิสูจน์ เพราะว่า $1 = 2^0 \cdot 1$ จะได้ว่า มี 0 และ 1 เพียงคู่เดียวที่ทำให้ $1 = 2^0 \cdot 1$
 สมมติว่า $n > 1$ จะได้ว่า n เป็นจำนวนเต็มคี่หรือ n เป็นจำนวนเต็มคู่
 ถ้า n เป็นจำนวนเต็มคี่ จะได้ว่า $n = 2^0 \cdot n$ และมี $t = 0$ และ $m = n$
 เพียงคู่เดียวที่ทำให้ $n = 2^t \cdot m$
 ถ้า n เป็นจำนวนเต็มคู่ แล้วจะมีจำนวนเต็มบวก $m < n$ ซึ่ง $n = 2m$
 สมมติว่ามี r และ k เพียงคู่เดียวเท่านั้นที่ทำให้ $m = 2^r \cdot k$
 โดยที่ $r \in \{0, 1, 2, \dots\}$ และ k เป็นจำนวนเต็มคี่
 ดังนั้น $n = 2m = 2 \cdot 2^r \cdot k = 2^{r+1} \cdot k$
 เนื่องจาก n เป็นจำนวนเต็มคู่ และถ้า $n = 2^{t+1} \cdot h = 2^{r+1} \cdot k$
 โดยที่ h และ k เป็นจำนวนเต็มคี่
 จะได้ว่า $2^t \cdot h = 2^r \cdot k$ โดยสมมติฐานแสดงว่า $t = r$ และ $h = k$
 นี้แสดงว่า n สามารถเขียนในรูป $2^{r+1} \cdot k$ ได้เพียงแบบเดียว
 เพราะฉะนั้นโดยหลักอุปนัยเชิงคณิตศาสตร์ที่ 2 สรุปว่า
 ทุกจำนวนเต็มบวก n จะมี $t \in \{0, 1, 2, \dots\}$ และ m เป็นจำนวนเต็มคี่
 เพียงคู่เดียวเท่านั้นที่ทำให้ $n = 2^t \cdot m$ □

ปัญหา 5 จงหาจำนวนเต็มบวก n ทั้งหมดที่ n สามารถเขียนได้ในรูปผลบวกของจำนวนเต็มบวกที่เรียงต่อเนื่องกันอย่างน้อย 2 จำนวน

1.4 ข้อแนะนำบางประการเกี่ยวกับจำนวนเต็ม

(1) ให้ a และ d เป็นจำนวนเต็มใด ๆ เราเรียกลำดับจำนวนเต็ม $a, a + d, a + 2d, a + 3d, \dots, a + (n - 1)d, \dots$ นี้ว่า **ลำดับเลขคณิต** (Arithmetic sequence) และเรียก a ว่า **พจน์แรก** (initial term) เรียก d ว่า **ผลต่างร่วม** (common difference)

เช่น ลำดับ 3, 7, 9, 11, 13, ... เป็นลำดับเลขคณิต ที่ $a = 3$ และ $d = 2$

(2) ให้ a และ r เป็นจำนวนเต็มใด ๆ เราเรียกลำดับจำนวน $a, ar, ar^2, ar^3, \dots, ar^{n-1}, \dots$ นี้ว่า **ลำดับเรขาคณิต** (Geometric sequence) และเรียก a ว่า **พจน์แรก** (initial term) เรียก r ว่า **อัตราส่วนร่วม** (common ratio)

เช่น ลำดับ 5, -15, 45, -135, ... เป็นลำดับเรขาคณิตที่ $a = 5$ และ $r = -3$

(3) ผลบวก n พจน์แรกของลำดับเลขคณิต

$$a + (a + d) + (a + 2d) + \cdots + (a + (n-1)d) = \frac{n}{2} [2a + (n-1)d]$$

และผลบวก n พจน์แรกของลำดับเรขาคณิต

$$a + ar + ar^2 + ar^3 + \cdots + ar^{n-1} = \frac{a(r^n - 1)}{r - 1}$$

เช่น $2 + 4 + 6 + 8 + 10 + \cdots + 400 = \frac{200}{2} [2(2) + (200 - 1)] = 40,200$

$$3 + 3 \cdot 2 + 3 \cdot 2^2 + 3 \cdot 2^3 + \cdots + 3 \cdot 2^{25} = \frac{3(2^{26} - 1)}{2 - 1} = 3(2^{26} - 1)$$

(4) **สัญลักษณ์แทนการบวก** (Summation notation) คือสัญลักษณ์ “ $\sum$ ” อ่านว่า ซิกมา (Sigma) ซึ่งมีความหมายดังนี้

$$\sum_{k=1}^n a_k = a_1 + a_2 + a_3 + \cdots + a_n$$

เช่น $\sum_{k=1}^6 (2k + 1) = (2 \cdot 1 + 1) + (2 \cdot 2 + 1) + (2 \cdot 3 + 1) + (2 \cdot 4 + 1) + (2 \cdot 5 + 1) + (2 \cdot 6 + 1)$

และ $\sum_{k=1}^n a_k = \sum_{j=1}^n a_j = \sum_{i=1}^n a_i$

เช่น $\sum_{j=1}^5 j = 1 + 2 + 3 + 4 + 5 = 15$

$$\sum_{j=1}^5 2 = 2 + 2 + 2 + 2 + 2 = 10$$

$$\sum_{k=1}^5 2^k = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = 62$$

หมายเหตุ การใช้สัญลักษณ์ “ $\sum$ ” นี้ เราอาจไม่เริ่มที่ 1 ก็ได้

เช่น $\sum_{k=m}^n a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n, \quad m \leq n$

$$\sum_{k=3}^5 k^2 = 3^2 + 4^2 + 5^2 = 50$$

$$\sum_{k=0}^2 3^k = 3^0 + 3^1 + 3^2 = 13$$

$$\sum_{k=-2}^1 k^3 = (-2)^3 + (-1)^3 + (0)^3 + (1)^3 = -8$$

(5) **สัญลักษณ์แทนการคูณ** (Product notation) คือสัญลักษณ์ “ $\prod$ ” อ่านว่า พาย (Pi) ซึ่งมีความหมายดังนี้

$$\prod_{j=1}^n a_j = a_1 \cdot a_2 \cdot a_3 \cdots a_n$$

เช่น $\prod_{j=1}^5 j = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$

$$\prod_{j=1}^5 2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32$$

$$\prod_{k=1}^n k = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-2)(n-1)(n) = n!$$

$$n! = n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1 \quad \text{เมื่อ } n \geq 1$$

Then $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$

สำหรับจำนวนเต็มบวก n และจำนวนเต็ม k ซึ่ง $0 \leq k \leq n$ นิยาม

$$\begin{aligned} \binom{n}{k} &= \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(k-1)}{(n-k)!} \\ &= \frac{n(n-1)\cdots(n-k+1)}{k!} \end{aligned}$$

$$\text{Ex } \binom{8}{3} = \frac{8!}{3! 5!} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{5!} = \frac{8 \cdot 7 \cdot 6}{3!} = 56$$
$$\binom{n}{0} = \binom{n}{n} = 1 \quad \text{และ} \quad \binom{n}{k} = \binom{n}{n-k}$$

เช่น $\binom{10}{0} = \binom{10}{10} = 1$ และ $\binom{10}{4} = \binom{10}{6}$

ในการหาสัมประสิทธิ์ของการกระจายผลบวกของเลขยกกำลังนั้น เราอาจใช้รูปแบบการเขียนสามเหลี่ยมปาสคาล (Pascal's triangle) ในการหาสัมประสิทธิ์ตัวที่ $k + 1$ ซึ่งเท่ากับ $\binom{n}{k}$ ได้ ซึ่งมีรายละเอียดต่อไปนี้

$$\begin{array}{ccccccc}
& & & 1 & & & \\
& & & & 1 & & 1 \\
& & & & & 1 & & 1 \\
& & & 1 & & 2 & & 1 \\
& & & & 1 & & 3 & & 1 \\
& & 1 & & 3 & & 3 & & 1 \\
& & & 1 & & 4 & & 6 & & 4 & & 1 \\
& 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
& & & & & \vdots & & & & & & &
\end{array}$$

จากสามเหลี่ยมปาสคาล เราจะได้

$$(a + b)^0 = 1 \quad (\text{ดูแถวที่ 1})$$

$$(a + b)^1 = a + b \quad (\text{ดูแถวที่ 2})$$

$$(a + b)^2 = a^2 + 2ab + b^2 \quad (\text{ดูแถวที่ 3})$$

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \quad (\text{ดูแถวที่ 4})$$

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \quad (\text{ดูแถวที่ 5})$$

ในทำนองเดียวกัน ถ้าต้องการกระจายผลบวกของยกกำลัง n ก็ดูแถวที่ $n + 1$ หรือเราอาจใช้

$$(a + b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

หรือเขียน

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

เช่น $(x + 1)^6 = \binom{6}{0}x^6 + \binom{6}{1}x^5 + \binom{6}{2}x^4 + \binom{6}{3}x^3 + \binom{6}{4}x^2 + \binom{6}{5}x + \binom{6}{6}$

$$(x + 2)^5 = \binom{5}{0}x^5 + \binom{5}{1}x^4 \cdot 2 + \binom{5}{2}x^3 \cdot 2^2 + \binom{5}{3}x^2 \cdot 2^3 + \binom{5}{4}x \cdot 2^4 + \binom{5}{5}2^5$$

$$2^n = (1 + 1)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n}$$

ข้อเสนอแนะเพิ่มเติม

ให้ $a \in \mathbb{Z}$ ค่าสัมบูรณ์ (Absolute value) ของ a เขียนแทนด้วย $|a|$ ซึ่งนิยามดังนี้

$$|a| = \begin{cases} 0 & \text{ถ้า } a = 0 \\ a & \text{ถ้า } a \in \mathbb{N} \\ -a & \text{ถ้า } -a \in \mathbb{N} \end{cases}$$

จากบทนิยามเราพบว่า

1. $|a| \geq 0$
2. $|a| = 0$ ก็ต่อเมื่อ $a = 0$
3. $-|a| \leq a \leq |a|$
4. $|a| \leq b$ ก็ต่อเมื่อ $-b \leq a \leq b$
 $|a| \geq b$ ก็ต่อเมื่อ $a \geq b$ หรือ $a \leq -b$
5. $|ab| = |a||b|$
6. $|a + b| \leq |a| + |b|$
7. $|a| - |b| \leq |a - b|$
8. $-(|a| + |b|) \leq a + b \leq |a| + |b|$
9. $||a| - |b|| \leq |a - b|$
10. $|a| = |b|$ ก็ต่อเมื่อ $a = b$ หรือ $a = -b$

โจทย์ปัญหาเสริมเรื่อง ความรู้เบื้องต้น

ปัญหา 1 จงหาเลขโดด 3 หลักสุดท้ายของ 7^{9999}

วิธีทำ เพราะว่า $7^4 = 2401$

$$\begin{aligned} \text{จะได้ว่า } 7^{4n} &= (2401)^n = (1 + 2400)^n \\ &= 1 + n \cdot 2400 + \binom{n}{2} 2400^2 + \dots \end{aligned}$$

ในการหาเลขโดด 3 หลักสุดท้าย เราจะพิจารณาเฉพาะ $1 + n \cdot 2400$ เท่านั้น
ดังนั้นเลขโดด 3 หลักสุดท้าย เราจะพิจารณาโดย

$$1 + n \cdot 2400 = 24n \cdot 100 + 1$$

ถ้า m เป็นเลขโดดตัวสุดท้ายของ $24n$ เราพบว่า

$$24n \cdot 100 + 1 = (\dots m)100 + 1 = \dots m01$$

ดังนั้น เลขโดด 3 หลักสุดท้ายคือ $m01$

ถ้าให้ $n = 2499$ จะได้ว่า $24n$ มีเลขโดดหลักสุดท้าย คือ 6 และเราพบว่า

$$7^{4n} = 7^{9996} \text{ มีเลขโดด 3 หลักสุดท้ายคือ } 601$$

เนื่องจาก $7^3 = 343$ เราจะได้ว่า

$$7^{9999} = 7^{9996} \cdot 7^3 = (\dots 601)(343) = \dots 143$$

ดังนั้น เราสรุปได้ว่า 7^{9999} มีเลขโดด 3 หลักสุดท้าย คือ 143 □

ปัญหา 2 จำนวนสามเหลี่ยม

จำนวนเต็มบวก n จะเรียกว่า จำนวนสามเหลี่ยม (*triangular numbers*) ก็ต่อเมื่อ

จำนวนเต็มบวก n เขียนอยู่ในรูป $n = 1 + 2 + 3 + \dots + k$

สำหรับจำนวนเต็มบวก k บางจำนวน

$$\text{เช่น } 6 = 1 + 2 + 3, 15 = 1 + 2 + 3 + 4 + 5,$$

$$28 = 1 + 2 + 3 + 4 + 5 + 6 + 7$$

ในการหาจำนวนสามเหลี่ยมนั้น เราสามารถหาได้จากการสร้างเป็นลำดับดังนี้

$$1, 3, 6, 10, 15, 21, 28, 36, 45, \dots$$

ถ้า t_n เป็นจำนวนสามเหลี่ยมตัวที่ n จะได้ว่า

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

$$\text{และ } t_n = t_{n-1} + n$$

เช่น t_{20} เป็นจำนวนสามเหลี่ยมตัวที่ 20 จะได้ว่า

$$t_{20} = 1 + 2 + 3 + \dots + 20 = \frac{20(20+1)}{2} = 210$$

ดังนั้น เราสามารถหาจำนวนสามเหลี่ยมได้เสมอ ฉะนั้น

ให้ 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136, 153, ...

เป็นลำดับของจำนวนสามเหลี่ยม จากความรู้เรื่องจำนวนสามเหลี่ยม

จงแสดงว่าข้อความต่อไปนี้จริง

(2.1) ถ้า E เป็นจำนวนเต็มคี่ แล้ว $E^2 - 1$ หารด้วย 8 เป็นจำนวนสามเหลี่ยมเสมอ

(2.2) จำนวนสามเหลี่ยมที่เป็นกำลังสองสมบูรณ์จะมีจำนวนไม่จำกัด เช่น 1, 36

(2.3) ผลต่างระหว่างกำลังสองของจำนวนสามเหลี่ยมในลำดับของจำนวนสามเหลี่ยมที่อยู่ติดกันเป็นกำลังสามสมบูรณ์เสมอ

(2.4) ผลบวกของส่วนกลับในลำดับของจำนวนสามเหลี่ยมมีค่าเท่ากับ 2

$$\text{นั่นคือ } \frac{1}{1} + \frac{1}{3} + \frac{1}{6} + \frac{1}{10} + \cdots + \frac{2}{n(n+1)} + \cdots = 2$$

วิธีทำ (2.1) ให้ E เป็นจำนวนเต็มคี่ จะได้ว่า $E = 2n + 1$ สำหรับจำนวนเต็มบวก n บางตัว และ

$$E^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 4n(n + 1) + 1$$

$$\text{ดังนั้น } \frac{E^2 - 1}{8} = \frac{[4n(n + 1) + 1] - 1}{8} = \frac{n(n + 1)}{2} = t_n$$

$$t_1 = \frac{3^2 - 1}{8} = \frac{1(1 + 1)}{2} = 1$$

$$t_2 = \frac{5^2 - 1}{8} = \frac{2(2 + 1)}{2} = 3$$

$$t_3 = \frac{7^2 - 1}{8} = \frac{3(3 + 1)}{2} = 6$$

$$t_4 = \frac{9^2 - 1}{8} = \frac{4(4 + 1)}{2} = 10$$

$$\text{ดังนั้น } t_n = \frac{n(n + 1)}{2} = \frac{[4n(n + 1) + 1] - 1}{8} = \frac{E^2 - 1}{8}$$

เป็นจำนวนสามเหลี่ยมเสมอ

(2.2) ให้ $t_n = \frac{n(n + 1)}{2}$ สำหรับทุกจำนวนเต็มบวก n เป็นจำนวนสามเหลี่ยม

แล้วจะมีจำนวนสามเหลี่ยม $t_m = \frac{m(m + 1)}{2} = k^2$ สำหรับจำนวนเต็มบวก k บางตัว

$$\text{เช่น } t_1 = \frac{1(1 + 1)}{2} = 1, t_8 = \frac{8(8 + 1)}{2} = 36$$

ต่อไปเราจะแสดงว่า มี $t_m = k^2$ ไม่จำกัด

$$\text{ถ้า } t_m = \frac{m(m + 1)}{2} = k^2 \text{ แล้ว } 4m(m + 1) = 8k^2$$

$$\begin{aligned} \text{และ } t_{4m(m+1)} &= t_{8k^2} = \frac{8k^2(8k^2 + 1)}{2} = 4k^2(8k^2 + 1) \\ &= 4k^2[4m(m + 1) + 1] \\ &= 4k^2(2m + 1)^2 \end{aligned}$$

$$= [2k(2m+1)]^2$$

ดังนั้น $t_{4m(m+1)} = [2k(2m+1)]^2$ สำหรับทุกจำนวนเต็มบวก m

แสดงว่าจำนวนสามเหลี่ยมที่เป็นกำลังสองสมบูรณ์ไม่มีจำกัดจำนวน เช่น

$$t_8, t_{24}, t_{48}, t_{80}, \dots, t_{4m(m+1)}, \dots$$

$$(2.3) \quad \text{เนื่องจาก} \quad 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2} = t_n$$

$$\text{จะได้ว่า} \quad 1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2 = t_n^2$$

$$\begin{aligned} \text{ดังนั้น} \quad t_{n+1}^2 - t_n^2 &= \left[\frac{(n+1)(n+2)}{2} \right]^2 - \left[\frac{n(n+1)}{2} \right]^2 \\ &= (n+1)^3 \end{aligned}$$

นั่นคือ ผลต่างระหว่างกำลังสองของจำนวนสามเหลี่ยมที่อยู่ติดกันในลำดับของจำนวนสามเหลี่ยมเป็นกำลังสามสมบูรณ์เสมอ เช่น

พิจารณาลำดับของจำนวนสามเหลี่ยม $\{t_n\} : 1, 3, 6, 10, 15, 21, \dots$

จะได้ว่า $\{t_n^2\} : 1, 9, 36, 100, 225, 441, \dots$

ให้ D_n แทนผลต่างระหว่าง t_{n+1}^2 และ t_n^2

จะได้ $\{D_n\} : 8, 27, 64, 125, 216, \dots$

ซึ่ง $D_1 = (1+1)^3, D_2 = (2+1)^3, D_3 = (3+1)^3, \dots$

ฉะนั้น $\forall n \in \mathbb{N}, D_n = (n+1)^3$

$$(2.4) \quad \text{เพราะว่าสำหรับทุกจำนวนเต็มบวก } n, \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1} \quad \text{จะได้ว่า}$$

$$1 + \frac{1}{3} + \frac{1}{6} + \frac{1}{10} + \dots + \frac{2}{n(n+1)} + \dots$$

$$= \sum_{n=1}^{\infty} \frac{2}{n(n+1)}$$

$$= 2 \sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1} \right)$$

$$= 2 \left[\left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \dots \right]$$

$$= 2$$

$$\text{ดังนั้น} \quad 1 + \frac{1}{3} + \frac{1}{6} + \frac{1}{10} + \frac{1}{15} + \frac{1}{21} + \dots = 2 \quad \square$$

ปัญหา 3 จงพิจารณาว่าข้อความในข้อใดต่อไปนี้เป็นจริง พร้อมทั้งให้เหตุผล

(3.1) ถ้า n_1 และ n_2 เป็นจำนวนสามเหลี่ยม แล้ว $n_1 + n_2$ เป็นจำนวนสามเหลี่ยม

(3.2) ถ้า n_1 และ n_2 เป็นจำนวนสามเหลี่ยม แล้ว $n_1 n_2$ เป็นจำนวนสามเหลี่ยม

(3.3) ถ้า n เป็นจำนวนสามเหลี่ยม แล้ว $9n + 1$ เป็นจำนวนสามเหลี่ยม

(3.4) ถ้า n เป็นจำนวนสามเหลี่ยม แล้ว $n + 1$ เป็นจำนวนสามเหลี่ยม

ปัญหา 4 ลำดับฟีโบนัคซี

พิจารณาลำดับของจำนวนเต็มบวก $\{f_n\}$: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

โดยที่ $f_1 = f_2 = 1$

และ $f_n = f_{n-1} + f_{n-2}$ สำหรับจำนวนเต็มบวก $n > 2$

เราเรียกลำดับชนิดนี้ว่า ลำดับฟีโบนัคซี (Fibonacci sequence) ซึ่งเป็นลำดับที่รู้จักกันอย่างดีในคณิตศาสตร์ โดยลำดับฟีโบนัคซีนี้เป็นลำดับที่มีสมบัติและบทประยุกต์ต่าง ๆ มากมาย ปัญหาที่เราสนใจเกี่ยวกับลำดับฟีโบนัคซี คือ

มีจำนวนพจน์ของลำดับฟีโบนัคซีที่พจน์ ที่ค่าของพจน์นั้นน้อยกว่าหรือเท่ากับจำนวนเต็มบวก N

ปัญหา 5 ให้ $a_1 = 3$ และ $a_{n+1} = a_n(a_n + 2)$ สำหรับจำนวนเต็มบวก n

จงหาพจน์ทั่วไป a_n ของลำดับนี้ในรูปของ n

วิธีทำ เนื่องจาก $a_1 = 3 = 2^2 - 1 = 2^{2^1} - 1$

$$a_2 = 3(3 + 2) = 15 = 2^4 - 1 = 2^{2^2} - 1$$

$$a_3 = 15(15 + 2) = 255 = 2^8 - 1 = 2^{2^3} - 1$$

$$a_4 = 255(255 + 2) = 65535 = 2^{16} - 1 = 2^{2^4} - 1$$

⋮

ดังนั้น $a_n = 2^{2^n} - 1$ สำหรับทุกจำนวนนับ n

□

ปัญหา 6 จงหาค่าของจำนวนเต็มบวก n ที่น้อยที่สุดที่ทำให้

$$\frac{1}{2^7} \cdot \frac{3}{2^7} \cdot 2^{\frac{2n+1}{7}} \dots$$

มีค่ามากกว่า 1,000

ปัญหา 7 จงหาจำนวนเต็มบวก n ที่เป็นคำตอบของสมการ

$$\frac{1+3+5+7+\dots+(2n-1)}{2+4+6+8+\dots+(2n)} = \frac{115}{116}$$

ปัญหา 8 จงหาค่าของ $1 - 2 + 2^2 - 2^3 + \dots + 2^{100}$

ปัญหา 9 ให้ A แทนผลบวกของจำนวนเต็มบวก 80 จำนวนแรก

และ B แทนผลบวกของจำนวนเต็มบวก 80 จำนวนแรก

จงหาค่าของ $B - A$

ปัญหา 10 จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $2^8 + 2^{11} + 2^n$ เป็นกำลังสองสมบูรณ์

ปัญหา 11 จงหาค่าของ $1^2 - 2^2 + 3^2 - 4^2 + \dots + 2001^2 - 2002^2 + 2003^2$

ปัญหา 12 จงหาผลบวกของเลขโดดทั้งหมดที่ใช้ในการเขียนจำนวนเต็มตั้งแต่ 1 ถึง 1,000,000

วิธีทำ จากการจับคู่ (0, 999999), (1, 999998), (2, 999997), ..., (499999, 500000)

พบว่าทั้งหมด 500,000 คู่ โดยแต่ละคู่มีผลบวกของเลขโดด เท่ากับ

$$9 + 9 + 9 + 9 + 9 + 9 = 54$$

เพราะฉะนั้น ผลบวกทั้ง 500,000 คู่เท่ากับ $500,000 \times 54 = 27,000,000$

ดังนั้น ผลบวกของเลขโดดทั้งหมดที่ใช้ในการเขียนจำนวนเต็มตั้งแต่ 1 ถึง 1,000,000 เท่ากับ

$$27,000,000 + (1 + 0 + 0 + 0 + 0 + 0 + 0) = 27,000,001 \quad \square$$

ปัญหา 13 ให้ S, E, N, D, M, O, R, G, L, Y แทนจำนวนเต็มตั้งแต่ 0 ถึง 9 ที่ต่างกัน

ถ้า $SEND + MORE + GOLD = MONEY$ แล้ว

จงหาค่าของ S, E, N, D, M, O, R, G, L, Y

ปัญหา 14 ให้ M, E, T, Y แทนจำนวนเต็มตั้งแต่ 0 ถึง 9 ที่ต่างกัน

ถ้า $(YE)(TE) = TTT$ แล้ว จงหาค่าของ $E + M + T + Y$

ปัญหา 15 บทนิยาม จำนวน *Squarish* คือจำนวนเต็ม 6 หลักที่สอดคล้องกับสมบัติต่อไปนี้

1. ไม่มีหลักใดเป็น 0
2. เป็นกำลังสองสมบูรณ์ และ
3. ถ้าพิจารณา 2 หลักแรก, 2 หลักกลาง และ 2 หลักสุดท้าย ในแง่ของจำนวนเต็มสองหลัก ทั้งสามจำนวนนั้นจะต้องเป็นกำลังสองสมบูรณ์

จงหาว่ามีจำนวน *squarish* กี่จำนวน

ปัญหา 16 จงหาผลบวกของเลขโดดทั้งหมดของ 4444^{4444}

ปัญหา 17 ให้ a, b และ c เป็นจำนวนเต็มบวก ซึ่งสอดคล้อง

$$a^3 - b^3 - c^3 = 3abc$$

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

จงหาค่าของ a, b และ c

วิธีทำ เนื่องจาก $3abc$ เป็นจำนวนเต็มบวก จะได้ว่า $a^3 > b^3$ และ $a^3 > c^3$

และจะได้ $b < a$ และ $c < a$ ดังนั้น $b + c < 2a$ จะได้ $2(b + c) < 4a$

เพราะว่า $a^2 = 2(b + c)$ ฉะนั้น $a^2 < 4a$ ดังนั้น $a < 4$

จาก $a^2 = 2(b + c)$ อีกครั้งแสดงว่า a เป็นจำนวนคู่บวกเท่านั้น

เพราะฉะนั้น $a = 2$ และ $b = c = 1$ □

ปัญหา 18 ให้ $N = \frac{2^{32}+1}{641}$ เป็นจำนวนเต็ม

จงแสดงว่า N สามารถเขียนอยู่ในรูปผลบวกของกำลังสองของจำนวนเต็ม 2 จำนวน

วิธีทำ เพราะว่า $\frac{a^2+b^2}{c^2+d^2} = \frac{(ac+bd)^2+(ad-bc)^2}{(c^2+d^2)^2}$

ให้ $a = 2^{16}$, $b = 1$, $c = 4$ และ $d = 25$

$$\begin{aligned} \text{เราพบว่า } \frac{2^{32}+1}{641} &= 6700417 = \frac{(2^{16})^2+1^2}{4^2+25^2} \\ &= \frac{(2^{16} \cdot 4 + 25)^2}{(16+625)^2} + \frac{(2^{16} \cdot 25 - 4)^2}{(16+625)^2} \\ &= \left(\frac{262169}{641}\right)^2 + \left(\frac{1638396}{641}\right)^2 \\ &= (409)^2 + (2556)^2 \end{aligned}$$

□

ปัญหา 19 จงหาจำนวนเต็มบวก 6 หลักที่มีค่าเป็น 6 เท่า หลังจากที่เราสลับ 3 หลักแรกกับ 3 หลักหลัง

วิธีทำ ให้ N เป็นจำนวนเต็มบวก 6 หลัก ซึ่ง $N = 1000A + B$

โดยที่ A และ B เป็นจำนวนเต็มบวก 3 หลัก

ฉะนั้นถ้าเราสลับ 3 หลักแรกกับ 3 หลักหลัง จะได้ว่า

$$1000B + A = 6(1000A + B) = 6000A + 6B$$

$$5999A = 994B$$

$$857A = 142B$$

เพราะว่า $(857, 142) = 1$ ดังนั้น $A = 142$, $B = 857$

เพราะฉะนั้น $N = 142,857$

□

ปัญหา 20 จงหาค่าของ $1 + 3 + 5 + 7 + \dots + (2n-1)$

ปัญหา 21 จงหาค่าของ $1 + 2 - 3 + 4 - 5 + 6 - 7 + \dots + 2000 - 2001 + 2002 - 2003$

ปัญหา 22 เพราะว่า $1^n + 2^n + 3^n + 4^n = 10$ เมื่อ $n = 1$ และเมื่อนำ 10 ไปหาร แล้วเหลือ เศษ 0
จงหาจำนวนเต็มบวก n ที่เป็นไปได้ทั้งหมดซึ่งทำให้เศษที่ได้จากการหาร $1^n + 2^n + 3^n + 4^n$ ด้วย 10 เท่ากับ 0

ปัญหา 23 เราจะเรียกจำนวนเต็มบวกว่า จำนวนพาลินโดม (Palindromic number) ก็ต่อเมื่อ
เราอ่านแต่ละหลักของจำนวนนั้นจากซ้ายไปขวาเหมือนกับการอ่านจำนวนนั้นจากขวาไปซ้าย
เช่น 5, 33, 121, 2002

จงหาจำนวนของจำนวนพาลินโดมที่มีค่าน้อยกว่า 1,000,000

ปัญหา 24 จงหาจำนวนพาลินโดม 9 จำนวนที่แตกต่างกันและมีผลบวกเป็น 99999

ปัญหา 25 จงหาพจน์ที่ 12 ของลำดับฟีโบนัชชี

ปัญหา 26 จงหาค่าของ $\frac{111 + 222 + 333 + \dots + 999}{100 + 200 + 300 + \dots + 900}$

แบบฝึกหัดเรื่อง ความรู้เบื้องต้น

1. จงพิสูจน์ว่าข้อความต่อไปนี้เป็นจริงสำหรับทุกจำนวนเต็มบวก n
 - (1.1) $a^{n+1} - 1 = (a - 1)(a^n + a^{n-1} + a^{n-2} + \cdots + a + 1)$
 - (1.2) $1 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1}n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$
 - (1.3) $1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (n-1) \cdot 2^{n+1} + 2$
 - (1.4) $1 + 2 + 2^2 + 2^3 + 2^4 + \cdots + 2^n = 2^{n+1} - 1$
 - (1.5) $1 \cdot 3 + 2 \cdot 5 + 3 \cdot 7 + \cdots + (3n-2)(3n+1) = n(3n^2 + 3n - 2)$
2. จงพิสูจน์ว่า $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$
เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 2$
3. จงพิสูจน์ว่า $\sum_{i=1}^n \frac{1}{(3i-2)(3i+1)} = \frac{n}{3n+1}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n
4. จงพิสูจน์ว่า $5^n + 5 < 5^{n+1}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n
5. จงพิสูจน์ว่า $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n
6. ถ้า a เป็นจำนวนเต็มซึ่ง $a > -1$ และ $a \neq 0$
จงพิสูจน์ว่า $(1+a)^n > 1+na$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n > 2$
7. ให้ $a, b, c, d \in \mathbb{Z}$ จงพิสูจน์ว่า
 - (7.1) $-a = (-1)a$
 - (7.2) $(a-b) + (c-d) = (a+c) - (b+d)$
 - (7.3) $(a-b) - (c-d) = (a+d) - (b+c)$
 - (7.4) $(a-b)(c-d) = (ac+bd) - (ad+bc)$
 - (7.5) $a-b = c-d$ ก็ต่อเมื่อ $a+d = b+c$
 - (7.6) $(a-b)c = ac - bc$
8. ให้ $a, b, c, x, y \in \mathbb{Z}$ จงพิสูจน์ว่า
 - (8.1) $a < b$ ก็ต่อเมื่อ $a+c < b+c$
 - (8.2) $a-x < a-y$ ก็ต่อเมื่อ $x > y$
 - (8.3) ถ้า $a < 0$ แล้ว $ax > ay$ ก็ต่อเมื่อ $x < y$
 - (8.4) ถ้า $c > 0$ และ $ac < bc$ แล้ว $a < b$
 - (8.5) ถ้า $x+x+x+x = 0$ แล้ว $x = 0$
 - (8.6) ถ้า $a < b$ แล้ว $a^3 < b^3$
9. จงพิสูจน์ว่า ถ้า $a^7 = b^7$ แล้ว $a = b$

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

11. จงใช้หลักอุปนัยเชิงคณิตศาสตร์พิสูจน์ว่า

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

สำหรับจำนวนเต็มบวก n ใด ๆ

12. สำหรับจำนวนเต็มบวก n ใด ๆ จงพิสูจน์ว่า

$$(12.1) \quad 2 \cdot 6 \cdot 10 \cdot 14 \cdots (4n-2) = \frac{(2n)!}{n!}$$

$$(12.2) \quad 2^n(n!)^2 \leq (2n)!$$

$$(12.3) \quad \frac{(2n)!}{2^n(n!)^2} \text{ เป็นจำนวนเต็ม สำหรับทุก } n \in \mathbb{N} \cup \{0\}$$

13. จงแสดงว่า ถ้า $2 \leq k \leq n-2$ แล้ว

$$\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$$

สำหรับ $n \geq 4$

14. จงพิสูจน์ว่า สำหรับ $n \in \mathbb{N}$, $\binom{2n}{n} = \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{1 \cdot 3 \cdot 5 \cdots n} \cdot 2^n$

15. จงพิสูจน์ว่า สำหรับจำนวนเต็ม $n \geq 2$

$$\binom{2}{2} + \binom{4}{2} + \binom{6}{2} + \cdots + \binom{2n}{2} = \frac{n(n+1)(n+2)}{6}$$

$$(\text{ข้อเสนอแนะ} \quad \text{สำหรับ } m \geq 2, \binom{2m}{2} = 2\binom{m}{2} + m^2)$$

บทที่ 2

การหารลงตัว

2.1 ขั้นตอนวิธีการหาร

ในการหาผลหารของจำนวนเต็มสองจำนวน เราอาจใช้วิธีการหารยาวดังตัวอย่างต่อไปนี้ พิจารณา 112 หารด้วย 25

$$\begin{array}{r} 4 \\ 25 \overline{)112} \\ \underline{100} \\ 12 \end{array}$$

แสดงว่า 112 หารด้วย 25 ไม่ลงตัว และได้ผลหารเท่ากับ 4 เศษเท่ากับ 12 เราสามารถเขียนความสัมพันธ์ระหว่างตัวเลข 4 ตัวนี้ได้เป็น $112 = 25(4) + 12$

ทฤษฎีบท 2.1.1 ขั้นตอนวิธีการหาร (The division algorithm)

ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$

แล้วจะมีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้น ที่ทำให้

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

จะเรียก q ว่า ผลหาร (quotient) และ r ว่า เศษ (remainder)

บทพิสูจน์ ตอน 1 จะพิสูจน์ว่ามี $q, r \in \mathbb{Z}$ ที่ทำให้ $b = aq + r$, $0 \leq r < |a|$

โดยจะแบ่งการพิสูจน์ออกเป็นสองกรณี

กรณี 1 ถ้า $a > 0$ แล้ว $|a| = a$

$$\text{ให้ } S = \{b - ax \mid x \in \mathbb{Z} \text{ และ } b - ax \geq 0\}$$

เนื่องจาก $a \geq 1$ จะได้ว่า $|b|a \geq |b|$

แสดงว่า $b - (-|b|)a \geq b + |b| \geq 0$ ดังนั้น $S \neq \emptyset$

แสดงว่า จะมี $s \in S$ ซึ่ง $s = 0$ หรือ $s > 0$

ถ้า $s = 0$ จะได้ว่ามี $q \in \mathbb{Z}$ ซึ่ง $s = b - aq$

นั่นคือ $b = aq + s$ เมื่อ $s = 0$

ถ้า $s > 0$ โดยหลักการจัดอันดับดี จะมี $r \in S$ ซึ่ง $r = s$ หรือ $r < s$ เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S

แสดงว่า จะมี $q \in \mathbb{Z}$ ซึ่ง $r = b - aq$

ดังนั้น $b = aq + r$ โดยที่ $r > 0$

ต่อไปจะแสดงว่า $r < a$ โดยสมมติว่า $r \geq a$

ดังนั้น $r - a = (b - aq) - a = b - a(q + 1) \geq 0$

แสดงว่า $r - a \in S$

แต่ $r - a < r$ ซึ่งขัดแย้งกับที่ r เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S

ดังนั้น $r < a = |a|$

เพราะฉะนั้น มี $q, r \in \mathbb{Z}$ ที่ทำให้

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

กรณี 2 ถ้า $a < 0$ แล้ว $|a| = -a$

จากกรณี 1 จะได้ว่ามี $d, r \in \mathbb{Z}$ ที่ทำให้

$$b = (-a)d + r = a(-d) + r, \quad 0 \leq r < -a = |a|$$

ให้ $q = -d$ แสดงว่ามี $q, r \in \mathbb{Z}$ ซึ่ง

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

ตอน 2 ต่อไปจะแสดงว่ามี $q, r \in \mathbb{Z}$ เพียงคู่เดียวเท่านั้นที่ทำให้ $b = aq + r$

โดยที่ $0 \leq r < |a|$ นั่นคือสมมติว่ามี $q, r, q', r' \in \mathbb{Z}$ ที่ทำให้

$$b = aq + r, \quad 0 \leq r < |a|$$

$$\text{และ } b = aq' + r', \quad 0 \leq r' < |a|$$

จะพิสูจน์ว่า $q = q'$ และ $r = r'$

$$\text{ให้ } b = aq + r, \quad 0 \leq r < |a|$$

$$\text{และ } b = aq' + r', \quad 0 \leq r' < |a|$$

$$\text{จะได้ว่า } |a||q - q'| = |r - r'| \quad \text{โดยที่ } 0 \leq |r - r'| < |a|$$

$$\text{ดังนั้น } 0 \leq |a||q - q'| < |a| \quad \text{แสดงว่า } 0 \leq |q - q'| < 1$$

และจาก $|q - q'|$ เป็นจำนวนเต็ม

$$\text{จะได้ว่า } |q - q'| = 0 \quad \text{และทำให้ } |r - r'| = 0$$

$$\text{นั่นคือ } q = q' \quad \text{และ } r = r'$$



ตัวอย่าง 1 (1.1) ให้ $b = 60$ และ $a = 7$ แล้วจะมี $q = 8$ และ $r = 4$

$$\text{ที่ทำให้ } b = qa + r, \quad 0 \leq r < |a|$$

$$60 = (8)7 + 4, \quad 0 \leq r < |7|$$

(1.2) ให้ $b = -39$ และ $a = 6$ แล้วจะมี $q = -7$ และ $r = 3$

$$\text{ที่ทำให้ } b = qa + r, \quad 0 \leq r < |a|$$

$$-39 = (-7)6 + 3, \quad 0 \leq 3 < |6|$$

□

ปัญหา 2 จงหาจำนวนเต็ม q และ r ที่เป็นไปตามทฤษฎีบท 2.1.1 จากค่า a, b ที่กำหนดให้ต่อไปนี้

(1.1) $b = 111, a = 11$

(1.2) $b = -114, a = 9$

(1.3) $b = 1205, a = -12$

(1.4) $b = -175, a = -5$

ปัญหา 3 จงพิสูจน์ว่า ถ้า $a, b \in \mathbb{Z}$ โดยที่ $a > 0$ แล้วจะมี $q, r \in \mathbb{Z}$ เพียงคู่เดียว

$$\text{เท่านั้นที่ทำให้ } b = aq + r, \quad 2a < r < 3a$$

ตัวอย่าง 4 จงแสดงว่า ถ้า n เป็นจำนวนเต็มคี่ แล้วจะมีจำนวนเต็ม k ที่ทำให้ $n^2 = 8k + 1$

วิธีทำ ให้ n เป็นจำนวนเต็มคี่ พิจารณาจำนวนเต็มใด ๆ และ 4 จากขั้นตอนวิธีการหาร

จะมีจำนวนเต็ม q ที่ทำให้จำนวนเต็มใด ๆ สามารถเขียนอยู่ในรูปของ $4q, 4q + 1, 4q + 2, 4q + 3$ เนื่องจาก n เป็นจำนวนเต็มคี่ จะได้ว่า

$$n = 4q + 1 \quad \text{หรือ} \quad n = 4q + 3$$

ดังนั้น $n^2 = (4q + 1)^2 \quad \text{หรือ} \quad n^2 = (4q + 3)^2$

นั่นคือ $n^2 = 8(2q^2 + q) + 1 \quad \text{หรือ} \quad n^2 = 8(2q^2 + 3q + 1) + 1$

กรณี $n^2 = 8(2q^2 + q) + 1$

ให้ $k = 2q^2 + q$ จะได้ว่า $n^2 = 8k + 1$

กรณี $n^2 = 8(2q^2 + 3q + 1) + 1$

ให้ $k = 2q^2 + 3q + 1$ จะได้ว่า $n^2 = 8k + 1$

สรุป กำลังสองของจำนวนเต็มคี่สามารถเขียนอยู่ในรูปของ $8k + 1$ เมื่อ $k \in \mathbb{Z}$

□

ปัญหา 5 จงแสดงว่า $\frac{a(a^2+2)}{3}$ เป็นจำนวนเต็มเสมอ เมื่อ a เป็นจำนวนเต็มบวก

(ข้อเสนอแนะ ใช้ขั้นตอนวิธีการหาร, a สามารถเขียนในรูปของ $3q$ หรือ $3q + 1$ หรือ $3q + 2$ สำหรับจำนวนเต็ม q บางจำนวน)

ปัญหา 6 มีจำนวนนับตั้งแต่ 1 ถึง 100 รวมทั้งสิ้นกี่จำนวนซึ่งเมื่อหารด้วย 6 แล้วเหลือเศษ 2 และเมื่อหารด้วย 14 แล้วเหลือเศษ 10

โจทย์ปัญหา 2.1

- จงใช้ขั้นตอนวิธีการหารเพื่อแสดงว่า
 - (1.1) กำลังสองของจำนวนเต็มใด ๆ สามารถเขียนอยู่ในรูปของ $3k$ หรือ $3k + 1$ สำหรับจำนวนเต็ม k บางจำนวน
 - (1.2) กำลังสามของจำนวนเต็มใด ๆ สามารถเขียนอยู่ในรูปของ $9k$ หรือ $9k + 1$ หรือ $9k + 8$ สำหรับจำนวนเต็ม k บางจำนวน
 - (1.3) กำลังสี่ของจำนวนเต็มใด ๆ สามารถเขียนอยู่ในรูปของ $5k$ หรือ $5k + 1$ สำหรับจำนวนเต็ม k บางจำนวน
- จงแสดงว่า จำนวนเต็มที่เขียนอยู่ในรูปของ $6k + 5$ โดยที่ k เป็นจำนวนเต็ม สามารถเขียนให้อยู่ในรูปของ $3j + 2$ ได้ สำหรับจำนวนเต็ม j บางจำนวน
- จงแสดงว่า $\frac{n(n+1)(2n+1)}{6}$ เป็นจำนวนเต็มเสมอ เมื่อ n เป็นจำนวนเต็มบวก
(ข้อเสนอแนะ ใช้ขั้นตอนวิธีการหาร n สามารถเขียนให้อยู่ในรูปใดรูปหนึ่งของ $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4, 6k + 5$ สำหรับจำนวนเต็ม k บางจำนวน)
- ถ้า n เป็นจำนวนเต็มคี่แล้ว จงแสดงว่า $n^4 + 4n^2 + 11$ สามารถเขียนอยู่ในรูปของ $16k$ สำหรับจำนวนเต็ม k บางจำนวน
- มีจำนวนนับตั้งแต่ 1 ถึง 200 รวมทั้งสิ้นกี่จำนวน ซึ่งเมื่อหารด้วย 6 แล้วเหลือเศษ 2 และเมื่อหารด้วย 14 แล้วเหลือเศษ 10

2.2 นิยามการหารลงตัว

ในการหารจำนวนเต็มด้วยจำนวนเต็ม เราพบว่า เศษที่เกิดจากการหารอาจเป็นศูนย์ได้ เช่น 132 หารด้วย 4 จะได้ว่า $132 = (33)(4) + 0$ ดังนั้น เศษของการหารคือ 0 เราจะเรียกการหารจำนวนเต็มด้วยจำนวนเต็มแล้วเหลือเศษศูนย์ว่า การหารลงตัว (*divisibility*) ซึ่งมีนิยามดังนี้

บทนิยาม 2.2.1 ถ้า a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ เราจะเรียกว่า a ว่าเป็น ตัวหาร (*divisor*) หรือ ตัวประกอบ (*factor*) ตัวหนึ่งของ b ก็ต่อเมื่อ มีจำนวนเต็ม q ที่ทำให้ $b = aq$
ในกรณีที่ a เป็นตัวหารของ b เราจะเรียกอีกแบบหนึ่งว่า a หาร b ลงตัว เขียนแทนด้วยสัญลักษณ์ $a \mid b$ และใช้สัญลักษณ์ $a \nmid b$ แทน a หาร b ไม่ลงตัว

- ตัวอย่าง 1**
- (1.1) $13 \mid 182$ เพราะมีจำนวนเต็ม 14 ที่ทำให้ $182 = (13)(14)$
 - (1.2) $-5 \mid 30$ เพราะมีจำนวนเต็ม -6 ที่ทำให้ $30 = (-5)(-6)$
 - (1.3) $17 \mid (-289)$ เพราะมีจำนวนเต็ม -17 ที่ทำให้ $-289 = (17)(-17)$
 - (1.4) $135 \mid 0$ เพราะมีจำนวนเต็ม 0 ที่ทำให้ $0 = (135)(0)$
 - (1.5) $4 \nmid 15$ เพราะไม่มีจำนวนเต็ม q ใด ๆ เลยที่ทำให้ $15 = 4q$

□

ปัญหา 2 จงหาตัวหารทั้งหมดของจำนวนเต็มต่อไปนี้

$$(2.1) \quad 100$$

$$(2.2) \quad 225$$

ตัวอย่าง 3 จงแสดงว่า ถ้า a เป็นจำนวนเต็ม แล้ว $3 \mid (a^3 - a)$

บทพิสูจน์ ให้ a เป็นจำนวนเต็มใด ๆ จากขั้นตอนวิธีการหาร a สามารถเขียนอยู่ในรูปของ $3k$ หรือ $3k + 1$ หรือ $3k + 2$ สำหรับจำนวนเต็ม k บางจำนวน

$$\text{ดังนั้น } a^3 - a = (3k)^3 - 3k = 3(9k^3 - k) \quad \text{จะได้ว่า } 3 \mid (a^3 - a)$$

$$\text{หรือ } a^3 - a = (3k + 1)^3 - (3k + 1) = 3(9k^3 + 9k^2 + 2k) \quad \text{จะได้ว่า } 3 \mid (a^3 - a)$$

$$\text{หรือ } a^3 - a = (3k + 2)^3 - (3k + 2) = 3(3k^3 + 18k^2 + 11k + 2)$$

$$\text{จะได้ว่า } 3 \mid (a^3 - a)$$

$$\text{สรุป ถ้า } a \text{ เป็นจำนวนเต็มใด ๆ แล้ว } 3 \mid (a^3 - a) \quad \square$$

ปัญหา 4 จงแสดงว่า ถ้า a เป็นจำนวนเต็มแล้ว $8 \mid (a^2 - 1)$

(ข้อเสนอแนะ) ใช้ขั้นตอนวิธีการหาร a สามารถเขียนอยู่ในรูปใดรูปหนึ่งของ $8k + 1, 8k + 3, 8k + 5, 8k + 7$ สำหรับจำนวนเต็ม k บางจำนวน)

โจทย์ปัญหา 2.2

1. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มแล้ว $16 \mid (a^4 + b^4 - 2)$
2. จงแสดงว่า ผลคูณของจำนวนเต็ม 3 จำนวนที่เรียงต่อเนื่องกันจะหารด้วย 6 ลงตัว และผลคูณของจำนวนเต็ม 4 จำนวนที่เรียงต่อเนื่องกันจะหารด้วย 24 ลงตัว
3. จงหาจำนวนเต็มบวกที่มีค่ามากที่สุดที่นำไปหาร $n(n+1)(n+2)(n+3)(n+4)$ ได้ลงตัวเสมอ สำหรับทุกจำนวนเต็มบวก n
4. สำหรับจำนวนเต็มบวก n , จงใช้หลักอุปนัยเชิงคณิตศาสตร์พิสูจน์ข้อความต่อไปนี้
 - (4.1) $8 \mid (5^{2n} + 7)$
(ข้อเสนอแนะ $5^{2(k+1)} + 7 = 5^2(5^{2k} + 7) + (7 - 5^2 \cdot 7)$)
 - (4.2) $15 \mid (2^{4n} - 1)$
 - (4.3) $5 \mid (3^{3n+1} + 2^{n+1})$
 - (4.4) $24 \mid (2 \cdot 7^n + 3 \cdot 5^n - 5)$
 - (4.5) $21 \mid (4^{n+1} + 5^{2n-1})$
5. จงพิสูจน์ว่า ถ้า n เป็นจำนวนเต็มบวก แล้ว $(3!)^n \mid (3n)!$

2.3 สมบัติเบื้องต้นของการหารลงตัว

ในการศึกษาเกี่ยวกับการหารลงตัว สมบัติเบื้องต้นที่ควรทราบ และเป็นข้อเท็จจริงที่จะใช้ในการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มและจำนวนธรรมชาตินั้น พอสรุปได้ดังนี้

ทฤษฎีบท 2.3.1 ให้ a, b, c เป็นจำนวนเต็ม จะได้ว่า

1. $a \mid 0, 1 \mid a, a \mid a$
2. $a \mid 1$ ก็ต่อเมื่อ $a = \pm 1$
3. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$
4. ถ้า $a \mid b$ และ $c \mid d$ แล้ว $ac \mid bd$
5. ถ้า $a \mid (b + c)$ และ $a \mid b$ แล้ว $a \mid c$
6. $a \mid b$ และ $b \mid a$ ก็ต่อเมื่อ $a = \pm b$
7. ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$
8. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bx + cy)$ สำหรับทุกจำนวนเต็ม x, y

บทพิสูจน์ เราจะพิสูจน์เฉพาะข้อ 4. – 8. สำหรับข้อ 1. – 3. ขอเว้นการพิสูจน์ไว้เป็นแบบฝึกหัด

4. ให้ $a \mid b$ และ $c \mid d$ จะได้ว่า มี $r, s \in \mathbb{Z}$ ซึ่ง $b = ar$ และ $d = cs$
 ดังนั้น $bd = (ar)(cs) = (ac)(rs)$ โดยที่ $rs \in \mathbb{Z}$ นั่นคือ $ac \mid bd$
5. ให้ $a \mid (b + c)$ และ $a \mid b$ จะได้ว่า มี $r, s \in \mathbb{Z}$ ซึ่ง $b + c = ar$ และ $b = as$
 ดังนั้น $c = ar - as = a(r - s)$ โดยที่ $r - s \in \mathbb{Z}$ นั่นคือ $a \mid c$
6. $(\Rightarrow)$ ให้ $a \mid b$ และ $b \mid a$ จะได้ว่า มี $r, s \in \mathbb{Z}$ ซึ่ง $b = ar$ และ $a = bs$
 ดังนั้น $b = (bs)r = b(sr)$ แสดงว่า $rs = 1$
 เพราะฉะนั้น $(r = 1 \text{ และ } s = 1) \text{ หรือ } (r = -1 \text{ และ } s = -1)$
 นั่นคือ $a = \pm b$
 $(\Leftarrow)$ ให้ $a = \pm b$ เห็นได้ชัดว่า $a \mid b$ และ $b \mid a$
7. ให้ $a \mid b$ และ $b \neq 0$ จะได้ว่า มี $r \in \mathbb{Z}$ โดยที่ $r \neq 0$ ที่ทำให้ $b = ar$
 เนื่องจาก $|b| = |a||r|$ และ $1 \leq |r|$ ดังนั้น $|a| \leq |a||r| = |b|$
8. ให้ $a \mid b$ และ $a \mid c$ และให้ x, y เป็นจำนวนเต็มใด ๆ
 จะได้ว่า มี $r, s \in \mathbb{Z}$ ซึ่ง $b = ar$ และ $c = as$
 ดังนั้น $bx = arx$ และ $cy = asy$
 แสดงว่า $bx + cy = arx + asy = a(rx + sy)$ โดยที่ $rx + sy \in \mathbb{Z}$
 นั่นคือ $a \mid (bx + cy)$

จากทฤษฎีบท 2.3.1 ข้อ 8. เราสามารถขยายผลได้ดังนี้

บทแทรก 2.3.2 สำหรับจำนวนเต็ม $a, b_1, b_2, \dots, b_n$ ใด ๆ ที่ $a \neq 0$ จะได้ว่า
ถ้า $a \mid b_1, a \mid b_2, \dots, a \mid b_n$ แล้ว $a \mid (b_1x_1 + b_2x_2 + \dots + b_nx_n)$
เมื่อ $x_1, x_2, \dots, x_n$ เป็นจำนวนเต็มใด ๆ

- ตัวอย่าง 1**
- (1.1) เพราะว่า $5 \mid 25$ และ $25 \mid 100$ จะได้ $5 \mid 100$
 - (1.2) เพราะว่า $-7 \mid 49$ และ $3 \mid 9$ จะได้ $-21 \mid 441$
 - (1.3) เพราะว่า $3 \mid 99$ และ $3 \mid 12$ จะได้ $3 \mid (99(-2) + 12(5))$
 - (1.4) ถ้า $x \mid 15$ และ $15 \mid x$ แล้ว $x = \pm 15$

□

ตัวอย่าง 2 ให้ a, b, c เป็นจำนวนเต็ม จงแสดงว่า

- (2.1) ถ้า $a \mid b$ แล้ว $a \mid bc$
- (2.2) ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a^2 \mid bc$

บทพิสูจน์

(2.1) ให้ $a \mid b$ จะได้ว่า มี $k \in \mathbb{Z}$ ซึ่งทำให้ $b = ak$
 c คูณตลอด จะได้ $bc = akc = a(kc) = am$ โดยที่ $m = kc \in \mathbb{Z}$
 ดังนั้น $a \mid bc$

(2.2) ให้ $a \mid b$ และ $a \mid c$ จะได้ว่า มี $m, n \in \mathbb{Z}$ ซึ่ง $b = am$ และ $c = an$
 จะได้ $bc = (am)(an) = a^2(mn) = a^2k$ โดยที่ $k = mn \in \mathbb{Z}$
 ดังนั้น $a^2 \mid bc$

□

ปัญหา 3 ให้ a, b, c เป็นจำนวนเต็ม จงตรวจสอบดูว่าถ้า $a \mid bc$ แล้ว $a \mid b$ หรือ $a \mid c$ เป็นจริงเสมอหรือไม่

ปัญหา 4 ให้ a, b, c เป็นจำนวนเต็ม จงแสดงว่าถ้า $a \mid (b + c)$ แล้ว $a \mid b$ หรือ $a \mid c$ เป็นจริงเสมอหรือไม่

โจทย์ปัญหา 2.3

- ให้ a, b เป็นจำนวนเต็มบวกซึ่ง $a \mid b^2, b^2 \mid a^3, a^3 \mid b^4, b^4 \mid a^5, \dots$ จงแสดงว่า $a = b$
- ให้ a, b, c เป็นจำนวนเต็มและ $c \neq 0$ จงแสดงว่า $a \mid b$ ก็ต่อเมื่อ $ac \mid bc$
- ให้ a, b เป็นจำนวนเต็มใด ๆ จงแสดงว่าถ้า $a \mid b$ แล้ว $a^n \mid b^n$ สำหรับทุกจำนวนเต็มบวก n
- จงหาจำนวนเต็ม n ทั้งหมดที่ทำให้ $(n - 3) \mid (n^3 - 3)$
- จงแสดงว่า ถ้า a เป็นจำนวนเต็ม แล้ว $3 \mid a(2a^2 + 7)$
- จงแสดงว่า ถ้า a เป็นจำนวนเต็มคี่ แล้ว $32 \mid (a^2 + 3)(a^2 + 7)$

2.4 ตัวหารร่วมมาก

ถ้า a, b เป็นจำนวนเต็มใด ๆ จำนวนเต็ม d จะเรียกว่า **ตัวหารร่วม** (*common divisor*) ของ a และ b ถ้า $d \mid a$ และ $d \mid b$ ดังนั้นเซตของตัวหารร่วมจะไม่เป็นเซตว่างเพราะว่ามี $1, -1$ เป็นตัวหารร่วมของ a และ b เสมอ เซตของตัวหารร่วมจะเป็นเซตจำกัด เมื่อ $a \neq 0$ หรือ $b \neq 0$ และเป็นเซตอนันต์เมื่อ $a = b = 0$

ตัวอย่าง 1 จงหาเซตของตัวหารร่วมทั้งหมดของ 50 และ 76

วิธีทำ เซตของตัวหารทั้งหมดของ 50 คือ $A = \{-1, -2, -5, -25, -50, 1, 2, 5, 25, 50\}$

เซตของตัวหารทั้งหมดของ 76 คือ $B = \{-1, -2, -4, -19, -38, -76, 1, 2, 4, 19, 38, 76\}$

จะได้ว่า $A \cap B = \{-1, -2, 1, 2\}$

ดังนั้นเซตของตัวหารร่วมทั้งหมดของ 50 และ 76 คือ $\{-1, -2, 1, 2\}$ □

จากตัวอย่างข้างต้นจะได้ว่าเซตของตัวหารร่วมจะมีสมาชิกที่มีค่ามากที่สุดหรือเป็นตัวหารร่วมที่มีค่ามากที่สุด ซึ่งนิยามดังนี้

บทนิยาม 2.4.1 ให้ a, b เป็นจำนวนเต็ม ซึ่ง $a \neq 0$ หรือ $b \neq 0$ เราจะเรียกจำนวนเต็มบวก d ว่า **ตัวหารร่วมมาก** (*greatest common divisor*) หรือ **ห.ร.ม.** (g.c.d.) ของ a และ b เขียนแทนด้วย (a, b) ก็ต่อเมื่อ d มีสมบัติต่อไปนี้

- (1) $d \mid a$ และ $d \mid b$
- (2) ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \leq d$

จากบทนิยาม เราพบว่า ถ้า $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ จะได้ว่า

- (1) เราสามารถหา (a, b) ได้เสมอ
- (2) (a, b) มีเพียงจำนวนเดียวเท่านั้น
- (3) $(a, b) = (a, -b) = (-a, b) = (-a, -b) = (b, a)$
- (4) $(a, 0) = |a|$ เมื่อ $a \neq 0$
- (5) ถ้า $a \mid b$ แล้ว $(a, b) = |a|$

- ตัวอย่าง 2
- (2.1) $(24, 84) = (84, 24) = 12$
 - (2.2) $(-6, -15) = (6, 15) = 3$
 - (2.3) $(-17, 289) = (17, -289) = 17$
 - (2.4) $(540, 450) = (-450, -540) = 90$ □

ทฤษฎีบท 2.4.2 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ หรือ $b \neq 0$ จะได้ว่า มี $x, y \in \mathbb{Z}$ ที่ทำให้

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

บทพิสูจน์ ให้ $X = \{am + bn \mid m, n \in \mathbb{Z} \text{ และ } am + bn > 0\}$

เนื่องจาก $a \neq 0$ หรือ $b \neq 0$ ดังนั้น $X \neq \emptyset$ และ $X \subseteq \mathbb{N}$

จากหลักการจัดอันดับดีจะได้ว่ามี $d \in X$ ซึ่ง d เป็นจำนวนเต็มบวกที่น้อยที่สุดใน X

ฉะนั้นมี $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$ ต่อไปจะแสดงว่า $d = (a, b)$

(i) จาก $a, d \in \mathbb{Z}$ และ $d \in X$ โดยขั้นตอนวิธีการหารจะได้ว่ามี $q, r \in \mathbb{Z}$ ที่ทำให้

$$a = dq + r, \quad 0 \leq r < d$$

$$a = (ax + by)q + r, \quad 0 \leq r < d \quad (\text{จาก } d = ax + by)$$

$$r = a - (ax + by)q, \quad 0 \leq r < d$$

$$\text{ดังนั้น } r = a(1 - xq) + b(-yq), \quad 0 \leq r < d$$

จาก $0 \leq r < d$ จะได้ว่า $r = 0$ หรือ $0 < r < d$

ถ้า $0 < r < d$ จะได้ $r \in X$ ซึ่งขัดแย้งกับการเลือก d เป็นจำนวนเต็มบวกที่น้อยที่สุดใน X

ดังนั้น $r = 0$ นั่นคือ $d \mid a$

จาก $b, d \in \mathbb{Z}$ และ $d \in X$ พิสูจน์ในทำนองเดียวกันจะได้ว่า $d \mid b$

(ii) ให้ $c \mid a$ และ $c \mid b$ จะได้ว่า $c \mid (ax + by)$ นั่นคือ $c \mid d$

จาก (i) และ (ii) จะได้ว่า มี $x, y \in \mathbb{Z}$ ซึ่งทำให้ $(a, b) = ax + by$ ■

บทแทรก 2.4.3 ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ จะได้ว่าสำหรับจำนวนเต็ม c ใด ๆ

ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid (a, b)$

บทพิสูจน์ ให้ $d = (a, b)$ โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$

และจาก $c \mid a$ และ $c \mid b$ โดยทฤษฎีบท 2.3.1 ข้อ 8. จะได้ว่า $c \mid (ax + by)$

นั่นคือ $c \mid d$ ■

ทฤษฎีบท 2.4.4 ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ จะได้ว่า

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

บทพิสูจน์ ($\Rightarrow$) สมมติว่า $(a, b) = 1$ โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $x, y \in \mathbb{Z}$ ซึ่ง $1 = ax + by$

($\Leftarrow$) สมมติว่ามี $x, y \in \mathbb{Z}$ ซึ่งทำให้ $1 = ax + by$ และให้ $d = (a, b)$

จะได้ว่า $d \mid a$ และ $d \mid b$ ดังนั้น $d \mid (ax + by)$

นั่นคือ $d \mid 1$ แสดงว่า $(a, b) = 1$ ■

ทฤษฎีบท 2.4.5 ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ และ m เป็นจำนวนเต็มบวก จะได้ว่า

$$(ma, mb) = m(a, b)$$

บทพิสูจน์ ให้ $D = (ma, mb)$ และ $d = (a, b)$ โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $x, y, u, v \in \mathbb{Z}$ ซึ่งทำให้

$$D = (ma)x + (mb)y \text{ และ } d = au + bv$$

(i) จาก $D = (ma, mb)$ จะได้ว่า $D \mid ma$ และ $D \mid mb$

ดังนั้น $D \mid (mau + mbv)$ นั่นคือ $D \mid md$

(ii) จาก $d = (a, b)$ จะได้ว่า $d \mid a$ และ $d \mid b$ ดังนั้น $d \mid (max + mby)$

นั่นคือ $md \mid D$

จาก (i) และ (ii) จะได้ว่า $D = md$

แสดงว่า $(ma, mb) = m(a, b)$ ■

ทฤษฎีบท 2.4.6 ถ้า $a, b \in \mathbb{Z}$ โดยที่ $d = (a, b)$ แล้ว $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

บทพิสูจน์ ให้ $d = (a, b)$ จะได้ว่า $d = \left(\frac{da}{d}, \frac{db}{d}\right)$

โดยทฤษฎีบท 2.4.5 จะได้ $d = d\left(\frac{a}{d}, \frac{b}{d}\right)$ ดังนั้น $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ ■

ทฤษฎีบท 2.4.7 ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ และ x เป็นจำนวนเต็ม จะได้ว่า

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

บทพิสูจน์ ให้ $d = (a, b)$ และ $g = (a, b + ax)$ โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $u, v, m, n \in \mathbb{Z}$ ที่ทำให้

$$d = au + bv \text{ และ } g = am + (b + ax)n$$

(i) จาก $d = (a, b)$ จะได้ว่า $d \mid a$ และ $d \mid b$

ดังนั้นโดยทฤษฎีบท 2.3.1 ข้อ 8 จะได้ $d \mid (am + bn + axn)$ นั่นคือ $d \mid g$

(ii) จาก $g = (a, b + ax)$ จะได้ว่า $g \mid a$ และ $g \mid (b + ax)$

ดังนั้น $g \mid ax$

โดยทฤษฎีบท 2.3.1 ข้อ 5. จะได้ว่า $g \mid b$ ดังนั้น $g \mid (au + bv)$

นั่นคือ $g \mid d$

จาก (i) และ (ii) จะได้ว่า $d = g$ แสดงว่า $(a, b) = (a, b + ax)$

และในทำนองเดียวกันเราสามารถพิสูจน์ได้ว่า $(a, b) = (a + bx, b)$ ■

ทฤษฎีบท 2.4.8 ให้ $a, b, c, m \in \mathbb{Z}$ เป็นจำนวนเต็ม จะได้ว่า

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

บทพิสูจน์ 1. ให้ $(a, m) = (b, m) = 1$ จะได้ว่ามี $x, y, u, v \in \mathbb{Z}$ ซึ่ง

$$ax + my = 1 \quad \text{และ} \quad bu + mv = 1$$

$$\text{ดังนั้น } 1 = (ax + my)(bu + mv) = ab(xu) + m(axv + ybu + myv)$$

$$\text{โดยทฤษฎีบท 2.4.4 จะได้ว่า } (ab, m) = 1$$

2. ให้ $(a, m) = 1$ และ $b \mid a$ จะได้ว่ามี $x, y, q \in \mathbb{Z}$ ซึ่ง $ax + my = 1$ และ $a = bq$

$$\text{ดังนั้น } 1 = (bq)x + my = b(qx) + my$$

$$\text{โดยทฤษฎีบท 2.4.4 จะได้ว่า } (b, m) = 1$$

3. ให้ $a \mid bc$ และ $(a, b) = 1$ จะได้ว่ามี $q, x, y \in \mathbb{Z}$ ซึ่ง $bc = aq$ และ $ax + by = 1$

$$\text{ดังนั้น } bcy = aqy \text{ และ } c = axc + byc$$

$$\text{ดังนั้น } c = axc + aqy = a(xc + qy) \quad \text{นั่นคือ } a \mid c$$

4. ให้ $a \mid c$ และ $b \mid c$ โดยที่ $(a, b) = 1$ จะได้ว่ามี $k_1, k_2, x, y \in \mathbb{Z}$ ซึ่ง

$$c = ak_1, \quad c = bk_2 \text{ และ } ax + by = 1$$

$$\text{ดังนั้น } c = cax + cby = (bk_2)ax + (ak_1)by = ab(k_1x + k_2y)$$

$$\text{นั่นคือ } ab \mid c \quad \blacksquare$$

ทฤษฎีบท 2.4.9 ให้ $a, b, q, r \in \mathbb{Z}$ โดยที่ $a > 0$ และ $b = aq + r$, $0 \leq r < a$
จะได้ว่า $(a, b) = (a, r)$

บทพิสูจน์ ให้ $d = (a, b)$ และ $g = (a, r)$ จะต้องพิสูจน์ว่า $d = g$

- (i) จาก $d = (a, b)$ จะได้ว่า $d \mid a$ และ $d \mid b$

$$\text{และจาก } b = aq + r \text{ เราได้ } d \mid a \text{ และ } d \mid r$$

$$\text{ดังนั้น } d \text{ เป็นตัวหารร่วมของ } a \text{ และ } r \text{ โดยบทแทรก 2.4.3 จะได้ว่า } d \mid g$$

- (ii) จาก $g = (a, r)$ จะได้ว่า $g \mid a$ และ $g \mid r$

$$\text{และจาก } r = aq - b \text{ เราได้ } g \mid d \text{ และ } g \mid b$$

$$\text{ดังนั้น } g \text{ เป็นตัวหารร่วมของ } a \text{ และ } b \text{ โดยบทแทรก 2.4.3 จะได้ว่า } g \mid d$$

จาก (i) และ (ii) สรุปได้ว่า $(a, b) = (a, r)$ ■

ตัวอย่าง 1 (1.1) $(252, 198) = (198, 54) = (54, 36) = (36, 18) = (18, 0) = 18$
 (1.2) $(927, 315) = (315, 297) = (297, 18) = (18, 9) = (9, 0) = 9$
 (1.3) $(1000, 925) = (925, 75) = (75, 25) = (25, 0) = 25$
 (1.4) $(2004, 1106) = (1106, 898) = (898, 208) = (208, 66)$
 $= (66, 10) = (10, 6) = (6, 4) = 2$ □

ปัญหา 2 ให้ a เป็นจำนวนเต็ม จงแสดงว่า

(2.1) $(2a + 1, 9a + 4) = 1$
 (2.2) $(5a + 2, 7a + 3) = 1$
 (2.3) ถ้า a เป็นจำนวนเต็มคี่ แล้ว $(3a, 3a + 2) = 1$

ปัญหา 3 จงแสดงว่า ถ้า k เป็นจำนวนเต็มบวกแล้ว $(3k + 2, 5k + 3) = 1$

ตัวอย่าง 4 จงหาค่าของ $(1769, 2378)$

วิธีทำ จาก $2378 = (1)(1769) + 609$ จะได้ $(1769, 2378) = (1769, 609)$
 จาก $1769 = (2)(609) + 551$ จะได้ $(1769, 609) = (609, 551)$
 จาก $609 = (1)(551) + 58$ จะได้ $(609, 551) = (551, 58)$
 จาก $551 = (9)(58) + 29$ จะได้ $(551, 58) = (58, 29) = 29$
 ดังนั้น $(1769, 2378) = 29$ □

เราอาจให้นิยามตัวหารร่วมมากของจำนวนเต็มที่มีมากกว่า 2 จำนวนได้ กล่าวคือ

บทนิยาม 2.4.10 ให้ $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}$ ซึ่งมี $a_i \neq 0$ สำหรับ i บางตัว เราจะเรียก $d \in \mathbb{Z}$ ว่า **ตัวหารร่วม** (common divisor) ของ $a_1, a_2, a_3, \dots, a_n$ ก็ต่อเมื่อ $d \mid a_i$ สำหรับ $i = 1, 2, 3, \dots, n$ และเรียก d ว่า **ตัวหารร่วมมาก** (greatest common divisor) ของ $a_1, a_2, a_3, \dots, a_n$ ก็ต่อเมื่อ d เป็นตัวหารร่วมที่มีค่ามากที่สุด ซึ่งเขียนแทนด้วย $(a_1, a_2, a_3, \dots, a_n)$

จากบทนิยาม เราพบว่า

- (1) เราสามารถหา $(a_1, a_2, a_3, \dots, a_n)$ ได้เสมอและมีเพียงค่าเดียวเท่านั้น
- (2) $(a_1, a_2, a_3, \dots, a_n) = ((a_1, a_2, a_3, \dots, a_{n-1}), a_n) = (a_1, a_2, \dots, (a_{n-1}, a_n))$
- (3) ถ้า $d = (a_1, a_2, a_3, \dots, a_n)$ จะได้ว่ามี $x_1, x_2, x_3, \dots, x_n \in \mathbb{Z}$ ที่ทำให้

$$d = a_1x_1 + a_2x_2 + a_3x_3 + \dots + a_nx_n$$
- (4) ให้ $d = (a_1, a_2, a_3, \dots, a_n)$ จะได้ว่าสำหรับทุก ๆ จำนวนเต็ม c ใด ๆ ถ้า $c \mid a_i$ สำหรับทุก $i = 1, 2, 3, \dots, n$ แล้ว $c \mid d$

- (5) ให้ $d = (a_1, a_2, a_3, \dots, a_n)$ จะได้ว่า $(a_1, a_2, a_3, \dots, a_n) = 1$ ก็ต่อเมื่อ มีจำนวนเต็ม $x_1, x_2, x_3, \dots, x_n$ ที่ทำให้ $a_1x_1 + a_2x_2 + a_3x_3 + \dots + a_nx_n = 1$

ตัวอย่าง 5 (5.1) $(12, 72, 18) = 6$

(5.2) $(42, 49, 19) = 1$

(5.3) $(198, 288, 512) = 2$

(5.4) $(1819, 3587, -997) = 1$ □

โจทย์ปัญหา 2.4

- จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มซึ่ง $(a, b) = 1$ แล้ว $(a + b, a - b) = 1$ หรือ 2
- จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มคู่ที่ไม่ใช่ศูนย์ทั้งคู่ แล้ว $(a, b) = 2\left(\frac{a}{2}, \frac{b}{2}\right)$
- จงแสดงว่า ถ้า a เป็นจำนวนเต็มคู่และ b เป็นจำนวนเต็มคี่ แล้ว $(a, b) = \left(\frac{a}{2}, b\right)$
- จงแสดงว่า ถ้า a, b และ c เป็นจำนวนเต็มซึ่ง $c \mid ab$ แล้ว $c \mid (a, c)(b, c)$
- จงใช้หลักอุปนัยเชิงคณิตศาสตร์แสดงว่าถ้า $a_1, a_2, a_3, \dots, a_n$ และ b เป็นจำนวนเต็มซึ่ง $(a_1, b) = (a_2, b) = \dots = (a_n, b) = 1$ แล้ว $(a_1a_2a_3 \dots a_n, b) = 1$
- จงแสดงว่า ถ้า $(a, b) = 1$ แล้ว $(a^n, b^n) = 1$ สำหรับทุกจำนวนเต็มบวก n
- จงแสดงว่า $(a^n, b^n) = (a, b)^n$ สำหรับทุกจำนวนเต็มบวก n
- จงพิสูจน์ว่า ถ้ามีจำนวนเต็ม x และ y ที่ทำให้ $ax + by = (a, b)$ แล้ว $(x, y) = 1$
- ให้ $a, b, c \in \mathbb{Z}$ และ $d = (a, b)$ จงพิสูจน์ว่า $a \mid bc$ ก็ต่อเมื่อ $\frac{a}{d} \mid c$

2.5 ขั้นตอนวิธีแบบยุคลิด

ในการค้นหาตัวหารร่วมมากของจำนวนเต็มสองจำนวนที่มีค่ามาก ๆ นั้น มีวิธีการหนึ่งที่มีประสิทธิภาพและสะดวกอย่างยิ่งในทางปฏิบัติคือ การใช้ขั้นตอนวิธีแบบยุคลิด ยุคลิดค้นพบว่าการหา ห.ร.ม. ของจำนวนเต็ม 2 จำนวนนั้นเกิดจากการใช้ขั้นตอนวิธีหารหลาย ๆ ครั้ง ทฤษฎีบทต่อไปนี้เป็นเครื่องมือในการหา ห.ร.ม. ของจำนวนเต็ม a, b และหาจำนวนเต็ม x, y ที่ทำให้ $(a, b) = ax + by$

ทฤษฎีบท 2.5.1 ขั้นตอนวิธีแบบยุคลิด (Euclidean Algorithm)

ให้ $a, b \in \mathbb{Z}$ และ $a > 0$ จะได้ว่า มี $q_1, q_2, q_3, \dots, q_n, q_{n+1}, r_1, r_2, r_3, \dots, r_n \in \mathbb{Z}$ ที่ทำให้

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

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

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

$$\vdots$$

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

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

$$\text{และ } (a, b) = (a, r_n) = r_n$$

บทพิสูจน์ การพิสูจน์ของทฤษฎีบทนี้แบ่งออกเป็นสองกรณี

กรณี 1 ถ้า $a \mid b$ โดยขั้นตอนวิธีหารหาร

จะได้ว่ามี $q, r \in \mathbb{Z}$ ซึ่ง $b = aq + r, r = 0$

และโดยทฤษฎีบท 2.4.8 จะได้ว่า $(a, b) = (a, r) = a$

กรณี 2 ถ้า $a \nmid b$ โดยขั้นตอนวิธีหารหาร จะได้ว่ามี $q_1, r_1 \in \mathbb{Z}$ ซึ่ง

$$b = a q_1 + r_1 \quad \text{เมื่อ } 0 < r_1 < a$$

จากความจริงที่ว่าจำนวนเต็มบวกที่น้อยกว่า a เป็นจำนวนจำกัด

และใช้การกระทำซ้ำ ๆ ของขั้นตอนวิธีหารหาร

จะได้ว่ามี $q_2, q_3, \dots, q_n, q_{n+1}, r_2, r_3, \dots, r_n \in \mathbb{Z}$ ที่ทำให้

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

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

$$\vdots$$

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2}$$

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

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

โดยทฤษฎีบท 2.4.8 จะได้ว่า

$$(a, b) = (a, r_1) = (r_1, r_2) = (r_2, r_3) = \dots$$

$$= (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n$$

■

จากทฤษฎีบทขั้นตอนวิธีแบบยุคลิด เราพบว่าในการหาค่า x และ y เมื่อ $(a, b) = ax + by$ นั้น สามารถหาแนวทางได้จากการกำจัดเศษ $r_{n-1}, \dots, r_2, r_1$ จากสมการข้างต้น ซึ่งมีวิธีการดังนี้

เริ่มจากสมการกลุ่มรองสุดท้าย

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

แล้วแทนค่า r_{n-1} ด้วยค่าในสมการขั้นตอนวิธีแบบยุคลิด จะได้ว่า

$$\begin{aligned} r_n &= r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) \\ &= r_{n-2}(1 + q_n q_{n-1}) + r_{n-3}(-q_n) \end{aligned}$$

จะเห็นว่า สมการที่ได้นี้แสดงการเขียน r_n ในรูปผลบวกของ r_{n-2} และ r_{n-3}

ขั้นตอนต่อไป ทำซ้ำเช่นนี้ไปเรื่อย ๆ ซึ่งจะก่าจัดเศษ $r_{n-1}, r_{n-2}, \dots, r_2, r_1$ ตามลำดับ จนในที่สุดจะได้สมการแสดงการเขียน r_n ในรูปผลบวกของ a และ b แต่ r_n คือ ห.ร.ม. ของ a และ b นั่นคือ วิธีการที่ทำให้เราทราบค่า x และ y ที่ทำให้ $(a, b) = ax + by$

ตัวอย่าง 1 จงใช้ขั้นตอนวิธีแบบยุคลิดในการหา $(12378, 3054)$

พร้อมทั้งแสดงวิธีการหาค่า x และ y ที่ทำให้ $(12378, 3054) = 12378x + 3054y$

วิธีทำ

$$12378 = (4)(3054) + 162$$

$$3054 = (18)(162) + 138$$

$$162 = (1)(138) + 24$$

$$138 = (5)(24) + 18$$

$$24 = (1)(18) + 6$$

$$18 = (3)(6)$$

$$\text{ดังนั้น } (12378, 3054) = 6$$

ในการหาค่า x และ y ซึ่ง $12378x + 3054y = 6$ เราสามารถหาได้โดยการทำย้อนกลับซึ่งมีวิธีดังนี้

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 138 \\ &= 6(162 - 138) - 138 \\ &= 6 \cdot 162 - 7 \cdot 138 \\ &= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\ &= 132 \cdot 162 - 7 \cdot 3054 \\ &= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\ &= 132 \cdot 12378 + (-535) \cdot 3054 \end{aligned}$$

$$\text{ดังนั้น } 6 = (12378)(132) + (3054)(-535)$$

จะได้ว่า $x = 132$ และ $y = -535$ □

ปัญหา 2 จากตัวอย่าง 1 มีค่าของ x และ y คู่อื่นที่มีสมบัติดังกล่าวหรือไม่

ปัญหา 3 จงใช้ขั้นตอนวิธีแบบยุคลิดหาค่าของ $(5767, 4453)$

พร้อมทั้งแสดงวิธีการหาค่า x และ y ที่ทำให้ $(5767, 4453) = 5767x + 4453y$

ปัญหา 4 จงหาค่า x และ y ที่สอดคล้องกับ

$$(4.1) \quad 243x + 198y = 9$$

$$(4.2) \quad 71x - 50y = 1$$

$$(4.3) \quad 43x + 64y = 1$$

$$(4.4) \quad 93x - 81y = 3$$

โจทย์ปัญหา 2.5

1. จงแสดงว่า ถ้า $(a, b) = 1$ และ $(a, c) = 1$ แล้ว $(a, bc) = 1$
2. จงแสดงว่า ถ้า $(a, b) = c$ แล้ว $(a^2, b^2) = c^2$
3. จงแสดงว่า ถ้า $a, m, n \in \mathbb{N}$ โดยที่ $m > n$ แล้ว $(a^{2^n} + 1) \mid (a^{2^m} - 1)$
4. จงแสดงว่า ไม่มีจำนวนเต็ม x, y ที่สอดคล้องกับ $x + y = 100$ และ $(x, y) = 3$
5. จงแสดงว่า มี $x, y \in \mathbb{Z}$ จำนวนอนันต์ที่สอดคล้องกับ $x + y = 100$ และ $(x, y) = 5$
6. จงพิสูจน์ว่า $(n^3 + 2n, n^4 + 3n^2 + 1) = 1$ สำหรับทุกจำนวนเต็มบวก n
7. ให้ $a, m, n \in \mathbb{N}$ โดยที่ $m > n$ จงพิสูจน์ว่า

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{ถ้า } a \text{ เป็นจำนวนเต็มคู่} \\ 2 & \text{ถ้า } a \text{ เป็นจำนวนเต็มคี่} \end{cases}$$

2.6 ตัวคูณร่วมน้อย

เรื่องที่มีความสัมพันธ์ควบคู่กับตัวหารร่วมมากของจำนวนเต็มสองจำนวน คือ ตัวคูณร่วมน้อย (ค.ร.น.) สำหรับจำนวนเต็ม c จะกล่าวว่า c เป็น ตัวคูณร่วม (common multiple) ของ a และ b ที่ต่างก็ไม่เท่ากับ ศูนย์ ถ้า $a \mid c$ และ $b \mid c$ จากความหมายนี้จะเห็นได้ว่า $0, ab, -ab$ ต่างก็เป็นตัวคูณร่วมของ a และ b เสมอ แสดงว่าเซตของตัวคูณร่วมที่เป็นบวกจะไม่ใช่เซตว่าง จากหลักการจัดอันดับดี จะได้ว่า เซตนี้จะมีจำนวนเต็มบวกที่น้อยที่สุด เช่น เซตของตัวคูณร่วมที่เป็นบวกของ 8 และ 10 คือ 40, 80, 120, ... จะได้ว่า 40 เป็นสมาชิกที่มีค่าน้อยที่สุด เราเรียกจำนวน 40 นี้ว่า ตัวคูณร่วมน้อยของ 8 และ 10 ซึ่งเราให้นิยามตัวคูณร่วมน้อยดังต่อไปนี้

บทนิยาม 2.6.1 ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ เราจะเรียกจำนวนเต็มบวก m ว่า **ตัวคูณร่วมน้อย** (least common multiple) หรือ **ค.ร.น.** (l.c.m.) ของ a และ b เขียนแทนด้วย $[a, b]$ ก็ต่อเมื่อ m มีสมบัติต่อไปนี้

- (1) $a \mid m$ และ $b \mid m$
- (2) สำหรับจำนวนเต็มบวก c , ถ้า $a \mid c$ และ $b \mid c$ แล้ว $m \leq c$

จากบทนิยามเราพบว่า ถ้า $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ จะได้ว่า

- (1) เซตของตัวคูณร่วมของ a และ b เป็นเซตอนันต์
- (2) ถ้า m เป็นตัวคูณร่วมของ a และ b จะได้ว่า $-m$ เป็นตัวคูณร่วมของ a และ b

$$(3) \quad [a, b] = [b, a] = [a, -b] = [-a, b] = [-a, -b]$$

$$(4) \quad \text{ถ้า } a|b \text{ แล้ว } [a, b] = |b|$$

ตัวอย่าง 1 (1.1) $[15, 21] = 105$

(1.2) $[-24, -36] = 72$

(1.3) $[3054, 12378] = 6,300,402$ □

ปัญหา 2 จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มบวก แล้ว $(a, b) | [a, b]$
และจงหาเงื่อนไขของ a และ b ที่ทำให้ $(a, b) = [a, b]$

ทฤษฎีบท 2.6.2 ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ จะได้ว่า สำหรับจำนวนเต็ม c ใด ๆ
ถ้า $a|c$ และ $b|c$ แล้ว $[a, b] | c$

บทพิสูจน์ ให้ $m = [a, b]$ และ c เป็นจำนวนเต็มใด ๆ ที่ $a|c$ และ $b|c$
โดยขั้นตอนวิธีการหารจะได้ว่า มี $q, r \in \mathbb{Z}$ ซึ่ง $c = mq + r$, $0 \leq r < m$
แสดงว่า $r = c - mq$, $0 \leq r < m$ จาก $a|c$ และ $b|c$ จะได้ว่า $a|r$ และ $b|r$
นั่นคือ r เป็นตัวคูณร่วมของ a และ b ถ้า $0 < r < m$ จะขัดแย้งกับ $m = [a, b]$
ดังนั้น $r = 0$ แสดงว่า $m|c$ ■

ทฤษฎีบทต่อไปนี้เป็นทฤษฎีบทที่แสดงถึงความสัมพันธ์ของ $a, b, (a, b)$ และ $[a, b]$

ทฤษฎีบท 2.6.3 ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ จะได้ว่า $(a, b)[a, b] = |ab|$

บทพิสูจน์ จาก $(a, b) = (|a|, |b|)$ และ $[a, b] = [|a|, |b|]$

ดังนั้น จึงเป็นการเพียงพอที่จะพิสูจน์กรณีที่ $a, b \in \mathbb{N}$

(i) ให้ $d = (a, b)$ จะได้ว่ามี $x, y \in \mathbb{Z}$ ซึ่ง $a = dx$ และ $b = dy$

$$\text{ให้ } m = \frac{ab}{d} = dxy \quad \text{จะได้ว่า } m = ay = bx$$

แสดงว่า $a|m$ และ $b|m$ นั่นคือ m เป็นตัวคูณร่วมของ a และ b

(ii) ให้ c เป็นจำนวนเต็มบวกที่ $a|c$ และ $b|c$

จะได้ว่ามี $u, v \in \mathbb{Z}$ ซึ่ง $c = au$ และ $c = bv$

จาก $a = dx$ และ $b = dy$ จะได้ว่า $dxu = dyv$

ดังนั้น $x|yv$ แต่ $(x, y) = 1$ แสดงว่า $x|v$

ดังนั้น จะมี $r \in \mathbb{Z}$ ซึ่ง $v = xr$ และจาก $m = bx$ และ $c = bv$

จะได้ว่า $c = bxr = mr$ ดังนั้น $m|c$

จาก (i) และ (ii) สรุปว่า $m = [a, b]$

นั่นคือ $(a, b)[a, b] = ab$ ■

ทฤษฎีบท 2.6.4 ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ และ $m \in \mathbb{N}$
จะได้ว่า $[ma, mb] = m[a, b]$

บทพิสูจน์ จากทฤษฎีบท 2.4.5 และทฤษฎีบท 2.6.3 จะได้ว่า

$$(ma, mb)[ma, mb] = m(a, b)[ma, mb] = |(ma)(mb)|$$

ดังนั้น $[ma, mb] = \frac{|m^2 ab|}{m(a, b)} = \frac{m|ab|}{m(a, b)} = m[a, b]$ ■

ในการทำงานเกี่ยวกับตัวหารร่วมมาก เราสามารถขยายบทนิยามของตัวคูณร่วมและตัวคูณร่วมน้อยของจำนวนเต็มมากกว่าสองจำนวนได้ดังนี้

บทนิยาม 2.6.5 ให้ $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}$ ซึ่ง $a_i \neq 0$ สำหรับ $i = 1, 2, 3, \dots, n$
เราเรียก $m \in \mathbb{Z}$ ว่า **ตัวคูณร่วม** (*common multiple*) ของ $a_1, a_2, a_3, \dots, a_n$
ก็ต่อเมื่อ $a_i | m$ สำหรับ $i = 1, 2, 3, \dots, n$ และเรียก m ว่า **ตัวคูณร่วมน้อย**
(*least common multiple*) ของ $a_1, a_2, a_3, \dots, a_n$ ก็ต่อเมื่อ $m \in \mathbb{N}$ และ m
เป็นตัวคูณร่วมที่มีค่าน้อยที่สุดของ ซึ่งเขียนแทนด้วย $[a_1, a_2, a_3, \dots, a_n]$

จากบทนิยามเราพบว่า

- (1) เราสามารถหา $[a_1, a_2, a_3, \dots, a_n]$ ได้เสมอและมีเพียงค่าเดียวเท่านั้น
- (2) $[a_1, a_2, a_3, \dots, a_n] = [[a_1, a_2, \dots, a_{n-1}], a_n] = [a_1, a_2, \dots, [a_{n-1}, a_n]]$
- (3) ให้ $m = [a_1, a_2, a_3, \dots, a_n]$ จะได้ว่าสำหรับทุกจำนวนเต็ม c ใด ๆ
ถ้า $a_i | c$ สำหรับ $i = 1, 2, 3, \dots, n$ แล้ว $m | c$

ตัวอย่าง 3 (3.1) $[7, 11, 13] = 1001$

$$\begin{aligned} (3.2) \quad [3, 8, 10, 15] &= [[3, 8, 10], 15] \\ &= [[[3, 8], 10], 15] \\ &= [[24, 10], 15] \\ &= [120, 15] \\ &= 120 \end{aligned}$$
 □

ปัญหา 4 สำหรับทุกจำนวนเต็มบวก $n \geq 2$

จงพิสูจน์ว่า ถ้า $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}$ ซึ่ง $(a_i, a_j) = 1$ สำหรับทุก $i \neq j$ แล้ว

$$[a_1, a_2, a_3, \dots, a_n] = a_1 a_2 a_3 \cdots a_n$$

โจทย์ปัญหา 2.6

1. ให้ a, b และ c เป็นจำนวนเต็ม จงแสดงว่า $[a, b] \mid c$ ก็ต่อเมื่อ $a \mid c$ และ $b \mid c$
2. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มบวก แล้ว $(a, b) = (a + b, [a, b])$
3. จงแสดงว่า ถ้า a, b และ c เป็นจำนวนเต็มบวก แล้ว

$$([a, b], c) = [(a, c), (b, c)] \quad \text{และ} \quad [(a, b), c] = ([a, c], [b, c])$$

4. จงแสดงว่า ถ้า a, b และ c เป็นจำนวนเต็มบวกแล้ว

$$(a, b, c)[a, b, c] = \frac{abc}{(a, b)(a, c)(b, c)}$$

5. จงแสดงว่า ถ้า $(a, b, c)[a, b, c] = abc$ แล้ว $(a, b) = (b, c) = (a, c) = 1$
6. จงแสดงว่า $(ab, bc, ca)[a, b, c] = |abc|$
7. จงพิจารณาว่าข้อความต่อไปนี้เป็นจริงหรือเท็จ ถ้าข้อความนั้นเป็นจริง จงพิสูจน์

ถ้าข้อความนั้นเป็นเท็จ จงยกตัวอย่างค้าน

$$(7.1) \quad \text{ถ้า } (a, b) = (a, c) \text{ แล้ว } [a, b] = [a, c]$$

$$(7.2) \quad \text{ถ้า } (a, b) = (a, c) \text{ แล้ว } (a^2, b^2) = (a^2, c^2)$$

$$(7.3) \quad \text{ถ้า } (a, b) = (a, c) \text{ แล้ว } (a, b) = (a, b, c)$$

$$(7.4) \quad \text{ถ้า } (a, b) = 1 \text{ แล้ว } (a^2, ab, b^2) = 1$$

$$(7.5) \quad [a^2, ab, b^2] = [a^2, b^2]$$

โจทย์ปัญหาเสริมเรื่อง การหารลงตัว

ปัญหา 1 ให้ $\mathcal{U} = \{1, 2, 3, \dots, 100\}$

$$A = \{x \in \mathcal{U} \mid 2 \text{ หาร } x \text{ ลงตัว}\}$$

$$B = \{x \in \mathcal{U} \mid 3 \text{ หาร } x \text{ ลงตัว}\}$$

$$C = \{x \in \mathcal{U} \mid 5 \text{ หาร } x \text{ ลงตัว}\}$$

จงหาจำนวนสมาชิกในเซตต่อไปนี้

$$(1.1) \quad A, B, C$$

$$(1.2) \quad A \cap B, A \cap C, B \cap C$$

$$(1.3) \quad A \cup B \cup C$$

$$(1.4) \quad A' \cap B' \cap C'$$

ข้อตกลง สัญลักษณ์ $\lfloor x \rfloor$ หมายถึงจำนวนเต็มที่ยกที่สุดที่น้อยกว่าหรือเท่ากับ x

$$\text{เช่น } \lfloor 2 \rfloor = 2, \lfloor 2.1 \rfloor = 2, \lfloor 2.95 \rfloor = 2 \text{ และ } \lfloor -1.5 \rfloor = -2$$

วิธีทำ (1.1) $n(A) = \left\lfloor \frac{100}{2} \right\rfloor = 50$, $n(B) = \left\lfloor \frac{100}{3} \right\rfloor = 33$ และ $n(C) = \left\lfloor \frac{100}{5} \right\rfloor = 20$

$$(1.2) \quad n(A \cap B) = \left\lfloor \frac{100}{6} \right\rfloor = 16, \quad n(A \cap C) = \left\lfloor \frac{100}{10} \right\rfloor = 10, \quad n(B \cap C) = \left\lfloor \frac{100}{15} \right\rfloor = 6,$$

$$n(A \cap B \cap C) = \left\lfloor \frac{100}{30} \right\rfloor = 3$$

$$(1.3) \quad \begin{aligned} n(A \cup B \cup C) &= n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) \\ &\quad + n(A \cap B \cap C) \\ &= 50 + 33 + 20 - 16 - 10 - 6 + 3 = 74 \end{aligned}$$

$$(1.4) \quad \begin{aligned} n(A' \cap B' \cap C') &= n[(A \cup B \cup C)'] \\ &= n(\mathcal{U}) - n(A \cup B \cup C) \\ &= 100 - 74 = 26 \end{aligned}$$

□

ปัญหา 2 ให้ $\mathcal{U} = \{10, 11, 12, \dots, 300\}$

$$S = \{x \in \mathcal{U} \mid 3 \text{ หาร } x \text{ ลงตัว}\}$$

$$E = \{x \in \mathcal{U} \mid 7 \text{ หาร } x \text{ ลงตัว}\}$$

จงหา $n(S)$ และ $n(E)$

ปัญหา 3 ให้ $N = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$ แทนจำนวนเต็ม

จงหาเงื่อนไขการหาร N ด้วย 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ลงตัว

วิธีทำ เมื่อเรากันเคยกกับจำนวนเต็มในแง่การหาร เราอาจตั้งข้อสังเกตได้ เช่น

1. ถ้าจำนวนเต็มที่ลงท้ายเลขคู่ แล้ว 2 จะหารลงตัว
2. ถ้าจำนวนเต็มที่ลงท้ายด้วยเลข 5 หรือ 0 แล้ว 5 จะหารลงตัว
3. ถ้าจำนวนเต็มที่ลงท้ายด้วยเลข 0 แล้ว 10 จะหารลงตัว

เราจะขอสรุปเงื่อนไขการหารด้วย 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ลงตัว

เมื่อ $N = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$ แทนจำนวนเต็มบวก

$2 \mid N$	ก็ต่อเมื่อ	$2 \mid a_0$
$3 \mid N$	ก็ต่อเมื่อ	$3 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$
$4 \mid N$	ก็ต่อเมื่อ	$4 \mid a_1 a_0$
$5 \mid N$	ก็ต่อเมื่อ	$a_0 = 5$ หรือ $a_0 = 0$
$6 \mid N$	ก็ต่อเมื่อ	$2 \mid N$ และ $3 \mid N$
$7 \mid N$	ก็ต่อเมื่อ	$7 \mid (a_n a_{n-1} \cdots a_1 - 2a_0)$
$8 \mid N$	ก็ต่อเมื่อ	$8 \mid a_2 a_1 a_0$
$9 \mid N$	ก็ต่อเมื่อ	$9 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$
$10 \mid N$	ก็ต่อเมื่อ	$a_0 = 0$
$11 \mid N$	ก็ต่อเมื่อ	$11 \mid (a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n)$
$12 \mid N$	ก็ต่อเมื่อ	$4 \mid N$ และ $3 \mid N$

□

ปัญหา 4 ในการเขียนจำนวนเต็มบวกตั้งแต่ 1, 2, 3, 4, 5, ..., 10000 จะต้องใช้เลข 0 (ศูนย์) ทั้งหมดกี่ตัว

วิธีทำ จำนวนเต็ม จาก 1 - 9 ไม่มีเลข 0 ปรากฏเลย

จำนวนเต็ม จาก 10 - 99 ใช้เลข 0 ทั้งหมด 9 ตัว

จำนวนเต็ม จาก 100 - 999 ใช้เลข 0 ทั้งหมด $90 + 90 = 180$ ตัว

จำนวนเต็ม จาก 1000 - 9999 ใช้เลข 0 ทั้งหมด $900 + 900 + 900 = 2700$ ตัว

จำนวนเต็ม 10000 ใช้เลข 0 ทั้งหมด 4 ตัว

ดังนั้น เลข 0 ที่จะใช้ทั้งหมดคือ $9 + 180 + 2700 + 4 = 2893$ ตัว

□

ปัญหา 5 ให้ $\mathcal{X} = \{1, 2, 3, \dots, 100\}$ และ $X = \{x \in \mathcal{X} \mid (x, 100) = 1\}$

จงหา $n(X)$

[โจทย์ข้อนี้อาจใช้ความรู้ $(x, 100) = 1$ ก็ต่อเมื่อ 2 หาร x ไม่ลงตัวและ 5 หาร x ไม่ลงตัว]

ปัญหา 6 ให้ $\mathcal{X} = \{1, 2, 3, 4, 5, \dots, 52920000\}$

และ $A = \{x \in \mathcal{X} \mid \text{ห.ร.ม. ของ } x \text{ กับ } 52920000 \text{ เท่ากับ } 2\}$

จงหาจำนวนสมาชิกของเซต A

ปัญหา 7 จงแสดงว่า $31 \mid (2^{35} - 1)$ และ $127 \mid (2^{35} - 1)$

ปัญหา 8 จงแสดงว่า ถ้า $d \mid n$ แล้ว $(2^d - 1) \mid (2^n - 1)$
(ข้อเสนอแนะ $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \dots + x + 1)$)

ปัญหา 9 ให้ x เป็นจำนวนเต็มที่อยู่ระหว่าง 0 ถึง 100 และ $(x, 15) = 1$
จงหาค่า x ทั้งหมดที่มีค่าจำนวน

วิธีทำ ให้ $\mathcal{X} = \{0, 1, 2, 3, \dots, 100\}$ และ $X = \{x \in \mathcal{X} \mid (x, 15) \neq 1\}$

จะได้ว่า $X = \{x \in \mathcal{X} \mid 3 \text{ หาร } x \text{ ลงตัว หรือ } 5 \text{ หาร } x \text{ ลงตัว}\}$

ให้ $A = \{x \in \mathcal{X} \mid 3 \text{ หาร } x \text{ ลงตัว}\}$

และ $B = \{x \in \mathcal{X} \mid 5 \text{ หาร } x \text{ ลงตัว}\}$

เพราะฉะนั้น $X = A \cup B$

จะได้ว่า $n(X) = n(A \cup B) = n(A) + n(B) - n(A \cap B)$

ดังนั้น $n(X) = 34 + 21 - 7 = 48$ □

ปัญหา 10 กำหนด n เป็นจำนวนเต็มบวกซึ่งหารด้วย 3, 4, 5, 6 และ 7 จะเหลือเศษ 2, 3, 4, 5 และ 6 ตามลำดับ ค่าของ n ที่น้อยที่สุดที่เป็นไปได้เท่ากับเท่าไร

ปัญหา 11 จงหาจำนวนเต็มบวกทั้งหมดที่สามารถเขียนได้ในรูปผลบวกของจำนวนเต็มบวกที่เรียงต่อเนื่องกันมากกว่า 1 จำนวน

$$\text{เช่น } 3 = 1 + 2$$

$$7 = 3 + 4$$

$$28 = 1 + 2 + 3 + 4 + 5 + 6 + 7$$

$$60 = 19 + 20 + 21$$

วิธีทำ พิจารณา $n = 2^t$ เมื่อ $t \in \mathbb{N} \cup \{0\}$

เมื่อ $t = 0$ ได้ $n = 1$, $t = 2$ ได้ $n = 4$

$t = 1$ ได้ $n = 2$, $t = 3$ ได้ $n = 8$

เห็นได้ชัดว่าถ้า $t = 0, 1, 2, 3$ แล้ว n ไม่สามารถเขียนอยู่ในรูปผลบวกของจำนวนเต็มบวกที่เรียง

ต่อเนื่องกันมากกว่า 1 จำนวนได้ ต่อไปจะแสดงว่า จำนวนเต็มบวก n สามารถเขียนอยู่ในรูปผลบวกของ

จำนวนเต็มบวกที่เรียงต่อเนื่องกันมากกว่า 1 จำนวน ก็ต่อเมื่อ $n \neq 2^t$ สำหรับ $t \in \mathbb{N} \cup \{0\}$

($\Rightarrow$) สมมติให้ $n = 2^t$, $t \geq 3$ และยอมรับว่า n สามารถเขียนอยู่ในรูปผลบวกของจำนวนเต็มบวกที่เรียงต่อเนื่องกันมากกว่า 1 จำนวน เราจะแสดงว่าเป็นไปไม่ได้

จาก $n = 2^t$ และจากสมมติฐานจะได้

สำหรับบางจำนวนเต็มบวก k, m

$$\begin{aligned}
 n &= m + (m + 1) + (m + 2) + \cdots + (m + k) \\
 &= \underbrace{(m + m + m + \cdots + m)}_{k+1 \text{ พจน์}} + (1 + 2 + 3 + \cdots + k) \\
 &= m(k + 1) + \frac{k(k + 1)}{2} \\
 &= \frac{1}{2}(k + 1)(2m + k)
 \end{aligned}$$

กรณี 1 ถ้า k เป็นจำนวนเต็มคี่บวก จะได้ว่า $2m + k$ เป็นจำนวนเต็มคี่ แต่ $\frac{k+1}{2}(2m + k) = 2^t$ เป็นจำนวนเต็มคู่ ดังนั้น $2m + k = 1$ ซึ่งเป็นไปไม่ได้

กรณี 2 ถ้า k เป็นจำนวนเต็มคู่บวกและ $(k + 1)\frac{2m + k}{2} = 2^t$ จะได้ว่า $k + 1$ เป็นจำนวนเต็มคี่ ดังนั้น $k + 1 = 1$ ซึ่งเป็นไปไม่ได้

เพราะฉะนั้น ถ้า $n = 2^t$ เป็นไปไม่ได้ ดังนั้น $n \neq 2^t$

($\Leftarrow$) ถ้ายอมรับ $n \neq 2^t$ แล้วจะต้องแสดงว่า n สามารถเขียนอยู่ในรูปผลบวกของจำนวนเต็มบวกที่เรียงต่อเนื่องกันมากกว่า 1 จำนวน

กรณี 1 ถ้า n เป็นจำนวนเต็มคี่บวก แล้ว $n = 2k + 1$ สำหรับบางจำนวนเต็มบวก k จะได้ว่า $n = k + (k + 1)$ ดังนั้น n สามารถเขียนอยู่ในรูปผลบวกของจำนวนเต็มบวกที่เรียงต่อเนื่องกันมากกว่า 1 จำนวน

กรณี 2 ถ้า n เป็นจำนวนเต็มคู่ แล้ว $n = 2^t \cdot m$ เมื่อ $m > 1$ และ $(2, m) = 1$

กรณี 2.1 ถ้า $m < 2^{t+1}$ จะได้ว่า

$$\begin{aligned}
 2^t \cdot m &= \left(2^t - \frac{m-1}{2}\right) + \left(2^t - \frac{m-3}{2}\right) \\
 &\quad + \left(2^t - \frac{m-5}{2}\right) + \cdots + (2^t - 1) \\
 &\quad + \left(2^t - \frac{m-m}{2}\right) + (2^t + 1) \\
 &\quad + (2^t + 2) + \cdots + \left(2^t + \frac{m-1}{2}\right)
 \end{aligned}$$

เนื่องจาก

$$2^t \cdot m = \underbrace{(2^t + 2^t + 2^t + \cdots + 2^t)}_{m \text{ พจน์}} + \frac{m-1}{2} - \frac{m-1}{2} + \cdots + (1 - 1)$$

ดังนั้น $n = 2^t \cdot m$ สามารถเขียนอยู่ในรูปผลบวกของจำนวนเต็มบวกที่เรียงต่อเนื่องกันมากกว่า 1 จำนวน

กรณี 2.2 ถ้า $m > 2^{t+1}$ จะได้ว่า

$$n = 2^t \cdot m = \frac{m - (2^{t+1} - 1)}{2} + \dots + \frac{m - 3}{2} + \frac{m - 1}{2} + \frac{m + 1}{2} \\ + \frac{m + 3}{2} + \dots + \frac{m + (2^{t+1} - 1)}{2}$$

เนื่องจาก

$$2^t \cdot m = \underbrace{\frac{m}{2} + \frac{m}{2} + \dots + \frac{m}{2}}_{2^{t+1} \text{ พจน์}} + \frac{2^{t+1} - 1}{2} - \frac{2^{t+1} - 1}{2} \\ + \dots + \frac{3}{2} - \frac{3}{2} + \frac{1}{2} - \frac{1}{2} \\ = \frac{m}{2} \cdot 2^{t+1} + 0 \\ = 2^t \cdot m$$

ดังนั้น $n = 2^t \cdot m$ สามารถเขียนอยู่ในรูปผลบวกของจำนวนเต็มบวกที่เรียงต่อเนื่องกันมากกว่า 1 จำนวน

จากทั้งสองกรณีเราจะได้ว่า ถ้า $n \neq 2^t$ แล้ว n สามารถเขียนอยู่ในรูปผลบวกของจำนวนเต็มบวกที่เรียงต่อเนื่องกันมากกว่า 1 จำนวน □

ปัญหา 12 ให้ n เป็นจำนวนเต็มบวก

จงหาจำนวนเต็มบวก k ที่มากที่สุดที่ทำให้ 2^k เป็นตัวประกอบของ $3^n + 1$

วิธีทำ ก่อนอื่นเรามาศึกษาข้อสังเกตต่อไปนี้ สำหรับทุกจำนวนเต็มบวก n

- (i) $3^n + 1$ เป็นจำนวนเต็มคู่เสมอ
- (ii) เมื่อ n เป็นจำนวนเต็มบวกเราสามารถเขียน $n = 2^p q$ โดยที่ $p \in \{0, 1, 2, 3, \dots\}$ และ $q \in \{1, 3, 5, 7, \dots\}$
- (iii) $x^{2n+1} + 1 = (x + 1)(x^{2n} - x^{2n-1} + x^{2n-2} - \dots + 1)$

จากข้อสังเกต (iii) และเมื่อ n เป็นจำนวนเต็มคี่ ฉะนั้นให้ $n = 2m + 1$ จะได้ว่า

$$3^n + 1 = 3^{2m+1} + 1 \\ = (3 + 1)(3^{2m} - 3^{2m-1} + 3^{2m-2} - \dots + 1) \\ = 4M \quad \text{โดยที่ } M = 3^{2m} - 3^{2m-1} + 3^{2m-2} - \dots + 1$$

จะเห็นได้ชัดว่า M เป็นผลบวกของจำนวนเต็มคี่ $2m + 1$ จำนวน

นั่นคือ $3^n + 1 = 3^{2m+1} + 1 = 4M = 2^2 M$

ดังนั้น เมื่อ n เป็นจำนวนเต็มคี่ แล้ว $k = 2$ ที่ทำให้ k เป็นจำนวนเต็มบวก

ที่มากที่สุดที่ทำให้ 2^k เป็นตัวประกอบของ $3^n + 1$

จากข้อสังเกต (ii) และเมื่อ n เป็นจำนวนเต็มคู่ จะได้ว่า $n = 2^p q$ เมื่อ $p \geq 1$

ดังนั้น

$$\begin{aligned}
 3^n + 1 &= (2 + 1)^n + 1 \\
 &= [2^n + \binom{n}{1} 2^{n-1} + \binom{n}{2} 2^{n-2} + \dots + \binom{n}{n-1} 2 + 1] + 1 \\
 &= 2^n + \binom{n}{1} 2^{n-1} + \binom{n}{2} 2^{n-2} + \dots + \binom{n}{n-1} 2 + 2 \\
 &= 2[2^{n-1} + \binom{n}{1} 2^{n-2} + \binom{n}{2} 2^{n-3} + \dots + \binom{n}{n-1} + 1] \\
 &= 2N
 \end{aligned}$$

เนื่องจาก $\binom{n}{n-1} = n = 2^p q$, $p \geq 1$ เป็นจำนวนเต็มคู่

จะได้ว่า

$2^{n-1} + \binom{n}{1} 2^{n-2} + \binom{n}{2} 2^{n-3} + \dots + \binom{n}{n-1}$ เป็นจำนวนเต็มคู่

ดังนั้น $N = 2^{n-1} + \binom{n}{1} 2^{n-2} + \binom{n}{2} 2^{n-3} + \dots + \binom{n}{n-1} + 1$ เป็นจำนวนเต็มคี่

นั่นคือ $3^n + 1 = 2N$ และ N เป็นจำนวนเต็มคี่

เราจึงสรุปได้ว่า เมื่อ n เป็นจำนวนเต็มคู่แล้ว $k = 1$ เป็นจำนวนบวกที่มากที่สุดที่ทำให้ 2^k เป็นตัวประกอบของ $3^n + 1$ □

ปัญหา 13 ผลคูณค่ามากที่สุด (Maximum Product)

พิจารณาจำนวนเต็ม 10 เราจะเขียน 10 ในรูปผลบวกของจำนวนเต็มบวกอย่างไรจึงจะทำให้ผลคูณของจำนวนเต็มเหล่านั้นมีค่ามากที่สุด

$10 = 5 + 5$	ผลคูณ คือ	$5 \cdot 5 = 25$
$10 = 1 + 9$	ผลคูณ คือ	$1 \cdot 9 = 9$
$10 = 3 + 3 + 3 + 1$	ผลคูณ คือ	$3 \cdot 3 \cdot 3 \cdot 1 = 27$
$10 = 3 + 3 + 4$	ผลคูณ คือ	$3 \cdot 3 \cdot 4 = 36$
$10 = 3 + 3 + 2 + 2$	ผลคูณ คือ	$3 \cdot 3 \cdot 2 \cdot 2 = 36$
$10 = 1 + 2 + 3 + 4$	ผลคูณ คือ	$1 \cdot 2 \cdot 3 \cdot 4 = 24$
$10 = 4 + 4 + 2$	ผลคูณ คือ	$4 \cdot 4 \cdot 2 = 32$

ดังนั้นเราจะต้องเขียน $10 = 3 + 3 + 2 + 2$ จึงทำให้ $3 \cdot 3 \cdot 2 \cdot 2$ มีค่ามากที่สุด ในการหาคำตอบนั้นไม่ยากอย่างที่คิด และถ้าเราสนใจจำนวนเต็มบวก N ใด ๆ เราจะมีวิธีการหาคำตอบได้อย่างไร ดังปัญหาต่อไปนี้

ให้ N เป็นจำนวนเต็มบวก เราสามารถเขียน N ในรูปผลบวกของจำนวนเต็มบวกได้หลายแบบ

จงหาวิธีการเขียน N ในรูป $\sum_{i=1}^k x_i$ ที่ทำให้ $\prod_{i=1}^k x_i$ มีค่ามากที่สุด

วิธีทำ ให้ N เป็นจำนวนเต็มบวก

กรณี 1 ถ้า $N = 3k$ สำหรับจำนวนเต็ม k บางจำนวน แล้วการเขียน

$$N = 3 + 3 + 3 + \cdots + 3 \quad (k \text{ ตัว})$$

จะทำให้ $3k$ มีค่ามากที่สุด

กรณี 2 ถ้า $N = 3k + 1$ สำหรับจำนวนเต็ม k บางจำนวน แล้วการเขียน

$$N = 3 + 3 + 3 + \cdots + 3 + 2 + 2 \quad (k + 1 \text{ ตัว})$$

$$= 3 + 3 + 3 + \cdots + 3 + 4 \quad (k \text{ ตัว})$$

จะทำให้ $4 \cdot 3^{k-1}$ มีค่ามากที่สุด

กรณี 3 ถ้า $N = 3k + 2$ สำหรับจำนวนเต็ม k บางจำนวน แล้วการเขียน

$$N = 3 + 3 + 3 + \cdots + 3 + 2 \quad (k + 1 \text{ ตัว})$$

จะทำให้ $2 \cdot 3^k$ มีค่ามากที่สุด

เหตุผลที่ทำให้ได้ข้อสรุปข้างต้นนี้เพราะว่า

(i) จะต้องไม่มี 1 ปรากฏอยู่ในการบวก

เพราะว่า ถ้า $n \in \mathbb{Z}$ แล้ว $n = 1 + (n - 1)$ ทำให้ $1 \cdot (n - 1) < n$

(ii) ถ้ามี 4 ปรากฏอยู่ในการบวก ให้ใช้ 4 หรือ $2 + 2$

เพราะว่า $4 = 2 + 2$ ซึ่งทำให้ $2 \cdot 2 = 4$

(iii) ถ้ามี $x > 4$ ปรากฏในการบวก ให้ใช้ $3 + (x - 3)$ แทน

และถ้าพบว่า $x - 3 > 4$ ก็ใช้หลักการเดิมคือ $3 + (x - 3)$ แทน $x - 3$

เพราะว่า $3(x - 3) = 3x - 9 = 2x - (9 - x) > 2x - x = x$

เช่น $x = 5$; $5 = 3 + 2$ และทำให้ $3 \cdot 2 = 6 > 5$

$x = 7$; $7 = 3 + 4$ และทำให้ $3 \cdot 4 = 12 > 7$

$x = 11$; $11 = 3 + 8$

$= 3 + 3 + 3 + 2$ และทำให้ $3 \cdot 3 \cdot 3 \cdot 2 = 54 > 11$ □

แบบฝึกหัดเรื่อง การหารลงตัว

1. จงแสดงว่า $(3n + 4, 2n + 3) = 1$ สำหรับทุก ๆ จำนวนเต็ม n
2. จงแสดงว่า ผลคูณของจำนวนเต็ม n ที่เรียงต่อเนื่องกันจะหารด้วย $n!$ ลงตัว
3. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ 2^{n-1} หาร $n!$ ลงตัว
4. ให้ n เป็นจำนวนเต็มบวก จงแสดงว่า $10^n + 18n - 1$ หารด้วย 27 ลงตัว
5. จงตรวจสอบว่า “ n หารผลบวกของจำนวนเต็มบวก n จำนวนที่เรียงต่อเนื่องลงตัวเสมอ”
จริงหรือไม่ พร้อมทั้งให้เหตุผล
6. จงหาจำนวนเซตที่สร้างจากจำนวนเต็มบวกอย่างน้อย 2 จำนวนที่ผลรวมของสมาชิกในเซตเท่ากับ 100
7. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มบวกแล้ว $(2^a - 1, 2^b - 1) = 2^{(a, b)} - 1$
(ข้อเสนอแนะ $x^a - 1 = (x^b - 1)(x^{a-b} + x^{a-2b} + \dots + x^{a-bg}) + x^r - 1$ เมื่อ $a = gb + r$)
8. จงแสดงว่า $n^5 - 5n^3 + 4$ หารด้วย 120 ลงตัว สำหรับทุก ๆ จำนวนเต็มบวก n
9. มีจำนวนนับตั้งแต่ 1 ถึง 100 รวมทั้งสิ้นกี่จำนวนซึ่งเมื่อหารด้วย 6 แล้วเหลือเศษ 2
และเมื่อหารด้วย 14 แล้วเหลือเศษ 1
10. จงหาจำนวนของจำนวนเต็มบวกที่หาร $(30)^4$ ลงตัว
11. จำนวนเต็มบวก n ที่มากที่สุดที่ทำให้ 10^n หาร 1005! ลงตัว มีค่าเท่าใด
12. จงหาจำนวนของจำนวนเต็มตั้งแต่ 1 ถึง 100 ที่หารด้วย 2, 3, 4, 5 ลงตัว
13. ให้ n เป็นจำนวนเต็ม จงแสดงว่า $n^5 - n$ หารด้วย 30 ลงตัว
14. มีจำนวนเต็มทั้งหมดกี่จำนวนที่อยู่ระหว่าง 1 ถึง 2545 ที่ 3 หรือ 7 หารลงตัว
15. จงหาจำนวนเต็มบวก x, y, z ทั้งหมดที่ $x < y < z$ และ $(x, y) = (x, z) = (y, z) = 1$
รวมทั้ง z หาร $x + y$
16. จงแสดงว่า ถ้า $n \in \mathbb{N}$ แล้ว $[n, n + 2] = \frac{1}{2}n(n + 2)$
17. จงแสดงว่า ถ้า $n \in \mathbb{Z}$ แล้ว $4 \nmid (n^2 + 1)$
18. จงแสดงว่า ถ้า $(a, 4) = 2$ และ $(b, 4) = 2$ แล้ว $(a + b, 4) = 2$
19. ให้ $a, b, c \in \mathbb{Z}$ จงพิสูจน์ว่า $6 \mid (a + b + c)$ ก็ต่อเมื่อ $6 \mid (a^3 + b^3 + c^3)$
20. ให้ $n, k \in \mathbb{N}$ โดยที่ $n \geq 2$ จงพิสูจน์ว่า $(n - 1)^2 \mid (n^k - 1)$ ก็ต่อเมื่อ $(n - 1) \mid k$
21. จงพิจารณาว่าข้อความต่อไปนี้เป็นจริงหรือเท็จ ถ้าข้อความนั้นเป็นจริงจงพิสูจน์
แต่ถ้าข้อความนั้นเป็นเท็จจงยกตัวอย่างค้าน
 - (21.1) ถ้า $(a, b) = 1$ แล้ว $(2a + b, a + 2b) = 1$ หรือ 3
 - (21.2) ถ้า $(a, b) = 1$ แล้ว $(a + b, a^2 + b^2) = 1$ หรือ 2
 - (21.3) ถ้า $(a, b) = 1$ แล้ว $(a + b, a^2 - ab + b^2) = 1$ หรือ 3
22. จงแสดงว่า ถ้า $(3!)^n \mid (3n)!$ สำหรับทุกจำนวนเต็ม n ที่ $n \geq 0$

บทที่ 3

จำนวนเฉพาะ

จากคำกล่าวของเกาส์ที่ว่า “*Mathematics is the queen of science, and number theory is the queen of mathematics*” และในปี ค.ศ. 1993 โค (K. M. Koh) กล่าวอีกว่า “*The theory of prime numbers is the queen of number theory*” ดังนั้นในการศึกษาวิชาทฤษฎีจำนวน จำนวนเฉพาะ (prime number) เป็นเรื่องหนึ่งที่มีบทบาทและสำคัญยิ่งต่อการศึกษาเพราะว่าจำนวนเต็มบวกสามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ ซึ่งแสดงว่าโมโนภาพเกี่ยวกับจำนวนเฉพาะจะสอดคล้องกันอยู่ทุก ๆ หัวข้อที่เกี่ยวข้องกับจำนวนเต็ม รวมทั้งยังมีข้อคาดเดามากมายที่เกี่ยวข้องกับจำนวนเฉพาะ

ในการศึกษาเกี่ยวกับจำนวนเฉพาะนั้น เราจะมุ่งเน้นการศึกษาสมบัติของจำนวนเฉพาะตลอดจนการพิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนเฉพาะ นอกจากนี้เรายังมุ่งเน้นให้ผู้เรียนได้เห็นวิวัฒนาการและความสวยงามของจำนวนเฉพาะที่นักคณิตศาสตร์ในอดีตได้ทุ่มเทความรู้ ความสามารถ เพื่อสร้างงานทางทฤษฎีจำนวน และยังให้ผู้เรียนได้นำความรู้ที่ได้รับจากการศึกษาดังกล่าวไปใช้ในการแก้ปัญหาต่าง ๆ รวมทั้งหาแนวทางในการตอบข้อคาดเดาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเฉพาะ

3.1 นิยามของจำนวนเฉพาะ

อริสโตเติล (Aristotle 384 – 322 ปีก่อนคริสต์ศักราช) และยุคลิด ได้แยกจำนวนเต็มบวกออกจากกันเป็นสองกลุ่ม โดยกลุ่มแรกได้แก่ 2, 3, 5, 7, 11, 13, ... ซึ่งเรียกว่าจำนวนเฉพาะ และอีกกลุ่มหนึ่งได้แก่ 4, 6, 8, 9, 10, 12, 14, ... ซึ่งเรียกว่าจำนวนประกอบ บทนิยามต่อไปจะกล่าวถึงการพิจารณาว่าจำนวนเต็มใดเป็นจำนวนเฉพาะ

บทนิยาม 3.1.1 เราจะเรียกจำนวนเต็ม p ว่า จำนวนเฉพาะ (prime number) ก็ต่อเมื่อ $p \neq \pm 1$ และถ้า $a, b \in \mathbb{Z}$ และ $p = ab$ แล้ว $a = \pm 1$ หรือ $b = \pm 1$

จากบทนิยามของจำนวนเฉพาะ เราพบว่า

- (1) 2, -2 เป็นจำนวนเฉพาะที่เป็นจำนวนเต็มคู่ จำนวนเฉพาะอื่น ๆ จะเป็นจำนวนเต็มคี่
- (2) ถ้า p เป็นจำนวนเฉพาะ แล้ว $-p$ เป็นจำนวนเฉพาะ
- (3) ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ ถ้า $a \mid p$ แล้ว $a = \pm 1$ หรือ $a = \pm p$
- (4) ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ จะได้ $p \nmid a$ ก็ต่อเมื่อ $(p, a) = 1$
- (5) ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ จะได้ว่า $p \mid a$ ก็ต่อเมื่อ $(p, a) = |p|$
- (6) ถ้า p และ q เป็นจำนวนเฉพาะและ $p \mid q$ แล้ว $p = q$

ข้อตกลง เราอาจกล่าวถึงจำนวนเฉพาะที่เป็นบวกเท่านั้น นั่นคือ ต่อไปนี้เมื่อกล่าวถึงจำนวนเฉพาะ p เราจะหมายถึงจำนวนเฉพาะ $p \in \mathbb{N}$ เท่านั้น และจำนวนเต็มที่มีมากกว่า 1 ที่ไม่ใช่จำนวนเฉพาะเรียกว่า **จำนวนประกอบ** (*composite number*) กล่าวคือ

n เป็นจำนวนประกอบ ก็ต่อเมื่อ มี $a, b \in \mathbb{N}$ ซึ่ง $1 < a \leq b < n$ ที่ทำให้ $n = ab$

ตัวอย่าง 1 จำนวนเฉพาะ 20 ตัวแรกได้แก่ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71 □

ตัวอย่าง 2 จงหาจำนวนเฉพาะที่มีค่าระหว่าง 100 ถึง 300

วิธีทำ จำนวนเฉพาะทั้งหมดที่มีค่าอยู่ระหว่าง 100 ถึง 300 คือ

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 □

ตัวอย่าง 3 จงแสดงว่า มีจำนวนเฉพาะ p ซึ่ง $2^p - 1$ ไม่เป็นจำนวนเฉพาะ

บทพิสูจน์ มีจำนวนเฉพาะ $p = 11$ ที่ทำให้ $2^{11} - 1 = 2047 = 23 \cdot 89$

ดังนั้น $2^{11} - 1$ ไม่เป็นจำนวนเฉพาะ □

ตัวอย่าง 4 จงแสดงว่า ถ้า n เป็นจำนวนประกอบ แล้ว $2^n - 1$ เป็นจำนวนประกอบ

บทพิสูจน์ สมมติว่า n เป็นจำนวนประกอบ จะต้องแสดงว่า $2^n - 1$ เป็นจำนวนประกอบ

เนื่องจาก n เป็นจำนวนประกอบ แสดงว่า จะมี $a, b \in \mathbb{N} \setminus \{1\}$ ซึ่ง $n = ab$

จาก $x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \cdots + x + 1)$ เมื่อ $x, b \in \mathbb{N}$

$$\begin{aligned} \text{จะได้ว่า } 2^n - 1 &= 2^{ab} - 1 = (2^a)^b - 1 \\ &= (2^a - 1)[(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1] \\ &= MN \end{aligned}$$

เมื่อ $M = 2^a - 1$ และ $N = (2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1$

นั่นคือ $M, N \in \mathbb{N} \setminus \{1\}$

ดังนั้น เราจึงได้ $2^n - 1$ เป็นจำนวนประกอบ □

ปัญหา 5 จงแสดงว่า ถ้า $2^n - 1$ เป็นจำนวนเฉพาะ แล้ว n เป็นจำนวนเฉพาะ

ปัญหา 6 จงตอบคำถามต่อไปนี้

(6.1) 30,031 เป็นจำนวนเฉพาะหรือจำนวนประกอบ

(6.2) มีจำนวนเฉพาะ p ที่มีค่ามากที่สุดหรือไม่ เพราะเหตุใด

ทฤษฎีบท 3.1.2 ทุกจำนวนเต็ม $n > 1$ จะมีจำนวนเฉพาะ p ซึ่ง $p \mid n$

บทพิสูจน์ ให้ $S = \{n \in \mathbb{N} \mid n > 1 \text{ และไม่มีจำนวนเฉพาะที่ } p \mid n\}$

สมมติว่า $S \neq \emptyset$ โดยหลักการจัดอันดับดี

จะมี $n_0 \in S$ ซึ่ง n_0 เป็นจำนวนเต็มบวกที่มีค่าน้อยที่สุดใน S

ดังนั้น n_0 ไม่เป็นจำนวนเฉพาะ

แสดงว่าจะมี $d \in \mathbb{N}$ ซึ่ง $1 < d < n_0$ ที่ทำให้ $d \mid n_0$

นั่นคือ จะมีจำนวน p ซึ่ง $p \mid d$

ทำให้ได้ว่า $p \mid n_0$ ซึ่งขัดแย้งกับสมบัติของ $n_0 \in S$

ดังนั้น $S = \emptyset$

สรุปได้ว่า ทุก ๆ จำนวนเต็ม $n > 1$ จะมีจำนวนเฉพาะ p ซึ่ง $p \mid n$ ■

ทฤษฎีบท 3.1.3 ให้ $a, b \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ จะได้ว่า

ถ้า $p \mid ab$ แล้ว $p \mid a$ หรือ $p \mid b$

บทพิสูจน์ ให้ $a, b \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ สมมติว่า $p \mid ab$ และ $p \nmid a$

จะได้ว่า $p \mid ab$ และ $(p, a) = 1$

โดยทฤษฎีบท 2.4.8 ข้อ 3. จะได้ว่า $p \mid b$ ■

ทฤษฎีบท 3.1.4 ให้ $a_1, a_2, \dots, a_n \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ จะได้ว่า

ถ้า $p \mid a_1 a_2 \cdots a_n$ แล้วจะมี a_i ที่ $1 \leq i \leq n$ ซึ่ง $p \mid a_i$

บทพิสูจน์ เราจะพิสูจน์ทฤษฎีบทนี้โดยใช้หลักการอุปนัยเชิงคณิตศาสตร์

(i) ถ้า $n = 1$ เห็นได้ชัดว่าทฤษฎีบทนี้เป็นจริง

ให้ $p \mid a_1 a_2$ จากทฤษฎีบท 3.1.2 จะได้ว่า $p \mid a_1$ หรือ $p \mid a_2$

ดังนั้น ทฤษฎีบทนี้เป็นจริงเมื่อ $n = 2$

(ii) สมมติว่าทฤษฎีบทนี้เป็นจริงเมื่อ $n = k$

จะต้องแสดงว่าทฤษฎีบทนี้เป็นจริงเมื่อ $n = k + 1$

ให้ $p \mid a_1 a_2 \cdots a_k a_{k+1}$ โดยทฤษฎีบท 3.1.3 จะได้ว่า $p \mid a_1 a_2 \cdots a_k$ หรือ $p \mid a_{k+1}$

กรณี 1 ถ้า $p \mid a_{k+1}$ จะได้ว่ามี $i = k+1$ ซึ่ง $p \mid a_i$

กรณี 2 ถ้า $p \mid a_1 a_2 \cdots a_k$ จากสมมติฐานจะได้ว่ามี a_i ที่ $1 \leq i \leq k$ ซึ่ง $p \mid a_i$ ดังนั้นจะมี a_i ที่ $1 \leq i \leq k+1$ ซึ่ง $p \mid a_i$

นั่นคือทฤษฎีบทนี้เป็นจริงเมื่อ $n = k+1$

จาก (i) และ (ii) จะได้ว่า ถ้า $p \mid a_1 a_2 \cdots a_n$ แล้วจะมี a_i ที่ $1 \leq i \leq n$ ซึ่ง $p \mid a_i$ เป็นจริง สำหรับทุกจำนวนเต็มบวก n ■

จาก $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ และพิจารณาลำดับของจำนวนเต็มบวกที่เรียงต่อเนื่องกันต่อไปนี้

ลำดับ 14, 15, 16 เป็นลำดับของจำนวนประกอบ 3 จำนวนเรียงกัน

ลำดับ 24, 25, 26, 27, 28 เป็นลำดับของจำนวนประกอบ 5 จำนวนเรียงกัน

ลำดับ 120, 121, 122, 123, 124, 125, 126 เป็นลำดับของจำนวนประกอบ 7 จำนวนเรียงกัน

ถ้าเราจะลองหาลำดับของจำนวนประกอบ 10 จำนวนเรียงกันหรือจำนวนประกอบ 20 จำนวนเรียงกัน จะหาได้หรือไม่ คำตอบก็คือหาได้ ซึ่งเราสามารถค้นหาได้จากวิธีการที่จะกล่าวในตัวอย่างต่อไป

ตัวอย่าง 7 ให้ $n \in \mathbb{N}$ จงแสดงว่ามีจำนวนประกอบเรียงต่อเนื่องกัน n จำนวน

วิธีทำ สำหรับ $i = 2, 3, 4, \dots, n+1$ จำนวน $(n+1)! + i$ เป็นจำนวนประกอบ

ดังนั้น ลำดับ $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$ เป็นลำดับของจำนวนประกอบ n จำนวนเรียงต่อเนื่องกัน ■

จากตัวอย่าง 7 ข้างต้นทำให้เรามีความรู้สึกว่า เมื่อเลือกจำนวนเต็มบวกที่มีค่ามาก ๆ โอกาสที่จำนวนนั้นจะเป็นจำนวนเฉพาะจะมีโอกาสน้อยมากและยังทำให้เราสงสัยต่อไปว่า จะมีจำนวนเฉพาะที่มีค่ามากที่สุดใดใน $\mathbb{N}$ หรือไม่ซึ่งคำตอบของปัญหานี้จะกล่าวถึงในบทที่ 4 ต่อไป

บทนิยาม 3.1.5 จำนวนเต็ม $a_1, a_2, a_3, \dots, a_n$ จะเรียกว่าเป็น **จำนวนเฉพาะสัมพัทธ์** (relatively prime numbers) ก็ต่อเมื่อ $(a_1, a_2, a_3, \dots, a_n) = 1$ และถ้าทุก i, j ที่ $i \neq j$, $(a_i, a_j) = 1$ แล้วเราจะกล่าวว่า $a_1, a_2, a_3, \dots, a_n$ เป็น **จำนวนเฉพาะสัมพัทธ์ทุกคู่** (pairwise relatively prime numbers)

ตัวอย่าง 8 (8.1) $(53, 122, 471) = 1$

(8.2) $(111, 1111, 11111) = 1$

(8.3) $(101, 10101, 1010101) = 1$ ■

ทฤษฎีบท 3.1.6 สำหรับจำนวนเต็ม $a_1, a_2, a_3, \dots, a_n$ ใด ๆ ถ้า $a_1, a_2, a_3, \dots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แล้ว $a_1, a_2, a_3, \dots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์

บทพิสูจน์ ให้ $a_1, a_2, a_3, \dots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ และให้ $d = (a_1, a_2, a_3, \dots, a_n)$ จะได้ว่า $d \mid a_1$ และ $d \mid a_2$ โดยบทแทรก 2.4.3 จะได้ว่า $d \mid (a_1, a_2)$ เพราะว่า $(a_1, a_2) = 1$ จะได้ $d = 1$ นั่นคือ $a_1, a_2, a_3, \dots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ ■

ปัญหา 9 จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็มบวก n ใด ๆ จะได้ว่า $n! + 1$ และ $(n + 1)! + 1$ เป็นจำนวนเฉพาะสัมพัทธ์

โจทย์ปัญหา 3.1

1. จงหาจำนวนเฉพาะทั้งหมดหารที่ $100!$ ลงตัว
2. จงตรวจสอบว่ามีจำนวนเฉพาะที่อยู่ระหว่าง 701 และ 1009 หรือไม่
3. ถ้า $p \geq q \geq 5$ และ p, q เป็นจำนวนเฉพาะทั้งคู่ จงแสดงว่า $24 \mid (p^2 - q^2)$
4. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะที่ $p \geq 5$ แล้ว $p^2 + 2$ เป็นจำนวนประกอบ
5. ให้ p เป็นจำนวนเฉพาะและ $p \mid a^n$ จงแสดงว่า $p^n \mid a^n$
6. จงตรวจว่าจำนวนเต็มที่อยู่ในรูป $8^n + 1$, $n \geq 1$ เป็นจำนวนประกอบเมื่อใด (ข้อเสนอแนะ $(2^n + 1) \mid (2^{3n} + 1)$)
7. ให้ $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}$ โดยที่ $n \geq 2$ จงพิสูจน์ว่า ถ้า $a_1, a_2, a_3, \dots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่แล้ว $[a_1, a_2, a_3, \dots, a_n] = a_1 a_2 a_3 \cdots a_n$

3.2 ทฤษฎีบทหลักมูลของเลขคณิต

ทฤษฎีบทต่อไปนี้เป็นทฤษฎีบทที่สำคัญอย่างยิ่งต่อการนำไปใช้ ในการศึกษาทฤษฎีบทต่าง ๆ ซึ่งยุคผลิตเขียนไว้ในหนังสือ Euclid's Elements Book IX : Proposition 14

ทฤษฎีบท 3.2 ทฤษฎีบทหลักมูลของเลขคณิต (The Fundamental Theorem of Arithmetic)

ให้ $n \in \mathbb{Z}$ และ $n > 1$ จะได้ว่า n สามารถเขียนได้ในรูป

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

โดยที่ $p_1, p_2, p_3, \dots, p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < \dots < p_k$

และ $a_i \in \mathbb{N}$ สำหรับทุก $i = 1, 2, 3, \dots, k$

และจะเขียน n ในรูปดังกล่าวได้เพียงแบบเดียวเท่านั้น

บทพิสูจน์ (i) ให้ $n \in \mathbb{Z}$ ซึ่ง $n > 1$

จะพิสูจน์ว่า n สามารถเขียนได้ในรูปของผลคูณของจำนวนเฉพาะ

กรณี 1 ถ้า n เป็นจำนวนเฉพาะ

จะได้ว่าการเขียน $n = n$ สามารถเขียนได้เพียงแบบเดียว

กรณี 2 ถ้า n เป็นจำนวนประกอบ จะได้ว่ามี $a, b \in \mathbb{N}$ ซึ่ง

$$1 < a \leq b < n \text{ ที่ทำให้ } n = ab$$

โดยหลักอุปนัยเชิงคณิตศาสตร์ที่ 2 ถ้าสมมติว่า a และ b สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ

ดังนั้น $n = ab$ ก็สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ

ภายใต้การจัดลำดับการคูณที่เหมาะสม จะได้ว่า n สามารถเขียนได้ในรูป

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

โดย p_i เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < \cdots < p_k$ และ $a_i \in \mathbb{N}$

สำหรับทุก $i = 1, 2, 3, \dots, k$

(ii) ต่อไปจะแสดงว่า การเขียน n ในรูปดังกล่าวจะเขียนได้เพียงแบบเดียว

สมมติให้ $n = p_1 p_2 \cdots p_r$ โดยที่ $p_1 \leq p_2 \leq \cdots \leq p_r$

และ $n = q_1 q_2 \cdots q_s$ โดยที่ $q_1 \leq q_2 \leq \cdots \leq q_s$

ดังนั้น $p_1 \mid q_1 q_2 \cdots q_s$

จากทฤษฎีบท 3.1.4 จะได้ว่า $p_1 \mid q_i$ สำหรับ i บางตัว

นั่นคือ $p_1 = q_i$ แสดงว่า $p_1 \geq q_1$

ในทำนองเดียวกันสามารถพิสูจน์ได้ว่า $q_1 \geq p_1$ แสดงว่า $p_1 = q_1$

จาก $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ และ $p_1 = q_1$

โดยสมบัติการตัดออกสำหรับการคูณ จะได้ว่า $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$

พิสูจน์ในทำนองจะได้ว่า $p_2 = q_2, p_3 = q_3, p_4 = q_4, \dots$ ตามลำดับ

ถ้า $r < s$ จะได้ว่า $1 = q_{r+1} q_{r+2} \cdots q_s$ ซึ่งเป็นไปไม่ได้

เพราะว่า $q_{r+1}, q_{r+2}, \dots, q_s > 1$

ถ้า $r > s$ จะได้ว่า $1 = p_{s+1} p_{s+2} \cdots p_r$ ซึ่งเป็นไปไม่ได้

เพราะว่า $p_{s+1}, p_{s+2}, \dots, p_r > 1$

ดังนั้น $r = s$ นั่นคือ $p_1 = q_1, p_2 = q_2, \dots, p_r = q_s = q_r$

จาก (i) และ (ii) สรุปได้ว่า n สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะได้แบบเดียว ■

ข้อตกลง เราจะเรียกการเขียน $n > 1$ ในรูป

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

โดยที่ $p_1, p_2, p_3, \dots, p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < \cdots < p_k$ และ $a_i \in \mathbb{N}$

สำหรับทุก $i = 1, 2, 3, \dots, k$ ว่าเป็นการเขียนในรูปแบบบัญญัติ (canonical form) ของ n

จากทฤษฎีบท 3.2.1 จะได้ว่า

(1) ทุกจำนวนเต็ม $n > 1$ สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะได้เพียงแบบเดียวเท่านั้น

(2) ให้ $m = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$ และ $n = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_k^{b_k}$

โดยที่แต่ละจำนวนเต็ม a_i, b_i ซึ่ง $a_i \geq 0$ และ $b_i \geq 0$ โดยที่ไม่เป็นศูนย์พร้อมกัน จะได้ว่า

$$(m, n) = p_1^{d_1} p_2^{d_2} p_3^{d_3} \cdots p_k^{d_k}$$

$$\text{และ } [m, n] = p_1^{c_1} p_2^{c_2} p_3^{c_3} \cdots p_k^{c_k}$$

$$\text{เมื่อทุก } i, d_i = \min\{a_i, b_i\} \text{ และ } c_i = \max\{a_i, b_i\}$$

จากข้อสังเกตข้างต้น เราสามารถสรุปได้ว่า $(m, n)[m, n] = mn$

ทฤษฎีบท 3.2 นี้ เป็นเครื่องมือที่สำคัญมากในการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็ม เพราะเราสามารถทำได้โดยการพิจารณาว่าจำนวนเต็มนั้นเป็นจำนวนเฉพาะหรือผลคูณของจำนวนเฉพาะ ซึ่งทำให้ง่ายต่อการพิจารณา ดังตัวอย่างต่อไปนี้

ตัวอย่าง 1 $48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$

$$15750 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 5 \cdot 7 = 2 \cdot 3^2 \cdot 5^3 \cdot 7$$

$$846846 = 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 47$$

□

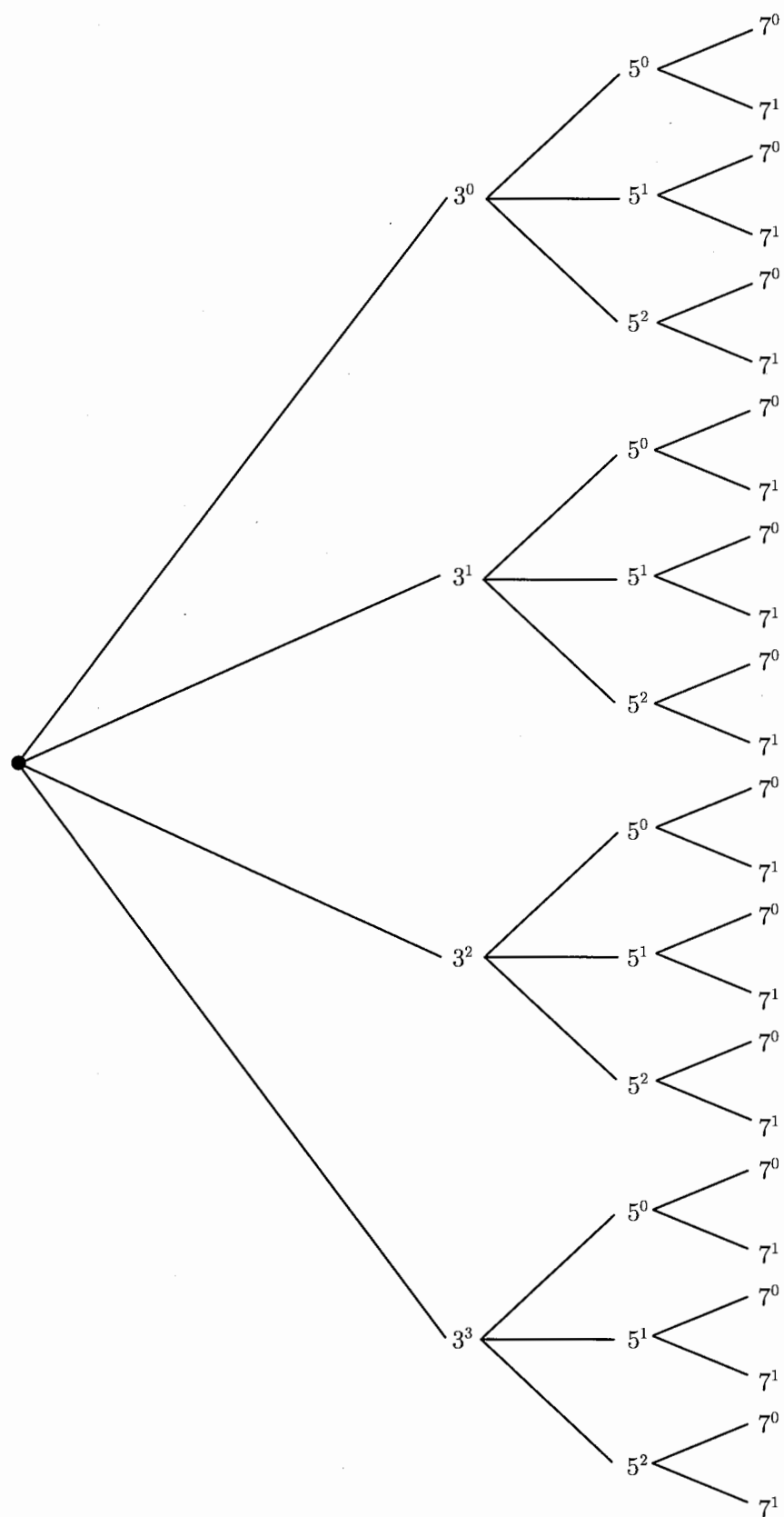
ตัวอย่าง 2 จงหาจำนวนตัวหารทั้งหมดของ 4725

วิธีทำ เนื่องจาก $4725 = 3^3 \cdot 5^2 \cdot 7$ จะได้ว่าตัวหารของ 4725 คือ

$$1, 3, 3^2, 3^3, 5, 5^2, 7, 3 \cdot 5, 3 \cdot 5^2, 3 \cdot 5 \cdot 7, 3 \cdot 5^2 \cdot 7, 3^2 \cdot 5, 3^2 \cdot 5^2, 3^2 \cdot 5 \cdot 7, \\ 3^2 \cdot 5^2 \cdot 7, 3^3 \cdot 5, 3^3 \cdot 5^2, 3^3 \cdot 5 \cdot 7, 3^3 \cdot 5^2 \cdot 7, 5 \cdot 7, 5^2 \cdot 7, 3 \cdot 7, 3^2 \cdot 7, 3^3 \cdot 7$$

ดังนั้น จำนวนตัวหารทั้งหมดของ 4725 คือ 24

หรือเราสามารถหาจำนวนตัวหารทั้งหมดของ $3^3 \cdot 5^2 \cdot 7$ ได้โดยพิจารณาจากแผนภาพต้นไม้ต่อไปนี้



ปัญหา 3 จงหาจำนวนตัวหารทั้งหมดของ 20!

ปัญหา 4 จงหาตัวหารร่วมมากและตัวคูณร่วมน้อยของ 31752 และ 4725

โจทย์ปัญหา 3.2

1. จงหา (308, 1176) และ [308, 1176]
2. จงตรวจสอบว่ามีจำนวนเฉพาะที่เขียนในรูป $6k + 3$ อยู่เป็นจำนวนอนันต์หรือไม่
3. จงหาจำนวนตัวหารทั้งหมดของ 846876
4. กำหนดให้ a, b และ c เป็นจำนวนเต็มบวก จงพิสูจน์ว่า

$$(4.1) \quad ([a, b], c) = [(a, b), (a, c)]$$

$$(4.2) \quad [(a, b), c] = ([a, b], [a, c])$$
 (ข้อเสนอแนะ ใช้ $\min\{\max\{x, y\}, z\} = \max\{\min\{x, z\}, \min\{y, z\}\}$)
5. กำหนดให้ $a_1, a_2, \dots, a_n$ และ b เป็นจำนวนเต็มบวก จงพิสูจน์ว่า

$$(5.1) \quad ([a_1, a_2, \dots, a_n], b) = [(a_1, b), (a_2, b), \dots, (a_n, b)]$$

$$(5.2) \quad [(a_1, a_2, \dots, a_n), b] = ([a_1, b], [a_2, b], \dots, [a_n, b])$$

3.3 การค้นหาจำนวนเฉพาะ

ถ้ากำหนดให้ n เป็นจำนวนเต็มบวก การที่จะตรวจสอบว่า n เป็นจำนวนเฉพาะหรือไม่ วิธีการหนึ่งก็คือ การหาจำนวนเต็มบวกที่เป็นตัวหารที่น้อยกว่า n ถ้าไม่มีจำนวนใดหาร n ลงตัว ก็แสดงว่า n เป็นจำนวนเฉพาะ แต่วิธีการนี้จะใช้ประโยชน์ได้อย่างมีประสิทธิภาพก็ต่อเมื่อ n มีค่าไม่มากนัก เราสามารถลดขั้นตอนการตรวจสอบการเป็นจำนวนเฉพาะของ n ได้โดยทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.3 ถ้า n เป็นจำนวนประกอบ แล้วจะมีจำนวนเฉพาะ p ที่ $p \leq \sqrt{n}$ และ $p \mid n$
(หรือ ถ้าไม่มีจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$ และ $p \mid n$ แล้ว n จะเป็นจำนวนเฉพาะ)

บทพิสูจน์ ให้ n เป็นจำนวนประกอบ จะได้ว่ามี $a, b \in \mathbb{N}$ ซึ่ง $1 < a \leq b < n$ ที่ทำให้ $n = ab$

ดังนั้น $a \mid n$ และ $b \mid n$ แสดงว่า $1 < a^2 \leq ab = n$

ดังนั้น $a \leq \sqrt{n}$

โดยทฤษฎีบท 3.1.2 จะมีจำนวนเฉพาะ p ซึ่ง $p \mid a$

ทำให้ได้ว่า $p \mid n$ และ $p \leq \sqrt{n}$ ■

ตัวอย่าง 1 จงตรวจสอบว่า 401 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เนื่องจาก $\sqrt{401} < 21$ จากทฤษฎีบท 3.3 ถ้า 401 เป็นจำนวนประกอบแล้วจะมีจำนวนเฉพาะ p ที่ $p < 21$ และ p หาร 401 ลงตัว แต่จากการตรวจสอบจำนวนเฉพาะทั้งหมดที่น้อยกว่า 21 คือ 2, 3,

5, 7, 11, 13, 17, 19 ไม่มีจำนวนใดเลยที่หาร 401 ลงตัว

ดังนั้นสรุปได้ว่า 401 เป็นจำนวนเฉพาะ

□

ตัวอย่าง 2 จงตรวจสอบว่า 2093 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เนื่องจาก $\sqrt{2093} < 46$ ดังนั้นจำนวนเฉพาะที่น้อยกว่า 46 คือ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 แต่จากการตรวจสอบพบว่า มี 7 หาร 2093 ได้ลงตัว

ดังนั้น $2093 = 7 \cdot 299$ เป็นจำนวนประกอบ

□

หมายเหตุ วิธีการดังกล่าวที่ใช้ตรวจสอบจำนวนเฉพาะนี้เรียกว่า **ตะแกรงเอราโตสเทเนส** (The Sieve of Eratosthenes) และวิธีการดังกล่าวนี้ยังนำไปใช้ในการหาจำนวนเฉพาะทั้งหมดที่น้อยกว่าจำนวนเต็มบวก n ที่กำหนดให้ได้ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3 จงหาจำนวนเฉพาะทั้งหมดที่น้อยกว่า 50

วิธีทำ (1) จำนวนเฉพาะทั้งหมดที่น้อยกว่า $\sqrt{50}$ คือ 2, 3, 5, 7

(2) เขียนจำนวนเต็มตั้งแต่ 1 ถึง 50 ลงไปในกระดาน

(3) วงกลม 2 แล้วตัดจำนวนทุกจำนวนที่ 2 หารลงตัว

(4) วงกลม 3 แล้วตัดจำนวนที่เหลือจาก (3) ทุกจำนวนที่ 3 หารลงตัว

ทำเช่นนี้ต่อไปจนถึงจำนวนเฉพาะ 7 และจำนวนที่เหลือจะเป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่า 50 ยกเว้น 1 กำจัดจำนวนเต็มที่หารด้วย 2, 3, 5 และ 7 ลงตัวด้วย /, \, // และ \\\ ตามลำดับ

1	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

ดังนั้น จำนวนเฉพาะที่น้อยกว่า 50 คือ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 และ 47

□

ตัวอย่าง 4 จงหาจำนวนเฉพาะที่สามารถเขียนอยู่ในรูป $3n + 1$ ที่มีค่าน้อยกว่า 50

วิธีทำ

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3n + 1$	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46	49

ดังนั้น จำนวนเฉพาะทั้งหมดที่สามารถเขียนได้ในรูป $3n + 1$ ที่น้อยกว่า 50 คือ 7, 13, 19, 31, 37 และ 43

□

โจทย์ปัญหา 3.3

1. (1.1) จงหาจำนวนเฉพาะที่สามารถเขียนได้ในรูป $4k + 3$, $k \geq 0$ มา 20 จำนวน
(1.2) จงหาจำนวนเฉพาะที่สามารถเขียนได้ในรูป $6k + 5$, $k \geq 0$ มา 20 จำนวน
(1.3) จงหาจำนวนเฉพาะที่สามารถเขียนได้ในรูป $k^2 + k + 41$, $k \geq 0$ มา 20 จำนวน
(1.4) จงหาจำนวนเฉพาะที่สามารถเขียนได้ในรูป $k^2 - 79k + 160$, $k \geq 0$ มา 20 จำนวน
2. เราสามารถหาจำนวนเฉพาะที่เขียนอยู่ในรูป $k^2 + k + 41$ ให้ติดต่อกัน 50 จำนวนได้หรือไม่
3. เราสามารถหาจำนวนเฉพาะที่เขียนอยู่ในรูป $k^2 + k + 17$ ให้ติดต่อกัน 100 จำนวนได้หรือไม่
4. จงตรวจสอบว่า $2^{19} - 1$ เป็นจำนวนเฉพาะหรือจำนวนประกอบ
5. จงหาจำนวนเฉพาะ p ซึ่ง $p < 100$ และ $p + 2$ เป็นจำนวนเฉพาะ
6. จงเขียนจำนวนเต็มคู่ n ซึ่ง $10 \leq n \leq 100$ ในรูปผลบวกของจำนวนเฉพาะ 2 จำนวน
7. มีจำนวนเต็ม n ซึ่ง $6 < n < 20$ จำนวนใดบ้างที่ทำให้ $n^2 + 1$ เป็นจำนวนเฉพาะ
8. จงหาจำนวนเฉพาะ 2 จำนวนที่มากกว่า 11 ซึ่งสามารถเขียนได้ในรูป $2^n - 1$
9. จงหาจำนวนเต็มที่น้อยที่สุดที่มากกว่า 17 ซึ่งสามารถเขียนได้ในรูป $2^n + 1$
10. จงแสดงว่า จำนวนเฉพาะที่เขียนในรูป $8n + 5$ มีจำนวนอนันต์

โจทย์ปัญหาเสริมเรื่อง จำนวนเฉพาะ

ปัญหา 1 จงหาจำนวนเฉพาะทั้งหมดที่น้อยกว่า 1000

วิธีทำ	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	409	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	857	859	863	877	881	883	887	907	911
	919	929	937	941	947	953	967	971	977	983	991	997

□

ปัญหา 2 จงตรวจสอบว่า จำนวน $25! + 1$ และ $25! + 29$ เป็นจำนวนเฉพาะหรือจำนวนประกอบ

วิธีทำ เป็นการง่ายที่จะแสดงว่า $25! + 2$, $25! + 3$, $25! + 4$, ..., $25! + 27$, $25! + 28$ เป็นจำนวนประกอบ ที่เรียงต่อเนื่องกัน 27 จำนวน แต่ไม่ยากนักที่จะตรวจสอบว่า $25! + 1$ และ $25! + 29$ เป็นจำนวนเฉพาะ หรือจำนวนประกอบ จากการใช้เครื่องคำนวณเราพบว่า

$$25! + 1 = (401)(38681321803817920159601)$$

$$\text{และ } 25! + 29 = (48511549)(319742625479367521)$$

ดังนั้น $25! + 1$ และ $25! + 29$ เป็นจำนวนประกอบ

□

ปัญหา 3 จงตรวจสอบว่ามีจำนวนเฉพาะปรากฏอยู่ในลำดับต่อไปนี้หรือไม่

$$10001, 100010001, 1000100010001, \dots$$

วิธีทำ จากลำดับข้างต้น เราสามารถเขียนได้เป็น

$$10^4 + 1, 10^8 + 10^4 + 1, \dots, 10^{4k} + 10^{4(k-1)} + \dots + 10^4 + 1, \dots$$

พิจารณาพจน์ที่ k ของลำดับ เราพบว่า

$$\begin{aligned} 10^{4k} + 10^{4(k-1)} + \dots + 10^4 + 1 &= \frac{10^{4(k+1)} - 1}{10^4 - 1} \\ &= \frac{10^{2(k+1)} + 1}{10^2 + 1} \cdot \frac{10^{2(k+1)} - 1}{10^2 - 1} \\ &= \frac{(10^{2k+2} + 1)(10^{2k} + 10^{2k-2} + \dots + 10^2 + 1)}{101} \end{aligned}$$

เนื่องจาก 101 เป็นจำนวนเฉพาะ จะได้ว่า

$$101 \mid (10^{2k+2} + 1) \quad \text{หรือ} \quad 101 \mid (10^{2k} + 10^{2k-2} + \dots + 10^2 + 1)$$

ถ้า $k > 1$ แล้ว $10^{2k+2} + 1$ และ $10^{2k} + 10^{2k-2} + \dots + 10^2 + 1$ จะมีค่ามากกว่า 101

นั่นคือ $10^{4k} + 10^{4(k-1)} + \dots + 10^4 + 1$ เป็นจำนวนประกอบ

ถ้า $k = 1$ แล้ว $10^4 + 1 = 137 \cdot 73$ ดังนั้น 10001 เป็นจำนวนประกอบ

ดังนั้น ในลำดับ 10001, 100010001, 1000100010001, ... ไม่มีจำนวนเฉพาะปรากฏอยู่เลย $\square$

ปัญหา 4 จากการคำนวณ เราพบว่า $2 + 1 = 3$, $2^2 + 1 = 5$, $2^4 + 1 = 17$ และ 3, 5, 17 เป็นจำนวนเฉพาะสัมพัทธ์กันทั้งคู่ จงตรวจสอบว่าจำนวนเต็มที่อยู่ในลำดับ

$$2 + 1, 2^2 + 1, 2^4 + 1, 2^8 + 1, \dots, 2^{2^n} + 1, \dots$$

เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่หรือไม่

วิธีทำ เขียนจำนวนเต็มแต่ละพจน์ของลำดับที่อยู่ในรูป $2^{2^n} + 1$ เป็น $(2^{2^n} - 1) + 2$

$$\text{เนื่องจาก } 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) \quad \text{ในทำนองเดียวกัน}$$

$$\begin{aligned} 2^{2^{n-1}} - 1 &= (2^{2^{n-2}} + 1)(2^{2^{n-2}} - 1) \\ &= (2^{2^{n-2}} + 1)(2^{2^{n-3}} + 1) \dots (2^{2^m} + 1) \dots (2^2 + 1)(2 + 1)(2 - 1) \end{aligned}$$

$$\text{ดังนั้น } 2^{2^n} + 1 = [(2^{2^{n-1}} + 1)(2^{2^{n-2}} + 1) \dots (2^{2^m} + 1) \dots (2^2 + 1)(2 + 1)(2 - 1)] + 2$$

สมมติว่า $(2^{2^n} + 1, 2^{2^m} + 1) = d$ เมื่อ $m < n$

แสดงว่า $d \mid (2^{2^n} + 1)$ และ $d \mid (2^{2^m} + 1)$ ซึ่งทำให้ได้ว่า $d \mid 2$

จะได้ว่า $d = 1$ หรือ 2 เนื่องจาก $2^{2^n} + 1$ และ $2^{2^m} + 1$ เป็นจำนวนเต็มคี่เสมอ

$$\text{ดังนั้น } (2^{2^n} + 1, 2^{2^m} + 1) = 1$$

นั่นคือ จำนวนเต็มที่อยู่ในรูป $2^{2^n} + 1$, $2^{2^m} + 1$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่

สำหรับจำนวนเต็มบวก m และ n ซึ่ง $m \neq n$ $\square$

ปัญหา 5 จงแสดงว่า ถ้า n เป็นจำนวนเฉพาะ แล้ว $n \mid (2^n - 2)$

ปัญหา 6 จงแสดงว่า $2^{13} - 1$ เป็นจำนวนเฉพาะ และ $2^{23} - 1$ ไม่ใช่จำนวนเฉพาะ

ปัญหา 7 จงตรวจสอบว่า 8009 เป็นจำนวนเฉพาะหรือจำนวนประกอบ

วิธีทำ เนื่องจาก $\sqrt{8009} < 90$

จะได้ว่าจำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ 90 ได้แก่ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83 และ 89

ซึ่งพบว่าจำนวนเฉพาะตั้งแต่ 2 ถึง 89 ไม่มีจำนวนใดหาร 8009 ลงตัว

ดังนั้น 8009 เป็นจำนวนเฉพาะ □

ปัญหา 8 ให้ $p \nmid n$ สำหรับจำนวนเฉพาะ p ทั้งหมดซึ่ง $p \leq \sqrt[3]{n}$

จงแสดงว่าจำนวนเต็มบวก $n > 1$ จะเป็นจำนวนเฉพาะหรือเขียนอยู่ในรูปผลคูณของจำนวนเฉพาะ 2 จำนวน

ปัญหา 9 ถ้า p และ $p^2 + 8$ เป็นจำนวนเฉพาะทั้งคู่ แล้วจงแสดงว่า $p^3 + 4$ เป็นจำนวนเฉพาะ

ปัญหา 10 จงตรวจสอบว่าข้อความต่อไปนี้เป็นจริงหรือเท็จ

(10.1) ถ้า p เป็นจำนวนเฉพาะและ $p \mid (a^2 + b^2)$ และ $p \mid (b^2 + c^2)$ แล้ว $p \mid (a^2 - c^2)$

(10.2) ถ้า p เป็นจำนวนเฉพาะและ $p \mid (a^2 + b^2)$ และ $p \mid (b^2 + c^2)$ แล้ว $p \mid (a^2 + c^2)$

ปัญหา 11 จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มบวก แล้ว $p \mid (a^p - a)$

ปัญหา 12 จงตรวจสอบว่า $4^{545} + 545^4$ เป็นจำนวนเฉพาะหรือจำนวนประกอบ

ปัญหา 13 จงหาจำนวนเฉพาะทั้งหมดที่เขียนอยู่ในรูป $n^n + 1$ เมื่อ $n = 1, 2, 3, \dots, 15$

ปัญหา 14 ให้ $g(n) = 103n^2 - 3945n + 34381$ จงแสดงว่า $g(n)$ เป็นจำนวนเฉพาะ ทุก ๆ n เมื่อ $0 \leq n \leq 44$

ปัญหา 15 จงแสดงว่า ถ้า $n > 0$ และ $n^3 + 1$ เป็นจำนวนเฉพาะ แล้ว $n = 1$

ปัญหา 16 ให้ $(a, b) = p$ เมื่อ p เป็นจำนวนเฉพาะ จงหา (a^2, b^2) , (a^2, b) และ (a^3, b^2)

ปัญหา 17 ให้ p เป็นจำนวนเฉพาะซึ่ง $p > 5$ จงแสดงว่า $10 \mid (p^2 - 1)$ หรือ $10 \mid (p^2 + 1)$

ปัญหา 18 ให้ $p = 2^k - 1$ เป็นจำนวนเฉพาะ จงแสดงว่า $k = 2$ หรือ k เป็นจำนวนเต็มคี่ซึ่ง $k > 1$

แบบฝึกหัดเรื่อง จำนวนเฉพาะ

1. กำหนดลำดับของจำนวนเต็มบวก
101, 10101, 1010101, ...
จงตรวจสอบว่ามีสมาชิกใดบ้างในลำดับข้างต้นที่เป็นจำนวนเฉพาะ
2. จงหาจำนวนเต็ม n ทั้งหมดที่ทำให้ $n^4 + 4$ เป็นจำนวนประกอบ
3. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะที่ $p, p+2, p+4$ เป็นจำนวนเฉพาะ แล้ว $p = 3$
4. ให้ p เป็นจำนวนเฉพาะซึ่ง $p > 3$ จงแสดงว่า $p^2 - 1$ หารด้วย 24 ลงตัว
5. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $n^4 + 4^n$ เป็นจำนวนเฉพาะ
6. จงหาจำนวนเฉพาะ p ทั้งหมดที่ทำให้ $17p + 1$ เป็นกำลังสองสมบูรณ์
7. จงหาจำนวนเฉพาะ p และ $q = p + 2$ ทั้งหมดที่ทำให้ $pq - 2$ เป็นจำนวนเฉพาะ
8. ในการเขียน 1000000! ในรูปของจำนวนเต็ม จะมี 0 ลงท้ายเรียงต่อเนื่องกันกี่ตัว
(ข้อเสนอนี้ ให้เขียน 1000000! ในรูป $M \cdot 10^k$ โดยที่ $10 \nmid M$)
9. ให้ $n = p^r$, p เป็นจำนวนเฉพาะ
จงหาจำนวนของจำนวนเต็ม k ซึ่ง $1 \leq k < n$ และ $(n, k) = 1$
10. จงหาจำนวนเต็มบวก n ที่มีค่าน้อยที่สุดที่ทำให้ $n^2 + n + 17$ เป็นจำนวนประกอบ
11. จงแสดงว่ามีจำนวนเฉพาะ p เพียงตัวเดียวเท่านั้นที่เขียนอยู่ในรูป $p = n^3 - 1$
สำหรับจำนวนเต็ม n บางจำนวน
12. จงแสดงว่า ถ้า p และ $p+2$ เป็นจำนวนเฉพาะทั้งคู่ที่ $p > 3$ แล้วผลบวกของ p และ $p+2$ หารด้วย 12 ลงตัว
13. ถ้า p และ $p^3 + 3$ เป็นจำนวนเฉพาะ จงแสดงว่า $p^3 + 4$ เป็นจำนวนประกอบ
14. ให้ n เป็นจำนวนเต็มบวกที่มากกว่า 2 จงแสดงว่า ถ้า $2^n - 1$ หรือ $2^n + 1$ ตัวใดตัวหนึ่งเป็นจำนวนเฉพาะแล้วอีกตัวหนึ่งจะเป็นจำนวนประกอบ
15. ถ้าจำนวนเต็มบวก $n > 1$ ซึ่งไม่เขียนอยู่ในรูป $6k + 3$ จงแสดงว่า $n^2 + 2^n$ เป็นจำนวนประกอบ
16. ให้ $n \in \mathbb{N}$ จงพิสูจน์ว่า $2^{2^n} + 2^{2^{n-1}} + 1$ จะมีตัวประกอบที่เป็นจำนวนเฉพาะที่แตกต่างกันอย่างน้อย n จำนวน
17. ให้ p เป็นจำนวนเฉพาะซึ่ง $3p + 1$ เป็นจำนวนกำลังสองสมบูรณ์ จงพิสูจน์ว่า $p = 5$
18. จงหาจำนวนเฉพาะ p และ q ทั้งหมดที่สอดคล้องกับสมการ $p - q = 3$
19. ให้ $n \in \mathbb{N}$ ที่ $n > 1$ จงแสดงว่า $n!$ ไม่สามารถเขียนได้ในรูปกำลังสองสมบูรณ์
20. จงหาจำนวนเต็มบวกทั้งหมดที่ทำให้ $n! + (n+1)! + (n+2)!$ เป็นกำลังสองสมบูรณ์

บทที่ 4

ข้อเท็จจริงบางประการ เกี่ยวกับจำนวนเฉพาะ

ในบทนี้เราจะกล่าวถึงข้อเท็จจริง (fact) และข้อคาดเดา (conjecture) ที่เกี่ยวข้องกับจำนวนเฉพาะบางส่วน เพื่อให้ผู้เรียนได้เห็นวิวัฒนาการและความสวยงามของจำนวนเฉพาะ ทั้งยังได้เห็นความพยายามของนักคณิตศาสตร์ในอดีตที่จะแก้ข้อคาดเดาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเฉพาะที่ยังไม่สามารถหาคำตอบได้

4.1 ทฤษฎีบทที่สำคัญของจำนวนเฉพาะ

ทฤษฎีบทหนึ่งที่สำคัญของจำนวนเฉพาะที่จะกล่าวต่อไป คือ “มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์” นอกจากทฤษฎีบทนี้แล้วยังมีทฤษฎีบทอีกหลายทฤษฎีบทที่สำคัญซึ่งเกี่ยวข้องกับจำนวนเฉพาะ โดยเราจะนำมากล่าวไว้ในหัวข้อนี้ ซึ่งบางทฤษฎีบทจะขอเว้นการพิสูจน์ไว้ เนื่องจากเนื้อหาบางส่วนของบทพิสูจน์ยากเกินกว่าที่จะนำมากล่าวไว้ในที่นี้

ยุคลิด ได้รับการยกย่องว่าเป็นนักคณิตศาสตร์คนแรกที่พิสูจน์ว่า “มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์” ซึ่งบทพิสูจน์ของเขาปรากฏในหนังสือ Euclid's Element Book IX

ทฤษฎีบท 4.1.1 (Euclid)

มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ (หรือไม่มีจำนวนเฉพาะที่มีค่ามากที่สุด)

บทพิสูจน์ สมมติว่ามีจำนวนเฉพาะอยู่เป็นจำนวนจำกัด

นั่นคือ ให้ $p_1, p_2, p_3, \dots, p_n$ เป็นลำดับของจำนวนเฉพาะทั้งหมดที่เรียงจากน้อยไปหามากและ p_n เป็นจำนวนเฉพาะที่มีค่ามากที่สุด

ให้ $N = p_1 p_2 p_3 \cdots p_n + 1$ จะได้ว่า $N > p_n$ แสดงว่า N เป็นจำนวนประกอบ

โดยทฤษฎีบท 3.1.2 จะมีจำนวนเฉพาะ p ซึ่ง $p \mid N$

และจากสมมติฐานจะได้ว่า $p \in \{p_1, p_2, \dots, p_n\}$

ดังนั้น $p \mid p_1 p_2 \cdots p_n$ แสดงว่า $p \mid 1$ ซึ่งเป็นไปไม่ได้

นั่นคือ มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ ■

การพิสูจน์ว่าจำนวนเฉพาะมีจำนวนอนันต์ของยุคลิดนั้น ได้รับการยอมรับกว่า 2000 ปีมาแล้ว ต่อมานักคณิตศาสตร์รุ่นหลังได้พยายามที่จะหาแนวทางการพิสูจน์ใหม่ของทฤษฎีบท 4.1.1 นี้ และอย่างน้อยที่เห็นปรากฏในหนังสือ Proofs from the Book (Aigner and Ziegler, 1998) ได้กล่าวถึงบทพิสูจน์ของทฤษฎีบทดังกล่าวนี้ที่แตกต่างกันไว้ถึง 6 แบบด้วยกัน ทฤษฎีบท 4.1.1 นี้ ถือว่ามีความสำคัญยิ่งของการนำไปสู่ข้อคาดเดาต่าง ๆ มากมาย โดยจะกล่าวในหัวข้อต่อไป

ให้ p เป็นจำนวนเฉพาะและกำหนด P^* แทนผลคูณของจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ p จากการคำนวณค่าของ P^* เมื่อ $p = 2, 3, 5, 7, 11$ จะพบว่า

$$2^* + 1 = 2 + 1 = 3$$

$$3^* + 1 = 2 \cdot 3 + 1 = 7$$

$$5^* + 1 = 2 \cdot 3 \cdot 5 + 1 = 31$$

$$7^* + 1 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

$$11^* + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

เป็นจำนวนเฉพาะทุกจำนวน

$$\text{อย่างไรก็ตาม } 13^* + 1 = 59 \cdot 509$$

$$17^* + 1 = 19 \cdot 97 \cdot 277$$

$$19^* + 1 = 347 \cdot 27953$$

ไม่เป็นจำนวนเฉพาะ

จากตัวอย่างข้างต้นทำให้เราสามารถตั้งข้อคาดเดาขึ้นมาได้ดังนี้

ข้อคาดเดา มีจำนวนเฉพาะหรือจำนวนประกอบอยู่จำนวนอนันต์หรือไม่ที่เขียนอยู่ในรูป $P^* + 1$

ในปี ค.ศ. 1995 เราพบว่า มีจำนวนเฉพาะ 18 จำนวนที่เขียนอยู่ในรูป $P^* + 1$ ซึ่งได้แก่ $2^* + 1$, $3^* + 1$, $5^* + 1$, $7^* + 1$, $11^* + 1$, $31^* + 1$, $379^* + 1$, $1019^* + 1$, $1021^* + 1$, $2657^* + 1$, $3229^* + 1$, $4547^* + 1$, $4787^* + 1$, $11549^* + 1$, $13649^* + 1$, $18523^* + 1$, $23801^* + 1$ และ $24029^* + 1$ และจำนวนที่ใหญ่ที่สุดของจำนวนเฉพาะดังกล่าวนี้ประกอบด้วยเลขโดด 10395 หลัก นอกจากนี้พบว่า $P^* + 1$ เป็นจำนวนประกอบเมื่อ $P \leq 35000$ ยกเว้น $P = 2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801$ และ 24029

เราจะเรียกจำนวนเต็มที่เขียนอยู่ในรูป $P^* + 1$ ว่า “จำนวนเต็มแบบยุคลิด” (Euclidean numbers) ทั้งนี้เพราะจำนวนเต็มดังกล่าวถูกพิจารณาโดยยุคลิด เมื่อเขาใช้พิสูจน์ข้อความ “มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์”

ทฤษฎีบทประกอบ 4.1.2 ให้ $p_1, p_2, p_3, \dots, p_n, p_{n+1}, \dots$ เป็นลำดับของจำนวนเฉพาะที่เรียงจากน้อยไปมาก
จะได้ว่า $p_{n+1} \leq p_1 p_2 p_3 \cdots p_n + 1$

บทพิสูจน์ กรณี 1 ถ้า $P^* = p_1 p_2 p_3 \cdots p_n + 1$ เป็นจำนวนเฉพาะ เห็นได้ชัดว่า $p_n < P^*$
ดังนั้น $p_{n+1} \leq P^*$

กรณี 2 ถ้า $P = p_1 p_2 p_3 \cdots p_n + 1$ เป็นจำนวนประกอบ
จะได้ว่ามีจำนวนเฉพาะ p' ที่เล็กที่สุดที่เป็นตัวหารของ p แต่
 $p_1 \nmid p, p_2 \nmid p, p_3 \nmid p, \dots, p_n \nmid p$
เพราะว่า ถ้า $p_i \mid p$ แล้ว $p_i \mid 1$ สำหรับทุก $i \in \{1, 2, 3, \dots, n\}$
ดังนั้นจำนวนเฉพาะ p' ที่หาร p ลงตัวจะต้องมีค่ามากกว่า p_n
ซึ่งสรุปได้ว่า $p_{n+1} \leq p'$ และจาก p' เป็นตัวหารของ p จะได้ว่า $p_{n+1} \leq p'$
จากทั้งสองกรณีจะได้ว่า จำนวนเฉพาะตัวที่ $n+1$ คือ

$$p_{n+1} \leq p = p_1 p_2 p_3 \cdots p_n + 1$$

ทฤษฎีบท 4.1.3 ให้ $p_1, p_2, p_3, \dots, p_n, \dots$ แทนลำดับของจำนวนเฉพาะทั้งหมดที่เรียงจากน้อยไปหามาก
จะได้ว่า $p_n \leq 2^{2^{n-1}}$ สำหรับทุกจำนวนเต็มบวก n

บทพิสูจน์ จะพิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ที่ 2

(i) $p_1 = 2 \leq 2^{2^0} = 2$ เป็นจริง

(ii) สมมติว่า $p_k \leq 2^{2^{k-1}}$ เป็นจริงสำหรับทุก $k \leq n$

จะต้องพิสูจน์ว่า $p_{n+1} \leq 2^{2^n}$

จาก $p_1 \leq 2^{2^{1-1}}, p_2 \leq 2^{2^{2-1}}, p_3 \leq 2^{2^{3-1}}, \dots, p_n \leq 2^{2^{n-1}}$

$$\begin{aligned} \text{จะได้ } p_1 p_2 p_3 \cdots p_n &\leq 2 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^{n-1}} \\ &= 2^{2^0 + 2^1 + 2^2 + \cdots + 2^{n-1}} = 2^{2^n - 1} \end{aligned}$$

$$\text{ดังนั้น } p_1 p_2 p_3 \cdots p_n + 1 \leq 2^{2^n - 1} + 2^{2^n - 1}$$

$$\text{นั่นคือ } p_1 p_2 p_3 \cdots p_n + 1 \leq 2^{2^n}$$

โดยทฤษฎีบทประกอบ 4.1.2 จะได้ว่า $p_{n+1} \leq 2^{2^n}$

เพราะฉะนั้นจาก (i) และ (ii) สรุปได้ว่า

$$p_n \leq 2^{2^{n-1}} \text{ สำหรับทุก } n \in \mathbb{N}$$

ตัวอย่าง (1) $p_{30} = 113 \leq 2^{2^{30-1}}$

(2) $p_{100} = 541 \leq 2^{2^{100-1}}$

บทแทรก 4.1.4 สำหรับจำนวนเต็มบวก n จะมีจำนวนเฉพาะอย่างน้อยที่สุด $n + 1$ จำนวนที่มีค่าน้อยกว่า 2^n

ในปี ค.ศ. 1845 โจเซฟ เบร์ทราน (Joseph Bertrand ค.ศ. 1822 – 1900) ได้ตั้งข้อคาดเดาว่า

“จะมีจำนวนเฉพาะหนึ่งจำนวนที่อยู่ระหว่าง n กับ $2n$ เมื่อ $n \geq 2$ ”

ซึ่งเขามีความเชื่อมั่นว่าข้อคาดเดาที่ตั้งขึ้นเป็นจริง โดยการแสดงให้เห็นจริงได้เมื่อ $n \leq 3,000,000$ โดยพบจำนวนเฉพาะที่อยู่ระหว่าง n กับ $2n$ คือ 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, 9973, 19937, 39869, 79699, 159389, ... ต่อมาในปี ค.ศ. 1850 พฟนุติ ลีโววิช เชบีเชฟ (Pafnuti Lvovich Tschebychev ค.ศ. 1821 – 1894) นักคณิตศาสตร์ชาวรัสเซีย สามารถพิสูจน์ข้อคาดเดาของเบร์ทรานได้ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.1.5 (*Tschebychev*)

ให้ $n \in \mathbb{N}$ และ $n \geq 2$ จะได้ว่า มีจำนวนเฉพาะอย่างน้อยหนึ่งจำนวนในลำดับ

$$n, n + 1, n + 2, \dots, 2n$$

บทพิสูจน์ของทฤษฎีบท 4.1.5 นี้ เชบีเชฟ ได้ใช้ความรู้ที่ลึกซึ้งและยาวมาก ต่อมาในปี ค.ศ. 1932 พอล เออร์ดอส (Paul Erdős ค.ศ. 1913 – 1996) นักคณิตศาสตร์ชาวฮังการี ได้แสดงการพิสูจน์ทฤษฎีบทนี้ที่ง่ายกว่าของเชบีเชฟ ซึ่งในขณะนั้นเขามีอายุเพียง 19 ปี และผลงานชิ้นนี้ถือว่าเป็นผลงานชิ้นแรกของเขาที่ได้รับการตีพิมพ์ ผู้สนใจสามารถศึกษารายละเอียดได้จากหนังสือ *Proofs from the Book* ของ Martin Aigner and Günter M. Ziegler หน้า 7 – 10 ในเวลา 65 ปีต่อมา เออร์ดอสสามารถสร้างผลงานทั้งหมดมากกว่า 1,500 ชิ้น

ทฤษฎีบทต่อไป ถือว่าเป็นทฤษฎีบทที่สำคัญอย่างยิ่งของจำนวนเฉพาะ ซึ่งมีชื่อว่า *ทฤษฎีบทของจำนวนเฉพาะ* (*The Prime Number Theorem*) โดยทฤษฎีบทนี้เกิดขึ้นจากการตั้งข้อคาดเดาของเกาส์ในปี ค.ศ. 1792 ซึ่งยังไม่มีการพิสูจน์ที่สมบูรณ์ ต่อมาในปี ค.ศ. 1896 ทฤษฎีบทนี้สามารถพิสูจน์ได้โดย อาดามาร์ด (J. S. Hadamard ค.ศ. 1865 – 1963) และ ปูแซง (C. V. Poussin ค.ศ. 1866 – 1962) ซึ่งให้การพิสูจน์ที่แตกต่างกัน แต่ใช้ความรู้ด้านการวิเคราะห์เชิงซ้อนเหมือนกัน ต่อมาในปี ค.ศ. 1949 อาเทิล เซลเบิร์ก (Atle Selberg) และ เออร์ดอส ได้พิสูจน์ทฤษฎีบทนี้โดยใช้ความรู้ทางเลขคณิตเท่านั้น จากผลงานของเซลเบิร์กในครั้งนี้ ทำให้เขาได้รับรางวัลสูงสุดคือ Fields Medal ซึ่งเทียบเท่ากับรางวัลโนเบล เมื่อปี ค.ศ. 1950 ในงาน International Congress of Mathematics ซึ่งจะจัดประจําทุก 4 ปี และสำหรับนักคณิตศาสตร์ที่อายุต่ำกว่า 40 ปี

ทฤษฎีบท 4.1.6 (*ทฤษฎีบทของจำนวนเฉพาะ*)

ให้ $\pi(n)$ แทนจำนวนของจำนวนเฉพาะ p ซึ่ง $p \leq n$ จะได้ว่า

$$\pi(n) \text{ มีค่าประมาณ } \frac{n}{\log n}$$

เมื่อ n มีค่ามาก ๆ และ $\log n$ หมายถึงลอการิทึมฐานธรรมชาติของ n

$$\text{นั่นคือ } \lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \log n} = 1$$

สำหรับบทพิสูจน์ของทฤษฎีบท 4.1.6 นี้สามารถศึกษาได้จากหนังสือ Elementary Number Theory ของ David M. Burton (ปี ค.ศ. 2002) หน้า 352 – 359

ถ้า n มีค่ามาก ๆ แล้ว $\pi(n)$ จะมีค่าใกล้เคียงกับ $\frac{n}{\log n}$ ซึ่งพิจารณาได้จากตาราง ต่อไปนี้

n	$\pi(n)$	$\frac{n}{\log n}$	$\frac{\pi(n)}{n/\log n}$
10^3	168	145	1.159
10^4	1229	1086	1.132
10^5	9592	8686	1.104
10^6	78498	72382	1.084
10^7	664579	620420	1.071
10^8	5761455	542868	1.061

ถ้าเราแบ่งเซตของจำนวนเต็มบวกออกเป็น 4 กลุ่ม โดยพิจารณาจากเศษที่เกิดจากการหารจำนวนเต็มบวกนั้น ด้วย 4 จะได้

$$\mathbb{N} = \{4k \mid k \in \mathbb{N}\} \cup \{4k+1 \mid k \in \mathbb{N}\} \cup \{4k+2 \mid k \in \mathbb{N}\} \cup \{4k+3 \mid k \in \mathbb{N}\}$$

และเราพบว่า ไม่มีจำนวนเฉพาะใน $\{4k \mid k \in \mathbb{N}\}$ และมี 2 ที่เป็นจำนวนเฉพาะเพียงจำนวนเดียวใน

$\{4k+2 \mid k \in \mathbb{N}\}$ ส่วนจำนวนเฉพาะที่เหลือจะกระจายอยู่ในเซต $\{4k+1 \mid k \in \mathbb{N}\} \cup \{4k+3 \mid k \in \mathbb{N}\}$

ให้ $A = \{4k+1 \mid k \in \mathbb{N}\}$ และ $B = \{4k+3 \mid k \in \mathbb{N}\}$ เราพบว่า ผลคูณของสมาชิก 2 ตัวใน A ยังคงเป็นสมาชิกใน A ในขณะที่ผลคูณของสมาชิก 2 ตัวใน B จะเป็นสมาชิกใน A จากข้อสังเกตนี้นำไปสู่ทฤษฎีบทต่อไปนี้

ทฤษฎีบทประกอบ 4.1.7 ผลคูณของจำนวนเต็มที่เขียนอยู่ในรูป $4k+1$ ตั้งแต่สองจำนวนขึ้นไป จะเป็นจำนวนเต็มที่เขียนอยู่ในรูป $4k+1$

บทพิสูจน์ ให้ $n_1 = 4k_1 + 1$ และ $n_2 = 4k_2 + 1$ เมื่อ k_1 และ k_2 เป็นจำนวนเต็ม

$$\text{ดังนั้น } n_1 n_2 = (4k_1 + 1)(4k_2 + 1)$$

$$= 4(4k_1 k_2 + k_1 + k_2) + 1$$

$$= 4k + 1 \quad \text{เมื่อ } k = 4k_1 k_2 + k_1 + k_2 \text{ เป็นจำนวนเต็ม}$$

โดยหลักอุปนัยเชิงคณิตศาสตร์ จะได้ว่า ทฤษฎีบทประกอบนี้เป็นจริง ■

ทฤษฎีบท 4.1.8 มีจำนวนเฉพาะที่เขียนอยู่ในรูป $4k + 3$ เป็นจำนวนอนันต์

บทพิสูจน์ สมมติว่ามีจำนวนเฉพาะที่เขียนอยู่ในรูป $4k + 3$ เป็นจำนวนจำกัด

นั่นคือ ให้ $p_1, p_2, \dots, p_n$ เป็นจำนวนเฉพาะที่เขียนอยู่ในรูป $4k + 3$ ทั้งหมดที่เรียงจากน้อยไปหามาก และ p_n มีค่ามากที่สุด

$$\text{ให้ } N = 4p_1p_2 \cdots p_n - 1 = 4(p_1p_2 \cdots p_n - 1) + 3$$

จะได้ว่า $N > 1$ และ $N > p_n$

แสดงว่า N เป็นจำนวนประกอบ โดยทฤษฎีบท 3.2 จะได้ว่า N สามารถเขียนได้ในรูปผลคูณของ

จำนวนเฉพาะ นั่นคือ $N = q_1q_2 \cdots q_i$ เมื่อ $q_1, q_2, \dots, q_i$ เป็นจำนวนเฉพาะ

เนื่องจาก N เป็นจำนวนเต็มคี่ ดังนั้น q_i จะเขียนอยู่ในรูป $4k + 1$ หรือ $4k + 3$

ถ้าทุก q_i อยู่ในรูป $4k + 1$ โดยทฤษฎีบทประกอบ 4.1.7 จะได้ว่า N จะเขียนอยู่ในรูป $4k + 1$ ซึ่งไม่จริง

ดังนั้น จะมี $q_r \in \{q_1, q_2, \dots, q_i\}$ ซึ่งเขียนอยู่ในรูป $4k + 3$

เพราะฉะนั้นมี $j \in \{1, 2, \dots, n\}$ ซึ่ง $q_r = p_j$

นั่นคือ $p_j \mid N$ แต่ $p_j \nmid p_1p_2 \cdots p_n$

ดังนั้น $p_j \mid 1$ ซึ่งเป็นไปไม่ได้

สรุปได้ว่ามีจำนวนเฉพาะที่อยู่ในรูป $4k + 3$ อยู่เป็นจำนวนอนันต์ ■

จากทฤษฎีบท 4.1.8 ข้างต้นผู้อ่านอาจตั้งคำถามว่า จำนวนเฉพาะที่เขียนอยู่ในรูป $4k + 1$ มีจำนวนอนันต์หรือไม่ หรือจำนวนเฉพาะที่เขียนในรูปแบบไหนจะมีจำนวนอนันต์ ปัญหานี้มีคำตอบแล้วโดยในปี ค.ศ. 1837 ดีริชเลต์ เป็นผู้นำเสนอบทพิสูจน์ โดยรายละเอียดของการพิสูจน์ปัญหานี้ยากเกินกว่าจะกล่าวไว้ ณ ที่นี้ ดังนั้น ผู้เขียนจะขอกล่าวเฉพาะตัวทฤษฎีบทเท่านั้นซึ่งมีรายละเอียดดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.1.9 (Dirichlet)

ถ้า $a, b \in \mathbb{N}$ และ $(a, b) = 1$ แล้วจะมีจำนวนเฉพาะปรากฏอยู่ในลำดับเลขคณิตอนันต์

$$a, a + b, a + 2b, a + 3b, \dots$$

เป็นจำนวนอนันต์

จากทฤษฎีบท 4.1.9 นี้ ถ้าเลือก $a = 999$ และ $b = 1000$ จะพบว่าจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ที่ลงท้ายด้วย 999 เช่น 1999, 100999, 1000999, ... ปรากฏอยู่ในลำดับเลขคณิตอนันต์ที่มีพจน์ที่ n คือ $1000n + 999$ ในทางกลับกันไม่มีลำดับเลขคณิตใดที่จะทำให้สมาชิกในลำดับนั้นทุกตัวเป็นจำนวนเฉพาะ ให้ $a, a + b, a + 2b, \dots$ เป็นลำดับเลขคณิตอนันต์ โดยที่ $a, b \in \mathbb{N}$ จะได้ว่า

พจน์ที่ $a + 1$ คือ $a + ab = a(1 + b)$ ดังนั้น ถ้า $a > 1$ แล้ว $a(1 + b)$ ไม่เป็นจำนวนเฉพาะ

เรื่องเกี่ยวกับจำนวนเฉพาะยังมีอีกมากมายทั้งที่เป็นข้อคาดเดาและเป็นข้อเท็จจริงที่มีการพิสูจน์ได้แล้ว ในปี ค.ศ. 1737 ออยเลอร์ ได้พิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.1.10 (Euler)

ให้ $p_1, p_2, p_3, \dots$ แทนลำดับของจำนวนเฉพาะที่เรียงจากน้อยไปมาก จะได้ว่าอนุกรม

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \dots$$

เป็นอนุกรมไดเวอร์เจนต์ (divergent series)

จากทฤษฎีบท 4.1.10 นี้ประกอบกับความจริงที่ว่า $1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots$ เป็นอนุกรมคอนเวอร์เจนต์ (convergent series) เราอาจกล่าวได้ว่ามีจำนวนเฉพาะมากกว่าจำนวนที่เป็นกำลังสองสมบูรณ์

โจทย์ปัญหา 4.1

1. สำหรับจำนวนเต็มบวก $n > 1$ จงแสดงว่า ทุกจำนวนเฉพาะที่หาร $n! + 1$ ลงตัวจะเป็นจำนวนเต็มคี่ที่มีค่ามากกว่า n
2. จงแสดงว่า ถ้า $n \in \mathbb{N}$ ซึ่ง $n > 2$ แล้วจะมีจำนวนเฉพาะ p ที่สอดคล้องกับ $n < p < n!$
(ข้อเสนอแนะ ถ้า $n! - 1$ ไม่เป็นจำนวนเฉพาะ แล้วจะมีจำนวนเฉพาะ p ซึ่ง
ถ้า $p \leq n$ แล้ว $p \mid n!$ ซึ่งจะได้ข้อขัดแย้ง)
3. ให้ p_n เป็นจำนวนเฉพาะตัวที่ n จงแสดงว่า $p_n > 2n - 1$ สำหรับ $n \geq 5$
4. ให้ $p_1, p_2, p_3, \dots, p_n$ เป็นลำดับของจำนวนเฉพาะ
จงตรวจสอบว่ามีจำนวนเต็มที่เขียนในรูป $P^* = p_1 p_2 p_3 \cdots p_n + 1$ เป็นกำลังสองสมบูรณ์หรือไม่
(ข้อเสนอแนะ p เขียนอยู่ในรูป $4k + 3$ สำหรับ $n > 1$)
5. จงแสดงว่าถ้า $n \in \mathbb{N}$ ซึ่ง $n \geq 2$ แล้วจะมีจำนวนเฉพาะ p ซึ่ง $p \leq n < 2p$

4.2 ข้อคาดเดาที่เกี่ยวข้องกับจำนวนเฉพาะ

ในหัวข้อนี้ผู้เขียนจะกล่าวถึงข้อคาดเดาที่เกี่ยวข้องกับจำนวนเฉพาะ เพื่อผู้อ่านจะได้เห็นวิวัฒนาการและความพยายามของนักคณิตศาสตร์ในอดีต

ข้อคาดเดาที่ 1 ข้อคาดเดาของโกลด์บัค (The Goldbach conjecture)

ในปี ค.ศ. 1742 โกลด์บัค (Christian Goldbach ค.ศ. 1690 – 1764) ได้ตั้งข้อคาดเดาไว้ 2 ข้อ คือ

- (1) ทุก ๆ จำนวนเต็มคู่ $N \geq 6$ สามารถเขียนอยู่ในรูปผลบวกของจำนวนเฉพาะคี่ 2 จำนวนได้
- (2) ทุก ๆ จำนวนเต็มคี่ $N \geq 9$ สามารถเขียนอยู่ในรูปผลบวกของจำนวนเฉพาะคี่ 3 จำนวนได้

ถ้าข้อคาดเดา (1) เป็นจริง แล้วข้อคาดเดา (2) สามารถพิสูจน์ให้เป็นจริงได้ไม่ยาก เพราะว่าถ้า n เป็นจำนวนเต็มคี่และ p เป็นจำนวนเฉพาะคี่ที่มีค่าน้อยกว่า n แล้ว $n - p$ จะเป็นจำนวนเต็มคู่ ถ้า $n - p$ เขียนอยู่ในรูปผลบวกของจำนวนเฉพาะคี่ 2 จำนวน คือ q และ r จะได้ $n - p = q + r$ นั่นคือ $n = p + q + r$

การตรวจสอบข้อคาดเดา (1) อาจทำได้โดยใช้จำนวนที่มีค่าน้อย เช่น

$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 3 + 7$$

$$12 = 5 + 7$$

$$14 = 3 + 11 = 7 + 7$$

$$16 = 3 + 13 = 5 + 11$$

$$18 = 5 + 13 = 7 + 11$$

$$20 = 3 + 17 = 7 + 13$$

ต่อไปนี้เป็นจำนวนเต็มคู่ n ซึ่ง $6 \leq n \leq 100$ สามารถเขียนในรูปผลบวกของจำนวนเฉพาะสองจำนวนได้

$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 5 + 5$$

$$10 = 3 + 7$$

$$12 = 5 + 7$$

$$14 = 7 + 7$$

$$14 = 3 + 11$$

$$16 = 5 + 11$$

$$16 = 3 + 13$$

$$18 = 7 + 11$$

$$18 = 5 + 13$$

$$20 = 7 + 13$$

$$20 = 3 + 17$$

$$22 = 11 + 11$$

$$22 = 5 + 17$$

$$22 = 3 + 19$$

$$24 = 11 + 13$$

$$24 = 7 + 17$$

$$24 = 5 + 19$$

$$26 = 13 + 13$$

$$26 = 7 + 19$$

$$26 = 3 + 23$$

$$28 = 11 + 17$$

$$28 = 5 + 23$$

$$30 = 13 + 17$$

$$30 = 11 + 19$$

$$30 = 11 + 23$$

$$32 = 13 + 19$$

$$32 = 3 + 29$$

$$34 = 17 + 17$$

$$34 = 11 + 23$$

$$34 = 5 + 29$$

$$34 = 3 + 31$$

$$36 = 17 + 19$$

$$36 = 13 + 23$$

$$36 = 7 + 29$$

$$40 = 11 + 29$$

$$40 = 3 + 37$$

$$42 = 19 + 23$$

$$42 = 13 + 29$$

$$42 = 11 + 31$$

$$42 = 5 + 37$$

$$44 = 13 + 31$$

$$44 = 7 + 37$$

$$44 = 3 + 41$$

$$46 = 23 + 23$$

$$46 = 17 + 29$$

$$46 = 5 + 41$$

$$46 = 3 + 43$$

$$48 = 19 + 29$$

$$48 = 17 + 31$$

$$48 = 11 + 37$$

$$48 = 7 + 41$$

$$48 = 5 + 43$$

$$50 = 19 + 31$$

$$50 = 13 + 37$$

$$50 = 7 + 43$$

$$50 = 3 + 47$$

$$52 = 23 + 29$$

$$52 = 11 + 41$$

$$52 = 5 + 47$$

$$54 = 23 + 31$$

$$54 = 17 + 37$$

$$54 = 13 + 41$$

$$54 = 11 + 43$$

$$54 = 7 + 47$$

$$56 = 19 + 37$$

$$56 = 13 + 43$$

$$56 = 3 + 53$$

$$58 = 29 + 29$$

$$58 = 17 + 41$$

$$58 = 11 + 47$$

$$58 = 5 + 53$$

$$60 = 29 + 31$$

$$60 = 23 + 37$$

$$60 = 19 + 41$$

$$60 = 17 + 43$$

$$60 = 13 + 47$$

$$60 = 7 + 53$$

$$62 = 31 + 31$$

$$62 = 19 + 43$$

$$62 = 3 + 59$$

$$64 = 23 + 41$$

$$64 = 17 + 47$$

$$64 = 11 + 53$$

$$64 = 5 + 59$$

$$64 = 3 + 61$$

$$66 = 29 + 37$$

$$66 = 23 + 43$$

$$66 = 19 + 47$$

$$66 = 13 + 53$$

$$66 = 7 + 59$$

$$66 = 5 + 61$$

$$68 = 31 + 37$$

$$68 = 7 + 61$$

$$70 = 29 + 41$$

$$70 = 23 + 47$$

$$70 = 17 + 53$$

$$70 = 11 + 59$$

$$70 = 3 + 67$$

$$72 = 31 + 41$$

$$72 = 29 + 43$$

$$72 = 19 + 53$$

$$72 = 13 + 59$$

$$72 = 11 + 61$$

$$72 = 5 + 67$$

$$74 = 37 + 37$$

$$74 = 31 + 43$$

$$74 = 13 + 61$$

$$74 = 7 + 67$$

$$74 = 3 + 71$$

$$76 = 29 + 47$$

$$76 = 23 + 53$$

$$76 = 17 + 59$$

$$76 = 5 + 71$$

$$76 = 3 + 73$$

78 = 37 + 41	78 = 31 + 47	78 = 19 + 59	78 = 17 + 61
78 = 11 + 67	78 = 7 + 71	78 = 5 + 73	80 = 37 + 43
80 = 19 + 61	80 = 13 + 67	80 = 7 + 73	82 = 41 + 41
82 = 29 + 53	82 = 23 + 59	82 = 11 + 71	82 = 3 + 79
84 = 41 + 43	84 = 37 + 47	84 = 31 + 53	84 = 23 + 61
84 = 17 + 67	84 = 13 + 71	84 = 11 + 73	84 = 5 + 79
86 = 43 + 43	86 = 19 + 67	86 = 13 + 73	86 = 7 + 79
86 = 3 + 83	88 = 41 + 47	88 = 29 + 59	88 = 17 + 71
88 = 5 + 83	90 = 43 + 47	90 = 37 + 53	90 = 31 + 59
90 = 29 + 61	90 = 23 + 67	90 = 19 + 71	90 = 17 + 73
90 = 11 + 79	90 = 7 + 83	92 = 31 + 61	92 = 19 + 73
92 = 13 + 79	92 = 3 + 89	94 = 47 + 47	94 = 41 + 53
94 = 23 + 71	94 = 11 + 83	94 = 5 + 89	96 = 43 + 53
96 = 23 + 73	96 = 17 + 79	96 = 13 + 83	96 = 7 + 89
98 = 37 + 61	98 = 31 + 67	98 = 19 + 79	100 = 47 + 53
100 = 41 + 59	100 = 29 + 71	100 = 17 + 83	100 = 11 + 89
100 = 3 + 97			

ปีพืง ได้ตรวจสอบข้อคาดเดานี้สำหรับจำนวนเต็มคู่จนถึง 100,000 และในปัจจุบันได้มีการตรวจสอบว่าข้อคาดเดานี้เป็นจริงสำหรับทุกจำนวนเต็มคู่ที่น้อยกว่า 10^{10} แต่การพิสูจน์ว่าข้อคาดเดานี้เป็นจริงสำหรับจำนวนเต็มคู่ที่มากกว่า 4 ยังไม่มีใครทราบ

ในขณะที่ข้อคาดเดาของโกลด์บัคยังไม่ได้พิสูจน์นั้น ได้มีนักคณิตศาสตร์ชาวรัสเซีย ชื่อ วินogradอฟ (Vinogradov) ได้พยายามพิสูจน์ข้อคาดเดา (2) ในปี ค.ศ. 1937 และแสดงว่า “จำนวนคี่ทุกจำนวนที่มีค่ามากพอจะสามารถเขียนอยู่ในรูปของผลบวกของจำนวนเฉพาะคี่ 3 จำนวนได้” อย่างไรก็ตาม การพิสูจน์นี้เป็นแค่การพิสูจน์การมีอยู่ (existence proof) แต่ยังไม่มีการบอกได้ว่าจำนวนที่มีค่ามากพอนั้นคือจำนวนใด จนกระทั่งในปี ค.ศ. 1988 มีผู้แสดงไว้ว่า จำนวนที่มีค่ามากพอคือ N ซึ่ง $N > k$ โดยที่ $k < 10^{400000}$

ข้อคาดเดาที่ 2 ให้ $n \in \mathbb{N}$ จะมีจำนวนเฉพาะ n จำนวนที่เรียงกันเป็นลำดับเลขคณิต

เออร์ตอส ได้ตั้งรางวัลสำหรับผู้ที่สามารถตอบข้อคาดเดาที่ 2 นี้ได้ไว้ถึง US \$5000 อย่างไรก็ตามนักคณิตศาสตร์ชั้นนำของโลกมีความเชื่อว่าข้อคาดเดาที่ 2 นั้นจะเป็นจริงและมีผู้ที่สามารถหาจำนวนเฉพาะที่เรียงติดต่อเนื่องกันเป็นลำดับเลขคณิตได้ถึง 21 จำนวนแล้ว

$$142072321123 + 1419763024n \quad (0 \leq n \leq 20)$$

จากการสังเกตพบว่า $1^2 + 1 = 2$, $2^2 + 1 = 5$, $4^2 + 1 = 17$, $6^2 + 1 = 37$ จากข้อสังเกตข้างต้นจึงเกิดข้อคาดเดาต่อไปนี้

ข้อคาดเดาที่ 3 มีจำนวนเฉพาะที่อยู่ในรูป $n^2 + 1$ อยู่ไม่จำกัดจำนวนหรือจำกัดจำนวน

ข้อคาดเดาที่ 4 จำนวนเฉพาะคู่แฝด (Twin primes) คือจำนวนเฉพาะ 2 จำนวนที่อยู่ในรูป $p, p + 2$ เรามีข้อคาดเดาว่า

จะมีจำนวนเฉพาะคู่แฝดเป็นจำนวนจำกัดหรือไม่จำกัด

จำนวนเฉพาะคู่แฝดที่น้อยกว่า 51 จะมีทั้งหมด 6 คู่ คือ (3, 5), (5, 7), (11, 13), (17, 19), (29, 31) และ (41, 43)

จากการใช้เครื่องคอมพิวเตอร์ พบว่ามีจำนวนเฉพาะคู่แฝดที่น้อยกว่า 30,000,000 อยู่ทั้งหมด 152,892 คู่ และจำนวนเฉพาะคู่แฝดที่อยู่ระหว่าง 999,999,990,000 และ 1,000,000,000,000 มี 15 คู่ และระหว่าง 1,000,000,000,000 และ 1,000,000,010,000 มี 20 คู่ คู่หนึ่งในจำนวนนี้ได้แก่ 1,000,000,000,061 และ 1,000,000,000,063 ในปี ค.ศ. 1989 มีผู้ค้นพบจำนวนเฉพาะคู่แฝดคู่หนึ่งคือ $1706595 \cdot 2^{11235} \pm 1$ โดยที่แต่ละจำนวนประกอบด้วย 3389 หลัก ต่อมาในปี ค.ศ. 2000 มีผู้ค้นพบจำนวนเฉพาะคู่แฝดคู่หนึ่งที่คิดว่าใหญ่ที่สุดคือ $665551035 \cdot 2^{80025} \pm 1$ โดยที่แต่ละจำนวนประกอบด้วย 24099 หลัก

โจทย์ปัญหา 4.2

1. จงพิสูจน์ว่าจำนวนเต็มบวก n เป็นจำนวนเฉพาะ ก็ต่อเมื่อ $n \mid [(n-1)! + 1]$
2. จงแสดงว่าจำนวนเต็ม 1884, 1960, 1988 สามารถเขียนในรูปผลบวกของจำนวนเฉพาะ 2 จำนวนได้
3. จงแสดงว่าจำนวนเต็ม 1745, 2215, 2785 สามารถเขียนในรูปผลบวกของจำนวนเฉพาะ 3 จำนวนได้
4. จงยกตัวอย่างการเขียนจำนวนเฉพาะเรียงกัน 3 จำนวน และเป็นลำดับเลขคณิตด้วย มา 2 ชุด

4.3 จำนวนเฉพาะแฟร์มาต์

ในปี ค.ศ. 1640 แฟร์มาต์ได้ศึกษาจำนวนเต็มที่อยู่ในรูป $2^{2^n} + 1$ ซึ่งมีรายละเอียดดังนี้

บทนิยาม 4.3.1 จำนวนแฟร์มาต์ (Fermat number) คือจำนวนเต็มที่อยู่ในรูป

$$F_n = 2^{2^n} + 1, \quad n \geq 0$$

ถ้า F_n เป็นจำนวนเฉพาะ เราจะเรียก F_n ว่า จำนวนเฉพาะแฟร์มาต์ (Fermat prime)

แฟร์มาต์ พบว่า จำนวนเต็ม $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ ต่างก็เป็นจำนวนเฉพาะ และเขายังตั้งข้อคาดเดาต่ออีกว่า

$$2^{2^1} + 1, 2^{2^2} + 1, 2^{2^3} + 1, 2^{2^4} + 1, \dots \text{ เป็นจำนวนเฉพาะทุกจำนวน}$$

แต่ต่อมาในปี ค.ศ. 1732 ออยเลอร์ พบว่า

$$F_5 = 2^{2^5} + 1 = 4,294,967,297 = 641 \cdot 6700417$$

เป็นจำนวนประกอบ ซึ่งทำให้ข้อคาดเดาของแฟร์มาต์ไม่เป็นจริง

ในช่วงปี ค.ศ. 1878 ลูคัส (Edouard Lucas ค.ศ. 1842 – 1891) นักคณิตศาสตร์ชาวฝรั่งเศส ได้พิสูจน์ว่า F_6 เป็นจำนวนประกอบ เนื่องจาก

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

จากการศึกษาค้นคว้าต่อมาพบว่า F_n เป็นจำนวนประกอบ สำหรับ $5 \leq n \leq 20$ และมีผู้พิสูจน์ได้ว่า F_{23472} เป็นจำนวนประกอบ อย่างไรก็ตาม ยังไม่มีผู้ใดพิสูจน์ได้ว่า มีจำนวนเฉพาะอยู่จำนวนอนันต์ที่สามารถเขียนได้ในรูป $2^{2^n} + 1$ หรือไม่ และยังไม่มีการค้นพบจำนวนเฉพาะแฟร์มาต์ตัวอื่น ๆ อีกเลย

ดังนั้นอาจกล่าวได้ว่า จำนวนเฉพาะแฟร์มาต์ที่ค้นพบในปัจจุบัน ตัวที่ใหญ่ที่สุดคือ $F_4 = 65537$ และข้อคาดเดาที่ดีที่สุดคือ จำนวนแฟร์มาต์ $F_n > F_4$ เป็นจำนวนประกอบ ถ้าข้อคาดเดานี้เป็นจริง แสดงว่าจำนวนเฉพาะแฟร์มาต์มีได้จำกัดเพียง 5 จำนวนเท่านั้น และมีความพยายามที่จะค้นหาคุณลักษณะของ F_n ในกรณีที่ n มีค่าน้อย ๆ เช่น

$$F_7 = 2^{2^7} + 1 = (59,649,589,127,497,217)(5,704,689,200,685,129,654,721)$$

$$F_8 = 2^{2^8} + 1 = (1,238,926,361,552,897)M \quad \text{เมื่อ } M \text{ เป็นจำนวนเต็มบวกที่มี 62 หลัก}$$

$$F_{17} = 2^{2^{17}} + 1 = (31,065,037,602,817)N \quad \text{เมื่อ } N \in \mathbb{N}$$

ตารางต่อไปนี้จะแสดงลักษณะการค้นพบจำนวนแฟร์มาต์ F_n , $0 \leq n \leq 30$

n	ลักษณะของ F_n
0, 1, 2, 3, 4	เป็นจำนวนเฉพาะ
5, 6, 7, 8, 9, 11	แยกเป็นผลคูณของจำนวนเฉพาะได้
10, 12, 13, 19, 30	เราทราบตัวประกอบเพียง 2 หรือ 4 ตัวประกอบ
15, 16, 17, 18, 21, 23, 25, 26, 27	เราทราบเพียง 1 ตัวประกอบที่เป็นจำนวนเฉพาะ
14, 20	เป็นจำนวนประกอบแต่ไม่ทราบว่ามีความประกอบอะไรบ้าง
22, 24, 28, 29	ไม่ทราบลักษณะใด ๆ เลย

ตัวอย่าง 1 ให้ F_n และ F_m เป็นจำนวนแฟร์มาต์ที่ $m > n$

$$\text{จงแสดงว่า } (F_m, F_n) = 1$$

$$(\text{ข้อเสนอแนะ } x^k - 1 = (x + 1)(x^{k-1} - x^{k-2} + \cdots + x - 1) \text{ เมื่อ } k \text{ เป็นจำนวนเต็มคู่})$$

วิธีทำ ให้ $d = (F_m, F_n)$ และจะแสดงว่า $d = 1$

$$\text{ให้ } x = 2^{2^n} \text{ และ } k = 2^{m-n} \text{ จะได้ว่า}$$

$$\frac{F_m - 2}{F_n} = \frac{(2^{2^n})^{2^{m-n}} - 1}{2^{2^n} - 1}$$

$$\text{ดังนั้น } \frac{F_m - 2}{F_n} = \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \cdots + x - 1$$

แสดงว่า $F_n \mid (F_m - 2)$ จาก $d \mid F_n$ จะได้ $d \mid (F_m - 2)$
 และจาก $d \mid F_m$ และ $d \mid (F_m - 2)$ สรุปได้ว่า $d \mid 2$ แต่ d เป็นจำนวนเต็มคี่
 ดังนั้น $d = 1$ เพราะฉะนั้น $(F_m, F_n) = 1$ □

โจทย์ปัญหา 4.3

1. สำหรับ $n > 0$ จงพิสูจน์ว่า มีจำนวนประกอบที่เขียนอยู่ในรูป $2^{2^n} + 3$ อยู่จำนวนอนันต์
2. จงแสดงว่า จำนวนเต็มที่เขียนอยู่ในรูป $2^{2^n} + 5$ เป็นจำนวนประกอบ
3. สำหรับ $n \geq 1$ จงแสดงว่า $(F_n, n) = 1$

4.4 จำนวนเฉพาะแมร์เซน

มาริน แมร์เซน (Marin Mersenne ค.ศ. 1588 – 1648) บาทหลวงชาวฝรั่งเศส เป็นนักคณิตศาสตร์คนหนึ่งที่มีความสนใจในการสร้างลำดับของจำนวนเต็มที่จะเป็นลำดับของจำนวนเฉพาะ โดยเขาศึกษาลำดับของจำนวนเต็มที่อยู่ในรูป

$$M_n = 2^n - 1, \quad n \in \mathbb{N}$$

เราจึงตั้งชื่อเพื่อเป็นเกียรติแก่แมร์เซน โดยเรียกจำนวน $M_n = 2^n - 1$ ว่า จำนวนแมร์เซน (Mersenne number) และถ้า M_n เป็นจำนวนเฉพาะ เราจะ M_n นี้ว่า จำนวนเฉพาะแมร์เซน (Mersenne prime)

จากการเขียน $n = ab$ เราพบวิธีการแยกตัวประกอบของ

$$M_n = 2^n - 1 = 2^{ab} - 1 = (2^a - 1)[(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1]$$

นี่คือการแสดงว่า ถ้า n เป็นจำนวนประกอบแล้ว $2^n - 1$ เป็นจำนวนประกอบ ซึ่งมีความหมายเหมือนกับทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.4.1 ถ้า M_n เป็นจำนวนเฉพาะแล้ว n เป็นจำนวนเฉพาะ

จากทฤษฎีบท 4.4.1 จะได้ว่าจำนวน M_p จะเป็นจำนวนเฉพาะแมร์เซนได้ ก็ต่อเมื่อ มีจำนวนเฉพาะ p ที่ทำให้ M_p เป็นจำนวนเฉพาะ เช่น $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, $M_{13} = 8191$, $M_{17} = 131071$ และ $M_{19} = 524287$

แมร์เซนได้ตั้งข้อสังเกตว่า มีเพียง M_p ที่เป็นจำนวนเฉพาะเมื่อ $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ และ 257 เท่านั้น และเป็นจำนวนประกอบสำหรับจำนวนเฉพาะ p อื่น ๆ ที่น้อยกว่า 257 นักคณิตศาสตร์คนอื่น ๆ ในสมัยนั้นเชื่อว่าแมร์เซนไม่ได้ทดสอบความเป็นจำนวนเฉพาะของจำนวนเหล่านั้นทุกจำนวน ต่อมาในปี ค.ศ. 1772 ออยเลอร์ได้พิสูจน์ว่า M_{31} เป็นจำนวนเฉพาะ โดยทดสอบกับตัวหารที่เป็นจำนวนเฉพาะจนถึง 46339 แต่ M_{67} , M_{127} และ M_{257} เป็นจำนวนที่มีค่ามากเกินไปที่จะตรวจสอบได้

จากการค้นคว้าต่อมาได้มีผู้พยายามตรวจสอบ M_p สำหรับจำนวนเฉพาะ p ซึ่งมีทั้งหมด 55 จำนวนที่น้อยกว่า 257 พบว่าข้อสังเกตของแมร์เซนผิดพลาดไป กล่าวคือ

M_{67} และ M_{257} เป็นจำนวนประกอบ

M_{61} , M_{89} และ M_{107} เป็นจำนวนเฉพาะ

ในปี ค.ศ. 1876 ลูคัส ได้พิสูจน์ว่า M_{67} เป็นจำนวนประกอบแต่ก็ไม่สามารถหาตัวประกอบออกมาได้ ในเดือนตุลาคมปี ค.ศ. 1903 ในการประชุม American Mathematical Society โคล (Frederick Nelson Cole, ค.ศ. 1861 – 1927) นักคณิตศาสตร์ชาวเยอรมัน ได้เสนอผลงานในหัวข้อ “On the Factorization of Large Numbers” เมื่อเขาถูกเชิญให้ขึ้นไปนำเสนอ โคลเดินตรงไปที่กระดานดำโดยไม่กล่าวอะไร แล้วบรรจุเขียน $2^{67} - 1$ จากนั้นคำนวณออกมาทีละขั้นพร้อมทั้งผลคูณซึ่ง

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

โคลไม่ได้พูดและอธิบายอะไร ซึ่งทุกคนก็ไม่สงสัยอะไรด้วย (ต่อมาโคลสารภาพกับเพื่อนของเขาว่า เขาใช้เวลาว่างตอนบ่ายวันอาทิตย์เป็นเวลา 20 ปี ในการหาตัวประกอบของ M_{67})

ในปี ค.ศ. 1932 เลห์เมอร์ (D. H. Lehmer) ได้แสดงว่า M_{257} ไม่เป็นจำนวนเฉพาะ ซึ่ง

$$M_{257} = (535006138814359)(1155685395246619182673033)N \text{ เมื่อ}$$

$$N = 374550598501810936581776630096313181393$$

จากการศึกษาจำนวนแมร์เซนพบว่า เมื่อนำจำนวนเฉพาะแมร์เซน 4 ตัวแรก คือ 3, 7, 31 และ 127 ไปแทน n ในสูตร $2^n - 1$ จะได้จำนวนแมร์เซนตัวใหม่ขึ้นมา จากการแทนค่านี้ นักคณิตศาสตร์ได้พากันคาดหวังว่าวิธีนี้อาจทำให้ได้ว่ามีจำนวนเฉพาะแมร์เซนอยู่จำนวนอนันต์ จึงได้มีข้อคาดเดาว่า ถ้า M_p เป็นจำนวนเฉพาะแล้ว M_{M_p} เป็นจำนวนเฉพาะด้วยแต่ความคาดหวังก็ดับลง ในปี ค.ศ. 1953 เมื่อพบว่า

$$M_{M_{13}} = 2^{M_{13}} - 1 = 2^{8191} - 1$$

เป็นจำนวนประกอบ (มีเลขโดด 2466 หลัก)

ในปี ค.ศ. 2001 พบว่า $M_{13466917}$ เป็นจำนวนเฉพาะแมร์เซนที่มีค่ามากที่สุด ปัญหาที่น่าสนใจในขณะนี้คือจำนวนเฉพาะ $M_p = 2^p - 1$ มีอยู่จำนวนอนันต์หรือไม่ ซึ่งปัญหานี้ยังเป็นปัญหาที่มีชื่อเสียงระดับโลกที่ยังไม่มีใครตอบได้

ตารางแสดงจำนวนเฉพาะแมร์เซนและจำนวนสมบูรณ์เท่าที่ทราบในปัจจุบัน

ให้ p เป็นจำนวนเฉพาะที่ทำให้ $M_p = 2^p - 1$ เป็นจำนวนเฉพาะ เราจะเรียกจำนวน P_p ซึ่ง $P_p = 2^{p-1}(2^p - 1)$ ว่าเป็น จำนวนสมบูรณ์ (perfect number)

ลำดับที่	จำนวนเฉพาะ (p)	ปีที่ค้นพบ (ค.ศ.)	ผู้ค้นพบ	ลำดับที่	จำนวนเฉพาะ (p)	ปีที่ค้นพบ (ค.ศ.)	ผู้ค้นพบ
1	2	-	-	21	9689	1963	Gillies
2	3	-	-	22	9941	1963	Gillies
3	5	-	-	23	11213	1963	Gillies
4	7	-	-	24	19937	1971	Tuckerman
5	13	1456	Anonymous	25	21701	1978	Noll & Nickel
6	17	1588	Cataldi	26	23209	1979	Noll
7	19	1588	Cataldi	27	44497	1979	Nelson&Slowinski
8	31	1772	Euler	28	86243	1982	Slowinski
9	61	1883	Pervushin	29	110503	1988	Colquilt&Welsh
10	89	1911	Powers	30	132049	1983	Slowinski
11	107	1914	Powers	31	216091	1985	Slowinski
12	127	1876	Lucas	32	756839	1992	Slowinski&Gage
13	521	1952	Robinson	33	859433	1994	Slowinski&Gage
14	607	1952	Robinson	34	1257787	1996	Slowinski&Gage
15	1279	1952	Robinson	35	1398269	1996	Armengudad,et.al.
16	2203	1952	Robinson	36	2976221	1997	Spence,et.al.
17	2281	1952	Robinson	37	3021377	1998	Claekson,et.al
18	3217	1957	Riesel	38	6972593	1999	Hajaratwala,et.al.
19	4253	1961	Herwitz	39	13466917	2001	Kurowski,et.al.
20	4423	1961	Herwitz	40	20996011	2003	Shafer,et.al.

ที่มา : Mersenne Primes : History, Theorems and Lists.

<http://www.utm.edu/research/primes/mersenne.shtml>

ทฤษฎีบท 4.4.2 ถ้า p และ $q = 2p + 1$ เป็นจำนวนเฉพาะ แล้ว $q \mid M_p$ หรือ $q \mid (M_p + 2)$ อย่างใดอย่างหนึ่งเพียงอย่างเดียวเท่านั้น

ทฤษฎีบท 4.4.3 ถ้า p เป็นจำนวนเฉพาะคี่ แล้วตัวหารของ M_p จะต้องเขียนอยู่ในรูป $2kp + 1$

- ตัวอย่าง 1 (1) พิจารณา $M_{17} = 2^{17} - 1 = 131071$ พบว่าจำนวนเต็มที่เป็นตัวหารของ M_{17} จะต้องเขียนอยู่ในรูป $2k(17) + 1 = 34k + 1$
- (2) พิจารณา $M_{23} = 2^{23} - 1$ พบว่าจำนวนเต็มที่เป็นตัวหารของ M_{23} จะต้องเขียนอยู่ในรูป $2k(23) + 1 = 46k + 1$ □

ตัวอย่าง 2 จงแสดงว่า จำนวนเฉพาะแมร์เซน M_{13} เป็นจำนวนเฉพาะ

วิธีทำ เนื่องจาก $M_{13} = 2^{13} - 1 = 8191$ และ $\sqrt{8191} \leq 91$

ดังนั้น ตัวหารของ M_{13} ที่เขียนอยู่ในรูป $2kp + 1 = 2k(13) + 1 = 26k + 1$

ซึ่งมีค่าน้อยกว่า 91 คือ 53 และ 79 ซึ่งเราพบว่า $53 \nmid 8191$ และ $79 \nmid 8191$

เพราะฉะนั้น M_{13} เป็นจำนวนเฉพาะ □

ปัญหา 3 จงแสดงว่า จำนวนแมร์เซน M_{23} เป็นจำนวนประกอบ

โจทย์ปัญหา 4.4

1. จงแสดงว่า M_{19} เป็นจำนวนเฉพาะ
2. จงแสดงว่า M_9 , M_{14} , M_{15} และ M_{20} เป็นจำนวนประกอบ
3. จงตรวจสอบว่า M_{M_5} เป็นจำนวนเฉพาะหรือไม่

โจทย์ปัญหาเสริมเรื่อง ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ

ปัญหา 1 มีสูตรในการหาจำนวนเฉพาะหรือไม่

วิธีทำ นักคณิตศาสตร์ได้พยายามคิดค้นหาสูตรที่ให้แต่จำนวนเฉพาะหลายสูตร เช่น

สูตรที่ 1 $f(n) = n^2 - n + 41$ จะเป็นจำนวนเฉพาะเมื่อแทน n ด้วย $0, 1, 2, 3, \dots, 40$

ถ้า $n = 0$ จะได้ $f(0) = 41$ เป็นจำนวนเฉพาะ

ถ้า $n = 1$ จะได้ $f(1) = 41$ เป็นจำนวนเฉพาะ

ถ้า $n = 2$ จะได้ $f(2) = 43$ เป็นจำนวนเฉพาะ

ถ้า $n = 3$ จะได้ $f(3) = 47$ เป็นจำนวนเฉพาะ

ถ้า $n = 4$ จะได้ $f(4) = 53$ เป็นจำนวนเฉพาะ

⋮

ถ้า $n = 40$ จะได้ $f(40) = 1601$ เป็นจำนวนเฉพาะ

แต่ถ้า $n = 41$ จะได้ $f(41) = (41)^2 = 1681$ ซึ่งเป็นจำนวนประกอบ เพราะสามารถหารด้วย 41 ลงตัว

สูตรที่ 2 $f(n) = n^2 + n + 17$ จะเป็นจำนวนเฉพาะเมื่อแทน n ด้วย $0, 1, 2, 3, \dots, 15$

แต่ถ้าแทน n ด้วย 16 จะได้ $f(16) = 289$ ซึ่งไม่เป็นจำนวนเฉพาะ เพราะสามารถหารด้วย 17 ลงตัว

สูตรที่ 3 $f(n) = n^2 - 79n + 1601$

จะเป็นจำนวนเฉพาะเมื่อแทน n ด้วย $0, 1, 2, 3, \dots, 79$

แต่ถ้าแทน n ด้วย 80

จะได้ $f(80) = 1681$ ซึ่งไม่เป็นจำนวนเฉพาะ เพราะสามารถหารด้วย 41 ลงตัว

จากสูตรที่ 1 ถึงสูตรที่ 3 เราพบว่าฟังก์ชันพหุนามบางฟังก์ชันสามารถกำหนดจำนวนเฉพาะได้บางค่าของ n คำถามที่น่าสนใจคือ “มีฟังก์ชันพหุนามซึ่งเมื่อแทน n ด้วยจำนวนเต็ม $0, 1, 2, 3, \dots$ แล้วได้ผลลัพธ์เป็นจำนวนเฉพาะเสมอ หรือไม่” คำตอบ คือ ไม่ ซึ่งคำตอบนี้ได้มีการพิสูจน์แล้วว่า “ไม่มีฟังก์ชันพหุนามใดที่มีสมบัติเป็นจำนวนเต็ม ซึ่งเมื่อแทน n ด้วย $0, 1, 2, 3, \dots$ แล้วได้ผลลัพธ์เป็นจำนวนเฉพาะ” (Ore 1948 : 69)

ในปี ค.ศ. 1947 มิลส์ (W. H. Mills) นักคณิตศาสตร์ชาวอเมริกัน ได้พิสูจน์ว่า “มีจำนวนจริง r ซึ่งฟังก์ชัน $f(n) = \lfloor r^{3^n} \rfloor$ ให้ผลลัพธ์เป็นจำนวนเฉพาะเสมอ เมื่อแทน n ด้วย $1, 2, 3, \dots$ ” ($\lfloor r^{3^n} \rfloor$ หมายถึงจำนวนเต็มที่ยกขึ้นน้อยกว่าหรือเท่ากับ r^{3^n}) แต่อย่างไรก็ดีการพิสูจน์ข้อความนี้ได้แสดงเพียงว่ามีจำนวนจริง r ดังกล่าวแต่ไม่อาจจะระบุว่า r คือจำนวนจริงใด (Barnett 1972 : 9)

แม้ไม่มีสูตรในการหาจำนวนเฉพาะ ในปี ค.ศ. 1964 เฮอรวิทซ์ (Alexander Hurwitz) และ เซลฟริดจ์ (John H. Selfridge) นักคณิตศาสตร์ชาวอเมริกัน ได้ค้นพบว่า $2^{11213} - 1$ เป็นจำนวนเฉพาะและประกอบด้วยเลขโดดประมาณ 3,400 หลัก

นักคณิตศาสตร์ได้ศึกษาค้นคว้าเรื่องราวเกี่ยวกับจำนวนเฉพาะอีกมากมาย ซึ่งเป็นข้อเสนอมหรือข้อคาดเดา เช่น ในปี ค.ศ. 1509 เดอ โบเวล (De Bouvelle) ตั้งข้อคาดเดาว่า “สำหรับจำนวนเต็ม n ทุกตัวซึ่ง $n > 1$ จะได้ว่า $6n + 1$ หรือ $6n - 1$ จะเป็นจำนวนเฉพาะจำนวนใดจำนวนหนึ่งหรือทั้งคู่” ซึ่งข้อคาดเดานี้เป็นเท็จ เช่น เมื่อ $n = 97$ จะได้ $6(97) + 1 = 583$ เป็นจำนวนประกอบ และ $6(97) - 1 = 581$ เป็นจำนวนประกอบ ในปี ค.ศ. 1556 ทาร์ทาเกลีย (Tartaglia) ตั้งข้อคาดเดาว่า

“ $1 + 2 + 4$, $1 + 2 + 4 + 8$, $1 + 2 + 4 + 8 + 16$, ... มีผลเป็นจำนวนเฉพาะสลับกับจำนวนประกอบ” ซึ่งข้อคาดเดานี้เป็นเท็จ เมื่อ

$$1 + 2 + 4 + 8 + 16 + 32 + 64 + 128 = 255 \text{ เป็นจำนวนประกอบ}$$

$$\text{และ } 1 + 2 + 4 + 8 + 16 + 32 + 64 + 128 + 256 = 511 \text{ เป็นจำนวนประกอบ} \quad \square$$

ปัญหา 2 จำนวนเต็มเรพูนิต (*Repunit integer*) คือจำนวนเต็มที่อยู่ในรูปของ 1 เขียนเรียงกัน เช่น 1, 11, 111, 1111, ... ซึ่งจะเขียนแทนด้วย

$$R_n = 111\dots111 \text{ (} n \text{ ตัว)}$$

ซึ่งมีตัวอย่างการเขียนดังนี้

$$R_2 = 11, R_3 = 111, R_4 = 1111, R_5 = 11111, R_6 = 111111, \dots$$

เราพบว่าจำนวนเฉพาะที่เขียนอยู่ในรูปดังกล่าว ซึ่งจะเรียกว่าจำนวนเฉพาะเรพูนิต

และได้มีข้อคาดเดาว่า จำนวนเต็มเรพูนิต R_n จะเป็นจำนวนเฉพาะเมื่อ n เป็นจำนวนเฉพาะ

แต่คำกล่าวนี้เป็นเท็จ เมื่อพบว่า $R_5 = 11111 = 417 \cdot 271$

$$\text{และ } R_7 = 1111111 = 239 \cdot 4649$$

และเป็นจริงสำหรับ $R_2, R_{19}, R_{23}, R_{317}$ และ R_{1031}

จากความรู้เรื่องจำนวนเรพูนิต จงแสดงว่า

$$(2.1) \quad R_{10} \text{ เป็นจำนวนประกอบ}$$

$$(2.2) \quad \text{ถ้า } n \mid m \text{ แล้ว } R_n \mid R_m$$

$$\begin{aligned} (\text{ข้อเสนอแนะ}) \quad x^m - 1 &= (x^n - 1)(x^{(k-1)n} + x^{(k-2)n} + \dots + x^2 + x + 1) \\ &\text{เมื่อ } m = kn \end{aligned}$$

$$(2.3) \quad \text{ถ้า } d \mid R_n \text{ และ } d \mid R_m \text{ แล้ว } d \mid R_{m+n}$$

$$(\text{ข้อเสนอแนะ}) \quad R_{m+n} = R_m 10^n + R_n$$

$$(2.4) \quad \text{ถ้า } (m, n) = 1 \text{ แล้ว } (R_m, R_n) = 1$$

ปัญหา 3 ในการเขียน $1000!$ ในรูปของจำนวนเต็มจะมี 0 ลงท้ายเรียงต่อเนื่องกันกี่ตัว

วิธีทำ จาก $n! = n(n-1)(n-2)(n-3) \cdots 3 \cdot 2 \cdot 1$

พิจารณา $20! = 2,432,902,008,176,640,000$

เห็นได้ชัดว่าในการเขียน $20!$ ในรูปของจำนวนเต็มจะมี 0 ลงท้ายเรียงกันต่อเนื่อง 4 ตัว

ในการหาคำตอบนี้ค่อนข้างเสียเวลา เพราะจะต้องหาคำของ $20!$ ซึ่งถ้าเราต้องการทราบว่า $1000!$ เมื่อเขียนในรูปของจำนวนเต็มจะมี 0 ลงท้ายเรียงกันต่อเนื่องกี่ตัวนั้น การใช้วิธีการเดิมหาคำตอบค่อนข้างลำบาก ดังนั้นเราจะใช้สูตรของเลอจองด์ (Legendre's formula) ในการช่วยหาคำตอบ ดังรายละเอียดต่อไปนี้

สูตรของเลอจองด์ เลขยกกำลังของจำนวนเฉพาะ p ที่เกิดจากการเขียน $n!$ ในรูปผลคูณของจำนวนเฉพาะ ($n! = p^k M$ ซึ่ง $p \nmid M$) คือ

$$k = \sum_{r \geq 1} \left\lfloor \frac{n}{p^r} \right\rfloor = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \cdots$$

เช่นต้องการหาเลขยกกำลังของ 5 ที่เกิดจากการเขียน $100!$ ในรูปผลคูณของจำนวนเฉพาะ

พิจารณา $100! = 5^k M$ ซึ่ง $5 \nmid M$

$$\begin{aligned} \text{จะได้ว่า } k &= \sum_{r \geq 1} \left\lfloor \frac{100}{5^r} \right\rfloor = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor + \left\lfloor \frac{100}{5^3} \right\rfloor + \left\lfloor \frac{100}{5^4} \right\rfloor + \cdots \\ &= 20 + 4 + 0 + 0 + \cdots = 24 \end{aligned}$$

ดังนั้นในการหาคำตอบของการเขียน $1000!$ ในรูปของจำนวนเต็มว่าจะมี 0 เรียง ต่อเนื่องกันกี่ตัวนั้น เป็นการเพียงพอที่จะหาเลขยกกำลังของ 5 เพราะว่า 0 ลงท้าย 1 ตัวเกิดจาก 5×2 แต่เลขยกกำลังของ 5 จะน้อยกว่าหรือเท่ากับเลขยกกำลังของ 2 เสมอ

ให้ $1000! = 5^k M$ ซึ่ง $5 \nmid M$

$$\begin{aligned} \text{จะได้ว่า } k &= \sum_{r \geq 1} \left\lfloor \frac{1000}{5^r} \right\rfloor = \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor + \cdots \\ &= 200 + 40 + 8 + 1 \\ &= 249 \end{aligned}$$

ดังนั้น การเขียน $1000!$ ในรูปของจำนวนเต็มจะมี 0 ลงท้ายเรียงต่อเนื่องกัน 249 ตัว □

ปัญหา 4 ถ้า $n = p^r q$ ซึ่ง p และ q เป็นจำนวนเฉพาะ

จงหาจำนวนของจำนวนเต็มบวก k ทั้งหมดซึ่ง $1 \leq k < n$ และ $(n, k) = 1$

แบบฝึกหัดเรื่อง

ข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ

1. จงตรวจสอบว่า มีจำนวนเฉพาะที่อยู่ในรูป $1^{1995} + 2^{1995} + 3^{1995} + \dots + n^{1995}$ เมื่อ n เป็นจำนวนเต็มบวกหรือไม่
2. ให้ p_n เป็นจำนวนเฉพาะตัวที่ n สำหรับ $n > 3$ จงแสดงว่า

$$p_n < p_1 + p_2 + p_3 + \dots + p_{n-1}$$
 (ข้อเสนอแนะ ให้หลักอุปนัยเชิงคณิตศาสตร์และข้อคาดเดาของเบอร์ทราน)
3. ถ้า $n > 1$ แล้วจงแสดงว่า $n!$ ไม่เป็นกำลังสองสมบูรณ์
4. จงพิสูจน์ว่า ถ้า $n \geq 2$ แล้วจะมีจำนวนเฉพาะ p ซึ่ง $p \leq n \leq 2p$
 (ข้อเสนอแนะ ในกรณีที่ $n = 2k + 1$ แล้วข้อคาดเดาของเบอร์ทรานจะมีจำนวนเฉพาะ p ซึ่ง $k < p < 2k$)
5. จงใช้ผลจากทฤษฎีบท 4.1.4 พิสูจน์ว่า $p_n < 2^n$ เมื่อ p_n คือจำนวนเฉพาะตัวที่ n
6. ให้ p_n เป็นจำนวนเฉพาะตัวที่ n สำหรับ $n \geq 3$ จงพิสูจน์ว่า $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$
 (ข้อเสนอแนะ $p_{n+3}^2 < 4p_{n+2}^2 < 8p_{n+1}p_{n+2}$)
7. จงแสดงว่า จำนวนแฟร์มาต์ไม่เป็นกำลังสองสมบูรณ์
8. สำหรับจำนวนเต็มคี่ n จงแสดงว่า $3 \mid (2^n + 1)$
9. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $n! + (n+1)! + (n+2)!$ เป็นกำลังสองสมบูรณ์
 (ข้อเสนอแนะ $n! + (n+1)! + (n+2)! = n!(n+2)^2$)
10. ข้อคาดเดา ทุก ๆ จำนวนเต็มคี่สามารถเขียนอยู่ในรูป $p + 2a^2$ เมื่อ p เป็นจำนวนเฉพาะ หรือ 1 และ $a \geq 0$
 จงแสดงว่า จำนวนเต็ม 5777 เป็นตัวอย่างค้านของข้อคาดเดานี้
 กล่าวคือ 5777 ไม่สามารถเขียนในรูปของ $p + 2a^2$ ได้
11. ข้อคาดเดาของลากรองจ์ ทุก ๆ จำนวนเต็มคี่ที่มากกว่า 5 สามารถเขียนให้อยู่ในรูปผลบวก $p_1 + 2p_2$ เมื่อ p_1 และ p_2 เป็นจำนวนเฉพาะ
 จงแสดงว่า ข้อคาดเดาข้างต้นเป็นจริงสำหรับทุก ๆ จำนวนเต็มคี่ n ซึ่ง $5 < n \leq 75$
12. จำนวนเต็มบวก $p, p+2, p+6$ ซึ่งต่างก็เป็นจำนวนเฉพาะทั้งหมดเรียกว่า *prime-triplet*
 จงหา prime-triplet มา 5 ชุด
13. ในปี ค.ศ. 1848 De Polignance ได้เสนอข้อคาดเดาว่า
 “จำนวนเต็มคี่ทุกจำนวนสามารถเขียนได้ในรูปผลบวกของจำนวนเฉพาะกับเลข 2 ยกกำลัง”
 เช่น $55 = 47 + 2^3 = 23 + 2^5$
 จงแสดงว่า 509 และ 877 ไม่สอดคล้องกับข้อคาดเดานี้

- 14 . จงยกตัวอย่างการเขียนจำนวนเต็มคู่บวก $n \geq 1000$ ให้อยู่ในรูปผลบวกของจำนวนเฉพาะ 2 จำนวน มา 50 ตัวอย่าง
15. จงหาจำนวนเฉพาะ p ทั้งหมดที่ทำให้ $p \mid (2^p + 1)$
และหาจำนวนเฉพาะ q ทั้งหมดที่ทำให้ $q \mid (2^q - 1)$
16. เรียกจำนวนประกอบ n ซึ่ง $n \mid (2^n - 2)$ ว่า จำนวนเฉพาะเทียม (Pseudoprime) จงแสดงว่า ถ้า n เป็นจำนวนเต็มคี่ที่เป็นจำนวนเฉพาะเทียม แล้วจำนวนเมอร์แซน M_n จะเป็นจำนวนเฉพาะเทียมด้วย และจงแสดงว่ามีจำนวนเฉพาะเทียมไม่จำกัดจำนวน
(ข้อเสนอแนะ ใช้ $n \mid (2^n - 2)$ และ $n \mid (2^{n-1} - 2)$ ซึ่ง $2^{n-1} - 1 = kn$
เมื่อ $k \in \mathbb{Z}$ แล้ว $2^{M_n-1} - 1 = 2^{2^n-2} - 1 = (2^n)^{2k} - 1$
จะได้ว่า $(2^n - 1) \mid 2 \cdot (2^{M_n-1} - 1)$)
17. จงตรวจสอบว่า ถ้า p และ $q = p + 2$ เป็นจำนวนเฉพาะแล้ว $pq - 2$ เป็นจำนวนเฉพาะหรือไม่

บทที่ 5

ฟังก์ชันเลขคณิต

ในบทนี้เราจะกล่าวถึงฟังก์ชันที่มีโดเมนเป็นเซตของจำนวนเต็มบวก และเรนจ์เป็นสับเซตของจำนวนเชิงซ้อน ซึ่งเราจะเรียกฟังก์ชันในลักษณะเช่นนี้ว่า **ฟังก์ชันเลขคณิต** (Arithmetic function) โดยสิ่งที่เราสนใจจะศึกษาก็คือสมบัติพิเศษของแต่ละฟังก์ชัน ฟังก์ชันเลขคณิตมีการศึกษากันอย่างกว้างขวางในแง่ของฟังก์ชันค่าเชิงซ้อน (complex-valued function) ในการศึกษาฟังก์ชันเลขคณิตเบื้องต้นนี้ เรามีวัตถุประสงค์เพื่อแนะนำฟังก์ชันเลขคณิตบางฟังก์ชันที่เป็นประโยชน์ในเชิงการนับ (combinatorics) และฟังก์ชันเลขคณิตที่จะกล่าวถึงในที่นี้จะเป็นฟังก์ชันที่เห็นบทประยุกต์มากมายในการศึกษาทฤษฎีจำนวน

ตัวอย่าง ฟังก์ชันต่อไปนี้ เป็นฟังก์ชันเลขคณิต

1. $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = 0$
2. $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = 1$
3. $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = n$
4. $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = 1 - n$
5. $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = n^2 + 40n - 41$
6. $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) =$ จำนวนตัวประกอบเฉพาะของ n
7. $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) =$ จำนวนของจำนวนเฉพาะที่น้อยกว่า n
8. $\lambda: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย

$$\lambda(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ (-1)^{a_1 + a_2 + \cdots + a_k} & \text{ถ้า } n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k} \\ & \text{โดยที่ } p_i \text{ เป็นจำนวนเฉพาะที่แตกต่างกัน} \end{cases}$$

เราจะเรียกฟังก์ชัน λ นี้ว่า **ฟังก์ชันลิอูวิลล์** (Liouville's function)

9. $A: \mathbb{N} \rightarrow \mathbb{R}$ กำหนดโดย

$$A(n) = \begin{cases} \log p & \text{ถ้า } n = p^a \text{ โดยที่ } p \text{ เป็นจำนวนเฉพาะและ } a \in \mathbb{N} \\ 0 & \text{ถ้า } n \text{ เขียนได้ในรูปอื่น ๆ ที่ไม่ใช่ } p^a \end{cases}$$

เราจะเรียกฟังก์ชัน A นี้ว่า ฟังก์ชันมานเกอลต์ (Mangoldt's function)

10. $\mu: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย

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

เราจะเรียกฟังก์ชัน μ นี้ว่า ฟังก์ชันเมอบิอุส (Möbius function)

ฟังก์ชันต่อไปนี้ไม่เป็นฟังก์ชันเลขคณิต

11. $f: \mathbb{R} \rightarrow \mathbb{R}$ กำหนดโดย $f(n) = n$

12. $f: \mathbb{Q} \rightarrow \mathbb{R}$ กำหนดโดย $f(n) = n^2$

13. $f: \mathbb{R} \rightarrow \mathbb{C}$. กำหนดโดย $f(n) = ni$

14. $f: \mathbb{R} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) =$ จำนวนเต็มที่มีค่ามากที่สุดแต่น้อยกว่า n

15. $f: \mathbb{Z} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) =$ จำนวนตัวประกอบของ n

5.1 ฟังก์ชันแยกคูณ

บทนิยาม 5.1.1 เราเรียกฟังก์ชันเลขคณิต f ว่าเป็น ฟังก์ชันแยกคูณ (multiplicative function) ก็ต่อเมื่อ $f(mn) = f(m)f(n)$ สำหรับทุก $m, n \in \mathbb{N}$ และ $(m, n) = 1$

ตัวอย่าง 1 ฟังก์ชันต่อไปนี้ เป็น ฟังก์ชันแยกคูณ

(1.1) $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = 0$

(1.2) $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = 1$

(1.3) $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = n$

(1.4) $I: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $I(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้า } n \neq 1 \end{cases}$

(1.5) $f: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย $f(n) = n^2$

□

ตัวอย่าง 2 ฟังก์ชันต่อไปนี้ไม่ใช่ฟังก์ชันแยกคูณ

$$(2.1) \quad f: \mathbb{N} \rightarrow \mathbb{Z} \quad \text{กำหนดโดย} \quad f(n) = 3$$

$$(2.1) \quad f: \mathbb{N} \rightarrow \mathbb{Z} \quad \text{กำหนดโดย} \quad f(n) = 2n + 1$$

$$(2.3) \quad f: \mathbb{N} \rightarrow \mathbb{Z} \quad \text{กำหนดโดย} \quad f(n) = n^2 + 2n$$

$$(2.4) \quad f: \mathbb{N} \rightarrow \mathbb{Z} \quad \text{กำหนดโดย} \quad f(n) = \text{จำนวนตัวประกอบเฉพาะของ } n$$

$$(2.5) \quad f: \mathbb{N} \rightarrow \mathbb{Z} \quad \text{กำหนดโดย} \quad f(n) = \text{จำนวนของจำนวนเฉพาะที่น้อยกว่า } n$$

□

ตัวอย่าง 3 จงแสดงว่า ฟังก์ชันลิวอิสเป็นฟังก์ชันแยกคูณ

บทพิสูจน์ ให้ $m, n \in \mathbb{N}$ โดยที่ $(m, n) = 1$ จะต้องแสดงว่า $\lambda(mn) = \lambda(m)\lambda(n)$

กรณี 1 ถ้า $m = 1$ หรือ $n = 1$

$$\text{จะได้ว่า} \quad \lambda(mn) = \lambda(n) \text{ หรือ } \lambda(mn) = \lambda(m)$$

$$\text{ดังนั้น} \quad \lambda(mn) = \lambda(m)\lambda(n)$$

กรณี 2 ถ้า $m > 1$ และ $n > 1$ ให้ $m = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$ และ

$n = q_1^{b_1} q_2^{b_2} q_3^{b_3} \cdots q_r^{b_r}$ เป็นการเขียนแทน m, n ในรูปแบบบัญญัติ จะได้ว่า

$$\lambda(mn) = (-1)^{(a_1 + a_2 + \cdots + a_k) + (b_1 + b_2 + \cdots + b_r)}$$

$$= (-1)^{a_1 + a_2 + \cdots + a_k} \cdot (-1)^{b_1 + b_2 + \cdots + b_r}$$

$$= \lambda(m)\lambda(n)$$

จากทั้งสองกรณีสรุปได้ว่า λ เป็นฟังก์ชันแยกคูณ

□

ปัญหา 4 จงตรวจสอบว่า ฟังก์ชันมานเกอลท์และฟังก์ชันเมอบิอุสเป็นฟังก์ชันแยกคูณหรือไม่

บทนิยาม 5.1.2 เราเรียกฟังก์ชันเลขคณิต f ว่าเป็น ฟังก์ชันแยกคูณแบบบริบูรณ์ (completely multiplicative function) ก็ต่อเมื่อ

$$f(mn) = f(m)f(n) \quad \text{สำหรับทุก } m, n \in \mathbb{N}$$

ตัวอย่าง 5 ฟังก์ชัน f ที่กำหนดในข้อ (1.1) – (1.5) ของตัวอย่าง 1 เป็นฟังก์ชันแยกคูณแบบบริบูรณ์

□

ตัวอย่าง 6 จงแสดงว่าฟังก์ชันมานเกอลท์ไม่ใช่ฟังก์ชันแยกคูณแบบบริบูรณ์

บทพิสูจน์ เนื่องจาก $A(4) = A(2^2) = \log 2$ และ $A(2)A(2) = (\log 2)^2$

$$\text{ดังนั้น} \quad A(4) \neq A(2)A(2)$$

จึงสรุปได้ว่า ฟังก์ชัน A ไม่ใช่ฟังก์ชันแยกคูณแบบบริบูรณ์

□

ปัญหา 7 จงตรวจสอบว่าฟังก์ชันลิวอิสและฟังก์ชันเมอบิอุสเป็นฟังก์ชันแยกคูณแบบบริบูรณ์หรือไม่

บทนิยาม 5.1.3 เราเรียกฟังก์ชันเลขคณิต f ว่าเป็น ฟังก์ชันแยกบวก (additive function) ก็ต่อเมื่อ $f(mn) = f(m) + f(n)$ สำหรับทุก $m, n \in \mathbb{N}$ และ $(m, n) = 1$

บทนิยาม 5.1.4 เราเรียกฟังก์ชันเลขคณิต f ว่าเป็น ฟังก์ชันแยกบวกแบบบริบูรณ์ (completely additive function) ก็ต่อเมื่อ

$$f(mn) = f(m) + f(n) \quad \text{สำหรับทุก } m, n \in \mathbb{N}$$

ตัวอย่าง 8 ฟังก์ชันต่อไปนี้ เป็นฟังก์ชันแยกบวก

$$(8.1) \quad f: \mathbb{N} \rightarrow \mathbb{Z} \quad \text{กำหนดโดย} \quad f(n) = 0$$

$$(8.2) \quad f: \mathbb{N} \rightarrow \mathbb{Z} \quad \text{กำหนดโดย} \quad f(n) = \log n$$

$$(8.3) \quad f: \mathbb{N} \rightarrow \mathbb{Z} \quad \text{กำหนดโดย} \quad f(n) = \text{จำนวนตัวประกอบเฉพาะของ } n \quad \square$$

ปัญหา 9 จงตรวจสอบว่าฟังก์ชันลิอูวิลล์, ฟังก์ชันมานเกอลท์ และฟังก์ชันเมอบิอุสเป็นฟังก์ชันแยกบวกหรือไม่

ปัญหา 10 จงยกตัวอย่างฟังก์ชันแยกบวกแบบบริบูรณ์มา 2 ตัวอย่าง

หมายเหตุ ให้ f เป็นฟังก์ชันแบบแยกคูณ เราพบว่า

$$f(1) = f(1 \cdot 1) = f(1)f(1) = [f(1)]^2$$

$$\text{ดังนั้น} \quad [f(1)]^2 - f(1) = f(1)(f(1) - 1) = 0$$

$$\text{นั่นคือ} \quad f(1) = 0 \quad \text{หรือ} \quad f(1) = 1$$

ในกรณีที่ f เป็นฟังก์ชันแยกคูณและ $f(1) = 0$ จะได้ว่า ทุก ๆ จำนวนเต็มบวก n

$$f(n) = f(n \cdot 1) = f(n)f(1) = 0$$

นี่คือการแสดงว่า ฟังก์ชันแยกคูณ f ที่ $f(1) = 0$ จะมีเพียงฟังก์ชันเดียวคือฟังก์ชัน f ซึ่ง

$$f(n) = 0 \quad \text{ทุก } n \in \mathbb{N}$$

ดังนั้น ในการกล่าวถึงฟังก์ชันแยกคูณ f ให้เป็นที่เข้าใจว่า เราสนใจเฉพาะฟังก์ชัน f ซึ่ง $f(1) = 1$ เท่านั้น

ในกรณีที่ f เป็นฟังก์ชันแยกบวก เราพบว่า

$$f(1) = f(1 \cdot 1) = f(1) + f(1)$$

$$\text{นั่นคือ} \quad f(1) = 0$$

ดังนั้น ในการกล่าวถึงฟังก์ชันแยกบวก f เราสามารถสรุปได้ว่า $f(1) = 0$ เสมอ

ทฤษฎีบท 5.1.5 ให้ f เป็นฟังก์ชันเลขคณิต โดยที่ $f(1) = 1$ และ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

เป็นการเขียนแทน n ในรูปแบบบัญญัติ จะได้ว่า f เป็นฟังก์ชันแยกคูณ ก็ต่อเมื่อ

$$f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}) \quad \text{สำหรับทุกจำนวนเต็มบวก } k$$

บทพิสูจน์ $(\Rightarrow)$ จะพิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์

(i) ถ้า $k = 2$ โดยบทนิยาม 5.1.1

$$\text{จะได้ว่า } f(p_1^{a_1} p_2^{a_2}) = f(p_1^{a_1}) f(p_2^{a_2})$$

(ii) สมมติว่า $f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k})$ เป็นจริง จะได้ว่า

$$\begin{aligned} f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} p_{k+1}^{a_{k+1}}) &= f((p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) p_{k+1}^{a_{k+1}}) \\ &= f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) f(p_{k+1}^{a_{k+1}}) \\ &= f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}) f(p_{k+1}^{a_{k+1}}) \end{aligned}$$

จาก (i) และ (ii) สรุปได้ว่า

$$f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k})$$

เป็นจริงสำหรับทุกจำนวนเต็มบวก k

$(\Leftarrow)$ ให้ $m, n \in \mathbb{N}$ โดยที่ $(m, n) = 1$

กรณี 1 ถ้า $m = 1$ หรือ $n = 1$

$$\text{จะได้ว่า } f(mn) = f(n) \text{ หรือ } f(mn) = f(m)$$

$$\text{ดังนั้น } f(mn) = f(m) f(n)$$

กรณี 2 ถ้า $m > 1$ และ $n > 1$

$$\text{ให้ } m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ และ}$$

$$n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s} \text{ เป็นการเขียนแทน } m, n \text{ ในรูปแบบบัญญัติ}$$

$$\text{จะได้ว่า } mn = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

เป็นการเขียนแทน mn ในรูปแบบบัญญัติ และ

$$\begin{aligned} f(mn) &= f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_r^{a_r}) f(q_1^{b_1}) f(q_2^{b_2}) \cdots f(q_s^{b_s}) \\ &= f(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) f(q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}) \\ &= f(m) f(n) \end{aligned}$$

จากทั้งสองกรณีสรุปได้ว่า f เป็นฟังก์ชันแยกคูณ ■

ทฤษฎีบท 5.1.6 ให้ f เป็นฟังก์ชันเลขคณิต โดยที่ $f(1) = 1$ และ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ จะได้ว่า f เป็นฟังก์ชันแยกคูณแบบบริบูรณ์ ก็ต่อเมื่อ

$$f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = f(p_1)^{a_1} f(p_2)^{a_2} \cdots f(p_k)^{a_k} \text{ สำหรับทุกจำนวนเต็มบวก } k$$

บทพิสูจน์ ทำนองเดียวกับการพิสูจน์ทฤษฎีบท 5.1.5 จึงเว้นไว้เป็นแบบฝึกหัด ■

บทแทรก 5.1.7 ให้ f เป็นฟังก์ชันแยกคูณโดยที่ $f(1) = 1$ และ $n \in \mathbb{N}$ จะได้ว่า

$$f \text{ เป็นฟังก์ชันแยกคูณแบบบริบูรณ์ ก็ต่อเมื่อ } f(p^m) = f(p)^m$$

โดยที่ p เป็นจำนวนเฉพาะซึ่ง $p \mid n$ และ $m \in \mathbb{N}$

หมายเหตุ ให้ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ จะได้ว่า

- (1) ถ้า f เป็นฟังก์ชันแยกคูณ แล้วการหาค่า $f(n)$ นั้นขึ้นกับการหาค่าของ $f(p_i^{a_i})$ สำหรับทุก $i = 1, 2, 3, \dots, k$
- (2) ถ้า f เป็นฟังก์ชันแยกคูณแบบบริบูรณ์ แล้วการหาค่า $f(n)$ นั้นขึ้นอยู่กับค่าของ $f(p_i)$ สำหรับทุก $i = 1, 2, 3, \dots, k$

โจทย์ปัญหา 5.1

1. จงพิสูจน์ว่า ถ้า f และ g เป็นฟังก์ชันแยกคูณแล้ว fg และ $\frac{f}{g}$ เป็นฟังก์ชันแยกคูณ

(ในกรณีที่ค่าของฟังก์ชัน g ไม่เท่ากับศูนย์)

2. ให้ $\nu: \mathbb{N} \rightarrow \mathbb{Z}$ กำหนดโดย

$$\nu(n) = \begin{cases} 0 & \text{ถ้า } n = 1 \\ k & \text{ถ้า } n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \end{cases}$$

โดยที่ p_i เป็นจำนวนเฉพาะที่แตกต่างกันและ $a_i \in \mathbb{N}$

จงพิสูจน์ว่า ฟังก์ชัน ν เป็นฟังก์ชันแยกบวก

3. ให้ f และ g เป็นฟังก์ชันเลขคณิต และ $n \in \mathbb{N}$

นิยาม ผลคูณดิริชเลต์ (Dirichlet product) ของ f และ g เขียนแทนด้วย $f * g$ โดย

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

จงพิสูจน์ว่า ถ้า f และ g เป็นฟังก์ชันแยกคูณ แล้ว $f * g$ เป็นฟังก์ชันแยกคูณ

4. จากข้อ 3. จงพิสูจน์ว่า ถ้า g และ $f * g$ เป็นฟังก์ชันแยกคูณ แล้ว f เป็นฟังก์ชันแยกคูณ
5. ให้ f และ g เป็นฟังก์ชันแยกคูณ จงพิสูจน์ว่า $f = g$ ก็ต่อเมื่อ $f(p^a) = g(p^a)$ สำหรับทุกจำนวนเฉพาะ p และทุกจำนวนเต็มบวก a
6. จงหาฟังก์ชันแยกคูณ f และ g ซึ่ง $f \neq g$ แต่ $f(p) = g(p)$ สำหรับทุกจำนวนเฉพาะ p

5.2 ฟังก์ชัน τ

การศึกษาเกี่ยวกับการหารลงตัวในระบบจำนวนเต็ม เราพบว่าถ้า a เป็นตัวหารของ b จะได้ว่ามี $c \in \mathbb{Z}$ ที่ทำให้ $b = ac$ นอกจากนั้นเราก็ได้ว่า c ก็เป็นตัวหารของ b ด้วย ถ้า a เป็นตัวหารของ b จะได้ว่า $-a$ ก็จะเป็นตัวหารของ b ด้วยเช่นกัน

ในการหาตัวหารทั้งหมดของจำนวนเต็มบวก n เราอาจสนใจเฉพาะตัวหารที่เป็นบวกเท่านั้น ดังนั้น จากนี้เป็นต้นไป เมื่อกล่าวถึงตัวหารให้หมายถึงตัวหารที่เป็นบวกเท่านั้น

บทนิยาม 5.2.1 ให้ $n \in \mathbb{N}$ กำหนด

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

เราจะเรียกฟังก์ชัน τ ว่า ฟังก์ชันเทา (tau function)

จากบทนิยามเราพบว่า τ เป็นฟังก์ชันเลขคณิตโดยที่ $\tau(1) = 1$ และ $\tau(n) = \sum_{d|n} 1$

ตัวอย่าง 1 (1.1) ให้ $n = 6$ จะพบว่า ตัวหารทั้งหมดของ 6 คือ 1, 2, 3, 6

$$\text{ดังนั้น } \tau(6) = 4$$

(1.2) ให้ $n = 308$ จะพบว่า ตัวหารทั้งหมดของ 308 คือ 1, 2, 4, 7, 11, 22, 28, 44, 77, 154, 308 ดังนั้น $\tau(308) = 12$

(1.3) ให้ $n = 31752$ จะพบว่า $31752 = 2^3 \cdot 3^4 \cdot 7^2$

$$\text{ดังนั้น ตัวหารทั้งหมดของ } 31752 \text{ คือ } 2^x \cdot 3^y \cdot 7^z$$

$$\text{โดยที่ } x = 0, 1, 2, 3, y = 0, 1, 2, 3, 4 \text{ และ } z = 0, 1, 2$$

$$\text{นั่นคือ } \tau(31752) = 60$$

□

ปัญหา 2 ให้ p และ q เป็นจำนวนเฉพาะที่แตกต่างกัน จงหา

(2.1) $\tau(p)$ และ $\tau(p^k)$ เมื่อ k เป็นจำนวนเต็มบวก

(2.2) $\tau(pq)$ และ $\tau(p^r q^s)$ เมื่อ r และ s เป็นจำนวนเต็มบวก

ทฤษฎีบท 5.2.2 ถ้า p เป็นจำนวนเฉพาะและ $n = p^a$, $a \geq 1$ จะได้ว่า

$$\tau(n) = a + 1$$

บทพิสูจน์ จาก $n = p^a$ เราพบว่าตัวหารทั้งหมดของ n คือ 1, p , p^2 , ..., p^a

$$\text{นั่นคือ } \tau(n) = \tau(p^a) = a + 1$$

■

ทฤษฎีบท 5.2.3 ถ้า $n \in \mathbb{N}$ โดยที่ $n > 1$ และให้ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ จะได้ว่า

$$\tau(n) = \prod_{i=1}^k (a_i + 1)$$

บทพิสูจน์ ให้ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ และให้

$$D = \{d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \mid b_i \text{ เป็นจำนวนเต็มที่ } 0 \leq b_i \leq a_i, i = 1, 2, 3, \dots, k\}$$

เห็นได้ชัดว่า D คือเซตของตัวหารทั้งหมดของ n

จาก $d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ เป็นตัวหารของ n ก็ต่อเมื่อ $0 \leq b_i \leq a_i$ สำหรับทุก $i = 1, 2, 3, \dots, k$ ดังนั้น ทุก i , $b_i = 0, 1, 2, 3, \dots, a_i$ ซึ่งมีอยู่ $a_i + 1$ ค่า

โดยกฎการนับเบื้องต้น จะได้ว่า

จำนวนสมาชิกทั้งหมดของ D คือ $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$

$$\text{นั่นคือ } \tau(n) = \prod_{i=1}^k (a_i + 1)$$

ทฤษฎีบท 5.2.4 ฟังก์ชัน τ เป็นฟังก์ชันแยกคูณ

บทพิสูจน์ ให้ $m, n \in \mathbb{N}$ โดยที่ $(m, n) = 1$

กรณี 1 ถ้า $m = 1$ หรือ $n = 1$

$$\text{จะได้ว่า } \tau(mn) = \tau(n) \text{ หรือ } \tau(mn) = \tau(m)$$

$$\text{ดังนั้น } \tau(mn) = \tau(m)\tau(n)$$

กรณี 2 ถ้า $m > 1$ และ $n > 1$ ให้ $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ และ

$$n = q_1^{b_1} q_2^{b_2} q_3^{b_3} \cdots q_r^{b_r} \text{ เป็นการเขียนแทน } m, n \text{ ในรูปแบบบัญญัติ}$$

โดยทฤษฎีบท 5.2.3 จะได้ว่า

$$\begin{aligned} \tau(mn) &= (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)(b_1 + 1)(b_2 + 1) \cdots (b_r + 1) \\ &= \tau(m)\tau(n) \end{aligned}$$

จากทั้งสองกรณีสรุปได้ว่า τ เป็นฟังก์ชันแยกคูณ

ปัญหา 3 จงตรวจสอบว่าฟังก์ชัน τ เป็นฟังก์ชันแยกคูณแบบบริบูรณ์หรือไม่ แสดงให้เห็นจริง

ตัวอย่าง 4 (4.1) $\tau(200) = \tau(2^3 \cdot 5^2) = (3 + 1)(2 + 1) = 12$

(4.2) $\tau(720) = \tau(2^4 \cdot 3^2 \cdot 5) = (4 + 1)(2 + 1)(1 + 1) = 30$

(4.3) $\tau(2^5 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11) = (5 + 1)(4 + 1)(3 + 1)(2 + 1)(1 + 1)$
 $= 720$

ตัวอย่าง 5 จงหา $\tau(10001)$, $\tau(10008)$ และ $\tau(100001)$

วิธีทำ $\tau(10001) = \tau(73 \cdot 137) = (1 + 1)(1 + 1) = 4$

$$\tau(10008) = \tau(2^3 \cdot 3^2 \cdot 139) = (3 + 1)(2 + 1)(1 + 1) = 24$$

$$\tau(100001) = \tau(11 \cdot 9091) = (1 + 1)(1 + 1) = 4$$

ตัวอย่าง 6 ให้ $2^k - 1$ เป็นจำนวนเฉพาะและ $n = 2^{k-1}(2^k - 1)$ จงหา $\tau(n)$

วิธีทำ จาก $(2^k - 1, 2^{k-1}) = 1$ และ τ เป็นฟังก์ชันแยกคูณ

$$\begin{aligned} \text{จะได้ว่า } \tau(2^{k-1}(2^k - 1)) &= \tau(2^{k-1})\tau(2^k - 1) \\ &= (k - 1 + 1)(1 + 1) = 2k \end{aligned}$$

โจทย์ปัญหา 5.2

1. จงตรวจสอบว่า $\pi(n) = \pi(n+1) = \pi(n+2) = \pi(n+3)$ เป็นจริงสำหรับ $n = 3655$ และ 4503 หรือไม่
2. จงหาเซตคำตอบของสมการ $\pi(x) = 1$, $\pi(x) = 2$, $\pi(x) = 3$ และ $\pi(x) = 4$
3. จงพิสูจน์ว่า เซตคำตอบของสมการ $\pi(x) = n$ เป็นเซตอนันต์ เมื่อ n เป็นจำนวนเต็มบวกที่มากกว่าหรือเท่ากับ 2
4. สำหรับจำนวนเต็มบวก n จงแสดงว่า $\pi(n) \leq 2\sqrt{n}$
(ข้อเสนอแนะ ถ้า $d|n$ แล้ว $d \leq \sqrt{n}$ หรือ $\frac{n}{d} \leq \sqrt{n}$)
5. จงพิสูจน์ว่า ถ้า $n \in \mathbb{N}$ แล้ว $\pi(n) \leq n$
6. สำหรับจำนวนเต็มบวก n ซึ่ง $n \geq 2$ จงพิสูจน์ว่า มี $n_1, n_2 \in \mathbb{N}$ ที่ทำให้ $\pi(n_1) + \pi(n_2) = n$
7. ให้ $n \in \mathbb{N}$ จงพิสูจน์ว่า $\sum_{d|n} [\pi(d)]^3 = [\sum_{d|n} \pi(d)]^2$
8. ให้ ν เป็นฟังก์ชันที่กำหนดในโจทย์ปัญหา 5.1 ข้อ 2.
จงตรวจสอบว่า $\pi(n^2) = \sum_{d|n} 2^{\nu(d)}$ เป็นจริงหรือไม่
9. ให้ $F(n) = \sum_{d|n} \pi(d)$ จงหา $F(n)$ เมื่อ $n = 1, 2, 3, 4, 6$
10. ให้ $m, n \in \mathbb{N}$ โดยที่ $(m, n) > 1$ จงพิสูจน์ว่า $\pi(mn) < \pi(m)\pi(n)$

5.3 ฟังก์ชัน σ และ σ_k

บทนิยาม 5.3.1 ให้ $n \in \mathbb{N}$ กำหนด

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

เราจะเรียกฟังก์ชัน σ ว่า ฟังก์ชันซิกมา (sigma function)

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

จากบทนิยามเราพบว่า σ และ σ_k ต่างก็เป็นฟังก์ชันเลขคณิต โดยที่ $\sigma(1) = 1$ และ $\sigma_k(1) = 1$ นอกจากนั้น $\sigma(n) = \sum_{d|n} d$ และ $\sigma_k(n) = \sum_{d|n} d^k$

ตัวอย่าง 1 (1.1) ให้ $n = 6$ จะพบว่าตัวหารของ 6 คือ 1, 2, 3, 6

$$\text{ดังนั้น } \sigma(6) = 1 + 2 + 3 + 6 = 12$$

$$\text{และ } \sigma_2(6) = 1^2 + 2^2 + 3^2 + 6^2 = 50$$

(1.2) ให้ $n = 81$ จะพบว่าตัวหารของ 81 คือ 1, 3, 9, 81

$$\text{ดังนั้น } \sigma(81) = 1 + 3 + 9 + 81 = 94$$

$$\text{และ } \sigma_3(81) = 1^3 + 3^3 + 9^3 + 81^3 = 532198$$

□

ตัวอย่าง 2 ให้ p และ q เป็นจำนวนเฉพาะซึ่ง $p \neq q$ จงหา

(2.1) $\sigma(p)$ และ $\sigma(p^k)$ เมื่อ k เป็นจำนวนเต็มบวก

(2.2) $\sigma(pq)$ และ $\sigma(p^\alpha q^\beta)$ เมื่อ α และ β เป็นจำนวนเต็มบวก

วิธีทำ (2.1) พิจารณาตารางข้างล่างต่อไปนี้

p	$1, p$	$1 + p$
p^2	$1, p, p^2$	$1 + p + p^2 = \frac{p^3 - 1}{p - 1}$
p^3	$1, p, p^2, p^3$	$1 + p + p^2 + p^3 = \frac{p^4 - 1}{p - 1}$
p^4	$1, p, p^2, p^3, p^4$	$1 + p + p^2 + p^3 + p^4 = \frac{p^5 - 1}{p - 1}$
$\vdots$	$\vdots$	$\vdots$
p^k	$1, p, p^2, p^3, \dots, p^k$	$\frac{p^{k+1} - 1}{p - 1}$

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

(2.2) พิจารณา

$$\begin{aligned} \sigma(pq) &= 1 + p + q + pq = (1 + p)(1 + q) \\ \sigma(p^2 q^2) &= 1 + p + q + p^2 + q^2 + pq + pq^2 + p^2 q + p^2 q^2 \\ &= (1 + p + p^2)(1 + q + q^2) \\ \sigma(p^\alpha q^\beta) &= 1(1 + q + q^2 + \dots + q^\beta) + p(1 + q + q^2 + \dots + q^\beta) \\ &\quad + p^2(1 + q + q^2 + \dots + q^\beta) + p^\alpha(1 + q + q^2 + \dots + q^\beta) \\ &= (1 + p + p^2 + \dots + p^\alpha)(1 + q + q^2 + \dots + q^\beta) \\ &= \sigma(p^\alpha) \sigma(q^\beta) \end{aligned}$$

□

จากตัวอย่าง 2 นี้ ทำให้เราได้ข้อสรุปดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 5.3.2 ถ้า p เป็นจำนวนเฉพาะและ $n = p^a$, $a \in \mathbb{N}$ จะได้ว่า

$$\begin{aligned} 1. \quad \sigma(n) &= \frac{p^{a+1} - 1}{p - 1} \\ 2. \quad \sigma_k(n) &= \frac{(p^k)^{a+1} - 1}{p^k - 1} \end{aligned}$$

บทพิสูจน์ 1. จาก $n = p^a$ เราพบว่าตัวหารทั้งหมดของ n คือ $1, p, p^2, \dots, p^a$

$$\begin{aligned}\text{นั่นคือ } \sigma(n) &= \sigma(p^a) \\ &= 1 + p + p^2 + \dots + p^a \\ &= \frac{p^{a+1} - 1}{p - 1}\end{aligned}$$

2. จาก 1. จะได้ว่า

$$\begin{aligned}\sigma_k(n) &= \sigma_k(p^a) \\ &= 1 + p^k + (p^k)^2 + \dots + (p^k)^a \\ &= \frac{(p^k)^{a+1} - 1}{p^k - 1}\end{aligned}$$

ทฤษฎีบทประกอบ 5.3.3 ให้ $n_1, n_2 \in \mathbb{N}$ โดยที่ $(n_1, n_2) = 1$ จะได้ว่า ทุก ๆ จำนวนเต็มบวก d , $d \mid n_1 n_2$ ก็ต่อเมื่อ มีจำนวนเต็มบวก d_1 และ d_2 ที่ทำให้

$$d = d_1 d_2 \text{ และ } d_1 \mid n_1, d_2 \mid n_2$$

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 $d_2 = d'_2$

บทพิสูจน์ ให้ $n_1, n_2 \in \mathbb{N}$ โดยที่ $(n_1, n_2) = 1$

กรณี 1 ถ้า $n_1 = 1$ หรือ $n_2 = 1$ จะได้ว่า ทฤษฎีบทประกอบนี้เป็นจริง

กรณี 2 ถ้า $n_1 > 1$ และ $n_2 > 1$ ให้ $n_1 = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ และ $n_2 = q_1^{b_1} q_2^{b_2} \dots q_t^{b_t}$ แทนการเขียน n_1 และ n_2 ในรูปแบบบัญญัติ ดังนั้น $n_1 n_2 = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} q_1^{b_1} q_2^{b_2} \dots q_t^{b_t}$

ให้ d เป็นจำนวนเต็มบวกที่ $d \mid n_1 n_2$ จะได้ว่า

$$d = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} q_1^{s_1} q_2^{s_2} \dots q_t^{s_t}$$

โดยที่ทุก $i, j, 0 \leq r_i \leq a_i, 0 \leq s_j \leq b_j$

ให้ $d_1 = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ และ $d_2 = q_1^{s_1} q_2^{s_2} \dots q_t^{s_t}$

ดังนั้น $d_1 \mid n_1, d_2 \mid n_2$ และ $d = d_1 d_2$

ในทางกลับกันให้ d_1, d_2 เป็นจำนวนเต็มบวกที่ $d_1 \mid n_1, d_2 \mid n_2$

และ $d = d_1 d_2$ ดังนั้น $d_1 d_2 \mid n_1 n_2$ นั่นคือ $d \mid n_1 n_2$

ต่อไปให้ $d_1 \mid n_1, d_2 \mid n_2$ และ $d'_1 \mid n_1, d'_2 \mid n_2$ โดยที่ $d_1 d_2 = d'_1 d'_2$

ดังนั้น $d_1 = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ และ $d'_1 = p_1^{u_1} p_2^{u_2} \dots p_k^{u_k}$

โดยที่ $0 \leq r_i, u_i \leq a_i$ ทุก i

และ $d_2 = q_1^{s_1} q_2^{s_2} \dots q_t^{s_t}$ และ $d'_2 = q_1^{v_1} q_2^{v_2} \dots q_t^{v_t}$

โดยที่ $0 \leq s_i, v_i \leq b_i$ ทุก i

และ $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} q_1^{s_1} q_2^{s_2} \dots q_t^{s_t} = p_1^{u_1} p_2^{u_2} \dots p_k^{u_k} q_1^{v_1} q_2^{v_2} \dots q_t^{v_t}$

เนื่องจากจำนวนเฉพาะที่แตกต่างกันจะหารกันไม่ลงตัว เราจะได้ว่า ทุก i, j ,

$r_i = 0$ ก็ต่อเมื่อ $u_i = 0$ และ $s_j = 0$ ก็ต่อเมื่อ $v_j = 0$
 โดยทฤษฎีบทหลักมูลของเลขคณิต จะได้ว่า ทุก i, j , $r_i = u_i$ และ $s_j = v_j$
 นั่นคือ $d_1 = d_1'$ และ $d_2 = d_2'$ ■

เราจะแสดงว่าฟังก์ชัน σ และ σ_k เป็นฟังก์ชันแยกคูณ โดยการพิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 5.3.4 ให้ f เป็นฟังก์ชันเลขคณิตที่ไม่ใช่ฟังก์ชันศูนย์และ F เป็นฟังก์ชันที่กำหนดโดย

$$F(n) = \sum_{d|n} f(d)$$

ถ้า f เป็นฟังก์ชันแยกคูณ แล้ว F เป็นฟังก์ชันแยกคูณ

บทพิสูจน์ ให้ $m, n \in \mathbb{N}$ โดยที่ $(m, n) = 1$

กรณี 1 ถ้า $m = 1$ หรือ $n = 1$

จะได้ว่า $F(mn) = F(n)$ หรือ $F(mn) = F(m)$ ตามลำดับ

ดังนั้น $F(mn) = F(m)F(n)$

กรณี 2 ถ้า $m > 1$ และ $n > 1$

ให้ $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ และ $n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$

แทนการเขียน m, n ในรูปแบบบัญญัติ จาก $(m, n) = 1$ จะได้ว่า

$$\{p_1, p_2, \dots, p_r\} \cap \{q_1, q_2, \dots, q_s\} = \emptyset$$

โดยทฤษฎีบทประกอบ 5.3.3 จะได้ว่า $d | mn$ ก็ต่อเมื่อมี d_1 เป็นตัวหารของ m และ d_2 เป็นตัวหารของ n ที่ทำให้ $d = d_1 d_2$

ตัวหาร d_1 ของ m และตัวหาร d_2 ของ n จะมีเพียงคู่เดียวเท่านั้นเมื่อกำหนด d ที่เป็นตัวหารของ mn ดังนั้น

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{d_1|m, d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= F(m)F(n) \end{aligned}$$

หมายเหตุ ให้ f, g และ h เป็นฟังก์ชันเลขคณิตที่กำหนดโดย $f(n) = 1$, $g(n) = n$ และ $h(n) = n^k$

เราพบว่า f, g และ h เป็นฟังก์ชันแยกคูณและจากบทนิยามของ τ, σ และ σ_k เราพบว่า

$$\tau(n) = \sum_{d|n} f(d), \quad \sigma(n) = \sum_{d|n} g(d) \quad \text{และ} \quad \sigma_k(n) = \sum_{d|n} h(d)$$

จะเป็นฟังก์ชันแยกคูณ

ทฤษฎีบท 5.3.5 ข้อความต่อไปนี้เป็นจริง

1. σ และ σ_k เป็นฟังก์ชันแยกคูณ
2. ให้ $n \in \mathbb{N}$ และ $n > 1$ และให้ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ จะได้ว่า

$$\sigma(n) = \prod_{i=1}^k \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

และ

$$\sigma_k(n) = \prod_{i=1}^k \frac{(p_i^k)^{a_i+1} - 1}{p_i^k - 1}$$

บทพิสูจน์ 1. เป็นผลโดยตรงจากทฤษฎีบท 5.3.4 ข้างต้น เนื่องจาก $\sigma(n) = \sum_{d|n} d$ และ

$$\sigma_k(n) = \sum_{d|n} d^k \quad \text{โดยที่ } f(n) = n \text{ และ } f(n) = n^k \text{ ตามลำดับ}$$

2. จาก σ และ σ_k เป็นฟังก์ชันแยกคูณ และโดยทฤษฎีบท 5.3.2 จะได้ว่า

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

ตัวอย่าง 3 จงแสดงว่า ถ้า $2^k - 1$ เป็นจำนวนเฉพาะ แล้ว $n = 2^{k-1}(2^k - 1)$ สอดคล้องกับ $\sigma(n) = 2n$

บทพิสูจน์ จาก $2^k - 1$ เป็นจำนวนเฉพาะ จะได้ว่า $(2^{k-1}, 2^k - 1) = 1$ และจาก σ เป็นฟังก์ชันแยกคูณ

$$\begin{aligned} \text{ดังนั้น } \sigma(n) &= \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) \\ &= (2^k - 1)(2^k) = 2 \cdot 2^{k-1}(2^k - 1) \end{aligned}$$

นั่นคือ $\sigma(n) = 2n$ □

ปัญหา 4 (4.1) จงแสดงว่า ถ้า $n \in \mathbb{N}$ แล้ว $\sigma(n) \geq n$

(4.2) จงหาจำนวนเต็มบวก n สัก 3 จำนวนที่สอดคล้องกับ $\sigma(n) \leq 2n$

(4.3) จงหาจำนวนเต็มบวก n สัก 3 จำนวนที่สอดคล้องกับ $\sigma(n) = 2n$

(4.4) จงหาจำนวนเต็มบวก n สัก 3 จำนวนที่สอดคล้องกับ $\sigma(n) \geq 2n$

(4.5) จงแสดงว่า $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$ สำหรับทุกจำนวนเต็มบวก n

โจทย์ปัญหา 5.3

1. จงหาจำนวนเต็มบวก n ที่น้อยที่สุดที่ทำให้สมการ $\sigma(x) = n$

(i) ไม่มีคำตอบ

(ii) มีเพียง 1 คำตอบ

(iii) มีเพียง 2 คำตอบ

(iv) มีเพียง 3 คำตอบ

2. จงหาจำนวนเต็มบวก m ที่น้อยที่สุดที่มี n ซึ่ง $m < n$ และ $\sigma(m) = \sigma(n)$

3. ให้ $m, n \in \mathbb{N}$ และ $(m, n) > 1$ จงพิสูจน์ว่า $\sigma(mn) < \sigma(m)\sigma(n)$

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

5. ให้ $n \in \mathbb{N}$ และ $\sigma(n) = n + k$ เมื่อ $k | n$ และ $1 \leq k < n$

จงพิสูจน์ว่า $k = 1$ นั่นคือ n จะต้องเป็นจำนวนเฉพาะ

6. จาก $\sigma(6) = 12$ และ $\sigma(28) = 56$ จงหาจำนวนเต็มบวก $n > 28$ และ $\sigma(n) = 2n$

7. ให้ f และ g เป็นฟังก์ชันเลขคณิตและ $F(n) = \sum_{d|n} f(d)$, $G(n) = \sum_{d|n} g(d)$

จงพิสูจน์ว่า $F = G$ ก็ต่อเมื่อ $f = g$

8. ให้ $n \in \mathbb{N}$ จงพิสูจน์ว่า

$$(8.1) \quad \sum_{d|n} \sigma(d) = \sum_{d|n} \left(\frac{n}{d}\right) \tau(d) \quad (8.2) \quad \sum_{d|n} \left(\frac{n}{d}\right) \sigma(d) = \sum_{d|n} d \tau(d)$$

(ข้อเสนอแนะ) เนื่องจากฟังก์ชัน F และฟังก์ชัน G ที่กำหนดโดย

$$F(n) = \sum_{d|n} \sigma(d) \quad \text{และ} \quad G(n) = \sum_{d|n} \left(\frac{n}{d}\right) \tau(d)$$

เป็นฟังก์ชันแยกคูณ ดังนั้นจึงเป็นการเพียงพอที่พิสูจน์ว่า $F(p^k) = G(p^k)$

โดยที่ p เป็นจำนวนเฉพาะที่ $p | n$ และ $k \in \mathbb{N}$)

9. ให้ $m, n \in \mathbb{N}$ โดยที่ $m | n$ จงพิสูจน์ว่า $\frac{\sigma(n)}{n} \geq \frac{\sigma(m)}{m}$

10. สำหรับจำนวนเต็มบวก n ใด ๆ จงพิสูจน์ว่า $\sigma(n^2) \leq \sigma^2(n)$

5.4 ฟังก์ชัน ϕ

ในหัวข้อนี้เราจะมาศึกษาฟังก์ชันอีกชนิดหนึ่งซึ่งเรียกว่า ออยเลอร์ ฟังก์ชัน (Euler ϕ -function) โดยฟังก์ชันชนิดนี้ออยเลอร์ได้นิยามขึ้นในปี ค.ศ. 1760 แต่สำหรับสัญลักษณ์ $\phi(n)$ นี้เป็นสัญลักษณ์ที่เกาส์เป็นผู้กำหนดขึ้น

$\phi(n)$ หมายถึง จำนวนของจำนวนเต็มบวกที่น้อยกว่าหรือเท่ากับ n และเป็นจำนวนเฉพาะสัมพัทธ์กับ n นั่นคือ ห.ร.ม. ของจำนวนเต็มบวกที่น้อยกว่าหรือเท่ากับ n และ n เป็น 1 เช่น $\phi(6) = 2$ เพราะมีจำนวนเต็มบวก 2 จำนวนที่น้อยกว่าหรือเท่ากับ 6 และเป็นจำนวนเฉพาะสัมพัทธ์กับ 6 ซึ่งจำนวนเต็มบวก 2 จำนวนนั้นคือ 1 และ 5

บทนิยาม 5.4.1 ให้ $n \in \mathbb{N}$ กำหนด

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

เราเรียกฟังก์ชัน ϕ ว่า ฟังก์ชันฟี (phi function)

จากบทนิยามจะได้ว่า $\phi(1) = 1$

ตัวอย่าง 1 ตารางต่อไปนี้แสดงการหาค่าของ $\phi(n)$ เมื่อ $7 \leq n \leq 15$

n	จำนวนเต็มบวก $k \leq n$ ซึ่ง $(k, n) = 1$	$\phi(n)$
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
11	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	10
12	1, 5, 7, 11	4
13	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	12
14	1, 3, 5, 9, 11, 13	6
15	1, 2, 4, 7, 8, 11, 13, 14	8

□

ปัญหา 2 จงหาค่าของ $\phi(1001)$, $\phi(5040)$ และ $\phi(36000)$

ตัวอย่าง 3 ให้ p เป็นจำนวนเฉพาะ จงหา $\phi(p)$ และ $\phi(p^k)$ เมื่อ $k \in \mathbb{N}$

วิธีทำ ข้อสังเกต

จำนวนนับ (n)	จำนวนเต็มบวก $k \leq n$ ซึ่ง $(k, n) > 1$	$\phi(n)$
p	p	$p - 1$
p^2	$p, 2p, 3p, \dots, pp$	$p^2 - p$
$\vdots$	$\vdots$	$\vdots$
p^k	$p, 2p, 3p, \dots, p^{k-1}p$	$p^k - p^{k-1}$

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

□

ทฤษฎีบท 5.4.2 ให้ p เป็นจำนวนเฉพาะและ $k \in \mathbb{N}$ จะได้ว่า

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

บทพิสูจน์ ให้ $\mathcal{Z} = \{x \in \mathbb{N} \mid x \leq p^k\}$ และ $A = \{x \in \mathcal{Z} \mid (x, p^k) = 1\}$

ดังนั้น $A' = \{x \in \mathcal{Z} \mid p \text{ หาร } x \text{ ลงตัว}\}$

เราเห็นได้ชัดว่า $A' = \{p \cdot 1, p \cdot 2, p \cdot 3, \dots, p \cdot p^{k-1}\}$

ดังนั้น $\phi(p^k) = |A| = |\mathcal{Z}| - |A'| = p^k - p^{k-1}$

■

ตัวอย่าง 4 (4.1) $\phi(4) = \phi(2^2) = 2^2 - 2 = 2$

(4.2) $\phi(25) = \phi(5^2) = 5^2 - 5 = 20$

(4.3) $\phi(81) = \phi(3^4) = 3^4 - 3^3 = 54$ □

ทฤษฎีบทประกอบ 5.4.3 ให้ m, n, r และ s เป็นจำนวนเต็มบวก โดยที่ $(m, n) = (s, n) = (r, m) = 1$
จะได้ว่า $(nr + ms, mn) = 1$

บทพิสูจน์ สมมติว่ามีจำนวนเฉพาะ p ซึ่ง $p \mid mn$ และ $p \mid (nr + ms)$
จะได้ว่า $(p \mid m$ หรือ $p \mid n)$ และ $p \mid (nr + ms)$
ถ้า $p \mid m$ และ $p \mid (nr + ms)$ จะได้ $p \mid nr$
ดังนั้น $p \mid n$ หรือ $p \mid r$ ซึ่งเป็นไปไม่ได้ เพราะว่า $(r, m) = (m, n) = 1$
ถ้า $p \mid n$ และ $p \mid (nr + ms)$ จะได้ $p \mid ms$
ดังนั้น $p \mid m$ หรือ $p \mid s$ ซึ่งเป็นไปไม่ได้เช่นกัน เพราะว่า $(s, n) = (m, n) = 1$
ดังนั้นเราจึงสรุปได้ว่า $(nr + ms, mn) = 1$ ■

ทฤษฎีบท 5.4.4 ϕ เป็นฟังก์ชันแยกคูณ

บทพิสูจน์ ให้ $X = \{x \mid 1 \leq x \leq m, (x, m) = 1\}$
 $Y = \{y \mid 1 \leq y \leq n, (y, n) = 1\}$
และ $Z = \{z \mid 1 \leq z \leq mn, (z, mn) = 1\}$
ถ้า $z \in Z$ จะได้ว่า $(z, mn) = 1$ ดังนั้น $(z, m) = (z, n) = 1$
นั่นคือจะมี $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ ซึ่ง
 $z = q_1 m + r_1, \quad 1 \leq r_1 < m$
 $z = q_2 n + r_2, \quad 1 \leq r_2 < n$
จะได้ว่า $(r_1, m) = (r_2, n) = 1$ ดังนั้น $r_1 \in X$ และ $r_2 \in Y$
นั่นคือ $\phi(mn) \leq \phi(m)\phi(n)$
ให้ $r \in X$ และ $s \in Y$ จากทฤษฎีบทประกอบ 5.4.3 ข้างต้นจะได้ว่า $(nr + ms, mn) = 1$
ดังนั้นจะมี $q, t \in \mathbb{Z}$ ซึ่ง $nr + ms = (mn)q + t, \quad 1 \leq t \leq mn$
และ $(t, mn) = (nr + ms, mn) = 1$
ดังนั้น $t \in Z$ นั่นคือ $\phi(mn) \geq \phi(m)\phi(n)$
เพราะฉะนั้น $\phi(mn) = \phi(m)\phi(n)$ ■

บทแทรก 5.4.5 ให้ $m_1, m_2, \dots, m_k \in \mathbb{N}$ ซึ่ง $(m_i, m_j) = 1, \quad 1 \leq i < j \leq k$ จะได้ว่า
 $\phi(m_1 m_2 \cdots m_k) = \phi(m_1) \phi(m_2) \cdots \phi(m_k)$

จากทฤษฎีบท 5.4.2 และบทแทรก 5.4.5 จะได้

ทฤษฎีบท 5.4.6 ถ้า $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ แล้ว

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

ตัวอย่าง 5 (5.1) จาก $100 = 2^2 \cdot 5^2$

$$\begin{aligned} \text{จะได้ว่า } \phi(100) &= \phi(2^2 \cdot 5^2) = \phi(2^2) \cdot \phi(5^2) \\ &= 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40 \end{aligned}$$

(5.2) จาก $120 = 2^3 \cdot 3 \cdot 5$

$$\begin{aligned} \text{จะได้ว่า } \phi(120) &= 120 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \\ &= 120 \cdot \frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{5} = 32 \end{aligned}$$

(5.3) จาก $360 = 2^3 \cdot 3^2 \cdot 5$

$$\begin{aligned} \text{จะได้ว่า } \phi(360) &= 360 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \\ &= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96 \end{aligned}$$

□

ปัญหา 6 (6.1) จงแสดงว่า ถ้า n เป็นจำนวนเต็มคี่ แล้ว $\phi(2n) = \phi(n)$

(6.2) จงแสดงว่า ถ้า n เป็นจำนวนเต็มคู่ แล้ว $\phi(2n) = 2\phi(n)$

พิจารณา $n = 60 = 2^2 \cdot 3 \cdot 5$ เราพบว่าตัวประกอบที่เป็นบวกของ 60 คือ

ตัวประกอบ (d)	1	2	3	4	5	6	10	12	15	20	30	60
$\phi(d)$	1	1	2	2	4	2	4	4	8	8	8	16

เราพบว่า $\sum_{d|60} \phi(d) = 1 + 1 + 2 + 2 + 4 + 2 + 4 + 4 + 8 + 8 + 8 + 16 = 60$

ทฤษฎีบทต่อไปนี้จะกล่าวถึงการหาค่าของ $\sum_{d|n} \phi(d)$ ซึ่งเป็นสิ่งสำคัญในการศึกษาเรื่อง *กลุ่มวัฏจักรจำกัด* (Finite cyclic group) ในพีชคณิตเชิงนามธรรม

ทฤษฎีบท 5.4.7 ให้ $n \in \mathbb{N}$ จะได้ว่า $\sum_{d|n} \phi(d) = n$

บทพิสูจน์ ให้ $n = 1$ จะได้ $\sum_{d|1} \phi(d) = \phi(1) = 1$ ดังนั้นทฤษฎีบทเป็นจริงเมื่อ $n = 1$

ให้ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ

พิจารณากรณีที่ $k = 1$ จะได้

$$\begin{aligned}
\sum_{d|n} \phi(d) &= \phi(1) + \phi(p_1) + \phi(p_1^2) + \cdots + \phi(p_1^{a_1}) \\
&= 1 + (p_1 - 1) + (p_1^2 - p_1) + \cdots + (p_1^{a_1} - p_1^{a_1-1}) \\
&= p_1^{a_1} = n
\end{aligned}$$

ดังนั้นทฤษฎีบทเป็นจริงเมื่อ $k = 1$

สมมติว่าทฤษฎีบทเป็นจริงเมื่อ $k = t$ และให้

$$m = p^a n = p^a \cdot p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t} \quad \text{โดยที่ } p \text{ เป็นจำนวนเฉพาะซึ่ง } p \neq p_i$$

ทุก ๆ $i = 1, 2, \dots, t$ จะได้

$$\begin{aligned}
\sum_{d|m} \phi(d) &= \sum_{d|p^a n} \phi(d) \\
&= \sum_{d|n} \phi(d) + \sum_{d|p^a n} \phi(pd) + \sum_{d|p^a n} \phi(p^2 d) + \cdots + \sum_{d|p^a n} \phi(p^a d) \\
&= \left(\sum_{d|n} \phi(d) \right) (1 + \phi(p) + \phi(p^2) + \cdots + \phi(p^a)) \\
&= n \cdot p^a = m
\end{aligned}$$

ดังนั้น $\sum_{d|p^a n} \phi(d) = n$ ทุก ๆ จำนวนเต็มบวก n ■

ตัวอย่าง 7 จงแสดงว่า ถ้า $n > 2$ แล้ว $\phi(n)$ เป็นจำนวนเต็มคู่บวกเสมอ

บทพิสูจน์ กรณี 1 ถ้า $n = 2^k m$ ซึ่ง $k \geq 1$ และ $(2^k, m) = 1$

$$\text{จะได้ว่า } \phi(n) = \phi(2^k) \phi(m) = 2^k \left(1 - \frac{1}{2}\right) \phi(m)$$

ดังนั้น $\phi(n)$ เป็นจำนวนเต็มคู่

กรณี 2 ถ้า $n = p^k m$ ซึ่ง $k \geq 1$ และ $(p^k, m) = 1$ โดยที่ $p > 2$

$$\text{จะได้ว่า } \phi(n) = \phi(p^k m) = \phi(p^k) \phi(m) = p^{k-1} (p-1) \phi(m)$$

แต่เนื่องจาก $p-1$ เป็นจำนวนคู่ ดังนั้น $2 | (p-1)$

จากทั้งสองกรณีสรุปได้ว่า $\phi(n)$ เป็นจำนวนคู่เสมอ เมื่อ $n > 2$ □

ปัญหา 8 จงแสดงว่า ถ้า $n = 2^k$ หรือ $n = 2^k \cdot 3^j$, $k, j \in \mathbb{N}$ แล้ว $\phi(n) | n$

ปัญหา 9 ถ้าทุก ๆ จำนวนเฉพาะที่หาร n ลงตัว แล้วจะหาร m ลงตัว

จงแสดงว่า $\phi(mn) = n \phi(m)$ และ $\phi(n^2) = n \phi(n)$ สำหรับทุกจำนวนเต็มบวก n

ปัญหา 10 จงพิสูจน์ว่า ถ้า n และ $n+2$ เป็นจำนวนเฉพาะคู่แฝดแล้ว $\phi(n+2) = \phi(n) + 2$

โจทย์ปัญหา 5.4

1. จงหา $\phi(n)$ เมื่อ $n = 16$, $n = 17$, $n = 4080$
2. จงหา $n \in \mathbb{N}$ ทั้งหมดที่ทำให้ $\phi(n)$ เป็นจำนวนเต็มคี่
3. จงหาเงื่อนไขที่จำเป็นและเพียงพอของจำนวนเต็มบวก m, n ที่ทำให้ $\phi(mn) = m \phi(n)$

4. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $\phi(2n) = \phi(n)$
5. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $\phi(2n) > \phi(n)$
6. จงหาคำตอบ $x \in \mathbb{N}$ ทั้งหมดที่ทำให้ $\phi(x) = 24$
7. ให้ $n \in \mathbb{N}$ จงแสดงว่าเซตคำตอบของสมการ $\phi(x) = n$ เป็นเซตจำกัด
8. จงหาจำนวนเต็มบวก n ที่น้อยที่สุดที่ทำให้สมการ $\phi(x) = n$
 - (i) ไม่มีคำตอบ
 - (ii) มีเพียง 2 คำตอบ
 - (iii) มีเพียง 3 คำตอบ
 - (iv) มีเพียง 4 คำตอบ

ได้มีผู้ตั้งข้อาคติเตว่า “ไม่มีจำนวนเต็มบวก n ที่ทำให้ $\phi(x) = n$ มีเพียง 1 คำตอบ”
ซึ่งในปัจจุบันยังไม่ผู้ใดให้คำตอบของข้อาคติเตนี้ว่า จริงหรือเท็จ
9. จากข้อ 8. ผู้อ่านคงตอบได้ว่า 14 เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้สมการ $\phi(x) = 14$ ไม่มีคำตอบ
จงหาจำนวนเต็มบวก n ที่น้อยที่สุดและ $n > 14$ ที่ทำให้ $\phi(x) = n$ ไม่มีคำตอบ
10. ให้ $n > 1$ และ $f(n)$ แทนผลบวกของจำนวนเต็มบวก k ซึ่ง $k < n$ และ $(k, n) = 1$
จงพิสูจน์ว่า $f(n) = \frac{n}{2} \phi(n)$
11. จาก f ที่กำหนดในข้อ 10. จงพิสูจน์ว่าถ้า $f(m) = f(n)$ แล้ว $m = n$
12. ถ้า $d | n$ และ $0 < d < n$ จงตรวจสอบว่า $n - \phi(n) = d - \phi(d)$ หรือไม่

5.5 ฟังก์ชัน μ

ฟังก์ชันเลขคณิตที่สำคัญอีกฟังก์ชันหนึ่ง คือ ฟังก์ชันเมอบิอุส ซึ่งได้กล่าวมาแล้วในตอนต้น ก่อนที่เราจะกล่าวถึงสมบัติต่าง ๆ ของฟังก์ชันเมอบิอุสนั้น เราจะขอทบทวนบทนิยามของฟังก์ชันชนิดนี้ก่อน

บทนิยาม 5.5.1 ฟังก์ชันเมอบิอุส (Möbius function) คือฟังก์ชัน $\mu : \mathbb{N} \rightarrow \mathbb{Z}$ ที่กำหนดโดย

$$\mu(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้า มีจำนวนเฉพาะ } p \text{ ซึ่ง } p^2 | n \\ (-1)^k & \text{ถ้า } n = p_1 p_2 \cdots p_k \end{cases}$$

โดยที่ p_i เป็นจำนวนเฉพาะที่แตกต่างกัน

ตัวอย่าง 1 $\mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1, \mu(6) = 1, \mu(7) = -1,$
 $\mu(8) = 0, \mu(9) = 0$ และ $\mu(10) = 1$ □

ฟังก์ชัน μ เป็นฟังก์ชันเลขคณิตที่มีบทบาททั้งในการศึกษาทฤษฎีจำนวนและการศึกษาคณิตศาสตร์เชิงการนับ (combinatorics) ทฤษฎีบทพื้นฐานที่เกี่ยวข้องกับฟังก์ชัน μ มีดังนี้

ทฤษฎีบท 5.5.2 μ เป็นฟังก์ชันแยกคูณ

บทพิสูจน์ ให้ $m, n \in \mathbb{N}$ โดยที่ $(m, n) = 1$

กรณี 1 ถ้า $m = 1$ หรือ $n = 1$ จะได้ $\mu(mn) = \mu(n)$ หรือ $\mu(mn) = \mu(m)$
ตามลำดับ และจากทั้งสองกรณีจะได้ว่า $\mu(mn) = \mu(m)\mu(n)$

กรณี 2 ถ้า $m > 1$ และ $n > 1$
และถ้ามีจำนวนเฉพาะ p ซึ่ง $p^2 \mid mn$ จะได้ว่า $p^2 \mid m$ หรือ $p^2 \mid n$
ดังนั้นทั้งสองกรณีสรุปได้ว่า $0 = \mu(mn) = \mu(m)\mu(n)$

ถ้า $m = p_1 p_2 \cdots p_r$ และ $n = q_1 q_2 \cdots q_s$ แทนการเขียน m และ n ในรูปแบบบัญญัติ
จาก $(m, n) = 1$ จะได้ $\{p_1, p_2, \dots, p_r\} \cap \{q_1, q_2, \dots, q_s\} = \emptyset$
ดังนั้น $\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n)$ ■

ทฤษฎีบทประกอบ 5.5.3 ให้ $n \in \mathbb{N}$ และ $F(n) = \sum_{d \mid n} \mu(d)$ จะได้ว่า

$$F(1) = 1 \quad \text{และ} \quad F(n) = 0 \quad \text{เมื่อ } n > 1$$

บทพิสูจน์ $F(1) = \mu(1) = 1$ จาก μ เป็นฟังก์ชันแยกคูณ โดยทฤษฎีบท 5.3.4 จะได้ว่า
 F เป็นฟังก์ชันแยกคูณ ดังนั้นเป็นการเพียงพอที่จะพิสูจน์ว่า $F(p^k) = 0$ เมื่อ p เป็นจำนวนเฉพาะ
และ $k \in \mathbb{N}$ ให้ $n = p^k$ โดยที่ p เป็นจำนวนเฉพาะและ $k \in \mathbb{N}$

$$\begin{aligned} \text{จะได้ว่า } F(n) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= 1 + (-1) + 0 + \cdots + 0 = 0 \end{aligned}$$

ดังนั้น $F(n) = 0$ ทุก ๆ $n > 1$

$$\text{นั่นคือ } \sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้า } n > 1 \end{cases} \quad \blacksquare$$

จากทฤษฎีบท 5.5.3 ข้างต้น ตัวหารของ 10 คือ 1, 2, 5, 10 และ

$$\sum_{d \mid 10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10) = 1 + (-1) + (-1) + 1 = 0$$

ทฤษฎีบทประกอบ 5.5.4 ให้ $c, d, n \in \mathbb{N}$ จะได้ว่า

$$d \mid n \text{ และ } c \mid \frac{n}{d} \quad \text{ก็ต่อเมื่อ} \quad c \mid n \text{ และ } d \mid \frac{n}{c}$$

บทพิสูจน์ เนื่องจาก $d \mid n$ ดังนั้นจะมี $s \in \mathbb{N}$ ที่ทำให้ $n = ds$

$$\text{ให้ } s = \frac{n}{d} \text{ และจาก } c \mid \frac{n}{d} \text{ จะได้ว่ามี } t \in \mathbb{N} \text{ ที่ทำให้ } s = \frac{n}{d} = ct$$

$$\text{นั่นคือ } n = ds = d(ct) = c(dt)$$

$$\text{ดังนั้น } c \mid n \text{ และ } d \mid \frac{n}{c} \quad \blacksquare$$

ทฤษฎีบท 5.5.5 (Möbius Inversion Formula)

ให้ f เป็นฟังก์ชันเลขคณิต และ F เป็นฟังก์ชันที่กำหนดโดย

$$F(n) = \sum_{d|n} f(d)$$

$$\text{จะได้ว่า } f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

บทพิสูจน์ จาก $\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c)$

$$= \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c)$$

จากทฤษฎีบทประกอบ 5.5.4 จะได้ว่า

$$\begin{aligned} \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c) &= \sum_{c|n} \sum_{d|\frac{n}{c}} f(c) \mu(d) \\ &= \sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d) \end{aligned}$$

จากทฤษฎีบท 5.5.3 จะได้ว่า

$$\sum_{d|\frac{n}{c}} \mu(d) = 1 \quad \text{ถ้า } c = n \quad \text{และ} \quad \sum_{d|\frac{n}{c}} \mu(d) = 0 \quad \text{ถ้า } c \neq n$$

$$\text{ดังนั้น } \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = f(n) \quad \blacksquare$$

จากทฤษฎีบท 5.5.5 และ $\tau(n) = \sum_{d|n} 1$ และ $\sigma(n) = \sum_{d|n} d$ จะได้ว่า

$$1 = \sum_{d|n} \mu(d) \tau\left(\frac{n}{d}\right) \quad \text{และ} \quad n = \sum_{d|n} \mu(d) \sigma\left(\frac{n}{d}\right)$$

และจากทฤษฎีบท 5.4.7 เราพบว่า $n = \sum_{d|n} \phi(d)$ ดังนั้น $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$

ทฤษฎีบทประกอบ 5.5.6 ถ้า $n \in \mathbb{N}$ แล้ว $\log n = \sum_{d|n} \Lambda(d)$ เมื่อ Λ คือฟังก์ชันมานเกอลท์ที่กำหนดโดย

$$\Lambda(n) = \begin{cases} \log p & \text{ถ้า } n = p^a \text{ โดยที่ } p \text{ เป็นจำนวนเฉพาะและ } a \in \mathbb{N} \\ 0 & \text{ถ้า } n \text{ เขียนได้ในรูปอื่น ๆ ที่ไม่ใช่ } p^a \end{cases}$$

บทพิสูจน์ (i) ถ้า $n = 1$ จะได้ว่า $\log 1 = 0$ และ $\sum_{d|1} \Lambda(d) = \Lambda(1) = 0$

$$\text{ดังนั้น } \log 1 = \sum_{d|1} \Lambda(d)$$

(ii) ถ้า $n > 1$ และให้ $n = \prod_{k=1}^r p_k^{a_k}$ จะได้ว่า $\log n = \sum_{k=1}^r a_k \log p_k$

$$\begin{aligned} \text{ดังนั้น } \sum_{d|n} \Lambda(d) &= \sum_{k=1}^r \sum_{m=1}^{a_k} \Lambda(p_k^m) \\ &= \sum_{k=1}^r \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^r a_k \log p_k = \log n \quad \blacksquare \end{aligned}$$

ทฤษฎีบท 5.5.7 ถ้า $n \in \mathbb{N}$ แล้ว $A(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d) \log d$

บทพิสูจน์ จากทฤษฎีบทประกอบ 5.5.6 และโดย Möbius inversion formula จะได้ว่า

$$A(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d$$

เนื่องจาก $\log n \sum_{d|n} \mu(d) = 0$ สำหรับทุกจำนวนเต็มบวก n

$$\text{ดังนั้น } A(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d) \log d \quad \blacksquare$$

โจทย์ปัญหา 5.5

1. จงหาจำนวนเต็มบวก n ที่ทำให้ $\mu(n) + \mu(n+1) + \mu(n+2) = 3$
2. จงพิสูจน์ว่าทุก ๆ $n \in \mathbb{N}$, $\mu(n) \mu(n+1) \mu(n+2) \mu(n+3) = 0$
3. จงหาค่าของ $\sum_{j=1}^{\infty} \mu(j!)$
4. ให้ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ จงพิสูจน์ว่า $\sum_{d|n} |\mu(d)| = 2^k$
5. ให้ n อยู่ในรูปข้อ 4. ข้างต้นและ f เป็นฟังก์ชันแยกคูณ จงพิสูจน์ว่า

$$F(n) = \sum_{d|n} \mu(d) f(d) = \prod_{i=1}^k (1 - f(p_i))$$

(ข้อเสนอนี้ โดยทฤษฎีบท 5.3.4, F เป็นฟังก์ชันแยกคูณ)

6. จาก n ที่เขียนในรูปข้อ 4. ข้างต้น จงตรวจสอบว่าข้อใดต่อไปนี้เป็นจริง

$$(6.1) \quad \sum_{d|n} \mu(d) \tau(d) = (-1)^k$$

$$(6.2) \quad \sum_{d|n} \mu(d) \sigma(d) = (-1)^k p_1 p_2 \cdots p_k$$

$$(6.3) \quad \sum_{d|n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$(6.4) \quad \sum_{d|n} d \mu(d) = (1 - p_1)(1 - p_2) \cdots (1 - p_k)$$

7. ให้ k เป็นจำนวนเต็มบวก จงพิสูจน์ว่ามีจำนวนเต็มบวก n ที่ทำให้

$$\mu(n+1) = \mu(n+2) = \mu(n+3)$$

8. จงพิสูจน์ว่า $\sum_{d^2|n} \mu(d) = [\mu(n)]^2$

9. ให้ $n \in \mathbb{N}$ จงหาค่าของ $\sum_{d|n} \mu(d) \sigma(d)$

10. ให้ n เป็นจำนวนเต็มบวกคู่ จงพิสูจน์ว่า $\sum_{d|n} \mu(d) \phi(d) = 0$

5.6 ฟังก์ชันจำนวนเต็มค่ามากที่สุด

ให้ $\mathcal{U} = \{1, 2, 3, \dots, 100\}$

$$A = \{x \in \mathcal{U} \mid 2 \text{ หาร } x \text{ ลงตัว}\}$$

$$B = \{x \in \mathcal{U} \mid 3 \text{ หาร } x \text{ ลงตัว}\}$$

และ $C = \{x \in \mathcal{U} \mid 6 \text{ หาร } x \text{ ลงตัว}\}$

ให้ $|X|$ แทนจำนวนสมาชิกของเซต X เราพบว่า

$$|\mathcal{U}| = 100, |A| = 50, |B| = 33 \text{ และ } |C| = 16$$

ในกรณีทั่ว ๆ ไป ให้ $\mathcal{V} = \{1, 2, 3, \dots, n\}$

$$D = \{x \in \mathcal{V} \mid 2 \text{ หาร } x \text{ ลงตัว}\}$$

$$E = \{x \in \mathcal{V} \mid 3 \text{ หาร } x \text{ ลงตัว}\}$$

และ $F = \{x \in \mathcal{V} \mid 6 \text{ หาร } x \text{ ลงตัว}\}$

เราพบว่า $|D| =$ จำนวนเต็มค่ามากที่สุดซึ่งน้อยกว่าหรือเท่ากับ $\frac{n}{2}$

$|E| =$ จำนวนเต็มค่ามากที่สุดซึ่งน้อยกว่าหรือเท่ากับ $\frac{n}{3}$

และ $|F| =$ จำนวนเต็มค่ามากที่สุดซึ่งน้อยกว่าหรือเท่ากับ $\frac{n}{6}$

จากที่กล่าวมาข้างต้นเราจะใช้สัญลักษณ์ $\lfloor x \rfloor$ แทนจำนวนเต็มค่ามากที่สุดซึ่งน้อยกว่าหรือเท่ากับ x

นั่นคือ $|A| = \left\lfloor \frac{100}{2} \right\rfloor = 50, |B| = \left\lfloor \frac{100}{3} \right\rfloor = 33, |C| = \left\lfloor \frac{100}{6} \right\rfloor = 16, |D| = \left\lfloor \frac{n}{2} \right\rfloor,$

$|E| = \left\lfloor \frac{n}{3} \right\rfloor$ และ $|F| = \left\lfloor \frac{n}{6} \right\rfloor$

ในกรณีเช่นนี้เราเรียก $\lfloor x \rfloor$ ว่า ฟังก์ชันจำนวนเต็มค่ามากที่สุด (The greatest integer function)

บทนิยาม 5.6.1 สำหรับจำนวนจริง x ใด ๆ $\lfloor x \rfloor$ คือจำนวนเต็มค่ามากที่สุดที่น้อยกว่าหรือเท่ากับ x

ตัวอย่าง 1 $\lfloor 1.2 \rfloor = 1, \lfloor \sqrt{3} \rfloor = 1, \lfloor -\sqrt{3} \rfloor = -2, \left\lfloor -\frac{5}{2} \right\rfloor = -3$ □

จากบทนิยามเราพบว่า

$$(1) \quad \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$

$$(2) \quad 0 \leq x - \lfloor x \rfloor < 1$$

จากสมบัติของจำนวนจริง สำหรับจำนวนจริง x ใด ๆ จะมีจำนวนเต็ม n ที่ $n \leq x < n+1$ ซึ่งทำให้ $x = n + (x - n)$ โดยที่ $0 \leq x - n < 1$

นั่นคือ สำหรับทุกจำนวนจริง $x, x = n + \varepsilon$ โดย $0 \leq \varepsilon < 1$ ซึ่งในกรณีนี้ $\lfloor x \rfloor = n$

ทฤษฎีบทต่อไปจะกล่าวถึงสมบัติเบื้องต้นของฟังก์ชัน $\lfloor x \rfloor$

ทฤษฎีบท 5.6.2 สำหรับจำนวนจริง x, y ใด ๆ จะได้ว่า

1. ถ้า $x \geq 0$ แล้ว $\sum_{1 \leq i \leq x} 1 = x$
2. $|x| + |-x| = \begin{cases} 0 & \text{ถ้า } x \text{ เป็นจำนวนเต็ม} \\ -1 & \text{ถ้า } x \text{ ไม่เป็นจำนวนเต็ม} \end{cases}$
3. $|x + m| = |x| + m$ เมื่อ m เป็นจำนวนเต็ม
4. $\left\lfloor \frac{x}{m} \right\rfloor = \left\lfloor \frac{|x|}{m} \right\rfloor$ เมื่อ m เป็นจำนวนเต็มบวก
5. $-|x| =$ จำนวนเต็มค่าน้อยสุดที่มากกว่าหรือเท่ากับ $-x$
6. ถ้า m และ n เป็นจำนวนเต็มบวก จะได้ว่า

จำนวนของจำนวนเต็มจากเซต $\{1, 2, 3, \dots, m\}$ ที่หารลงตัวด้วย n คือ $\left\lfloor \frac{m}{n} \right\rfloor$

บทพิสูจน์

1. ให้ $x \geq 0$ ดังนั้น $\sum_{1 \leq i \leq x} 1$ จะเป็นการนับจำนวนเต็มบวก i ที่ $i \leq x$ คือ $1, 2, 3, \dots, |x|$ ซึ่งมีอยู่ $|x|$ จำนวน ดังนั้น $\sum_{1 \leq i \leq x} 1 = |x|$
2. ให้ $x = n + \varepsilon$ เมื่อ n เป็นจำนวนเต็มและ $0 \leq \varepsilon < 1$
กรณี 1 x เป็นจำนวนเต็ม นั่นคือ $\varepsilon = 0$ ดังนั้น $|x| = n$ และ $|-x| = -n$
 จึงได้ว่า $|x| + |-x| = 0$
กรณี 2 x ไม่เป็นจำนวนเต็ม นั่นคือ $0 < \varepsilon < 1$ ดังนั้น $-1 < -\varepsilon < 0$
 ทำให้ $0 < -\varepsilon + 1 < 1$ และ $-x = -n - \varepsilon = (-n - 1) + (-\varepsilon + 1)$
 โดยที่ $-n - 1$ เป็นจำนวนเต็มและ $0 < -\varepsilon + 1 < 1$
 ดังนั้น $|-x| = -n - 1$ ทำให้ $|x| + |-x| = n + (-n - 1) = -1$
3. ให้ $x = n + \varepsilon$ โดยที่ n เป็นจำนวนเต็มและ $0 \leq \varepsilon < 1$
 ดังนั้น $x + m = n + m + \varepsilon$ โดยที่ $n + m$ เป็นจำนวนเต็มและ $0 \leq \varepsilon < 1$
 ทำให้ $|x + m| = |x| + m$
4. ให้ m เป็นจำนวนเต็มบวก ให้ $x = n + \varepsilon$ โดยที่ n เป็นจำนวนเต็มและ $0 \leq \varepsilon < 1$
 โดยขั้นตอนวิธีการหาร จะมีจำนวนเต็ม q และ r ที่ทำให้ $n = mq + r$, $0 \leq r < m$
 ดังนั้น $\frac{n}{m} = q + \frac{r}{m}$ โดยที่ $0 \leq \frac{r}{m} < 1$ ทำให้ $\left\lfloor \frac{|x|}{m} \right\rfloor = \left\lfloor \frac{n}{m} \right\rfloor = q$

$$\frac{x}{m} = \frac{n + \varepsilon}{m} = \frac{mq + r + \varepsilon}{m} = q + \frac{r + \varepsilon}{m}$$
 จากที่ $r < m$ ทำให้ $m - r > 0$ ดังนั้น $m - r \geq 1 > \varepsilon$
 นั่นคือ $r + \varepsilon < m$ ทำให้ $0 \leq \frac{r + \varepsilon}{m} < 1$
 เราจึงได้ว่า $\left\lfloor \frac{x}{m} \right\rfloor = q$ เพราะฉะนั้น $\left\lfloor \frac{x}{m} \right\rfloor = \left\lfloor \frac{|x|}{m} \right\rfloor$
5. จากบทนิยาม $|-x| =$ จำนวนเต็มค่ามากที่สุดที่น้อยกว่าหรือเท่ากับ $-x$
 ดังนั้น $|-x| \leq -x$ ทำให้ $-|-x| \geq x$

ต่อไปให้ k เป็นจำนวนเต็มใด ๆ ที่ $k \geq x$

ดังนั้น $-k \leq -x$ ทำให้ $-k \leq \lfloor -x \rfloor$ และ $k \geq -\lfloor -x \rfloor$

สรุปได้ว่า $-\lfloor -x \rfloor$ เป็นจำนวนเต็มค่าน้อยสุดที่มากกว่าหรือเท่ากับ x

6. ให้ m และ n เป็นจำนวนเต็มบวกใด ๆ

ถ้า $m < n$ จะได้ว่า $\frac{m}{n} < 1$ ทำให้ $\left\lfloor \frac{m}{n} \right\rfloor = 0$

และในกรณีนี้สมาชิกในเซต $\{1, 2, 3, \dots, m\}$ ไม่มีตัวใดเลยที่หารลงตัวด้วย n

ต่อไปพิจารณากรณีที่ $m \geq n$

ให้ $n, 2n, 3n, \dots, kn$ เป็นจำนวนเต็มในเซต $\{1, 2, 3, \dots, m\}$ ที่หารลงตัวด้วย n

ทั้งหมด เราพิสูจน์ว่า $\left\lfloor \frac{m}{n} \right\rfloor = k$ จากการที่ $kn \in \{1, 2, 3, \dots, m\}$

และ $(k+1)n \notin \{1, 2, 3, \dots, m\}$ เราได้ว่า $kn \leq m$ และ $(k+1)n > m$

ดังนั้น $k \leq \frac{m}{n} < k+1$

นั่นคือ $\left\lfloor \frac{m}{n} \right\rfloor = k$ ■

ในการหารจำนวนเต็ม a ด้วยจำนวนเต็ม b ที่ $b > 0$ โดยขั้นตอนวิธีการหารผลลัพธ์ q และเศษ r สอดคล้องกับ $a = bq + r$, $0 \leq r < b$ ทำให้ได้ว่า

$$\frac{a}{b} = q + \frac{r}{b} \quad \text{โดยที่ } 0 \leq \frac{r}{b} < 1$$

นั่นคือ $q = \left\lfloor \frac{a}{b} \right\rfloor$ และ $r = a - bq = b\left(\frac{a}{b} - \left\lfloor \frac{a}{b} \right\rfloor\right)$

ตัวอย่าง 2 ให้ $a = -815$ และ $b = 233$

$$\text{จาก } -\frac{815}{233} = -3.5 \quad \text{จะได้ว่า } q = \left\lfloor -\frac{815}{233} \right\rfloor = -4$$

$$\text{และ } r = a - bq = -815 - 233(-4) = -815 + 932 = 117 \quad \square$$

ทฤษฎีบท 5.6.3 ให้ $\mathcal{U} = \{1, 2, 3, \dots, n\}$ และ $a, b \in \mathbb{N}$

$$A = \{x \in \mathcal{U} \mid a \text{ หาร } x \text{ ลงตัว}\}$$

$$\text{และ } B = \{x \in \mathcal{U} \mid b \text{ หาร } x \text{ ลงตัว}\}$$

$$\text{จะได้ว่า } |A| = \left\lfloor \frac{n}{a} \right\rfloor, \quad |B| = \left\lfloor \frac{n}{b} \right\rfloor$$

$$\text{และ } |A \cap B| = \left\lfloor \frac{n}{c} \right\rfloor \quad \text{เมื่อ } c = [a, b]$$

นอกจากฟังก์ชัน $|$ จะช่วยในการหาจำนวนสมาชิกในเซตที่ได้กล่าวมาแล้วข้างต้น ฟังก์ชัน $|$ ยังช่วยในการหาสูตรเพื่อแสดงคำตอบปัญหาต่อไปนี้

$$(1) \quad \text{ให้ } 100! = 2^k K \quad \text{โดยที่ } (2, K) = 1 \quad \text{จงหา } k$$

$$(2) \quad \text{ให้ } 100! = 3^h H \quad \text{โดยที่ } (3, H) = 1 \quad \text{จงหา } h$$

$$(3) \quad \text{ให้ } 100! = 5^m M \quad \text{โดยที่ } (5, M) = 1 \quad \text{จงหา } m$$

พิจารณา (1) จาก $100! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots 97 \cdot 98 \cdot 99 \cdot 100$ เรพบว่ถ้า $\mathcal{Z} = \{1, 2, 3, \dots, 100\}$ แล้ว

$$\text{ใน } \mathcal{Z} \text{ จะมี } 50 \text{ จำนวนที่มี } 2 \text{ เป็นตัวประกอบ} \quad (50 = \left\lfloor \frac{100}{2} \right\rfloor)$$

$$\text{ใน } \mathcal{Z} \text{ จะมี } 25 \text{ จำนวนที่มี } 2^2 \text{ เป็นตัวประกอบ} \quad (25 = \left\lfloor \frac{100}{2^2} \right\rfloor)$$

$$\text{ใน } \mathcal{Z} \text{ จะมี } 12 \text{ จำนวนที่มี } 2^3 \text{ เป็นตัวประกอบ} \quad (12 = \left\lfloor \frac{100}{2^3} \right\rfloor)$$

$$\text{ใน } \mathcal{Z} \text{ จะมี } 6 \text{ จำนวนที่มี } 2^4 \text{ เป็นตัวประกอบ} \quad (6 = \left\lfloor \frac{100}{2^4} \right\rfloor)$$

$$\text{ใน } \mathcal{Z} \text{ จะมี } 3 \text{ จำนวนที่มี } 2^5 \text{ เป็นตัวประกอบ} \quad (3 = \left\lfloor \frac{100}{2^5} \right\rfloor)$$

$$\text{ใน } \mathcal{Z} \text{ จะมี } 1 \text{ จำนวนที่มี } 2^6 \text{ เป็นตัวประกอบ} \quad (1 = \left\lfloor \frac{100}{2^6} \right\rfloor)$$

$$\text{ดังนั้น} \quad k = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

$$\text{นั่นคือ} \quad k = \sum_{i=1}^6 \left\lfloor \frac{100}{2^i} \right\rfloor \quad \text{แต่} \quad \left\lfloor \frac{100}{2^i} \right\rfloor = 0 \quad \text{เมื่อ } i \geq 7$$

$$\text{ดังนั้นเราสามารถเขียน } k = \sum_{i=1}^{\infty} \left\lfloor \frac{100}{2^i} \right\rfloor$$

จาก (2) และ (3) จะได้

$$h = \sum_{i=1}^{\infty} \left\lfloor \frac{100}{3^i} \right\rfloor \quad \text{และ} \quad m = \sum_{i=1}^{\infty} \left\lfloor \frac{100}{5^i} \right\rfloor$$

ทฤษฎีบท 5.6.4 ให้ n เป็นจำนวนเต็มบวกและ p เป็นจำนวนเฉพาะ จะได้ว่า

$$\text{ถ้า } n! = p^k K \text{ และ } (p, K) = 1 \text{ แล้ว } k = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

บทพิสูจน์ ให้ $\mathcal{Z} = \{1, 2, 3, \dots, n\}$ เรพบว่

$$\text{ใน } \mathcal{Z} \text{ จะมี } \left\lfloor \frac{n}{p} \right\rfloor \text{ จำนวนที่มี } p \text{ เป็นตัวประกอบ}$$

$$\text{ใน } \mathcal{Z} \text{ จะมี } \left\lfloor \frac{n}{p^2} \right\rfloor \text{ จำนวนที่มี } p^2 \text{ เป็นตัวประกอบ}$$

$\vdots$

$$\text{ใน } \mathcal{Z} \text{ จะมี } \left\lfloor \frac{n}{p^i} \right\rfloor \text{ จำนวนที่มี } p^i \text{ เป็นตัวประกอบ}$$

นอกจากนั้นจำนวนแต่ละจำนวนใน $\mathcal{Z}$ ที่มี p^i เป็นตัวประกอบก็จะเป็นจำนวนที่มี $p, p^2, \dots, p^{i-1}$ เป็นตัวประกอบด้วย

นั่นคือ จำนวนใน $\mathcal{Z}$ ที่มี p^i เป็นตัวประกอบถูกนับมาแล้ว $i-1$ ครั้ง

และถูกนับอีก 1 ครั้งในการคำนวณ $\left\lfloor \frac{n}{p^i} \right\rfloor$ ดังนั้น $k = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$ ■

โปรดสังเกตว่า $\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$ เป็นผลบวกเพียงจำกัดพจน์ที่ไม่เป็น 0 เนื่องจากถ้า $p^i > n$

จะได้ว่า $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$

ทฤษฎีบท 5.6.5 ถ้า n และ r เป็นจำนวนเต็มบวกซึ่ง $1 \leq r \leq n$ จะได้ว่าสัมประสิทธิ์ทวินาม

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

จะเป็นจำนวนเต็ม

บทพิสูจน์ จากการคำนวณ $|x|$ เมื่อ x เป็นจำนวนจริง เราพบว่า

$$x = |x| + \varepsilon \quad \text{เมื่อ } 0 \leq \varepsilon < 1$$

ดังนั้น $|x| + |y| = (x - \varepsilon_1) + (y - \varepsilon_2)$ สำหรับ $\varepsilon_1, \varepsilon_2$ บางค่าซึ่ง $0 \leq \varepsilon_1 < 1$

และ $0 \leq \varepsilon_2 < 1$

ดังนั้น $|x| + |y| = (x + y) - (\varepsilon_1 + \varepsilon_2) \leq (x + y) - \varepsilon$ เมื่อ $0 \leq \varepsilon < 1$

นี่คือการแสดงว่า $|x| + |y| \leq |x + y|$

ให้ p เป็นจำนวนเฉพาะซึ่ง $p \leq n$ เราพบว่า

$$\left\lfloor \frac{r}{p^k} \right\rfloor + \left\lfloor \frac{n-r}{p^k} \right\rfloor \leq \left\lfloor \frac{n}{p^k} \right\rfloor, \quad k = 1, 2, 3, \dots$$

ดังนั้น $\sum_{k=1}^{\infty} \left\lfloor \frac{r}{p^k} \right\rfloor + \sum_{k=1}^{\infty} \left\lfloor \frac{n-r}{p^k} \right\rfloor \leq \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$

นี่คือการแสดงว่า ถ้า $n! = p^a A$, $(p, A) = 1$ และ $r!(n-r)! = p^b B$, $(p, B) = 1$ แล้ว

$b \leq a$ และค่ากล่าวข้างต้นเป็นจริงสำหรับจำนวนเฉพาะ p

ดังนั้น $r!(n-r)!$ เป็นตัวหารของ $n!$ ■

จากทฤษฎีบท 5.6.5 เราจะได้บทแทรกต่อไปนี้

บทแทรก 5.6.6 ผลคูณของจำนวนเต็มบวก r จำนวนที่เรียงต่อเนื่องกัน จะหารด้วย $r!$ ลงตัว

บทพิสูจน์ ให้ $n, n-1, n-2, \dots, n-r+1$ ($n \geq r$) เป็นจำนวนเต็มบวก r จำนวนเรียงกันจากมากไปหาน้อย

$$N = n(n-1)(n-2) \cdots (n-r+1)$$

$$= \frac{n!}{(n-r)!} = \left(\frac{n!}{r!(n-r)!} \right) r! = \binom{n}{r} r!$$

จากทฤษฎีบท 5.6.5 เราพบว่า $\binom{n}{r}$ เป็นจำนวนเต็มบวก ดังนั้น $r! \mid N$ ■

โจทย์ปัญหา 5.5

1. ให้ a, b เป็นจำนวนเต็มซึ่ง $b > 0$ จงแสดงว่ามีจำนวนเต็ม r ซึ่ง $0 \leq r < b$ เพียงจำนวนเดียวเท่านั้น
ซึ่ง $a = \left\lfloor \frac{a}{b} \right\rfloor b + r$
2. ให้ x เป็นจำนวนจริง จงพิสูจน์สมบัติแต่ละข้อของฟังก์ชัน $\lfloor \cdot \rfloor$
(2.1) $\left\lfloor \frac{nm}{k} \right\rfloor \geq n \left\lfloor \frac{m}{k} \right\rfloor$ เมื่อ $m, n, k \in \mathbb{N}$
(2.2) $\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$
3. ให้ $1000! = 5^a A$ เมื่อ $(5, A) = 1$ จงหา a และ
ให้ $1000! = 7^b B$ เมื่อ $(7, B) = 1$ จงหา b
4. ให้ $n \in \mathbb{N}$ และ $n \geq 0$ จงแสดงว่า $\left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{-n}{2} \right\rfloor = n$
5. (5.1) จงแสดงว่าเมื่อเขียน $1000!$ ในรูปจำนวนในระบบฐานสิบจะเป็นจำนวนที่ลงท้ายด้วย 0 เรียงต่อเนื่องกัน
ถึง 249 ตัว
(5.2) จงหา $n \in \mathbb{N}$ ที่ทำให้ $n!$ เป็นจำนวนที่ลงท้ายด้วย 0 เรียงต่อเนื่องกัน 37 จำนวน

โจทย์ปัญหาเสริมเรื่อง ฟังก์ชันเลขคณิต

ปัญหา 1 จงแสดงว่า ถ้า $2^k - 3$ เป็นจำนวนเฉพาะ แล้ว $n = 2^{k-1}(2^k - 3)$ สอดคล้องกับ

$$\sigma(n) = 2n + 2$$

ปัญหา 2 จงตรวจสอบว่า $\phi(3n) = 3\phi(n)$ ก็ต่อเมื่อ $3 \mid n$ เป็นจริงหรือไม่

ปัญหา 3 จงตรวจสอบว่า $\phi(3n) = 2\phi(n)$ ก็ต่อเมื่อ $3 \nmid n$ เป็นจริงหรือไม่

ปัญหา 4 จงตรวจสอบว่า $\phi(n) = \frac{n}{2}$ ก็ต่อเมื่อ มี $k \in \mathbb{N}$ ซึ่ง $n = 2^k$ เป็นจริงหรือไม่

ปัญหา 5 ถ้า $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ แล้วจงแสดงว่า

$$(5.1) \quad \sigma(n)\phi(n) \geq n^2 \left(1 - \frac{1}{p_1^2}\right) \left(1 - \frac{1}{p_2^2}\right) \cdots \left(1 - \frac{1}{p_r^2}\right)$$

$$(5.2) \quad \tau(n)\phi(n) \geq n$$

$$(\text{ข้อเสนอแนะ}) \quad \tau(n)\phi(n) \geq 2^r \cdot n \left(\frac{1}{2}\right)^r$$

ปัญหา 6 ให้ p เป็นจำนวนเฉพาะใด ๆ จงแสดงว่า

$$(6.1) \quad \tau(p!) = 2 \tau((p-1)!)$$

$$(6.2) \quad \sigma(p!) = (p+1)\sigma((p-1)!)$$

$$(6.3) \quad \phi(p!) = (p-1)\phi((p-1)!)$$

ปัญหา 7 ให้ $\mathcal{X} = \{1, 2, 3, \dots, m\}$ เมื่อ $m = 2^3 \cdot 3^2 \cdot 5^7 \cdot 7^5$

$$A = \{x \in \mathcal{X} \mid (x, m) = 1\}$$

$$B = \{x \in \mathcal{X} \mid (x, m) = 2\}$$

$$C = \{x \in \mathcal{X} \mid (x, m) = 14\}$$

$$D = \{x \in \mathcal{X} \mid (x, m) = 27\}$$

$$\text{และ } E = \{x \in \mathcal{X} \mid (x, m) \neq 12\}$$

$$\text{จงหา } n(A), n(B), n(C), n(D) \text{ และ } n(E)$$

วิธีทำ หา $n(A)$: เนื่องจาก $m = 2^3 \cdot 3^2 \cdot 5^7 \cdot 7^5$

$$\text{จะได้ว่า } n(A) = \phi(m) = \phi(2^3 \cdot 3^2 \cdot 5^7 \cdot 7^5)$$

$$= 2^3 \cdot 3^2 \cdot 5^7 \cdot 7^5 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right)$$

$$= 2^6 \cdot 3^2 \cdot 5^6 \cdot 7^4$$

$$\text{ดังนั้น } n(A) = 2^6 \cdot 3^2 \cdot 5^6 \cdot 7^4$$

หา $n(B)$: เนื่องจาก $2 \mid m$ จะได้ว่าถ้า $x \in A$ แล้ว $(2x, m) = 2$

ให้ $X = \{2x \mid x \in A\}$ ฉะนั้น $B = X \cap \mathcal{Z}$

$$\text{จะได้ว่า } n(B) = n(X \cap \mathcal{Z}) = \frac{n(X)}{2}$$

$$= \phi(2^2 \cdot 3^2 \cdot 5^7 \cdot 7^5)$$

$$= 2^2 \cdot 3^2 \cdot 5^7 \cdot 7^5 (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{7})$$

$$\text{ดังนั้น } n(B) = 2^5 \cdot 3^2 \cdot 5^6 \cdot 7^4$$

หา $n(C)$: ในทำนองเดียวกัน

$$n(C) = \phi(2^2 \cdot 3^2 \cdot 5^7 \cdot 7^4)$$

$$= 2^2 \cdot 3^2 \cdot 5^7 \cdot 7^4 (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{7})$$

$$\text{ดังนั้น } n(C) = 2^5 \cdot 3^2 \cdot 5^6 \cdot 7^3$$

หา $n(D)$: เนื่องจาก $27 \nmid m$ จะได้ว่า $D = \emptyset$

$$\text{ดังนั้น } n(D) = 0$$

หา $n(E)$: ให้ $E' = \{x \in \mathcal{Z} \mid (x, m) = 12\}$

$$\text{จะได้ } n(E) = n(\mathcal{Z}) - n(E')$$

$$= 2^3 \cdot 3^2 \cdot 5^7 \cdot 7^5 - \phi(2 \cdot 3 \cdot 5^7 \cdot 7^5)$$

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

$$2 \cdot 3 \cdot 5^7 \cdot 7^5 (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{7})$$

$$\text{ดังนั้น } n(E) = 2^3 \cdot 3^2 \cdot 5^7 \cdot 7^5 - 2^4 \cdot 3 \cdot 5^6 \cdot 7^4$$

□

ปัญหา 8 จงตรวจสอบว่า สำหรับจำนวนเต็มบวก $n > 1$, $\sigma(n) + \phi(n) = n \tau(n)$ หรือไม่

วิธีทำ ให้ n เป็นจำนวนเต็มบวกที่มากกว่า 1

กรณี 1 ถ้า n เป็นจำนวนเฉพาะ จะได้ว่า $\sigma(n) = n + 1$, $\tau(n) = 2$

$$\text{และ } \phi(n) = n - 1 \quad \text{เพราะว่า } (n + 1) + (n - 1) = n \cdot 2$$

$$\text{ดังนั้น } \sigma(n) + \phi(n) = n \tau(n)$$

กรณี 2 ถ้า n ไม่เป็นจำนวนเฉพาะและ $n > 1$ จะได้ว่า $\phi(n) < n$

ถ้าให้ $\tau(n) = k$ และตัวหารของ n คือ $d_1 = 1, d_2, d_3, \dots, d_k = n$ ซึ่ง

$$d_1 < d_2 < d_3 < \dots < d_k$$

จะได้ว่า $\tau(n) = k \geq 3$ และ $d_2 < n$ ซึ่งทำให้ $n - d_2 \geq 1$

$$\begin{aligned}\text{เราพบว่า } n\tau(n) - \sigma(n) &= nk - (d_1 + d_2 + \cdots + d_k) \\ &= (n - d_1) + (n - d_2) + \cdots + (n - d_k) \\ &\geq (n - d_1) + (n - d_2) + \cdots + (n - d_k) \\ &\geq (n - 1) + 1 + 0 = n\end{aligned}$$

เพราะฉะนั้น $n\tau(n) - \sigma(n) \geq n$ แต่ $\phi(n) < n$

ดังนั้นสรุปได้ว่า $\sigma(n) + \phi(n) < n\tau(n)$ ซึ่งทำให้ $\sigma(n) + \phi(n) \neq n\tau(n)$

สำหรับจำนวนเต็ม $n > 1$ และเป็นจำนวนประกอบ

ดังนั้นจากทั้งสองกรณี $\sigma(n) + \tau(n) = n\tau(n)$ เป็นจริงเมื่อ n เป็นจำนวนเฉพาะเท่านั้น $\square$

ปัญหา 8 ในสมัยกรีกโบราณค้นพบว่าจำนวนธรรมชาติ n ที่มีสมบัติว่า n เท่ากับผลบวกของตัวหารที่เป็นบวกของ n ยกเว้น n เช่นพิจารณา $n = 28$ จะได้ว่าตัวหารของ 28 ที่ไม่ใช่ 28 คือ 1, 2, 4, 7, 14 และพบว่า $1 + 2 + 4 + 7 + 14 = 28$ เราเรียก $n = 28$ นี้ว่า **จำนวนสมบูรณ์** ตัวอย่างของจำนวนสมบูรณ์ 5 จำนวนแรกคือ 6, 28, 496, 8128, 33550336 และในปี ค.ศ. 2004 เราพบจำนวนสมบูรณ์เพิ่มขึ้นเป็น 40 จำนวน โดยจำนวนที่ใหญ่ที่สุดคือ $2^{20996001}(2^{20996001} - 1)$ ซึ่งมีจำนวนเลขโดดมากกว่า 6 ล้านหลัก จากการศึกษาเรื่องฟังก์ชันเลขคณิตเราพบว่า

n เป็นจำนวนสมบูรณ์ ก็ต่อเมื่อ $\sigma(n) = 2n$

ในศตวรรษที่ 18 ออยเลอร์ได้พิสูจน์ว่า “ทุก ๆ จำนวนเต็มคู่บวก m ที่เป็นจำนวนสมบูรณ์สามารถเขียนอยู่ในรูป $m = 2^{n-1}(2^n - 1)$ เมื่อ $2^n - 1$ เป็นจำนวนเฉพาะ”

การแสดงผลของออยเลอร์ใช้สมบัติดังนี้

1. ถ้า $2^n - 1$ เป็นจำนวนเฉพาะ แล้ว n เป็นจำนวนเฉพาะด้วย
2. ถ้า $(a, b) = 1$ แล้ว $\sigma(ab) = \sigma(a)\sigma(b)$

จากการใช้ความรู้พื้นฐานข้างต้น จงหาจำนวนสมบูรณ์ n ทั้งหมดที่ทำให้ $\sigma(\sigma(n))$ เป็นจำนวนสมบูรณ์ด้วย

วิธีทำ กรณี 1 ถ้า n เป็นจำนวนเต็มคี่ที่เป็นจำนวนสมบูรณ์

จะได้ว่า $\sigma(n) = 2n$ และ $(2, n) = 1$

พิจารณา $\sigma(\sigma(n)) = \sigma(2n) = \sigma(2)\sigma(n) = 3\sigma(n) = 3 \cdot 2n = 6n$

เห็นได้ชัดว่า $6n$ เป็นจำนวนเต็มคู่ และถ้าให้ $6n$ เป็นจำนวนสมบูรณ์ จะได้ว่า

$$6n = 2^{p-1}(2^p - 1) \quad \text{สำหรับจำนวนเฉพาะ } p \text{ บางตัว}$$

(เพราะว่าถ้า $2^p - 1$ เป็นจำนวนเฉพาะแล้ว p จะต้องเป็นจำนวนเฉพาะด้วย)

เนื่องจาก n เป็นจำนวนเต็มคี่ จะได้ว่า $6n$ มี 2 เป็นตัวประกอบเพียงตัวเดียว

ดังนั้น $2^{p-1} = 2^1$ จึงทำให้ $p = 2$ และ $6n = 2^{p-1}(2^p - 1) = 2^1(2^2 - 1)$

จึงส่งผลให้ $n = 1$ ซึ่งเป็นไปไม่ได้ เพราะว่า 1 ไม่ใช่จำนวนสมบูรณ์

ดังนั้นสรุปได้ว่า ไม่มีจำนวนเต็มคี่ n ที่เป็นจำนวนสมบูรณ์ที่ทำให้ $\sigma(\sigma(n))$

เป็นจำนวนสมบูรณ์ด้วย

กรณี 2 ถ้า n เป็นจำนวนเต็มคู่ที่เป็นจำนวนสมบูรณ์ จะได้ว่า

$$n = 2^{p-1}(2^p - 1) \quad \text{เมื่อ } 2^p - 1 \text{ เป็นจำนวนเฉพาะ}$$

ในกรณีนี้เราพบว่า $(2, 2^p - 1) = 1$ ดังนั้น

$$\begin{aligned} \sigma(\sigma(n)) &= \sigma(2n) = \sigma(2 \cdot 2^{p-1}(2^p - 1)) \\ &= \sigma(2^p(2^p - 1)) \\ &= \sigma(2^p)\sigma(2^p - 1) \\ &= (1 + 2 + 2^2 + 2^3 + \dots + 2^p)[1 + (2^p - 1)] \\ &= (2^{p+1} - 1) \cdot 2^p \end{aligned}$$

$$\text{ดังนั้น } \sigma(\sigma(n)) = 2^p(2^{p+1} - 1)$$

ถ้าเรายอมรับว่า $\sigma(\sigma(n))$ เป็นจำนวนสมบูรณ์ จะได้ว่า $2^{p+1} - 1$ เป็นจำนวนเฉพาะ

ดังนั้น $p + 1$ จะต้องเป็นจำนวนเฉพาะด้วย ซึ่งทำให้ได้ว่า p และ $p + 1$ เป็นจำนวนเฉพาะทั้งคู่ จาก p และ $p + 1$ เป็นจำนวนเฉพาะ จะได้ว่า $p = 2$ เท่านั้น

จึงจะทำให้ $p + 1 = 3$ เป็นจำนวนเฉพาะด้วย

$$\text{ดังนั้น } n = 2^{p-1}(2^p - 1) = 2(2^2 - 1) = 6$$

$$\text{และทำให้ } \sigma(\sigma(n)) = \sigma(\sigma(6)) = \sigma(12) = 28$$

เพราะฉะนั้น จำนวนเต็ม n ที่เป็นจำนวนสมบูรณ์และทำให้ $\sigma(\sigma(n))$ เป็นจำนวนสมบูรณ์ด้วย มีเพียงจำนวนเดียวเท่านั้นคือ $n = 6$ □

แบบฝึกหัดเรื่อง ฟังก์ชันเลขคณิต

1. จงแสดงว่ามีจำนวนเต็มบวก m และ n อย่างน้อยสองคู่ที่ทำให้ $\sigma(m) = \sigma(n) = m + n$
2. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $\sigma(2n) = 2n$
3. สำหรับจำนวนเต็มบวก $n > 1$ จงพิสูจน์ว่า มีจำนวนเต็มบวก n_1 และ n_2 ที่ทำให้

$$\tau(n_1) + \tau(n_2) = n \quad \text{และ} \quad \sigma(n_1) + \sigma(n_2) = 2n$$
4. จงแสดงว่า ไม่มีจำนวนเต็มบวก n ที่ทำให้ $\sigma(n) = 10$
(ข้อเสนอแนะ $n > 1, \sigma(n) > n$)
5. ถ้า $n = 2(2p - 1)$ โดยที่ p และ $2p - 1$ เป็นจำนวนเฉพาะคี่ทั้งคู่
จงแสดงว่า $\phi(n) = \phi(n + 2)$
6. จงพิสูจน์ว่า ถ้า p และ $2p + 1$ เป็นจำนวนเฉพาะคี่ทั้งคู่ แล้ว $n = 4p$ จะสอดคล้องกับ

$$\phi(n + 2) = \phi(n) + 2$$
7. จงแสดงว่า ถ้า $n = 2^k$ หรือ $2^k \cdot 3^j$ ซึ่ง k และ j เป็นจำนวนเต็มบวก แล้ว $\phi(n) \mid n$
8. ถ้า p เป็นจำนวนเฉพาะและ $k \geq 2$ แล้ว จงแสดงว่า $\phi(\phi(p^k)) = p^{k-2}\phi(p - 1)^2$
9. จงแสดงว่าทุก ๆ จำนวนเต็มบวก $2n$ จะมีจำนวนเต็มบวก n_1 และ n_2 ซึ่ง $\phi(n_1) + \phi(n_2) = 2n$
10. กำหนดให้ d และ n เป็นจำนวนเต็มบวกที่ $d \mid n$ จงแสดงว่า $\phi(d) \mid \phi(n)$
11. จงพิสูจน์ว่า $\tau(n)$ เป็นจำนวนเต็มบวกก็ต่อเมื่อ n เป็นกำลังสองสมบูรณ์
12. จงพิสูจน์ว่า $\sigma(n)$ เป็นจำนวนเต็มก็ต่อเมื่อ n เป็นกำลังสองสมบูรณ์หรือสองเท่าของจำนวนกำลังสองสมบูรณ์
(ข้อเสนอแนะ ถ้า p เป็นจำนวนเต็มคี่แล้ว $1 + p + p^2 + \dots + p^k$ เป็นจำนวนเต็มก็ต่อเมื่อ k เป็นจำนวนเต็มคู่)
13. ถ้า $\phi(m) = \phi(mn)$ และ $n > 1$ จงพิสูจน์ว่า $n = 2$ และ m เป็นจำนวนเต็มคี่
14. ให้ $f(n)$ แทนผลบวกของจำนวนเต็มบวก k ซึ่ง $k < n$ และ $(k, n) = 1$
จงพิสูจน์ว่า $2f(n) = n\phi(n)$
15. จาก $f(n)$ ที่นิยามในข้อ 14. จงพิสูจน์ว่า ถ้า $f(m) = f(n)$ แล้ว $m = n$
16. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $\phi(n) + \sigma(n) = 2n$
17. จงหาจำนวนเต็มบวก $n \leq 100$ ที่ทำให้ $\sigma(n) = 2n$
18. จงหาจำนวนเต็มบวก n ทั้งหมด ที่ทำให้ $\tau(n) = 10$
19. กำหนดให้ $m = 3^k \cdot 568$ และ $n = 3^k \cdot 638$ สำหรับ $k \geq 0$
จงพิสูจน์ว่า $\tau(m) = \tau(n)$, $\sigma(m) = \sigma(n)$ และ $\phi(m) = \phi(n)$
20. กำหนดให้ $n = 14, 260$ และ 957 จงแสดงว่า $\sigma(n) = \sigma(n + 1)$
21. จงแสดงว่ามีจำนวนเต็มบวก m และ n ที่แตกต่างกันไม่จำกัดคู่ที่ทำให้ $\sigma(m^2) = \sigma(n^2)$
22. จงหาจำนวนเต็มบวก n ที่ทำให้ $\sigma(n) = 546$

23. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $\phi(n)$ เป็นจำนวนเต็มคี่
24. จงหาจำนวนเต็ม n ทั้งหมดที่ทำให้ $\phi(n) = 24$
25. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $\phi(n) = \phi(2n)$
26. จงหาจำนวนเต็มบวก n ทั้งหมดที่ทำให้ $\phi(2n) > \phi(n)$
27. จงหาจำนวนเต็ม n ที่น้อยที่สุดที่ทำให้ $\phi(n) = n$
28. จงหาจำนวนเต็มบวก n ที่น้อยที่สุดที่ทำให้ $\tau(n) = n$
29. จงหาจำนวนเต็มบวก n ที่น้อยที่สุดที่ทำให้ $\phi(n) = 6$
30. จงหาจำนวนเต็มบวก m ที่น้อยที่สุดที่มี n ซึ่ง $m \neq n$ และทำให้ $\phi(m) = \phi(n)$
31. ถ้า $n \geq 1$ จงพิสูจน์ว่า $\frac{(2n)!}{(n!)^2}$ เป็นจำนวนเต็มคู่
32. ให้ p เป็นจำนวนเฉพาะที่เป็นตัวหารของ $\frac{(2n)!}{(n!)^2}$ ถ้า $\frac{(2n)!}{(n!)^2} = p^a A$ เมื่อ $(p, A) = 1$
 จงแสดงว่า
$$a = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

บทที่ 6

คอนกรูเอนซ์

จากทฤษฎีบท 2.4.9 เมื่อ $a, b \in \mathbb{N}$ และ $b = aq + r$, $0 \leq r < a$ จะได้ว่า $(a, b) = (a, r)$ นี่คือการแสดงว่าถ้า a, b เป็นจำนวนเต็มบวกที่มีค่ามาก ๆ ในการหา (a, b) อาจทำได้ยากกว่าการหา (a, r) ซึ่ง a, r เป็นจำนวนเต็มบวกที่ r มีค่าลดลง และจากขั้นตอนวิธีนี้ทำให้เราสามารถหา (a, b) ได้โดยการทำซ้ำ ๆ

ในการตรวจสอบจำนวนเต็มบวกที่ให้มาว่าจะหารด้วย 2 ลงตัวหรือไม่ เราอาจดูเฉพาะค่าประจำหลักหน่วยเท่านั้น ก็สามารถสรุปได้ ในการตรวจสอบว่าจำนวนเต็มบวกที่ให้มาว่าจะหารด้วย 5 ลงตัวหรือไม่ เราอาจดูที่หลักหน่วยของจำนวนนั้นเท่านั้น เช่นกัน กล่าวคือ

ถ้า $n = a_k a_{k-1} \dots a_2 a_1 a_0$ เป็นการเขียนแทน n ในระบบฐาน 10 จะได้ว่า

$$2 \mid n \quad \text{ก็ต่อเมื่อ} \quad 2 \mid a_0$$

และ $5 \mid n \quad \text{ก็ต่อเมื่อ} \quad 5 \mid a_0$

จากแนวคิดที่กล่าวมาข้างต้นคือส่วนหนึ่งของ คอนกรูเอนซ์ (congruence) และแนวคิดที่เรียกว่าคอนกรูเอนซ์ นี้ได้ปรากฏขึ้นอย่างเป็นระบบ และได้แสดงให้เห็นว่าเป็นเครื่องมือที่สำคัญในการศึกษาทฤษฎีจำนวน ในปี ค.ศ. 1801 โดย คาร์ล ฟรีดริค เกาส์ (Carl Friedrich Gauss ค.ศ. 1777 – 1855) นักคณิตศาสตร์ชาวเยอรมัน ผู้ซึ่งได้รับการยกย่องว่าเป็นนักคณิตศาสตร์ที่ยอดเยี่ยมตลอดกาล เกาส์ได้กำหนดบทนิยามของคอนกรูเอนซ์ ซึ่งปรากฏในหนังสือของเขาเอง ชื่อ Disquisitiones Arithmeticae ในขณะที่เขามีอายุเพียง 24 ปี และผลงานชิ้นนี้ของเกาส์ได้นำไปสู่พัฒนาการทางด้านทฤษฎีจำนวนอย่างมาก

มีเรื่องเล่าว่าเกาส์ได้ส่งผลงานชิ้นนี้ไปยัง French Academy ในปี ค.ศ. 1800 เพื่อขอเผยแพร่ผลงาน แต่ถูกปฏิเสธจากผู้อ่านผลงานในขณะนั้น โดยผู้อ่านผลงานให้เหตุผลว่าผลงานชิ้นนี้ไม่ได้คุณภาพ อย่างไรก็ตาม เมื่อมีผู้พยายามตรวจสอบเพื่อหาข้อผิดพลาดตามเรื่องที่เล่านี้ ผลปรากฏว่าในปี ค.ศ. 1935 ทาง French Academy รายงานว่าไม่มีประวัติการส่งผลงานของเกาส์ปรากฏอยู่ในฐานข้อมูล

เลโอพอลด์ โครเนเคอร์ (Leopold Kronecker ค.ศ. 1823 – 1891) นักคณิตศาสตร์ชาวเยอรมัน ได้กล่าวสดุดีเกาส์ว่า “น่าประหลาดใจจริง ๆ ที่คนเพียงคนเดียวและอายุก็ยังน้อยสามารถที่จะนำแสงสว่างและผลงานอันล้ำค่ามาตีแผ่และเหนือสิ่งอื่นใด การนำเสนอผลงานใหม่นี้ทำได้อย่างดีและรวบรวมได้อย่างเหมาะสม” ผลงานของเกาส์ยังมี

อีกมากมายทั้งในสาขาคณิตศาสตร์บริสุทธิ์และคณิตศาสตร์ประยุกต์เกาส์ได้รับปริญญเอกเมื่อเขามีอายุ 22 ปี โดยการเขียนวิทยานิพนธ์ที่แสดงการพิสูจน์ ทฤษฎีบทพื้นฐานทางพีชคณิต (*The Fundamental Theorem of Algebra*)

เนื่องจากเกาส์ได้สร้างผลงานไว้มากมาย รวมทั้งผลงานทางด้านวิทยาศาสตร์ประกอบกับในช่วงคริสต์ศตวรรษที่ 19 มีนักคณิตศาสตร์และนักวิทยาศาสตร์ที่มีชื่อเสียงเกิดขึ้นมากมายในยุโรป เกาส์ได้รับการเสนอชื่อให้เป็นนักคณิตศาสตร์ที่ยอดเยี่ยมที่สุด และเขาได้รับการยกย่องว่าเป็น *Princeps Mathematicorum* (Prince of Mathematicians) ซึ่งการยกย่องนี้ถือได้ว่าเป็นผู้ที่มีเกียรติเทียบได้กับ อาร์คิมิดีส (Archimedes ประมาณ 287 – 212 ปีก่อนคริสต์ศักราช) และ เซอร์ ไอแซก นิวตัน (Sir Isaac Newton ค.ศ.1643 - 1727) คำกล่าวของเกาส์ที่แสดงให้เห็นถึงความสำคัญของคณิตศาสตร์และทฤษฎีจำนวน ซึ่งพวกเราชาวคณิตศาสตร์และวิทยาศาสตร์มักจะไดยินอยู่เสมอก็คือ

“Mathematics is the Queen of Science, and the theory of number is the Queen of Mathematics.”

6.1 นิยามและสมบัติของคอนกรูเอนซ์

ในบทแรกของ *Disquisitiones Arithmeticae* เกาส์ได้ให้บทนิยามและสมบัติเบื้องต้นของคอนกรูเอนซ์ (congruence) และเขาได้ใช้สัญลักษณ์ “ $\equiv$ ” แทนคอนกรูเอนซ์ของจำนวนเต็ม 2 จำนวน เนื่องจากสมบัติของคอนกรูเอนซ์และสมบัติของการเท่ากันของจำนวนเต็มมีข้อคล้ายคลึงกันอย่างมากจนน่าอัศจรรย์

บทนิยาม 6.1.1 ให้ n เป็นจำนวนเต็มบวก สำหรับจำนวนเต็ม a และ b เราจะกล่าวว่า a คอนกรูเอนซ์กับ b มอดุโล n เขียนแทนด้วย $a \equiv b \pmod{n}$ ก็ต่อเมื่อ n หาร $a - b$ ลงตัว และถ้า n หาร $a - b$ ไม่ลงตัว เราจะกล่าวว่า a ไม่คอนกรูเอนซ์กับ b มอดุโล n ซึ่งเขียนแทนด้วยสัญลักษณ์ $a \not\equiv b \pmod{n}$ ในที่นี้เรียกจำนวนเต็มบวก n ว่า **มอดุลัส (modulus)**

จากบทนิยามเราพบว่า สำหรับจำนวนเต็ม a, b และจำนวนเต็มบวก n จะได้ว่า

- (1) $a \equiv b \pmod{n}$ ก็ต่อเมื่อ $n \mid (a - b)$
- (2) $a \not\equiv b \pmod{n}$ ก็ต่อเมื่อ $n \nmid (a - b)$
- (3) $a \equiv b \pmod{1}$ และ $a \equiv a \pmod{n}$

ตัวอย่าง 1

(1.1)	$10 \equiv 2 \pmod{4}$	เพราะว่า	$4 \mid (10 - 2)$
(1.2)	$7 \not\equiv 3 \pmod{3}$	เพราะว่า	$3 \nmid (7 - 3)$
(1.3)	$-31 \equiv 11 \pmod{7}$	เพราะว่า	$7 \mid (-31 - 11)$
(1.4)	$37 \equiv 112 \pmod{25}$	เพราะว่า	$25 \mid (37 - 112)$
(1.5)	$2^{10} \equiv 1 \pmod{3}$	เพราะว่า	$3 \mid (2^{10} - 1)$
(1.5)	$-15 \not\equiv -63 \pmod{7}$	เพราะว่า	$7 \nmid (-15 + 63)$

□

จากบทนิยามของคอนกรูเอนซ์ ทำให้ได้ข้อสรุปอีกรูปแบบหนึ่ง คือ

ทฤษฎีบท 6.1.2 สำหรับจำนวนเต็ม a และ b ใด ๆ

$a \equiv b \pmod{n}$ ก็ต่อเมื่อ a และ b มีเศษที่เหลือจากการหารด้วย n เท่ากัน

บทพิสูจน์ $(\Rightarrow)$ ให้ $a, b \in \mathbb{Z}$ และ $n \in \mathbb{N}$ โดยขั้นตอนวิธีการหาร จะมี $k_1, k_2, r_1, r_2 \in \mathbb{Z}$ ที่ทำให้

$$\left. \begin{aligned} a &= nk_1 + r_1, \quad 0 \leq r_1 < n \\ \text{และ} \quad b &= nk_2 + r_2, \quad 0 \leq r_2 < n \end{aligned} \right\} \dots\dots\dots (*)$$

ดังนั้น $a - b = n(k_1 - k_2) + (r_1 - r_2)$ โดยที่ $0 \leq |r_1 - r_2| < n$

จาก $n \mid (a - b)$ และ $n \mid n(k_1 - k_2)$ จะได้ว่า $n \mid (r_1 - r_2)$

ถ้า $0 < |r_1 - r_2| < n$ จะได้ว่า $n \nmid (r_1 - r_2)$ ดังนั้น $|r_1 - r_2| = 0$

ดังนั้น $r_1 = r_2$

$(\Leftarrow)$ จาก $(*)$ สมมติว่า $r_1 = r_2$ จะได้ว่า $a - b = (nk_1 + r_1) - (nk_2 + r_2)$

ดังนั้น $a - b = n(k_1 - k_2)$ แสดงว่า $n \mid (a - b)$

นั่นคือ $a \equiv b \pmod{n}$ ■

ตัวอย่าง 2 จงหาเศษที่เกิดจากการหาร 3^{10} ด้วย 8

วิธีทำ เนื่องจาก $3^{10} \equiv 1 \pmod{8}$ ดังนั้น 3^{10} หารด้วย 8 แล้วเหลือเศษ 1 □

สมบัติของคอนกรูเอนซ์

ทฤษฎีบทต่อไปนี้จะกล่าวเกี่ยวกับข้อคล้ายคลึงกันระหว่างการเท่ากันและการคอนกรูเอนซ์กันของจำนวนเต็ม

ทฤษฎีบท 6.1.3 ให้ $n \in \mathbb{N}$ และ $a, b, c, d, x, y \in \mathbb{Z}$ จะได้ว่า

1. ถ้า $a \equiv b \pmod{n}$ แล้ว $b \equiv a \pmod{n}$
2. ถ้า $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$ แล้ว $a \equiv c \pmod{n}$
3. ถ้า $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$ แล้ว $a + c \equiv b + d \pmod{n}$
และ $ac \equiv bd \pmod{n}$
4. ถ้า $a \equiv b \pmod{n}$ แล้ว $a + c \equiv b + c \pmod{n}$
และ $ac \equiv bc \pmod{n}$
5. ถ้า $a \equiv b \pmod{n}$ แล้ว $a^k \equiv b^k \pmod{n}$ สำหรับจำนวนเต็มบวก k
6. ถ้า $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$
แล้ว $ax + cy \equiv bx + dy \pmod{n}$
7. ถ้า $a \equiv b \pmod{n}$ และ $d \mid n$ โดยที่ $d > 0$ แล้ว $a \equiv b \pmod{d}$

บทพิสูจน์ ให้ $n \in \mathbb{N}$ และ $a, b, c, d, x, y \in \mathbb{Z}$

1. ให้ $a \equiv b \pmod{n}$
 จะได้ว่า $n \mid (a - b)$ แสดงว่ามี $k \in \mathbb{Z}$ ซึ่ง $a - b = nk$
 ดังนั้น $b - a = n(-k)$ ทำให้ได้ว่า $n \mid (b - a)$
 นั่นคือ $b \equiv a \pmod{n}$
2. ให้ $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$
 จะได้ว่า $n \mid (a - b)$ และ $n \mid (b - c)$
 แสดงว่า $n \mid [(a - b) + (b - c)]$ ทำให้ได้ว่า $n \mid (a - c)$
 ดังนั้น $a \equiv c \pmod{n}$
3. ให้ $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$
 จะได้ว่า $n \mid (a - b)$ และ $n \mid (c - d)$
 แสดงว่า $n \mid [(a - b) + (c - d)]$
 และจะมี $k_1, k_2 \in \mathbb{Z}$ ซึ่ง $a - b = nk_1$ และ $c - d = nk_2$
 ดังนั้น $n \mid [(a + c) - (b + d)]$
 และ $ac = (nk_1 + b)(nk_2 + d) = n(nk_1k_2 + k_1d + bk_2) + bd$
 ทำให้ได้ว่า $n \mid (ac - bd)$
 นั่นคือ $a + c \equiv b + d \pmod{n}$ และ $ac \equiv bd \pmod{n}$
4. ให้ $a \equiv b \pmod{n}$ เพราะว่า $c \equiv c \pmod{n}$ จากข้อ 3. ข้างต้น
 จะได้ว่า $a + c \equiv b + d \pmod{n}$ และ $ac \equiv bc \pmod{n}$
5. ให้ $a \equiv b \pmod{n}$ และ $k \in \mathbb{N}$ โดยหลักอุปนัยเชิงคณิตศาสตร์
 $k = 1$ เป็นจริงโดยการกำหนดให้
 สมมติว่า $a^k \equiv b^k \pmod{n}$ เป็นจริง
 โดยข้อ 3. จะได้ว่า $a \cdot a^k \equiv b \cdot b^k \pmod{n}$
 ดังนั้น $a^{k+1} \equiv b^{k+1} \pmod{n}$
 เพราะฉะนั้น $a^k \equiv b^k \pmod{n}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก k
6. ให้ $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$ โดยข้อ 4. ข้างต้น
 จะได้ว่า $ax \equiv bx \pmod{n}$ และ $cy \equiv dy \pmod{n}$
 โดยข้อ 3. จะได้ $ax + cy \equiv bx + dy \pmod{n}$
7. ให้ $a \equiv b \pmod{n}$ และ $d \mid n$ โดยที่ $d > 0$
 จะได้ว่า $n \mid (a - b)$
 ดังนั้น $d \mid (a - b)$ นั่นคือ $a \equiv b \pmod{d}$



หมายเหตุ จากความจริงที่ว่า

$$(i) \quad a \equiv a \pmod{n}$$

$$(ii) \quad \text{ถ้า } a \equiv b \pmod{n} \text{ แล้ว } b \equiv a \pmod{n}$$

$$(iii) \quad \text{ถ้า } a \equiv b \pmod{n} \text{ และ } b \equiv c \pmod{n} \text{ แล้ว } a \equiv c \pmod{n}$$

สรุปได้ว่าความสัมพันธ์คอนกรูเอนซ์มอดุโล n เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ (equivalence relation on $\mathbb{Z}$)

ตัวอย่าง 3 จงแสดงว่า 41 หาร $2^{20} - 1$ ลงตัว

พิสูจน์ เนื่องจาก $2^5 \equiv -9 \pmod{41}$

โดยทฤษฎีบท 6.1.3 ข้อ 5. จะได้ว่า $(2^5)^4 \equiv (-9)^4 \pmod{41}$.

นั่นคือ $2^{20} \equiv (81)(81) \pmod{41}$

แต่ $81 \equiv -1 \pmod{41}$

โดยทฤษฎีบท 6.1.3 ข้อ 5. อีกครั้ง จะได้ว่า $(81)(81) \equiv (-1)(-1) \pmod{41}$

ฉะนั้นจาก $2^{20} \equiv (81)(81) \pmod{41}$ และ $(81)(81) \equiv 1 \pmod{41}$

โดยทฤษฎีบท 6.1.3 ข้อ 2. จะได้ว่า $2^{20} \equiv 1 \pmod{41}$

ดังนั้น $41 \mid (2^{20} - 1)$ □

ตัวอย่าง 4 จงหาเศษที่เกิดจากการหาร 7^{10} ด้วย 51

วิธีทำ เราต้องการหาเศษ x ซึ่ง $0 \leq x < 51$ ที่ทำให้ $7^{10} \equiv x \pmod{51}$

เนื่องจาก $49 \equiv -2 \pmod{51}$ จะได้ว่า $(49)^5 \equiv (-2)^5 \pmod{51}$

เพราะฉะนั้น $7^{10} \equiv (7^2)^5 = (49)^5 \equiv (-2)^5 = -32 \pmod{51}$

เนื่องจาก $-32 \equiv 19 \pmod{51}$

ฉะนั้นจาก $7^{10} \equiv -32 \pmod{51}$ และ $-32 \equiv 19 \pmod{51}$

จะได้ว่า $7^{10} \equiv 19 \pmod{51}$

ดังนั้น เศษที่เกิดจากการหาร 7^{10} ด้วย 51 คือ 19 □

ปัญหา 5 จงหาเศษที่เกิดจากการหาร 2^{11} ด้วย 23

จากสมบัติของคอนกรูเอนซ์เท่าที่ได้กล่าวมา เราพบว่า คอนกรูเอนซ์มีสมบัติที่คล้ายกับสมบัติของการเท่ากัน แต่อาจมีสมบัติบางข้อที่ต้องพึงระวัง เช่น ในระบบจำนวนเต็ม ถ้า $ax = ay$ และ $a \neq 0$ แล้ว $x = y$ แต่เราจะพบว่า “ถ้า $ax \equiv ay \pmod{m}$ และ $a \neq 0$ แล้ว $x \equiv y \pmod{m}$ ” เป็นคำกล่าวที่ไม่จริง

ทฤษฎีบท 6.1.4 ให้ $n \in \mathbb{N}$ และ $a, b, x, y \in \mathbb{Z}$ จะได้ว่า

1. ถ้า $a \equiv b \pmod{n}$ แล้ว $(a, n) = (b, n)$
2. $ax \equiv ay \pmod{n}$ ก็ต่อเมื่อ $x \equiv y \pmod{\frac{n}{(a, n)}}$
3. ถ้า $ax \equiv ay \pmod{n}$ และ $(a, n) = 1$ แล้ว $x \equiv y \pmod{n}$
4. ถ้า $ax \equiv ay \pmod{n}$ และ n เป็นจำนวนเฉพาะซึ่ง $n \nmid a$ แล้ว $x \equiv y \pmod{n}$

$n)$

บทพิสูจน์ 1. ให้ $a \equiv b \pmod{n}$ จะได้ว่า $n \mid (a - b)$

แสดงว่ามี $k \in \mathbb{Z}$ ซึ่ง $a - b = nk$

นั่นคือ $a = b + nk$ ให้ $(b, n) = d$ โดยทฤษฎีบท 2.4.7 จะได้ว่า

$(b + nk, n) = d$ นั่นคือ $(a, n) = (b, n)$

2. $(\Rightarrow)$ ให้ $ax \equiv ay \pmod{n}$ จะได้ว่า $n \mid (ax - ay)$

แสดงว่ามี $k \in \mathbb{Z}$ ซึ่ง $a(x - y) = nk$

ให้ $d = (a, n)$ จะได้ $d \mid a$ และ $d \mid n$

ดังนั้น $\frac{n}{d} \mid \frac{a}{d}(x - y)$

โดยทฤษฎีบท 2.4.6 จะได้ $(\frac{a}{d}, \frac{n}{d}) = 1$

ดังนั้นโดยทฤษฎีบท 2.4.8 ข้อ 3. สรุปได้ว่า $\frac{n}{d} \mid (x - y)$

นั่นคือ $x \equiv y \pmod{\frac{n}{(a, n)}}$

$(\Leftarrow)$ ให้ $d = (a, n)$ และ $x \equiv y \pmod{\frac{n}{d}}$ จะได้ $\frac{n}{d} \mid (x - y)$

แสดงว่ามี $k \in \mathbb{Z}$ ซึ่ง $x - y = \frac{n}{d}k$ ดังนั้น $a(x - y) = a(\frac{n}{d})k$

และจาก $d \mid a$ สรุปได้ว่า $n \mid a(x - y)$ นั่นคือ $ax \equiv ay \pmod{n}$

3. ให้ $ax \equiv ay \pmod{n}$ และ $(a, n) = 1$ โดยข้อ 2. ข้างต้น จะได้ว่า

$x \equiv y \pmod{\frac{n}{(a, n)}}$ นั่นคือ $x \equiv y \pmod{n}$

4. ให้ $ax \equiv ay \pmod{n}$ และ n เป็นจำนวนเฉพาะซึ่ง $n \nmid a$

แสดงว่า $(n, a) = 1$

โดยข้อ 3. ข้างต้น จะได้ว่า $x \equiv y \pmod{n}$ ■

ทฤษฎีบท 6.1.5 ให้ $a, b \in \mathbb{Z}$ และ $n_1, n_2, \dots, n_r$ เป็นจำนวนเต็มบวกใด ๆ จะได้ว่า

1. $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, \dots, r$
ก็ต่อเมื่อ $a \equiv b \pmod{[n_1, n_2, \dots, n_r]}$
2. ถ้า $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, \dots, r$ และ $n_1, n_2, \dots, n_r$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แล้ว $a \equiv b \pmod{n_1 n_2 \cdots n_r}$

- บทพิสูจน์** 1. $(\Rightarrow)$ ให้ $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, \dots, r$
 จะได้ว่า $n_i \mid (a - b)$ สำหรับ $i = 1, 2, \dots, r$
 แสดงว่า $a - b$ เป็นตัวคูณร่วมของ $n_1, n_2, \dots, n_r$
 โดยทฤษฎีบท 2.6.2 จะได้ $[n_1, n_2, \dots, n_r] \mid (a - b)$
 นั่นคือ $a \equiv b \pmod{[n_1, n_2, \dots, n_r]}$
 $(\Leftarrow)$ ให้ $a \equiv b \pmod{[n_1, n_2, \dots, n_r]}$ จะได้ $[n_1, n_2, \dots, n_r] \mid (a - b)$
 เนื่องจาก $n_i \mid [n_1, n_2, \dots, n_r]$ สำหรับ $i = 1, 2, \dots, r$
 ดังนั้น $n_i \mid (a - b)$ สำหรับ $i = 1, 2, \dots, r$
 นั่นคือ $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, \dots, r$
 2. ให้ $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, \dots, r$ และ $n_1, n_2, \dots, n_r$ เป็นจำนวนเฉพาะ
 สัมพัทธ์ทุกคู่ แสดงว่า $[n_1, n_2, \dots, n_r] = n_1 n_2 \cdots n_r$
 โดยข้อ 1. ข้างต้น จะได้ว่า $a \equiv b \pmod{n_1 n_2 \cdots n_r}$ ■

ทฤษฎีบท 6.1.6 ให้ $a \in \mathbb{Z}$ และ $n \in \mathbb{N}$ จะได้ว่ามี $r \in \mathbb{Z}$ ซึ่ง $0 \leq r < n$ เพียงค่าเดียว
 ที่ทำให้ $a \equiv r \pmod{n}$

บทพิสูจน์ ให้ $a \in \mathbb{Z}$ และ $n \in \mathbb{N}$ โดยขั้นตอนวิธีการหาร จะได้ว่า มี q, r เพียงคู่เดียวที่ทำให้

$$a = nq + r \quad \text{โดยที่} \quad 0 \leq r < n$$

 แสดงว่า $a - r = nq$
 ดังนั้น $a \equiv r \pmod{n}$ โดยที่ $0 \leq r < n$ (*)
 ต่อไปจะแสดงว่ามี r เพียงค่าเดียวที่สอดคล้องสมการ (*)
 ให้ $r_1, r_2 \in \mathbb{Z}$ ซึ่ง $0 \leq r_1 \leq r_2 < n$ ที่สอดคล้อง

$$a \equiv r_1 \pmod{n} \quad \text{และ} \quad a \equiv r_2 \pmod{n}$$

 จะได้ว่า $n \mid (a - r_1)$ และ $n \mid (a - r_2)$ โดยที่ $0 \leq r_2 - r_1 < n$
 ดังนั้น $n \mid [(a - r_1) - (a - r_2)]$ นั่นคือ $n \mid (r_2 - r_1)$
 ถ้า $0 < r_2 - r_1 < n$ จะได้ว่า $n \nmid (r_2 - r_1)$
 ดังนั้น $r_2 - r_1 = 0$ นั่นคือ $r_1 = r_2$
 เพราะฉะนั้นสำหรับจำนวนเต็ม a ใด ๆ จะมีจำนวนเต็ม r ซึ่ง $0 \leq r < n$ เพียงค่าเดียว
 ที่ทำให้ $a \equiv r \pmod{n}$ ■

จากทฤษฎีบท 6.1.6 เราพบว่า

- (1) ถ้า $r_1, r_2 \in \{0, 1, 2, \dots, n-1\}$ โดยที่ $r_1 \equiv r_2 \pmod{n}$ แล้ว $r_1 = r_2$
- (2) สมาชิกในเซต $\{0, 1, 2, \dots, n-1\}$ ที่ต่างกัน จะไม่คอนกรูเอนซ์กันในมอดุโล n
- (3) ทุก ๆ จำนวนเต็ม a จะมี $r \in \{0, 1, 2, \dots, n-1\}$ เพียงค่าเดียวที่ทำให้ $a \equiv r \pmod{n}$
 และค่า r นี้ คือเศษเหลือจากการหาร a ด้วย n

บทนิยาม 6.1.7 ถ้า $a \equiv b \pmod{n}$ จะเรียก b ว่าเป็น **ส่วนตกค้าง (residue)** ของ a มอดุโล n และเรียกเซตของจำนวนเต็ม $\{a_1, a_2, \dots, a_n\}$ ว่าเป็น **ระบบส่วนตกค้างบริบูรณ์ (complete residue system)** มอดุโล n ก็ต่อเมื่อ ทุก ๆ จำนวนเต็ม a จะมี a_i เพียงตัวเดียวที่ทำให้

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

ชั้นสมมูลของ a_i คือ $\{a \mid a \text{ เป็นจำนวนเต็มและ } a \equiv a_i \pmod{n}\}$ เรียกว่า

ชั้นส่วนตกค้าง (residue class) ของ a_i มอดุโล n

หมายเหตุ ให้ $x, q, r, n \in \mathbb{Z}$ โดยที่ $n \in \mathbb{N}$ และ $x = nq + r$ เราพบว่า $x \equiv r \pmod{n}$

และจะได้ว่า r เป็นส่วนตกค้างของ x มอดุโล n แต่ถ้าเรากำหนด $x = nq + r$

โดยที่ $0 \leq r < n$ เราจะเรียก r ว่า **ส่วนตกค้างที่ไม่เป็นลบค่าน้อยสุด**ของ x มอดุโล n

ดังนั้น $\{0, 1, 2, \dots, n-1\}$ เรียกว่า **ระบบส่วนตกค้างบริบูรณ์ที่ไม่เป็นลบค่าน้อยสุด**

(least non-negative residue system) มอดุโล n นั่นคือ จะมี $r \in \{0, 1, 2, \dots, n-1\}$

เพียงจำนวนเดียวเท่านั้นที่เป็นส่วนตกค้างของ x มอดุโล n

จากบทนิยามเราพบว่า

- (1) $\{0, 1, 2, \dots, n-1\}$ และ $\{1, 2, 3, \dots, n\}$ ต่างก็เป็นระบบส่วนตกค้างบริบูรณ์ มอดุโล n
- (2) ถ้า $\{a_1, a_2, \dots, a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n และ $c \in \mathbb{Z}$ แล้ว $\{a_1 + c, a_2 + c, \dots, a_n + c\}$ จะเป็นระบบส่วนตกค้างบริบูรณ์ มอดุโล n
- (3) $\{a_1, a_2, \dots, a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n ก็ต่อเมื่อ ทุก ๆ a_i, a_j ถ้า $a_i \equiv a_j \pmod{n}$ แล้ว $a_i = a_j$
- (4) ถ้า $\{a_1, a_2, \dots, a_n\}$ และ $\{b_1, b_2, \dots, b_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n แล้ว สำหรับทุก ๆ a_i จะมี b_j เพียงตัวเดียวที่ทำให้ $a_i \equiv b_j \pmod{n}$

ตัวอย่าง 6 (6.1) $\{7, 4, -2, 8, -4, 9, 20\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 7

เพราะว่า $7 \equiv 0 \pmod{7}$, $8 \equiv 1 \pmod{7}$, $9 \equiv 2 \pmod{7}$, $-4 \equiv 3 \pmod{7}$, $4 \equiv 4 \pmod{7}$, $-2 \equiv 5 \pmod{7}$ และ $20 \equiv 6 \pmod{7}$

(6.2) $\{0, 1, 2, 3, 4, 5\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 6 จะได้ว่า

$\{2, 3, 4, 5, 6, 7\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 6 แต่

$\{0, 2, 4, 6, 8, 10\}$ ไม่เป็นระบบส่วนตกค้างมอดุโล 6

เพราะว่า $2 \equiv 8 \pmod{6}$

□

จากตัวอย่าง (6.2) ทำให้สรุปได้ว่า ถ้า $\{a_1, a_2, \dots, a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n และ $c \in \mathbb{Z}$ แล้ว $\{ca_1, ca_2, \dots, ca_n\}$ อาจไม่เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

ทฤษฎีบทต่อไปนี้จะแสดงเงื่อนไขที่จำเป็นและเพียงพอที่จะทำให้ $\{ca_1, ca_2, \dots, ca_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

ทฤษฎีบท 6.1.8 ให้ $\{a_1, a_2, \dots, a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n และ $(c, n) = 1$ จะได้ว่า $\{ca_1, ca_2, \dots, ca_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

บทพิสูจน์ สมมติว่า $\{ca_1, ca_2, \dots, ca_n\}$ ไม่เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n แสดงว่าจะมี $i \neq j$ ซึ่ง $ca_i \equiv ca_j \pmod{n}$ เนื่องจาก $(c, n) = 1$ ดังนั้น $a_i \equiv a_j \pmod{n}$ เมื่อ $i \neq j$ ขัดแย้งกับสิ่งที่กำหนดให้ นั่นคือ $\{ca_1, ca_2, \dots, ca_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n ■

ปัญหา 7 ให้ $n > 2$ เป็นจำนวนเต็ม จงพิจารณาพร้อมทั้งให้เหตุผลประกอบว่าเซตใดต่อไปนี้ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

$$(7.1) \quad \{2, 4, 6, \dots, 2n\}$$

$$(7.2) \quad \{1^2, 2^2, 3^2, \dots, n^2\}$$

ปัญหา 8 จงหาเศษที่เกิดจากการหาร $1^5 + 2^5 + 3^5 + \dots + 99^5 + 100^5$ ด้วย 4

ปัญหา 9 จงพิสูจน์ว่า $19 \nmid (4n^2 + 4)$ สำหรับทุกจำนวนเต็มบวก n

โจทย์ปัญหา 6.1

1. จงหาเศษที่เกิดจากการหาร 3^{10} ด้วย 51 และการหาร 21^{10} ด้วย 51
2. จงแสดงว่า ถ้า $(n, 7) = 1$ แล้ว $n^6 - 1$ หารด้วย 7 ลงตัว
3. จงแสดงว่า $n^7 - n$ หารด้วย 42 ลงตัว สำหรับทุกจำนวนเต็มบวก n
4. จงหาเลขโดดหลักสุดท้ายของ 3^{400}
(ข้อเสนอแนะ ใช้ $3^4 \equiv 1 \pmod{5}$ และ $3^4 \equiv 1 \pmod{2}$)
5. จงหาเลขโดดสองหลักสุดท้ายของ 3^{4000}
(ข้อเสนอแนะ ใช้ $3^{20} \equiv 1 \pmod{25}$ และ $3^2 \equiv 1 \pmod{4}$
ดังนั้น $3^{20} \equiv 1 \pmod{4}$ ซึ่งจะได้ $3^{20} \equiv 1 \pmod{100}$)
6. ให้ p เป็นจำนวนเฉพาะซึ่ง $n < p < 2n$ จงพิสูจน์ว่า $\binom{2n}{n} \equiv 0 \pmod{p}$
7. จงพิสูจน์ว่า สำหรับจำนวนเต็มบวกใด ๆ $1 + 2 + 3 + \dots + (n-1) \equiv 0 \pmod{n}$
ข้อความนี้ยังเป็นจริงหรือไม่ ถ้า n เป็นจำนวนเต็มบวกคู่
8. จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็มบวก n , $4^n \equiv 1 + 3n \pmod{9}$
9. ให้ p เป็นจำนวนเฉพาะ จงพิสูจน์ว่าสำหรับทุก ๆ จำนวนเต็ม x , $x^2 \equiv x \pmod{p}$
ก็ต่อเมื่อ $x \equiv 0$ หรือ $1 \pmod{p}$

10. จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็มบวก n , $11 \mid (2^{4n+3} + 5^{n+2})$ โดยไม่ใช้หลักอุปนัยเชิงคณิตศาสตร์
11. จงพิสูจน์ว่า ถ้า $a \equiv 2 \pmod{4}$ แล้ว จะไม่มีจำนวนเต็ม b และ $m > 1$ ซึ่ง $a = b^m$
12. ให้ $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ โดยที่ a_i เป็นจำนวนเต็มที่ $0 \leq a_i \leq 9$
 จงพิสูจน์ว่า
 (12.1) $9 \mid a$ ก็ต่อเมื่อ $9 \mid (a_0 + a_1 + \cdots + a_n)$
 (12.2) $11 \mid a$ ก็ต่อเมื่อ $11 \mid (a_0 - a_1 + a_2 - \cdots + (-1)^n a_n)$
13. ให้ a เหมือนในข้อ 12. สำหรับจำนวนเต็มบวก k ซึ่ง $k \leq n$
 ให้ $b_k = a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$
 นั่นคือ b_k เป็นจำนวนเต็มบวกที่ประกอบด้วยตัวเลข k หลักจากทางขวาของ a
 จงพิสูจน์ว่า $2^k \mid a$ ก็ต่อเมื่อ $2^k \mid b_k$
14. ให้ a และ n เป็นจำนวนเต็มบวกที่ $(a, n) = 1$ จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็ม b
 $\{b, b+a, b+2a, \dots, b+(n-1)a\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n
15. ให้ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่าเซตต่อไปนี้ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n
 (15.1) $\{-\frac{n-1}{2}, -\frac{n-3}{2}, \dots, \frac{n-3}{2}, \frac{n-1}{2}\}$ เมื่อ n เป็นจำนวนเต็มคี่
 (15.2) $\{-\frac{n}{2}, -\frac{n-2}{2}, \dots, \frac{n-2}{2}, \frac{n}{2}\}$ เมื่อ n เป็นจำนวนเต็มคู่

6.2 สมการคอนกรูเอนซ์

ในหัวข้อนี้เราจะศึกษาการหาคำตอบของสมการพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็มและทำให้เราทราบวิธีการหาคำตอบทั้งหมดของสมการพหุนามในแง่ของคอนกรูเอนซ์มอดุโล n ซึ่งมีรายละเอียดดังนี้

ทฤษฎีบท 6.2.1 ให้ $f(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0$ เป็นพหุนามที่มี $c_i \in \mathbb{Z}$ และ $c_m \neq 0$ จะได้ว่า

1. ถ้า $a \equiv b \pmod{n}$ แล้ว $f(a) \equiv f(b) \pmod{n}$
2. ถ้า a เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$ และ $a \equiv b \pmod{n}$ แล้ว b จะเป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$

บทพิสูจน์ 1. จาก $a \equiv b \pmod{n}$ โดยทฤษฎีบท 6.1.3 ข้อ 5. จะได้ว่า

$$a^i \equiv b^i \pmod{n} \quad \text{ทุก } i = 1, 2, \dots, m$$

และโดยทฤษฎีบท 6.1.3 ข้อ 4. จะได้ว่า $c_i a^i \equiv c_i b^i \pmod{n}$ ทุก $i = 1, 2, \dots, m$

ดังนั้น โดยทฤษฎีบท 6.1.3 ข้อ 3. จะได้

$$c_m a^m + c_{m-1} a^{m-1} + \cdots + c_1 a + c_0 \equiv c_m b^m + c_{m-1} b^{m-1} + \cdots + c_1 b + c_0 \pmod{n}$$

นั่นคือ $f(a) \equiv f(b) \pmod{n}$

2. จาก a เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$ และ $a \equiv b \pmod{n}$

จะได้ว่า $f(a) \equiv 0 \pmod{n}$

โดยข้อ 1. ข้างต้น จะได้ว่า $f(a) \equiv f(b) \pmod{n}$

ดังนั้น $f(b) \equiv 0 \pmod{n}$

นั่นคือ b เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$ ■

ให้ $i \in \{0, 1, 2, 3, 4, 5\}$ กำหนด $[i] = \{6k + i \mid k \in \mathbb{Z}\}$ เราพบว่า

$$(i) \quad [i] \neq \emptyset$$

$$(ii) \quad [i] \cap [j] = \emptyset \quad \text{ทุก } i, j \text{ ซึ่ง } 0 \leq i < j \leq 5$$

$$(iii) \quad \bigcup_{i=0}^5 [i] = \mathbb{Z}$$

จากความจริงข้างต้น แสดงถึงการแบ่งเซตของจำนวนเต็มออกเป็น 6 สับเซตที่แต่ละ 2 สับเซตที่แตกต่างกัน ไม่มีสมาชิกร่วมกัน ในกรณีทั่วไป ถ้า $n \in \mathbb{N}$ เราสามารถกำหนด

$$[i] = \{nk + i \mid k \in \mathbb{Z}\}, \quad 0 \leq i \leq n-1$$

จะได้ว่า $[i] \neq \emptyset, [i] \cap [j] = \emptyset, \quad 0 \leq i < j \leq n-1$

และ $\bigcup_{i=0}^{n-1} [i] = \mathbb{Z}$ จึงส่งผลให้เซตของจำนวนเต็มถูกแบ่งออกเป็น n สับเซต

ให้ $n \in \mathbb{N}$ กำหนด $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$

เราจะเรียก $\mathbb{Z}_n$ ว่า เซตของจำนวนเต็มมอดุโล n

$\mathbb{Z}_n$ มีบทบาทมากในการศึกษาทฤษฎีจำนวนโดยเฉพาะอย่างยิ่ง $\mathbb{Z}_n$ เป็นสิ่งสำคัญในการกำหนดแนวทางการศึกษา “สมการคอนกรูเอนซ์” ซึ่งจะได้กล่าวต่อไปในแง่ของโครงสร้างของ $\langle \mathbb{Z}_n, +, \cdot \rangle$ เมื่อโอเปอเรชัน “+” และ “ $\cdot$ ” ได้ถูกกำหนดขึ้นบน $\mathbb{Z}_n$ จะทำให้เกิดโครงสร้างทางพีชคณิตจำกัดที่น่าสนใจและมักจะใช้เป็นตัวอย่างในการศึกษาพีชคณิตเชิงนามธรรมเพื่อให้ผู้เรียนเกิดความเข้าใจเพราะระบบ $\langle \mathbb{Z}_n, +, \cdot \rangle$ มีโครงสร้างบางอย่างเหมือนกับ $\langle \mathbb{Z}, +, \cdot \rangle$ และมีโครงสร้างบางอย่างที่ต่างกัน

ผู้อ่านอาจคุ้นเคยกับการแก้สมการ เช่น การแก้สมการ

$$x^2 + x - 2 = 0$$

หมายถึงการหาจำนวนจริง x_0 ซึ่ง $x_0^2 + x_0 - 2 = 0$ จากการใช้พีชคณิตเบื้องต้นเราทราบว่า

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

ดังนั้น 1 และ -2 ต่างก็เป็นคำตอบของสมการ $x^2 + x - 2 = 0$

เราอาจพิจารณาการหาคำตอบของสมการ $2^x = 8$ ซึ่งเราพบว่า $x = 3$ คือคำตอบของสมการ $2^x = 8$

สำหรับการศึกษสมการคอนกรูเอนซ์ เช่น

$$x^2 + x - 2 \equiv 0 \pmod{5}$$

เรามุ่งในการหาคำตอบ x_0 ที่เป็นจำนวนเต็มซึ่ง $x_0^2 + x_0 - 2 \equiv 0 \pmod{5}$

ถ้าจะกล่าวโดยทั่วไป ให้ f แทนฟังก์ชันที่มี x เป็นตัวแปรและกำหนดขอบเขตของตัวแปร x คือเซตของจำนวนเต็มและสำหรับทุก ๆ จำนวนเต็ม x ค่าของ $f(x)$ เป็นจำนวนเต็ม เราอาจสนใจการหาคำตอบของสมการ

$$f(x) \equiv 0 \pmod{n}$$

กล่าวคือเราจะศึกษาสมการคอนกรูเอนซ์ $f(x) \equiv 0 \pmod{n}$ ก็ต่อเมื่อ f มีสมบัติว่าถ้า $a \equiv b \pmod{n}$ แล้ว $f(a) \equiv f(b) \pmod{n}$

จากทฤษฎีบท 6.2.1 เราพบว่า ทุก ๆ พหุนาม $f(x)$ ที่มีสัมประสิทธิ์เป็นจำนวนเต็มสอดคล้องกับสมบัติดังกล่าว ในขณะที่สมการ $2^x - 8 \equiv 0 \pmod{5}$ เป็นสมการที่ไม่สอดคล้องกับสมบัติพื้นฐานที่เราเพิ่งจะศึกษา นอกจากนั้น ถ้าพิจารณาสมการ

$$|2x + 3| - 2 \equiv 0 \pmod{5}$$

เราพบว่า $2 \equiv -3 \pmod{5}$ แต่

$$|2(2) + 3| - 2 = 5 \not\equiv 1 = |2(-3) + 3| - 2 \pmod{5}$$

ดังนั้นฟังก์ชัน f ที่กำหนดโดย $f(x) = |2x + 3| - 2$ จะเป็นฟังก์ชันที่ไม่สอดคล้องสมบัติ พื้นฐานเช่นกัน

จากความจริงข้างต้นเราพบว่า ในการหาคำตอบของสมการคอนกรูเอนซ์ $f(x) \equiv 0 \pmod{n}$ ทั้งหมดนั้นเราอาจหาได้โดยการหาค่า $f(0), f(1), \dots, f(n-1)$ และถ้า $f(i) \equiv 0 \pmod{n}$, $0 \leq i < n-1$ จะได้ว่า $x = i + nk$ เป็นคำตอบของสมการดังกล่าว สำหรับทุกจำนวนเต็ม k

ตัวอย่าง 1 จงหาคำตอบของสมการ $x^2 + x - 2 \equiv 0 \pmod{5}$

วิธีทำ จากทฤษฎีบท 6.2.1 พบว่า ถ้า $a \equiv b \pmod{5}$ แล้ว $a^2 + a - 2 \equiv b^2 + b - 2 \pmod{5}$

ซึ่งหมายความว่าคำตอบ $x_0 \in \mathbb{Z}$ ทั้งหมดที่ทำให้ $x_0^2 + x_0 - 2 \equiv 0 \pmod{5}$ เป็นการเพียงพอกที่จะเลือก x_0 จากสมาชิกแต่ละตัวในเซต $\{0, 1, 2, 3, 4\}$

$$\text{เพราะว่า } 0^2 + 0 - 2 \not\equiv 0 \pmod{5}$$

$$1^2 + 1 - 2 \equiv 0 \pmod{5}$$

$$2^2 + 2 - 2 \not\equiv 0 \pmod{5}$$

$$3^2 + 3 - 2 \equiv 0 \pmod{5}.$$

$$\text{และ } 4^2 + 4 - 2 \not\equiv 0 \pmod{5}$$

ดังนั้น คำตอบ x_0 ของสมการ $x^2 + x - 2 \equiv 0 \pmod{5}$ ในเซต $\{0, 1, 2, 3, 4\}$ คือ $x_0 = 1, 3$

นั่นคือ คำตอบทั้งหมดของสมการ $x^2 + x - 2 \equiv 0 \pmod{5}$ คือ

$$\{x \in \mathbb{Z} \mid x \equiv 1 \pmod{5}\} \cup \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{5}\}$$

□

จากตัวอย่าง 1 ข้างต้น ทำให้เราไม่มีความจำเป็นที่จะต้องจำแนกความแตกต่างระหว่างคำตอบ 2 คำตอบที่คอนกรูเอนซ์กัน เช่นทั้ง 1 และ 6 ต่างก็เป็นคำตอบของสมการ $x^2 + x - 2 \equiv 0 \pmod{5}$ แต่ $1 \equiv 6 \pmod{5}$ เมื่อเป็นเช่นนี้เราจะกล่าวว่า 1 และ 6 เป็นคำตอบที่คอนกรูเอนซ์ในมอดุโล 5 ดังนั้น สมการ $x^2 + x - 2 \equiv 0 \pmod{5}$ มีเพียง 2 คำตอบเท่านั้นที่ไม่คอนกรูเอนซ์กันในมอดุโล 5 คือ 1 และ 3

ตัวอย่าง 2 จงหาคำตอบ (ที่แตกต่างกัน) ทั้งหมดของ $x^2 + x - 2 \equiv 0 \pmod{9}$

ที่ไม่คอนกรูเอนซ์กันในมอดุโล 9

วิธีทำ ในการหาคำตอบของสมการคอนกรูเอนซ์ข้างต้น เป็นการเพียงพอที่จะหาคำตอบ x_0

เมื่อ $x_0 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ เท่านั้น

เพราะว่า $0^2 + 0 - 2 \not\equiv 0 \pmod{9}$

$$1^2 + 1 - 2 \equiv 0 \pmod{9}$$

$$2^2 + 2 - 2 \not\equiv 0 \pmod{9}$$

$$3^2 + 3 - 2 \not\equiv 0 \pmod{9}$$

$$4^2 + 4 - 2 \equiv 0 \pmod{9}$$

$$5^2 + 5 - 2 \equiv 0 \pmod{9}$$

$$6^2 + 6 - 2 \not\equiv 0 \pmod{9}$$

$$7^2 + 7 - 2 \equiv 0 \pmod{9}$$

และ $8^2 + 8 - 2 \not\equiv 0 \pmod{9}$

ดังนั้น คำตอบ x_0 ของสมการ $x^2 + x - 2 \equiv 0 \pmod{9}$ ในเซต $\{0, 1, 2, \dots, 8\}$

คือ $x_0 = 1, 4, 7$ □

ตัวอย่าง 3 จงหาคำตอบ (ที่แตกต่างกัน) ทั้งหมดของสมการคอนกรูเอนซ์ต่อไปนี้

$$(3.1) \quad 5x \equiv 3 \pmod{6}$$

$$(3.2) \quad 6x \equiv 3 \pmod{9}$$

$$(3.3) \quad 3x \equiv 5 \pmod{6}$$

วิธีทำ (3.1) จากการเลือก $x_0 \in \{0, 1, 2, 3, 4, 5\}$ เพื่อตรวจสอบ เราพบว่าในมอดุโล 6,

$$5(0) \not\equiv 3, 5(1) \not\equiv 3, 5(2) \not\equiv 3, 5(3) \equiv 3, 5(4) \not\equiv 3 \text{ และ } 5(5) \not\equiv 3$$

ดังนั้นคำตอบ x_0 ของสมการ $5x \equiv 3 \pmod{6}$ มีเพียงคำตอบที่แตกต่างกัน

เพียงคำตอบเดียวในมอดุโล 6 คือ $x_0 = 3$

(3.2) จากการเลือก $x_0 \in \{0, 1, 2, \dots, 8\}$ เพื่อตรวจสอบ เราพบว่าในมอดุโล 9,

$$6(0) \not\equiv 3, 6(1) \not\equiv 3, 6(2) \equiv 3, 6(3) \not\equiv 3, 6(4) \not\equiv 3, 6(5) \equiv 3, 6(6) \not\equiv 3,$$

$$6(7) \not\equiv 3 \text{ และ } 6(8) \equiv 3$$

ดังนั้น คำตอบ x_0 ของสมการ $6x \equiv 3 \pmod{9}$ มีด้วยกัน 3 คำตอบที่แตกต่างกันในมอดุโล 9

คือ $x_0 = 2, 5, 8$

(3.3) จากการเลือก $x_0 \in \{0, 1, 2, 3, 4, 5\}$ เพื่อตรวจสอบ เราพบว่าในมอดุโล 6,

$$3(0) \not\equiv 5, 3(1) \not\equiv 5, 3(2) \not\equiv 5, 3(3) \not\equiv 5, 3(4) \not\equiv 5 \text{ และ } 3(5) \not\equiv 5$$

นั่นเป็นการแสดงว่าสมการ $3x \equiv 5 \pmod{6}$ ไม่มีคำตอบ □

จากตัวอย่างข้างต้น เราพบสมการที่อยู่ในรูป $ax \equiv b \pmod{n}$ อาจมีคำตอบหรือไม่มีคำตอบ และในกรณี
ที่สมการมีคำตอบอาจมีคำตอบมากกว่า 1 คำตอบก็ได้ ทฤษฎีบทต่อไปจะแสดงเงื่อนไขที่จำเป็นและเพียงพอที่จะทำให้
สมการ $ax \equiv b \pmod{n}$ มีคำตอบ

ทฤษฎีบท 6.2.2 ให้ $a, b, n \in \mathbb{Z}$ โดยที่ $n > 0$ และ $(a, n) = d$ จะได้ว่า

1. สมการคอนกรูเอนซ์เชิงเส้น (linear congruence equation) $ax \equiv b \pmod{n}$ มีคำตอบ $x \in \mathbb{Z}$ ก็ต่อเมื่อ $d \mid b$
2. ถ้า $d \mid b$ แล้วสมการคอนกรูเอนซ์เชิงเส้น $ax \equiv b \pmod{n}$ มีคำตอบอยู่ d คำตอบที่ไม่คอนกรูเอนซ์กันในมอดุโล n และคำตอบเหล่านั้นคือ

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

โดยที่ x_0 คือคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$

- บทพิสูจน์** 1. $(\Rightarrow)$ สมมติว่าสมการ $ax \equiv b \pmod{n}$ มีคำตอบ
จะได้ว่ามี $x_0 \in \mathbb{Z}$ ซึ่ง $ax_0 \equiv b \pmod{n}$ แสดงว่า $n \mid (ax_0 - b)$
เนื่องจาก $d \mid n$ และ $d \mid a$ ดังนั้น $d \mid b$
 $(\Leftarrow)$ สมมติว่า $d \mid b$ จะได้ว่ามี $k \in \mathbb{Z}$ ซึ่ง $b = dk$ และจาก $d = (a, n)$

โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $x_0, y_0 \in \mathbb{Z}$ ซึ่ง $d = ax_0 + ny_0$

ทำให้ได้ว่า $b = dk = ax_0k + ny_0k$

ดังนั้น $n \mid (ax_0k - b)$ นั่นคือ $ax_0k \equiv b \pmod{n}$

แสดงว่าสมการ $ax \equiv b \pmod{n}$ มีคำตอบ $x = x_0k$

2. **ตอน 1** จาก $(\frac{a}{d}, \frac{n}{d}) = 1$ และ $1 \mid \frac{b}{d}$

แสดงว่าสมการ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ มีคำตอบ

ให้ x_0 เป็นคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$

จะได้ว่า $\frac{n}{d} \mid (\frac{a}{d}x_0 - \frac{b}{d})$ แสดงว่าจะมี $k \in \mathbb{Z}$ ซึ่ง

$$\frac{a}{d}x_0 - \frac{b}{d} = \frac{n}{d}k \quad \dots\dots\dots (*)$$

ให้ $t \in \mathbb{Z}$ จะแสดงว่า $x_0 + \frac{n}{d}t$ เป็นคำตอบของสมการ

$$\begin{aligned} \text{เพราะว่า } a(x_0 + \frac{n}{d}t) - b &= ax_0 + \frac{an}{d}t - b \\ &= \frac{adx_0}{d} + \frac{ant}{d} - \frac{bd}{d} \\ &= d(\frac{a}{d}x_0 - \frac{b}{d}) + \frac{a}{d}nt \\ &= d(\frac{n}{d})k + \frac{a}{d}nt \quad (\text{แทนค่าจาก } (*)) \\ &= n(k + \frac{a}{d}t) \end{aligned}$$

จาก $d \mid a$ และ $t \in \mathbb{Z}$ จะได้ $n \mid [a(x_0 + \frac{n}{d}t) - b]$

นั่นคือ $a(x_0 + \frac{n}{d}t) \equiv b \pmod{n}$ แสดงว่า $x_0 + \frac{n}{d}t$ เป็นคำตอบของ

สมการ $ax \equiv b \pmod{n}$ สำหรับทุกจำนวนเต็ม t

ต่อไปจะแสดงว่าคำตอบของสมการ $ax \equiv b \pmod{n}$ จะเขียนอยู่ในรูป

$$x_0 + \frac{n}{d}q \quad \text{เมื่อ } q \in \mathbb{Z}$$

ให้ x_1 เป็นคำตอบใด ๆ ของสมการ $ax \equiv b \pmod{n}$

จะได้ $ax_1 \equiv b \pmod{n}$ เนื่องจาก $a(x_0 + \frac{n}{d}t) \equiv b \pmod{n}$

จะได้ว่า $ax_1 \equiv a(x_0 + \frac{n}{d}t) \pmod{n}$

ดังนั้น $\frac{a}{d}x_1 \equiv \frac{a}{d}(x_0 + \frac{n}{d}t) \pmod{\frac{n}{d}}$

จาก $(\frac{a}{d}, \frac{n}{d}) = 1$ โดยทฤษฎีบท 6.1.4 ข้อ 3. จะได้ว่า

$$x_1 \equiv (x_0 + \frac{n}{d}t) \pmod{\frac{n}{d}}$$

แสดงว่า จะมี $t_1 \in \mathbb{Z}$ ซึ่ง $x_1 - (x_0 + \frac{n}{d}t) = \frac{n}{d}t_1$

ทำให้ได้ว่า $x_1 = x_0 + \frac{n}{d}(t + t_1)$

นั่นคือ มี $q = t + t_1 \in \mathbb{Z}$ ที่ทำให้ $x_1 = x_0 + \frac{n}{d}q$

สรุป คำตอบของสมการ $ax \equiv b \pmod{n}$ จะเขียนอยู่ในรูป

$$x \equiv x_0 + t(\frac{n}{d}) \pmod{n} \quad \text{เมื่อ } t \in \mathbb{Z}$$

โดยที่ x_0 เป็นคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$

ทฤษฎีบท 2 ให้ $d = (a, n)$ และ $t \in \mathbb{Z}$ จะต้องแสดงว่า

สมการ $ax \equiv b \pmod{n}$ มีคำตอบอยู่ d คำตอบที่ไม่คอนกรูเอนซ์กันในมอดุโล n

จาก $d, t \in \mathbb{Z}$ โดยขั้นตอนวิธีการหารจะได้ว่ามี $q, r \in \mathbb{Z}$ ที่ทำให้

$$t = dq + r \quad \text{โดยที่ } 0 \leq r < d$$

ดังนั้น $x_0 + t\frac{n}{d} = x_0 + (dq + r)\frac{n}{d} = x_0 + nq + r\frac{n}{d}$

แสดงว่า $x_0 + t\frac{n}{d} \equiv x_0 + r\frac{n}{d} \pmod{n}$ โดยที่ $0 \leq r \leq d-1$

สรุป คำตอบของสมการ $ax \equiv b \pmod{n}$ จะมีอยู่ d คำตอบเท่านั้นที่ไม่คอนกรูเอนซ์กันในมอดุโล n คือ

$$x \equiv x_0 + \frac{n}{d}t \pmod{n}$$

เมื่อ $t = 0, 1, 2, \dots, d-1$ ■

จากทฤษฎีบท 6.2.2 เราพบว่า

(1) ถ้า $d \nmid b$ แล้ว สมการคอนกรีตเชิงเส้น $ax \equiv b \pmod{n}$ ไม่มีคำตอบ

(2) ถ้า x_0 เป็นคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv 1 \pmod{\frac{n}{d}}$ แล้ว $x_1 = \frac{b}{d}x_0$ จะเป็นคำตอบของ

$$\text{สมการ } \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

ดังนั้น ในการหาคำตอบของสมการคอนกรีตเชิงเส้น $ax \equiv b \pmod{n}$ เราอาจหาคำตอบหนึ่งคือ x_0 จากสมการ $\frac{a}{d}x \equiv 1 \pmod{\frac{n}{d}}$ และให้ $x_1 = \frac{b}{d}x_0$ จะได้ว่า x_1 เป็นคำตอบหนึ่งของสมการ

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

บทแทรก 6.2.3 ถ้า $(a, n) = 1$ แล้ว สมการคอนกรีตเชิงเส้น $ax \equiv b \pmod{n}$ มีคำตอบเพียงคำตอบเดียว กล่าวคือ ถ้า x_1 และ x_2 เป็นคำตอบของสมการ $ax \equiv b \pmod{n}$ แล้ว $x_1 \equiv x_2 \pmod{n}$

ตัวอย่าง 4 (4.1) สมการคอนกรีตเชิงเส้น $14x \equiv 13 \pmod{21}$ ไม่มีคำตอบเพราะว่า $(14, 21) = 7$ และ $7 \nmid 13$

(4.2) สมการคอนกรีตเชิงเส้น $9x \equiv 15 \pmod{21}$ มีคำตอบเพราะว่า $(9, 21) = 3$ และ $3 \mid 15$ และสมการคอนกรีตเชิงเส้นนี้มีคำตอบอยู่ 3 คำตอบที่ไม่คอนกรีตกันในมอดุโล 21 เนื่องจาก $9x \equiv 15 \pmod{21}$ จะได้ $3x \equiv 5 \pmod{7}$

เพราะว่า $12 \equiv 5 \pmod{7}$ และ $(3, 7) = 1$

ดังนั้น $x \equiv 4 \pmod{7}$

นั่นคือสมการคอนกรีตเชิงเส้น จะมีคำตอบคือ

$$x \equiv 4, 11, 18 \pmod{21}$$

□

ตัวอย่าง 5 จงหาคำตอบของสมการคอนกรีตเชิงเส้น $91x \equiv 98 \pmod{119}$

วิธีทำ เนื่องจาก $(91, 119) = 7$ และ $7 \mid 98$ ดังนั้นสมการคอนกรีตเชิงเส้นนี้มีคำตอบอยู่ 7 คำตอบที่ไม่คอนกรีตกันในมอดุโล 119

จาก $91x \equiv 98 \pmod{119}$ จะได้ว่า $13x \equiv 14 \pmod{17}$

เพราะว่า $(13, 17) = 1$ จะได้ว่าสมการคอนกรีตเชิงเส้นสุดท้ายนี้มีคำตอบ คือ

$$x \equiv 5 \pmod{17}$$

ดังนั้น สมการคอนกรีตเชิงเส้นที่กำหนดให้มีคำตอบ คือ

$$x \equiv 5, 22, 39, 56, 73, 90, 107 \pmod{119}$$

□

ปัญหา 6 จงหาคำตอบของสมการคอนกรูเอนซ์เชิงเส้น

$$(6.1) \quad 18x \equiv 30 \pmod{42}$$

$$(6.2) \quad 9x \equiv 21 \pmod{30}$$

$$(6.3) \quad 7x \equiv 22 \pmod{39}$$

ตัวอย่าง 7 จงหาคำตอบของสมการคอนกรูเอนซ์เชิงเส้น $39x \equiv 65 \pmod{52}$

วิธีทำ เพราะว่า $(39, 52) = 13$ และ $13 \mid 65$ แสดงว่าสมการคอนกรูเอนซ์เชิงเส้นนี้มี คำตอบของสมการ 13 คำตอบที่ไม่คอนกรูเอนซ์กันในมอดุโล 52 การหาคำตอบเริ่มจากการหา x_0 โดยพิจารณาจาก

$$\frac{39}{13}x_0 \equiv \frac{65}{13} \pmod{\frac{52}{13}}$$

$$3x_0 \equiv 5 \pmod{4}$$

ดังนั้น คำตอบของสมการคือ $x \equiv 3 + \frac{52}{13}t \pmod{52}$ เมื่อ $t = 0, 1, 2, \dots, 12$

ซึ่งได้แก่ $x \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51 \pmod{52}$ □

มีอีกวิธีการหนึ่งที่นิยมใช้ในการหาคำตอบของสมการ $ax \equiv b \pmod{n}$ ก็คือการเขียน

$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ ซึ่งเป็นการเขียนในรูปแบบบัญญัติและ $n_i = p_i^{a_i}$ เราพบว่าการหาคำตอบของสมการ

$ax \equiv b \pmod{n}$ เมื่อ $n = [n_1, n_2, \dots, n_k]$ นั้น จะเหมือนกับการหาคำตอบของระบบสมการ

$ax \equiv b \pmod{n_i}$ และดูเหมือนว่าการหาคำตอบของสมการ $ax \equiv b \pmod{n_i}$ แต่ละสมการนั้น จะหาได้ง่าย เนื่องจาก $n_i \leq n$

ต่อไปถ้าสมมติว่าเรามีคำตอบ $u_1, u_2, \dots, u_k$ ซึ่ง $x \equiv u_i \pmod{n_i}$ เป็นคำตอบของสมการ

$ax \equiv b \pmod{n_i}$ จากปัญหาเดิมคือ การหาคำตอบของสมการ $ax \equiv b \pmod{n}$ เราจำเป็นที่จะต้องหาคำตอบ x ซึ่ง $ax \equiv b \pmod{n_i}$ สำหรับทุก $i = 1, 2, 3, \dots, k$ เพื่อสรุปว่า $ax \equiv b \pmod{n}$

โดยที่ $n = [n_1, n_2, \dots, n_k]$

ทฤษฎีบทต่อไปนี้จะแสดงวิธีการหาคำตอบของสมการ $ax \equiv b \pmod{n}$ เมื่อกำหนดว่าแต่ละสมการ $ax \equiv b \pmod{n_i}$ มีคำตอบ

ทฤษฎีบทเศษเหลือของจีน

ให้ $a, b \in \mathbb{N}$ และ $(a, b) = 1$ จะได้ว่าสมการ

$$ax \equiv 1 \pmod{b} \quad \text{และ} \quad by \equiv 1 \pmod{a}$$

มีคำตอบ $x \in \{0, 1, 2, \dots, b-1\}$ และ $y \in \{0, 1, 2, \dots, a-1\}$ เพียงสมการละ 1 คำตอบเท่านั้น

ให้ x_0 และ y_0 เป็นคำตอบของสมการ $ax \equiv 1 \pmod{b}$ และ $by \equiv 1 \pmod{a}$ ตามลำดับ
จะได้ว่า ทุก ๆ $c, d \in \mathbb{Z}$

$$ax_0c \equiv c \pmod{b} \quad \text{และ} \quad by_0d \equiv d \pmod{a}$$

นั่นคือ x_0c และ y_0d เป็นคำตอบของ $ax \equiv c \pmod{b}$ และ $by \equiv d \pmod{a}$ ตามลำดับ

$$\text{ให้ } z = ax_0c + by_0d$$

$$\text{เราพบว่า } z = ax_0c + by_0d \equiv ax_0c + 0 \equiv c \pmod{b}$$

$$\text{และ } z = ax_0c + by_0d \equiv 0 + by_0d \equiv d \pmod{a}$$

นี่คือการแสดงว่า $z = ax_0c + by_0d$ เป็นคำตอบของระบบสมการ

$$x \equiv c \pmod{b}$$

$$x \equiv d \pmod{a}$$

ตัวอย่าง 8 จงหาคำตอบทั้งหมดของระบบสมการคอนกรูเอนซ์

$$(*) \dots\dots\dots \begin{cases} x \equiv 2 \pmod{4} & \dots\dots\dots(1) \\ x \equiv 4 \pmod{7} & \dots\dots\dots(2) \end{cases}$$

วิธีทำ ให้ $A = \{2 + 4k \mid k \in \mathbb{Z}\}$ และ $B = \{4 + 7k \mid k \in \mathbb{Z}\}$

จะเห็นได้ชัดว่า A คือเซตคำตอบของสมการ (1) ในขณะที่ B คือเซตคำตอบของสมการ (2)

จากการกำหนดค่า k ที่เหมาะสมของแต่ละเซต จะพบว่า $18 \in A \cap B$

นั่นคือ 18 เป็นคำตอบของระบบสมการ (*)

ให้ z เป็นคำตอบของระบบสมการ (*) นั่นคือ $z \in A \cap B$

$$\text{ดังนั้น } z \equiv 18 \pmod{4} \text{ และ } z \equiv 18 \pmod{7}$$

$$\text{แสดงว่า } z \equiv 18 \pmod{28} \text{ นั่นคือ ทุก ๆ } z \text{ ซึ่ง } z \equiv 18 \pmod{28}$$

จะเป็นคำตอบของระบบสมการ (*) ทั้งสิ้น

$$\text{ดังนั้น เซตคำตอบของระบบสมการ (*) คือ } \{18 + 28k \mid k \in \mathbb{Z}\}$$

□

เนื่องจากระบบสมการ (*) มีเพียง 2 สมการเท่านั้นซึ่งเราสามารถหาคำตอบรวมได้โดยง่าย เพื่อให้การแก้ปัญหาข้างต้นมีวิธีการที่สามารถใช้ได้กับทุก ๆ ระบบสมการ เราต้องมาวิเคราะห์ถึงสิ่งที่ต้องการหาเพื่อที่จะแก้ระบบสมการดังกล่าว

(i) จาก $a = 7$ และ $b = 4$ ให้ x_0 และ y_0 เป็นคำตอบของสมการ

$$7x \equiv 1 \pmod{4} \text{ และ } 4y \equiv 1 \pmod{7}$$

$$\text{ดังนั้น } x_0 \equiv -1 \pmod{4} \text{ และ } y_0 \equiv 2 \pmod{7}$$

(ii) จาก $c = 2$ และ $d = 4$

$$\text{จะได้ } z = ax_0c + by_0d = 7 \cdot (-1) \cdot 2 + 4 \cdot 2 \cdot 4 = 18$$

จากที่กล่าวมาทั้งหมดในหัวข้อนี้ เราสามารถสรุปเป็นทฤษฎีบทได้ดังนี้

ทฤษฎีบท 6.2.4 ให้ $n_1, n_2 \in \mathbb{N}$ และ $(n_1, n_2) = 1$ จะได้ว่าระบบสมการ

$$x \equiv a_1 \pmod{n_1} \quad \text{และ} \quad x \equiv a_2 \pmod{n_2}$$

มีคำตอบของระบบสมการเพียงคำตอบเดียวในมอดุโล $n = n_1 n_2$

กล่าวคือจะมี $x_0 \in \mathbb{Z}$ ซึ่ง $x_0 \equiv a_i \pmod{n_i}$ ทุก $i = 1, 2$

และถ้า x_1 และ x_2 เป็นคำตอบของสมการ $ax \equiv b \pmod{n}$ แล้ว $x_1 \equiv x_2 \pmod{n_1 n_2}$

ในกรณีที่มีระบบสมการมีมากกว่า 2 สมการ เช่นจงหาคำตอบของระบบสมการ

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_3 \pmod{n_3}$$

เมื่อ $(n_1, n_2) = (n_2, n_3) = (n_3, n_1) = 1$

ให้ $z = n_2 n_3 x_1 a_1 + n_1 n_3 x_2 a_2 + n_1 n_2 x_3 a_3$ เราพบว่าทุก ๆ จำนวนเต็ม x_1, x_2, x_3

จะได้ $z \equiv n_2 n_3 x_1 a_1 + 0 + 0 \pmod{n_1}$

$$\equiv 0 + n_1 n_3 x_2 a_2 + 0 \pmod{n_2}$$

$$\equiv 0 + 0 + n_1 n_2 x_3 a_3 \pmod{n_3}$$

ดังนั้น ในการหาคำตอบของระบบสมการข้างต้นเราอาจเลือก x_1, x_2, x_3 ที่สอดคล้องกับสมการ

$n_2 n_3 x \equiv 1 \pmod{n_1}$, $n_1 n_3 x \equiv 1 \pmod{n_2}$, $n_1 n_2 x \equiv 1 \pmod{n_3}$ ตามลำดับ ซึ่งจะได้

$z = n_2 n_3 x_1 a_1 + n_1 n_3 x_2 a_2 + n_1 n_2 x_3 a_3$ เป็นคำตอบของระบบสมการตามต้องการ นอกจากนั้น

ถ้า x_1, x_2 เป็นคำตอบของระบบสมการจะได้ว่า $x_1 \equiv x_2 \pmod{n_1 n_2 n_3}$

จากวิธีการที่ได้กล่าวข้างต้น ถ้าให้ $n = n_1 n_2 n_3$, $N_1 = n_2 n_3$, $N_2 = n_1 n_3$ และ $N_3 = n_1 n_2$ เราก็สามารถเขียนรูปแบบของสมการคอนกรูเอนซ์และคำตอบได้ง่ายขึ้น เช่นคำตอบของระบบสมการข้างต้นที่อยู่ในรูป

$$\begin{aligned} x_0 &= n_2 n_3 x_1 a_1 + n_1 n_3 x_2 a_2 + n_1 n_2 x_3 a_3 \\ &= N_1 x_1 a_1 + N_2 x_2 a_2 + N_3 x_3 a_3 \end{aligned}$$

ตัวอย่าง 9 จงหาคำตอบทั้งหมดของระบบสมการ

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

$$x \equiv 5 \pmod{4}$$

$$x \equiv -3 \pmod{7}$$

วิธีทำ ให้ $n_1 = 3$, $n_2 = 4$, $n_3 = 7$ จะได้ $n = 3 \cdot 4 \cdot 7 = 84$, $N_1 = 4 \cdot 7 = 28$,

$N_2 = 3 \cdot 7 = 21$ และ $N_3 = 3 \cdot 4 = 12$

ให้ x_1, x_2, x_3 เป็นคำตอบของสมการ

$$28x_1 \equiv 1 \pmod{3}$$

$$21x_2 \equiv 1 \pmod{4}$$

$$12x_3 \equiv 1 \pmod{7}$$

จะได้ว่า $x_1 = 1$, $x_2 = 1$, $x_3 = 3$

$$\begin{aligned} \text{ดังนั้น } x_0 &= N_1x_1a_1 + N_2x_2a_2 + N_3x_3a_3 \\ &= 28 \cdot 1 \cdot 2 + 21 \cdot 1 \cdot 5 + 12 \cdot 3 \cdot (-3) = 53 \end{aligned}$$

ดังนั้น คำตอบทั้งหมดของระบบสมการข้างต้น สามารถเขียนได้ในรูป

$$53 + 84k, \quad k \in \mathbb{Z}$$

□

ทฤษฎีบทต่อไปนี้จะกล่าวถึงการมีคำตอบของระบบสมการที่ประกอบด้วย r สมการและผู้อ่านจะพบว่า วิธีการในการหาคำตอบของระบบสมการนี้ ไม่ได้แตกต่างจากวิธีการเมื่อ $n = 2$ ทฤษฎีบทต่อไปนี้มีชื่อว่า **ทฤษฎีบทเศษเหลือของจีน** (Chinese Remainder Theorem) เหตุที่เรียกเช่นนี้ก็เพราะว่า ชาวจีนได้ใช้ความรู้ที่คล้ายกับทฤษฎีบทนี้มาตั้งแต่คริสต์ศตวรรษที่ 1 แล้ว และหลังจากนั้นชาวจีนได้นำไปเผยแพร่ในยุโรป ซึ่งครั้งแรกๆ ที่นำไปเผยแพร่ในชาวจีนยังใช้การเขียนทฤษฎีบทนี้ด้วยภาษาจีน

ทฤษฎีบท 6.2.5 ทฤษฎีบทเศษเหลือของจีน (Chinese Remainder Theorem)

ให้ $n_1, n_2, \dots, n_r$ เป็นจำนวนเต็มบวกซึ่ง $(n_i, n_j) = 1$ สำหรับทุก $i \neq j$
จะได้ว่า ระบบสมการคอนกรูเอนซ์

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

มีคำตอบของระบบสมการเพียงคำตอบเดียวในมอดุโล $n = n_1n_2 \cdots n_r$

กล่าวคือ จะมี $x_0 \in \mathbb{Z}$ ซึ่ง $x_0 \equiv a_i \pmod{n_i}$ ทุก $i = 1, 2, \dots, r$ และ

ถ้า x_1 และ x_2 เป็นคำตอบของระบบสมการ แล้ว $x_1 \equiv x_2 \pmod{n}$

บทพิสูจน์ ให้ $n = n_1n_2 \cdots n_r$

จะได้ว่า $\frac{n}{n_j}$ เป็นจำนวนเต็ม และ $(\frac{n}{n_j}, n_j) = 1$ สำหรับทุก $j = 1, 2, \dots, r$

ดังนั้น จะมี $b_j \in \mathbb{Z}$ ที่ทำให้ $\frac{n}{n_j} b_j \equiv 1 \pmod{n_j}$ สำหรับทุก $j = 1, 2, \dots, r$

จาก $\frac{n}{n_j} = n_1n_2 \cdots n_{j-1}n_{j+1} \cdots n_r$ จะได้ว่า $\frac{n}{n_j} b_j \equiv 0 \pmod{n_i}$ เมื่อ $i \neq j$

$$\text{ให้ } x_0 = \sum_{j=1}^r \frac{n}{n_j} b_j a_j = \frac{n}{n_1} b_1 a_1 + \frac{n}{n_2} b_2 a_2 + \cdots + \frac{n}{n_i} b_i a_i + \cdots + \frac{n}{n_r} b_r a_r$$

จะได้ว่า $x_0 \equiv \frac{n}{n_i} b_i a_i \equiv a_i \pmod{n_i}$ สำหรับทุก $i = 1, 2, \dots, r$

ดังนั้น x_0 คือคำตอบของสมการ $x \equiv a_i \pmod{n_i}$ สำหรับทุก $i = 1, 2, \dots, r$

ต่อไปจะแสดงว่า คำตอบของระบบสมการมีเพียงคำตอบเดียวในมอดุโล n

ให้ x_1 เป็นคำตอบใด ๆ ของระบบสมการ

ดังนั้น $x_1 \equiv a_i \equiv x_0 \pmod{n_i}$ สำหรับทุก $i = 1, 2, \dots, r$

แสดงว่า $x_i \equiv x_0 \pmod{n_i}$ สำหรับทุก $i = 1, 2, \dots, r$

โดยทฤษฎีบท 6.1.5 จะได้ว่า $x_1 \equiv x_0 \pmod{n}$ ■

เราสามารถนำรูปแบบการพิสูจน์ทฤษฎีบทเศษเหลือของจีน ไปใช้เป็นวิธีการหาคำตอบของระบบสมการคอนกรูเอนซ์เชิงเส้นได้ ดังตัวอย่างที่ได้กล่าวมาข้างต้นและตัวอย่างต่อไปนี้

ตัวอย่าง 10 จงหาคำตอบของระบบสมการ

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

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

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

วิธีทำ ให้ $n = 3 \cdot 5 \cdot 7 = 105$ และ $N_1 = \frac{105}{3} = 35$, $N_2 = \frac{105}{5} = 21$, $N_3 = \frac{105}{7} = 15$

และให้ x_1, x_2, x_3 เป็นคำตอบของสมการ

$$35x_1 \equiv 1 \pmod{3}$$

$$21x_2 \equiv 1 \pmod{5}$$

$$15x_3 \equiv 1 \pmod{7}$$

จะได้ว่า $x_1 = 2$, $x_2 = 1$ และ $x_3 = 1$

ดังนั้นคำตอบร่วมของสมการ $x \equiv a_i \pmod{n_i}$ เมื่อ $a_1 = 2$, $a_2 = 3$, $a_3 = 2$

และ $n_1 = 3$, $n_2 = 5$, $n_3 = 7$ สามารถเขียนได้ในรูป

$$\begin{aligned} x_0 &= \sum_{j=1}^3 N_j a_j x_j \\ &= (35 \cdot 2 \cdot 2) + (21 \cdot 3 \cdot 1) + (15 \cdot 2 \cdot 1) = 233 \end{aligned}$$

ซึ่งทำให้ $x_0 = 233 \equiv 23 \pmod{105}$

แสดงว่าคำตอบของระบบสมการคือ

$$x \equiv 23 \pmod{105} \quad \square$$

ปัญหา 11 จงหาคำตอบของสมการคอนกรูเอนซ์เชิงเส้น $17x \equiv 9 \pmod{276}$

แนวคิด เป็นการเพียงพอที่จะหาคำตอบจากระบบสมการคอนกรูเอนซ์เชิงเส้นต่อไปนี้

$$17x \equiv 9 \pmod{3}$$

$$17x \equiv 9 \pmod{4}$$

$$17x \equiv 9 \pmod{23}$$

ตัวอย่าง 12 อายุของชายผู้หนึ่งเมื่อหารด้วย 3 เหลือเศษ 2 เมื่อหารด้วย 4 เหลือเศษ 1 และเมื่อหารด้วย 5 เหลือเศษ 2 จงหาอายุของชายผู้นี้

วิธีทำ ให้ x เป็นอายุของชายผู้นี้ จากโจทย์จะได้ว่า

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

$$x \equiv 1 \pmod{4}$$

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

เพราะว่า $(3, 4) = 1$, $(3, 5) = 1$, $(4, 5) = 1$ จะได้ว่าระบบสมการคอนกรูเอนซ์นี้มีคำตอบ เพียงชุดเดียวในมอดุโล 60 ($60 = 3 \cdot 4 \cdot 5$)

จากทฤษฎีบทเศษเหลือของจีน ให้ $n = 3 \cdot 4 \cdot 5 = 60$ และ $N_1 = \frac{60}{3} = 20$,

$N_2 = \frac{60}{4} = 15$, $N_3 = \frac{60}{5} = 12$ และให้ x_1, x_2, x_3 เป็นคำตอบของสมการ

$$20x_1 \equiv 1 \pmod{3}$$

$$15x_2 \equiv 1 \pmod{4}$$

$$12x_3 \equiv 1 \pmod{5}$$

จะได้ว่า $x_1 = 2$, $x_2 = 3$ และ $x_3 = 3$

ดังนั้น คำตอบร่วมกันของสมการเชิงเส้น $x \equiv a_i \pmod{n_i}$

เมื่อ $a_1 = 2$, $a_2 = 1$, $a_3 = 2$ และ $n_1 = 3$, $n_2 = 4$, $n_3 = 5$

$$\begin{aligned} \text{สามารถเขียนได้ในรูป } x_0 &= \sum_{j=1}^3 N_j a_j x_j \\ &= (20 \cdot 2 \cdot 2) + (15 \cdot 1 \cdot 3) + (12 \cdot 2 \cdot 3) \\ &= 197 \end{aligned}$$

ซึ่งทำให้ $x_0 = 197 \equiv 17 \pmod{60}$

แสดงว่า คำตอบของระบบสมการคือ $x \equiv 17 \pmod{60}$

ดังนั้น ชายผู้นี้มีอายุ 17 ปี หรือ 77 ปี หรือ 137 ปี □

ตัวอย่าง 11 จงหาจำนวนเต็มบวกทั้งหมดที่หารด้วย 3, 4, 5 แล้วเหลือเศษ 1 หรือ 2

วิธีทำ โจทย์ในตัวอย่างนี้สามารถแปลงให้อยู่ในรูปของสมการคอนกรูเอนซ์ได้ กล่าวคือ

เราต้องการคำตอบของระบบสมการ

$$x \equiv 1 \text{ หรือ } 2 \pmod{3}$$

$$x \equiv 1 \text{ หรือ } 2 \pmod{4}$$

$$x \equiv 1 \text{ หรือ } 2 \pmod{5}$$

ให้ $n_1 = 3$, $n_2 = 4$, $n_3 = 5$ ดังนั้น $n = 3 \cdot 4 \cdot 5 = 60$ และ

$$N_1 = \frac{60}{3} = 20, N_2 = \frac{60}{4} = 15, N_3 = \frac{60}{5} = 12$$

และให้ x_1, x_2, x_3 เป็นคำตอบของสมการ

$$20x_1 \equiv 1 \pmod{3}$$

$$15x_2 \equiv 1 \pmod{4}$$

$$12x_3 \equiv 1 \pmod{5}$$

จะได้ว่า $x_1 = 2$, $x_2 = 3$ และ $x_3 = 3$

ดังนั้น คำตอบร่วมกันของสมการ $x \equiv a_i \pmod{n_i}$ เมื่อ $a_i = 1$ หรือ 2

$$\text{คือ } x_0 = \sum_{j=1}^3 N_j a_j x_j = (20)(a_1)(2) + (15)(a_2)(3) + (12)(a_3)(3)$$

ซึ่งตารางต่อไปนี้จะแสดงคำตอบเมื่อกำหนดค่า $a_i = 1$ หรือ 2

a_1	a_2	a_3	$x \pmod{60}$
1	1	1	$40 + 45 + 36 \equiv 121 \equiv 1$
1	1	2	$40 + 45 + 72 \equiv 157 \equiv 37$
1	2	1	$40 + 90 + 36 \equiv 166 \equiv 46$
1	2	2	$40 + 90 + 72 \equiv 202 \equiv 22$
2	1	1	$80 + 45 + 36 \equiv 161 \equiv 41$
2	1	2	$80 + 45 + 72 \equiv 197 \equiv 17$
2	2	1	$80 + 90 + 36 \equiv 206 \equiv 26$
2	2	2	$80 + 90 + 72 \equiv 242 \equiv 2$

ดังนั้น จำนวนเต็มทั้งหมดที่หารด้วย 3, 4, 5 แล้วเหลือเศษ 1 หรือ 2 คือ

$$x \equiv 1, 2, 17, 22, 26, 37, 41 \text{ หรือ } 46 \pmod{60}$$

□

ปัญหา 14 จงหาคำตอบของระบบสมการคอนกรูเอนซ์

$$x \equiv 1 \pmod{3}$$

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

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

ต่อไปเราจะพิจารณาการหาคำตอบของระบบสมการคอนกรูเอนซ์เชิงเส้น ในกรณีทั่วไป ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 6.2.6 ให้ $n_1, n_2 \in \mathbb{N}$ และ $a_1, a_2 \in \mathbb{Z}$ จะได้ว่า

ระบบสมการคอนกรูเอนซ์เชิงเส้น

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

.....(*)

มีคำตอบ ก็ต่อเมื่อ $(n_1, n_2) \mid (a_1 - a_2)$

และถ้ามีคำตอบ แล้ว จะมีคำตอบเพียงคำตอบเดียวในมอดุโล $[n_1, n_2]$

บทพิสูจน์ ให้ $d = (n_1, n_2)$ และ $n = [n_1, n_2]$

($\Rightarrow$) สมมติว่าระบบสมการ (*) มีคำตอบเป็น x_0

จะได้ว่า $n_1 \mid (x_0 - a_1)$ และ $n_2 \mid (x_0 - a_2)$

แสดงว่า $d \mid (x_0 - a_1)$ และ $d \mid (x_0 - a_2)$ ดังนั้น $d \mid [(x_0 - a_2) - (x_0 - a_1)]$

นั่นคือ $d \mid (a_1 - a_2)$

($\Leftarrow$) สมมติว่า $d \mid (a_1 - a_2)$ และคำตอบของสมการ $x \equiv a_1 \pmod{n_1}$ คือ

$x = a_1 + n_1 k$ เมื่อ k เป็นจำนวนเต็มใด ๆ

จาก $d \mid (a_1 - a_2)$ จะได้ว่าสมการ $n_1 x \equiv (a_2 - a_1) \pmod{n_2}$ มีคำตอบ

ให้ k_1 เป็นคำตอบของสมการ $n_1 x \equiv (a_2 - a_1) \pmod{n_2}$

แสดงว่า $n_1 k_1 + a_1 \equiv a_2 \pmod{n_2}$

ดังนั้น $x_0 = a_1 + n_1 k_1$ เป็นคำตอบของระบบสมการ (*)

ต่อไปจะพิสูจน์ว่า ระบบสมการ (*) มีเพียงคำตอบเดียวในมอดุโล $n = [n_1, n_2]$

ให้ x_1 เป็นคำตอบใด ๆ ของ (*) จะได้ว่า

$$x_1 \equiv a_1 \pmod{n_1}$$

$$x_1 \equiv a_2 \pmod{n_2}$$

ดังนั้น $x_1 \equiv x_0 \pmod{n_1}$ และ $x_1 \equiv x_0 \pmod{n_2}$

โดยทฤษฎีบท 6.1.4 ข้อ 1. จะได้ว่า $x_1 \equiv x_0 \pmod{n}$

นั่นคือ ระบบสมการ (*) นี้มีเพียงคำตอบเดียวในมอดุโล $[n_1, n_2]$ ■

ตัวอย่าง 15 จงหาคำตอบของระบบสมการคอนกรูเอนซ์เชิงเส้น

$$x \equiv 9 \pmod{14}$$

$$x \equiv 6 \pmod{20}$$

วิธีทำ เพราะว่า $(14, 20) = 2$ และ $2 \nmid (9 - 6)$ ดังนั้น ระบบสมการนี้ไม่มีคำตอบ □

ทฤษฎีบทต่อไปจะเป็นการกล่าวถึงการมีคำตอบของระบบสมการคอนกรูเอนซ์เชิงเส้นที่มีมากกว่า 2 สมการ

ทฤษฎีบท 6.2.7 ให้ $n_1, n_2, \dots, n_r \in \mathbb{N}$ และ $a_1, a_2, \dots, a_r \in \mathbb{Z}$ จะได้ว่า

ระบบสมการคอนกรูเอนซ์

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_3 \pmod{n_3}$$

$\vdots$

$$x \equiv a_r \pmod{n_r}$$

จะมีคำตอบ ก็ต่อเมื่อ $(n_i, n_j) \mid (a_i - a_j)$ สำหรับทุก $i, j \in \{1, 2, \dots, r\}$

และถ้ามีคำตอบ จะมีคำตอบเดียวในมอดุโล $[n_1, n_2, \dots, n_r]$

ตัวอย่าง 16 จงหาคำตอบของระบบสมการคอนกรูเอนซ์เชิงเส้น

$$\begin{aligned}x &\equiv 5 \pmod{6} \\x &\equiv 17 \pmod{21} \qquad \dots\dots\dots (*) \\x &\equiv 3 \pmod{28}\end{aligned}$$

วิธีทำ เพราะว่า $(6, 21) = 3$ ซึ่ง $3 \mid (5 - 17)$, $(21, 28) = 7$ ซึ่ง $7 \mid (17 - 3)$ และ

$(6, 28) = 2$ ซึ่ง $2 \mid (5 - 3)$ ดังนั้น ระบบสมการ (*) มีคำตอบ

จาก $x \equiv 5 \pmod{6}$ มีคำตอบเดียวกับคำตอบของระบบสมการ

$$x \equiv 5 \equiv 1 \pmod{2}$$

$$\text{และ } x \equiv 5 \equiv 2 \pmod{3}$$

จาก $x \equiv 17 \pmod{21}$ มีคำตอบเดียวกับคำตอบของระบบสมการ

$$x \equiv 17 \equiv 2 \pmod{3}$$

$$\text{และ } x \equiv 17 \equiv 3 \pmod{7}$$

จาก $x \equiv 3 \pmod{28}$ มีคำตอบเดียวกับคำตอบของระบบสมการ

$$x \equiv 3 \pmod{4}$$

$$\text{และ } x \equiv 3 \pmod{7}$$

เนื่องจากคำตอบของสมการ $x \equiv 3 \pmod{4}$ จะเป็นคำตอบเดียวกับคำตอบของ

สมการ $x \equiv 1 \pmod{2}$ ดังนั้น คำตอบของระบบสมการ (*) จะมีคำตอบเดียวกับระบบสมการ

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

$$x \equiv 3 \pmod{4} \qquad \dots\dots\dots (**)$$

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

โดยใช้ทฤษฎีบทเศษเหลือของจีน จะได้ว่าคำตอบของระบบสมการ (**) คือ

$$x \equiv 59 \pmod{84}$$

□

ปัญหา 17 จงหาคำตอบของระบบสมการเชิงเส้นต่อไปนี้

$$(15.1) \quad x \equiv 1 \pmod{10}$$

$$x \equiv 3 \pmod{15}$$

$$(15.3) \quad x \equiv 2 \pmod{4}$$

$$x \equiv 11 \pmod{9}$$

$$(15.2) \quad x \equiv 2 \pmod{6}$$

$$x \equiv 11 \pmod{9}$$

$$(15.4) \quad 2x \equiv 1 \pmod{5}$$

$$3x \equiv 5 \pmod{17}$$

สมการคอนกรูเอนซ์ที่มีดีกรีมากกว่าหนึ่ง

ในการหาคำตอบของสมการคอนกรูเอนซ์ที่มีดีกรีมากกว่าหนึ่งนั้นมีความแตกต่างจากการหาคำตอบของสมการคอนกรูเอนซ์เชิงเส้นมาก ทั้งนี้เพราะไม่มีวิธีการสำหรับที่จะสรุปได้เด่นชัดว่าสมการที่กำหนดให้จะมีคำตอบหรือไม่ และถ้ามีคำตอบจะมีจำนวนคำตอบเท่าไร

ให้ $f(x) = c_m x^m + c_{m-1} x^{m-1} + \dots + c_1 x + c_0$ โดยที่ $c_i \in \mathbb{Z}$ และ $c_m \neq 0$

เราพบว่า ถ้า u เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$ และ $u \equiv v \pmod{n}$

จะได้โดยทฤษฎีบท 6.2.1 ข้อ 2 ว่า v เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$

จากข้อความข้างต้นเราพบว่า ถ้า n มีค่าน้อย เราสามารถแทนค่า x ในสมการด้วย $0, 1, 2, \dots, n-1$ เราก็จะได้คำตอบของสมการดังกล่าว

จากการประยุกต์ทฤษฎีบท 6.1.3 ข้อ 7. เราพบว่า ถ้า $d \mid n$ และ $d > 0$ และ ถ้า u เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$ แล้ว u จะเป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{d}$

ดังนั้น ถ้า $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ และ u เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$ แล้ว u จะเป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ สำหรับทุก $i = 1, 2, \dots, r$ จากทฤษฎีบทเศษเหลือของจีน เราสามารถแสดงได้ว่าถ้าระบบสมการ $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ มีคำตอบสำหรับทุก $i = 1, 2, \dots, r$ จะได้ว่าสมการ $f(x) \equiv 0 \pmod{n}$ จะมีคำตอบ ฉะนั้นเราจึงได้ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 6.2.7 ให้ $f(x) = c_m x^m + c_{m-1} x^{m-1} + \dots + c_1 x + c_0$ โดยที่ $c_i \in \mathbb{Z}$, $c_m \neq 0$ และ

$n \in \mathbb{N}$ ซึ่ง $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ

จะได้ว่า สมการ $f(x) \equiv 0 \pmod{n}$ มีคำตอบ ก็ต่อเมื่อ

สมการ $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ มีคำตอบ สำหรับทุก $i = 1, 2, \dots, r$

บทพิสูจน์ ให้ $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ

และ $f(x) = c_m x^m + c_{m-1} x^{m-1} + \dots + c_1 x + c_0$ โดยที่ $c_i \in \mathbb{Z}$ และ $c_m \neq 0$

($\Rightarrow$) สมมติว่าสมการ $f(x) \equiv 0 \pmod{n}$ มีคำตอบ จะได้ว่ามี $b_0 \in \mathbb{Z}$ ซึ่ง

$$f(b_0) \equiv 0 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}}$$

แสดงว่า $f(b_0) \equiv 0 \pmod{p_i^{\alpha_i}}$ สำหรับทุก $i = 1, 2, \dots, r$

นั่นคือสมการ $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ สำหรับทุก $i = 1, 2, \dots, r$

($\Leftarrow$) สมมติว่าสมการ $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ สำหรับทุก $i = 1, 2, \dots, r$

จะได้ว่ามี $a_i \in \mathbb{Z}$ ซึ่ง $f(a_i) \equiv 0 \pmod{p_i^{\alpha_i}}$ สำหรับทุก $i = 1, 2, \dots, r$

และเมื่อ $n_i = p_i^{\alpha_i}$ โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า ระบบสมการ

$$x \equiv a_i \pmod{n_i} \quad \text{มีคำตอบ } u = \sum_{j=1}^r \frac{n}{n_j} b_j a_j$$

เมื่อ b_j เป็นคำตอบของสมการ $\frac{n}{n_j} x \equiv 1 \pmod{n_j}$

จะเห็นได้ชัดว่า u เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$ ■

ตัวอย่าง 17 จงหาคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{15}$

วิธีทำ เพราะว่า $15 = 3 \cdot 5$ ดังนั้นการหาคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{15}$

ก็จะเหมือนกับการหาคำตอบของระบบสมการ

$$x^2 + x + 7 \equiv 0 \pmod{3} \quad \dots\dots\dots(1)$$

$$x^2 + x + 7 \equiv 0 \pmod{5} \quad \dots\dots\dots(2)$$

จากการแทนค่า $x = 0, 1, 2$ ใน (1) พบว่า $x \equiv 1 \pmod{3}$ เป็นคำตอบของ (1)

จากการแทนค่า $x = 0, 1, 2, 3, 4$ ใน (2) พบว่า สมการ (2) ไม่มีคำตอบ

ดังนั้น สมการ $x^2 + x + 7 \equiv 0 \pmod{15}$ ไม่มีคำตอบ □

ตัวอย่าง 18 จงหาคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$

วิธีทำ เพราะว่า $189 = 3^3 \cdot 7$ ดังนั้นการหาคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$

ก็เหมือนกับการหาคำตอบของระบบสมการ

$$x^2 + x + 7 \equiv 0 \pmod{3^3} \quad \dots\dots\dots(1)$$

$$x^2 + x + 7 \equiv 0 \pmod{7} \quad \dots\dots\dots(2)$$

เพราะว่าคำตอบของสมการ (1) คือ $x \equiv 4, 13, 22 \pmod{3^3}$

และคำตอบของสมการ (2) คือ $x \equiv 0, 6 \pmod{7}$

ฉะนั้นคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$ จะมี 6 คำตอบ

โดยการใช้ทฤษฎีบทเศษเหลือของจีน จะได้ $b_1 \equiv 4 \pmod{3^3}$, $b_2 \equiv 6 \pmod{7}$

และคำตอบทั้ง 6 คำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$ สามารถเขียนได้ในรูป

$$u \equiv \frac{189}{27}(4)a_1 + \frac{189}{7}(6)a_2 \pmod{189}$$

โดยที่ $a_1 = 4, 13, 22$ และ $a_2 = 0, 6$

และจะได้ $u \equiv 28a_1 + 162a_2 \pmod{189}$

ดังนั้นจากการแทนค่า a_1 และ a_2 ในทุก ๆ กรณีจะได้

$$u \equiv 28(4) + 162(0) \equiv 112 \pmod{189},$$

$$u \equiv 28(4) + 162(6) \equiv 139 \pmod{189},$$

$$u \equiv 28(13) + 162(0) \equiv 175 \pmod{189},$$

$$u \equiv 28(13) + 162(6) \equiv 13 \pmod{189},$$

$$u \equiv 28(22) + 162(0) \equiv 49 \pmod{189},$$

$$u \equiv 28(22) + 162(6) \equiv 76 \pmod{189}$$

เพราะฉะนั้นคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$ คือ

$$x \equiv 13, 49, 76, 112, 139, 175 \pmod{189} \quad \square$$

โจทย์ปัญหา 6.2

1. จงหาคำตอบทั้งหมดของสมการในแต่ละข้อต่อไปนี้

(1.1) $20x \equiv 4 \pmod{30}$

(1.2) $20x \equiv 3 \pmod{4}$

(1.3) $353x \equiv 254 \pmod{400}$

2. จงหาคำตอบของระบบสมการต่อไปนี้

$$x \equiv 1 \pmod{4}$$

$$x \equiv 0 \pmod{3}$$

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

3. จงหาคำตอบของระบบสมการต่อไปนี้

$$x \equiv 1 \pmod{2}$$

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

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

$$x \equiv 4 \pmod{7}$$

4. จงหาจำนวนเต็มบวกทั้งหมดที่หารด้วย 2, 3, 6 และ 12 แล้วเหลือเศษ 1, 2, 5 และ 5 ตามลำดับ

5. ถ้า $f(x) \equiv 0 \pmod{p}$ มี j คำตอบ เมื่อ p เป็นจำนวนเฉพาะและ $g(x) \equiv 0 \pmod{p}$ ไม่มีคำตอบ จงพิสูจน์ว่า $f(x)g(x) \equiv 0 \pmod{p}$ มีเพียง j คำตอบเท่านั้น

6. ถ้าสมการ $f(x) \equiv 0 \pmod{n}$ มี n คำตอบ จงพิสูจน์ว่าจำนวนเต็มทุกจำนวนจะเป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{n}$

7. จงพิสูจน์ว่า nl จะหารผลคูณของจำนวนเต็ม n จำนวนเรียงต่อเนื่องกัน

8. จงหาคำตอบของสมการในแต่ละข้อต่อไปนี้

$$(8.1) \quad x^3 + 4x + 8 \equiv 0 \pmod{15}$$

$$(8.2) \quad x^2 + 2x - 3 \equiv 0 \pmod{45}$$

$$(8.3) \quad x^3 + 2x - 3 \equiv 0 \pmod{9}$$

$$(8.4) \quad x^2 + 2x - 3 \equiv 0 \pmod{5}$$

$$(8.5) \quad x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{503}$$

$$(8.6) \quad x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$$

6.3 ทฤษฎีบทของแฟร์มาต์และออยเลอร์

ทฤษฎีบทของแฟร์มาต์ที่จะกล่าวถึงในหัวข้อนี้ รู้จักกันในชื่อว่า *Fermat's little Theorem* ซึ่งเป็นชื่อเรียกให้แตกต่างจากทฤษฎีบทของแฟร์มาต์ที่รู้จักกันดีอีกทฤษฎีบทหนึ่ง คือ ทฤษฎีบทสุดท้ายของแฟร์มาต์ (*Fermat's Last Theorem*) ซึ่งจะได้อีกกล่าวถึงในบทต่อไป

ทฤษฎีบทของแฟร์มาต์ที่จะศึกษาในหัวข้อนี้มีใจความว่า ถ้า p เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มใด ๆ ที่หารด้วย p ไม่ลงตัว แล้ว p จะหาร $a^{p-1} - 1$ ทฤษฎีบทดังกล่าวนี้แฟร์มาต์เขียนถึงเบสซี (Bessy ค.ศ. 1605 - 1670) ในปี ค.ศ. 1640 ซึ่งเขาไม่ได้พิสูจน์อะไรเป็นหลักฐานไว้ จนเวลาผ่านไปเกือบ 100 ปี ออยเลอร์ได้พบวิธีพิสูจน์และได้ตีพิมพ์เป็นครั้งแรกในปี ค.ศ. 1736

ก่อนการศึกษาทฤษฎีบทของแฟร์มาต์และออยเลอร์นั้น พื้นฐานที่จำเป็นอย่างหนึ่งคือ เราจะต้องรู้จักระบบส่วนตกค้างลดทอน ซึ่งมีรายละเอียดดังบทนิยามต่อไปนี้

บทนิยาม 6.3.1 ระบบส่วนตกค้างลดทอน (*reduced residue system*) มอดุโล n คือ เซตของจำนวนเต็มในระบบส่วนตกค้างบริบูรณ์ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ n
 ระบบส่วนตกค้างลดทอนมอดุโล n ที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{0, 1, 2, \dots, n-1\}$ ซึ่งคือ $\{k \mid 0 \leq k < n \text{ ที่ } (k, n) = 1\}$ เรียกว่า ระบบส่วนตกค้างลดทอนที่ไม่เป็นลบค่าน้อยสุด (*least non-negative reduced residue system*) มอดุโล n

จากบทนิยามเราพบว่า

- (1) เซตของจำนวนเต็ม r_i เป็นระบบส่วนตกค้างลดทอนมอดุโล n ก็ต่อเมื่อ
 - (1.1) $(r_i, n) = 1$ ทุก ๆ r_i
 - (1.2) ถ้า $i \neq j$ แล้ว $r_i \not\equiv r_j \pmod{n}$
 - (1.3) ถ้า x เป็นจำนวนเต็มที่ $(x, n) = 1$ แล้ว มี r_i ที่ $x \equiv r_i \pmod{n}$
- (2) ระบบส่วนตกค้างลดทอนมอดุโล n ทุกระบบจะมีจำนวนสมาชิกเท่ากัน

จากบทนิยามของ $\phi(n)$ ในหัวข้อ 5.4 เราพบว่า จำนวนสมาชิกของระบบส่วนตกค้างลดทอนมอดุโล n คือ $\phi(n)$

- ตัวอย่าง 1**
- (1.1) ระบบส่วนตกค้างลดทอนมอดุโล 8 ที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{0, 1, 2, 3, 4, 5, 6, 7\}$ คือ $\{1, 3, 5, 7\}$ และที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{8, -7, 2, 11, 4, 5, 14, 15\}$ คือ $\{-7, 11, 5, 15\}$
 - (1.2) ให้ p เป็นจำนวนเฉพาะ ระบบส่วนตกค้างลดทอนมอดุโล p ที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{0, 1, 2, \dots, p-1\}$ คือ $\{1, 2, 3, \dots, p-1\}$ □

ทฤษฎีบทประกอบ 6.3.2 ถ้า $\{a_1, a_2, \dots, a_{\phi(n)}\}$ เป็นเซตของจำนวนเต็มซึ่งทุก ๆ i , $(a_i, n) = 1$ และทุก ๆ $i \neq j$, $a_i \not\equiv a_j \pmod{n}$ แล้ว $\{a_1, a_2, \dots, a_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n

บทพิสูจน์ ให้ r_i เป็นเศษจากการหาร a_i ด้วย n

ดังนั้น $a_i \equiv r_i \pmod{n}$ และ $(r_i, n) = 1$ โดยทฤษฎีบท 6.1.3 ข้อ 1. แสดงว่า

$\{r_1, r_2, \dots, r_{\phi(n)}\} \subseteq \{0, 1, 2, \dots, n-1\}$ ที่มีสมาชิก $\phi(n)$ ตัว

ดังนั้น $\{r_1, r_2, \dots, r_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n ที่ไม่เป็นลบค่าน้อยสุด

ให้ a เป็นจำนวนเต็มใด ๆ ที่ $(a, n) = 1$ และให้ r เป็นเศษเหลือจากการหาร a ด้วย n

ทำให้ได้ว่า $a \equiv r \pmod{n}$ และ $(r, n) = 1$

ดังนั้น จะมี i ที่ $r = r_i$ นั่นคือ $a \equiv r = r_i \equiv a_i \pmod{n}$

สรุปได้ว่า $\{a_1, a_2, \dots, a_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n ■

ทฤษฎีบท 6.3.3 ให้ $(a, n) = 1$ และให้ $\{r_1, r_2, \dots, r_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n
จะได้ว่า $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n ด้วย

บทพิสูจน์ เนื่องจาก $(a, n) = 1$ และ $(r_i, n) = 1$ ดังนั้น $(ar_i, n) = 1$
เนื่องจาก $ar_1, ar_2, \dots, ar_{\phi(n)}$ มี $\phi(n)$ ตัว ดังนั้นโดยทฤษฎีบทประกอบ 6.3.2
เราเพียงแต่แสดงว่า แต่ละคู่จะไม่คอนกรูเอนซ์กัน สมมติว่า $ar_i \equiv ar_j \pmod{n}$
เนื่องจาก $(a, n) = 1$ ดังนั้นโดยทฤษฎีบท 6.1.3 ข้อ 2. จะได้ว่า $r_i \equiv r_j \pmod{n}$
ทำให้ได้ว่า $i = j$ ■

ทฤษฎีบท 6.3.4 ทฤษฎีบทของออยเลอร์ (Euler's Theorem)

ถ้า $a \in \mathbb{Z}$ และ $n \in \mathbb{N}$ ซึ่ง $(a, n) = 1$ แล้ว $a^{\phi(n)} \equiv 1 \pmod{n}$

บทพิสูจน์ ให้ $r_1, r_2, \dots, r_{\phi(n)}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n โดยทฤษฎีบท 6.3.3 ได้ว่า
 $ar_1, ar_2, \dots, ar_{\phi(n)}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n ด้วย
นั่นคือ ทุก ๆ r_i จะมี ar_j ซึ่ง $ar_j \equiv r_i \pmod{n}$
ดังนั้น $ar_1 \cdot ar_2 \cdots ar_{\phi(n)} \equiv r_1 \cdot r_2 \cdots r_{\phi(n)} \pmod{n}$
แสดงว่า $a^{\phi(n)} [r_1 \cdot r_2 \cdots r_{\phi(n)}] \equiv r_1 \cdot r_2 \cdots r_{\phi(n)} \pmod{n}$
เนื่องจากแต่ละ i , $(r_i, n) = 1$ ดังนั้น $(r_1 \cdot r_2 \cdots r_{\phi(n)}, n) = 1$
โดยทฤษฎีบท 6.1.3 ข้อ 3. จะได้ว่า $a^{\phi(n)} \equiv 1 \pmod{n}$ ■

บทแทรก 6.3.5 ทฤษฎีบทของแฟร์มาต์ (Fermat's Little Theorem)

ให้ p เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มที่ $p \nmid a$ จะได้ว่า $a^{p-1} \equiv 1 \pmod{p}$

บทพิสูจน์ จาก $p \nmid a$ และ p เป็นจำนวนเฉพาะ จะได้ $(a, p) = 1$ และ $\phi(p) = p - 1$
ดังนั้น $a^{p-1} \equiv 1 \pmod{p}$ ■

บทแทรก 6.3.6 ให้ p เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มใด ๆ

จะได้ว่า $a^p \equiv a \pmod{p}$

บทพิสูจน์ ให้ a เป็นจำนวนเต็มใด ๆ และ p เป็นจำนวนเฉพาะ

กรณี 1 $p \mid a$ จะได้ว่า $a \equiv 0 \pmod{p}$ และ $a^p \equiv 0 \pmod{p}$

ดังนั้น $a^p \equiv a \pmod{p}$

กรณี 2 $p \nmid a$ จากบทแทรก 6.3.5 จะได้ว่า $a^{p-1} \equiv 1 \pmod{p}$

ดังนั้น $a^p \equiv a \pmod{p}$ ■

ตัวอย่าง 2 จงหาเศษที่เกิดจากการหาร 3^{1000} ด้วย 17

วิธีทำ จากทฤษฎีบทของแฟร์มาต์ จะได้ว่า $3^{16} \equiv 1 \pmod{17}$

$$\text{ดังนั้น } 3^{1000} = (3^{16})^{62} \cdot 3^8 \equiv 1^{62} \cdot 3^4 \cdot 3^4 \equiv (-4)(-4) = 16 \pmod{17}$$

นั่นคือ เศษที่เกิดจากการหาร 3^{1000} ด้วย 17 ลงตัวคือ 16 □

ตัวอย่าง 3 จงพิจารณาว่า $2^{117} - 2$ หารด้วย 117 ลงตัวหรือไม่

วิธีทำ เนื่องจาก $2^7 = 128 \equiv 11 \pmod{117}$

$$\text{จะได้ว่า } (2^7)^{16} \cdot 2^5 \equiv (11)^{16} \cdot 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}$$

$$\text{แต่ } 2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}$$

$$\text{ดังนั้น } 2^{117} \equiv 44 \pmod{117} \text{ และจาก } 44 \equiv 2 \pmod{117}$$

นั่นคือ $2^{117} \equiv 2 \pmod{117}$ แสดงว่า $2^{117} - 2$ หารด้วย 117 ไม่ลงตัว □

ตัวอย่าง 4 จงแสดงว่า $3^{256} \equiv 21 \pmod{100}$

พิสูจน์ เพราะว่า $3^{\phi(100)} \equiv 1 \pmod{100}$ แสดงว่า $3^{40} \equiv 1 \pmod{100}$

$$\text{จะได้ว่า } (3^{40})^6 \cdot 3^{16} \equiv 1^6 \cdot 3^{16} \pmod{100}$$

$$\text{และ } 3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2 \equiv (61)^2 \equiv 21 \pmod{100}$$

$$\text{ดังนั้น } 3^{256} \equiv 21 \pmod{100} \quad \square$$

ตัวอย่าง 5 จงหาเลขโดดสามหลักสุดท้ายของ 7^{1000}

วิธีทำ เพราะว่า $7^{\phi(1000)} \equiv 1 \pmod{1000}$

$$\text{แสดงว่า } 7^{400} \equiv 1 \pmod{1000} \text{ และ } 7^{1000} = (7^{400})^{25} \equiv 1^{25} = 1 \pmod{1000}$$

ดังนั้น เลขโดดสามหลักสุดท้ายของ 7^{1000} คือ 001 □

ตัวอย่าง 6 จงหาค่า a เมื่อ $102^{1999} + 103^{1999} \equiv a \pmod{1999}$ โดยที่ $0 \leq a < 1999$

วิธีทำ เพราะว่า 1999 เป็นจำนวนเฉพาะ จะได้ว่า

$$102^{1998} \equiv 1 \pmod{1999} \quad \text{และ} \quad 103^{1998} \equiv 1 \pmod{1999}$$

$$\text{ดังนั้น } 102^{1999} \equiv 102 \pmod{1999} \quad \text{และ} \quad 103^{1999} \equiv 103 \pmod{1999}$$

$$\text{แสดงว่า } 102^{1999} + 103^{1999} \equiv 102 + 103 \pmod{1999}$$

$$\text{นั่นคือ } a = 205 \quad \square$$

ทฤษฎีบท 6.3.7 ถ้า p และ q เป็นจำนวนเฉพาะที่แตกต่างกันซึ่ง $a^q \equiv a \pmod{p}$

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

บทพิสูจน์ ให้ p และ q เป็นจำนวนเฉพาะที่แตกต่างกัน และ $a \in \mathbb{Z}$ โดยบทแทรก 6.3.6 จะได้ว่า

$$a^q \equiv a \pmod{q} \quad \text{และ} \quad a^p \equiv a \pmod{p}$$

เนื่องจาก $a^q \equiv a \pmod{p}$ และ $a^p \equiv a \pmod{q}$
 ดังนั้น $(a^q)^p \equiv a^p \pmod{p}$ และ $(a^p)^q \equiv a^q \pmod{q}$
 แสดงว่า $a^{pq} \equiv a^p \equiv a \pmod{p}$ และ $a^{pq} \equiv a^q \equiv a \pmod{q}$
 โดยทฤษฎีบท 6.1.5 จะได้ว่า $a^{pq} \equiv a \pmod{pq}$ ■

ตัวอย่าง 7 จงแสดงว่า $2^{340} \equiv 1 \pmod{341}$

บทพิสูจน์ เนื่องจาก $341 = 11 \cdot 13$ และ $2^{10} = 1024 = 31 \cdot 33 + 1$
 จะได้ว่า $2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$
 และ $2^{31} = 2(2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}$
 ดังนั้น $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$
 นั่นคือ $2^{341} \equiv 2 \pmod{341}$ ทำให้ $2^{340} \equiv 1 \pmod{341}$ □

ทฤษฎีบท 6.3.8 ให้ p เป็นจำนวนเฉพาะ จะได้ว่า

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

บทพิสูจน์ ($\Rightarrow$) สมมติว่า $x^2 \equiv 1 \pmod{p}$ ดังนั้น $p \mid (x^2 - 1)$
 นั่นคือ $p \mid [(x-1)(x+1)]$
 ทำให้ได้ว่า $p \mid (x-1)$ หรือ $p \mid (x+1)$
 นั่นคือ $x \equiv 1$ หรือ $-1 \pmod{p}$
 ($\Leftarrow$) สมมติว่า $x \equiv 1$ หรือ $-1 \pmod{p}$
 ดังนั้น $p \mid (x-1)$ หรือ $p \mid (x+1)$
 เพราะฉะนั้น $p \mid [(x-1)(x+1)]$ นั่นคือ $p \mid (x^2 - 1)$
 ดังนั้น $x^2 \equiv 1 \pmod{p}$ ■

หมายเหตุ ในทฤษฎีบท 6.3.8 ถ้า p ไม่เป็นจำนวนเฉพาะ ข้อความนี้จะไม่เป็นจริง เช่น พิจารณา
 $x \equiv 3 \pmod{8}$ จะได้ว่า $x^2 \equiv 1 \pmod{8}$ แต่ $x \not\equiv 1$ และ $x \not\equiv -1 \pmod{8}$
 ทฤษฎีบทที่จะกล่าวต่อไปเป็นข้อคาดเดาของวิลสันแต่สามารถพิสูจน์ได้โดยลากรองจ์

ทฤษฎีบท 6.3.9 ทฤษฎีบทของวิลสัน (Wilson's Theorem)

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

บทพิสูจน์ ถ้า $p = 2$ หรือ 3 จะเห็นได้โดยง่ายว่า $(p-1)! \equiv -1 \pmod{p}$
 สำหรับ $p \geq 5$ ให้ a เป็นจำนวนเต็มซึ่ง $1 \leq a \leq p-1$
 ดังนั้น $(a, p) = 1$ โดยบทแทรก 6.2.3 จะมีจำนวนเต็ม a' ซึ่ง $1 \leq a' \leq p-1$
 ที่ทำให้ $aa' \equiv 1 \pmod{p}$
 ถ้า $a = a'$ จะได้ว่า $a^2 \equiv 1 \pmod{p}$ ดังนั้น โดยทฤษฎีบท 6.3.8 จะได้ว่า

$a \equiv 1$ หรือ $-1 \pmod{p}$ ดังนั้น $a = 1$ หรือ $p-1$ ทำให้ได้ว่า
 ทุก a ที่ $2 \leq a \leq p-2$ มี a' เพียงตัวเดียวที่ $2 \leq a' \leq p-2$
 และทำให้ $aa' \equiv 1 \pmod{p}$ นั่นคือ $2 \cdot 3 \cdot 4 \cdots (p-2)$ จะจับคู่กันได้ $\frac{p-3}{2}$ คู่
 ที่ผลคูณของแต่ละคู่จะคอนกรูเอนซ์กับ 1 มอดุโล p
 เพราะฉะนั้น $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p}$ ซึ่งทำให้
 $(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-2) (p-1) \equiv p-1 \equiv -1 \pmod{p}$

ตัวอย่าง 8 จงหาเศษที่เกิดจากการหาร $15!$ ด้วย 17

วิธีทำ เนื่องจาก 17 เป็นจำนวนเฉพาะ จากทฤษฎีบทของวิลสัน

จะได้ว่า $16! = 16 \cdot 15! \equiv -1 \pmod{17}$

เนื่องจาก $16 \equiv -1 \pmod{17}$ ฉะนั้น $16 \cdot 15! \equiv 16 \pmod{17}$

จาก $(16, 17) = 1$ โดยทฤษฎีบท 6.1.4 ข้อ 3. จะได้ว่า $15! \equiv 1 \pmod{17}$

นั่นคือ เศษที่เกิดจากการหาร $15!$ ด้วย 17 คือ 1

ตัวอย่าง 9 จงแสดงว่า $18! \equiv -1 \pmod{437}$

บทพิสูจน์ จาก $437 = 19 \cdot 23$ ซึ่ง 19 และ 23 เป็นจำนวนเฉพาะ โดยทฤษฎีบทของวิลสัน

จะได้ว่า $18! \equiv -1 \pmod{19}$ และ $22! \equiv -1 \pmod{23}$

เนื่องจาก $22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23}$

และ $-1 \equiv -22 \cdot 21 \cdot 20 \cdot 19 \pmod{23}$

ดังนั้น $22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -22 \cdot 21 \cdot 20 \cdot 19 \pmod{23}$

จาก $(22 \cdot 21 \cdot 20 \cdot 19, 23) = 1$ โดยทฤษฎีบท 6.1.4 ข้อ 3. จะได้ว่า $18! \equiv -1 \pmod{23}$

ดังนั้นจาก $18! \equiv -1 \pmod{19}$ และ $18! \equiv -1 \pmod{23}$

จะได้ว่า $18! \equiv -1 \pmod{437}$

ปัญหา 10 จงหาเศษที่เกิดจากการหาร $2(26!)$ ด้วย 29

ทฤษฎีบทของวิลสันได้ถูกนำไปประยุกต์ใช้ดังนี้

ทฤษฎีบท 6.3.10 ให้ p เป็นจำนวนเฉพาะ จะได้ว่า $x^2 \equiv -1 \pmod{p}$ มีคำตอบ ก็ต่อเมื่อ
 $p = 2$ หรือ $p \equiv 1 \pmod{4}$

บทพิสูจน์ ($\Rightarrow$) ให้ a เป็นคำตอบของ $x^2 \equiv -1 \pmod{p}$ และ p เป็นจำนวนเฉพาะคือ
 นั่นคือ $a^2 \equiv -1 \pmod{p}$

ดังนั้น $p \nmid a$ และ $1 \equiv a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$

เนื่องจาก $\frac{p-1}{2}$ เป็นจำนวนเต็ม ดังนั้น $(-1)^{\frac{p-1}{2}} = 1$ หรือ -1

แต่ $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ และ $-1 \not\equiv 1 \pmod{p}$

ดังนั้น $(-1)^{\frac{p-1}{2}} = 1$ ทำให้ได้ว่า $\frac{p-1}{2}$ เป็นจำนวนเต็มคู่

นั่นคือ $4 \mid (p-1)$ แสดงว่า $p \equiv 1 \pmod{4}$

($\Leftarrow$) ให้ $p \equiv 1 \pmod{4}$ ดังนั้น $\frac{p-1}{2}$ เป็นจำนวนเต็มคู่ จากทฤษฎีบทของวิลสัน จะได้ว่า

$$-1 \equiv 1 \cdot 2 \cdot \dots \cdot \left(\frac{p-1}{2}\right) \left(\frac{p+1}{2}\right) \dots (p-2)(p-1) \equiv (p-1)! \pmod{p}$$

$$\equiv \prod_{j=1}^n j(p-j) \pmod{p} \quad \text{เมื่อ } n = \frac{p-1}{2}$$

$$\equiv \prod_{j=1}^n (-j^2) = (-1)^{\frac{p-1}{2}} \prod_{j=1}^n j^2 = (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

$$\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

แสดงว่า สมการ $x^2 \equiv -1 \pmod{p}$ มีคำตอบ และคำตอบคือ $x = \left(\frac{p-1}{2}\right)!$ ■

จากทฤษฎีบทของวิลสัน จะได้ว่ามีจำนวนประกอบไม่จำกัดที่อยู่ในรูป $n! + 1$ และในทางกลับกัน มีคำกล่าวว่า มีจำนวนเฉพาะไม่จำกัดหรือไม่ที่อยู่ในรูป $n! + 1$ ขณะนี้เราทราบว่าจำนวนเฉพาะที่มีค่ามากที่สุดที่อยู่ในรูป $n! + 1$ คือ $1477! + 1$ ค้นพบในปี ค.ศ. 1984 และพบว่าถ้า $1 \leq n \leq 100$ แล้วจำนวนเฉพาะที่อยู่ในรูป $n! + 1$ คือ $n = 1, 2, 3, 11, 27, 37, 41, 73$ และ 77

โจทย์ปัญหา 6.3

1. จงหาเศษที่เกิดจากการหาร $2^{1000000}$ ด้วย 17
2. จงหาเศษที่เกิดจากการหาร $10^{10} + 10^{10^2} + 10^{10^3} + \dots + 10^{10^{10}}$ ด้วย 7
3. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะคี่ แล้ว $2(p-3)! \equiv -1 \pmod{p}$
4. จงแสดงว่า $11^{320} - 1$ หารด้วย 17 ลงตัว
5. จงแสดงว่า $1835^{1910} + 1986^{2061} \equiv 0 \pmod{7}$
6. จงแสดงว่า $561 \mid (2^{561} - 2)$ และ $561 \mid (3^{561} - 3)$
7. จงแสดงว่า $2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$
8. จงแสดงว่า ถ้า p และ q เป็นจำนวนเฉพาะที่ต่างกัน แล้ว $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$
9. จงแสดงว่า ถ้า a เป็นจำนวนเต็มคี่ แล้ว $a^{33} \equiv a \pmod{4080}$
10. ถ้า m และ n เป็นจำนวนเฉพาะสัมพัทธ์ จงพิสูจน์ว่า

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$
11. จงหาจำนวนเต็มบวก r ที่น้อยที่สุดที่ทำให้ $100! + 102! \equiv r \pmod{101}$

โจทย์ปัญหาเสริมเรื่อง คอนกรูเอนซ์

- ปัญหา 1** ให้ p เป็นจำนวนเฉพาะซึ่ง $p > 5$ จงพิสูจน์ว่า จะมีสมาชิกในลำดับ $9, 99, 999, \dots$ เป็นจำนวนไม่จำกัดที่มี p เป็นตัวหาร
- ปัญหา 2** ให้ p เป็นจำนวนเฉพาะซึ่ง $p > 5$ จงพิสูจน์ว่า จะมีสมาชิกในลำดับ $1, 11, 111, 1111, \dots$ เป็นจำนวนไม่จำกัดที่มี p เป็นตัวหาร
- ปัญหา 3** จงพิสูจน์ว่า ถ้า $f(x)$ เป็นพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็ม และ $f(x) \equiv k \pmod{m}$ แล้ว $f(a + tm) \equiv k \pmod{m}$ สำหรับจำนวนเต็ม t ใด ๆ
- ปัญหา 4** จงพิสูจน์ว่า กำลังสองของจำนวนเต็มใด ๆ จะต้องมียุทธศาสตร์เป็นจำนวนเต็มจำนวนหนึ่ง คือ $0, 1, 4, 5, 6, 9$
- ปัญหา 5** ถ้า p เป็นจำนวนเฉพาะ จงพิสูจน์ว่า $(p-1)! + 1 = p^k$ สำหรับจำนวนเต็ม k บางตัว ก็ต่อเมื่อ $p = 2, 3$ หรือ 5
- ปัญหา 6** จงพิสูจน์ว่า $(p-1)! \equiv (p-1) \pmod{1+2+3+\dots+(p-1)}$ เมื่อ p เป็นจำนวนเฉพาะ
- ปัญหา 7** ให้ p เป็นจำนวนเฉพาะและ $h+k = p-1$ เมื่อ $h \geq 0$ และ $k \geq 0$ จงพิสูจน์ว่า $h!k! + (-1)^h \equiv 0 \pmod{p}$
- ปัญหา 8** ให้ p เป็นจำนวนเฉพาะ ถ้า $a^p \equiv b^p \pmod{p}$ จงพิสูจน์ว่า $a^p \equiv b^p \pmod{p^2}$
- ปัญหา 9** ถ้า n เป็นจำนวนประกอบ จงพิสูจน์ว่า $(n-1)! + 1$ ไม่สามารถเขียนอยู่ในรูป n^k สำหรับจำนวนเต็มบวก k ใด ๆ
- ปัญหา 10** จงแสดงว่า $36^{36} + 41^{41}$ หารด้วย 77 ลงตัว
- วิธีทำ** เนื่องจาก $36 \equiv 1 \pmod{7}$ และ $36^5 \equiv 3^5 \equiv 1 \pmod{11}$
 จะได้ว่า $36^5 \equiv 1 \pmod{77}$
 เนื่องจาก $41 \equiv -36 \pmod{77}$

เราพบว่า $36^{36} + 41^{41} \equiv [36^{36} + (-36)^{41}] \pmod{77}$
 $\equiv 36^{36}[1 - (36)^5] \pmod{77}$
 เนื่องจาก $36^5 \equiv 1 \pmod{77}$ จะได้ว่า $[1 - 36^5] \equiv 0 \pmod{77}$
 และจาก $(36)^{35} \equiv 1 \pmod{77}$ และ $36 \equiv 36 \pmod{77}$
 จะได้ว่า $36^{36} \equiv 36 \pmod{77}$
 พิจารณาจาก $36^{36} \equiv 36 \pmod{77}$ และ $(1 - 36^5) \equiv 0 \pmod{77}$
 จะได้ว่า $(36)^{36}[1 - (36)^5] \equiv (36)(0) \pmod{77}$
 $\equiv 0 \pmod{77}$
 ดังนั้น $36^{36} + 41^{41}$ หารด้วย 77 ลงตัว □

ปัญหา 11 จงแสดงว่า $19^{19} + 69^{19}$ หารด้วย 44 ลงตัว และ $2^{70} + 3^{70}$ หารด้วย 13 ลงตัว

ปัญหา 12 จงหาเลขโดดสามหลักสุดท้ายของจำนวน 13^{398}

ปัญหา 13 จงแสดงว่า $20^{15} - 1$ หารด้วย $11 \cdot 31 \cdot 61$ ลงตัว

ปัญหา 14 จงหาเศษที่เกิดจากการหาร $1! + 2! + 3! + \dots + 100!$ ด้วย 12

วิธีทำ ถ้า $n! = 4!, 5!, 6!, \dots, 100!$ จะได้ว่า 12 จะหารด้วย $n!$ ลงตัวเสมอ

เนื่องจาก $4! \equiv 0 \pmod{12}$
 $5! \equiv 0 \pmod{12}$
 $6! \equiv 0 \pmod{12}$
 $\vdots$
 $100! \equiv 0 \pmod{12}$
 จะได้ว่า $4! + 5! + \dots + 100! \equiv 0 \pmod{12}$
 และจาก $1! + 2! + 3! \equiv 9 \pmod{12}$
 ดังนั้น $1! + 2! + 3! + 4! + 5! + \dots + 100! \equiv 9 + 0 + 0 + \dots + 0 \pmod{12}$
 สรุปได้ว่า 12 หาร $1! + 2! + 3! + \dots + 100!$ แล้วเหลือเศษ 9 □

ปัญหา 15 จงแสดงว่า ถ้า p และ $p + 2$ เป็นจำนวนเฉพาะคี่แล้ว

$$4[(p-1)! + 1] + p \equiv 0 \pmod{p(p+2)}$$

ปัญหา 16 จงแสดงว่า 97^{104} หารด้วย 105 มีเศษเหลือเป็น 1

วิธีทำ เนื่องจาก $105 = 3 \cdot 5 \cdot 7$ และ $97 \equiv 1 \pmod{3}$

จะได้ว่า $97^{104} \equiv 1 \pmod{3}$

จาก $97 \equiv 2 \pmod{5}$ และ $97^2 \equiv 2^2 \equiv -1 \pmod{5}$

$$\text{จะได้ว่า } 97^{104} = [(97)^{52}]^2 \equiv (-1)^{52} \equiv 1 \pmod{5}$$

$$\text{จาก } 97 \equiv (-1) \pmod{7} \quad \text{จะได้ว่า } (97)^{104} \equiv (-1)^{104} \equiv 1 \pmod{7}$$

$$\text{เนื่องจาก } [3, 5, 7] = 105 \quad \text{ดังนั้น } (97)^{104} \equiv 1 \pmod{105}$$

แสดงว่า 97^{104} หารด้วย 105 มีเศษเหลือเป็น 1 □

ปัญหา 17 จงหาเลขโดดสามหลักสุดท้ายของ F_{73}

วิธีทำ พิจารณาเลขโดดสามหลักสุดท้ายของ $F_{73} = 2^{2^{73}} + 1$

$$\text{เนื่องจาก } 2^{20} \equiv 1 \pmod{25} \quad \text{ดังนั้น } 2^{73} \equiv 2^{60+13} \equiv 2^{13} \pmod{25}$$

$$\text{และ } 2^{73} \equiv 2^{13} \pmod{4} \quad \text{ดังนั้น } 2^{73} \equiv 2^{60+13} \equiv 2^{13} \pmod{100}$$

$$\text{จาก } 2^{13} = 2^3 \cdot 2^{10} = 8(1024) \quad \text{ดังนั้น } 2^{73} \equiv 8(24) \equiv 192 \equiv 92 \pmod{100}$$

$$\text{ดังนั้น จะมีจำนวนเต็ม } g \text{ ที่ทำให้ } 2^{73} = 100g + 92$$

$$\text{จากสมบัติของคอนกรูเอนซ์ จะได้ว่า } 2^{100} \equiv 1 \pmod{125} \text{ และ } 2^{100g+92} \equiv 2^{92} \pmod{125}$$

$$\text{ดังนั้น } 2^{2^{73}} = 2^{100g+92} \equiv 2^{92} \pmod{1000}$$

$$\text{แต่ } 2^{92} \equiv 896 \pmod{1000} \quad \text{และ } 2^{2^{73}} \equiv 896 \pmod{1000}$$

$$\text{ดังนั้นเลขโดดสามหลักสุดท้ายของ } F_{73} = 2^{2^{73}} + 1 \text{ คือ } 896 + 1 = 897$$

ในการคำนวณหาค่า F_{73} นี้ได้มีผู้คิดคำนวณโดยใช้คอมพิวเตอร์คือ St. Germain และ Steen คำนวณออกมาว่า เลขโดด 40 หลักสุดท้ายของ F_{73} คือ

$$8947301518995672165296423935786246864897$$

□

ปัญหา 18 จงหาเลขโดดสามหลักสุดท้ายของ F_{1945}

ปัญหา 19 บทนิยาม ให้ N เป็นจำนวนเต็มบวก เราจะเรียก N ว่าเป็นจำนวนเต็มที่ปราศจากกำลังสอง (*Square free integer*) ก็ต่อเมื่อ $N = p_1 p_2 p_3 \cdots p_k$ โดยที่ p_i เป็นจำนวนเฉพาะที่แตกต่างกัน

เช่น 3, 5, 11, 13, 14, 15, 19 เป็นจำนวนเต็มที่ปราศจากกำลังสอง

จำนวนเต็มที่ปราศจากกำลังสองที่เขียนเรียงต่อเนื่องกันที่มีความยาวเท่ากับ 3 เช่น 5, 6, 7 และ 13, 14, 15

แต่ถ้าเราสนใจการเขียนจำนวนเต็มที่เรียงต่อเนื่องกันโดยไม่มีจำนวนใดเลยเป็นจำนวนเต็มที่ปราศจากกำลังสอง เช่น 8, 9 และ 24, 25 และ 44, 45 ซึ่งเราเคยพบว่าการเขียนจำนวนประกอบที่เรียงต่อเนื่องกันที่มีความยาว n นั้นเราสามารถเขียนได้ เช่น 24, 25, 26, 27, 28 และ 32, 33, 34, 35, 36 ซึ่งมีความยาว 4 และ $101! + 2, 101! + 3, 101! + 4, \dots, 101! + 101$ ซึ่งมีความยาว 100

จงหาความยาวที่มากที่สุดของจำนวนเต็มที่เขียนเรียงต่อเนื่องกันโดยไม่มีจำนวนใดเลยเป็นจำนวนเต็มที่ปราศจากกำลังสอง

ปัญหา 20 $10^{5^{10^{10}}} + 5^{10^{5^{10^5}}}$ หารด้วย 11 ลงตัวหรือไม่

วิธีทำ เนื่องจาก $(5, 11) = 1$ และ 11 เป็นจำนวนเฉพาะ โดยทฤษฎีบทของแฟร์มาต์

จะได้ว่า $5^{10} \equiv 1 \pmod{11}$

พิจารณา $10 \equiv -1 \pmod{11}$ จะได้ว่า $10^n \equiv (-1)^n \pmod{11}$

เมื่อ n เป็นจำนวนเต็มบวกก็ เราจะได้ $10^n \equiv -1 \pmod{11}$

เราพบว่า 5^m เป็นเลขคี่เสมอ เมื่อ m เป็นจำนวนเต็มบวกใด ๆ

เพราะฉะนั้น $10^{5^{10^{10}}} \equiv -1 \pmod{11}$

พิจารณาค่าของ $10^{5^{10^{10}}}$ จะอยู่ในรูปผลคูณของ 10 เสมอ

จะได้ว่า $10^{5^{10^{10}}} = 10^k$ สำหรับจำนวนเต็มบวก k บางจำนวน

จาก $5^{10} \equiv 1 \pmod{11}$ จะได้ว่า $(5^{10})^k \equiv 1^k \pmod{11}$

นั่นคือ $5^{10k} \equiv 1 \pmod{11}$ ฉะนั้น $5^{10^{5^{10^5}}} \equiv 1 \pmod{11}$

ดังนั้นเราจึงได้ $10^{5^{10^{10}}} + 5^{10^{5^{10^5}}} \equiv (-1) + 1 \pmod{11}$

เพราะฉะนั้น 11 หาร $10^{5^{10^{10}}} + 5^{10^{5^{10^5}}}$ ลงตัว

□

แบบฝึกหัดเรื่อง คอนกรูเอนซ์

1. จงพิสูจน์ว่า ถ้า k เป็นจำนวนเต็มใด ๆ แล้ว $k^2 + k \equiv 0 \pmod{2}$
2. จงพิสูจน์ว่า ถ้า k เป็นจำนวนเต็มใด ๆ แล้ว $k^2 \equiv 1 \pmod{8}$
3. จงพิสูจน์ว่า ถ้า p เป็นจำนวนเฉพาะที่มากกว่า 3 แล้ว $p^2 \equiv 1 \pmod{24}$
(ข้อเสนอแนะ $3 \mid (p-1)$ หรือ $3 \mid (p+1)$)
4. จงหาเศษที่เกิดจากการหาร $1^5 + 2^5 + 3^5 + \dots + 99^5 + 100^5$ ด้วย 4
5. จงแสดงว่า $39 \mid (53^{103} + 103^{53})$ และ $7 \mid (111^{333} + 333^{111})$
6. สำหรับจำนวนเต็มบวก n จงแสดงว่า $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$
(ข้อเสนอแนะ $(-13)^2 \equiv -13 + 1 \pmod{181}$ และใช้หลักอุปนัยเชิงคณิตศาสตร์)
7. สำหรับจำนวนเฉพาะ $p > 3$ จงพิสูจน์ว่า 13 หาร $10^{2p} - 10^p + 1$ ลงตัว
(ข้อเสนอแนะ $10^6 \equiv 1 \pmod{13}$)
8. จงหาเลขโดดสองหลักสุดท้ายของ 9^{9^9}
(ข้อเสนอแนะ $9^9 \equiv 9 \pmod{10}$ ดังนั้น $9^{9^9} = 9^{9+10k}$
เราใช้ความจริงที่ว่า $9^9 \equiv 89 \pmod{100}$)
9. จงหาเศษที่เกิดจากการหาร 4444^{4444} ด้วย 9
(ข้อเสนอแนะ $2^3 \equiv -1 \pmod{9}$)
10. จงหาเลขโดดสามหลักสุดท้ายของ 7^{999}
(ข้อเสนอแนะ $7^{4n} \equiv (1 + 2400)^n \equiv 1 + 2400n \pmod{1000}$)
11. จงแสดงว่า $n^{6k} - 1$ หารด้วย 7 ลงตัว ถ้า $(n, 7) = 1$ และ $k \in \mathbb{N}$
12. จงพิสูจน์ว่า ถ้า p เป็นจำนวนเฉพาะและ $a^2 \equiv b^2 \pmod{p}$ แล้ว $p \mid (a+b)$ หรือ $p \mid (a-b)$
13. จงพิสูจน์ว่า จำนวนเต็ม $m > 1$ เป็นจำนวนเฉพาะ ก็ต่อเมื่อ m เป็นตัวหารของ $(m-1)! + 1$
14. ถ้า p เป็นจำนวนเฉพาะซึ่ง $p > 2$ จงพิสูจน์ว่า
$$1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$
15. จงพิสูจน์ว่า ถ้า p เป็นจำนวนเฉพาะ แล้ว $(a+b)^p \equiv a^p + b^p \pmod{p}$
16. จงหาคำตอบของสมการในแต่ละข้อต่อไปนี้
 - (16.1) $15x \equiv 25 \pmod{35}$
 - (16.2) $15x \equiv 24 \pmod{35}$
 - (16.3) $15x \equiv 0 \pmod{35}$

17. จงหาจำนวนเต็มบวก x_0 ที่น้อยที่สุดซึ่ง $x_0 > 1$ ที่สอดคล้องกับระบบสมการ

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{7} \end{aligned}$$
18. จงแสดงว่า ถ้า a เป็นจำนวนเต็มคู่ แล้ว $a^2 \equiv 0 \pmod{4}$ และถ้า a เป็นจำนวนเต็มคี่ แล้ว $a^2 \equiv 1 \pmod{4}$
19. จงพิจารณาว่า มีจำนวนเต็มบวก n หรือไม่ที่ทำให้

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod{n}$$
20. จงหาเศษที่เกิดจากการหาร 10^{49} ด้วย 7
(ข้อเสนอแนะ $10^6 \equiv 1 \pmod{7}$)
21. จงแสดงว่า

$$\begin{aligned} (21.1) \quad &7 \mid (9^{50} - 4) \\ (21.2) \quad &13 \mid (5^{36} - 1) \\ (21.3) \quad &19 \mid (17^{75} + 8) \end{aligned}$$
22. จงยกตัวอย่างที่แสดงว่า $a^2 \equiv b^2 \pmod{n}$ แต่ $a \not\equiv b \pmod{n}$
23. จงหาจำนวนเต็ม x ทั้งหมดซึ่ง $1 \leq x \leq 100$ และ $x \equiv 7 \pmod{17}$
24. จงหาจำนวนเต็มบวก x ที่น้อยที่สุดที่ทำให้ $13 \mid (x^2 + 1)$
25. จงหาคำตอบทั้งหมดของสมการ $3x \equiv 5 \pmod{11}$
26. จงแสดงว่า $n^{13} - n$ หารด้วย 2, 3, 4, 5, 7 และ 13 ลงตัว สำหรับจำนวนเต็ม n ใด ๆ
27. จงแสดงว่า ถ้า $(a, 13) = (n, 13) = 1$ แล้ว $n^{12} - a^{12}$ หารด้วย 13 ลงตัว
28. จงแสดงว่า ถ้า $(a, 91) = (n, 91) = 1$ แล้ว $n^{12} - a^{12}$ หารด้วย 91 ลงตัว
29. จงแสดงว่า ถ้า $(n, 7) = 1$ แล้ว $n^{12} - 1$ หารด้วย 7 ลงตัว
30. จงหา a และ m ที่ทำให้สมการ $x \equiv a \pmod{m}$ แทนระบบสมการ

$$x \equiv 1 \pmod{4} \quad \text{และ} \quad x \equiv 2 \pmod{3}$$
31. จงหาคำตอบทั้งหมดของสมการต่อไปนี้

$$\begin{aligned} (31.1) \quad &20x \equiv 4 \pmod{30} \\ (31.2) \quad &20x \equiv 30 \pmod{4} \\ (31.3) \quad &355x \equiv 254 \pmod{400} \end{aligned}$$
32. จงหาจำนวนเต็มทั้งหมดที่สอดคล้องกับระบบสมการ

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

33. จงหาคำตอบของระบบสมการต่อไปนี้

$$x \equiv 1 \pmod{4}$$

$$x \equiv 0 \pmod{3}$$

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

34. จงหาจำนวนเต็มทั้งหมดที่หารด้วย 3, 4, 5 เหลือเศษ 1, 2, 3 ตามลำดับ

บทที่ 7

สมการไดโอแฟนไทน์

7.1 บทนำ

สมการไดโอแฟนไทน์ ชื่อนี้ตั้งขึ้นเพื่อเป็นเกียรติแก่นักคณิตศาสตร์ชาวกรีก ชื่อ ดีโอฟานโตส (Diophantos) หรือที่เรียกว่า ดีโอฟานโตส แห่งอะเล็กซานเดรีย (Diophantos of Alexandria ประมาณ ค.ศ. 250) เนื่องจากเขาเกิดและอาศัยอยู่ในเมือง Alexandria และเชื่อกันว่าเขามีชีวิตอยู่ในช่วงปี ค.ศ. 250 ถึง ค.ศ. 300 (โดยประมาณ) เป็นที่น่าเสียดายว่าไม่ค่อยมีใครทราบชีวประวัติของดีโอฟานโตสมากนักนอกจากผลงานที่เขาได้สร้างขึ้น และในผลงานของเขาที่ประกอบด้วยหนังสือชื่อ “เลขคณิต” (Arithmetica) 13 เล่มที่เขียนด้วยภาษากรีก เขาได้แสดงความเป็นอัจฉริยะในการสร้างสรรค์ผลงานทางคณิตศาสตร์ จุดเด่นในงานเขียนของเขาที่ได้รับการยกย่องก็คือ การหาคำตอบของสมการที่มีตัวไม่ทราบค่า (unknowns) และคำตอบที่เขาสนใจก็คือคำตอบที่เป็นจำนวนตรรกยะเท่านั้น

ดีโอฟานโตสได้รับการยกย่องว่าเป็น “บิดาของพีชคณิต” ผลงานเขียนที่มีชื่อเสียงมากคือหนังสือเลขคณิต ซึ่งมีทั้งหมด 13 เล่มนั่นเอง แต่มีเหลือไว้ให้ศึกษาเพียง 6 เล่มประกอบด้วยการแก้ปัญหามากกว่า 130 ปัญหา เพื่อเป็นเกียรติแก่ดีโอฟานโตส เรียกปัญหาในหนังสือเลขคณิตว่า ปัญหาของดีโอฟานโตส

ต่อมานักคณิตศาสตร์เห็นความสำคัญของการศึกษาสมการของดีโอฟานโตส ทั้งเห็นการประยุกต์และได้นำผล การศึกษานี้ไปใช้ตอบปัญหาต่าง ๆ เพื่อการพัฒนาทางด้านคณิตศาสตร์และคณิตศาสตร์ประยุกต์ และมักสนใจคำตอบในระบบจำนวนเต็มเท่านั้น อย่างไรก็ตาม สมการบางสมการแม้ว่าจะเกี่ยวข้องกับระบบจำนวนเต็มเท่านั้น แต่การหาคำตอบหรือการแสดงว่าไม่มีคำตอบอาจจะต้องใช้ความรู้จากระบบจำนวนเต็ม เช่น การแสดงว่าสมการ $x^3 + y^3 = z^3$ ไม่มีคำตอบ (x_0, y_0, z_0) ซึ่ง $x_0, y_0, z_0 \in \mathbb{N}$ เราจะต้องใช้ความรู้เกี่ยวกับระบบจำนวนเชิงซ้อน

แฟร์มาต์ เคยเขียนไว้ว่าเขาพบวิธีการที่จะพิสูจน์ว่า สมการ $x^n + y^n = z^n$ ไม่มีคำตอบ (x_0, y_0, z_0) , $x_0, y_0, z_0 \in \mathbb{N}$ เมื่อ $n \geq 3$ แต่แฟร์มาต์ไม่ได้เขียนการพิสูจน์ไว้ นักคณิตศาสตร์รุ่นหลังได้พยายามหาวิธีการพิสูจน์ ข้อความที่แฟร์มาต์ได้กล่าวไว้จริงหรือไม่ แต่ยังไม่มีความสามารถพิสูจน์ได้จนกระทั่งนักคณิตศาสตร์มีความเชื่อว่าแฟร์มาต์ ก็คงไม่มีบทพิสูจน์อย่างถูกต้อง ดังนั้น คำกล่าวของแฟร์มาต์จึงเป็นข้อคาดเดาเรื่อยมาและรู้จักกันดีในชื่อ “ทฤษฎีบทสุดท้ายของแฟร์มาต์ (Fermat's Last Theorem)” คูมเมอร์ ได้เสนอการพิสูจน์ทฤษฎีบทสุดท้ายของแฟร์มาต์

และตอนหลังพบว่า การพิสูจน์ของเขามีข้อผิดพลาดและเป็นข้อผิดพลาดที่เกิดจากการสมมติโครงสร้างของไอดีล (ideal) ในริงของจำนวนเต็มของฟิลด์ $\mathbb{Q}[\sqrt{m}]$ ซึ่งข้อผิดพลาดนี้ส่งผลให้เกิดคณิตศาสตร์สาขาใหม่ คือ **ทฤษฎีจำนวนเชิงพีชคณิต** (Algebraic Number Theory) และทำให้เขาได้รับการยกย่องว่าเป็นบิดาของสาขาวิชานี้

จนกระทั่งในปี ค.ศ. 1988 มีนักคณิตศาสตร์ชาวญี่ปุ่น ที่ทำงานอยู่ในเยอรมันได้เสนอการพิสูจน์ทฤษฎีบทสุดท้ายของแฟร์มาต์ แต่หลังจากนั้น 1 เดือน ก็มีผู้ค้นพบข้อผิดพลาดของการพิสูจน์ของเขา ดังนั้นทฤษฎีบทสุดท้ายของแฟร์มาต์ยังคงเป็นข้อคาดเดาเรื่อยมา จนในปี ค.ศ. 1993 แอนดรู ไวลด์ (Andrew Wiles ค.ศ. 1952 -) ได้พิสูจน์ทฤษฎีบทสุดท้ายของแฟร์มาต์ได้สำเร็จโดยใช้เวลาในการพิสูจน์ประมาณ 10 ปี และได้เสนอบทพิสูจน์ซึ่งมีความยาวกว่า 200 หน้า ซึ่งใช้ความรู้ที่ลึกซึ้งและมีความซับซ้อนมาก อย่างไรก็ตามบทพิสูจน์ของไวลด์ยังมีข้อบกพร่องอยู่บางประการ ดังนั้น เขาและเทย์เลอร์ จึงปรับปรุงแก้ไขเพื่อให้บทพิสูจน์ของเขาสมบูรณ์ยิ่งขึ้นและงานของเขาก็สำเร็จลุล่วงไปได้ในปี ค.ศ. 1994 นั่นคือข้อคาดเดาที่ใช้เวลากว่า 300 ปีในการคิดค้นหาบทพิสูจน์จนสำเร็จ

ในปัจจุบันเมื่อก้าวถึงสมการของดีโอแฟนโตสจะหมายถึงว่าเราสนใจคำตอบที่เป็นจำนวนเต็มเท่านั้นและเรียกสมการที่เราสนใจคำตอบที่เป็นจำนวนเต็มว่า **สมการไดโอแฟนไทน์** (Diophantine equations) ซึ่งอาจเป็นสมการดีกรีหนึ่ง หรือดีกรีที่มากกว่าหนึ่ง อาจมีตัวแปรหนึ่งตัวหรือหลายตัวหรืออาจเป็นระบบสมการที่กำหนดตัวแปรมากกว่าจำนวนของสมการ เช่น

$$6x + 8y = 46, \quad x^2 + y^2 = z^2, \quad 10x^2 - 7y^2 = 17, \quad x(y+1)^2 = 243y \quad \text{ เป็นต้น}$$

สมการ $ax + by = c$ และ $x^n + y^n = z^n$ คือตัวอย่างของสมการไดโอแฟนไทน์ อย่างไรก็ตาม ในการหาคำตอบที่เป็นจำนวนเต็มของสมการ เราจะไม่ค่อยพบทฤษฎีบททั่ว ๆ ไปที่สามารถประยุกต์ใช้ได้กับสมการหลายๆประเภท แต่เรามักจะพบเทคนิคเฉพาะที่ใช้ในการแก้สมการในแต่ละรูปแบบเท่านั้น

7.2 สมการเชิงเส้นดีกรีหนึ่ง

ในหัวข้อนี้เราจะหาเงื่อนไขที่จำเป็นและเพียงพอ เพื่อแสดงว่า สมการ $ax + by = c$ โดยที่ $a, b, c \in \mathbb{Z}$ มีคำตอบในระบบจำนวนเต็ม

ถ้า $a = 0$ หรือ $b = 0$ แล้วคำตอบของสมการ $ax + by = c$ หาได้ง่าย ดังนั้น เราอาจสมมติว่า $a \neq 0$ และ $b \neq 0$ เราสามารถสรุปวิธีการหาคำตอบของสมการได้ ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 7.2.1 สมการ $ax + by = c$ มีคำตอบ $x, y \in \mathbb{Z}$ ก็ต่อเมื่อ $(a, b) \mid c$

บทพิสูจน์ ให้ $d = (a, b)$

($\Rightarrow$) สมมติว่าสมการ $ax + by = c$ มีคำตอบและให้ $x_0, y_0 \in \mathbb{Z}$ เป็นคำตอบของสมการ

ดังนั้น $ax_0 + by_0 = c$ จากสมบัติของ d เราพบว่า $d \mid a$ และ $d \mid b$

ดังนั้น $d \mid (ax_0 + by_0)$ นั่นคือ $d \mid c$

($\Leftarrow$) สมมติว่า $d \mid c$ และจาก $d = (a, b)$ ดังนั้นจะมี $x_1, y_1 \in \mathbb{Z}$ ซึ่ง $ax_1 + by_1 = d$

แต่ $d \mid c$ ดังนั้นจะมี $k \in \mathbb{Z}$ ซึ่ง $c = dk$

นั่นคือ $a(ka_1) + b(ky_1) = dk = c$

ดังนั้น สมการ $ax + by = c$ มีคำตอบ

ทฤษฎีบท 7.2.2 ถ้าสมการ $ax + by = c$ มีคำตอบ $x = x_0, y = y_0$ และ $d = (a, b)$ แล้ว
ทุก ๆ คำตอบของสมการ $ax + by = c$ สามารถเขียนได้ในรูป

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

เมื่อ $t \in \mathbb{Z}$

บทพิสูจน์ ให้ $t \in \mathbb{Z}$ และ x_0, y_0 เป็นคำตอบของสมการ $ax + by = c$

(1) จะพิสูจน์ว่า $x = x_0 + \frac{b}{d}t$ และ $y = y_0 - \frac{a}{d}t$ เป็นคำตอบของสมการเมื่อ $t \in \mathbb{Z}$

เนื่องจาก $ax_0 + by_0 = c$ และให้ $x = x_0 + \frac{b}{d}t$ และ $y = y_0 - \frac{a}{d}t$

$$\begin{aligned} \text{เราพบว่า} \quad ax + by &= a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) \\ &= ax_0 + by_0 + \frac{ab}{d}t - \frac{ab}{d}t \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

ดังนั้น $x = x_0 + \frac{b}{d}t$ และ $y = y_0 - \frac{a}{d}t$ เป็นคำตอบของสมการ $ax + by = c$

(2) ต่อไปจะพิสูจน์ว่า ทุกคำตอบของสมการจะสามารถเขียนในรูป

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

ให้ x', y' เป็นคำตอบใด ๆ ของสมการและ x_0, y_0 เป็นคำตอบหนึ่งของสมการ

จะได้ว่า $ax' + by' = c = ax_0 + by_0$

ดังนั้น $a(x' - x_0) = b(y_0 - y')$

เนื่องจาก $d = (a, b)$ จะได้ว่า $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ ให้ $r = \frac{a}{d}$ และ $s = \frac{b}{d}$

ดังนั้น $rd(x' - x_0) = sd(y_0 - y')$ แสดงว่า $r \mid s(y_0 - y')$

แต่ $(r, s) = 1$ จะได้ $r \mid (y_0 - y')$ นั่นคือ จะมี $t \in \mathbb{Z}$ ซึ่ง $y_0 - y' = rt$

แทนค่า $y_0 - y' = rt$ ในสมการ $a(x' - x_0) = b(y_0 - y')$

จะได้ว่า $r(x' - x_0) = st$ เพราะฉะนั้น $x' - x_0 = st$

ดังนั้น $x_0 = x' + st$

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

เมื่อ t เป็นจำนวนเต็ม

หมายเหตุ เรียกคำตอบ x_0 และ y_0 ของสมการ $ax + by = c$ ว่า คำตอบเฉพาะราย (particular solution)

บทแทรก 7.2.3 ถ้า $(a, b) = 1$ และ x_0, y_0 เป็นคำตอบของสมการ $ax + by = c$ แล้ว
ทุก ๆ คำตอบของสมการสามารถเขียนได้ในรูป

$$x = x_0 + bt, \quad y = y_0 - at \quad \text{เมื่อ } t \in \mathbb{Z}$$

สรุปการหาคำตอบของสมการ $ax + by = c$

1. หา $d = (a, b)$
2. ตรวจสอบว่า $d \mid c$ หรือ $d \nmid c$
3. ถ้า $d \nmid c$ แล้วสมการ $ax + by = c$ ไม่มีคำตอบในระบบจำนวนเต็ม
4. ถ้า $d \mid c$ เราเขียน $d = ax_1 + by_1$ โดยการใช้ขั้นตอนวิธีแบบยุคลิด
5. จากการเขียน $c = kd$ สำหรับบาง $k \in \mathbb{Z}$ เราเลือก $x_0 = kx_1$ และ $y_0 = ky_1$
6. สร้างคำตอบทั้งหมด $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ เมื่อ $t \in \mathbb{Z}$

ตัวอย่าง 1 ตรวจสอบว่าสมการไดโอแฟนไทน์ $4x + 2y = 11$ มีคำตอบหรือไม่

วิธีทำ พิจารณาสมการ $4x + 2y = 11$ จะมีคำตอบ ก็ต่อเมื่อ $(4, 2) \mid 11$

เนื่องจาก $(4, 2) = 2$ และ $2 \nmid 11$

ดังนั้น สมการ $4x + 2y = 11$ ไม่มีคำตอบ □

ตัวอย่าง 2 (2.1) สมการไดโอแฟนไทน์ $2x + 6y = 8$ มีคำตอบ เพราะว่า $(2, 6) = 2$ และ $2 \mid 8$

(2.2) สมการไดโอแฟนไทน์ $6x + 21y = 4$ ไม่มีคำตอบ

เพราะว่า $(6, 21) = 3$ และ $3 \nmid 4$ □

ตัวอย่าง 3 จงหาคำตอบของสมการไดโอแฟนไทน์ $2x + 6y = 8$

วิธีทำ จากตัวอย่าง (2.1) จะได้ว่าสมการ $2x + 6y = 8$ มีคำตอบ

โดยการแทนค่าจะพบว่า $x_0 = 1$ และ $y_0 = 1$ เป็นคำตอบ

ในที่นี้ $a = 2$ และ $b = 6$ จะได้ว่า $d = (a, b) = (2, 6) = 2$

ดังนั้นคำตอบทั้งหมดของสมการคือ

$$x = 1 + \frac{6}{2}t = 1 + 3t$$

$$y = 1 - \frac{2}{2}t = 1 - t$$

เมื่อ t เป็นจำนวนเต็มใด ๆ □

โดยทฤษฎีบท 7.2.2 ถ้าเราสามารถหาคำตอบเฉพาะราย x_0, y_0 ของสมการไดโอแฟนไทน์ $ax + by = c$ แล้วเราสามารถหาคำตอบทั้งหมดได้ ดังนั้น ปัญหาการหาคำตอบของสมการเหลือเพียงการหาคำตอบเฉพาะราย

การหาคำตอบเฉพาะราย

การหาคำตอบเฉพาะรายของสมการไดโอแฟนไทน์ $ax + by = c$ สามารถหาได้จากวิธีการหาคำตอบของสมการคอนกรูเอนซ์ ทั้งนี้เพราะ

$$\begin{array}{lll} \text{จากสมการไดโอแฟนไทน์} & ax + by = c \\ \text{จะพบว่า} & ax - c = -by & \text{หรือ} & by - c = -ax \\ \text{จะได้ว่า} & b \mid (ax - c) & \text{หรือ} & a \mid (by - c) \\ \text{นั่นคือ} & ax \equiv c \pmod{b} & \text{หรือ} & by \equiv c \pmod{a} \end{array}$$

ตัวอย่าง 4 จงหาคำตอบเฉพาะรายของสมการไดโอแฟนไทน์ $56x + 72y = 40$

วิธีทำ เราจะหาคำตอบโดยใช้สมการคอนกรูเอนซ์

มีสมการคอนกรูเอนซ์ 2 สมการที่ได้จากสมการ $56x + 72y = 40$ คือ

$$56x \equiv 40 \pmod{72} \quad \text{และ} \quad 72y \equiv 40 \pmod{56}$$

$$\text{เลือกใช้} \quad 72y \equiv 40 \pmod{56} \quad \text{จะได้ว่า} \quad \frac{72}{8}y \equiv \frac{40}{8} \pmod{\frac{56}{8}}$$

$$\text{นั่นคือ} \quad 9y \equiv 5 \pmod{7}$$

โดยการแทนค่า y ด้วย 0, 1, 2, 3, 4, 5, 6

พบว่า 6 เป็นคำตอบหนึ่งของสมการ $9y \equiv 5 \pmod{7}$

แทนค่า $y = 6$ ในสมการไดโอแฟนไทน์ $56x + 72y = 40$ จะได้ $x = -7$

ดังนั้น $x_0 = -7$, $y_0 = 6$ เป็นคำตอบหนึ่งของสมการไดโอแฟนไทน์ $56x + 72y = 40$ □

หมายเหตุ 1. ถ้า d เป็นตัวประกอบร่วม m , r และ s จะได้ว่า

$$m \equiv r \pmod{s} \quad \text{ก็ต่อเมื่อ} \quad \frac{m}{d} \equiv \frac{r}{s} \pmod{\frac{s}{d}}$$

2. ในการหาคำตอบเฉพาะราย x_0 , y_0 ของสมการไดโอแฟนไทน์ $ax + by = c$ นั้น

สามารถหาได้จากวิธีการที่ใช้ในการพิสูจน์ทฤษฎีบท 7.2.2 ได้ กล่าวคือ

ใช้ขั้นตอนวิธีแบบยุคลิด ในการหา ห.ร.ม. ได้

ให้ x_1 และ y_1 ซึ่ง $ax_1 + by_1 = (a, b)$

แล้วหาจำนวนเต็ม k ที่คูณ (a, b) แล้วเท่ากับ c มาคูณตลอดสมการนี้
สมมติให้เป็น k จะได้

$$kax_1 + kby_1 = k(a, b)$$

$$a(kx_1) + b(ky_1) = c$$

จะได้ $x_0 = kx_1$, $y_0 = ky_1$ ซึ่งเป็นคำตอบหนึ่งของสมการ

จากตัวอย่าง 4 ใช้ขั้นตอนวิธีแบบยุคลิด หา ห.ร.ม. ของ a และ b (คือ 56 และ 72)

$$72 = 1(56) + 16 \quad \dots\dots\dots(1)$$

$$56 = 3(16) + 8 \quad \dots\dots\dots(2).$$

$$16 = 2(8)$$

ดังนั้น $(56, 72) = 8$

จากนั้นเขียน 8 ในรูป $56m + 72n$ โดยการย้อนกลับดังนี้ จาก (2) จะได้ว่า

$$\begin{aligned} 8 &= 56 - 3(16) \\ &= 56 - 3[72 - 1(56)] \quad (\text{จาก (1) แทนค่า } 16 = 72 - 1(56)) \end{aligned}$$

นั่นคือ $8 = 4(56) - 3(72)$

คูณด้วย 5 จะได้

$$40 = 20(56) - 15(72) = 56(20) + 72(-5)$$

ดังนั้น $x_0 = 20, y_0 = -15$ เป็นคำตอบของสมการไดโอแฟนไทน์ $56x + 72y = 40$

ตัวอย่าง 5 จงหาคำตอบของสมการไดโอแฟนไทน์ $172x + 20y = 1000$

วิธีทำ ใช้ขั้นตอนวิธีแบบยุคลิด หา ห.ร.ม. ของ 172 และ 20 ดังนี้

$$172 = 8(20) + 12$$

$$20 = 1(12) + 8$$

$$12 = 1(8) + 4$$

$$8 = 2(4)$$

เพราะว่า $(172, 20) = 4$ และ $4 \mid 1000$ ดังนั้นสมการนี้มีคำตอบ

ต่อไปจะเขียน 4 ในรูป $172m + 20n$ โดยการย้อนกลับจากขั้นตอนวิธีแบบยุคลิด ดังนี้

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2(12) - 20 \\ &= 2(172 - 8(20)) - 20 \end{aligned}$$

ดังนั้น $4 = 2(172) + (-17)(20)$

คูณด้วย 250 จะได้ $1000 = 500(172) + (-4250)(20)$

จะได้ $x_0 = 500$ และ $y_0 = -4250$ เป็นคำตอบเฉพาะราย

ดังนั้น คำตอบของสมการคือ

$$x = 500 + \frac{20}{4}t = 500 + 5t$$

และ $y = -4250 - \frac{172}{4}t = -4250 - 43t$ เมื่อ $t \in \mathbb{Z}$ □

ตัวอย่าง 6 จงหาคำตอบของสมการไดโอแฟนไทน์ $4x - 83y = -6$

วิธีทำ เพราะ $(4, -83) = 1$ และ $1 \mid (-6)$ ดังนั้น $4x - 83y = -6$ มีคำตอบ

พิจารณาสมการคอนกรูเอนซ์ที่มี y เป็นตัวแปร จะได้

$$83y \equiv 6 \pmod{4}$$

จาก $83y \equiv -y \pmod{4}$ และ $6 \equiv -2 \pmod{4}$

ดังนั้น $-y \equiv -2 \pmod{4}$ นั่นคือ $y \equiv 2 \pmod{4}$

ฉะนั้น $y = 2 + 4t$ เมื่อ $t \in \mathbb{Z}$

แทนค่า y ในสมการไดโอแฟนไทน์ จะได้ $4x - 83(2 + 4t) = -6$

ซึ่งจะได้ $x = 40 + 83t$

ดังนั้น คำตอบของสมการ คือ $x = 40 + 83t, y = 2 + 4t$ เมื่อ $t \in \mathbb{Z}$ □

ปัญหา 7 จงหาจำนวนเต็ม x และ y ทั้งหมดที่เป็นคำตอบของสมการ $999x - 49y = 500$

ปัญหา 8 จงหาจำนวนเต็ม x และ y ทั้งหมดที่เป็นคำตอบของสมการ $247x + 589y = 817$

ปัญหา 9 จงหาจำนวนเต็ม x และ y ทั้งหมดที่เป็นคำตอบของสมการ $101x + 99y = 437$

สมการไดโอแฟนไทน์เชิงเส้นที่มีตัวแปรมากกว่า 2 ตัว จะมีวิธีการหาคำตอบทำนองเดียวกับสมการที่มีตัวแปร 2 ตัว และการพิจารณาว่าสมการนั้น ๆ มีคำตอบหรือไม่ก็อาศัยการพิจารณาว่า ห.ร.ม. ของสัมประสิทธิ์ทั้งหมดหารตัวคงที่ทางขวาของสมการได้ลงตัวหรือไม่

ทฤษฎีบท 7.2.4 ให้ $d = (a_1, a_2, \dots, a_k)$

สมการ $a_1x_1 + a_2x_2 + \dots + a_kx_k = c$ มีคำตอบเป็นจำนวนเต็ม ก็ต่อเมื่อ $d \mid c$

การหาคำตอบที่เป็นจำนวนเต็มของสมการที่มีตัวแปรมากกว่า 2 ตัว

กำหนดสมการไดโอแฟนไทน์ $ax + by + cz = n$ (*)

เป็นสมการที่ต้องการหาคำตอบ ให้ $(a, b, c) = g$ และ $g \mid n$ โดยทฤษฎีบท 7.2.4 เราได้ว่าสมการนี้มีคำตอบ สมมติให้ $(a, b) = d$

เนื่องจาก $g \mid a$ และ $g \mid b$ จะได้ $g \mid (a, b)$ นั่นคือ $g \mid d$

ต่อไปเราจะจัดสมการให้อยู่ในรูป $ax + by = n - cz$ พิจารณาในลักษณะสมการที่มี 2 ตัวแปร ซึ่งมีคำตอบเป็นจำนวนเต็ม เมื่อ $d \mid (n - cz)$ หรือ $n - cz \equiv 0 \pmod{d}$

เราจะได้สมการคอนกรูเอนซ์เชิงเส้น $cz \equiv n \pmod{d}$ (**)

และสมการคอนกรูเอนซ์นี้มีคำตอบเพราะ $((a, b), c) = g$ และ $g \mid n$

สมมติให้ z_1 เป็นคำตอบหนึ่งที่เป็นจำนวนเต็มของสมการ (**) จะได้ว่าคำตอบอื่น ๆ ที่เป็นจำนวนเต็มคือ

$$z = z_1 + \frac{d}{g}t_1 \quad \text{เมื่อ } t_1 \text{ เป็นจำนวนเต็ม}$$

เมื่อแทนค่า z ที่หาได้ในสมการ (*) ทำให้ได้ว่าสมการ (*) ก็จะกลายเป็นสมการไดโอแฟนไทน์ที่มี 2 ตัวแปร แล้วดำเนินการหาคำตอบของสมการที่มี 2 ตัวแปรต่อไปตามวิธีการที่ได้กล่าวมาแล้ว

ตัวอย่าง 10 จงหาคำตอบของสมการไดโอแฟนไทน์ $3x - 6y + 9z = 63$

วิธีทำ สมการ $3x - 6y + 9z = 63$ มีคำตอบ เพราะว่า $(3, -6, 9) = 3$ และ $3 \mid 63$

จัดสมการจะได้ $3x - 6y = 63 - 9z$ (1)

จะเห็นว่า $(3, -6) = 3$ และ $3 \mid (63 - 9z)$ เสมอ สำหรับทุกจำนวนเต็ม z

จึงให้ $z = t_1$ เมื่อ $t_1 \in \mathbb{Z}$

แทนค่า z ใน (1) จะได้ $3x - 6y = 63 - 9t_1$ นั่นคือ $x - 2y = 21 - 3t_1$

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

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

ดังนั้นคำตอบของสมการคือ

$$\left. \begin{array}{l} x = 2t_2 + 21 - 3t_1 \\ y = t_2 \\ z = t_1 \end{array} \right\} \quad \text{เมื่อ } t_1, t_2 \in \mathbb{Z}$$

□

ตัวอย่าง 11 จงหาคำตอบของสมการไดโอแฟนไทน์ $3x - 6y + 2z = 11$

วิธีทำ สมการ $3x - 6y + 2z = 11$ มีคำตอบ เพราะว่า $(3, -6, 2) = 1$ และ $1 \mid 11$

จัดสมการจะได้ $3x - 6y = 11 - 2z$ (1)

จะเห็นว่า $(3, -6) = 3$ ดังนั้นสมการ (1) มีคำตอบก็ต่อเมื่อ $3 \mid (11 - 2z)$

เราจะหา z ที่ทำให้ $3 \mid (11 - 2z)$ โดยเขียนในรูปคอนกรูเอนซ์ ดังนี้

$$2z \equiv 11 \pmod{3}$$

แต่ $2z \equiv -z \pmod{3}$ และ $11 \equiv -1 \pmod{3}$

ดังนั้น $-z \equiv -1 \pmod{3}$ หรือ $z \equiv 1 \pmod{3}$

จะได้ $z = 1 + 3t_1$ เมื่อ $t_1 \in \mathbb{Z}$

แทนค่า z ใน (1) จะได้ $3x - 6y = 11 - 2(1 + 3t_1)$

$$x - 2y = 3 - 2t_1 \quad \text{.....(2)}$$

เนื่องจาก $(1, -2) = 1$ และ $1 \mid (3 - 2t_1)$ เป็นจริงเสมอ

ดังนั้น สมการมีคำตอบจาก (2) ให้ $y = t_2$ เมื่อ $t_2 \in \mathbb{Z}$

จะได้ $x = 3 - 2t_1 + 2t_2$

ดังนั้น คำตอบของสมการคือ

$$\left. \begin{array}{l} x = 3 - 2t_1 + 2t_2 \\ y = t_2 \\ z = 1 + 3t_1 \end{array} \right\} \quad \text{เมื่อ } t_1, t_2 \in \mathbb{Z}$$

□

ในการหาคำตอบของสมการไดโอแฟนไทน์ที่มีตัวแปร 4 ตัวหรือมากกว่า 4 ตัว ก็จะมีวิธีการหาคำตอบเดียวกันกับสมการที่มี 3 ตัวแปร ดังตัวอย่างต่อไปนี้

ตัวอย่าง 12 จงหาคำตอบที่เป็นจำนวนเต็มของสมการ $14x + 6y + 30z + 90w = 200$ มา 3 ชุด

วิธีทำ เนื่องจาก $(14, 6, 30, 9) = 2$ และ $2 \mid 200$ ดังนั้นสมการมีคำตอบเป็นจำนวนเต็ม

เนื่องจาก $14x + 6y + 30z + 90w = 200$ จะได้ว่า $7x + 3y + 15z + 45w = 100$

ดังนั้น $7x + 3y + 15z = 100 - 45w$

จะเห็นว่า $(7, 3, 15) = 1$ และ $1 \mid (100 - 45w)$ เสมอ สำหรับทุกจำนวนเต็ม w

ดังนั้น สมการนี้มีคำตอบ เมื่อ w เป็นจำนวนเต็มใด ๆ ให้ $w = t_3$ เมื่อ $t_3 \in \mathbb{Z}$

เขียนรูปสมการใหม่เป็น $7x + 3y = 100 - 45t_3 - 15z$

เนื่องจาก $(7, 3) = 1$ ทำนองเดียวกับตอนต้น สมการนี้จะมีคำตอบเป็นจำนวนเต็ม

เมื่อ z เป็นจำนวนเต็มใด ๆ ก็ได้ ให้ $z = t_2$ เมื่อ $t_2 \in \mathbb{Z}$

ต่อไปเราจะหาคำตอบของสมการ $7x + 3y = 100 - 45t_3 - 15t_2$ โดยใช้วิธีการหาคำตอบที่เป็นจำนวนเต็มของสมการที่มี 2 ตัวแปร ซึ่งหาได้จาก

$$7x \equiv 100 - 45t_3 - 15t_2 \pmod{3}$$

ให้ $t_2 = 0, t_3 = 0$ จะได้ว่า $x \equiv 1 \pmod{3}$

นั่นคือ $x = 1 + 3t_1$ เมื่อ $t_1 \in \mathbb{Z}$

โดยการแทนค่า x, z, w ในสมการ $14x + 6y + 30z + 90w = 200$

จะได้ว่า $y = \frac{1}{3}(93 - 45t_3 - 15t_2 - 21t_1) = 31 - 15t_3 - 5t_2 - 7t_1$

ตัวอย่างคำตอบที่เป็นไปได้คือ $x = 4, y = 4, z = 1, w = 1$

$$x = 1, y = 11, z = 1, w = 1$$

$$x = 1, y = 6, z = 2, w = 1$$

□

โจทย์ปัญหา 7.2

1. จงหาคำตอบที่อยู่ในระบบจำนวนเต็มทั้งหมดของสมการต่อไปนี้

$$(1.1) \quad 5x + 3y = 52$$

$$(1.2) \quad 15x + 7y = 111$$

$$(1.3) \quad 40x + 63y = 521$$

$$(1.4) \quad 12x + 501y = 1$$

$$(1.5) \quad 12x + 501y = 274$$

$$(1.6) \quad 97x + 98y = 1000$$

$$(1.7) \quad 10x + 16y - 4z = 48$$

$$(1.8) \quad 7x + 8y + 9z = 1$$

$$(1.9) \quad 15x + 12y + 30z = 24$$

$$(1.10) \quad 2x + 3y + 4z = 5$$

2. จงหาจำนวนเต็มบวก m ที่น้อยที่สุดที่ทำให้สมการ $533x + 299y = 1000 + m$ มีคำตอบ

3. จงแสดงว่า สมการ $213x + 441y = 10002$ มีคำตอบในระบบจำนวนเต็ม แต่ไม่มีคำตอบเป็นจำนวนเต็มบวกทั้งคู่

4. จงพิสูจน์ว่า สมการ $ax + by = a + c$ มีคำตอบ ก็ต่อเมื่อ สมการ $ax + by = c$ มีคำตอบ

5. จงพิสูจน์ว่า สมการ $ax + by = c$ มีคำตอบ ก็ต่อเมื่อ $(a, b) = (a, b, c)$

6. ถ้า (x_0, y_0) และ (x_1, y_1) เป็นคำตอบของสมการ $ax + by = c$ ซึ่ง $x_1 = 1 + x_0$

และ $(a, b) = 1$ จงพิสูจน์ว่า $b = \pm 1$

7.3 สมการของพีทาโกรัส

ในหัวข้อนี้เราจะศึกษาวิธีการหาคำตอบที่เป็นจำนวนเต็มบวกทั้งหมดของสมการ

$$x^2 + y^2 = z^2 \quad \dots\dots\dots(1)$$

สมการนี้คือสมการพีทาโกรัสที่มี 3 ตัวแปร หรือกล่าวอีกนัยหนึ่งก็คือ การหาความยาวของด้านทั้งสามของรูปสามเหลี่ยมมุมฉากทุกรูปที่มีความยาวของด้านแต่ละด้านเป็นจำนวนเต็ม ปัญหานี้ได้รับความสนใจจากนักเรขาคณิตตั้งแต่สมัยบาบิโลเนียน พีทาโกรัสได้รับการยกย่องว่าเป็นผู้ทำสูตรที่แสดงความสัมพันธ์ของด้านทั้งสามของสามเหลี่ยมมุมฉาก และในกรณีที่ด้านทั้งสามของสามเหลี่ยมมุมฉากมีความยาวเป็นจำนวนเต็มบวกทั้งสามด้าน พีทาโกรัสสามารถหาสูตรแสดงว่ามีสามเหลี่ยมเป็นจำนวนไม่จำกัดรูปที่แต่ละด้านมีความยาวเป็นจำนวนเต็ม นั่นคือ พีทาโกรัสได้แสดงว่า

$$x = 2n + 1, \quad y = 2n^2 + 2n, \quad z = 2n^2 + 2n + 1 \quad \dots\dots\dots(2)$$

เมื่อ n เป็นจำนวนเต็มบวกใด ๆ เป็นคำตอบของสมการ (1)

สูตรของพีทาโกรัสข้างต้นพบว่า ค่าของ z มากกว่าค่าของ y อยู่ 1 และจาก

$$8^2 + 15^2 = 64 + 225 = 289 = 17^2$$

ดังนั้น (2) ไม่ใช่คำตอบทั้งหมดของสมการ (1) จากประวัติศาสตร์พบว่าคำตอบที่เป็นจำนวนเต็มทั้งหมดของสมการ (1) ปรากฏอยู่ในหนังสืออีลิเมนต์ของยูคลิดซึ่งเขียนในรูปแบบทางเรขาคณิต ซึ่งหลักฐานเกี่ยวกับการหาคำตอบของสมการนี้อยู่ที่ห้องสมุดฟิลิปตัน มหาวิทยาลัยโคลัมเบีย เป็นศิลาจารึกของชาวบาบิโลเนียนซึ่งมีอายุอย่างน้อย 1000 ปีก่อนกลุ่มพีทาโกเรียน

สำหรับรูปแบบทางพีชคณิต คำตอบทั่วไปของสมการ $x^2 + y^2 = z^2$ คือ $x = a^2 - b^2$, $y = 2ab$ และ $z = a^2 + b^2$ โดย a และ b เป็นจำนวนเต็มบวก ถ้าเรากำหนดว่า x, y และ z ไม่มีตัวประกอบร่วม เราต้องการกำหนดเงื่อนไขว่า a และ b ไม่มีตัวประกอบร่วม รวมทั้ง a และ b จะมีลักษณะตรงข้ามกัน คือ ถ้าจำนวนหนึ่งเป็นจำนวนคู่ อีกจำนวนหนึ่งจะเป็นจำนวนคี่ ซึ่งจะกล่าวรายละเอียดในทฤษฎีบทต่อไป

คำตอบที่เป็นจำนวนเต็มบวกของสมการ $x^2 + y^2 = z^2$ เขียนแทนด้วย (x_0, y_0, z_0) กล่าวคือ เราเรียกชุดของจำนวนเต็มบวก (x, y, z) สามจำนวนที่สอดคล้องสมการ $x^2 + y^2 = z^2$ ว่า สามจำนวนของพีทาโกรัส (Pythagorean Triple) เช่น $(3, 4, 5)$, $(4, 3, 5)$, $(6, 8, 10)$, $(5, 12, 13)$, $(360, 319, 481)$, $(4800, 4061, 6649)$, $(6840, 4961, 8161)$, $(12709, 13500, 18541)$ เป็นต้น

ในการพิสูจน์ทฤษฎีบทต่อไปนี้อาจพบสัญลักษณ์ (x, y, z) ที่ใช้แทนทั้งสามจำนวนของพีทาโกรัสและแทนห.ร.ม. ของ x, y, z ซึ่งทั้งสองสิ่งนี้มีความหมายที่แตกต่างกันมาก และหวังว่าผู้อ่านคงจะสามารถแยกแยะและทำความเข้าใจในการใช้สัญลักษณ์ได้

ทฤษฎีบท 7.3.1 ถ้า (x_0, y_0, z_0) เป็นสามจำนวนของพีทาโกรัส และ $c \in \mathbb{N}$ จะได้ว่า (cx_0, cy_0, cz_0) เป็นสามจำนวนของพีทาโกรัส

บทพิสูจน์ เพราะว่า $(cx_0)^2 + (cy_0)^2 = c^2(x_0^2 + y_0^2) = c^2z_0^2 = (cz_0)^2$

ดังนั้น (cx_0, cy_0, cz_0) เป็นสามจำนวนของพีทาโกรัส ■

ทฤษฎีบท 7.3.2 ถ้า (x_0, y_0, z_0) เป็นสามจำนวนของพีทาโกรัส และ $d = (x_0, y_0, z_0)$ จะได้ว่า $(\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d})$ เป็นสามจำนวนของพีทาโกรัส และ $(\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d}) = 1$

บทพิสูจน์ เพราะว่า $(\frac{x_0}{d})^2 + (\frac{y_0}{d})^2 = \frac{x_0^2 + y_0^2}{d^2} = \frac{z_0^2}{d^2} = (\frac{z_0}{d})^2$
 ดังนั้น $(\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d})$ เป็นสามจำนวนของพีทาโกรัส ■

ทฤษฎีบท 7.3.3 ถ้า (x_0, y_0, z_0) เป็นสามจำนวนของพีทาโกรัส และ $(x_0, y_0, z_0) = 1$ จะได้ว่า $(x_0, y_0) = (y_0, z_0) = (z_0, x_0) = 1$

บทพิสูจน์ ให้ p เป็นจำนวนเฉพาะซึ่ง $p \mid (x_0, y_0)$ จะได้ว่า $p \mid (x_0^2 + y_0^2)$
 ดังนั้น $p \mid z_0^2$ จะได้ $p \mid z_0$ แต่ $(x_0, y_0, z_0) = 1$
 ดังนั้น ไม่มีจำนวนเฉพาะตัวใดที่เป็นตัวหารของ (x_0, y_0) นั่นคือ $(x_0, y_0) = 1$
 ในทำนองเดียวกัน เราสามารถพิสูจน์ได้ว่า $(y_0, z_0) = (z_0, x_0) = 1$ ■

บทนิยาม 7.3.4 เราจะเรียกสามจำนวนของพีทาโกรัส (x_0, y_0, z_0) ว่า **พริมีทีฟ (Primitive Pythagorean Triple)** ก็ต่อเมื่อ $(x_0, y_0, z_0) = 1$

จากทฤษฎีบท 7.3.1 และ 7.3.2 พบว่า ในการหาสามจำนวนของพีทาโกรัสทั้งหมดเป็นการเพียงพอที่จะหาเฉพาะพริมีทีฟเท่านั้น

ทฤษฎีบท 7.3.5 ถ้า (x_0, y_0, z_0) เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ จะได้ว่า $x_0 \not\equiv y_0 \pmod{2}$

บทพิสูจน์ จากทฤษฎีบท 7.3.3 เราพบว่า $(x_0, y_0) = (x_0, y_0, z_0) = 1$
 ดังนั้น x_0 และ y_0 จะเป็นจำนวนเต็มคู่พร้อมกันไม่ได้
 ถ้า x_0 และ y_0 เป็นจำนวนเต็มคี่ จะได้ว่า $x_0^2 \equiv 1 \pmod{4}$ และ $y_0^2 \equiv 1 \pmod{4}$
 ดังนั้น $z_0^2 = x_0^2 + y_0^2 \equiv 2 \pmod{4}$ ซึ่งเป็นไปไม่ได้เพราะ z_0 เป็นจำนวนเต็มคู่
 ฉะนั้น $z_0^2 \equiv 0 \pmod{4}$
 นั่นคือ x_0 และ y_0 จะเป็นจำนวนเต็มคี่พร้อมกันไม่ได้ ■

จากทฤษฎีบท 7.3.5 เราอาจสมมติว่า x_0 เป็นจำนวนเต็มคี่ และ y_0 เป็นจำนวนเต็มคู่ และเราจะไม่ถือว่า (x_0, y_0, z_0) และ (y_0, x_0, z_0) เป็นสามจำนวนของพีทาโกรัสที่แตกต่างกัน

จากทฤษฎีบทข้างต้น เราพบว่า ถ้า (x, y, z) เป็นสามจำนวนของพีทาโกรัสแล้ว x หรือ y จะต้องเป็นจำนวนประกอบ นั่นคือเราไม่สามารถหา (x_0, y_0, z_0) ที่เป็นสามจำนวนของพีทาโกรัสที่ x, y, z เป็นจำนวนเฉพาะจากการพิจารณา $(3, 4, 5)$, $(11, 60, 61)$, $(19, 180, 181)$ ต่างก็เป็นสามจำนวนของพีทาโกรัสซึ่ง x และ z ต่างก็เป็นจำนวนเฉพาะ ซึ่งในปัจจุบันยังไม่มีผู้ใดสามารถพิสูจน์ได้ว่าสามจำนวนของพีทาโกรัส (x, y, z) ซึ่ง x, z เป็นจำนวนเฉพาะทั้งคู่อยู่จำกัดชุดหรือไม่จำกัดชุด ประกอบกับ ถ้า (x, y, z) เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ

แล้ว (y, x, z) ก็จะเป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟด้วย เราอาจสมมติว่า y เป็นจำนวนเต็มคู่, x และ z เป็นจำนวนเต็มคี่

ทฤษฎีบท 7.3.6 ให้ (x, y, z) เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ จะได้ว่ามีจำนวนเต็มบวก u, v ซึ่ง $u > v > 0$, $(u, v) = 1$ และ $u \not\equiv v \pmod{2}$ ที่ทำให้

$$x = u^2 - v^2, y = 2uv \text{ และ } z = u^2 + v^2$$

และถ้า u, v เป็นจำนวนเต็มซึ่ง $u > v > 0$, $(u, v) = 1$ และ $u \not\equiv v \pmod{2}$ ที่ทำให้

$$x = u^2 - v^2, y = 2uv \text{ และ } z = u^2 + v^2$$

จะได้ว่า (x, y, z) เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ

บทพิสูจน์ เพราะว่า z และ x เป็นจำนวนเต็มคี่ และ $z > x$ ดังนั้น เราสามารถกำหนด

$$2r = z + x \text{ และ } 2s = z - x$$

จาก $x^2 + y^2 = z^2$ จะได้ $y^2 = z^2 - x^2 = (z+x)(z-x)$

$$\text{ดังนั้น } \left(\frac{y}{2}\right)^2 = \frac{z+x}{2} \cdot \frac{z-x}{2} = rs$$

เราจะแสดงต่อไปว่า $(r, s) = 1$ โดยการสมมติว่า มีจำนวนเฉพาะ p ซึ่ง $p \mid r$ และ $p \mid s$

จะได้ว่า $p \mid y^2$ นั่นคือ $p \mid y$ และจาก $r+s = z$, $r-s = x$

เราพบว่า $p \mid x$ และ $p \mid y$ จึงขัดแย้งกับสมมติฐานที่ว่า $(x, y, z) = 1$ ดังนั้น $(r, s) = 1$

และจาก $rs = \left(\frac{y}{2}\right)^2$ จะได้ว่ามี u, v ซึ่ง $r = u^2$, $s = v^2$ ที่ทำให้

$$x = r - s = u^2 - v^2$$

$$z = r + s = u^2 + v^2$$

$$y^2 = 4rs = 4u^2v^2$$

$$y = 2uv$$

เนื่องจากเราต้องการหาเพียง (x, y, z) เมื่อ x, y, z เป็นจำนวนเต็มบวก

เราจึงพบว่า $x = u^2 - v^2 > 0$ นั่นคือ $u > v > 0$

และจาก $(r, s) = 1 = (u^2, v^2) = (u, v)$ และจากสมมติฐานว่า x เป็นจำนวนเต็มคี่

เราจึงพบว่า $u^2 \not\equiv v^2 \pmod{2}$ นั่นคือ $u \not\equiv v \pmod{2}$

ต่อไปจะแสดงว่า ถ้า u และ v เป็นจำนวนเต็มที่สอดคล้องกับ $u > v > 0$, $(u, v) = 1$

และ $u \not\equiv v \pmod{2}$

จะได้ว่า $(u^2 - v^2, 2uv, u^2 + v^2)$ เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ

$$\text{จาก } (u^2 - v^2)^2 + (2uv)^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2$$

$$= u^4 + 2u^2v^2 + v^4$$

$$= (u^2 + v^2)^2$$

นั่นคือ $(u^2 - v^2, 2uv, u^2 + v^2)$ เป็นสามจำนวนของพีทาโกรัส

ให้ p เป็นจำนวนเฉพาะซึ่ง $p \mid (u^2 - v^2)$, $p \mid 2uv$ และ $p \mid (u^2 + v^2)$

จะได้ว่า $p \mid 2u^2$ และ $p \mid 2v^2$ จาก x เป็นจำนวนเต็มคี่ ดังนั้น $p \neq 2$
 นั่นคือ $p \mid u^2$ และ $p \mid v^2$ แสดงว่า $p \mid u$ และ $p \mid v$ จึงเกิดข้อขัดแย้งที่ว่า $(u, v) = 1$
 เพราะฉะนั้น $(u^2 - v^2, 2uv, u^2 + v^2)$ เป็นสามจำนวนพีทาโกรัสที่เป็นพริมีทีฟ ■

ตัวอย่าง 1 ตารางต่อไปนี้แสดงให้เห็นถึงการหาสามจำนวนของพีทาโกรัส โดยอาศัยผลจากทฤษฎีบท 7.3.6

u	v	$x = u^2 - v^2$	$y = 2uv$	$z = u^2 + v^2$
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
7	2	45	28	53

จากตาราง จะสังเกตได้ว่าสามจำนวนของพีทาโกรัสในแต่ละชุด จะมีอยู่จำนวนหนึ่งที่หารด้วย 3 ลงตัว

วิธีการหาสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ

ให้ A เป็นหนึ่งในสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ เราสามารถหาสามจำนวนของพีทาโกรัสอีกสองจำนวนที่เหลือ ได้ดังนี้

ถ้า A เป็นจำนวนเต็มคี่

- แยกตัวประกอบของ A เป็นผลคูณของสองจำนวน
(ถ้า A เป็นจำนวนเฉพาะ จะได้ตัวประกอบของ A คือ A และ 1)
- เขียนตัวประกอบที่มีค่ามากในรูป $u + v$
เขียนตัวประกอบที่มีค่าน้อยในรูป $u - v$
- แก้สมการจากข้อ 2. เพื่อหาค่า u และ v
- หาค่า x, y, z จาก $x = u^2 - v^2, y = 2uv, z = u^2 + v^2$

ตัวอย่าง 2 ถ้ากำหนดให้ 35 เป็นจำนวนหนึ่งในสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ
จงหาอีกสองจำนวนที่เหลือ

- วิธีทำ
- $35 = 7 \cdot 5$
 - ให้ $u + v = 7$ และ $u - v = 5$
 - โดยการแก้สมการใน 2. จะได้ $u = 6$ และ $v = 1$
 - $x = u^2 - v^2 = 36 - 1 = 35$
 $y = 2uv = 2(6)(1) = 12$

$$z = u^2 + v^2 = 36 + 1 = 37$$

จะได้ว่า $(12, 35, 37)$ เป็นสามจำนวนของพีทาโกรัส □

ถ้า A เป็นจำนวนเต็มคู่

1. ถ้า $4 \nmid A$ แล้วแสดงว่า A ไม่เป็นหนึ่งในสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ
2. ถ้า $4 \mid A$ เราสามารถดำเนินการหาต่อไป ดังนี้
 - 2.1 เขียน A ในรูป $2uv$ โดยที่ $(u, v) = 1$ และมี u หรือ v เป็นจำนวนเต็มคู่ และอีกจำนวนหนึ่งเป็นจำนวนเต็มคี่
 - 2.2 หาค่า x, y, z จาก $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$

ตัวอย่าง 3 ถ้ากำหนดให้ 8 เป็นหนึ่งในสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ จงหาอีก 2 จำนวนที่เหลือ

วิธีทำ 1. $4 \mid 8$

$$2. 8 = 2(4)(1)$$

$$3. x = 4^2 - 1^2 = 15$$

$$y = 2(4)(1) = 8$$

$$z = 4^2 + 1 = 17$$

จะได้ว่า $(8, 5, 17)$ เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ □

จากความจริงที่ว่า ถ้า (x, y, z) เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ แล้ว (y, z, x) ก็จะเป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟด้วย ดังนั้น เราอาจสมมติได้ว่า x เป็นจำนวนเต็มคู่ และ y, z เป็นจำนวนเต็มคี่ได้ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 5 จงหาสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟทั้งหมดที่ $x = 28$

วิธีทำ จาก $x = 2uv = 28$ จะได้ $uv = 14$ ดังนั้น จากทฤษฎีบท 7.3.6 ข้างต้น

จะได้ $u = 14, v = 1$ หรือ $u = 7, v = 2$

แต่ละคู่ของ u, v ข้างต้นจะได้ว่า $(28, 195, 197)$ และ $(28, 45, 53)$ ตามลำดับ □

ตัวอย่าง 6 จงหาสามจำนวนของพีทาโกรัสทั้งหมดที่ $x = 28$

วิธีทำ จากตัวอย่าง 5 ข้างต้นเราพบว่า $(28, 195, 197)$ และ $(28, 45, 53)$ เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟและ $x = 28$ สำหรับสามจำนวนของพีทาโกรัสที่ไม่เป็นพริมีทีฟที่มี $x = 28$ จะอยู่ในรูป

$$(28, y, z) = (ka, kb, kc) \text{ เมื่อ } k > 1 \text{ และ } (a, b, c) \text{ เป็นพริมีทีฟ และ } a \text{ เป็นตัวหารที่เป็นบวกของ } 28$$

นอกจากนั้นเราอาจสมมติว่า a เป็นจำนวนเต็มคู่และ b เป็นจำนวนเต็มคี่

จากตัวหารที่เป็นบวกของ 28 คือ 1, 2, 4, 7, 14, 28

ถ้า $a = 2$ จะได้ว่า $a = 2uv = 2$ นั่นคือ $uv = 1$ ในกรณีนี้เป็นไปไม่ได้

ถ้า $a = 4$ จะได้ว่า $a = 2uv = 4$ นั่นคือ $uv = 2$ ในกรณีนี้จะได้ $u = 2$ และ

$v = 1$ และ $(4, 3, 5)$ เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟและ $(28, 21, 35)$ เป็นสามจำนวนของ

9. จงหาสามจำนวนของพีทาโกรัสที่เรียงกันเป็น

(9.1) ลำดับเลขคณิต

(9.2) ลำดับเรขาคณิต

10. ถ้า n เป็นจำนวนเต็มซึ่ง $n \geq 3$ จงแสดงว่า มีสามจำนวนของพีทาโกรัสที่มี n เป็นหนึ่งในสามจำนวนนั้น

11. ถ้า (a, b, c) เป็นสามจำนวนของพีทาโกรัส และ $g = (a, b, c)$

จงพิสูจน์ว่า $(a, b) = (b, c) = (c, a) = g$

7.4 สมการ $x^4 + y^4 = z^2$ และสมการ $x^4 + y^4 = z^4$

ในหัวข้อนี้เราจะแสดงว่า สมการ $x^4 + y^4 = z^2$ และ $x^4 + y^4 = z^4$ ไม่มีคำตอบที่เป็นจำนวนเต็มบวก

ทฤษฎีบท 7.4.1 สมการ $x^4 + y^4 = z^2$ ไม่มีคำตอบ $x, y, z \in \mathbb{N}$

บทพิสูจน์ ให้ $S = \{c \in \mathbb{N} \mid \text{มี } a, b \in \mathbb{Z} \text{ และ } a^4 + b^4 = c^2\}$ เราจะพิสูจน์ว่า $S = \emptyset$

สมมติว่า $S \neq \emptyset$ เลือก c เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S

นั่นคือมี $a, b \in \mathbb{Z}$ ซึ่ง $a^4 + b^4 = c^2$

ให้ $d = (a, b, c)$ จะได้ว่า $d \mid a$, $d \mid b$ และ $d \mid c$ และ

$$\left(\frac{a}{d}\right)^4 + \left(\frac{b}{d}\right)^4 = \frac{a^4 + b^4}{d^4} = \frac{c^2}{d^4} = \left(\frac{c}{d^2}\right)^2$$

ดังนั้น $\frac{c}{d^2} \in S$ แต่ c เป็นสมาชิกที่มีค่าน้อยที่สุดใน S จะได้ $d = 1$

นอกจากนั้น เราสามารถสรุปได้ว่า (a^2, b^2, c) จะเป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ

ดังนั้นจะมี u, v ซึ่ง $u > v > 0$, $(u, v) = 1$ และ $u \not\equiv v \pmod{2}$ ที่ทำให้

$$a^2 = u^2 - v^2, \quad b^2 = 2uv \quad \text{และ} \quad c = u^2 + v^2$$

จาก $a^2 = u^2 - v^2$ จะได้ว่า $a^2 + v^2 = u^2$ และ $(u, v) = 1$

จะได้ (a, v, u) เป็นสามจำนวนของพีทาโกรัสที่เป็นพริมีทีฟ ดังนั้น จะมี r, s ซึ่ง

$r > s > 0$, $(r, s) = 1$ และ $r \not\equiv s \pmod{2}$ ซึ่ง

$$a = r^2 - s^2, \quad v = 2rs \quad \text{และ} \quad u = r^2 + s^2$$

จาก $b^2 = 2uv$, v เป็นจำนวนเต็มคู่ และ $(u, v) = 1$ จะได้ $\left(\frac{b}{2}\right)^2 = u\left(\frac{v}{2}\right)$

ดังนั้นจะมี $e, f > 0$ ซึ่ง $u = e^2$ และ $\frac{v}{2} = f^2$ และจาก $rs = \frac{v}{2} = f^2$ และ

$(r, s) = 1$ ดังนั้นจะมี $b_1, c_1 > 0$ ซึ่ง $r = b_1^2$ และ $s = c_1^2$

และจาก $u = r^2 + s^2 = (b_1^2)^2 + (c_1^2)^2$

ดังนั้น $e^2 = u = b_1^4 + c_1^4$ และ $0 < e \leq u < u^2 + v^2 = c$

นั่นคือจะมี (b_1^2, c_1^2, e) เป็นคำตอบของสมการ $x^4 + y^4 = z^2$ โดยที่ $e < c$

เกิดข้อขัดแย้งกับการเลือก c ที่มีค่าน้อยที่สุดใน S

เราจึงสรุปได้ว่า สมการ $x^4 + y^4 = z^2$ ไม่มีคำตอบ $x, y, z \in \mathbb{N}$ ■

บทแทรก 7.4.2 สมการ $x^4 + y^4 = z^4$ ไม่มีคำตอบ $x, y, z \in \mathbb{N}$

บทพิสูจน์ ถ้า a, b, c เป็นจำนวนเต็มบวก ซึ่ง $a^4 + b^4 = c^4$ จะได้ว่า (a, b, c^2) จะเป็นคำตอบของ $x^4 + y^4 = z^2$ ซึ่งขัดแย้งกับทฤษฎีบท 7.4.1 ข้างต้น ■

บทแทรก 7.4.3 สมการ $x^n + y^n = z^n$ ไม่มีคำตอบ $x, y, z \in \mathbb{N}$ เมื่อ $n \equiv 0 \pmod{4}$

ทฤษฎีบท 7.4.4 ให้ p เป็นจำนวนเฉพาะซึ่ง $p \mid n$ ถ้าสมการ $x^p + y^p = z^p$ ไม่มีคำตอบที่เป็นจำนวนเต็มบวกแล้ว $x^n + y^n = z^n$ ไม่มีคำตอบที่เป็นจำนวนเต็มบวก

จากทฤษฎีบท 7.4.4 เราพบว่า ทฤษฎีบทสุดท้ายของแฟร์มาต์นั้นอาจแสดงเพียงว่าเมื่อ p เป็นจำนวนเฉพาะซึ่ง $p \geq 3$ แล้ว สมการ $x^p + y^p = z^p$ ไม่มีคำตอบที่เป็นจำนวนเต็มบวก ซึ่งเราได้กล่าวถึงประวัติความเป็นมาของทฤษฎีบทนี้อยู่ในหัวข้อ 7.1 นอกจากนั้น เรายังได้กล่าวถึงผู้ที่กำหนดบทพิสูจน์ที่สมบูรณ์ของทฤษฎีบทสุดท้ายของแฟร์มาต์ ในหัวข้อ 7.1 เช่นกัน สำหรับผู้ที่ต้องการทราบข้อมูลเพิ่มเติมสามารถศึกษาได้ใน website ตามที่อยู่ <http://www.ams.org/new-in-math/fermat.html>

โจทย์ปัญหา 7.4

- จงพิสูจน์ว่า สมการ $x^4 - y^4 = z^2$ ไม่มีคำตอบ $x, y, z \in \mathbb{N}$
- จงพิสูจน์ว่า ไม่มีจำนวนเต็มบวก a, b ที่ทำให้ $a^2 + b^2$ และ $a^2 - b^2$ เป็นจำนวนกำลังสองสมบูรณ์
- จงพิสูจน์ว่า สมการ $x^4 - 4y^4 = z^2$ ไม่มีคำตอบ $x, y, z \in \mathbb{N}$
- จงพิสูจน์ว่า สมการ $x^2 + y^2 = z^3$ มีคำตอบ $x, y, z \in \mathbb{N}$ ไม่จำกัดชุด
(ข้อเสนอแนะ พิจารณา $x = n(n^2 - 3)$ และ $y = 3n^2 - 1$)
- จงพิสูจน์ว่า สมการ $x^4 - y^4 = 2z^2$ ไม่มีคำตอบ $x, y, z \in \mathbb{N}$
(ข้อเสนอแนะ เนื่องจากคำตอบ x, y, z ของสมการ, $x \equiv y \pmod{2}$, $x^2 + y^2 = 2a^2$,
 $x + y = 2b^2$, $x - y = 2c^2$ สำหรับบาง $a, b, c \in \mathbb{N}$ ดังนั้น $a^2 = b^4 + c^4$)
- จงพิสูจน์ว่า ถ้า $x, y, z \in \mathbb{N}$ เป็นคำตอบของสมการ $x^4 + y^4 = 2z^2$ และ $(x, y, z) = 1$
แล้ว $x = y = z = 1$
(ข้อเสนอแนะ พิจารณาสมการ $z^4 - (xy)^4 = \left(\frac{x^4 - y^4}{2}\right)^2$)

7. ให้ $x, y, z \in \mathbb{N}$ เป็นคำตอบของสมการ

$$\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2} \quad \text{และ} \quad (x, y, z) = 1$$

จงพิสูจน์ว่า $x = 2st(s^2 + t^2)$, $y = s^4 - t^4$, $z = 2st(s^2 - t^2)$

โดยที่ $s, t \in \mathbb{N}$, $s > t$, $(s, t) = 1$ และ $s \not\equiv t \pmod{2}$

8. จงพิสูจน์ว่าสมการ $\frac{1}{x^4} + \frac{1}{y^4} = \frac{1}{z^2}$ ไม่มีคำตอบ $x, y, z \in \mathbb{N}$

9. จงพิสูจน์ว่าระบบสมการ

$$x^2 + y^2 = z^2$$

$$x^2 - y^2 = w^2$$

ไม่มีคำตอบ $x, y, z, w \in \mathbb{N}$

7.5 สมการไดโอแฟนไทน์กำลังสอง

ในหัวข้อนี้จะได้กล่าวถึงลักษณะของสมการในรูปแบบอื่นที่แตกต่างจากที่กล่าวมาแล้ว กล่าวคือ คำตอบของแต่ละสมการจะขึ้นอยู่กับข้อกำหนด n และเราต้องการจะหาจำนวนเต็ม n ทั้งหมดที่ทำให้สมการมีคำตอบ

ทฤษฎีบท 7.5.1 สมการ $n = x^2 - y^2$ จะมีคำตอบ $x, y \in \mathbb{Z}$ ก็ต่อเมื่อ n เป็นจำนวนเต็มคี่ หรือ $4 \mid n$

บทพิสูจน์ ($\Leftarrow$) สมมติว่า n เป็นจำนวนเต็มคี่ ดังนั้นจะมี $k \in \mathbb{Z}$ ที่ทำให้ $n = 2k - 1$

$$\text{และจะได้} \quad x^2 - y^2 = (x - y)(x + y) = 2k - 1$$

$$\text{ให้ } x - y = 1 \text{ และ } x + y = 2k - 1 \quad \text{จะได้ } x = k \text{ และ } y = k - 1$$

$$\text{ถ้า } 4 \mid n \text{ จะได้ว่ามี } k \in \mathbb{Z} \text{ ซึ่ง } n = 4k$$

$$\text{ฉะนั้น } x^2 - y^2 = (x - y)(x + y) = n = 4k$$

$$\text{ให้ } x - y = 2 \text{ และ } x + y = 2k \quad \text{จะได้ } x = k + 1 \text{ และ } y = k - 1$$

($\Rightarrow$) สมมติว่า $n = x^2 - y^2$ มีคำตอบ จะได้ว่า ถ้า $x \equiv y \pmod{2}$

$$\text{จะได้ว่า } 2 \mid (x - y) \text{ และ } 2 \mid (x + y)$$

$$\text{ดังนั้น } 4 \mid (x^2 - y^2) \quad \text{นั่นคือ } 4 \mid n$$

$$\text{และถ้า } x \not\equiv y \pmod{2} \quad \text{จะได้ว่า } x^2 - y^2 = n \text{ เป็นจำนวนเต็มคี่}$$

ทฤษฎีบท 7.5.2 ให้ n เป็นจำนวนเต็ม จะได้ว่ามีจำนวนเต็ม x, y, z ที่ทำให้ $n = x^2 + y^2 - z^2$

บทพิสูจน์ ให้ n เป็นจำนวนเต็ม จะได้มีจำนวนเต็ม x ที่ทำให้ $n - x^2$ เป็นจำนวนเต็มคี่

$$\text{ดังนั้นจากทฤษฎีบท 7.5.1 เราพบว่า จะมีจำนวนเต็ม } y, z \text{ ที่ทำให้ } n - x^2 = y^2 - z^2$$

$$\text{นั่นคือ จะมีจำนวนเต็ม } x, y, z \text{ ที่ทำให้ } n = x^2 + y^2 - z^2$$

ต่อไปเราจะแสดงว่าจำนวนเต็มบวก n สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 4 จำนวน

ทฤษฎีบท 7.5.3 (Euler)

$$\begin{aligned} & (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 + (x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3)^2 \\ & \quad + (x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4)^2 + (x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2)^2 \dots\dots\dots (*) \end{aligned}$$

สมการ (*) ข้างต้นถูกค้นพบโดย ออยเลอร์ ซึ่งสามารถแสดงได้โดยการกระจายทั้งสองข้างของสมการ และเราจะเห็นว่า ถ้าจำนวนเต็มบวก m และ n สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 4 จำนวน จะได้ว่า mn ก็สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 4 จำนวนได้

เนื่องจาก $1 = 1^2 + 0^2 + 0^2 + 0^2$ และ $2 = 1^2 + 1^2 + 0^2 + 0^2$ ดังนั้น การที่จะแสดงว่า จำนวนเต็มบวก n ทุกจำนวนสามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 4 จำนวนได้นั้น เป็นการเพียงพอที่จะแสดงเพียงกรณีที่ n เป็นจำนวนเฉพาะที่มากกว่า 2 ซึ่งเราจะแบ่งการพิสูจน์ออกเป็น 2 ทฤษฎีบท ต่อไปนี้

ทฤษฎีบท 7.5.4 ถ้า p เป็นจำนวนเฉพาะ ซึ่ง $p \geq 3$ จะได้ว่ามีจำนวนเต็ม m, x_1, x_2, x_3, x_4 ซึ่ง

$$1 \leq m < p \quad \text{และ} \quad mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

บทพิสูจน์ ให้ $S_1 = \{0^2, 1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2\}$

$$\text{และ } S_2 = \{-0^2 - 1, -1^2 - 1, -2^2 - 1, \dots, -\left(\frac{p-1}{2}\right)^2 - 1\}$$

เพราะว่า ถ้า $x^2 \equiv y^2 \pmod{p}$ แล้ว $p \mid (x - y)$ หรือ $p \mid (x + y)$

ดังนั้น ไม่มีสมาชิก 2 ตัวใดที่ต่างกันใน S_1 (ใน S_2) ที่คอนกรูเอนซ์กันมอดุโล p แต่

$$\text{จำนวนสมาชิกใน } S_1 = \text{จำนวนสมาชิกใน } S_2 = \frac{p-1}{2} + 1$$

ดังนั้น จำนวนสมาชิกของ $S_1 \cup S_2 = p + 1$ แสดงว่าจะมีสมาชิกอย่างน้อย 1 ตัวใน S_1

เรียกว่า x^2 และสมาชิกอย่างน้อยหนึ่งตัวใน S_2 เรียกว่า $-y^2 - 1$, ที่ทำให้ $x^2 \equiv -y^2 - 1 \pmod{p}$

$$\text{นั่นคือ } x^2 + y^2 + 1 \equiv 0 \pmod{p} \quad \text{โดยที่ } 0 \leq x, y \leq \frac{p-1}{2}$$

ดังนั้น $x^2 + y^2 + 1^2 + 0^2 = mp$ และ

$$\begin{aligned} 1 &\leq m = \frac{1}{p}(x^2 + y^2 + 1) \\ &\leq \frac{1}{p}\left(2\left(\frac{p-1}{2}\right)^2 + 1\right) \\ &\leq \frac{1}{p}\left(\frac{p^2}{2} + 1\right) < p \end{aligned}$$

■

ทฤษฎีบท 7.5.5 ถ้า m เป็นจำนวนเต็มบวกที่น้อยที่สุดที่สอดคล้องกับทฤษฎีบท 7.5.4 จะได้ว่า $m = 1$

บทพิสูจน์ จาก ทฤษฎีบท 7.5.4 เราพบว่า มี m อย่างน้อยหนึ่งตัว ซึ่ง $1 \leq m < p$

ที่ทำให้ $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$

สมมติว่า m เป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่งสอดคล้องกับทฤษฎีบท 7.5.4

สมมติว่า m เป็นจำนวนเต็มคู่และ $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$

จะได้ว่า x_1, x_2, x_3, x_4 เป็นจำนวนเต็มคู่ทั้งหมด หรือมี 2 จำนวนที่เป็นจำนวนเต็มคู่ หรือทุกจำนวนเป็นจำนวนเต็มคู่ สำหรับกรณีที่ 1 จำนวนเต็มคู่ 2 จำนวน เราอาจสมมติว่า x_1, x_2 เป็นจำนวนเต็มคู่

ดังนั้นในทุก ๆ กรณีเราพบว่า $x_1 + x_2, x_3 + x_4$ ต่างก็เป็นจำนวนเต็มคู่ และ

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{m}{2}p$$

ดังนั้นเกิดข้อขัดแย้งในการเลือก m จะได้ว่า m เป็นจำนวนเต็มคี่

สมมติว่า m เป็นจำนวนเต็มคี่ และ $3 \leq m < p$

ให้ $S = \{y \mid -\frac{m-1}{2} \leq y \leq \frac{m-1}{2}\}$ เป็นระบบเศษตกค้างบริบูรณ์มอดุโล m

ฉะนั้น สำหรับ x_1, x_2, x_3, x_4 จะมี $y_1, y_2, y_3, y_4 \in S$ ที่ทำให้ $x_i \equiv y_i \pmod{m}$

เราอาจสังเกตได้ว่า y_1, y_2, y_3, y_4 อาจไม่แตกต่างกันทั้งหมด

ดังนั้น $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv y_1^2 + y_2^2 + y_3^2 + y_4^2 \pmod{m}$

และจาก $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$

เราจะได้ $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m}$

นั่นคือ จะมีจำนวนเต็ม n ที่ทำให้

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mn$$

ถ้า $n = 0$ จะได้ว่า $y_1 = y_2 = y_3 = y_4 = 0$ และ

$$x_1 \equiv x_2 \equiv x_3 \equiv x_4 \pmod{m} \quad \text{ซึ่งเป็นไปไม่ได้}$$

เพราะว่า $3 \leq m < p$ ดังนั้น เราจึงสรุปได้ว่า

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mn \quad \text{โดยที่ } mn < 4\left(\frac{m}{2}\right)^2 = m^2$$

นั่นคือ $1 \leq n < m$

$$\begin{aligned} \text{ดังนั้น } m^2 np &= (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= A_1^2 + A_2^2 + A_3^2 + A_4^2 \quad (\text{ทฤษฎีบท 7.5.3}) \end{aligned}$$

และจากการพิจารณาแต่ละ A_i ในทฤษฎีบท 7.5.3 เราพบว่า $A_i \equiv 0 \pmod{m}$

$$\text{ดังนั้น } np = \left(\frac{A_1}{m}\right)^2 + \left(\frac{A_2}{m}\right)^2 + \left(\frac{A_3}{m}\right)^2 + \left(\frac{A_4}{m}\right)^2$$

และ $0 < n < m$ จึงเกิดข้อขัดแย้งกับการเลือก m ดังนั้น m ต้องเป็นจำนวนเต็มคี่ที่น้อยกว่า 3 นั่นคือ $m = 1$ เราจึงสรุปได้ว่าจำนวนเฉพาะ $p \geq 3$ สามารถเขียนได้ในรูป

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

ทฤษฎีบท 7.5.6 จำนวนเต็มบวกที่อยู่ในรูป $8k + 7$ ไม่สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 3 จำนวน

บทพิสูจน์ สมมติว่ามี x_1, x_2, x_3 ซึ่ง $x_1^2 + x_2^2 + x_3^2 = 8k + 7, k \geq 0$ เราอาจสมมติว่า x_1 เป็นจำนวนเต็มคี่ x_2, x_3 เป็นจำนวนเต็มคู่ หรือ x_1, x_2, x_3 เป็นจำนวนเต็มคี่ ถ้า x_1 เป็นจำนวนเต็มคี่ x_2, x_3 เป็นจำนวนเต็มคู่ จะได้ว่ามี $a, b, c \in \mathbb{Z}$ ที่ทำให้

$$x_1 = 2a + 1, x_2 = 2b \text{ และ } x_3 = 2c$$

$$\text{นั่นคือ } (2a + 1)^2 + (2b)^2 + (2c)^2 = 8k + 7$$

$$\text{ดังนั้น } 4a^2 + 4a + 1 + 4b^2 + 4c^2 = 8k + 7 \text{ จะได้ } 6 \equiv 0 \pmod{4} \text{ ซึ่งเป็นไปไม่ได้}$$

$$\text{ถ้า } x_1, x_2, x_3 \text{ เป็นจำนวนเต็มคี่ จะได้ว่ามี } a, b, c \in \mathbb{Z} \text{ ที่ทำให้}$$

$$x_1 = 2a + 1, x_2 = 2b + 1 \text{ และ } x_3 = 2c + 1$$

$$\text{นั่นคือ } (2a + 1)^2 + (2b + 1)^2 + (2c + 1)^2 = 8k + 7$$

$$\text{จะได้ว่า } 4(a^2 + a) + 4(b^2 + b) + 4(c^2 + c) = 8k + 4$$

$$\text{ดังนั้น } a^2 + a + b^2 + b + c^2 + c = 2k + 1$$

$$\text{แต่ } a^2 + a, b^2 + b, c^2 + c \text{ ต่างก็เป็นจำนวนเต็มคู่ จึงเกิดข้อขัดแย้ง}$$

ดังนั้น จำนวนเต็มบวกที่อยู่ในรูป $8k + 7$ ไม่สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 3 จำนวน ■

จากทฤษฎีบท 7.5.6 เราพบว่า มีจำนวนเต็มบางจำนวนที่ไม่สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 3 จำนวน ที่จริงแล้วจำนวนเต็มบวกไม่สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 3 จำนวนได้ คือ จำนวนเต็มที่อยู่ในรูป $4^m(8k + 7)$

ในตอนท้ายของหัวข้อนี้ เราจะหาจำนวนเต็มบวกทั้งหมดที่สามารถเขียนได้ในรูปผลบวกของจำนวนเต็มบวก 2 จำนวน

ทฤษฎีบท 7.5.7 สำหรับจำนวนเต็ม x_1, x_2, y_1, y_2 จะได้

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$$

ทฤษฎีบท 7.5.7 นี้ เป็นเพียงส่วนหนึ่งของทฤษฎีบท 7.5.3

ดังนั้น เราจะพบว่า ถ้า m, n สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 2 จำนวน จะได้ว่า mn สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 2 จำนวนได้

บทนิยาม 7.5.8 เราจะเรียกคำตอบของสมการ $x^2 + y^2 = n$ ว่า **พริมีทีฟ** (primitive) ก็ต่อเมื่อ $(x, y) = 1$

จากบทนิยามเราพบว่า ถ้า n เป็นจำนวนเฉพาะและมี $x, y \in \mathbb{Z}$ ซึ่ง $x^2 + y^2 = n$ จะได้ว่า x และ y จะเป็นคำตอบพหุคูณที่พหุคูณ นอกจากนั้น $1 \leq |x| < n$ และ $1 \leq |y| < n$

จากทฤษฎีบท 7.5.7 การตอบปัญหาที่ว่า จำนวนเต็ม n จำนวนใดบ้างที่สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็มบวก 2 จำนวน เป็นการเพียงพอที่จะตอบเฉพาะเมื่อ n เป็นจำนวนเฉพาะ และเนื่องจาก $1 = 1^2 + 0^2$ และ $2 = 1^2 + 1^2$ ดังนั้น เราจึงพิจารณาแต่จำนวนเฉพาะ n ซึ่ง $n \geq 3$

ทฤษฎีบท 7.5.9 ให้ p เป็นจำนวนเฉพาะและสมการ $p = x^2 + y^2$ มีคำตอบที่เป็นจำนวนเต็มบวก x, y จะได้ว่า สมการ $u^2 \equiv -1 \pmod{p}$ มีคำตอบ

บทพิสูจน์ เพราะว่า $(y, p) = 1$ ดังนั้น จะมีจำนวนเต็ม s ซึ่ง $sy \equiv x \pmod{p}$
ให้ y' เป็นคำตอบของสมการ $yy' \equiv 1 \pmod{p}$ จะได้ $sy y' \equiv s \pmod{p}$
จะได้ว่า $xy' \equiv s \pmod{p}$ ดังนั้น $x^2(y')^2 \equiv s^2 \pmod{p}$
และจาก $p = x^2 + y^2$ จะได้ $-y^2(y')^2 \equiv s^2 \pmod{p}$
ฉะนั้น $s^2 \equiv -(yy')^2 \equiv -1 \pmod{p}$
นั่นคือสมการ $u^2 \equiv -1 \pmod{p}$ มีคำตอบ ■

ทฤษฎีบท 7.5.10 ให้ p เป็นจำนวนเฉพาะและสมการ $u^2 \equiv -1 \pmod{p}$ มีคำตอบ จะได้ว่า มีจำนวนเต็มบวก x, y ซึ่ง $p = x^2 + y^2$

บทพิสูจน์ ให้ s เป็นคำตอบของสมการ $u^2 \equiv -1 \pmod{p}$
และให้ $S = \{u - sv \mid u, v \in \mathbb{Z} \text{ และ } 0 \leq u^2, v^2 < p\}$
เราพบว่า S มีสมาชิกมากกว่า p ตัว ดังนั้นจะมี $u_1 - sv_1, u_2 - sv_2$ ที่แตกต่างกัน
และ $u_1 - sv_1 \equiv u_2 - sv_2 \pmod{p}$ จะได้ว่า $u_1 - u_2 \equiv s(v_1 - v_2) \pmod{p}$
ให้ $u_0 = |u_1 - u_2|$ และ $v_0 = |v_1 - v_2|$
จะได้ว่า $0 \leq u_0^2, v_0^2 < p$ และ $u_0 \neq 0$ หรือ $v_0 \neq 0$
ดังนั้น $1 \leq u_0^2 + v_0^2 < 2p$ และจาก $sv_0 \equiv u_0 \pmod{p}$
เราจึงได้ว่า $u_0^2 + v_0^2 \equiv s^2 v_0^2 + v_0^2 = (s^2 + 1)v_0^2 \equiv 0 \pmod{p}$
เพราะฉะนั้น มี $k \in \mathbb{Z}$ ซึ่ง $u_0^2 + v_0^2 = pk$ แต่ $u_0^2 + v_0^2 < 2p$ ดังนั้น $k = 1$
แสดงว่า $u_0^2 + v_0^2 = p$ ■

จากทฤษฎีบท 7.5.9 และทฤษฎีบท 7.5.10 และรวมกับผลจากทฤษฎีบทที่ผ่านมา จะได้

ทฤษฎีบท 7.5.11 ให้ p เป็นจำนวนเฉพาะ จะได้ว่า มีจำนวนเต็มบวก x, y ที่ทำให้ $p = x^2 + y^2$ ก็ต่อเมื่อ $p = 2$ หรือ $p \equiv 1 \pmod{4}$

ทฤษฎีบท 7.5.12 ให้ $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ แทนการเขียน n ในรูปแบบบัญญัติ จะได้ว่า n สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็ม 2 จำนวนได้ ก็ต่อเมื่อ สำหรับแต่ละ $i \in \{1, 2, \dots, k\}$ ถ้า p_i เป็นจำนวนเฉพาะ ซึ่ง $p_i \equiv 3 \pmod{4}$ แล้ว $a_i \equiv 0 \pmod{2}$

บทพิสูจน์ จาก $2 = 1^2 + 1^2$ และเราทราบจากทฤษฎีบท 7.5.11 ว่า ทุก ๆ $u, v \in \mathbb{Z}$ จะได้ว่า $u^2 + v^2 \equiv 0, 1$ หรือ $2 \pmod{4}$ นั่นคือ ทุก ๆ จำนวนเฉพาะ p ซึ่ง $p \equiv 3 \pmod{4}$ ไม่สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็มสองจำนวนได้ ดังนั้นการพิสูจน์ทฤษฎีบทนี้ จึงเป็นการเพียงพอที่จะพิสูจน์แต่เพียงว่า ทุก ๆ จำนวนเฉพาะ p ซึ่ง $p \equiv 1 \pmod{4}$ สมการ $p = u^2 + v^2$ มีคำตอบ $u, v \in \mathbb{Z}$ จากทฤษฎีบท 2.4.7 เราพบว่าสมการ

$$x^2 + 1 \equiv 0 \pmod{p}$$

มีคำตอบ $x \in \mathbb{Z}$ ก็ต่อเมื่อ $p = 2$ หรือ $p \equiv 1 \pmod{4}$

ให้ p เป็นจำนวนเฉพาะซึ่ง $p \equiv 1 \pmod{4}$ และ x เป็นคำตอบของสมการ

$$x^2 + 1 \equiv 0 \pmod{p} \quad \dots\dots\dots(1)$$

ให้ $S = \{rx + s \mid r, s \in \mathbb{Z}, 0 \leq r < \sqrt{p}, 0 \leq s < \sqrt{p}\}$

เราพบว่าจำนวนสมาชิกใน S มีมากกว่า $\sqrt{p} \cdot \sqrt{p} = p$

ดังนั้นจะมี $r_1x + s_1, r_2x + s_2 \in S$ ซึ่ง $r_1x + s_1 \neq r_2x + s_2$ ที่ทำให้

$$r_1x + s_1 \equiv r_2x + s_2 \pmod{p}$$

ดังนั้น $(r_1 - r_2)x \equiv s_2 - s_1 \pmod{p}$

ให้ $u = |r_1 - r_2|$ และ $v = |s_2 - s_1|$ จาก (6.8) จะได้

$$ux \equiv \pm v \pmod{p} \quad \dots\dots\dots(2)$$

จาก $r_1x + s_1 \neq r_2x + s_2$ เราพบว่า $u \neq 0$ หรือ $v \neq 0$ และจาก (1) และ (2) จะได้

$$0 \equiv u^2(x^2 + 1) \equiv (ux)^2 + u^2 \equiv v^2 + u^2 \pmod{p}$$

นั่นคือ $u^2 + v^2 = kp$ แต่ $u^2 + v^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p$

ดังนั้น $k = 1$ และ $u^2 + v^2 = p$ ■

ตัวอย่าง 1 จากตัวอย่างข้างต้นเราพบว่า จำนวนเต็มตั้งแต่ 1 ถึง 15 ที่สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็มสองจำนวนได้ คือ 1, 2, 4, 5, 8, 9, 10 และ 13 จำนวนที่เหลือได้แก่ 3, 6, 12 และ 15 มี 3^1 เป็นตัวประกอบ และ 7, 14 มี 7^1 เป็นตัวประกอบ ถ้าเราวิเคราะห์จำนวนเต็มจาก 51 ถึง 60 เราพบว่า

$$51 = 3 \cdot 17 \quad (\text{มี } 3^1 \text{ เป็นตัวประกอบ})$$

$$52 = 2^2 \cdot 13 = 4^2 + 6^2$$

$$53 = 2^2 + 7^2$$

$$54 = 2 \cdot 3^3 \quad (\text{มี } 3^3 \text{ เป็นตัวประกอบ})$$

$$\begin{aligned}
 55 &= 5 \cdot 11 && (\text{มี } 11^1 \text{ เป็นตัวประกอบ}) \\
 56 &= 2^3 \cdot 7 && (\text{มี } 7^1 \text{ เป็นตัวประกอบ}) \\
 57 &= 3 \cdot 19 && (\text{มี } 3^1 \text{ และ } 19^1 \text{ เป็นตัวประกอบ}) \\
 58 &= 2 \cdot 29 = 3^2 + 7^2 \\
 59 &\equiv 3 \pmod{4} \\
 60 &= 2^3 \cdot 3 \cdot 5 && (\text{มี } 3^1 \text{ เป็นตัวประกอบ})
 \end{aligned}$$

□

โจทย์ปัญหา 7.5

1. จงหาจำนวนเต็มบวก a, b, c, d ที่แตกต่างกันทั้ง 4 จำนวนซึ่ง $a^2 + b^2 = c^2 + d^2 = 493097$
(ข้อเสนอแนะ $493097 = 577 \cdot 761$)
2. จงแสดงว่า มีจำนวนเฉพาะ p ซึ่ง $p \equiv 1 \pmod{8}$ เป็นจำนวนไม่จำกัด
3. จงแสดงว่า มีจำนวนเฉพาะ p ซึ่ง $p \equiv 5 \pmod{8}$ เป็นจำนวนไม่จำกัด
4. จงพิสูจน์ว่า ถ้า $n \equiv 7 \pmod{8}$ แล้ว n ไม่สามารถเขียนได้ในรูปผลบวกของกำลังสองของจำนวนเต็มสามจำนวนได้
5. จงแสดงว่า ถ้า $4 \mid (x^2 + y^2 + z^2)$ แล้ว x, y, z จะต้องเป็นจำนวนเต็มคู่
6. ให้ $n = 4^k(8m + 7)$ จงพิสูจน์ว่า n ไม่สามารถเขียนในรูปผลบวกของกำลังสองของจำนวนเต็มสามจำนวนได้
7. ให้ p เป็นจำนวนเฉพาะซึ่ง $p \equiv 1 \pmod{4}$ จงพิสูจน์ว่ามี $u, v \in \mathbb{Z}$ ซึ่ง

$$(u, v) = 1 \quad \text{และ} \quad p = u^2 + v^2$$
8. ให้ p, q เป็นจำนวนเฉพาะซึ่ง $p \neq q$ และ $p \equiv 1 \pmod{4}, q \equiv 1 \pmod{4}$
 จงพิสูจน์ว่า $pq = u^2 + v^2, 0 < u < v$ มีอย่างน้อย 2 คำตอบที่แตกต่างกัน
9. ให้ p เป็นจำนวนเฉพาะซึ่ง $p \geq 3$ จงพิสูจน์ว่า $x^4 \equiv -1 \pmod{p}$ มีคำตอบ $x \in \mathbb{Z}$
 ก็ต่อเมื่อ $p \equiv 1 \pmod{8}$

โจทย์ปัญหาเสริมเรื่อง สมการไดโอแฟนไทน์

ปัญหา 1 จงหาชุดของจำนวนเฉพาะที่เป็นบวก (x, y, z) ทุกชุด ซึ่ง $x^y + 1 = z$

วิธีทำ กรณี 1 ถ้า y เป็นจำนวนเฉพาะคี่ ซึ่ง $y \geq 3$

$$\text{จะได้ว่า } x^y + 1 = (x + 1)(x^{y-1} - x^{y-2} + x^{y-3} - \dots + 1)$$

ดังนั้น $z = x^y + 1$ ไม่ใช่จำนวนเฉพาะ ซึ่งเป็นไปไม่ได้

กรณี 2 ถ้า y เป็นจำนวนเฉพาะคู่ นั่นคือ $y = 2$ จะได้ $x^2 + 1 = z$

ถ้า x เป็นจำนวนเฉพาะคี่ จะได้ว่า z เป็นจำนวนเฉพาะคู่ ฉะนั้น $z = 2$

จึงเป็นไปไม่ได้เพราะว่า $x \geq 3$ ฉะนั้น $x^2 + 1 \neq 2$

เพราะฉะนั้น x เป็นจำนวนเฉพาะคู่ จะได้ว่า $x = 2$

$$\text{และจะได้ } z = 2^2 + 1 = 5$$

ดังนั้นชุดของจำนวนเฉพาะที่เป็นบวกที่ต้องการเพียงชุดเดียว คือ $(2, 2, 5)$ □

ปัญหา 2 จงหาคำตอบ x และ y ที่เป็นจำนวนเต็มทั้งหมดที่สอดคล้องกับสมการ

$$x^2 + y^2 + x + y = 3$$

วิธีทำ ให้ $L(x, y) = x^2 + y^2 + x + y = x(x + 1) + y(y + 1)$

จากความจริงที่ว่าสำหรับจำนวนเต็ม x ใด ๆ $x(x + 1)$ จะต้องเป็นจำนวนเต็มคู่

ในทำนองเดียวกันเราจึงได้ว่า $y(y + 1)$ ก็ต้องเป็นจำนวนเต็มคู่

ดังนั้น $L(x, y)$ จะต้องเป็นจำนวนเต็มคู่

เราจึงสรุปได้ว่าสมการ $L(x, y) = 3$ ไม่มีคำตอบในระบบจำนวนเต็ม □

ปัญหา 3 จงหาจำนวนเต็ม x, y ทุกคู่ที่เป็นคำตอบของสมการ $x(y + 1)^2 = 243y$

วิธีทำ เนื่องจาก $(y + 1, y) = 1$ จะได้ว่า $(y + 1)^2 \mid 243$

แต่ $243 = 3^5$ ดังนั้นค่าของ $(y + 1)^2$ ที่เป็นไปได้ทั้งหมดคือ $1, 3^2, 3^4$

$$\text{จะได้ว่า } y = 0, -2, 2, -4, 8, -10$$

$$\text{เนื่องจาก } x = \frac{243y}{(y + 1)^2}$$

$$\text{ดังนั้น } x = 0, -486, 54, -108, 24, -30$$

เพราะฉะนั้น จำนวนเต็ม x, y ที่เป็นคำตอบของสมการนี้คือ

$$(x, y) = (0, 0), (-486, -2), (54, 2), (-108, -4), (24, 8) \text{ และ } (-30, -10) \quad \square$$

ปัญหา 4 จงพิสูจน์ว่า ไม่มีจำนวนเต็ม x และ y ที่เป็นคำตอบของสมการ $3x^2 + 8 = y^2$

วิธีทำ สมมติว่ามีจำนวนเต็ม x, y ที่เป็นคำตอบของสมการ $3x^2 + 8 = y^2$

$$\text{จาก } 3x^2 + 8 = y^2 \text{ จะได้ว่า } 3x^2 + 6 = y^2 - 2$$

$$\text{และ } 3(x^2 + 2) = y^2 - 2 \quad \text{แสดงว่า } y^2 \equiv 2 \pmod{3}$$

$$\text{แต่ } y^2 \equiv 0, 1, 1 \pmod{3} \text{ สำหรับ } y \equiv 0, 1, 2 \pmod{3}$$

$$\text{จึงเป็นไปไม่ได้ที่ } y^2 \equiv 2 \pmod{3}$$

ฉะนั้นไม่มีจำนวนเต็ม x, y ที่เป็นคำตอบของสมการนี้ □

ปัญหา 5 จงตรวจสอบว่า สมการ $a^2 + b^2 + c^2 = a^2b^2$ มีคำตอบหรือไม่ เมื่อ $a, b, c \in \mathbb{N}$

ปัญหา 6 จงหาจำนวนเต็มบวก x และ y ทุกคู่ที่เป็นคำตอบของสมการ $x^2 - xy + y = 3$

วิธีทำ จาก $x^2 - xy + y = 3$

$$x^2 - xy + y - 1 = 2$$

$$4(x^2 - xy + y - 1) = 8$$

$$4x^2 - 4xy + y^2 - y^2 + 4y - 4 = 8$$

$$(2x - y)^2 - (y - 2)^2 = 8$$

$$\text{ให้ } a = 2x - y \text{ และ } b = y - 2 \text{ จะได้ว่า } a^2 - b^2 = (a - b)(a + b) = 8$$

$$\text{ดังนั้น } a - b = 2 \text{ และ } a + b = 4 \quad \text{แสดงว่า } a = 3 \text{ และ } b = 1$$

$$\text{เพราะฉะนั้น } 2x - y = 3 \text{ และ } y - 2 = 1 \text{ ซึ่งทำให้ } x = 3 \text{ และ } y = 3 \quad \square$$

ปัญหา 7 จงหาจำนวนเต็มบวก a, b, c ที่เป็นคำตอบของสมการ

$$a^3 - b^3 - c^3 = 3abc$$

และ $a^2 = 2(b + c)$

วิธีทำ เนื่องจาก $3abc$ เป็นจำนวนเต็มบวก จะได้ว่า $b^3 < a^3$ และ $c^3 < a^3$

$$\text{จะได้ } b < a \text{ และ } c < a \quad \text{ดังนั้น } b + c < 2a$$

$$\text{พิจารณา } 2(b + c) < 4a \text{ จะได้ว่า } a^2 < 4a \text{ และทำให้ } a < 4$$

$$\text{จาก } a \text{ เป็นจำนวนเต็มคู่ เพราะฉะนั้น } a = 2, b = c = 1 \quad \square$$

แบบฝึกหัดเรื่อง สมการไดโอแฟนไทน์

1. จงหาจำนวนเต็มบวก x และ z ทุกคู่ที่ทำให้ $x^2 = z^2 + 120$
2. จงหาจำนวนเต็มบวก x และ z ทุกคู่ที่ทำให้ $x^3 = z^3 + 721$
3. จงหาจำนวนเต็ม x และ y ทุกคู่ที่เป็นคำตอบของสมการ $15x^2 - 7y^2 = 9$
4. จงหาจำนวนเต็ม x และ y ทุกคู่ที่เป็นคำตอบของสมการ $1 + x + x^2 + x^3 = 2^y$
5. จงหาจำนวนเต็ม x และ y ทุกคู่ที่เป็นคำตอบของสมการ $x^2 + xy + y^2 = x^2y^2$
6. จงหาจำนวนเต็มบวก x และ y ทุกคู่ที่เป็นคำตอบของสมการ $1! + 2! + 3! + \cdots + x! = y^2$
7. จงหาจำนวนเต็มบวก a, b, c ทั้งหมดที่เป็นคำตอบของสมการ $3^a + 1 = 5^b + 7^c$
8. จงหาจำนวนเต็ม x และ y ทุกคู่ที่เป็นคำตอบของสมการ $x^4 + (n+1)^4 = y^2 + (y+1)^2$
9. จงแสดงว่าสมการ $\frac{1}{x^4} - \frac{1}{y^4} = \frac{1}{z^4}$ ไม่มีคำตอบที่เป็นจำนวนเต็มบวก
10. จงแสดงว่าสมการ $x^2 + y^2 = z^3$ มีคำตอบเป็นจำนวนเต็มบวกได้ไม่จำกัดจำนวน
11. กำหนดสมการ $x^2 + y^2 = z^2 + 18$ เมื่อ x, y และ z เป็นจำนวนเต็มบวก
 - (11.1) จงพิสูจน์ว่า z จะต้องเป็นจำนวนเต็มคู่
 - (11.2) จงพิสูจน์ว่า สมการนี้มีคำตอบอยู่ในรูป $z = y + 1$ ไม่จำกัดชุด
 - (11.3) จงพิสูจน์ว่า สมการนี้ไม่มีคำตอบในรูป $z = y + 5$
 - (11.4) จงพิสูจน์ว่า สมการนี้ไม่มีคำตอบ x, y, z ที่เรียงกันเป็นลำดับเลขคณิต
 - (11.5) จงพิสูจน์ว่า สมการนี้ไม่มีคำตอบ x, y, z ที่เรียงกันเป็นลำดับเรขาคณิต
 - (11.6) จงหาคำตอบของสมการนี้มาสัก 1 ชุด เมื่อ $x = y$
 - (11.7) จงพิสูจน์ว่า สมการนี้มีคำตอบไม่จำกัดชุดเมื่อ $x = y$
12. จงแสดงว่า ทุก ๆ จำนวนเต็มบวก z จะมีจำนวนเต็ม x และ y ที่สอดคล้องสมการ $x^2 - y^2 = z^3$
13. จงแสดงว่า สมการไดโอแฟนไทน์ $5m^2 - 6mn + 7n^2 = 1988$ ไม่มีคำตอบ
14. จงแสดงว่า ไม่มีจำนวนเต็ม a, b, c ที่เป็นคำตอบของสมการ $a^2 + b^2 - 8c = 6$
15. ให้ n เป็นจำนวนเต็ม จงพิสูจน์ว่า ถ้า $2 + 2\sqrt{28n^2 + 1}$ เป็นจำนวนเต็ม แล้วจำนวนดังกล่าวนี้จะเป็นกำลังสองสมบูรณ์
16. ให้ p เป็นจำนวนเฉพาะซึ่ง $p > 5$ จงพิสูจน์ว่าสมการ $x^2 + 4x = p$ ไม่มีคำตอบ

บรรณานุกรม

ภาษาไทย

1. ณรงค์ ปันนัม. **ทฤษฎีจำนวน**. กรุงเทพฯ: สำนักพิมพ์ภูมิบัณฑิต, 2545.
2. นิตติยา ปภาพจน์. **ทฤษฎีจำนวน**. กรุงเทพฯ: เอกสารประกอบการสอน มหาวิทยาลัยหอการค้าไทย, 2544.
3. สมใจ จิตพิทักษ์. **ทฤษฎีจำนวน**. พิมพ์ปรับปรุงครั้งที่ 2 สงขลา : มหาวิทยาลัยทักษิณ, 2545.
4. สมวงศ์ แปลงประสพโชค. **ทฤษฎีจำนวน**. กรุงเทพฯ : ชมรมคณิตศาสตร์ สถาบันราชภัฏพระนคร, 2537.

ภาษาอังกฤษ

1. Aigner, M. and Ziegler, G. M., **Proofs from the Book**, Springer-Verlag, Berlin Heidelberg, 1998.
2. Apostol, T. M., **Introduction to Analytic Number Theory**, Springer-Verlag, New York, 1976.
3. Burton, D. M., **Elementary Number Theory**, 5th ed, The McGraw-Hill Companies, Inc., New York, 2002.
4. Euclid, **The Elements**, 3 vols. New York, 1956.
5. Eynden, C. V., **Elementary Number Theory**, 2nd ed., The McGraw-Hill Companies, Inc., New York, 2001
6. Hardy, G. H. and Wright, E. M., **An Introduction to the Theory of Numbers**, 5th ed., Oxford University Press, Oxford, 1981.
7. McCoy, N. H., **The Theory of Numbers**, The Macmillan Company, New York, 1965.
8. Niven, I., Zuckerman, H. S. and Montgomery, H. L., **An Introduction to the Theory of Number**, 5th ed., John Wiley & Sons, Inc., New York, 1991.
9. Ore, O., **Invitation to Number Theory**, The Mathematical Association of America, Washington, 1967.

10. Rosen, K.H., **Elementary Number Theory and Its Applications**, 3rd ed., Addison-Wesley Publishing Company, Massachusetts, 1993.
11. Rose, H. E., **A Course in Number Theory**, Clarendon Press, Oxford, 1988.
12. Shapiro, H. N., **Introduction to the Theory of Numbers**, John Wiley & Sons, New York, 1983.
13. Simon, Singh, **Fermat's Last Theorem**, London : Fourth Estate Limited, 1998.
14. Vander Eynden, Charles, **Elementary Number Theory**, 2nd ed. The McGraw-Hill Companies, Inc., New York, 2001.

ดัชนี

ก		จำนวนเฉพาะเทียม	93
การหารลงตัว	32	จำนวนเฉพาะเมอร์แซนน์	4, 85
เกาส์ (Gauss : 1777 – 1855)	1	จำนวนเฉพาะสัมพัทธ์	61
โกลด์บาค (Goldbach : 1690 – 1764)	4, 79	จำนวนเฉพาะสัมพัทธ์ทุกคู่	61
		จำนวนแฟร์มาต์	3, 83
ข		จำนวนเต็มที่ปราศจากกำลังสอง	163
ขั้นตอนวิธีการหาร	29	จำนวนเต็มแบบยุคลิด	74
ขั้นตอนวิธีแบบยุคลิด	42	จำนวนเต็มเรพุนิต	88
		จำนวนพาลินโดม	26
ค		จำนวนมิติกราฟ	2
คอนกรูเอนซ์	128	จำนวนแมร์เซิน	85
ค่าสัมบูรณ์	19	จำนวนสมบูรณ์	2, 87
คำตอบเฉพาะราย	171	จำนวนสามเหลี่ยม	20
คুমเมอร์ (Kummer : 1810 – 1893)	5	จำนวน squarish	24
โค (Koh)	57		
โครเนกเคอร์ (Kronecker : 1823 – 1891)	129	ช	
โคล (Cole : 1861 – 1927)	85	เชน (Chen)	2
		เชบีเชฟ (Tshebychef : 1821 – 1894)	76
จ			
จำนวนประกอบ	58		
จำนวนมิติกราฟ	2	ช	
จำนวนสมบูรณ์	2, 87	เซลฟรีดจ์ (Selfridge)	88
จำนวนเฉพาะ	57	เซลเบิร์ก (Selberg)	4
จำนวนเฉพาะคู่แฝด	4, 82		
จำนวนเฉพาะแฟร์มาต์	3, 83		

ด		ปีปปิง (Pipping)	4
ดิริชเลต์ (Dirichlet : 1805 – 1859)	3	ปีทาโกรัส (Pythagorus : 569 – 500 B.C.)	1
ดีโอฟานโตสแห่งอะเล็กซานเดรีย	2		
(Diophantos of Alexandria : 250 – 300)		พ	
เดส์การ์ตส์ (Descartes : 1596 – 1859)	2	พรีมิตีฟ	192
เดอ โบเวล (De Bouvelle)	90		
		ฟ	
ด		ฟังก์ชันค่าเชิงซ้อน	95
ตะแกรงเอราโตสเทเนส	67	ฟังก์ชันจำนวนเต็มค่ามากที่สุด	117
ตัวคูณร่วม	44	ฟังก์ชันซิกมา	103
ตัวคูณร่วมน้อย	44	ฟังก์ชันเทา	101
ตัวประกอบ	32	ฟังก์ชันฟี	108
ตัวหารร่วม	36	ฟังก์ชันแยกคูณ	96
ตัวหารร่วมมาก	36	ฟังก์ชันแยกคูณแบบบริบูรณ์	97
		ฟังก์ชันแยกบวก	98
ท		ฟังก์ชันแยกบวกแบบบริบูรณ์	98
ทฤษฎีจำนวนเชิงพีชคณิต	168	ฟังก์ชันมานเกอลท์	96
ทฤษฎีบทของจำนวนเฉพาะ	4, 76	ฟังก์ชันเมอบิอุส	96, 113
ทฤษฎีบทของแฟร์มาต์	154	ฟังก์ชันลีอูวิลล์	95
ทฤษฎีบทของวิลสัน	156	ฟังก์ชันเลขคณิต	95
ทฤษฎีบทของออยเลอร์	154	แฟลททอเรียล	18
ทฤษฎีบทพื้นฐานทางพีชคณิต	128	แฟร์มาต์ (Fermat : 1601 – 1665)	2
ทฤษฎีบทหลักมูลของเลขคณิต	62		
ทฤษฎีบทสุดท้ายของแฟร์มาต์	5, 152	ผ	
ทฤษฎีบทเศษเหลือของจีน	142	ผลคูณค่ามากที่สุด	53
ทาร์ตาเลีย (Tartaglia)	90	ผลคูณดิริชเลต์	100
เทย์เลอร์ (Taylor)	5	ผลต่างร่วม	16
		ผลหาร	29
บ			
บอโรซดกิน (Borozzdkin)	5	ม	
เบสซี (Bessy : 1605 – 1670)	154	มอดุลัส	131
เบอร์ทราน (Bertrand : 1822 – 1900)	76	มอดุโล	131
		แมร์เซน (Mersenne : 1588 – 1648)	85
ป		มิลล์ (Mills)	89
ปัญหาฉนวน	5		
ปูแซง (Poussin : 1866 – 1962)	4, 76		

ย		สมบัติทางพีชคณิต	6
ยุคลิด	2	สมบัติไตรวิภาค	6, 8
(Euclid of Alexandria : 450 – 380 B.C.)		ส่วนตกค้าง	134
		ส่วนตกค้างที่ไม่เป็นลบค่าน้อยสุด	134
ร		สัมประสิทธิ์ทวินาม	18
ระบบจำนวนเต็ม	6	สามจำนวนของปีทาโกรัส	178
ระบบส่วนตกค้างบริบูรณ์	136	สามเหลี่ยมปาสคาล	18
ระบบส่วนตกค้างบริบูรณ์ที่ไม่เป็นลบค่าน้อยสุด	136	สูตรของเลอจองด์	89
ระบบส่วนตกค้างลดทอน	157		
ระบบส่วนตกค้างลดทอนที่ไม่เป็นลบค่าน้อยสุด	157	ห	
รูปแบบบัญญัติ	63	หนังสือ Euclid's Element Book IX	60
		หลักการจัดอันดับดี	6, 10
ล		หลักอุปนัยเชิงคณิตศาสตร์	11
ลากรองจ์ (Lagrange : 1736 – 1813)	3	หลักอุปนัยเชิงคณิตศาสตร์ที่ 1	12
ลำดับฟีโบนัชชี	23	หลักอุปนัยเชิงคณิตศาสตร์ที่ 2	14
ลำดับลูคัส	15	หลักอุปนัยอย่างเข้ม	15
ลำดับเลขคณิต	16		
ลำดับเรขาคณิต	16	อ	
ลูคัส (Lucas : 1842 – 1891)	83	ออยเลอร์ (Euler : 1707 – 1783)	2
เลห์เมอร์ (Lehmer)	86	ออยเลอร์ พี – ฟังก์ชัน	108
เลม (Lame : 1795 – 1870)	5	อนุกรมคอนเวอร์เจนท์	79
เลอจองด์ (Legrenge : 1752 – 1833)	2	อนุกรมไดเวอร์เจนท์	79
		อริสโตเติล (Aristotle : 384 – 322 B.C.)	57
ว		อัตราส่วนร่วม	16
วโนกราดอฟ (Vinogradov)	5, 81	ฮาดามาร์ (Hadamard : 1865 – 1973)	4, 76
วูดส์ (Woods)	2	เออดอส (Erdős : 1913 – 1996)	4
ไวล์ (Wiles : 1953 –)	5		
		ฮ	
ส		ฮาร์ดี (Hardy : 1877 – 1947)	5
สมการของปีทาโกรัส	178	เฮอร์วิทซ์ (Hurwitz)	90
สมการคอนกรูเอนซ์	137		
สมการคอนกรูเอนซ์เชิงเส้น	140	Prime – triplet	92
สมการคอนกรูเอนซ์ที่มีดีกรีมากกว่าหนึ่ง	159	Möbius Inversion Formula	115
สมการไดโอแฟนไทน์	2, 170		
สมการไดโอแฟนไทน์กำลังสอง	186		
สมบัติของอาร์คิมิดีส	11		

บัญชีสัญลักษณ์

สัญลักษณ์

ความหมาย

$\mathbb{Z}$

เซตของจำนวนเต็ม 6

$\mathbb{N}$

เซตของจำนวนเต็มบวก 7

$a \mid b$

a หาร b ลงตัว 32

$a \nmid b$

a หาร b ไม่ลงตัว 32

(a, b)

ตัวหารร่วมมากของ a และ b 36

$(a_1, a_2, \dots, a_n)$

ตัวหารร่วมมากของ $a_1, a_2, \dots$ และ a_n 40

$[a, b]$

ตัวคูณร่วมน้อยของ a และ b 44

$[a_1, a_2, \dots, a_n]$

ตัวคูณร่วมน้อยของ $a_1, a_2, \dots$ และ a_n 46

$\lfloor x \rfloor$

จำนวนเต็มที่มากที่สุดที่น้อยกว่าหรือเท่ากับ x 48

$P^* + 1$

จำนวนเต็มแบบยุคลิด 74

$\pi(n)$

จำนวนของจำนวนเฉพาะ p ที่ $p \leq n$ 76

λ

ฟังก์ชันลิอูวิลล์ 95

Λ

ฟังก์ชันมานเกอลท์ 96

μ

ฟังก์ชันเมอบิอุส 96

τ

ฟังก์ชันเทา 101

σ

ฟังก์ชันซิกมา 103

$\sigma(n)$

ผลบวกของตัวหารทั้งหมดของ n 103

$\sigma_k(n)$

ผลบวกกำลัง k ของตัวหารทั้งหมดของ n 103

ϕ

ฟังก์ชันฟี 108

$a \equiv b \pmod{n}$

a คอนกรูเอนซ์กับ b มอดุโลกับ n 130

$a \not\equiv b \pmod{n}$

a ไม่คอนกรูเอนซ์กับ b มอดุโลกับ n 130

$\mathbb{Z}_n$

เซตของจำนวนเต็มมอดุโล n 139

(x, y, z)

สามจำนวนของพีทาโกรัส 180



มูลนิธิส่งเสริมโอลิมปิกวิชาการและพัฒนามาตรฐานวิทยาศาสตร์ศึกษา

ในพระอุปถัมภ์สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์

สำนักงานตั้งอยู่ในบริเวณ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ถนนพญาไท ปทุมวัน กทม. 10330

โทร. 0-2252-8916, 0-2252-8917, แฟกซ์. 0-2252-8917

ทฤษฎีจำนวน
ISBN 974 - 92235 - 1 - 9



9 789749 223512

C 112

4000 240.00 บาท