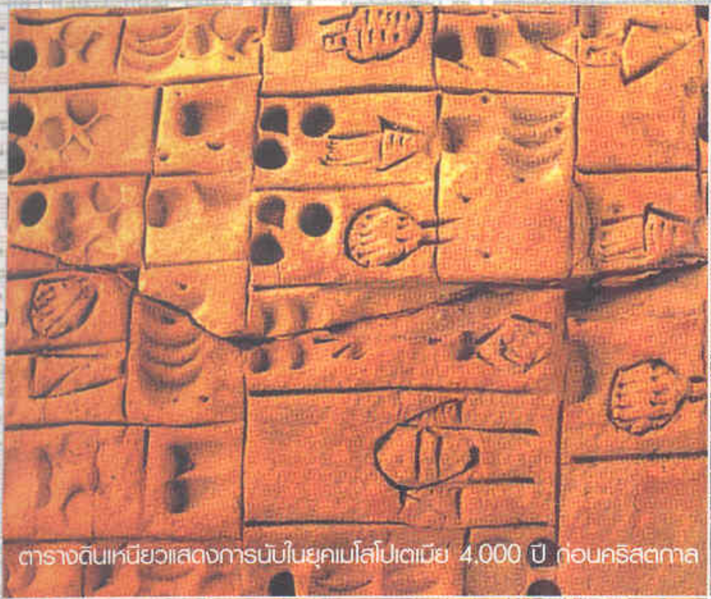
คณิตศาสตร์พื้นฐาน สำหรับคอมพิวเตอร์

(ตรรกศาสตร์ เซต ความสัมพันธ์และฟังก์ชัน ทฤษฎีจำนวน คณิตศาสตร์เชิงการจัด เมทริกซ์)



ตารางดินเหนียวแสดงการนับในยุคเมโสโปเตเมีย 4,000 ปี ก่อนคริสตกาล

ภาพแสดงการนับโดยใช้ลูกคิดของชาวเอเชีย เช่น จีน ญี่ปุ่น เป็นต้น

ภาพแสดงการนับในสมัยเรเนซองซ์ นิยมใช้ในประเทศที่ใช้ภาษาเยอรมัน

เครื่องคำนวณในยุคแรกๆ สร้างโดยไลบ์นิตซ์ ประมาณปี ค.ศ. 1690

โครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.

คณิตศาสตร์พื้นฐาน สำหรับคอมพิวเตอร์

(ตรรกศาสตร์ เซต ความสัมพันธ์และฟังก์ชัน ทฤษฎีจำนวน คณิตศาสตร์เชิงการจัด เมทริกซ์)

การแสดงวิธีการคำนวณทางคณิตศาสตร์ ของ MARGARITA
นักปรัชญาที่มีชื่อ ปี ค.ศ. 1503 (จากหนังสือ ARITHMEUM)

โครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.

มูลนิธิส่งเสริมโอลิมปิกวิชาการและพัฒนามาตรฐานวิทยาศาสตร์ศึกษา
ในพระอุปถัมภ์สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา
กรมหลวงนราธิวาสราชนครินทร์ (สอวน.)

<u>ความเป็นมา</u>

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

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

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

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

<u>วัตถุประสงค์</u>

1. ส่งเสริมให้นักเรียนในระดับมัธยมศึกษาตอนปลายทั่วประเทศที่มีความสามารถทางวิทยาศาสตร์และคณิตศาสตร์ มีโอกาสได้รับการพัฒนาศักยภาพทางด้านคณิตศาสตร์ คอมพิวเตอร์ เคมี ฟิสิกส์ และชีววิทยา ตามความถนัดทั้งด้านทฤษฎีและทักษะด้านปฏิบัติ ให้สามารถคิดวิเคราะห์และแก้ปัญหาที่ซับซ้อนได้ 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 และเพื่อขยายผลจากประสบการณ์ที่ได้เข้าแข่งขันโอลิมปิกวิชาการระหว่างประเทศมาพัฒนามาตรฐานวิทยาศาสตร์และคณิตศาสตร์ของไทยให้สูงขึ้นเทียบเท่าสากล

ในการอบรมนักเรียนของศูนย์ สอวน. มูลนิธิ สอวน.ได้พิจารณาเห็นว่าตำราที่มีความสมบูรณ์ของเนื้อหาตามหลักสูตรของ สอวน. จะช่วยพัฒนาศักยภาพของนักเรียนในศูนย์สอวน.ให้สูงยิ่งขึ้นได้ นอกจากนั้นตำราเรียนในวิชาวิทยาศาสตร์และคณิตศาสตร์ในระดับมัธยมศึกษาตอนปลายที่มีความสมบูรณ์ถูกต้องยังขาดแคลน นักเรียนและครูสามารถนำตำราที่พัฒนาขึ้นมานี้ไปใช้เป็นหนังสืออ้างอิงประกอบการเรียนการสอนได้อีกด้วย มูลนิธิ สอวน. จึงได้มี "โครงการจัดทำตำราส่งเสริมพัฒนาศักยภาพของนักเรียนด้านวิทยาศาสตร์ คณิตศาสตร์และคอมพิวเตอร์" ขึ้น เพื่อผลิตตำราคณิตศาสตร์ คอมพิวเตอร์ เคมี ชีววิทยาและฟิสิกส์ที่มีเนื้อหาหลักสูตรตามมาตรฐานสากล โดยมีวัตถุประสงค์

1. เพื่อเป็นที่ระลึกในมหามงคลสมัยที่สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ ทรงเจริญพระชนมายุ 80 พรรษา ซึ่งพระองค์ทรงมีพระมหากรุณาธิคุณต่อโครงการจัดส่งผู้แทนประเทศไทยไปแข่งขันโอลิมปิกวิชาการระหว่างประเทศและทรงสนับสนุนการดำเนินงานเพื่อพัฒนามาตรฐานการศึกษาวิทยาศาสตร์และคณิตศาสตร์ของไทยอย่างหาที่สุดมิได้

2. เพื่อผลิตหนังสือคณิตศาสตร์ คอมพิวเตอร์ เคมี ชีววิทยาและฟิสิกส์ระดับมัธยมศึกษาตอนปลายถึงระดับชั้นปีที่ 1 ของคณะวิทยาศาสตร์ในมหาวิทยาลัยให้มีคุณภาพเทียบเท่าสากล เรียบเรียงโดยคณาจารย์จากมหาวิทยาลัยของรัฐที่มีประสบการณ์สูงและที่มีส่วนรวมในการฝึกอบรมนักเรียนในค่าย 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 ขอขอบคุณพิพิธภัณฑ์ ARITHMEUM, Bonn ที่อนุญาต
ให้ประธานคณะกรรมการฯ เข้าถ่ายภาพในพิพิธภัณฑ์ เพื่อนำมาเผยแพร่

คณะกรรมการโครงการตำราวิทยาศาสตร์และคณิตศาสตร์มูลนิธิ สอวน.

คณะกรรมการที่ปรึกษา

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

คณะกรรมการดำเนินงานโครงการตำราฯ

1. ศาสตราจารย์ศักดา ศิริพันธุ์ (ราชบัณฑิต) เลขาธิการมูลนิธิ สอวน.	ประธาน
2. รองศาสตราจารย์เย็นใจ สมวิเชียร	รองประธาน
3. รองศาสตราจารย์ ดร. ณรงค์ ปั้นนิ่ม	กรรมการ (วิชาคณิตศาสตร์)
4. รองศาสตราจารย์ยืน ภู่วรวรรณ	กรรมการ (วิชาคอมพิวเตอร์)
5. รองศาสตราจารย์ ดร. พินิติ รตะนานุกูล	กรรมการ (วิชาเคมี)
6. ผู้ช่วยศาสตราจารย์ ดร.วุฑฒิพันธุ์ ปรัชญพฤทธิ์	กรรมการ (วิชาฟิสิกส์)
7. ศาสตราจารย์อักษร ศรีเปล่ง	กรรมการ (วิชาชีววิทยา ประเภทพืช)
8. รองศาสตราจารย์ ดร. อุษณีย์ ยศยิ่งยวด	กรรมการ (วิชาชีววิทยา ประเภทสัตว์)

คณะผู้เขียนวิชาคอมพิวเตอร์

1. รองศาสตราจารย์ยืน ภู่วรวรรณ	ประธานคณะอนุกรรมการ
2. รองศาสตราจารย์ ดร. อนงค์นาฏ ศรีวิหค	อนุกรรมการ
3. ผู้ช่วยศาสตราจารย์อุมาพร ศิรธรานนท์	อนุกรรมการ
4. ผู้ช่วยศาสตราจารย์กัลยาณี บรรจงจิตร	อนุกรรมการ
5. ผู้ช่วยศาสตราจารย์นงนุช สุขวารี	อนุกรรมการ
6. ผู้ช่วยศาสตราจารย์กรรณิกา คงสาคร	อนุกรรมการ
7. อาจารย์ศิริกร จันทร์นวล	อนุกรรมการ
8. อาจารย์พบสิทธิ์ กมลเวช	อนุกรรมการ
9. ดร. นวลวรรณ สุนทรภิษัช	อนุกรรมการ
10. ดร. สุขุมาล กิติสิน	อนุกรรมการ
11. อาจารย์พัชรี เลิศจิตรศิลป์	อนุกรรมการ
12. อาจารย์มาริสา มัยยะ	อนุกรรมการ

คำนำ

การแก้ปัญหาทางคอมพิวเตอร์นักเรียนจำเป็นต้องใช้พื้นความรู้ทางคณิตศาสตร์ เพื่อตอบสนองความต้องการดังกล่าว จึงได้จัดทำหนังสือคณิตศาสตร์พื้นฐานสำหรับคอมพิวเตอร์เล่มนี้ขึ้นโดยเน้นเนื้อหาพื้นฐานที่จำเป็น คณะผู้เขียนได้พยายามเขียนให้นักเรียนอ่านได้ง่ายและสามารถทำความเข้าใจได้ด้วยตนเอง โดยเนื้อหาจะเป็นความรู้คณิตศาสตร์พื้นฐานอันประกอบด้วย การทบทวนความรู้ทางตรรกศาสตร์ ในเรื่องของประพจน์ ตารางค่าความจริงและตัวดำเนินการชนิดตรรกะ สัจนิรันดร์ ข้อขัดแย้ง ประพจน์สมมูล ประโยคเปิดและตัวบ่งปริมาณ ความหมายของเซต เซตจำกัดและเซตอนันต์ การดำเนินการบนเซต แผนภาพของเวนน์ ความสัมพันธ์และฟังก์ชัน ความสัมพันธ์สมมูล ฟังก์ชันและชนิดของฟังก์ชัน การหารลงตัว จำนวนเฉพาะ ขั้นตอนวิธีการหารตัวหารร่วมมากและตัวคูณร่วมน้อย คอนกรูเอนซ์และการประยุกต์ จำนวนเต็มและขั้นตอนวิธีของยุคลิด วิธีการนับ วิธีเรียงสับเปลี่ยน วิธีจัดหมู่ สัมประสิทธิ์ทวินาม การทดลองสุ่ม แซมเปิลสเปซ ความน่าจะเป็น ความหมายของเมทริกซ์ การดำเนินการบนเมทริกซ์ เมทริกซ์ชนิดต่างๆ เมทริกซ์ผกผันและดีเทอร์มิแนนต์ ความรู้เรื่องเมทริกซ์ในเรื่องของความสัมพันธ์ได้โดยการแทนความสัมพันธ์ที่กำหนดด้วยเมทริกซ์ 0-1

สำหรับภาคผนวกท้ายเล่ม เพื่อความสะดวกในการศึกษาคณะผู้เขียนได้รวบรวมความรู้ที่ต้องการทราบเพิ่มเติมและการพิสูจน์ทฤษฎีบทต่างๆ

คณะผู้เขียนหวังว่าหนังสือคณิตศาสตร์พื้นฐานสำหรับคอมพิวเตอร์เล่มนี้ จะเป็นประโยชน์สำหรับนักเรียนเพื่อที่จะได้เตรียมตัวให้พร้อมก่อนที่จะเข้ารับการฝึกอบรมในโครงการ สอวน.

ที่ปรึกษา

รองศาสตราจารย์ยืน ภู่วรวรรณ

วศ.บ. (วิศวกรรมไฟฟ้าสื่อสาร) เกียรตินิยม, วศ. ม. (วิศวกรรมไฟฟ้า) จุฬาลงกรณ์มหาวิทยาลัย

M.Eng (Industrial Engineering and Management) at Asian Institute of Technology

ผู้เขียน

ผู้ช่วยศาสตราจารย์นงนุช สุขวารี

วท.ม. (คณิตศาสตร์) จุฬาลงกรณ์มหาวิทยาลัย

ผู้ช่วยศาสตราจารย์กรรณิกา คงสาคร

วท.ม. (คณิตศาสตร์ประยุกต์) มหาวิทยาลัยมหิดล

อาจารย์พัชรี เลิศวิจิตรศิลป์

วท.ม. (คณิตศาสตร์) จุฬาลงกรณ์มหาวิทยาลัย

อาจารย์มาริสา มัยยะ

ศศ.ม. (การสอนคณิตศาสตร์) มหาวิทยาลัยเกษตรศาสตร์

อาจารย์ศิริกร จันทร์นวล

M.S. (Computer Science) Syracuse University

ISBN 974-92235-3-5

จัดพิมพ์โดย มูลนิธิ สอวน.

พิมพ์ครั้งที่ 2 พ.ศ.2548 (2005)

ออกแบบปก หน้ารองปกและหน้านำบทที่ 1 โดย ศาสตราจารย์ศักดา ศิริพันธุ์

ศิลปกรรม: นายปรีชา ฉัตระเนตร

พิมพ์ที่ บริษัทด่านสุทธาการพิมพ์ จำกัด

แยกสี / เพลท เอ็นอาร์ ฟิล์ม

สารบัญ

ตรรกศาสตร์

อะริสโตเติล
384 – 322 ปีก่อนคริสต์ศักราช, กรีซ

ชาวกรีซในสมัยโบราณได้สนใจศึกษากฎต่าง ๆ ในทางคณิตศาสตร์และทางปรัชญากันมาก อะริสโตเติลเป็นผู้หนึ่งที่ได้เขียนตำราทางตรรกศาสตร์ที่เป็นระบบขึ้นเป็นครั้งแรก ซึ่งมีผลต่อความคิดทางปรัชญา ทางวิทยาศาสตร์และทางศาสนาเป็นอย่างมาก

ประพจน์

ประพจน์ หมายถึงประโยคที่มีค่าความจริงเป็นจริงหรือเท็จอย่างใดอย่างหนึ่ง ประโยคที่มีค่าความจริงเป็นจริงเรียกว่า **ประพจน์จริง** และประโยคที่มีค่าความจริงเป็นเท็จเรียกว่า **ประพจน์เท็จ**

ตัวอย่าง 1.1 ประโยคต่อไปนี้**เป็น**ประพจน์

(1) รุ้งมีเจ็ดสี

(2) หัวเราะมากเกินไป จิตใจจะหม่นหมอง

(3) ถ้านักเรียนคุยกันเสียงดัง แล้วคุณครูจะไม่สอนหนังสือ

(4) ผลลัพธ์ของ $\frac{100}{2}$ คือ 50

(5) 29 เป็นจำนวนเฉพาะ □

ตัวอย่าง 1.2 ประโยคต่อไปนี้**ไม่เป็น**ประพจน์

(1) ทานข้าวเสร็จแล้วเก็บจานให้เป็นระเบียบ

(2) ทำไมมดถึงเดินตามกันเป็นแถว

(3) ลูกผู้ชายตัวจริง กระทิงแดง

(4) $x = 15$

(5) $x + 5 > y - 10$ □

ประโยคบางประโยคอาจยากเกินกว่าจะหาค่าความจริงที่แท้จริงได้ อย่างไรก็ตาม ถ้าสามารถบอกได้ว่าประโยคนั้นจะมีค่าความจริงเป็นอย่างใดอย่างหนึ่งระหว่างจริงหรือเท็จ ก็จะสามารถจัดประโยคเหล่านั้นเป็นประพจน์ได้

ถ้าตัวแปร $P, Q, R, \ldots$ แทนประพจน์ใด ๆ จะเรียก $P, Q, R, \ldots$ ว่าเป็น**ตัวแปรประพจน์** ค่าความจริงของตัวแปรประพจน์ขึ้นกับค่าความจริงของประพจน์ที่จะมาแทนที่ตัวแปรประพจน์นั้น ๆ เช่น ถ้าให้ตัวแปรประพจน์ P แทนประพจน์ "นกกระจอกเทศวิ่งเร็วกว่าสุนัขจิ้งจอก" แล้ว P จะมีค่าความจริงเป็นจริง แต่ถ้าให้ตัวแปรประพจน์ P แทนประพจน์ "กระต่ายมีอายุยืนกว่าเต่า" แล้ว P จะมีค่าความจริงเป็นเท็จ

ตัวแปรประพจน์ตั้งแต่ 2 ตัวขึ้นไป เมื่อถูกเชื่อมเข้าด้วยกัน จะได้เป็นประพจน์ใหม่ที่มีความหมายครอบคลุมเงื่อนไขหลายอย่าง การประเมินค่าความจริงของประพจน์ใหม่ดังกล่าวจะมีความซับซ้อนมากยิ่งขึ้น โดยค่าความจริงของประพจน์ใหม่ขึ้นกับค่าความจริงของตัวแปรประพจน์แต่ละตัว และความหมายของตัวเชื่อมประพจน์ ลักษณะเดียวกับที่ค่าของนิพจน์คณิตศาสตร์ เช่น $x + y$ ขึ้นกับค่าของตัวแปร x และตัวแปร y และความหมายของการดำเนินการบวก

ตัวเชื่อมประพจน์ ได้แก่ "และ" "หรือ" และ "นิเสธ" เป็นต้น จัดเป็นตัวดำเนินการชนิดตรรกะที่มีประพจน์เป็นตัวถูกดำเนินการ

ในส่วนถัดไปจะกล่าวถึงความหมายของตัวเชื่อมประพจน์ และเครื่องมือที่ใช้ในการประเมินค่าความจริงของประพจน์ ที่ประกอบด้วยตัวเชื่อมประพจน์ต่าง ๆ ซึ่งมีชื่อเรียกว่า ตารางค่าความจริง

ตารางค่าความจริงและตัวดำเนินการตรรกะ

ตารางค่าความจริง ใช้สำหรับแจกแจงค่าความจริงที่เป็นไปได้ทั้งหมดของประพจน์ โดยแจกแจงค่าความจริงที่เป็นไปได้ทั้งหมดของตัวแปรประพจน์ที่เป็นตัวถูกดำเนินการทุกตัว ตามความหมายของตัวเชื่อมประพจน์

ตัวดำเนินการ "นิเสธ"

ให้ P เป็นตัวแปรประพจน์ใด ๆ ตารางค่าความจริงของตัวดำเนินการ "นิเสธ" ซึ่งเขียนแทนด้วยสัญลักษณ์ $\sim$ สามารถแสดงได้ ดังนี้

P	$\sim P$
เท็จ	จริง
จริง	เท็จ

โดยทั่วไป มักจะใช้สัญลักษณ์ 0 แทน เท็จ และสัญลักษณ์ 1 แทน จริง ดังนั้น ตารางค่าความจริงของตัวดำเนินการนิเสธจามารถเขียนได้เป็น

P	$\sim P$
0	1
1	0

ตัวดำเนินการนิเสธจัดเป็นตัวดำเนินการเอกภาค ที่ใช้เปลี่ยนค่าความจริงเป็นตรงกันข้าม

ตัวดำเนินการ "และ" และตัวดำเนินการ "หรือ"

ตัวดำเนินการ "และ" ซึ่งเขียนแทนด้วยสัญลักษณ์ $\wedge$ และตัวดำเนินการ "หรือ" ซึ่งเขียนแทนด้วยสัญลักษณ์ $\vee$ เป็นตัวดำเนินการทวิภาค ถ้าให้ P และ Q เป็นตัวแปรประพจน์ใด ๆ ตารางค่าความจริงของตัวดำเนินการทั้งสองสามารถแสดงได้ ดังนี้

P	Q	$P \wedge Q$	$P \vee Q$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

จะเห็นได้ว่าค่าความจริงของประพจน์ $P \wedge Q$ มีค่าเป็นจริงก็ต่อเมื่อประพจน์ P และ Q เป็นจริงทั้งคู่ ในขณะที่ค่าความจริงของประพจน์ $P \vee Q$ มีค่าเป็นจริงก็ต่อเมื่อประพจน์ P หรือ Q เป็นจริงอย่างน้อยหนึ่งประพจน์ เรียกตัวดำเนินการ "หรือ" ที่มีนิยามค่าความจริงดังแสดงในตารางข้างต้นว่า **อินคลูซีฟออร์**

นอกจากนี้มีการนิยามตัวดำเนินการ **เอกซ์คลูซีฟออร์** ซึ่งเขียนแทนด้วยสัญลักษณ์ $\oplus$ ดังนี้

		$P \oplus Q$
0	0	0
0	1	1
1	0	1
1	1	0

นั่นคือ ค่าความจริงของประพจน์ $P \oplus Q$ มีค่าเป็นจริงก็ต่อเมื่อประพจน์ P หรือ Q เป็นจริงเพียงประพจน์ใดประพจน์หนึ่งเท่านั้น ในบทเรียนนี้ ตัวดำเนินการ "หรือ" หมายถึงตัวดำเนินการอินคลูซีฟออร์

ตัวดำเนินการ "ถ้า...แล้ว..." และตัวดำเนินการ "...ก็ต่อเมื่อ..."

ตัวดำเนินการชนิดตรรกะ "ถ้า...แล้ว..." ซึ่งเขียนแทนด้วยสัญลักษณ์ $\rightarrow$ ถ้าให้ P และ Q เป็นตัวแปรประพจน์ใดๆ ในประพจน์ "ถ้า P แล้ว Q" ซึ่งเขียนแทนด้วยสัญลักษณ์ $P \rightarrow Q$ โดยมีประพจน์ P เป็นเหตุและประพจน์ Q เป็นผล ตารางค่าความจริงของตัวดำเนินการ $\rightarrow$ สามารถสรุปได้ ดังนี้

		$P \rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

ประพจน์ $P \rightarrow Q$ มีค่าความจริงเป็นเท็จเพียงกรณีเดียว นั่นคือ เมื่อประพจน์ P เป็นจริง และประพจน์ Q เป็นเท็จ ในกรณีที่ประพจน์ $P \rightarrow Q$ มีค่าความจริงเป็นจริง จะกล่าวได้ว่าประพจน์ P มีความหนักแน่นมากกว่าประพจน์ Q เช่น ประพจน์ "ถ้า x เป็นจำนวนเต็มบวก แล้ว x เป็นจำนวนเต็ม" จะเห็นได้ว่าประพจน์ "x เป็นจำนวนเต็มบวก" มีความหนักแน่นกว่าประพจน์ "x เป็นจำนวนเต็ม"

ตัวอย่าง 1.3 ประพจน์ต่อไปนี้เป็นประพจน์ของตัวดำเนินการ "ถ้า...แล้ว..."

(1) ถ้าร้องไห้มาก ๆ แล้วตาจะบวม

(2) ถ้าก้อนเมฆเป็นสีแดงแล้วรุ้งจะมีเจ็ดสี

(3) ถ้าโทรทัศน์ส่งกลิ่นได้ แล้วจะซื้อโทรทัศน์อีก 10 เครื่อง

(4) ถ้า 2 เป็นจำนวนคู่แล้ว $2+2$ เป็นจำนวนคู่

(5) ถ้า 3 หารด้วย 2 ลงตัวแล้ว 6 จะหารด้วย 2 ลงตัว □

ในทางคณิตศาสตร์ถึงแม้ประพจน์ P และประพจน์ Q ในประพจน์ $P \rightarrow Q$ จะมีความหมายที่ไม่เป็นเหตุและเป็นผลซึ่งกันและกัน แต่ก็สามารถจะประเมินค่าความจริงของประพจน์ดังกล่าวได้

ถ้าประพจน์ P และ Q มีค่าความจริงตรงกัน จะเรียกประพจน์ P **สมมูล**กับประพจน์ Q ตัวดำเนินการสมมูล เขียนแทนด้วยสัญลักษณ์ $\leftrightarrow$ ในประพจน์ $P \leftrightarrow Q$ มีค่าความจริงเป็นจริงเมื่อประพจน์ P และประพจน์ Q มีค่าความจริงตรงกัน ดังแสดงในตาราง

P	Q	$P \leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

เมื่อเปรียบเทียบตารางค่าความจริงของตัวดำเนินการ "ถ้า...แล้ว..." และตัวดำเนินการสมมูล จะพบว่า ถ้าประพจน์ $P \leftrightarrow Q$ เป็นจริง แล้วประพจน์ $P \rightarrow Q$ และประพจน์ $Q \rightarrow P$ จะเป็นจริงทั้งสองประพจน์ ในทางกลับกัน ถ้าประพจน์ $P \rightarrow Q$ และประพจน์ $Q \rightarrow P$ เป็นจริง แล้วประพจน์ $P \leftrightarrow Q$ จะเป็นจริง อาจเรียกประพจน์ $P \leftrightarrow Q$ ว่า "P **สมมูลกับ** Q" หรือ "P **ก็ต่อเมื่อ** Q" ก็ได้

ตัวอย่าง 1.4 ประพจน์ต่อไปนี้เป็นประพจน์ของตัวดำเนินการ "...ก็ต่อเมื่อ..."

(1) ฝนดาวตกจะมองเห็นได้ชัดเจน ก็ต่อเมื่อท้องฟ้าโปร่ง

(2) น้องพลับร้องเพลงเก่ง ก็ต่อเมื่อน้องพลับหมั่นฝึกฝนเป็นประจำ

(3) น้ำจะท่วม ก็ต่อเมื่อฝนตกหนักติดต่อกันเป็นเวลาหลายวัน

(4) $x + 15 = 20$ ก็ต่อเมื่อ $x = 8$

(5) คำตอบของข้อสอบข้อ 2 จะถูกต้อง ก็ต่อเมื่อคำตอบมีค่าเป็น 100 □

ประพจน์ย่อยหลาย ๆ ประพจน์สามารถเชื่อมเข้าด้วยกัน โดยอาศัยตัวดำเนินการต่าง ๆ ที่ได้กล่าวมาแล้ว เพื่อให้ได้ประพจน์ที่มีเงื่อนไขซับซ้อนมากยิ่งขึ้น และสามารถใช้ตารางค่าความจริงเพื่อหาค่าความจริงของประพจน์นี้ โดยผนวกตารางค่าความจริงของประพจน์ย่อยเข้าด้วยกัน

ตารางค่าความจริง ใช้สำหรับแจกแจงค่าความจริงที่เป็นไปได้ทั้งหมดของตัวแปรประพจน์แต่ละตัวในประพจน์ที่กำหนดให้ จากการที่ค่าความจริงที่เป็นไปได้ของตัวแปรประพจน์แต่ละตัวมีค่าเป็นจริงหรือเท็จอย่างใดอย่างหนึ่ง ดังนั้น ตารางค่าความจริงของประพจน์ที่ประกอบด้วยตัวแปรประพจน์ k ตัว จะมีกรณีที่เป็นไปได้ทั้งหมด 2^k กรณี

ตัวอย่าง 1.5 แสดงตารางค่าความจริงของประพจน์ต่อไปนี้

(1) $P \vee \sim P$

P	$\sim P$	$P \vee \sim P$
0	1	1
1	0	1

(2) $P \wedge \sim P$

P	$\sim P$	$P \wedge \sim P$
0	1	0
1	0	0

(3) $(Q \wedge \sim P) \rightarrow P$

P	Q	$\sim P$	$Q \wedge \sim P$	$(Q \wedge \sim P) \rightarrow P$
0	0	1	0	1
0	1	1	1	0
1	0	0	0	1
1	1	0	0	1

(4) $[(P \wedge Q) \vee \sim R] \leftrightarrow P$

P	Q	R	$P \wedge Q$	$\sim R$	$(P \wedge Q) \vee \sim R$	$[(P \wedge Q) \vee \sim R] \leftrightarrow P$
0	0	0	0	1	1	0
0	0	1	0	0	0	1
0	1	0	0	1	1	0
0	1	1	0	0	0	1
1	0	0	0	1	1	1
1	0	1	0	0	0	0
1	1	0	1	1	1	1
1	1	1	1	0	1	1

□

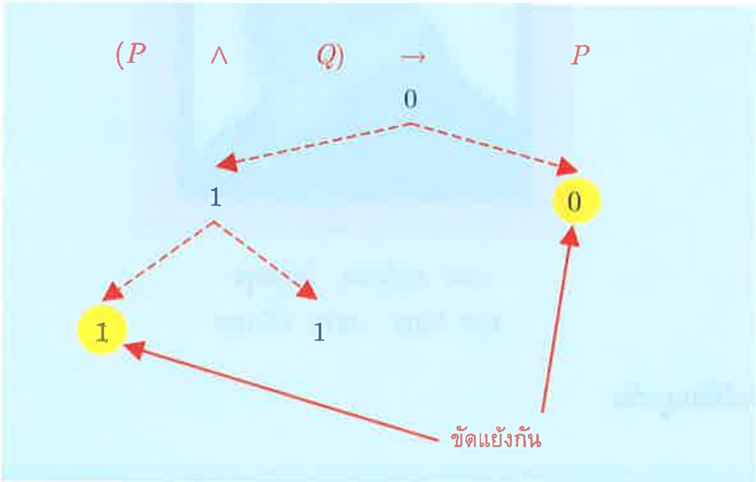
สัจนิรันดร์ ข้อขัดแย้ง และประพจน์สมมูล

ประพจน์ที่มีค่าความจริงเป็นจริงในทุกกรณีที่เป็นไปได้ของตัวแปรประพจน์ เรียกว่า **สัจนิรันดร์** และประพจน์ที่มีค่าความจริงเป็นเท็จในทุกกรณีที่เป็นไปได้ของตัวแปรประพจน์ เรียกว่า **ข้อขัดแย้ง** ดังนั้นประพจน์ $P \vee \sim P$ เป็นสัจนิรันดร์ และประพจน์ $P \wedge \sim P$ เป็นข้อขัดแย้ง

ในการแสดงว่าประพจน์ที่กำหนดให้เป็นสัจนิรันดร์หรือเป็นข้อขัดแย้ง จำเป็นต้องแสดงให้ครบทุกกรณีที่เป็นไปได้ของตัวแปรประพจน์ทั้งหมดว่ามีค่าความจริงเป็นจริงทั้งหมดหรือเป็นเท็จทั้งหมด ตามลำดับ

ตัวอย่าง 1.6 จงพิจารณาว่า $(P \wedge Q) \rightarrow P$ เป็นสัจนิรันดร์หรือไม่

วิธีทำ $(P \wedge Q) \rightarrow P$ จะเป็นสัจนิรันดร์ ก็ต่อเมื่อประพจน์ดังกล่าวมีค่าความจริงเป็นจริงในทุกกรณี แต่ถ้าสมมติให้ $(P \wedge Q) \rightarrow P$ ไม่เป็นสัจนิรันดร์ แสดงเพียงกรณีเดียวเท่านั้นที่ $(P \wedge Q) \rightarrow P$ เป็นเท็จ และถ้ากรณีที่เป็นเท็จดังกล่าวไม่มีโอกาสเกิดขึ้น จะกล่าวได้ว่า $(P \wedge Q) \rightarrow P$ เป็นสัจนิรันดร์



ขั้นที่ 1 : $(P \wedge Q) \rightarrow P$ เป็นเท็จ เมื่อ $(P \wedge Q) \rightarrow P$ เป็นจริง และ P เป็นเท็จ

ขั้นที่ 2 : $P \wedge Q$ จะเป็นจริง ก็ต่อเมื่อ ทั้ง P และ Q เป็นจริง

จากขั้นที่ 1 และขั้นที่ 2 จะเห็นได้ว่า P มีค่าความจริงที่ขัดแย้งกัน

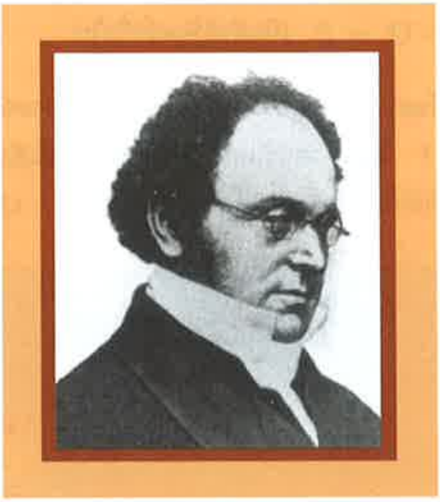
ดังนั้น $(P \wedge Q) \rightarrow P$ จึงไม่มีโอกาสเป็นเท็จ

นั่นคือ $(P \wedge Q) \rightarrow P$ เป็นสัจนิรันดร์ □

ตัวอย่างประพจน์ที่เป็นสัจนิรันดร์

	ประพจน์	สมบัติ
1.	$P \rightarrow (P \vee Q)$	แอดดิชัน
2.	$(P \wedge Q) \rightarrow P$	ซิมพลิฟิเคชัน
3.	$[P \wedge (P \rightarrow Q)] \rightarrow Q$	โมดัสโพเนนส์
4.	$[(P \rightarrow Q) \wedge \sim Q)] \rightarrow \sim P$	โมดัสโทเลนส์

ในการทำงานกับประพจน์ นิยมแทนประพจน์ด้วยประพจน์อื่นที่สมมูลกัน เพื่อให้ได้ประพจน์ใหม่ในรูปแบบที่ง่ายต่อการทำความเข้าใจมากขึ้น แต่ในขณะเดียวกันยังคงมีค่าความจริงเหมือนเดิม เช่น P สมมูลกับ $P \vee P$ ดังนั้น $(P \vee P) \vee Q$ สมมูลกับ $P \vee Q$ เป็นต้น



เดอ มอร์กอง, โอกุสตุส
ค.ศ. 1806 – 1871, ฝรั่งเศส

ตัวอย่างรูปแบบประพจน์ที่สมมูลกัน

	ประพจน์	สมบัติ
1.	$P \leftrightarrow (P \vee P)$	สมบัติสะท้อนของ $\vee$
2.	$P \leftrightarrow (P \wedge P)$	สมบัติสะท้อนของ $\wedge$
3.	$(P \vee Q) \leftrightarrow (Q \vee P)$	สมบัติสลับที่ของ $\vee$
4.	$(P \wedge Q) \leftrightarrow (Q \wedge P)$	สมบัติสลับที่ของ $\wedge$
5.	$[(P \vee Q) \vee R] \leftrightarrow [(P \vee (Q \vee R)]$	สมบัติจัดกลุ่มของ $\vee$
6.	$[(P \wedge Q) \wedge R] \leftrightarrow [(P \wedge (Q \wedge R)]$	สมบัติจัดกลุ่มของ $\wedge$
7.	$\sim(P \vee Q) \leftrightarrow (\sim P \wedge \sim Q)$	กฎเดอมอร์แกน
8.	$\sim(P \wedge Q) \leftrightarrow (\sim P \vee \sim Q)$	กฎเดอมอร์แกน
9.	$[P \wedge (Q \vee R)] \leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$	สมบัติกระจายของ $\wedge$ เหนือ $\vee$
10.	$[P \vee (Q \wedge R)] \leftrightarrow [(P \vee Q) \wedge (P \vee R)]$	สมบัติกระจายของ $\vee$ เหนือ $\wedge$
11.	$(P \vee 1) \leftrightarrow 1$	
12.	$(P \wedge 1) \leftrightarrow P$	
13.	$(P \vee 0) \leftrightarrow P$	
14.	$(P \wedge 0) \leftrightarrow 0$	
15.	$(P \vee \sim P) \leftrightarrow 1$	สัจนิรันดร์
16.	$(P \wedge \sim P) \leftrightarrow 0$	ข้อขัดแย้ง
17.	$P \leftrightarrow \sim(\sim P)$	นิเสธซ้อน
18.	$(P \rightarrow Q) \leftrightarrow (\sim P \vee Q)$	อิมพลิเคชัน
19.	$(P \leftrightarrow Q) \leftrightarrow [(P \rightarrow Q) \wedge (Q \rightarrow P)]$	สมบัติสมมูล

ตัวอย่าง 1.7 จงแสดงว่า $P \rightarrow Q$ สมมูลกับ $\sim P \vee Q$ โดยการใช้ตารางค่าความจริง

วิธีทำ

P	Q	$\sim P$	$P \rightarrow Q$	$\sim P \vee Q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

จากตารางค่าความจริง พบว่าค่าความจริงของ $P \rightarrow Q$ และ $\sim P \vee Q$ มีค่าตรงกัน จึงได้ว่าประพจน์ทั้งสองสมมูลกัน □

นอกจากนี้ สามารถใช้ประพจน์ที่สมมูลกันเพื่อลดรูปประพจน์ที่กำหนด ให้อยู่ในรูปอย่างง่ายโดยยังมีค่าความจริงเหมือนเดิม

ตัวอย่าง 1.8 จงลดรูปประพจน์ $[(P \rightarrow Q) \vee (P \rightarrow R)] \rightarrow (Q \vee R)$ ให้อยู่ในรูปอย่างง่าย

วิธีทำ $[(P \rightarrow Q) \vee (P \rightarrow R)] \rightarrow (Q \vee R)$

$\leftrightarrow [(\sim P \vee Q) \vee (\sim P \vee R)] \rightarrow (Q \vee R)$ (สมบัติอิมพลิเคชัน)

$\leftrightarrow [(Q \vee \sim P) \vee (\sim P \vee R)] \rightarrow (Q \vee R)$ (สมบัติสลับที่ของ $\vee$)

$\leftrightarrow [(Q \vee \sim P \vee \sim P) \vee R)] \rightarrow (Q \vee R)$ (สมบัติจัดกลุ่มของ $\vee$)

$\leftrightarrow [(Q \vee \sim P) \vee R)] \rightarrow (Q \vee R)$ (สมบัติสะท้อนของ $\vee$)

$\leftrightarrow [(\sim P \vee Q) \vee R] \rightarrow (Q \vee R)$ (สมบัติสลับที่ของ $\vee$)

$\leftrightarrow [\sim P \vee (Q \vee R)] \rightarrow (Q \vee R)$ (สมบัติจัดกลุ่มของ $\vee$)

$\leftrightarrow \sim[\sim P \vee (Q \vee R)] \vee (Q \vee R)$ (สมบัติอิมพลิเคชัน)

$\leftrightarrow [\sim(\sim P) \wedge \sim(Q \vee R)] \vee (Q \vee R)$ (กฎของเดอมอร์แกน)

$\leftrightarrow [P \wedge \sim(Q \vee R)] \vee (Q \vee R)$ (สมบัตินิเสธซ้อน)

$\leftrightarrow [P \vee (Q \vee R)] \wedge [\sim(Q \vee R)] \vee (Q \vee R)]$ (สมบัติกระจายของ $\vee$ เหนือ $\wedge$)

$\leftrightarrow (P \vee Q \vee R) \wedge 1$ (สัจนิรันดร์)

$\leftrightarrow P \vee Q \vee R$ (สมบัติข้อ 12)

นั่นคือ $[(P \rightarrow Q) \vee (P \rightarrow R)] \rightarrow (Q \vee R) \leftrightarrow (P \vee Q \vee R)$ □

ประโยคเปิดและตัวบ่งปริมาณ

เมื่อพิจารณาประโยค "$x \geq y$", "$y = x$" และ "$x = y - z$" พบว่าประโยคเหล่านี้**ไม่เป็น**ประพจน์ เนื่องจากไม่สามารถประเมินค่าความจริงเป็นอย่างใดอย่างหนึ่งได้ และเรียกประโยคลักษณะนี้ว่า **ประโยคเปิด** แต่ถ้าได้กำหนดค่าให้กับตัวแปร x และ y ของประโยคเปิด จะทำให้ประโยคเปิดถูกแปลงเป็นประพจน์

จะเห็นได้ว่าประโยคเปิดจะใช้ตัวแปรเป็นตัวแบบ เพื่อแสดงความสัมพันธ์ระหว่างค่าต่าง ๆ และเมื่อมีการแทนค่าตัวแปรจะทำให้ประโยคเปิดกลายเป็นประพจน์ คำสั่งควบคุมของโปรแกรมคอมพิวเตอร์นิยมใช้ประโยคเปิด เช่น

If $x > 10$ **Then**
  $y = 1$
Else
  $y = 0$

ขณะประมวลผลประโยค $x > 10$ จะถูกประเมินค่า โดยอาศัยค่าของตัวแปร x ในขณะนั้น และประโยค $y = 0$ ซึ่งหมายถึงการกำหนดให้ตัวแปร y มีค่าเป็น 0 หรือประโยค $y = 1$ ซึ่งหมายถึงการกำหนดให้ตัวแปร y มีค่าเป็น 1 จะถูกประมวลผลเมื่อ $x > 10$ เป็นจริงหรือเมื่อ $x > 10$ เป็นเท็จตามลำดับ นั่นคือ การที่โปรแกรมจะกำหนดค่าใดให้กับ y ขึ้นกับค่าของ x ในขณะนั้นนั่นเอง

เพื่อความถูกต้องและชัดเจนในการประมวลผล ค่าของ x อาจเป็นจำนวนเต็มหรือจำนวนจริง ทั้งนี้เพื่อหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นเมื่อ x มีค่าใด ๆ ซึ่งอาจไม่เป็นตัวเลข เช่น ในประโยค "Color > 10" ซึ่งไม่สามารถประมวลผลได้ เป็นต้น

ถ้าประโยคเปิดประกอบด้วยตัวแปร n ตัว เมื่อ n เป็นจำนวนนับ เช่น ประโยค "$y = x$" จะได้ n มีค่าเป็น 2 นั่นคือประโยคเปิดประกอบด้วยตัวแปร 2 ตัว จะเขียนแทนประโยคดังกล่าวด้วยสัญลักษณ์ $P(x, y)$ โดยค่าของตัวแปร x และ y สมมติให้เป็น c_1 และ c_2 ตามลำดับ ดังนั้น $P(c_1, c_2)$ จะสามารถหาค่าความจริงได้จึงจัดเป็นประพจน์

ตัวอย่าง 1.9 พิจารณาการเปลี่ยนประโยคเปิดต่อไปนี้ให้เป็นประพจน์

(1) ประโยคเปิด "$x \neq 0$" ซึ่งเขียนแทนด้วย $P(x)$ ถ้ากำหนดให้ x มีค่าเป็น $-4, 0.5$ และ 0 จะได้ประพจน์ $P(-4)$, $P(0.5)$ และ $P(0)$ มีค่าความจริงเป็นจริง, จริง และเท็จ ตามลำดับ

(2) ประโยคเปิด "$y = x$" ซึ่งเขียนแทนด้วย $P(x, y)$ ถ้ากำหนดให้ x และ y มีค่าเป็น 2 และ 3 ตามลำดับ จะได้ $P(2, 3)$ เป็นประพจน์ซึ่งมีค่าความจริงเป็นเท็จ แต่ถ้ากำหนดให้ x และ y มีค่าเป็น 4 จะได้ $P(4, 4)$ มีค่าความจริงเป็นจริง

(3) ประโยคเปิด "$(x \geq 0) \wedge (x \leq 50) \wedge (x + y + z \leq 0)$" ซึ่งเขียนแทนด้วย $P(x, y, z)$ จะได้ว่าประพจน์ $P(26, 50, -120)$, $P(-5, -10, -8)$ และ $P(0, -10, 11)$ มีค่าความจริงเป็นจริง, เท็จ และเท็จ ตามลำดับ □

ในการเปลี่ยนประโยคเปิดให้เป็นเป็นประพจน์ ตัวแปรแต่ละตัวของประโยคเปิดจะต้องถูกแทนค่าด้วยค่าใดค่าหนึ่ง ซึ่งนอกจากการกระทำโดยการกำหนดค่าให้กับตัวแปรแต่ละตัวโดยตรงแล้ว ยังสามารถใช้**ตัวบ่งปริมาณ**กำกับตัวแปรแต่ละตัว เช่น ถ้า $P(x)$ เป็นประโยคเปิดที่มีตัวแปร 1 ตัว ดังนั้น ประโยค

"สำหรับทุก x, $P(x)$"

ซึ่งมีความหมายเดียวกับ

"สำหรับทุกค่าที่เป็นไปได้ของ x ประโยค $P(x)$ เป็นจริง"

เป็นประพจน์

ตัวบ่งปริมาณที่ใช้เป็นส่วนมากมีอยู่ 2 รูปแบบคือ **ตัวบ่งปริมาณสำหรับทุกตัว** เขียนแทนด้วยสัญลักษณ์ $\forall$ และ **ตัวบ่งปริมาณสำหรับตัวมีจริง** เขียนแทนด้วยสัญลักษณ์ $\exists$

ตัวบ่งปริมาณสำหรับทุกตัว

สัญลักษณ์ $\forall$ ใช้แทนข้อความ "สำหรับทุก" ดังนั้น ประโยค

"สำหรับทุก x, $P(x)$" จะเขียนแทนด้วย "$\forall x[P(x)]$"

ถ้าประโยค $P(x)$ เป็นจริงสำหรับทุกค่าของ x แล้ว $\forall x[P(x)]$ เป็นจริง แต่ถ้ามีบางค่า x ที่ทำให้ $P(x)$ เป็นเท็จ แล้ว $\forall x[P(x)]$ เป็นเท็จ

ตัวอย่าง 1.10 พิจารณาค่าความจริงของประพจน์ต่อไปนี้

(1) $\forall x[x < x+1]$, เมื่อ x เป็นจำนวนเต็ม

(2) $\forall x[x = 10]$, เมื่อ x เป็นจำนวนเต็ม

(3) $\forall x \forall y[x+y > x]$, เมื่อ x และ y เป็นจำนวนเต็มบวก

วิธีทำ (1) ประโยค $x < x+1$ เป็นจริงสำหรับทุกค่าของ x ที่เป็นจำนวนเต็ม
ดังนั้น $\forall x[x < x+1]$ เป็นจริง

(2) ประโยค $x = 10$ เป็นเท็จ เพราะ ถ้ากำหนดให้ x มีค่าเป็น 9
ดังนั้น $\forall x[x = 10]$ เป็นเท็จ

(3) $\forall x \forall y[x+y > x]$ เป็นจริง สำหรับทุกค่าของ x และ y ที่เป็นจำนวนเต็มบวก
แต่ถ้า x และ y เป็นจำนวนเต็ม จะได้ว่าประโยค $\forall x \forall y[x+y > x]$ เป็นเท็จ
เช่น แทน $x = 3$ และ $y = -5$ □

ตัวบ่งปริมาณสำหรับตัวมีจริง

ตัวบ่งปริมาณสำหรับตัวมีจริง ใช้สัญลักษณ์ $\exists$ แทนข้อความ "มีบาง" ดังนั้น ประโยค

"มีบาง x, $P(x)$" จะเขียนแทนด้วย "$\exists x[P(x)]$"

ซึ่งมีความหมายว่า ถ้ามี x บางค่าที่ทำให้ $P(x)$ เป็นจริง แล้ว $\exists x[P(x)]$ เป็นจริง แต่ถ้าทุกค่าของ x ทำให้ $P(x)$ เป็นเท็จ แล้ว $\exists x[P(x)]$ เป็นเท็จ

ตัวอย่าง 1.11 พิจารณาค่าความจริงของประพจน์ต่อไปนี้

(1) $\exists x[x < x+1]$, เมื่อ x เป็นจำนวนเต็ม

(2) $\exists x[x = 10]$, เมื่อ x เป็นจำนวนเต็ม

(3) $\exists x[x = x+1]$, เมื่อ x เป็นจำนวนจริง

วิธีทำ (1) และ (2) มีค่าความจริงเป็นจริงเสมอ

(3) มีค่าความจริงเป็นเท็จในทุกกรณี $\square$

นอกจากนี้ยังมีตัวบ่งปริมาณอีกรูปแบบหนึ่งซึ่งใช้สัญลักษณ์ $\exists!$ แทนข้อความ "มีเพียงค่าเดียวเท่านั้น" ดังนั้น ประโยค

"มี x เพียงค่าเดียวเท่านั้น, $P(x)$" จะเขียนแทนด้วย "$\exists! x[P(x)]$"

ซึ่งมีความหมายว่า มี x เพียงค่าเดียวเท่านั้นที่ทำให้ $P(x)$ เป็นจริง แต่ถ้ามีค่า x มากกว่าหนึ่งค่าที่ทำให้ $P(x)$ เป็นจริง แล้ว $\exists! x[P(x)]$ จะเป็นเท็จ

ตัวอย่าง 1.12 กำหนดให้ x เป็นจำนวนนับ พิจารณาค่าความจริงของประพจน์ต่อไปนี้

(1) $\exists! x[x < 1]$

(2) $\exists! x[x = 10]$

(3) $\exists! x[x > 1]$

วิธีทำ (1) $\exists! x[x < 1]$ เป็นเท็จ เพราะไม่มีจำนวนนับใด ๆ ที่มีค่าน้อยกว่า 1

(2) $\exists! x[x = 10]$ เป็นจริง เพราะ x มีค่าเป็น 10 เพียงค่าเดียวเท่านั้น

(3) $\exists! x[x > 1]$ เป็นเท็จ เนื่องจาก $x > 1$ มีค่าเป็นจริง เมื่อกำหนดให้ x เป็นค่าใด ๆ ยกเว้น 1

$\square$

แบบฝึกหัดบทที่ 1

1. จงพิจารณาประโยคต่อไปนี้ ว่าเป็นประพจน์หรือไม่ และถ้าเป็นประพจน์ มีค่าความจริงเป็นอย่างไร
   1.1 ประเทศไทยมี 2 ฤดู คือ ฤดูร้อนและฤดูฝน
   1.2 อธิบายพอสังเขป
   1.3 เส้นที่เชื่อมระหว่างจุด 2 จุดใด ๆ เส้นตรงเป็นเส้นที่สั้นที่สุด
   1.4 $a + b$ สมมูลกับ $b + a$
   1.5 รักมิใช่ดวงดาวที่พราวแสง ไม่ร้อนแรงดั่งแสงอาทิตย์ส่อง

2. กำหนดให้ P, Q และ R เป็นประพจน์ โดย
   P แทน น้อยหน่าไม่ตั้งใจเรียนวิชาคณิตศาสตร์
   Q แทน น้อยหน่าไม่ได้มาสอบไล่วิชาคณิตศาสตร์
   R แทน น้อยหน่าสอบผ่านวิชาคณิตศาสตร์

   จงเขียนประพจน์ต่อไปนี้ในรูปของประโยคข้อความ
   2.1 $P \rightarrow \sim R$
   2.2 $\sim Q \leftrightarrow R$
   2.3 $(\sim P \wedge \sim Q) \rightarrow R$
   2.4 $(P \rightarrow \sim R) \vee (Q \rightarrow \sim R)$
   2.5 $(P \wedge Q) \vee (\sim Q \wedge R)$

3. กำหนดให้ P และ Q เป็นประพจน์ โดย
   P แทน วันนี้อากาศร้อนมาก
   Q แทน วันนี้ฝนตกตอนบ่าย

   จงเขียนประโยคข้อความต่อไปนี้โดยใช้ประพจน์ P และ Q และตัวเชื่อมประพจน์
   3.1 วันนี้อากาศร้อนมาก และมีฝนตกตอนบ่าย
   3.2 วันนี้อากาศร้อนมาก แต่ไม่มีฝนตกตอนบ่าย
   3.3 วันนี้อากาศร้อนมากจนทำให้มีฝนตกในตอนบ่าย
   3.4 วันนี้อากาศไม่ร้อน แต่มีฝนตกในตอนบ่าย
   3.5 ฝนตกในตอนบ่าย ก็ต่อเมื่ออากาศร้อนมาก

4. จงสร้างตารางค่าความจริงของประพจน์ที่กำหนดในแต่ละข้อต่อไปนี้
   4.1 $(P \vee Q) \wedge R$
   4.2 $P \rightarrow \sim Q$
   4.3 $(P \vee Q) \wedge \sim R$
   4.4 $(P \vee \sim Q) \rightarrow Q$
   4.5 $(P \rightarrow Q) \rightarrow (Q \rightarrow P)$
   4.6 $(P \vee Q) \rightarrow (P \wedge Q)$
   4.7 $(P \leftrightarrow Q) \vee (\sim Q \leftrightarrow R)$
   4.8 $(P \leftrightarrow Q) \vee (\sim P \leftrightarrow Q)$

4.9 $(P \rightarrow Q) \wedge (\sim P \rightarrow R)$ 4.10 $(P \leftrightarrow Q) \leftrightarrow (R \leftrightarrow S)$

5. พิจารณาส่วนของโปรแกรมต่อไปนี้

```
If (x ≤ 40) Then
    grade = "F"
If (x > 40) and (x ≤ 60) Then
    grade = "D"
If (x > 60) and (x ≤ 70) Then
    grade = "C"
If (x > 70) and (x ≤ 80) Then
    grade = "B"
Else
    grade = "A"
```

จงหาค่าของตัวแปร grade เมื่อ

5.1 x = 35 5.2 x = 60

5.3 x = 72 5.4 x = 100

5.5 x = 300

6. กำหนดให้เมื่อเริ่มต้นตัวแปร x มีค่าเท่ากับ 1
จงหาค่าของตัวแปร x เมื่อประโยคต่อไปนี้ทำงานเสร็จลง

6.1 **If** $(3 > 1)$ **Then** $x = x * 2$

6.2 **If** $(1 + 0 = 1) \vee (2 + 2 = 2)$ **Then** $x = x + 1$

6.3 **If** $(1 + 0 = 1) \rightarrow (1 + 5 = 10)$ **Then** $x = x * 2$

6.4 **If** $(3 > 1) \wedge (1 + 5 = 10)$ **Then** $x = x + 1$

6.5 **If** $(x \geq 1) \wedge (1 + 0 = 1)$ **Then** $x = x * 2$

7. จงพิจารณาว่าประพจน์ที่กำหนดในแต่ละข้อต่อไปนี้เป็นสัจนิรันดร์ หรือข้อขัดแย้ง หรือไม่ใช่ทั้งสองอย่าง

7.1 $P \vee \sim P$ 7.2 $P \wedge \sim P$

7.3 $P \rightarrow \sim(\sim P)$ 7.4 $(P \rightarrow Q) \leftrightarrow (\sim Q \rightarrow \sim P)$

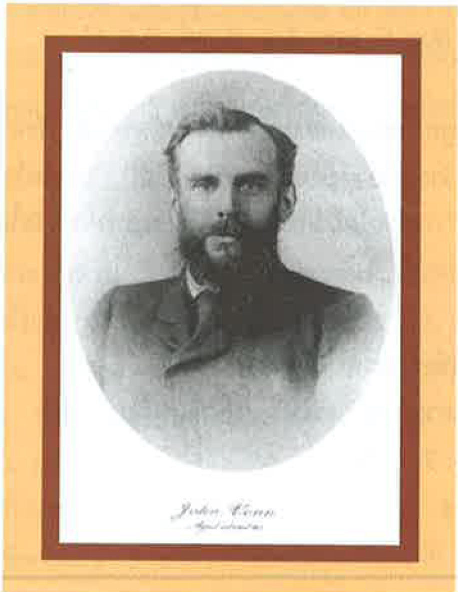
7.5 $(P \rightarrow Q) \wedge (Q \rightarrow P)$

8. จงหาประพจน์ที่ใช้เฉพาะตัวเชื่อม $\wedge$ และตัวเชื่อม $\vee$ ที่สมมูลกับประพจน์ในแต่ละข้อต่อไปนี้

8.1 $P \vee Q \vee \sim R$ 8.2 $P \vee [(\sim Q \wedge R) \rightarrow P]$

9. จงเขียนโปรแกรมเพื่อสร้างตารางค่าความจริงของประพจน์ที่ประกอบด้วยตัวแปรประพจน์ 4 ตัว คือ P, Q, R และ S

เซต



เวนน์, จอห์น
ค.ศ. 1824 – 1923 , อังกฤษ

ความหมายของเซต

เซต หมายถึง กลุ่มของสิ่งต่าง ๆ และเรียกสิ่งของต่าง ๆ ที่อยู่ในเซตว่า **สมาชิก**

กำหนดให้ x แทนสิ่งสิ่งหนึ่ง และ S แทนเซต ถ้า x เป็นสมาชิกของ S เราสามารถเขียนแทนด้วย $x \in S$ แต่ถ้า x ไม่เป็นสมาชิกของ S สามารถเขียนแทนด้วย $\sim(x \in S)$ หรือ $x \notin S$ การ "เป็นสมาชิกของ" เป็นความสัมพันธ์ระหว่างสมาชิก x และเซต S ซึ่งความสัมพันธ์นี้เป็นพื้นฐานเบื้องต้นที่สำคัญเมื่อกล่าวถึงเซต

จากบทนิยาม 2.1 จะพบว่า เซตที่เขียนแทนด้วย $\{1, 2, 3\}$ เป็นเซตเดียวกันกับเซตที่เขียนแทนด้วย $\{3, 1, 2\}$ ในทำนองเดียวกัน เซตที่เขียนแทนด้วย $\{1, 1, 1, 2, 3, 3\}$ และ $\{1, 2, 2, 3\}$ เป็นเซตเดียวกันกับเซตที่เขียนแทนด้วย $\{1, 2, 3\}$ นั่นคือ ลำดับของสมาชิกภายในเซตและการซ้ำกันของสมาชิกภายในเซตไม่มีผลต่อสมบัติการเท่ากันของเซต

ตัวอย่าง 2.5 ให้ $A = \{1, 3, 5, 7, 9\}$ และ $B = \{x \mid x$ เป็นจำนวนคี่ที่อยู่ระหว่าง 0 ถึง $10\}$
จากบทนิยาม 2.1 เราได้ว่า $A = B$ □

บทนิยาม 2.2 ให้ A และ B เป็นเซตใด ๆ เซต A เป็น**สับเซต**ของเซต B เขียนแทนด้วย $A \subseteq B$ ก็ต่อเมื่อ ทุกสมาชิกของเซต A เป็นสมาชิกของเซต B
นั่นคือ $A \subseteq B \leftrightarrow \forall x[x \in A \rightarrow x \in B]$

ถ้า $A \subseteq B$ จะกล่าวได้ว่า เซต B เป็น**ซูเปอร์เซต**ของเซต A
ถ้า $A \subseteq B$ และ $A \neq B$ จะเรียกเซต A ว่าเป็น**สับเซตแท้**ของ B เขียนแทนด้วย $A \subset B$
ถ้าเซต A ไม่เป็นสับเซตของเซต B จะเขียนแทนด้วย $A \nsubseteq B$

ตัวอย่าง 2.6 พิจารณาการเป็นสับเซตและสับเซตแท้ของเซตที่กำหนดให้ต่อไปนี้

(1) ให้ A เป็นเซตของวรรณคดีไทย และ $B = \{$รามเกียรติ์, พระอภัยมณี$\}$
ดังนั้น $B \subset A$

(2) ให้ $A = \{x \mid x$ เป็นชื่อเดือนที่ลงท้ายด้วย “คม”$\}$
และ $B = \{y \mid y$ เป็นชื่อเดือนที่มี 31 วัน$\}$
ดังนั้น $A \subseteq B$ และ $B \subseteq A$

(3) เซตของจำนวนเต็มบวกเป็นสับเซตแท้ของเซตของจำนวนเต็ม

(4) $\{2, 4, 6, 8\} \subset \{x \mid x$ เป็นจำนวนเต็มซึ่ง $0 \leq x \leq 10\}$

(5) $\{2, 4, 6, 8\} \subseteq \{x \mid x$ เป็นจำนวนคู่ซึ่ง $0 < x < 10\}$ □

หมายเหตุ จะกล่าวว่า $\mathscr{U}$ เป็น**เอกภพสัมพัทธ์** ก็ต่อเมื่อ $\mathscr{U}$ เป็นเซตที่กำหนดขึ้นโดยมีข้อตกลงว่าจะไม่กล่าวถึงสิ่งใดที่นอกเหนือไปจากสมาชิกของ $\mathscr{U}$
จะเห็นได้โดยง่ายว่า ทุก ๆ เซต A เป็นสับเซตของ $\mathscr{U}$ ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.1 ให้ $\mathscr{U}$ เป็นเอกภพสัมพัทธ์ และ A เป็นเซต แล้ว $A \subseteq \mathscr{U}$

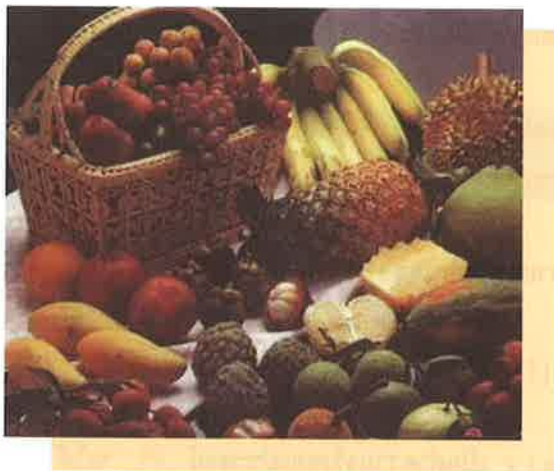
จากตัวอย่าง 2.6 ข้อ (5) พบว่าในทางกลับกัน $\{x \mid x$ เป็นจำนวนคู่ซึ่ง $0 < x < 10\} \subseteq \{2, 4, 6, 8\}$ นั่นคือ $\{x \mid x$ เป็นจำนวนคู่ซึ่ง $0 < x < 10\} = \{2, 4, 6, 8\}$

ดังนั้นสามารถสรุปได้ว่า A และ B เป็นสับเซตซึ่งกันและกัน ก็ต่อเมื่อ A และ B เป็นเซตเดียวกัน หรือเป็นเซตที่เท่ากัน ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.2 ให้ A และ B เป็นเซตใด ๆ
$A = B$ ก็ต่อเมื่อ $A \subseteq B$ และ $B \subseteq A$

จากทฤษฎีบทเกี่ยวกับการเท่ากันของเซต 2 เซต จะได้ว่า $A \subseteq A$ เมื่อ A เป็นเซตใด ๆ

ทฤษฎีบท 2.3 ให้ A, B และ C เป็นเซต
ถ้า $A \subseteq B$ และ $B \subseteq C$ แล้ว $A \subseteq C$



ตัวอย่าง 2.7 เนื่องจาก {มะละกอ, ส้มโอ} $\subseteq$ {มะม่วง, มะละกอ, กล้วย, ส้มโอ, สับปะรด}
และ {มะม่วง, มะละกอ, กล้วย, ส้ม} $\subseteq$ {ขนุน, มะม่วง, มะละกอ, กล้วย, ส้ม}
ดังนั้น {มะละกอ, ส้มโอ} $\subseteq$ {ขนุน, มะม่วง, มะละกอ, กล้วย, ส้มโอ} □

บทนิยาม 2.3 เซตที่ไม่มีสมาชิกอยู่เลย เรียกว่า **เซตว่าง** เขียนแทนด้วย $\varnothing$ หรือ $\{\}$
นั่นคือ $n(\varnothing) = 0$

ตัวอย่าง 2.8 ให้ $A = \{x \mid x$ เป็นจำนวนคู่ซึ่ง $0 \leq x < 10$ และหารด้วย 5 ลงตัว$\}$
จะได้ว่า $n(A) = 0$ ดังนั้น $A = \varnothing$ □

ทฤษฎีบท 2.4 ให้ A เป็นเซต แล้ว $\varnothing \subseteq A$

สังเกตว่า $\varnothing$ ไม่เหมือนกับ $\{\varnothing\}$ เพราะว่า $\varnothing$ เป็นเซตที่ไม่มีสมาชิกอยู่เลย แต่ $\{\varnothing\}$ มีสมาชิก 1 ตัวคือ $\varnothing$ และเซตต่อไปนี้เป็นเซตที่แตกต่างกันทั้งหมด

$$\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\{\{\varnothing\}\}\}, \{\{\{\{\varnothing\}\}\}\}, \ldots$$

โดยที่เซตทุกเซตยกเว้นเซตแรกประกอบด้วยสมาชิก 1 ตัว

ตัวอย่าง 2.9 พิจารณาการเป็นสับเซตและการเป็นสมาชิกของเซตที่กำหนดให้ต่อไปนี้

(1) สับเซตของ $\{2, 4\}$ ประกอบด้วย $\varnothing, \{2\}, \{4\}, \{2. 4\}$

สังเกตว่า $\{2\} \subseteq \{2, 4\}$ และ $2 \in \{2, 4\}$ และ $\varnothing \subseteq \{2, 4\}$ แต่ $\varnothing \notin \{2, 4\}$

(2) สับเซตของ $\{8\}$ ประกอบด้วย $\varnothing, \{8\}$

(3) สับเซตของเซตของแม่สี {สีแดง, สีเหลือง, สีน้ำเงิน} ประกอบด้วย $\varnothing$, {สีแดง}, {สีเหลือง}, {สีน้ำเงิน}, {สีแดง, สีเหลือง}, {สีแดง, สีน้ำเงิน}, {สีเหลือง, สีน้ำเงิน}, {สีแดง, สีเหลือง, สีน้ำเงิน}

□

ข้อสังเกต เซตที่มีจำนวนสมาชิก n ตัว จะมีจำนวนสับเซตทั้งหมด 2^n เซต

บทนิยาม 2.4 ให้ A เป็นเซตใด ๆ **เพาเวอร์เซต**ของ A เขียนแทนด้วย $P(A)$ หมายถึงเซตของสับเซตทั้งหมดของ A

ตัวอย่าง 2.10 พิจารณาการหาเพาเวอร์เซตของเซตที่กำหนดให้ต่อไปนี้

(1) ให้ $A = \varnothing$ จะได้ $P(A) = \{\varnothing\}$

(2) ให้ $A = \{1, 3, 5\}$ จะได้ $P(A) = \{\varnothing, \{1\}, \{3\}, \{5\}, \{1, 3\}, \{1, 5\}, \{3, 5\}, \{1, 3, 5\}\}$

(3) ให้ $A = \{x \mid x$ เป็นค่าความจริงของประพจน์ $P\}$ จะได้

$P(A) = \{\varnothing$, {จริง}, {เท็จ}, {จริง, เท็จ}$\}$

(4) ให้ $A = \{\varnothing, \{\varnothing\}\}$ จะได้ $P(A) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$ □

ข้อสังเกต ถ้าเซต A เป็นเซตจำกัดที่มีสมาชิก n ตัว แล้ว $P(A)$ เป็นเซตจำกัดเช่นกันและมีสมาชิก 2^n ตัว แต่ถ้าเซต A เป็นเซตอนันต์ แล้ว $P(A)$ ก็จะเป็นเซตอนันต์

การดำเนินการบนเซต

ในหัวข้อนี้จะกล่าวถึงการสร้างเซตใหม่ขึ้นจากเซตเดิม โดยการดำเนินการยูเนียน อินเตอร์เซกชัน และผลต่างของเซต ดังบทนิยามต่อไปนี้

บทนิยาม 2.5 ให้ A และ B เป็นเซตใด ๆ

1. **ยูเนียน**ของ A และ B เขียนแทนด้วย $A \cup B$ หมายถึงเซต

$$A \cup B = \{x \mid x \in A \ \vee \ x \in B\}$$

2. **อินเตอร์เซกชัน**ของ A และ B เขียนแทนด้วย $A \cap B$ หมายถึงเซต

$$A \cap B = \{x \mid x \in A \ \wedge \ x \in B\}$$

3. **ผลต่าง**ของ A และ B เขียนแทนด้วย $A - B$ หมายถึงเซต

$$A - B = \{x \mid x \in A \ \wedge \ x \notin B\}$$

ตัวอย่าง 2.11 ให้ $A = \{0, 2, 4, 6, 8\}$ และ $B = \{1, 2, 3, 4\}$ จะได้

(1) $A \cup B = \{0, 1, 2, 3, 4, 6, 8\}$

(2) $A \cap B = \{2, 4\}$

(3) $A - B = \{0, 6, 8\}$

(4) $B - A = \{1, 3\}$

(5) $(A \cup B) - A = \{1, 2, 3, 4\}$

(6) $(A \cap B) \cap (A - B) = \varnothing$

(7) $(A - B) \cup (B - A) = \{0, 1, 3, 6, 8\}$ □

ตัวอย่าง 2.12 ให้ A = {คณิตศาสตร์, เคมี, ชีววิทยา, ฟิสิกส์, ภาษาอังกฤษ}

และ B = {คณิตศาสตร์, ภาษาอังกฤษ, ภาษาไทย, สังคมศึกษา} จะได้

(1) $A \cup B$ = {คณิตศาสตร์, เคมี, ชีววิทยา, ฟิสิกส์, ภาษาอังกฤษ, ภาษาไทย, สังคมศึกษา}

(2) $A \cap B$ = {คณิตศาสตร์, ภาษาอังกฤษ}

(3) $A - B$ = {เคมี, ชีววิทยา, ฟิสิกส์}

(4) $B - A$ = {ภาษาไทย, สังคมศึกษา} □

บทนิยาม 2.6 ให้ A และ B เป็นเซตใด ๆ

ถ้า $A \cap B = \varnothing$ แล้วเซต A และเซต B เป็น**เซตไม่มีส่วนร่วม**

ตัวอย่าง 2.13 ให้ $A = \{a, b, c, \ldots, z\}$ และ B = {ก, ข, ค, ..., ฮ} จะเห็นได้ว่า $A \cap B = \varnothing$ ดังนั้น A และ B เป็นเซตไม่มีส่วนร่วม □

การดำเนินการยูเนียนและการดำเนินการอินเตอร์เซกชันมี**สมบัติการสลับที่** **สมบัติการจัดกลุ่ม** และ**สมบัติการกระจาย** ดังนี้

ทฤษฎีบท 2.5 ให้ A, B และ C เป็นเซตใด ๆ

สมบัติการสลับที่

(i) $A \cup B = B \cup A$

(ii) $A \cap B = B \cap A$

สมบัติการจัดกลุ่ม

(iii) $(A \cup B) \cup C = A \cup (B \cup C)$

(iv) $(A \cap B) \cap C = A \cap (B \cap C)$

สมบัติการกระจาย

(v) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(vi) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

ประพจน์ที่เกี่ยวกับการดำเนินการต่าง ๆ บนเซต ที่เป็นจริง มีดังนี้

ทฤษฎีบท 2.6 ให้ A, B, C และ D เป็นเซตใด ๆ

(i) $A \cup A = A$

(ii) $A \cap A = A$

(iii) $A \cup \varnothing = A$

(iv) $A \cap \varnothing = \varnothing$

(v) $A \cup \mathscr{U} = \mathscr{U}$

(vi) $A \cap \mathscr{U} = A$

(vii) $A - B \subseteq A$

(viii) ถ้า $A \subseteq B$ และ $C \subseteq D$ แล้ว $A \cup C \subseteq B \cup D$

(ix) ถ้า $A \subseteq B$ และ $C \subseteq D$ แล้ว $A \cap C \subseteq B \cap D$

(x) $A \subseteq A \cup B$

(xi) $A \cap B \subseteq A$

(xii) ถ้า $A \subseteq B$ แล้ว $A \cup B = B$

(xiii) ถ้า $A \subseteq B$ แล้ว $A \cap B = A$

(xiv) $A - \varnothing = A$

(xv) $A \cap (B - A) = \varnothing$

(xvi) $A \cup (B - A) = A \cup B$

(xvii) $A - (B \cup C) = (A - B) \cap (A - C)$

(xviii) $A - (B \cap C) = (A - B) \cup (A - C)$

บทนิยาม 2.7 ให้ $\mathscr{U}$ เป็นเอกภพสัมพัทธ์ และ A เป็นสับเซตของ $\mathscr{U}$ **คอมพลีเมนต์ของ** A เขียนแทนด้วย A' หมายถึงเซต

$$A' = \mathscr{U} - A = \{x \mid x \notin A\}$$

ตัวอย่าง 2.14 จงหาคอมพลีเมนต์ของเซตที่กำหนดให้

(1) ให้ $\mathscr{U} =$ {ม่วง, คราม, น้ำเงิน, เขียว, เหลือง, แสด, แดง}
และ $A =$ {แดง, เหลือง, น้ำเงิน} จะได้ $A' =$ {ม่วง, คราม, เขียว, แสด}

(2) ให้ $\mathscr{U} = \{1, 3, 5, 7, 9\}$ และ $A = \{1, 3\}$ จะได้ $A' = \{5, 7, 9\}$

(3) ให้ $\mathscr{U} = \{x \mid x$ เป็นจำนวนเต็ม$\}$ และ $A = \{y \mid y$ เป็นจำนวนเต็มคี่$\}$
จะได้ $A' = \{z \mid z$ เป็นจำนวนเต็มคู่$\}$ □

ทฤษฎีบท 2.7 ให้ $\mathscr{U}$ เป็นเอกภพสัมพัทธ์ และ A เป็นสับเซตของ $\mathscr{U}$ จะได้ว่า

(*i*) $A \cup A' = \mathscr{U}$

(*ii*) $A \cap A' = \varnothing$

ตัวอย่าง 2.15 ให้ $\mathscr{U} =$ {จันทร์, อังคาร, พุธ, พฤหัสบดี, ศุกร์, เสาร์, อาทิตย์}
และ $A =$ {จันทร์, อังคาร, พุธ, พฤหัสบดี, ศุกร์}
ดังนั้น $A' =$ {เสาร์, อาทิตย์}
จะเห็นได้ว่า $A \cup A' =$ {จันทร์, อังคาร, พุธ, พฤหัสบดี, ศุกร์, เสาร์, อาทิตย์} $= \mathscr{U}$
และ $A \cup A' = \varnothing$ □

ทฤษฎีบท 2.8 ให้ $\mathscr{U}$ เป็นเอกภพสัมพัทธ์ จะได้ว่า

(*i*) $\mathscr{U} = \varnothing$

(*ii*) $\varnothing' = \mathscr{U}$

ทฤษฎีบท 2.9 ให้ A และ B เป็นเซตใด ๆ ซึ่ง $A \subseteq \mathscr{U}$ และ $B \subseteq \mathscr{U}$ จะได้ว่า
$B = A'$ ก็ต่อเมื่อ $A \cup B = \mathscr{U}$ และ $A \cap B = \varnothing$

ตัวอย่าง 2.16 ให้ $\mathscr{U} =$ {เบสิก, โคบอล, ฟอร์แทรน, ปาสคาล, ซี, จาวา}
$A =$ {เบสิก, โคบอล, ฟอร์แทรน}
และ $B =$ {ปาสคาล, ซี, จาวา}
จะเห็นได้ว่า $A \subseteq \mathscr{U}$ และ $B \subseteq \mathscr{U}$ และ
$A' =$ {ปาสคาล, ซี, จาวา} $= B$ ก็ต่อเมื่อ
$A \cup B =$ {เบสิก, โคบอล, ฟอร์แทรน, ปาสคาล, ซี, จาวา} $= \mathscr{U}$ และ
$A \cap B = \varnothing$ □

ทฤษฎีบท 2.10 ให้ $\mathscr{U}$ เป็นเอกภพสัมพัทธ์ และ A เป็นสับเซตของ $\mathscr{U}$ จะได้ว่า $(A')' = A$

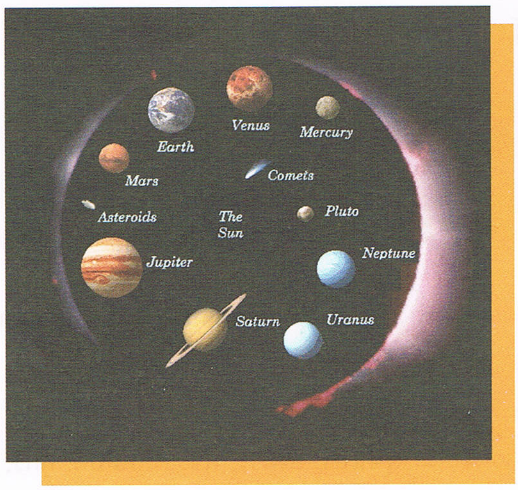
ตัวอย่าง 2.17 ให้ $\mathscr{U}$ = {ดาวพุธ, ดาวศุกร์, โลก, ดาวอังคาร, ดาวพฤหัสบดี, ดาวเสาร์, ดาวยูเรนัส, ดาวเนปจูน, ดาวพลูโต}

และ A = {ดาวพุธ, ดาวศุกร์, โลก}

จะเห็นได้ว่า $A \subseteq$ U และ

A' = {ดาวอังคาร, ดาวพฤหัสบดี, ดาวเสาร์, ดาวยูเรนัส, ดาวเนปจูน, ดาวพลูโต}

ดังนั้น $(A')'$ = {ดาวพุธ, ดาวศุกร์, โลก} $= A$ □



ทฤษฎีบท 2.11 *กฎเดอมอร์แกน*

ให้ A และ B เป็นเซตใด ๆ ซึ่ง $A \subseteq \mathscr{U}$ และ $B \subseteq \mathscr{U}$ จะได้ว่า

(i) $(A \cup B)' = A' \cap B'$

(ii) $(A \cap B)' = A' \cup B'$

ตัวอย่าง 2.18 ให้ $\mathscr{U}$ = {เรือ, รถไฟ, รถไฟฟ้า, รถยนต์, รถบรรทุก, รถมอเตอร์ไซค์, เครื่องบิน, เฮลิคอปเตอร์}

A = {เรือ}

และ B = {รถไฟ, รถไฟฟ้า, รถยนต์, รถบรรทุก, รถมอเตอร์ไซค์}

เราจะได้ว่า

$A \cup B$ = {เรือ, รถไฟ, รถไฟฟ้า, รถยนต์, รถบรรทุก, รถมอเตอร์ไซค์}

$(A \cup B)'$ = {เครื่องบิน, เฮลิคอปเตอร์}

A' = {รถไฟ, รถไฟฟ้า, รถยนต์, รถบรรทุก, รถมอเตอร์ไซค์, เครื่องบิน, เฮลิคอปเตอร์}

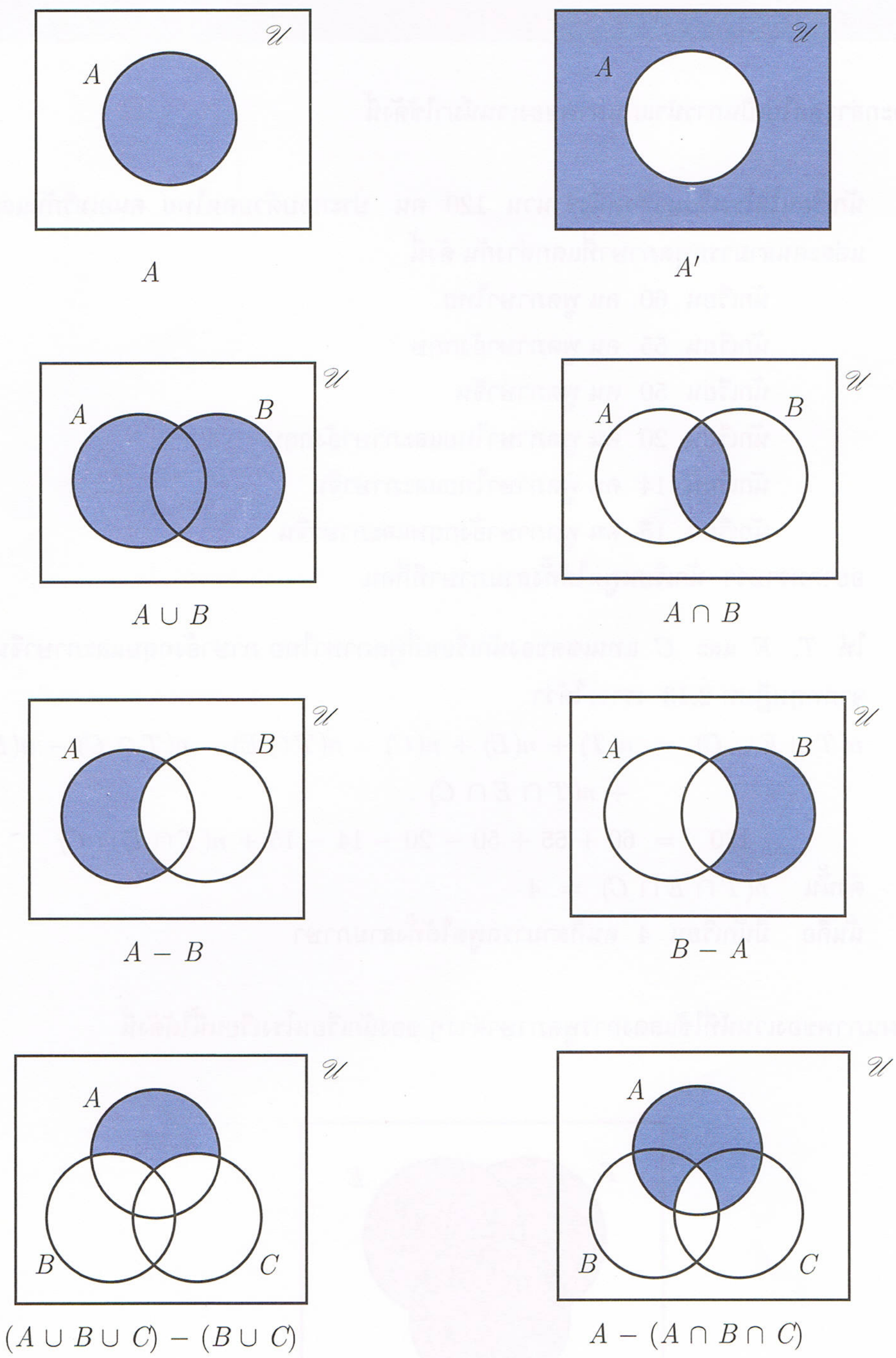
B' = {เรือ, เครื่องบิน, เฮลิคอปเตอร์}

$A' \cap B'$ = {เครื่องบิน, เฮลิคอปเตอร์}

ดังนั้น $(A \cup B)' = A' \cap B'$ □

แผนภาพของเวนน์

ในหัวข้อนี้จะแสดงการดำเนินการต่าง ๆ บนเซตด้วย**แผนภาพของเวนน์** โดยพื้นที่ของการแรเงา หมายถึง พื้นที่ของเซตที่ระบุ ทั้งนี้เซตทั้งหมดนิยามอยู่บนเอกภพสัมพัทธ์ $\mathscr{U}$ แสดงดังรูป 2.1



รูป 2.1 แสดงแผนภาพของเวนน์

ทฤษฎีบท 2.12 ให้ A และ B เป็นเซตจำกัด แล้ว $A \cup B$ และ $A \cap B$ เป็นเซตจำกัด และได้ว่า

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

ทฤษฎีบท 2.13 ให้ A, B และ C เป็นเซตจำกัด แล้ว $A \cup B \cup C$ เป็นเซตจำกัด และได้ว่า

$$\begin{aligned} n(A \cup B \cup C) &= n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) \\ &\quad + n(A \cap B \cap C) \end{aligned}$$

ตัวอย่างที่จะกล่าวต่อไปเป็นการนำแผนภาพของเวนน์มาใช้ดังนี้

ตัวอย่าง 2.20 นักเรียนในโรงเรียนแห่งหนึ่งจำนวน 120 คน ประกอบด้วยคนไทย คนอเมริกันและคนจีน นักเรียนแต่ละคนสามารถพูดภาษาที่แตกต่างกัน ดังนี้

นักเรียน 60 คน พูดภาษาไทย
นักเรียน 55 คน พูดภาษาอังกฤษ
นักเรียน 50 คน พูดภาษาจีน
นักเรียน 20 คน พูดภาษาไทยและภาษาอังกฤษ
นักเรียน 14 คน พูดภาษาไทยและภาษาจีน
นักเรียน 15 คน พูดภาษาอังกฤษและภาษาจีน

อยากทราบว่า นักเรียนพูดได้ทั้งสามภาษาทีกี่คน

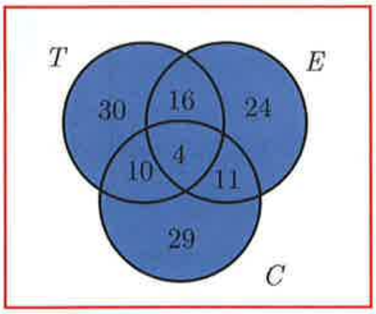
วิธีทำ ให้ T, E และ C แทนเซตของนักเรียนที่พูดภาษาไทย ภาษาอังกฤษและภาษาจีน ตามลำดับ จากทฤษฎีบท 2.13 เราจะได้ว่า

$$\begin{aligned} n(T \cup E \cup C) &= n(T) + n(E) + n(C) - n(T \cap E) - n(T \cap C) - n(E \cap C) \\ &\quad + n(T \cap E \cap C) \\ 120 &= 60 + 55 + 50 - 20 - 14 - 15 + n(T \cap E \cap C) \end{aligned}$$

ดังนั้น $n(T \cap E \cap C) = 4$

นั่นคือ มีนักเรียน 4 คนที่สามารถพูดได้ทั้งสามภาษา □

ข้อสังเกต แผนภาพของเวนน์ที่ใช้แสดงการพูดภาษาต่าง ๆ ของนักเรียนโรงเรียนนี้ได้ดังนี้



จะเห็นว่า

จำนวนนักเรียนที่พูดภาษาไทยและภาษาอังกฤษ แต่ไม่พูดภาษาจีน $= 20 - 4 = 16$ คน

จำนวนนักเรียนที่พูดภาษาไทยและภาษาจีน แต่ไม่พูดภาษาอังกฤษ $= 14 - 4 = 10$ คน

จำนวนนักเรียนที่พูดภาษาอังกฤษและภาษาจีน แต่ไม่พูดภาษาไทย $= 15 - 4 = 11$ คน

จำนวนนักเรียนที่พูดภาษาไทยได้อย่างเดียว $= 60 - 16 - 4 - 10 = 30$ คน

จำนวนนักเรียนที่พูดภาษาอังกฤษได้อย่างเดียว $= 55 - 16 - 4 - 11 = 24$ คน

จำนวนนักเรียนที่พูดภาษาจีนได้อย่างเดียว $= 50 - 10 - 4 - 11 = 25$ คน

จำนวนนักเรียนที่สามารถพูดได้เพียงหนึ่งภาษา $= 30 + 24 + 25 = 79$ คน

จำนวนนักเรียนที่สามารถพูดได้สองภาษา $= 16 + 11 + 10 = 37$ คน

แบบฝึกหัดบทที่ 2

1. จงเขียนสัญลักษณ์แทนเซตต่อไปนี้โดยการแจกแจงสมาชิกที่อยู่ในเซต
   1.1 เซตของจำนวนที่เป็นพหุคูณของน้ำหนักของนักเรียน
   1.2 เซตของวิชาที่นักเรียนชอบเรียนมากที่สุด 3 อันดับแรก
   1.3 เซตของรายการอาหารเช้าที่นักเรียนรับประทานใน 1 สัปดาห์
   1.4 เซตของ URL ที่นักเรียนใช้สำหรับค้นหาความรู้ต่าง ๆ
   1.5 เซตของชื่อเพื่อนในห้องเรียนที่มีพยัญชนะต้นของชื่อซ้ำกับพยัญชนะต้นของนามสกุล

2. จงเขียนสัญลักษณ์แทนเซตต่อไปนี้โดยการระบุสมบัติสมาชิกที่อยู่ในเซต
   2.1 $\{1, 2, 3, 4, 6, 8, 12, 24\}$
   2.2 $\{0, 1, 4, 9, 16, 25, \ldots\}$
   2.3 {นนทบุรี, ปทุมธานี, สมุทรปราการ}
   2.4 {ก, จ, ด, ต, ฎ, ฏ, บ, ป, อ}
   2.5 $\varnothing$

3. จงเขียนประโยคต่อไปนี้โดยใช้สัญลักษณ์ของเซต
   3.1 1 ไม่เป็นสมาชิกของเซต A
   3.2 โดราเอมอนเป็นสมาชิกของเซต B
   3.3 สุดสาครและหนุมานเป็นสมาชิกของเซต C
   3.4 เซต D ประกอบด้วยสมาชิกทั้งหมดในเซต A
   3.5 เซต E ประกอบด้วยสมาชิกที่ไม่ซ้ำกันของเซต A และ B
   3.6 เซต F ประกอบด้วยสมาชิกที่ไม่อยู่ในเซต A แต่อยู่ในเซต B และ C

4. จงยกตัวอย่างเซตที่มีสมบัติต่อไปนี้
   4.1 A และ B เป็นเซตที่ไม่มีสมาชิกร่วมกัน
   4.2 A และ B เป็นเซตซึ่ง B เป็นสับเซตแท้ของ A
   4.3 เซตที่มีจำนวนสมาชิกเป็นศูนย์
   4.4 A และ B เป็นเซตที่มีจำนวนสมาชิกเท่ากัน
   4.5 A, B และ C เป็นเซตที่ทั้งสามเซตมีสมาชิกซึ่งมีสมบัติต่างกัน

5. จงเขียนเพาเวอร์เซตของเซตต่อไปนี้
   5.1 {ศูนย์, 0}
   5.2 $\{0, 1, 2, 2, 5, 0\}$
   5.3 {00, 01, 10, 11}
   5.4 {ฟักทอง, มะละกอ, ส้ม}
   5.5 เซตของวันในสัปดาห์ที่ไม่มีสระ

6. กำหนดให้เซต A, B และ C เป็นสมาชิกของเซตเอกภพสัมพัทธ์ $\mathscr{U}$
   จงเขียนแผนภาพของเวนน์เพื่อแทนเซตต่อไปนี้
   6.1 $A' \cap B \cap C$
   6.2 $A \cap B' \cap C$
   6.3 $A \cap B \cap C'$
   6.4 $A' \cup B \cup C$
   6.5 $A' \cup B'$

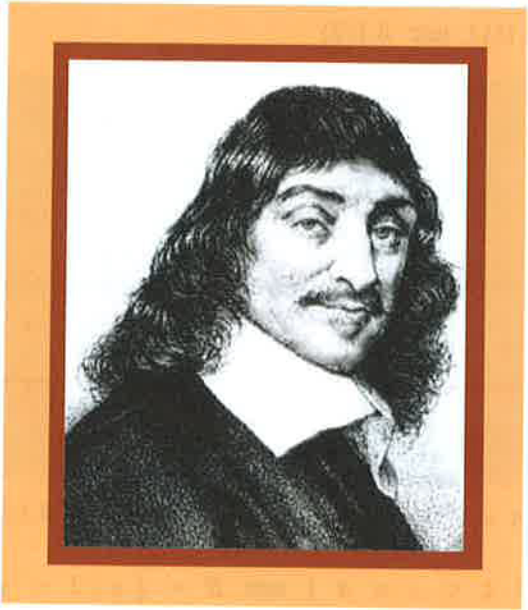
7. จากการสำรวจข้อมูลโดยการสอบถามนักเรียนจำนวน 100 คน ว่าแต่ละคนสนใจเรียนวิชาใดบ้างใน 3 วิชาต่อไปนี้ คือ วิชาประวัติศาสตร์ไทย วิชาธรรมชาติและสิ่งแวดล้อม และวิชาโบราณคดี พบว่า
   นักเรียน 45 คนสนใจเรียนวิชาประวัติศาสตร์ไทย
   นักเรียน 38 คนสนใจเรียนวิชาธรรมชาติและสิ่งแวดล้อม
   นักเรียน 21 คนสนใจเรียนวิชาโบราณคดี
   นักเรียน 18 คนสนใจเรียนวิชาประวัติศาสตร์ไทยและวิชาธรรมชาติและสิ่งแวดล้อม
   นักเรียน 9 คนสนใจเรียนวิชาประวัติศาสตร์ไทยและวิชาโบราณคดี
   นักเรียน 5 คนสนใจเรียนวิชาวิชาธรรมชาติและสิ่งแวดล้อมและวิชาโบราณคดี
   7.1 จงเขียนแผนภาพของเวนน์เพื่อแสดงผลการสำรวจข้างต้น โดยกำหนดให้
   เซต A แทนเซตของจำนวนนักเรียนที่สนใจเรียนวิชาประวัติศาสตร์ไทย
   เซต B แทนเซตของจำนวนนักเรียนที่สนใจเรียนวิชาธรรมชาติและสิ่งแวดล้อม
   เซต C แทนเซตของจำนวนนักเรียนที่สนใจเรียนวิชาโบราณคดี
   7.2 จงหาว่ามีนักเรียนจำนวนกี่คนที่สนใจเรียนเพียงวิชาเดียวเท่านั้น
   7.3 จงหาว่ามีนักเรียนจำนวนกี่คนที่สนใจเรียนเพียง 2 วิชาเท่านั้น
   7.4 จงหาว่ามีนักเรียนจำนวนกี่คนที่สนใจเรียนทั้ง 3 วิชา

8. จงพิสูจน์ทฤษฎีบทต่าง ๆ ต่อไปนี้
   8.1 ทฤษฎีบท 2.5 ข้อ (ii), (iv) และ (vi)
   8.2 ทฤษฎีบท 2.6 ข้อ (ii), (iii), (v), (vi), $(viii)$, (x), (xi), (xii), (xv), (xvi) และ $(xvii)$
   8.3 ทฤษฎีบท 2.10
   8.4 ทฤษฎีบท 2.11 ข้อ (ii)

9. กำหนดให้มีเซต A และ B เป็นเซตใด ๆ จงเขียนโปรแกรมเพื่อทำงานดังต่อไปนี้
   9.1 พิจารณาว่าเซต A และ B เป็นเซตที่เท่ากัน
   9.2 พิจารณาว่าเซต A เป็นซูเปอร์เซตของเซต B หรือเซต B เป็นซูเปอร์เซตของเซต A
   9.3 พิจารณาว่า m เป็นสมาชิกของเซตหรือไม่
   9.4 หาผลต่างของเซต A และ B
   9.5 หาจำนวนสมาชิกของเพาเวอร์เซตของเซต A (หรือ $n(P(A))$)

10. กำหนดให้สมาชิกของเซต A เป็นจำนวนเต็มบวกที่มีค่าไม่เกิน 100 จงเขียนโปรแกรมเพื่อสร้างเซตใหม่โดยคัดลอกสมาชิกจากเซต A ที่มีค่าตั้งแต่ x ถึง y เมื่อ x และ y เป็นจำนวนเต็มบวกที่มีค่าไม่เกิน 100

ความสัมพันธ์และฟังก์ชัน



เดส์การ์ต, เรอเน
ค.ศ. 1596 – 1650, ฝรั่งเศส

ความสัมพันธ์

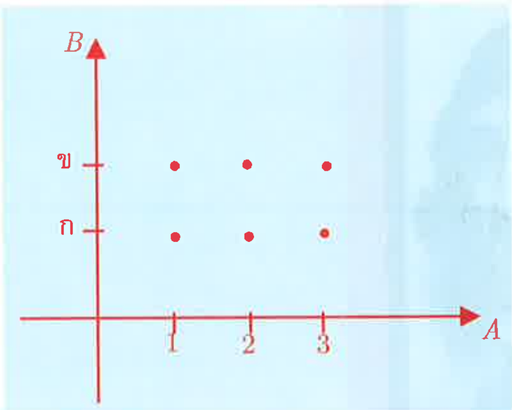
ในชีวิตประจำวันมักพบความสัมพันธ์ระหว่างของสองสิ่ง เช่น ความสัมพันธ์ระหว่างงานกับรายได้ต่อเดือน ความสัมพันธ์ระหว่างการเป็นสมาชิกของพรรคการเมือง ความสัมพันธ์ระหว่างแม่กับลูก หรือ ความสัมพันธ์ระหว่างจำนวนเต็มสองจำนวนที่ผลบวกหารด้วย 5 ลงตัว เป็นต้น ต่อไปจะพิจารณาการเขียนเซตในรูปแบบของการแจกแจงสมาชิกที่มีความสัมพันธ์กันในรูปคู่อันดับ

ถ้าให้ a และ b เป็นสมาชิกใด ๆ อันดับของการเขียนสมาชิก a และ b ซึ่งเขียนได้ในรูป (a, b) เรียกว่า **คู่อันดับ** เรียก a ว่า **สมาชิกตัวหน้า** และเรียก b ว่า **สมาชิกตัวหลัง** ของคู่อันดับ เนื่องจากอันดับของการเขียนมีความสำคัญต่อคู่อันดับ เพราะฉะนั้น $(a, b) \neq (b, a)$

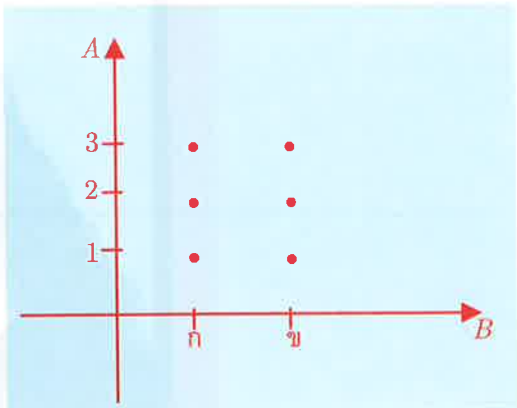
บทนิยาม 3.1 ให้ (a, b) และ (c, d) เป็นคู่อันดับใด ๆ แล้ว
$(a, b) = (c, d)$ ก็ต่อเมื่อ $a = c$ และ $b = d$

บทนิยาม 3.2 ให้ A และ B เป็นเซตใด ๆ **ผลคูณคาร์ทีเซียน**ของเซต A และเซต B จะเขียนแทนด้วย $A \times B$ คือ เซตของคู่อันดับ (a, b) ที่ $a \in A$ และ $b \in B$
นั่นคือ $A \times B = \{(a, b) \mid a \in A$ และ $b \in B\}$

ตัวอย่าง 3.1 ให้ $A = \{1, 2, 3\}$ และ $B = \{$ก, ข$\}$
จะได้ $A \times B = \{(1,$ ก$), (1,$ ข$), (2,$ ก$), (2,$ ข$), (3,$ ก$), (3,$ ข$)\}$
$B \times A = \{($ก$, 1), ($ก$, 2), ($ก$, 3), ($ข$, 1), ($ข$, 2), ($ข$, 3)\}$
แสดงได้ดังรูป 3.1(1) และ 3.1(2)



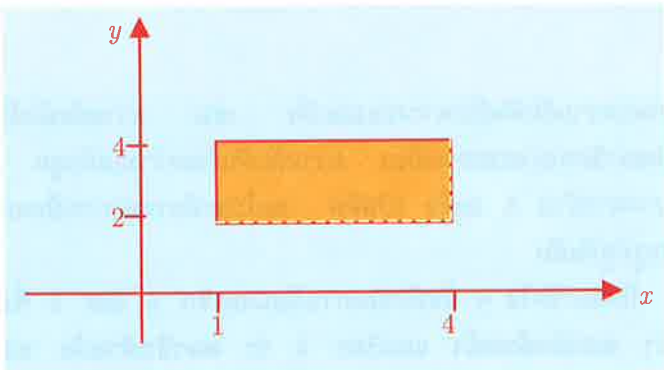
รูป 3.1(1) แสดง $A \times B$



รูป 3.1(2) แสดง $B \times A$

□

ตัวอย่าง 3.2 ให้ $A = \{x \mid 1 \leq x < 4\}$ และ $B = \{y \mid 2 < y \leq 4\}$
จะได้ $A \times B = \{(x, y) \mid 1 \leq x < 4$ และ $2 < y \leq 4\}$
แสดงได้ดังรูป 3.2



รูป 3.2 แสดง $A \times B$

□

ข้อสังเกต 1. โดยทั่วไปจะได้ว่า $A \times B \neq B \times A$ ยกเว้น $A = B$ หรือ $A = \varnothing$ หรือ $B = \varnothing$

2. ถ้า A และ B เป็นเซตจำกัด จะได้ว่า

$$\begin{aligned} n(A \times B) &= n(B \times A) \\ &= n(A) \cdot n(B) \end{aligned}$$

บทนิยาม 3.3 ให้ A และ B เป็นเซตใด ๆ r เป็น**ความสัมพันธ์**จาก A ไป B ก็ต่อเมื่อ $r \subseteq A \times B$
ถ้า $(a, b) \in r$ จะกล่าวว่า a **มีความสัมพันธ์** r **กับ** b เขียนแทนด้วย $a\,r\,b$
ถ้า $(a, b) \notin r$ จะกล่าวว่า a **ไม่มีความสัมพันธ์** r **กับ** b เขียนแทนด้วย $a \not r\, b$
ถ้า $A = B$ จะกล่าวว่า r เป็น**ความสัมพันธ์บน A** ก็ต่อเมื่อ $r \subseteq A \times A$

ตัวอย่างต่อไปจะแสดงความสัมพันธ์ในรูปการแจกแจงสมาชิกของคู่อันดับที่มีความสัมพันธ์กัน

ตัวอย่าง 3.3 ให้ $A = \{$ก, ข$\}$, $B = \{1, 2, 3\}$
และ $r_1 = \{($ก$, 1), ($ข$, 3), ($ก$, 2)\}$
$r_2 = \{($ก$, 2), ($ข$, 2)\}$
ดังนั้น r_1 และ r_2 เป็นความสัมพันธ์จาก A ไป B และ
ก r_1 1, ข r_1 3, ก r_1 2, ก r_2 2, ข r_2 2, ข $\not r_2$ 3, ก $\not r_2$ 1 □

เนื่องจากความสัมพันธ์เป็นเซต ดังนั้นสามารถใช้การดำเนินการของเซตกับความสัมพันธ์ได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.4 ให้ $A = \{0, 1, 2\}$ และ $B = \{1, 2, 3, 4\}$
ให้ $r_1 = \{(0, 1), (1, 2), (2, 3)\}$
และ $r_2 = \{(0, 1), (0, 2), (0, 3), (0, 4)\}$ เป็นความสัมพันธ์จาก A ไป B
จะได้ $r_1 \cup r_2 = \{(0, 1), (0, 2), (0, 3), (0, 4), (1, 2), (2, 3)\}$
$r_1 \cap r_2 = \{(0, 1)\}$
$r_1 - r_2 = \{(1, 2), (2, 3)\}$
และ $r_2 - r_1 = \{(0, 2), (0, 3), (0, 4)\}$ เป็นความสัมพันธ์จาก A ไป B □

ตัวอย่าง 3.5 ให้ $A = \{$สุดา, มาลี, สุธี, ศิริ$\}$ และ $B = \{$นม, โอวัลติน, น้ำส้ม$\}$
ให้ r_1 เป็นความสัมพันธ์ "คนที่ดื่มโอวัลติน"
และ r_2 เป็นความสัมพันธ์ "คนที่ดื่มน้ำส้ม" จาก A ไป B
นั่นคือ $(a,$ โอวัลติน$) \in r_1$ ก็ต่อเมื่อ a ดื่มโอวัลติน
และ $(a,$ น้ำส้ม$) \in r_2$ ก็ต่อเมื่อ a ดื่มน้ำส้ม
ดังนั้น $r_1 \cup r_2$ เป็นความสัมพันธ์ของคนที่ดื่มโอวัลตินหรือน้ำส้ม
ซึ่งเป็นความสัมพันธ์จาก A ไป B
เช่น ถ้า $($สุธี, โอวัลติน$) \in r_1$ หมายความว่า สุธีดื่มโอวัลติน

ถ้า (สุดา, น้ำส้ม) $\in r_2$ หมายความว่า สุดาดื่มน้ำส้ม

ถ้า (มาลี, โอวัลติน) $\in r_1 \cup r_2$ หมายความว่า มาลีดื่มโอวัลตินหรือน้ำส้ม □

ตัวอย่าง 3.6 ให้ A = {สุดา, มาลี, สุธี, ศิริ, พัชรี, นงนุช, ไอศุริย}

และ r เป็นความสัมพันธ์ "เป็นญาติกับ" บน A

ดังนั้น $r = \{(a, b) \in A \times A \mid a$ เป็นญาติกับ $b\}$

เช่น (สุธี, พัชรี) $\in r$ หมายความว่า สุธีเป็นญาติกับพัชรี □

สำหรับความสัมพันธ์ r ใด ๆ บางครั้งเพื่อความสะดวกเราจะเขียนแทน $(a, b) \in r$ ด้วย $a\,r\,b$ เช่น ถ้า r เป็นความสัมพันธ์ "น้อยกว่า" บนเซตของจำนวนจริง จะเขียนแทน $(a, b) \in r$ ด้วย $a < b$ เป็นต้น

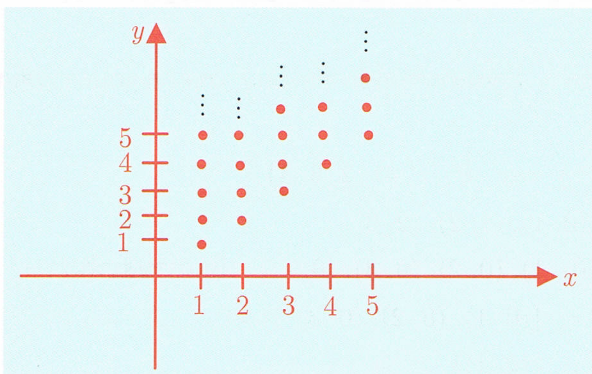
ตัวอย่าง 3.7 ให้ $\mathbb{N}$ แทนเซตของจำนวนเต็มบวก

ให้ $r_1 = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x < y\}$

และ $r_2 = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x = y\}$ เป็นความสัมพันธ์บน $\mathbb{N}$

จะได้ว่า $r_1 \cup r_2 = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$ เป็นความสัมพันธ์บน $\mathbb{N}$

แสดงได้ดังรูป 3.3



รูป 3.3 แสดง $r = r_1 \cup r_2$ □

นอกจากการดำเนินการของเซตแล้วยังพิจารณาความสัมพันธ์กับการดำเนินการอื่น ๆ เช่น ความสัมพันธ์ผกผัน และความสัมพันธ์ประกอบ ดังบทนิยามต่อไปนี้

บทนิยาม 3.4 ถ้า r เป็นความสัมพันธ์จาก A ไป B **ความสัมพันธ์ผกผัน**ของ r คือ ความสัมพันธ์จาก B ไป A เขียนแทนด้วย r^{-1} กำหนดโดย $(y, x) \in r^{-1}$ ก็ต่อเมื่อ $(x, y) \in r$

นั่นคือ $r^{-1} = \{(y, x) \mid (x, y) \in r\}$ หรือ $r^{-1} = \{(x, y) \mid (y, x) \in r\}$

ตัวอย่างต่อไปนี้จะพิจารณาความสัมพันธ์ผกผัน

ตัวอย่าง 3.8 ให้ A = เซตของคน และให้ r_1 เป็นความสัมพันธ์ "สูงกว่า", r_2 เป็นความสัมพันธ์ "เป็นแม่" และ r_3 เป็นความสัมพันธ์ "สนิทกับ" บน A ดังนั้น

$$r_1 = \{(a, b) \mid a \text{ สูงกว่า } b\}$$

จะได้ $$r_1^{-1} = \{(b, a) \mid a \text{ สูงกว่า } b\} = \{(a, b) \mid b \text{ สูงกว่า } a\}$$

$$r_2 = \{(a, b) \mid a \text{ เป็นแม่ของ } b\}$$

จะได้ $$r_2^{-1} = \{(b, a) \mid a \text{ เป็นแม่ของ } b\} = \{(a, b) \mid b \text{ เป็นแม่ของ } a\}$$

และ $$r_3 = \{(a, b) \mid a \text{ สนิทกับ } b\}$$

จะได้ $$r_3^{-1} = \{(b, a) \mid a \text{ สนิทกับ } b\} = \{(a, b) \mid b \text{ สนิทกับ } a\}$$ □

ตัวอย่าง 3.9 ให้ $\mathbb{R}$ แทนเซตของจำนวนจริง

ให้ $$r_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x\}$$

$$r_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq 2x^2\}$$

และ $$r_3 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = \frac{x+1}{3}\}$$

จงหา r_1^{-1}, r_2^{-1} และ r_3^{-1}

วิธีทำ จาก $$r_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x\}$$

ดังนั้น $$r_1^{-1} = \{(y, x) \in \mathbb{R} \times \mathbb{R} \mid y = x\} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$$

จาก $$r_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq 2x^2\}$$

ดังนั้น $$r_2^{-1} = \{(y, x) \in \mathbb{R} \times \mathbb{R} \mid y \geq 2x^2\} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq 2y^2\}$$

จาก $$r_3 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = \frac{x+1}{3}\}$$

ดังนั้น $$r_3^{-1} = \{(y, x) \in \mathbb{R} \times \mathbb{R} \mid y = \frac{x+1}{3}\} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = \frac{y+1}{3}\}$$ □

ข้อสังเกต
1. ถ้า r เป็นความสัมพันธ์จาก A ไป B แล้วสามารถหาความสัมพันธ์ผกผัน r^{-1} จาก B ไป A ได้เสมอ
2. ความสัมพันธ์บางความสัมพันธ์เมื่อหาความสัมพันธ์ผกผันแล้วจะได้ความสัมพันธ์เดิม นั่นคือ $r = r^{-1}$
   ดังความสัมพันธ์ r_3 ในตัวอย่าง 3.8 และ r_1 ในตัวอย่าง 3.9

บทนิยาม 3.5 ให้ r เป็นความสัมพันธ์จาก A ไป B
โดเมนของ r คือ เซตที่ประกอบด้วยสมาชิกตัวหน้าของคู่อันดับใน r เขียนแทนด้วย D_r
นั่นคือ $D_r = \{x \in A \mid$ มี $y \in B$ ที่ $(x, y) \in r\}$
พิสัยของ r คือ เซตที่ประกอบด้วยสมาชิกตัวหลังของคู่อันดับใน r เขียนแทนด้วย R_r
นั่นคือ $R_r = \{y \in B \mid$ มี $x \in A$ ที่ $(x, y) \in r\}$

ตัวอย่าง 3.10 ให้ $A = \{1, 2, 3\}$ และ $B = \{$ก, ข$\}$
และ $r = \{(1,$ ก$), (1,$ ข$), (2,$ ก$)\}$
ดังนั้น $D_r = \{1, 2\}$ และ $R_r = \{$ก, ข$\}$
พิจารณาโดเมนและพิสัยของ r^{-1}
จาก $r^{-1} = \{($ก$, 1), ($ข$, 1), ($ก$, 2)\}$
ดังนั้น $D_{r^{-1}} = \{$ก, ข$\}$ และ $R_{r^{-1}} = \{1, 2\}$ □

ข้อสังเกต ถ้า r เป็นความสัมพันธ์จาก A ไป B จะได้ $D_r = R_{r^{-1}}$ และ $R_r = D_{r^{-1}}$

บทนิยาม 3.6 ให้ r เป็นความสัมพันธ์จาก A ไป B และ s เป็นความสัมพันธ์จาก B ไป C
ความสัมพันธ์ประกอบของ r และ s เป็นความสัมพันธ์จาก A ไป C เขียนแทนด้วย $s \circ r$
กำหนดโดย

$$s \circ r = \{(x, z) \mid \text{ มี } y \in B \text{ ที่ } (x, y) \in r \text{ และ } (y, z) \in s\}$$

จากบทนิยามจะได้ว่า ถ้า $R_r \cap D_s \neq \varnothing$ แล้ว $s \circ r \neq \varnothing$

ตัวอย่าง 3.11 ให้ r เป็นความสัมพันธ์จาก $\{1, 2, 3\}$ ไปยัง $\{1, 2, 3, 4\}$
และ s เป็นความสัมพันธ์จาก $\{1, 2, 3, 4\}$ ไปยัง $\{0, 1, 2\}$ กำหนดโดย
$r = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$
และ $s = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$ ตามลำดับ
จะได้ $s \circ r = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}$ □

ตัวอย่าง 3.12 ให้ $A = \{$สุดา, มาริสา, สุธี, กรศิริ, พัชรี, นงนุช, ไอศุริย, กรรณิกา$\}$
และ $B = \{$ค 011, ค 012, ค 013, ค 014, ค 015, ค 016$\}$
ให้ r_1, r_2 เป็นความสัมพันธ์จาก A ไป B และ s เป็นความสัมพันธ์บน B กำหนดโดย
$(x, y) \in r_1$ ก็ต่อเมื่อ นักเรียน x เรียนวิชา y
$(x, y) \in r_2$ ก็ต่อเมื่อ นักเรียน x สอบวิชา y ผ่าน
และ $(x, y) \in s$ ก็ต่อเมื่อ สอบวิชา x ผ่านก่อนเรียนวิชา y ที่เป็นวิชารหัสถัดจาก x
จงหาความหมายของความสัมพันธ์ $r_1 \cup r_2,\ r_1 \cap r_2,\ r_1 - r_2$ และ $s \circ r_1$

วิธีทำ ความสัมพันธ์ $r_1 \cup r_2$ หมายถึง เซตที่ประกอบด้วยคู่อันดับ (x, y) ที่ x เรียนวิชา y หรือสอบวิชา y ผ่าน

เช่น (มาริสา, ค013) $\in r_1 \cup r_2$ หมายความว่า มาริสา เรียนวิชา ค 013 หรือ สอบวิชา ค 013 ผ่าน

ความสัมพันธ์ $r_1 \cap r_2$ หมายถึง เซตที่ประกอบด้วยคู่อันดับ (x, y) ที่ x เรียนวิชา y และ สอบผ่าน

ความสัมพันธ์ $r_1 - r_2$ หมายถึง เซตที่ประกอบด้วยคู่อันดับ (x, y) ที่ x เรียนวิชา y แต่สอบไม่ผ่าน

เช่น (ไอศุริย, ค 014) $\in r_1 - r_2$ หมายความว่า ไอศุริย เรียนวิชา ค 014 แต่สอบไม่ผ่าน

ความสัมพันธ์ $s \circ r_2$ หมายถึง เซตที่ประกอบด้วยคู่อันดับ (x, z) ที่นักเรียน x สามารถเรียนวิชา z ได้โดยต้องสอบผ่านวิชา y ที่เป็นวิชารหัสก่อนวิชา z

เช่น (กรรณิกา, ค 016) $\in s$ หมายความว่า กรรณิกา สามารถเรียนวิชา ค 016 ได้เพราะสอบผ่านวิชา ค 015 □

ข้อสังเกต ให้ r เป็นความสัมพันธ์บน A ความสัมพันธ์ประกอบของ r กำหนดได้ดังนี้

$$r^1 = r \quad \text{และ} \quad r^{n+1} = r^n \circ r \quad \text{สำหรับ } n = 1, 2, 3, \ldots$$

เช่น $r^2 = r \circ r,\ r^3 = r^2 \circ r$

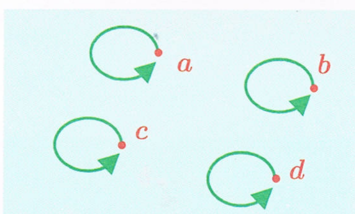
ตัวอย่าง 3.13 ให้ $r = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$ เป็นความสัมพันธ์บน $\{1, 2, 3, 4\}$

จะได้
$$\begin{aligned} r^2 &= r \circ r = \{(1, 1), (2, 1), (3, 1), (4, 2)\} \\ r^3 &= r^2 \circ r = \{(1, 1), (2, 1), (3, 1), (4, 1)\} \\ r^4 &= r^3 \circ r = \{(1, 1), (2, 1), (3, 1), (4, 1)\} \end{aligned}$$ □

จากตัวอย่างข้างต้นจะสังเกตได้ว่าความสัมพันธ์บางความสัมพันธ์มีสมบัติบางประการที่ต่างออกไป ดังบทนิยามต่อไปนี้

บทนิยาม 3.7 ให้ r เป็นความสัมพันธ์บน A
จะกล่าวว่า r มี**สมบัติสะท้อน** ถ้าทุก ๆ สมาชิกของ A มีความสัมพันธ์ r กับตัวเอง
นั่นคือ สำหรับแต่ละ $a \in A$, $(a, a) \in r$

แสดงได้ดังรูป 3.4



รูป 3.4 แสดงสมบัติสะท้อน

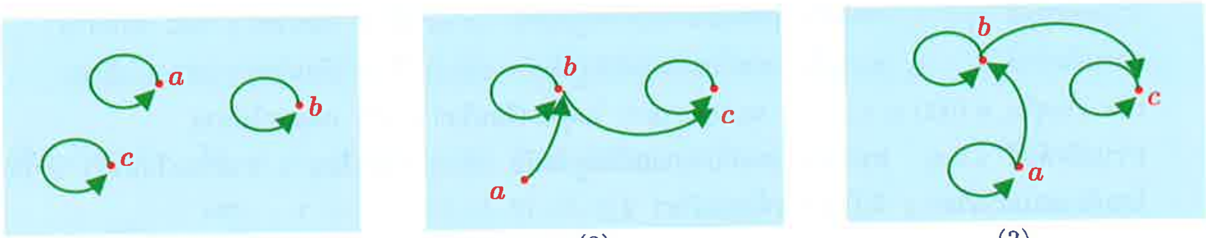
ตัวอย่าง 3.14 พิจารณาความสัมพันธ์บน $\{a, b, c\}$ ต่อไปนี้

$$\begin{aligned} r_1 &= \{(a, a), (b, b), (c, c)\} \\ r_2 &= \{(a, b), (b, b), (b, c), (c, c)\} \end{aligned}$$

และ $r_3 = \{(a, a), (a, b), (b, b), (b, c), (c, c)\}$

จากบทนิยามจะได้ r_1 และ r_3 มีสมบัติสะท้อน ดังรูป 3.5(1) และ 3.5(3) ตามลำดับ

แต่ r_2 ไม่มีสมบัติสะท้อน เพราะ $(a, a) \notin r_2$ ดังรูป 3.5(2)



(1) (2) (3)

รูป 3.5

$\square$

ตัวอย่าง 3.15 ให้ $\mathbb{Z}$ แทนเซตของจำนวนเต็ม และ $\mathbb{R}$ แทนเซตของจำนวนจริง พิจารณาความสัมพันธ์ต่อไปนี้

$r_1 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x$ หาร y ลงตัว$\}$

$r_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x > y\}$

และ $r_3 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 \leq 1\}$

จะได้ r_1 มีสมบัติสะท้อน เพราะ x หาร x ลงตัว ทุกค่า $x \in \mathbb{Z}$

นั่นคือ $(x, x) \in r_1$ ทุก $x \in \mathbb{Z}$

r_2 ไม่มีสมบัติสะท้อน เพราะ $x \not> x$ ทุกค่า $x \in \mathbb{R}$

นั่นคือ $(x, x) \notin r_2$ ทุก $x \in \mathbb{R}$

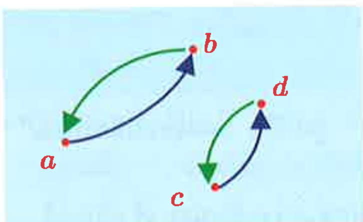
และ r_3 ไม่มีสมบัติสะท้อน เพราะ $1^2 + 1^2 = 2 > 1$ นั่นคือ $(1, 1) \notin r_3$ $\square$

บทนิยาม 3.8 ให้ r เป็นความสัมพันธ์บน A จะกล่าวว่า

r **มีสมบัติสมมาตร** ถ้า a มีความสัมพันธ์ r กับ b แล้ว b มีความสัมพันธ์ r กับ a

นั่นคือ สำหรับแต่ละ $a, b \in A$, ถ้า $(a, b) \in r$ แล้ว $(b, a) \in r$

แสดงได้ดังรูป 3.6



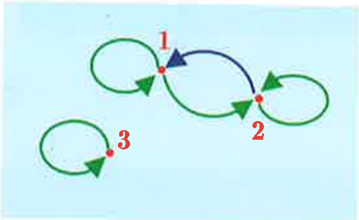
รูป 3.6 แสดงสมบัติสมมาตร

ตัวอย่าง 3.16 พิจารณาความสัมพันธ์บน $\{1, 2, 3\}$ ต่อไปนี้

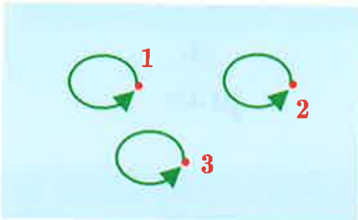
$$r_1 = \{(1, 1), (1, 2), (2, 1), (3, 3)\}$$
$$r_2 = \{(1, 1), (2, 2), (3, 3)\}$$
และ $$r_3 = \{(1, 1), (1, 3), (2, 1), (2, 3), (3, 2)\}$$

จากบทนิยามจะได้ r_1 และ r_2 มีสมบัติสมมาตร ดังรูป 3.7(1) และ 3.7(2)

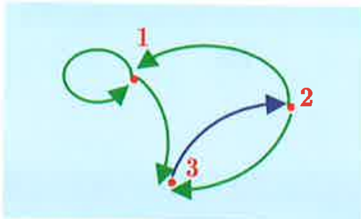
แต่ r_3 ไม่มีสมบัติสมมาตร เพราะ $(1, 3) \in r_3$ แต่ $(3, 1) \notin r_3$ ดังรูป 3.7(3)



(1)



(2)



(3)

รูป 3.7 □

ตัวอย่าง 3.17 ให้ r_1 เป็นความสัมพันธ์ "ขนานกัน" บนเซตของเส้นตรงในระนาบ

r_2 เป็นความสัมพันธ์ "อยู่อำเภอเดียวกัน" บนเซตของคน

และ r_3 เป็นความสัมพันธ์ "ไม่มากกว่า" บนเซตของจำนวนจริง

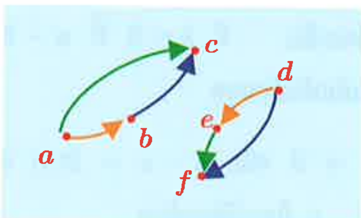
จากบทนิยามจะได้ r_1 และ r_2 มีสมบัติสมมาตร

แต่ r_3 ไม่มีสมบัติสมมาตร เพราะ $(-1, 1) \in r_3$ แต่ $(1, -1) \notin r_3$ □

บทนิยาม 3.9 ให้ r เป็นความสัมพันธ์บน A จะกล่าวว่า r **มีสมบัติถ่ายทอด** ถ้า a มีความสัมพันธ์ r กับ b และ b มีความสัมพันธ์ r กับ c แล้ว a มีความสัมพันธ์ r กับ c ด้วย

นั่นคือ สำหรับแต่ละ $a, b, c \in A$, ถ้า $(a, b) \in r$ และ $(b, c) \in r$ แล้ว $(a, c) \in r$

แสดงได้ดังรูป 3.8

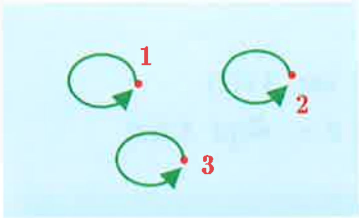


รูป 3.8 แสดงสมบัติถ่ายทอด

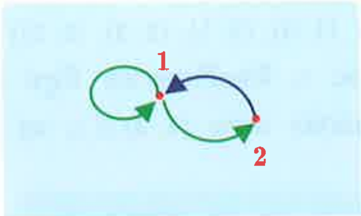
ตัวอย่าง 3.18 พิจารณาความสัมพันธ์บน $\{1, 2, 3\}$ ต่อไปนี้

$$r_1 = \{(1, 1), (2, 2), (3, 3)\}$$
$$r_2 = \{(1, 1), (1, 2), (2, 1)\}$$
และ $$r_3 = \{(1, 1), (1, 2), (2, 1), (2, 3), (3, 1)\}$$

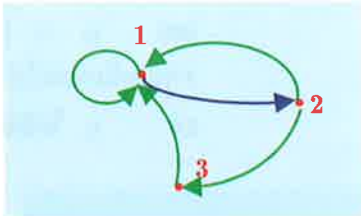
จากบทนิยามจะได้ r_1 และ r_2 มีสมบัติถ่ายทอด ดังรูป 3.9(1) และ 3.9(2)
แต่ r_3 ไม่มีสมบัติถ่ายทอด เพราะ $(3, 1), (1, 2) \in r_4$ แต่ $(3, 2) \notin r_4$ ดังรูป 3.9(3)



(1)



(2)



(3)

รูป 3.9 □

บทนิยาม 3.10 ให้ r เป็นความสัมพันธ์บน A จะกล่าวว่า
r **เป็นความสัมพันธ์สมมูลบน** A ถ้า r มีสมบัติสะท้อน สมมาตร และถ่ายทอด
นั่นคือ ถ้า r เป็นความสัมพันธ์สมมูลบน A แล้ว

1. สำหรับแต่ละ $a \in A$, $(a, a) \in r$
2. สำหรับแต่ละ $a, b \in A$, ถ้า $(a, b) \in r$ แล้ว $(b, a) \in r$
3. สำหรับแต่ละ $a, b, c \in A$, ถ้า $(a, b) \in r$ และ $(b, c) \in r$ แล้ว $(a, c) \in r$

ตัวอย่าง 3.19 ให้ r_1 เป็นความสัมพันธ์ "ขนานกัน" บนเซตของเส้นตรงในระนาบ
r_2 เป็นความสัมพันธ์ "อยู่อำเภอเดียวกัน" บนเซตของคน
r_3 เป็นความสัมพันธ์ "มากกว่า" บนเซตของจำนวนจริง
และ r_4 เป็นความสัมพันธ์ "คล้ายกัน" บนเซตของสามเหลี่ยมในระนาบ
จากบทนิยาม 3.10 จะได้ r_1, r_2 และ r_4 เป็นความสัมพันธ์สมมูล
แต่ r_3 ไม่เป็นความสัมพันธ์สมมูล เพราะ r_3 ไม่มีสมบัติสะท้อนและสมมาตร □

ตัวอย่าง 3.20 ให้ r เป็นความสัมพันธ์บน $\mathbb{Z}$ กำหนดโดย

$(a, b) \in r$ ก็ต่อเมื่อ มี $k \in \mathbb{Z}$ ที่ $a - b = 2k$

จงแสดงว่า r เป็นความสัมพันธ์สมมูล

วิธีทำ
1. ให้ $a \in \mathbb{Z}$ จะได้ $a - a = 0$ หรือ $a - a = 2(0)$ เมื่อ $0 \in \mathbb{Z}$
   ดังนั้น $(a, a) \in r$ นั่นคือ r มีสมบัติสะท้อน
2. ให้ $a, b \in \mathbb{Z}$ และ $(a, b) \in r$ จะได้ว่า มี $k \in \mathbb{Z}$ ที่ $a - b = 2k$
   เพราะว่า $b - a = -(a - b)$ เพราะฉะนั้น $b - a = -2k$ หรือ $b - a = 2(-k)$ เมื่อ $-k \in \mathbb{Z}$
   ดังนั้น $(b, a) \in r$ นั่นคือ r มีสมบัติสมมาตร
3. ให้ $a, b, c \in \mathbb{Z}$ และ $(a, b), (b, c) \in r$ จะได้ว่า มี $k, k' \in \mathbb{Z}$ ที่ $a - b = 2k$ และ
   $b - c = 2k'$ จะได้ $(a - b) + (b - c) = 2k + 2k'$ หรือ $a - c = 2(k + k')$

เมื่อ $k + k' \in \mathbb{Z}$

ดังนั้น $(a, c) \in r$ นั่นคือ r มีสมบัติถ่ายทอด

จาก 1. – 3. จะได้ r เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ □

จากตัวอย่างข้างต้นจะสังเกตได้ว่า r เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ สมาชิกในความสัมพันธ์จะแบ่ง $\mathbb{Z}$ ออกเป็น 2 ส่วนด้วยกันคือ

$\mathbb{Z}_0 = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ และ $\mathbb{Z}_1 = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$

ที่ $\mathbb{Z}_0 \cup \mathbb{Z}_1 = \mathbb{Z}$ และ $\mathbb{Z}_0 \cap \mathbb{Z}_1 = \varnothing$

ฟังก์ชัน

สำหรับเซต A และ B ใด ๆ เราสามารถกำหนดความสัมพันธ์จาก A ไป B ได้หลายรูปแบบ ยิ่งกว่านั้นสามารถนับจำนวนความสัมพันธ์ได้ ถ้า A และ B เป็นเซตจำกัด นั่นคือ ถ้า $n(A) = m$ และ $n(B) = n$ แล้ว $n(A \times B) = mn$ เพราะว่าความสัมพันธ์จาก A ไป B เป็นสับเซตของ $A \times B$ ดังนั้น จำนวนความสัมพันธ์จาก A ไป B เท่ากับ 2^{mn} จากการสร้างความสัมพันธ์ได้หลายแบบนี้เอง จะพบว่ามีความสัมพันธ์แบบหนึ่งซึ่งมีลักษณะพิเศษ เช่น ตัวอย่างต่อไปนี้

ความสัมพันธ์ระหว่างระยะทางกับเวลา $r = \{(t, s) \in \mathbb{R} \times \mathbb{R} \mid s = 2t^2 + t + 1\}$ เป็นความสัมพันธ์ระหว่างเซตของเวลาไปยังเซตของระยะทาง จะสังเกตได้ว่าเมื่อเวลาเปลี่ยนระยะทางก็เปลี่ยนไปด้วย

ความสัมพันธ์ระหว่างนักเรียนที่ได้ระดับคะแนนวิชาคณิตศาสตร์เป็น 4, 3, 2, 1, 0 เป็นความสัมพันธ์ระหว่างเซตของนักเรียนที่เรียนคณิตศาสตร์ ไปยังเซตของระดับคะแนน 4, 3, 2, 1, 0 จะสังเกตได้ว่า นักเรียนที่เรียนคณิตศาสตร์แต่ละคนจะได้ระดับคะแนนแต่เพียงระดับเดียว ความสัมพันธ์เช่นนี้เรียกว่า ฟังก์ชัน ดังบทนิยามต่อไปนี้

บทนิยาม 3.11 กำหนด A และ B เป็นเซตใด ๆ f เป็นความสัมพันธ์จาก A ไป B จะกล่าวว่า f เป็น**ฟังก์ชัน** ก็ต่อเมื่อ สำหรับแต่ละ $x \in A$ และแต่ละ $y, z \in B$,

ถ้า $(x, y) \in f$ และ $(x, z) \in f$ แล้ว $y = z$

ตัวอย่าง 3.21 กำหนด $A = \{1, 2, 3\}$ และ $B = \{a, b\}$

ให้ $f = \{(1, a), (2, b)\}$

$g = \{(1, b), (3, b), (2, a)\}$

และ $h = \{(1, a), (1, b), (2, a)\}$

จะได้ว่า f และ g เป็นฟังก์ชัน และ h ไม่เป็นฟังก์ชัน

เพราะว่า $(1, a), (1, b) \in h$ แต่ $a \neq b$ □

ตัวอย่าง 3.22 จงพิจารณาว่าความสัมพันธ์ที่กำหนดให้ต่อไปนี้เป็นฟังก์ชันหรือไม่

(1) ให้ A แทนเซตของประชากรในเขตกรุงเทพมหานครทั้งหมด

B แทนเซตของผู้ลงสมัครเป็นผู้ว่าราชการกรุงเทพมหานคร

และให้ r เป็นความสัมพันธ์ของผู้มีสิทธิเลือกผู้สมัครเป็นผู้ว่าราชการกรุงเทพมหานคร

จะได้ r เป็นความสัมพันธ์จาก A ไป B และ r เป็นความสัมพันธ์ที่เป็นฟังก์ชัน

(2) ให้ r เป็นความสัมพันธ์ "พื้นที่ (A) ของวงกลมรัศมี R" บนเซตของจำนวนจริง กำหนดโดย

$$(A,\, R) \in r \quad \text{ก็ต่อเมื่อ} \quad A = \pi R^2$$

จะได้ r เป็นความสัมพันธ์ที่เป็นฟังก์ชัน □

ข้อสังเกต

1. ฟังก์ชันเป็นความสัมพันธ์แบบหนึ่ง แต่ความสัมพันธ์บางความสัมพันธ์อาจไม่เป็นฟังก์ชัน
2. สมาชิกตัวหน้าของฟังก์ชันจะไม่ซ้ำกัน และสมาชิกตัวหลังจะมีเพียงตัวเดียวที่สมนัยกับสมาชิกตัวหน้า
3. เนื่องจากฟังก์ชันเป็นความสัมพันธ์ เพราะฉะนั้นโดเมนและพิสัยของฟังก์ชันจะนิยามเช่นเดียวกับความสัมพันธ์ นั่นคือ ถ้า f เป็นฟังก์ชัน จะได้

$$D_f = \{x \mid \text{ มี } y \text{ ที่ } (x,\, y) \in f\} \quad \text{และ} \quad R_f = \{y \mid \text{ มี } x \text{ ที่ } (x,\, y) \in f\}$$

จากบทนิยามและข้อสังเกตของฟังก์ชัน จะกล่าวได้ว่า ฟังก์ชัน f คือ **กฎ** ที่ได้ผลลัพธ์เพียงผลลัพธ์เดียวที่สมนัยกับการใส่ข้อมูลเข้าไปในกฎนั้น ซึ่งสามารถมองฟังก์ชันคล้ายกับการโปรแกรมคอมพิวเตอร์ที่เมื่อใส่ข้อมูลเข้าไปแล้วดำเนินการตามกฎจะได้ผลลัพธ์ออกมา ดังรูป 3.10 ผลลัพธ์ที่ได้จะเรียกว่า ค่าของฟังก์ชัน f ที่ x หรือ พิสัยของ x ภายใต้ f

รูป 3.10 แสดง y เป็นค่าของฟังก์ชัน f ที่ x

การเขียนฟังก์ชันจะไม่นิยมเขียนในรูปแบบของคู่อันดับ เพื่อความสะดวกในการหาค่าของฟังก์ชัน f ที่ขึ้นกับตัวแปร x จะนิยามการเขียนฟังก์ชันให้ง่ายขึ้นได้ดังนี้

บทนิยาม 3.12 ให้ A และ B เป็นเซตใด ๆ และ f เป็นฟังก์ชัน A ไป B ถ้า $(x,\, y) \in f$ เรียก y ว่า**ตัวแปรตามที่ขึ้นกับตัวแปรอิสระ** x นิยามโดย y เป็นค่าของฟังก์ชัน f ที่ x เขียนแทนด้วย $y = f(x)$

ตัวอย่างเช่น $(2,\, 4) \in f$ หมายความว่า $f(2) = 4$

เราสามารถแสดงฟังก์ชันโดยอาศัยบทนิยาม 3.12 ได้เช่น

$f = \{(1,\, a),\, (2,\, b),\, (3,\, c)\}$ แสดงได้ด้วย $f(1) = a,\ f(2) = b,\ f(3) = c$

และ $g = \{(x,\, y) \in \mathbb{R} \times \mathbb{R} \mid y = \sqrt{x^2 + 25}\,\}$ แสดงได้ด้วย $g(x) = \sqrt{x^2 + 25}$ สำหรับ $x \in \mathbb{R}$

ตัวอย่าง 3.23

(1) พิจารณาความสัมพันธ์

$$f(x) = \begin{cases} x^2+1 & ; \quad x < 1 \\ x-1 & ; \quad 1 \le x < 3 \\ 2 & ; \quad x \ge 3 \end{cases}$$

จงหา $f(-1), f(2)$ และ $f(5)$

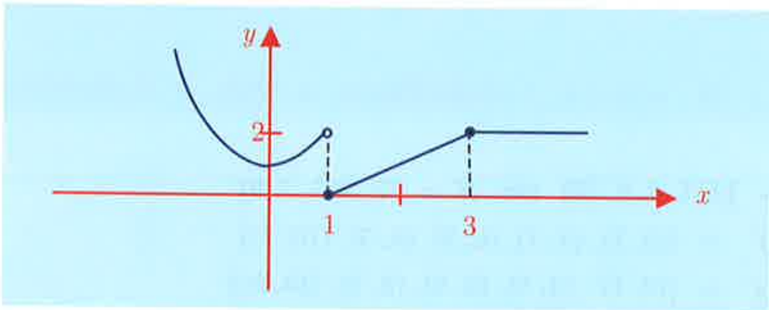
วิธีทำ แทนค่า $x = -1, 2, 5$ ในความสัมพันธ์ที่กำหนดให้ จะได้

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

$f(2) = (2) - 1 = 1$

$f(5) = 2$

ยิ่งไปกว่านั้น ความสัมพันธ์ f เป็นฟังก์ชัน แสดงได้ดังรูป 3.11



รูป 3.11 แสดงกราฟของ f

(2) กำหนดความสัมพันธ์

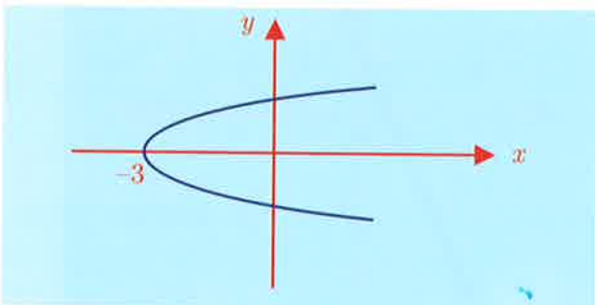
$$g = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y^2 - 3\}$$

จงพิจารณาว่าความสัมพันธ์ g เป็นฟังก์ชันหรือไม่

วิธีทำ เนื่องจากเมื่อแทนค่า $x = 1$ ในความสัมพันธ์ g จะได้ $1 = (2)^2 - 3$ และ $1 = (-2)^2 - 3$

ดังนั้น $(1, 2), (1, -2) \in g$ แต่ $2 \neq -2$

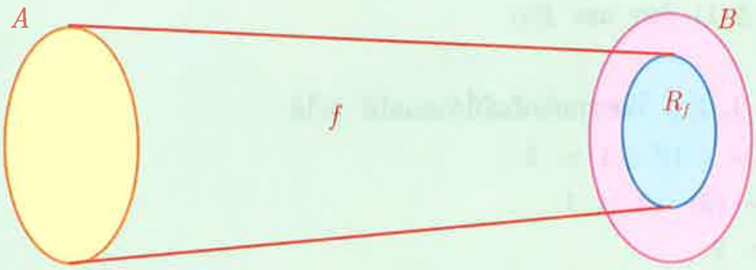
นั่นคือ g ไม่เป็นฟังก์ชัน แสดงได้ดังรูป 3.12



รูป 3.12 แสดงกราฟของสมการ $x = y^2 - 3$ □

จะสังเกตได้ว่าค่าของฟังก์ชัน f ที่ x มีเพียงค่าเดียวโดยที่ x อาจมีค่าเดียวหรือหลายค่าก็ได้ เช่นนี้ทำให้ได้ว่าฟังก์ชันมีลักษณะต่าง ๆ กัน บทนิยามต่อไปนี้จะกล่าวถึงลักษณะที่สำคัญของฟังก์ชัน

บทนิยาม 3.13 ให้ A และ B เป็นเซตใด ๆ และ f เป็นฟังก์ชันที่ $D_f = A$ ถ้า $R_f \subset B$ จะกล่าวว่า f **เป็นฟังก์ชันจาก A ไป B** เขียนแทนด้วย $f: A \to B$ ดังรูป 3.13



รูป 3.13 แสดง $f: A \to B$

ถ้า $R_f = B$ จะกล่าวว่า f **เป็นฟังก์ชันจาก A ทั่วถึง B** เขียนแทนด้วย $f: A \xrightarrow{\text{ทั่วถึง}} B$

ตัวอย่าง 3.24 ให้ $A = \{2, 4, 6, 8, 10\}$ และ $B = \{1, 3, 5, 7, 9\}$

และ $f = \{(2, 1), (4, 1), (6, 3), (8, 5), (10, 7)\}$

$g = \{(2, 1), (4, 3), (6, 5), (8, 7), (10, 9)\}$

$h = \{(2, 1), (6, 3), (10, 7)\}$

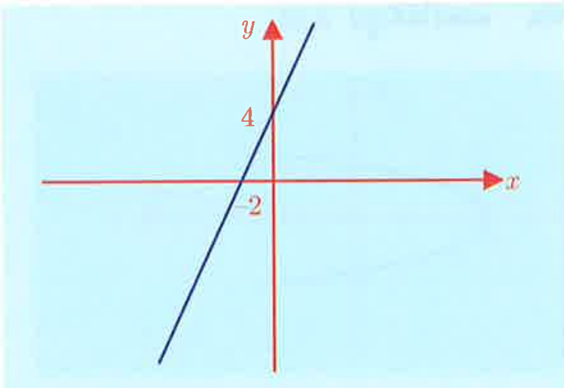
จะเห็นว่า $f: A \to B$ เพราะ $D_f = A$ และ $R_f = \{1, 3, 5, 7\} \subset B$

$g: A \xrightarrow{\text{ทั่วถึง}} B$ เพราะ $D_g = A$ และ $R_g = B$

และ h เป็นฟังก์ชัน แต่ไม่เป็นฟังก์ชันจาก A ไป B เพราะ $D_h \neq A$

นั่นคือ h เป็นฟังก์ชันจาก $\{2, 6, 10\}$ ไป B □

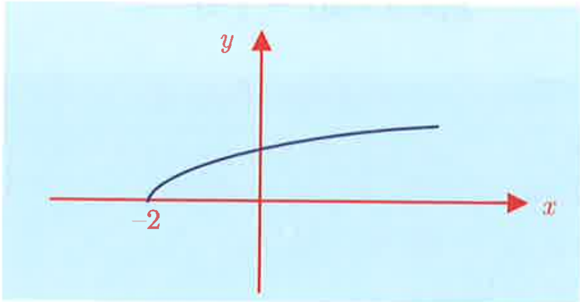
ตัวอย่าง 3.25 พิจารณาฟังก์ชัน $f(x) = 2x + 4$ เมื่อ $x \in \mathbb{R}$ แสดงได้ด้วยกราฟดังรูป 3.14



รูป 3.14 แสดงกราฟ $f(x) = 2x + 4$

จะได้ว่า $D_f = \mathbb{R}$ และ $R_f = \mathbb{R}$ ดังนั้น $f: \mathbb{R} \xrightarrow{\text{ทั่วถึง}} \mathbb{R}$ □

ตัวอย่าง 3.26 พิจารณาฟังก์ชัน $f(x) = \sqrt{x+2}$ แสดงได้ด้วยกราฟดังรูป 3.15



รูป 3.15 แสดงกราฟ $f(x)$

จาก $y = f(x) = \sqrt{x+2}$ จะได้ว่า $x+2 \geq 0$ ทำให้ y หาค่าได้
นั่นคือ $x \geq -2$
ดังนั้น $D_f = \{x \mid x \geq -2\}$ และ $R_f = \{x \mid x \geq 0\}$
เพราะฉะนั้น $f:\{\, x \mid x \geq -2 \,\} \to \mathbb{R}$ □

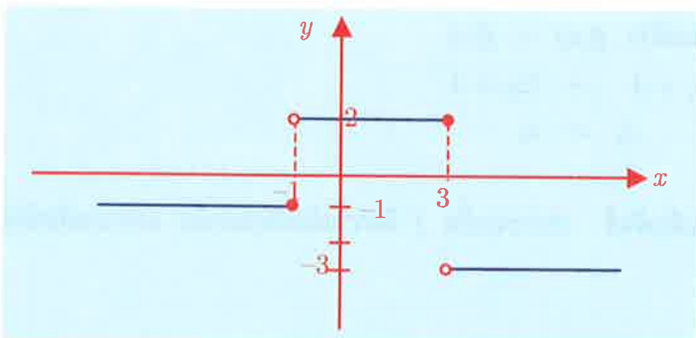
หมายเหตุ ถ้า $f: A \to B$ และ $S \subseteq A$ จะได้ว่า $f(S) \subseteq f(A) \subseteq B$ เมื่อกำหนด

$$f(S) = \{f(x) \in B \mid x \in S\}$$

ตัวอย่าง 3.27 พิจารณาฟังก์ชัน

$$f(x) = \begin{cases} -1 & ; \quad x \leq -1 \\ 2 & ; \quad -1 < x \leq 3 \\ -3 & ; \quad x > 3 \end{cases}$$

แสดงได้ด้วยกราฟดังรูป 3.16



รูป 3.16 แสดงกราฟของ f

จะได้ว่า $D_f = \mathbb{R}$ และ $R_f = \{-1, -2, -3\}$ ดังนั้น $f: \mathbb{R} \xrightarrow{\text{ทั่วถึง}} \{-1, -2, -3\}$

ยิ่งไปกว่านั้น จะได้ว่า $f(\{x \mid x \le -1\}) = \{-1\}$

$f(\{x \mid -1 < x \le 3\}) = \{2\}$

และ $f(\{x \mid x > 3\}) = \{-3\}$ □

บทนิยาม 3.14 ให้ $f : A \to B$ จะกล่าวว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อ สำหรับแต่ละ $x_1, x_2 \in A$ และแต่ละ $y \in B$ ถ้า $(x_1, y) \in f$ และ $(x_2, y) \in f$ แล้ว $x_1 = x_2$

หรือ f เป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อ สำหรับแต่ละ $x_1, x_2 \in A$

ถ้า $x_1 \ne x_2$ แล้ว $f(x_1) \ne f(x_2)$

เขียนแทนด้วย $f : A \xrightarrow{1-1} B$

ตัวอย่าง 3.28 ให้ $A = \{2, 4, 6, 8, 10\}$ และ $B = \{1, 3, 5, 7, 9, 11\}$

ให้ $f, g, h : A \to B$ ที่

$$f = \{(2, 1), (4, 3), (6, 5), (8, 7), (10, 9)\}$$
$$g = \{(2, 1), (4, 1), (6, 3), (8, 5), (10, 7)\}$$
$$h = \{(2, 3), (4, 1), (6, 7), (8, 5), (10, 11)\}$$

จะได้ว่า f และ h เป็นฟังก์ชันหนึ่งต่อหนึ่ง

และ g ไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะ $(2, 1), (4, 1) \in g$ แต่ $2 \ne 4$ □

ตัวอย่าง 3.29 พิจารณาฟังก์ชัน $f(x) = x^2 - 1$ เมื่อ $x \in \mathbb{R}$ เป็นฟังก์ชันหนึ่งต่อหนึ่งหรือไม่

วิธีทำ เนื่องจาก $1, -1 \in \mathbb{R}$ ที่ $f(1) = 0$ และ $f(-1) = 0$ แต่ $1 \ne -1$

ดังนั้น f ไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง □

ตัวอย่าง 3.30 พิจารณาฟังก์ชัน $f(x) = 2x + 4$ เมื่อ $x \in \mathbb{R}$ จงแสดงว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง

วิธีทำ ให้ $x_1, x_2 \in D_f$ สมมติว่า $f(x_1) = f(x_2)$

จะได้ว่า $2x_1 + 4 = 2x_2 + 4$

ดังนั้น $x_1 = x_2$ □

เพราะว่า f เป็นความสัมพันธ์ เพราะฉะนั้น f มีความสัมพันธ์ผกผัน แต่ความสัมพันธ์ผกผันของ f อาจไม่เป็นฟังก์ชัน ก็ได้

ตัวอย่าง 3.31 จงพิจารณาว่าฟังก์ชัน f ต่อไปนี้ f^{-1} เป็นฟังก์ชันหรือไม่

(1) ให้ $f = \{(2, 1), (3, 2), (4, 3)\}$ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก $\{2, 3, 4\}$ ไป $\{1, 2, 3\}$

จะได้ $f^{-1} = \{(1, 2), (2, 3), (3, 4)\}$ เป็นฟังก์ชันด้วย

(2) ให้ $f = \{(1, 2), (3, 4), (4, 6), (6, 2)\}$ เป็นฟังก์ชันแต่ไม่หนึ่งต่อหนึ่งจาก $\{1, 3, 4, 6\}$ ไป $\{2, 4, 6\}$ จะได้ $f^{-1} = \{(2, 1), (4, 3), (5, 4), (2, 6)\}$ ไม่เป็นฟังก์ชัน เพราะว่า $(2, 1), (2, 6) \in f^{-1}$ แต่ $1 \neq 6$

(3) ให้ $f = \{(x, y) \mid y = 2x - 3\}$ เป็นฟังก์ชันหนึ่งต่อหนึ่งบน $\mathbb{R}$
จะได้ $f^{-1} = \{(x, y) \mid (y, x) \in f\} = \{(x, y) \mid x = 2y - 3\}$ เป็นฟังก์ชันด้วย

(4) ให้ $f = \{(x, y) \mid y = x^2\}$ เป็นฟังก์ชันแต่ไม่หนึ่งต่อหนึ่งบน $\mathbb{R}$
จะได้ $f^{-1} = \{(x, y) \mid (y, x) \in f$ ที่ $y \geq 0\} = \{(x, y) \mid x = y^2$ ที่ $x \geq 0\}$
$= \{(x, y) \mid y = \pm\sqrt{x}$ ที่ $x \geq 0\}$ ไม่เป็นฟังก์ชัน □

บทนิยาม 3.15 กำหนด $f: A \to B$ ถ้า f^{-1} เป็นฟังก์ชัน จะเรียก f^{-1} ว่า**ฟังก์ชันผกผัน**ของ f และ $f^{-1}: f(A) \to A$

จะสังเกตจากตัวอย่างข้างต้นได้ว่า f^{-1} เป็นฟังก์ชัน ถ้า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง ซึ่งสามารถสรุปเป็นทฤษฎีบทได้ดังต่อไปนี้

ทฤษฎีบท 3.1 กำหนด $f: A \to B$
f มีฟังก์ชันผกผัน ก็ต่อเมื่อ f เป็นฟังก์ชันหนึ่งต่อหนึ่ง

การพิสูจน์ $(\Rightarrow)$ สมมติว่า f มี f^{-1} เป็นฟังก์ชัน จะแสดงว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง
ให้ $x_1, x_2 \in A$ และ $y \in B$ ที่ $(x_1, y), (x_2, y) \in f$
ดังนั้น $(y, x_1), (y, x_2) \in f^{-1}$
เพราะว่า f^{-1} เป็นฟังก์ชัน เพราะฉะนั้น $x_1 = x_2$
ดังนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่ง

$(\Leftarrow)$ สมมติว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง จะแสดงว่า f^{-1} เป็นฟังก์ชัน $(f^{-1}: B \to A)$
ให้ $y \in B$ และ $x_1, x_2 \in A$ ที่ $(y, x_1), (y, x_2) \in f^{-1}$ ดังนั้น $(x_1, y), (x_2, y) \in f$
เพราะว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น $x_1 = x_2$
ดังนั้น f^{-1} เป็นฟังก์ชัน □

ทฤษฎีบท 3.2 ถ้า $f: A \underset{\text{ทั่วถึง}}{\xrightarrow{1-1}} B$ แล้ว $f^{-1}: B \underset{\text{ทั่วถึง}}{\xrightarrow{1-1}} A$

บทนิยาม 3.16 ให้ A และ B เป็นเซตใด ๆ เราจะกล่าวว่า A **สมมูลกับ** B ก็ต่อเมื่อ มีฟังก์ชันหนึ่งต่อหนึ่งจาก A ไปทั่วถึง B เขียนแทนด้วย $A \sim B$

จากทฤษฎีบท 3.2 จะได้ $A \sim B$ ก็ต่อเมื่อ $B \sim A$

ตัวอย่าง 3.32 จงพิจารณาว่าเซตที่กำหนดให้สมมูลกันหรือไม่

(1) กำหนดให้ $A = \{$ก, ข, ค, ง$\}$ และ $B = \{1, 2, 3, 4\}$
เลือกฟังก์ชัน $f: A \to B$ โดยที่

$f($ก$) = 1$, $f($ข$) = 2$, $f($ค$) = 2$ และ $f($ง$) = 4$

เพราะฉะนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก A ไปทั่วถึง B
นั่นคือ $A \sim B$

(2) กำหนดให้ $A = \{2, 4, 6, 8, 10, \ldots\}$ เลือกฟังก์ชัน $f: \mathbb{N} \to A$ โดยที่

$f(m) = 2m$ ทุก $m \in \mathbb{N}$

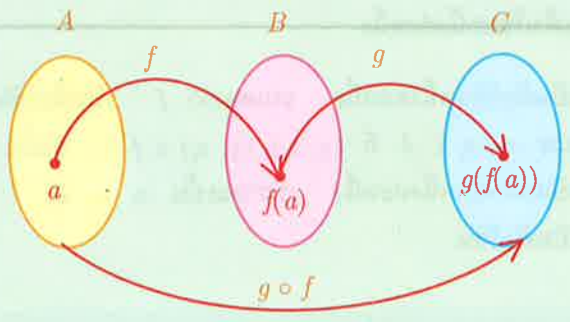
เพราะฉะนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก $\mathbb{N}$ ไปทั่วถึง A
นั่นคือ $\{2, 4, 6, 8, \ldots\} \sim \mathbb{N}$ □

ถ้าเปรียบเทียบฟังก์ชันกับการทำงานในโรงงานผลิตเสื้อสำเร็จรูป เมื่อนำผ้าผืนส่งแผนกตัดเป็นชิ้น เช่น ปก แขน ตัวเสื้อ เป็นต้น แล้วนำส่งไปแผนกเย็บเข้ารูป ก็จะได้เป็นตัวเสื้อออกมา นั่นหมายถึงถ้าให้ f เป็นแผนกตัด และ g เป็นแผนกเย็บ ถ้าใส่วัตถุดิบเข้าแผนกตัด f จะได้ผลลัพธ์ออกมา นำผลลัพธ์ที่ได้เป็นวัตถุดิบเข้าแผนก g จะได้ผลลัพธ์ออกมาเป็นตัวเสื้อนั่นเอง การพิจารณาฟังก์ชันเช่นนี้เรียกว่าฟังก์ชันประกอบดังนิยามต่อไปนี้

บทนิยาม 3.18 ให้ $f: A \to B$ และ $g: B \to C$ **ฟังก์ชันประกอบ**ของ f และ g เขียนแทนด้วย $g \circ f$ กำหนดโดย

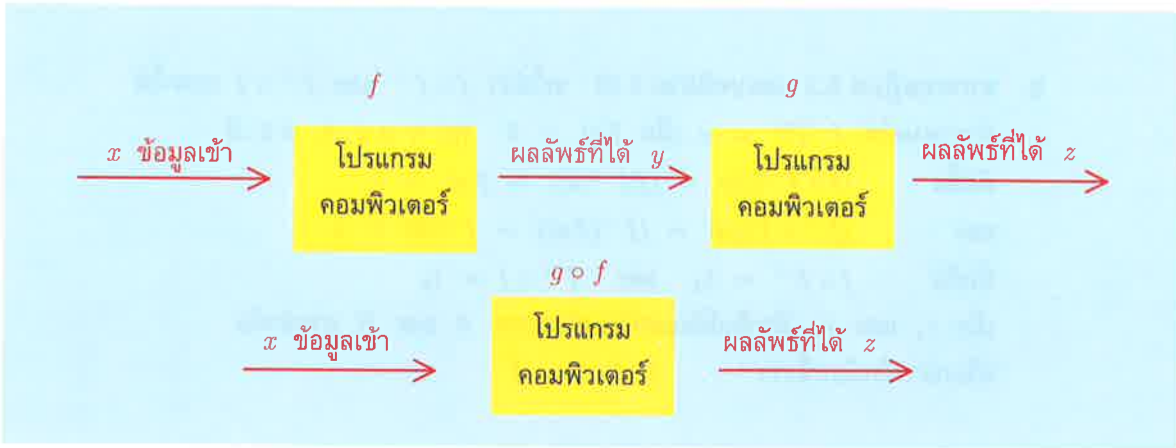
$(g \circ f)(a) = g(f(a))$ สำหรับ $a \in A$

นั่นคือ $g \circ f = \{(x, z) \mid$ มี $y \in B$, $(x, y) \in f$ และ $(y, z) \in g\}$ ดังรูป 3.17



รูป 3.17 แสดงฟังก์ชันประกอบของ f และ g

สำหรับการเขียนโปรแกรมบางครั้งก็ใช้โปรแกรมมากกว่าหนึ่งโปรแกรมเพื่อให้ได้ผลลัพธ์ เพื่อลดขั้นตอนในการประมวลผลโดยอาศัยฟังก์ชันประกอบให้เหลือเพียงโปรแกรมเดียว ดังรูป 3.18



รูป 3.18

ข้อสังเกต จากบทนิยามจะได้ว่า ฟังก์ชันประกอบของ f และ g จะหาค่าได้ ก็ต่อเมื่อ $R_f \cap D_g \neq \varnothing$

ตัวอย่าง 3.33 พิจารณาฟังก์ชันประกอบเมื่อกำหนดฟังก์ชัน f และ g ต่อไปนี้

(1) ให้ $f, g : \mathbb{Z} \to \mathbb{Z}$ กำหนดโดย $f(x) = 3x - 4$ และ $g(x) = 2x + 1$

จะได้ว่า $f \circ g$ และ $g \circ f$ หาค่าได้ โดยที่

$$(f \circ g)(x) = f(g(x)) = f(2x+1) = 3(2x+1) - 4 = 6x - 1$$

และ

$$(g \circ f)(x) = g(f(x)) = g(3x-4) = 2(3x-4) + 1 = 6x - 7$$

(2) ให้ $f, g : \mathbb{N} \to \mathbb{N}$ กำหนดโดย $f(x) = x + 1$ และ $g(x) = x - 1$

จะได้ว่า $f \circ g$ และ $g \circ f$ หาค่าได้ โดยที่

$$(f \circ g)(x) = f(g(x)) = f(x-1) = (x-1) + 1 = x$$

และ

$$(g \circ f)(x) = g(f(x)) = g(x+1) = (x+1) - 1 = x$$

□

ข้อสังเกต 1. ถึงแม้ว่า $f \circ g$ และ $g \circ f$ หาค่าได้ สำหรับฟังก์ชัน f และ g ในตัวอย่าง 3.33 จะเห็นได้ว่า การเท่ากันของฟังก์ชัน $f \circ g$ และ $g \circ f$ ไม่จำเป็นต้องเท่ากัน หรือกล่าวอีกนัยหนึ่งคือ ฟังก์ชันประกอบไม่มีสมบัติสลับที่ ตัวอย่างเช่น

$f(x)$	$g(x)$	$(g \circ f)(x)$	$(f \circ g)(x)$
$x^2 + 2$	x^8	$(x^2+2)^8$	$x^{16} + 2$
$\sin x$	x^3	$\sin^3 x$	$\sin(x^3)$
$\tan x$	$\sqrt{x}$	$\sqrt{\tan x}$	$\tan \sqrt{x}$
$\sqrt{x+2}$	$x + 3$	$\sqrt{x+2} + 3$	$\sqrt{x+5}$

2. จากทฤษฎีบท 3.2 และบทนิยาม 3.18 จะได้ว่า $f \circ f^{-1}$ และ $f^{-1} \circ f$ หาค่าได้
ถ้ากำหนดให้ $f^{-1}(b) = a$ เมื่อ $f(a) = b$ ทุก ๆ $a \in A,\ b \in B$
ดังนั้น $(f \circ f^{-1})(b) = (f(f^{-1}(b)) = f(a) = b$
และ $(f^{-1} \circ f)(a) = (f^{-1}(f(a)) = f^{-1}(b) = a$
นั่นคือ $f \circ f^{-1} = i_A$ และ $f^{-1} \circ f = i_B$
เมื่อ i_A และ i_B เป็นฟังก์ชันเอกลักษณ์บนเซต A และ B ตามลำดับ
หรือกล่าวอีกนัยหนึ่งว่า $(f^{-1})^{-1} = f$

พีชคณิตของฟังก์ชัน

ในการสร้างฟังก์ชันใหม่ไม่เพียงแต่การใช้ฟังก์ชันประกอบเท่านั้น สามารถสร้างฟังก์ชันใหม่จากการดำเนินการระหว่างฟังก์ชันสองฟังก์ชันด้วย การบวก การลบ การคูณ หรือการหาร ได้ดังบทนิยามต่อไปนี้

บทนิยาม 3.20 ถ้า f และ g เป็นฟังก์ชัน $f+g,\ f-g,\ fg$ และ f/g คือฟังก์ชันที่กำหนดโดย

$$(f+g)(x) = f(x)+g(x)$$
$$(f-g)(x) = f(x)-g(x)$$
$$(fg)(x) = f(x)+g(x)$$
$$(f/g)(x) = f(x)/g(x)$$

เรียก $f+g,\ f-g,\ fg$ และ f/g ว่า **ผลบวก ผลต่าง ผลคูณ** และ **ผลหาร**ของ f และ g ตามลำดับ และจะได้ว่า $f+g,\ f-g,\ fg$ และ f/g หาค่าได้ ก็ต่อเมื่อ

$$D_{f+g} = D_{f-g} = D_{fg} = D_f \cap D_g$$
และ $D_{f/g} = \{x \mid x \in D_f \cap D_g \text{ และ } g(x) \neq 0\}$

ตัวอย่าง 3.34 กำหนดให้ $f(x) = 1+\sqrt{x-2}$ และ $g(x) = x-3$
จงหา $f+g,\ f-g,\ fg$ และ $\dfrac{f}{g}$

วิธีทำ จากโจทย์จะได้ว่า $D_{f+g} = D_{f-g} = D_{fg} = D_f \cap D_g = \{\, x \mid x \geq 2 \,\}$ และ
$D_{f/g} = \{\, x \mid x \geq 2$ และ $x \neq 3\}$
ดังนั้น $f+g,\ f-g,\ fg$ และ $\dfrac{f}{g}$ หาค่าได้

$$(f+g)(x) = x+\sqrt{x-2}-2$$

$$(f-g)(x) = \sqrt{x-2}-x+4$$

$$(fg)(x) = x+(x-3)\sqrt{x-2}-3$$

$$(\frac{f}{g})(x) = \frac{1+\sqrt{x-2}}{x-3} \quad \text{เมื่อ } x \neq 3$$ □

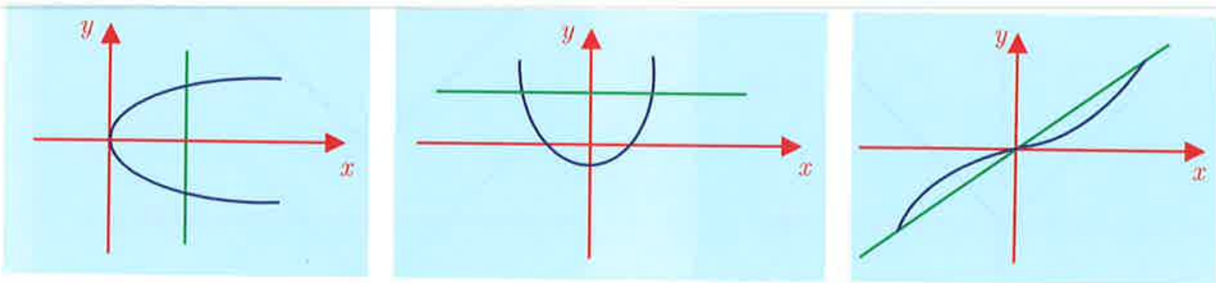
กราฟของฟังก์ชัน

ในหัวข้อนี้จะเน้นการเขียนกราฟแบบคร่าว ๆ โดยพิจารณาการเขียนกราฟของฟังก์ชันคล้ายๆกัน กราฟที่ได้จะเป็นรูปเดียวกันแต่ถูกเลื่อนไปตามแนวที่ขนานกับแกนพิกัด

บทนิยาม 3.21 กราฟของฟังก์ชัน f คือเซตของจุดในระนาบ xy ที่แต่ละจุดแทนสมาชิกของฟังก์ชัน f

เพื่อให้การเขียนกราฟทำได้สะดวกและรวดเร็ว จะนำหลักเกณฑ์ต่าง ๆ มาช่วยในการเขียนกราฟดังนี้

1. **ส่วนตัดแกน** พิจารณาจุดตัดแกน x และแกน y คือ $(x_0, 0)$ และ $(0, y_0)$ ตามลำดับ จะได้ส่วนตัดแกน x คือ $x = x_0$ และส่วนตัดแกน y คือ $y = y_0$
2. **สมมาตร** ทำการพิจารณาการสมมาตรได้ดังนี้
   - 2.1 แทน y ด้วย $-y$ ในสมการเส้นโค้งแล้วสมการคงเดิม จะได้ว่าเส้นโค้งมีสมมาตรกับแกน x ดังรูป 3.19 (1)
   - 2.2 แทน x ด้วย $-x$ ในสมการเส้นโค้งแล้วสมการคงเดิม จะได้ว่าเส้นโค้งมีสมมาตรกับแกน y ดังรูป 3.19 (2)
   - 2.3 แทน x ด้วย $-x$ และแทน y ด้วย $-y$ ในสมการเส้นโค้งแล้วสมการคงเดิม จะได้ว่าเส้นโค้งมีสมมาตรกับจุดกำเนิด ดังรูป 3.19 (3)
3. **ขอบเขต** พิจารณา โดเมน และ พิสัย



(1) (2) (3)

รูป 3.19 แสดงสมมาตร แกน x (1), สมมาตรแกน y (2) และ สมมาตรจุดกำเนิด (3)

ข้อสังเกต 1. สำหรับกราฟของฟังก์ชัน f ที่สมมาตรกับแกน y จะได้สมการ $y = f(x)$ และ $y = f(-x)$

ดังนั้น $f(x) = f(-x)$ จะเรียกฟังก์ชันนี้ว่า **ฟังก์ชันคู่**

ตัวอย่างเช่น $x^2,\ x^4,\ x^6,\ \ldots,\ \cos x$

2. สำหรับกราฟของฟังก์ชัน f ที่สมมาตรกับจุดกำเนิด

จะได้สมการ $y = f(x)$ และ $-y = f(-x)$

ดังนั้น $f(x) = -f(-x)$ จะเรียกฟังก์ชันนี้ว่า **ฟังก์ชันคี่**

ตัวอย่างเช่น $x,\ x^3,\ x^5,\ \ldots,\ \sin x$

การเลื่อนทางขนานของกราฟ

จากการเขียนกราฟของสมการ $y = f(x)$ สามารถนำมาช่วยในการเขียนกราฟของสมการ $y = f(x) + c$, $y = f(x) - c$, $y = f(x+c)$, $y = f(x-c)$ เมื่อ c เป็นค่าคงตัวบวก

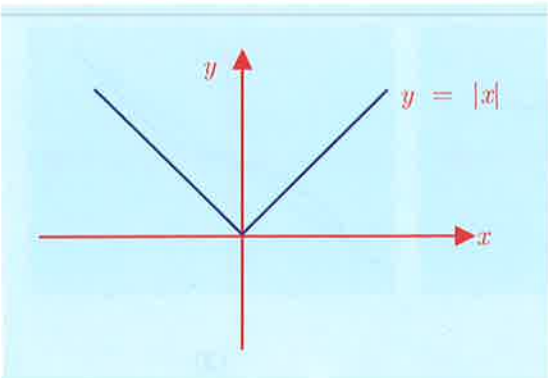
การนำค่าคงตัว c มาบวกหรือลบจาก $f(x)$ จะมีผลต่อการเขียนกราฟด้วยการเลื่อนกราฟของสมการ $y = f(x)$ ในทางขนานกับแกน y ส่วนการนำค่าคงตัว c มาบวกหรือลบจากตัวแปรอิสระ x จะมีผล ต่อการเขียนกราฟด้วยการเลื่อนกราฟของสมการ $y = f(x)$ ในทางขนานกับแกน x เช่นตัวอย่างต่อไปนี้

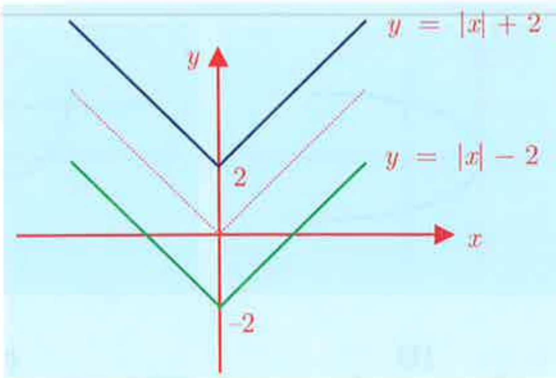
ตัวอย่าง 3.33 จงเขียนกราฟของ

(1) $y = |x| + 2$

(2) $y = |x| - 2$

วิธีทำ เริ่มต้นการเขียนกราฟด้วยกราฟของ $y = |x|$ ก่อน กราฟที่ต้องการจะเป็นการเลื่อนในทางขนานกับแกน y ดังรูป 3.20





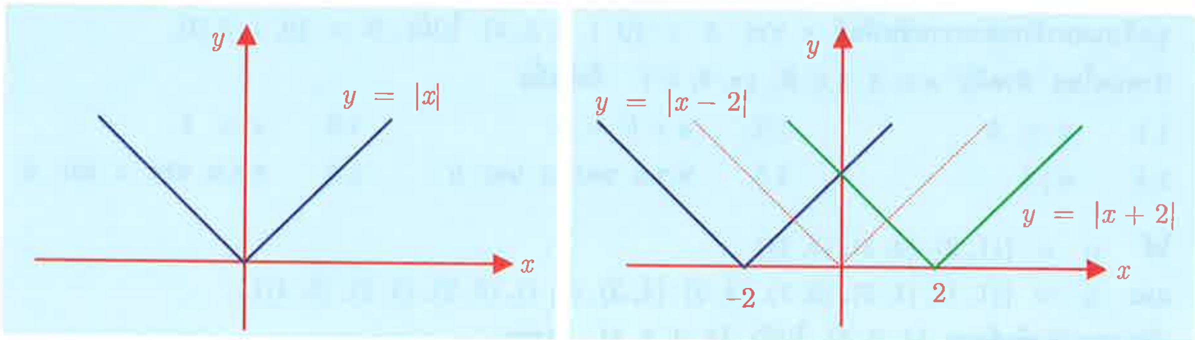
รูป 3.20 แสดงกราฟ $y = |x| + 2$ และ $y = |x| - 2$ □

ตัวอย่าง 3.34 จงเขียนกราฟของ

(1) $y = |x+2|$

(2) $y = |x-2|$

วิธีทำ เริ่มต้นการเขียนกราฟด้วยกราฟของ $y = |x|$ ก่อน กราฟที่ต้องการจะเป็นการเลื่อนในทางขนานกับแกน x ดังรูป 3.21

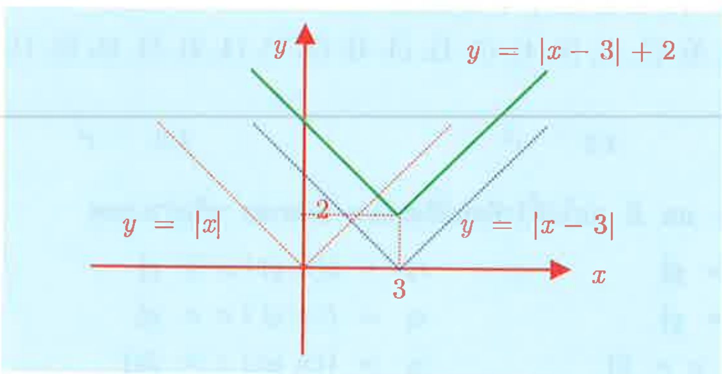


รูป 3.21 แสดงกราฟ $y = |x+2|$ และ $y = |x-2|$

$\square$

ตัวอย่าง 3.35 จงเขียนกราฟของ $y = |x-3|+2$

วิธีทำ เริ่มต้นการเขียนกราฟด้วยกราฟของ $y = |x|$ ก่อน กราฟที่ต้องการจะเป็นการเลื่อนในทางขนานกับแกน x และแกน y ดังรูป 3.22



รูป 3.21 แสดงกราฟ $y = |x-3|+2$

$\square$

แบบฝึกหัดบทที่ 3

1. จงเขียนสมาชิกของความสัมพันธ์ r จาก $A = \{0, 1, 2, 3, 4\}$ ไปยัง $B = \{0, 1, 2, 3\}$ กำหนดโดย สำหรับ $a \in A, b \in B,\ (a, b) \in r$ ก็ต่อเมื่อ

   1.1 $a = b$ 1.2 $a + b = 4$ 1.3 $a > b$

   1.4 $a \mid b$ 1.5 ห.ร.ม. ของ a และ b 1.6 ค.ร.น. ของ a และ b

2. ให้ $r_1 = \{(1, 2), (2, 3), (3, 4)\}$
   และ $r_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (3, 4)\}$
   เป็นความสัมพันธ์จาก $\{1, 2, 3\}$ ไปยัง $\{1, 2, 3, 4\}$ จงหา

   2.1 $r_1 \cup r_2$ 2.2 $r_1 \cap r_2$

   2.3 $r_1 - r_2$ 2.4 $r_2 - r_1$

3. ให้ r และ s เป็นความสัมพันธ์ที่กำหนดโดย

   $r = \{(1, 2), (1, 3), (2, 3), (2, 4), (3, 1)\}$

   $s = \{(2, 1), (3, 1), (3, 2), (4, 2)\}$

   จงหา $s \circ r$

4. ให้ r เป็นความสัมพันธ์บน $\{1, 2, 3, 4, 5\}$ กำหนดโดย
   $r = \{(1, 1), (1, 2), (1, 3), (2, 3), (2, 4), (3, 1), (3, 4), (3, 5), (4, 2), (4, 5), (5, 1), (5, 2), (5, 4)\}$
   จงหา

   4.1 r^2 4.2 r^3 4.3 r^4

5. จงพิจารณาความสัมพันธ์ r บน $\mathbb{Z}$ ต่อไปนี้ว่ามีสมบัติสะท้อน สมมาตร หรือถ่ายทอด

   $r_1 = \{(x, y) \mid x = y\}$ $r_2 = \{(x, y) \mid x \geq y\}$

   $r_3 = \{(x, y) \mid x \neq y\}$ $r_4 = \{(x, y) \mid x < y\}$

   $r_5 = \{(x, y) \mid x - y = 3\}$ $r_6 = \{(x, y) \mid x = 2y\}$

6. จงพิจารณาว่าความสัมพันธ์บนเซต X ต่อไปนี้เป็นความสัมพันธ์สมมูลหรือไม่ ถ้าไม่จงบอกว่าขาดสมบัติข้อใด

ความสัมพันธ์ r	เซต X
พื้นที่เท่ากัน	รูปสามเหลี่ยมในระนาบ
ตั้งฉากกัน	เส้นตรงในระนาบ
สูงกว่า	คน

7. กำหนดให้ $r = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid$ มี $k \in \mathbb{Z}$ ที่ $x - y = 7k\}$
จงแสดงว่า r เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$

8. กำหนด $A = \mathbb{N} \times \mathbb{N}$ จงพิจารณาว่า r เป็นความสัมพันธ์สมมูลบน A หรือไม่ เมื่อกำหนด
   8.1 $(a, b)\ r\ (c, d)$ ก็ต่อเมื่อ $a + d = b + c$
   8.2 $(a, b)\ r\ (c, d)$ ก็ต่อเมื่อ $\sqrt{a^2 + b^2} = \sqrt{c^2 + d^2}$
   8.3 $(a, b)\ r\ (c, d)$ ก็ต่อเมื่อ $ad = bc$

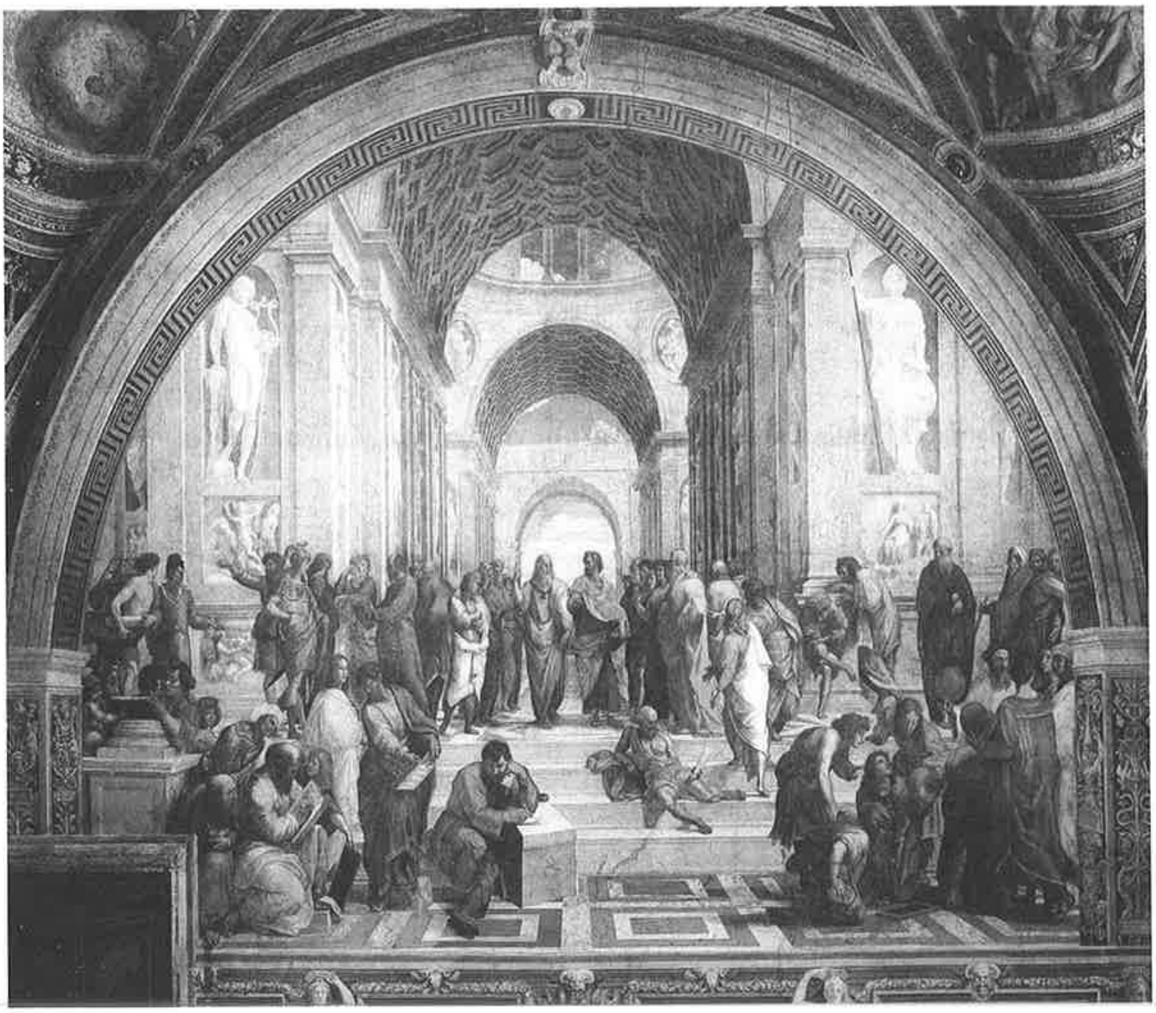
9. จงพิจารณาว่าเซตใดต่อไปนี้เป็นฟังก์ชัน เมื่อกำหนดให้โดเมนของทุกเซตเป็นจำนวนจริง
   9.1 $\{(x, y) \mid y = x + 3\}$
   9.2 $\{(x, y) \mid y = x^2 + 3x - 2\}$
   9.3 $\{(x, y) \mid x = 7\}$
   9.4 $\{(x, y) \mid x = y + 1\}$
   9.3 $\{(x, y) \mid y < x\}$

10. จงพิจารณาว่าฟังก์ชันต่อไปนี้เป็นฟังก์ชันหนึ่งต่อหนึ่งหรือไม่ ถ้าเป็น จงหาฟังก์ชันผกผันด้วย
   10.1 $f(x) = x + 3$
   10.2 $f(x) = x^2 - 3x + 2$
   10.3 $f(x) = \dfrac{x+1}{x-2}$
   10.4 $f(x) = \begin{cases} 3\ ; & x \le -2 \\ 1\ ; & -2 < x \le 3 \\ 0\ ; & x > 3 \end{cases}$
   10.5 $f(x) = x + \dfrac{1}{x}$

11. จงหารูปแบบของฟังก์ชัน $f + g$, $f - g$, fg และ $\dfrac{f}{g}$ เมื่อกำหนด f และ g ดังต่อไปนี้
   11.1 $f(x) = 3x - 2,\ g(x) = |x|$
   11.2 $f(x) = 2x,\ g(x) = x + 1$
   11.3 $f(x) = \dfrac{x}{1+x},\ g(x) = \dfrac{1}{x}$

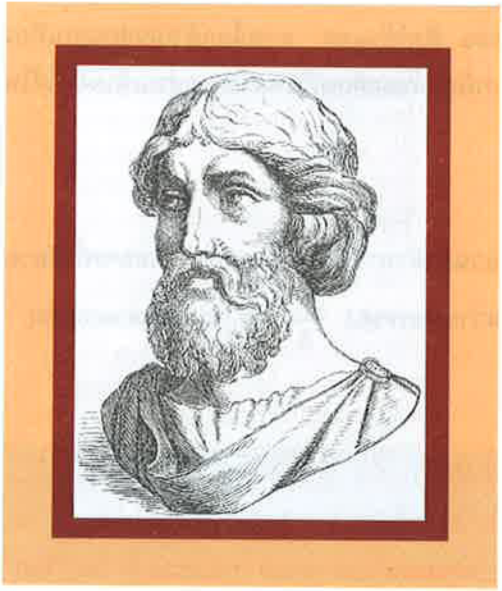
12. กำหนดให้ $f(x) = \sqrt{x}$ และ $g(x) = x + 1$ จงหา
   12.1 $f(g(2))$
   12.2 $g(f(4))$
   12.3 $g(g(1))$
   12.4 $g(f(f(16)))$

13. จงเขียนกราฟของสมการต่อไปนี้โดยวิธีของการเลื่อน
   13.1 $y = |x + 2| - 1$
   13.2 $y = 1 - |x - 2|$
   13.3 $y = 1 + (x - 2)$
   13.4 $y = 2 - (x + 1)$



โรงเรียนของปีทาโกรัส
ณ กรุงเอเธน
ประเทศกรีซ

ทฤษฎีจำนวน



ปีทาโกรัสแห่งซามอส
ประมาณ 580 – 496 ปีก่อนคริสต์ศักราช, กรีซ

เราได้ใช้ความรู้ในเรื่องของจำนวนในชีวิตประจำวันอยู่ตลอดเวลา จำนวนได้มีพัฒนาการมาตั้งแต่สมัยโบราณ และมีการเขียนสัญลักษณ์ขึ้นสำหรับแทนจำนวนที่เรียกว่า **ตัวเลข**

ทฤษฎีจำนวนเป็นสาขาหนึ่งในวิชาคณิตศาสตร์ที่เกิดขึ้นมานานมากกว่า 4000 ปีแล้ว เป็นสาขาที่ศึกษาเกี่ยวกับสมบัติของจำนวนเต็ม ซึ่งคือ จำนวน

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

จากบันทึกที่เป็นหลักฐานชิ้นแรกเป็นของเมโสโปเตเมีย (Mesopotamia [2000 ปีก่อนคริสตกาล]) ซึ่งปรากฏในหนังสือที่ชื่อว่า "*concrete problems and only one solution given with no attempt to generalize*" ต่อมา ปีทาโกรัส (Pythagorus [550 ปีก่อนคริสตกาล]) เป็นผู้ที่ศึกษาเกี่ยวกับสมบัติและความจริงต่าง ๆ ของ

จำนวนเต็มบวก แต่งานเขียนชิ้นแรกของทฤษฎีจำนวนที่เป็นระบบนั้นเป็นของยุคลิด (Euclid [300 ปีก่อนคริสตกาล]) ที่ชื่อว่า "*Euclid's Elements*" ซึ่งจะมีกฎที่สำคัญ ๆ ทางเลขคณิต เช่น ขั้นตอนวิธีของยุคลิด จำนวนเฉพาะมีเป็นจำนวนอนันต์ตัว และทฤษฎีบทพื้นฐานทางเลขคณิตของจำนวนเฉพาะ เป็นต้น

จำนวนเต็มกับการหารลงตัว

ในหัวข้อนี้จะศึกษาสมบัติพื้นฐานและบทนิยามที่สำคัญของจำนวนเต็มรวมถึงวิธีการพิสูจน์ทฤษฎีบทต่าง ๆ เช่น ตัวหารร่วมมาก ตัวคูณร่วมน้อย จำนวนเฉพาะ ทฤษฎีบทหลักมูลของเลขคณิต ขั้นตอนวิธีการหารและคอนกรูเอนซ์ โดยความรู้ที่กล่าวมานี้ล้วนแล้วแต่มีแนวความคิดมาจากเรื่องการหารลงตัว นอกจากนี้ยังจะกล่าวถึงการนำไปประยุกต์ใช้ในสาขาวิชาวิทยาการคอมพิวเตอร์ เช่น ฟังก์ชันแฮช การเลือกตัวเลขสุ่มแบบเทียม การรักษาความปลอดภัยของข้อมูลโดยการเข้ารหัส เป็นต้น สำหรับบทพิสูจน์ของทฤษฎีบทสามารถอ่านเพิ่มเติมได้ในภาคผนวก

การหารลงตัว

พิจารณาจำนวนเต็มสองจำนวนซึ่งตัวหารไม่เท่ากับศูนย์ ผลหารที่ได้อาจเป็นหรือไม่เป็นจำนวนเต็มก็ได้ เช่น $\frac{27}{3} = 9$, $\frac{15}{2} = 7.5$ จะเห็นว่าผลหารของ $\frac{27}{3}$ คือ 9 เป็นจำนวนเต็ม ซึ่งเราจะกล่าวว่า 3 หาร 27 ลงตัว ดังบทนิยามต่อไปนี้

บทนิยาม 4.1 ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ จะกล่าวว่า
***a* หาร *b* ลงตัว** ก็ต่อเมื่อ มีจำนวนเต็ม c ซึ่งทำให้ $b = ac$ เขียนแทนด้วย $a \mid b$
เรียก a ว่า **ตัวประกอบหรือตัวหารตัวหนึ่งของ** b และเรียก b ว่า **พหุคูณของ *a***
และถ้า a หาร b ไม่ลงตัว เขียนแทนด้วย $a \nmid b$

ตัวอย่าง 4.1 จงพิจารณาว่า $4 \mid 20$, $7 \mid (-42)$, $21 \mid 0$ และ $10 \mid 18$ หรือไม่

วิธีทำ เนื่องจาก $20 = 4(5)$, $-42 = 7(-6)$ และ $0 = 21(0)$
ดังนั้น $4 \mid 20$, $7 \mid (-42)$ และ $21 \mid 0$ ตามลำดับ
และเนื่องจาก $\frac{18}{10} = 1.8$ ไม่เป็นจำนวนเต็ม จะได้ว่า $10 \nmid 18$ □

หมายเหตุ ในการใช้สัญลักษณ์ $a \mid b$ จะหมายถึง ตัวหาร $a \neq 0$

ข้อสังเกต สำหรับจำนวนเต็ม a และ b ใด ๆ จะเห็นได้โดยง่ายว่า

1. ถ้า $a \neq 0$ แล้ว $a \mid 0$ และ $a \mid a$
2. $a \mid 1$ ก็ต่อเมื่อ $a = 1$ หรือ $a = -1$

ตัวอย่าง 4.2 จงหาเซตของตัวหารทั้งหมดของ 100

วิธีทำ ให้ A แทนเซตของตัวหารทั้งหมดของ 100 ดังนั้นได้

$$A = \{-100, -50, -25, -20, -10, -5, -4, -2, -1, 1, 2, 4, 5, 10, 20, 25, 50, 100\}$$ □

บทนิยาม 4.2 ให้ x เป็นจำนวนจริงใด ๆ
ฟังก์ชันจำนวนเต็มมากสุดของ x เขียนแทนด้วยสัญลักษณ์ $[x]$ หมายถึงจำนวนเต็มที่มากที่สุดซึ่งน้อยกว่าหรือเท่ากับ x

ตัวอย่าง 4.3 $[50.9] = 50$, $[-1.2] = -2$, $[10] = 10$ และ $\left[\dfrac{100}{6}\right] = 16$ □

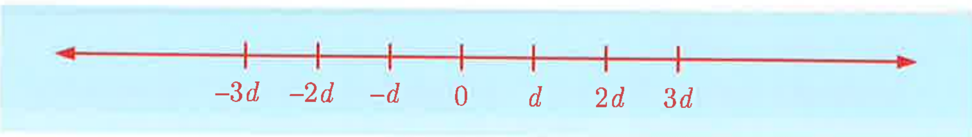
ตัวอย่าง 4.4 ให้

$$\begin{aligned} \mathscr{U} &= \{1, 2, 3, \dots, 100\} \\ A &= \{x \in \mathscr{U} \mid 2 \text{ หาร } x \text{ ลงตัว}\} \\ B &= \{x \in \mathscr{U} \mid 6 \text{ หาร } x \text{ ลงตัว}\} \\ \text{และ } C &= \{x \in \mathscr{U} \mid 7 \text{ หาร } x \text{ ลงตัว}\} \end{aligned}$$

จงหา $n(A)$, $n(B)$ และ $n(C)$

วิธีทำ $n(A) = \left[\dfrac{100}{2}\right] = 50$, $n(B) = \left[\dfrac{100}{6}\right] = 16$ และ $n(C) = \left[\dfrac{100}{7}\right] = 14$ □

ข้อสังเกต จากตัวอย่าง 4.4 สามารถสรุปเป็นกรณีทั่วไป ได้ดังนี้
ให้ $\mathscr{U} = \{1, 2, 3, \dots, n\}$ และ d เป็นจำนวนเต็มบวกและให้ $A = \{x \in \mathscr{U} \mid d \text{ หาร } x \text{ ลงตัว}\}$ จะได้ว่า จำนวนเต็มบวกที่หารด้วย d ลงตัว คือ จำนวนเต็มที่อยู่ในรูป dk โดยที่ k เป็นจำนวนเต็มบวก



ดังนั้นได้จำนวนเต็มบวกที่หารด้วย d ลงตัวและจำนวนนั้นมีค่าน้อยกว่าหรือเท่ากับ n คือจำนวนของจำนวนเต็มบวก k ซึ่ง $0 < dk \leq n$ หรือ $0 < k \leq \dfrac{n}{d}$

เพราะฉะนั้น $n(A) = \left[\dfrac{n}{d}\right]$

นั่นคือ จำนวนที่มีค่าไม่เกิน n ที่หารด้วยจำนวนเต็มบวก d ลงตัว มี $\left[\dfrac{n}{d}\right]$ จำนวน

การศึกษาเกี่ยวกับการหารลงตัว ยังมีสมบัติพื้นฐานที่ควรทราบซึ่งจะนำไปใช้ในการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็ม ดังต่อไปนี้

ทฤษฎีบท 4.1 สำหรับจำนวนเต็ม a, b และ c ใด ๆ จะได้ว่า

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

(ii) ถ้า $a \mid b$ แล้ว $a \mid bc$

(iii) ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$

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

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

ตัวอย่าง 4.5 พิจารณาการสมบัติของการหารลงตัว

(1) เนื่องจาก $-3 \mid 42$ และ $42 \mid 378$ ดังนั้นได้ $-3 \mid 378$

(2) เนื่องจาก $13 \mid 65$ ดังนั้น $13 \mid 65(15)$ นั่นคือ $13 \mid 975$

(3) เนื่องจาก $-7 \mid -35$ และ $-35 \neq 0$ ดังนั้น $|-7| \leq |-35|$ นั่นคือ $7 \leq 35$

(4) เนื่องจาก $8 \mid 168$ และ $8 \mid 24$ ดังนั้น $8 \mid (168 + 24)$ นั่นคือ $8 \mid 192$

(5) เนื่องจาก $11 \mid (33 + 143)$ และ $11 \mid 33$ ดังนั้น $11 \mid 143$ □

จำนวนเฉพาะ

สำหรับทุกจำนวนเต็มบวกที่มากกว่า 1 จะมีตัวหารที่เป็นบวกอย่างน้อยสองตัว คือ 1 และตัวมันเอง และถ้าจำนวนเต็มนั้นมีตัวหารที่เป็นบวกสองตัวนี้เท่านั้น จะเรียกจำนวนเต็มบวกนั้นว่า จำนวนเฉพาะ การประยุกต์ทางทฤษฎีจำนวนเรื่องหนึ่ง คือ การเข้ารหัสและถอดรหัสนั้น จำเป็นต้องใช้จำนวนเต็มบวกที่เป็นจำนวนเฉพาะ ในหัวข้อนี้เราจะศึกษาสมบัติพื้นฐานของจำนวนเฉพาะก่อนดังนี้

บทนิยาม 4.3 จำนวนเต็มบวก p ที่มากกว่า 1 จะเรียกว่า **จำนวนเฉพาะ** ก็ต่อเมื่อ ตัวประกอบที่เป็นบวกของ p คือ 1 และ p เท่านั้น
และเรียกจำนวนเต็มบวกที่มากกว่า 1 ซึ่งไม่เป็นจำนวนเฉพาะว่า **จำนวนประกอบ**

ตัวอย่าง 4.6 11 เป็นจำนวนเฉพาะ เพราะมีตัวประกอบที่เป็นบวก คือ 1 และ 11 เท่านั้น
15 เป็นจำนวนประกอบ เพราะมีตัวประกอบที่เป็นบวก คือ 3 และ 5 □

ทฤษฎีบท 4.2 *ทฤษฎีบทหลักมูลของเลขคณิต*
ทุกจำนวนเต็มบวก n ที่มากกว่า 1 จะได้ว่า n เป็นจำนวนเฉพาะหรือ n สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะได้เพียงแบบเดียวเท่านั้น โดยไม่คำนึงถึงตำแหน่งของจำนวนเฉพาะในผลคูณ

ข้อสังเกต ทฤษฎีบทหลักมูลของเลขคณิตสามารถกล่าวได้อีกแบบโดยใช้หลักการจัดอันดับการคูณ คือ
"ทุกจำนวนเต็มบวก n ที่มากกว่า 1 จะได้ว่า n เป็นจำนวนเฉพาะหรือ n สามารถแยกตัวประกอบ

ที่เป็นจำนวนเฉพาะได้เพียงรูปเดียวเท่านั้น คือ

$$n = p_1^{c_1} p_2^{c_2} p_3^{c_3} \cdots p_k^{c_k}$$

โดยที่ $p_1 < p_2 < \ldots < p_k$ และ p_i เป็นจำนวนเฉพาะ c_i เป็นจำนวนเต็มบวก ทุก $i = 1, 2, \ldots, k$"

และเรียก n ที่อยู่ในรูปนี้ว่า **รูปแบบบัญญัติ**

ตัวอย่าง 4.7 รูปแบบบัญญัติ ของ 300, 101, 693 และ 2048 คือ

$$\begin{aligned} 300 &= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3 \cdot 5^2 \\ 101 &= 101 \\ 693 &= 3 \cdot 3 \cdot 7 \cdot 11 = 3^2 \cdot 7 \cdot 11 \\ 2048 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{11} \end{aligned}$$

□

ในการพิจารณาว่าจำนวนเต็มบวกที่มีค่ามาก ๆ จำนวนนั้นเป็นจำนวนเฉพาะหรือไม่ เราจะใช้ทฤษฎีบทที่จะกล่าวถึงต่อไปนี้

ทฤษฎีบท 4.3 ถ้า n เป็นจำนวนประกอบที่มากกว่า 1 แล้ว n จะมีตัวหารที่เป็นจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$

ข้อสังเกต จากทฤษฎีบท 4.3 ได้ว่า

"ถ้า n ไม่มีตัวหารที่เป็นจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$ แล้วจะได้ว่า n จะเป็นจำนวนเฉพาะ"

ซึ่งเราจะนำไปใช้ในการทดสอบว่าจำนวนนั้นเป็นจำนวนเฉพาะหรือไม่ ดังตัวอย่าง

ตัวอย่าง 4.8 จงแสดงว่า 103 เป็นจำนวนเฉพาะ

วิธีทำ จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{103}$ คือ 2, 3, 5 และ 7

เนื่องจาก 2, 3, 5 และ 7 หาร 103 ไม่ลงตัว ดังนั้นได้ 103 เป็นจำนวนเฉพาะ □

ตัวอย่าง 4.9 จงแสดงว่า 2873 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{2873}$ คือ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 และ 53

เนื่องจาก 13 หาร 2873 ลงตัว ดังนั้นได้ 2873 เป็นจำนวนประกอบ □

เนื่องจากทุกจำนวนเต็มบวก n ซึ่งมากกว่า 1 จะมีตัวประกอบที่เป็นจำนวนเฉพาะเสมอ จากตัวอย่าง 4.9 สามารถหาตัวประกอบที่เป็นจำนวนเฉพาะได้เพียงบางตัวเท่านั้น ขั้นตอนที่จะกล่าวต่อไปนี้เป็นประโยชน์อย่างมากที่จะหาตัวประกอบที่เป็นจำนวนเฉพาะทุกตัวของ n

ขั้นตอนการหาตัวประกอบที่เป็นจำนวนเฉพาะของ n

1. หา $\sqrt{n}$
2. หาจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$
3. พิจารณาว่าจำนวนเฉพาะ p ในขั้นที่ 2. จำนวนใดที่เป็นตัวประกอบของ n บ้าง โดยเริ่มจากจำนวนเฉพาะที่มี ค่าน้อยที่สุดก่อน
   - 3.1 ถ้าไม่มีจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$ จำนวนใดเลยที่หาร n ลงตัว จะได้ว่า n จะเป็นจำนวนเฉพาะ จบขั้นตอนการหาตัวประกอบที่เป็นจำนวนเฉพาะของ n
   - 3.2 ถ้ามีจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$ และหาร n ลงตัว แล้วจะได้ว่า n จะเป็นจำนวนประกอบ ซึ่งในขั้นตอนนี้ เราจะพบตัวประกอบที่เป็นจำนวนเฉพาะตัวหนึ่งของ n เท่านั้น สมมติให้เป็น p_1 ดังนั้นได้ $\frac{n}{p_1}$ เป็นจำนวนเต็ม ทำขั้นที่ 4. ต่อ
4. ทำซ้ำขั้นที่ 1., 2. และ 3. กับจำนวน $\frac{n}{p_1}$ ซึ่งจะสังเกตเห็นว่า ถ้า $\frac{n}{p_1}$ มีตัวประกอบที่เป็นจำนวนเฉพาะให้เป็น p_2 แล้วจะได้ว่า $p_1 \leq p_2$ และ $\frac{n}{p_1p_2}$ เป็นจำนวนเต็ม
5. ทำซ้ำขั้นที่ 1., 2. และ 3. กับจำนวน $\frac{n}{p_1p_2}$ เช่นนี้ไปเรื่อย ๆ

ขั้นตอนการหาตัวประกอบที่เป็นจำนวนเฉพาะของ n นี้จะจบลงเมื่อ $\frac{n}{p_1p_2\cdots p_k}$ เป็นจำนวนเฉพาะ ดังตัวอย่าง

ตัวอย่าง 4.10 จงหาตัวประกอบที่เป็นจำนวนเฉพาะของ 77077 มาทั้งหมด

วิธีทำ 1. $\sqrt{77077} < 278$

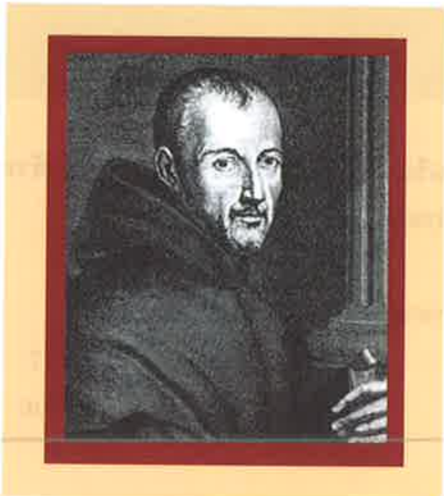
2. จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{77077}$ คือ 2, 3, 5, 7, ..., 277
3. จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{77077}$ ตัวที่มีค่าน้อยที่สุด คือ 2 แต่ 2 หาร 77077 ไม่ลงตัว พิจารณาจำนวนเฉพาะตัวถัดไป คือ 3 และ 5 ซึ่งจะได้ว่า 3 และ 5 หาร 77077 ไม่ลงตัวเช่นกัน พิจารณาจำนวนเฉพาะตัวถัดไปอีก คือ 7
   เนื่องจาก 7 หาร 77077 ลงตัว ดังนั้นได้ 7 เป็นตัวประกอบตัวหนึ่งของ 77077
4. ต่อไปพิจารณาจำนวน $\frac{77077}{7} = 11011$ ทำซ้ำขั้นที่ 1., 2. และ 3. อีก ดังนี้
   จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{11011}$ ตัวที่มีค่าน้อยที่สุด คือ 2, 3 และ 5
   แต่ทั้งสามจำนวนจะหาร 11011 ไม่ลงตัวแน่นอนจากขั้นตอนที่ 3 เลยเริ่มพิจารณาจำนวนเฉพาะตัวถัดมา คือ 7 เนื่องจาก 7 หาร 11011 ลงตัว ดังนั้นได้ 7 เป็นตัวประกอบอีกตัวหนึ่งของ 11011
5. ต่อไปพิจารณาจำนวน $\frac{11011}{7} = 1573$ ทำซ้ำขั้นที่ 1., 2. และ 3. อีก ดังนี้
   จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{1573}$ ตัวที่มีค่าน้อยที่สุด คือ 2, 3 และ 5
   แต่ทั้งสามจำนวนจะหาร 1573 ไม่ลงตัวแน่นอน จากขั้นตอนที่ 4. มาพิจารณาจำนวนเฉพาะตัวถัดมา คือ 7 แต่ 7 หาร 1573 ไม่ลงตัว ดังนั้นพิจารณาจำนวนเฉพาะตัวถัดไปอีก คือ 11 พบว่า 11 หาร 1573 ลงตัว และ $\frac{1573}{11} = 143$

6. ต่อไปพิจารณาจำนวน $\frac{1573}{11} = 143$ ทำซ้ำขั้นที่ 1., 2. และ 3. อีก ดังนี้
จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{143}$ ตัวที่มีค่าน้อยที่สุด คือ $2, 3, 5$ และ 7
แต่ทั้งสี่จำนวนจะหาร 143 ไม่ลงตัวแน่นอนจากขั้นตอนที่ 5 พิจารณาจำนวนเฉพาะตัวถัดมาอีก คือ 11
พบว่า 11 หาร 143 ลงตัว และ $\frac{143}{11} = 13$ ซึ่ง 13 เป็นจำนวนเฉพาะ
จึงจบขั้นตอนการหาตัวประกอบที่เป็นจำนวนเฉพาะนี้ ดังนั้นได้

$$77077 = 7 \cdot 7 \cdot 11 \cdot 11 \cdot 13 = 7^2 \cdot 11^2 \cdot 13 \qquad \square$$

จำนวนเฉพาะได้มีการศึกษากันมาเป็นเวลานานแล้ว และสงสัยว่าจำนวนเฉพาะตัวที่มีค่ามากที่สุดคือจำนวนใด ยุคลิดได้พบความจริงที่สำคัญมาก คือ จำนวนเฉพาะมีอยู่เป็นจำนวนอนันต์ตัว นั่นหมายความว่าไม่มีจำนวนเฉพาะที่มีค่ามากที่สุด ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.4 จำนวนเฉพาะมีอยู่เป็นจำนวนอนันต์ตัว



แมร์เซน, มาริน
ค.ศ. 1588 – 1648, ฝรั่งเศส

ในช่วง 300 ปีที่ผ่านมานี้ได้มีการค้นพบจำนวนเฉพาะที่มีค่ามากและมากขึ้นเรื่อย ๆ จำนวนเฉพาะรูปหนึ่งที่น่าสนใจ คือ $2^p - 1$ โดยที่ p เป็นจำนวนเฉพาะ เรียกจำนวนที่อยู่ในรูปนี้ว่า **จำนวนเฉพาะแมร์เซน** เพราะค้นพบโดย มาริน แมร์เซน บาทหลวงชาวฝรั่งเศส ในศตวรรษที่ 17 ซึ่งจำนวนที่อยู่ในรูป $2^p - 1$ นี้บางจำนวนเป็นจำนวนเฉพาะแต่บางจำนวนก็เป็นจำนวนประกอบ เช่น

$2^2 - 1 = 3,\ 2^3 - 1 = 7$ และ $2^5 - 1 = 31$ เป็นจำนวนเฉพาะแมร์เซน

แต่ $2^{11} - 1 = 2047 = 23 \cdot 89$ ไม่เป็นจำนวนเฉพาะแมร์เซน

ในปัจจุบันเราได้ใช้ซุปเปอร์คอมพิวเตอร์ช่วยในการค้นหาจำนวนเฉพาะแมร์เซน ด้วยวิธีการ Lucas – Lehmer test โดยการนำจำนวนเฉพาะแมร์เซนตัวก่อนหน้ามาแทนลงในสูตร $2^p - 1$ ก็จะได้จำนวนแมร์เซนตัวใหม่ขึ้นมาแล้วต้องตรวจสอบว่าเป็นจำนวนเฉพาะหรือไม่ เมื่อเดือนธันวาคม พ.ศ. 2546 ได้ค้นพบจำนวนเฉพาะแมร์เซนแล้ว 40 จำนวน และจำนวนที่มีค่ามากที่สุดเท่าที่ทราบ คือ $2^{20996011} - 1$ ซึ่งเป็นจำนวนเฉพาะที่มีขนาดใหญ่มากกว่า 6 ล้านหลัก

ขั้นตอนวิธีการหาร

จำนวนเต็มสองจำนวนอาจจะหารกันลงตัวหรือไม่ก็ได้ อย่างไรก็ตามจะได้ว่า ถ้าตัวหารเป็นจำนวนเต็มที่ไม่เป็นศูนย์ แล้วจะได้ผลหารและเศษที่เหลือจากการหาร ดังขั้นตอนวิธีการหารที่จะกล่าวต่อไปนี้

ทฤษฎีบท 4.5 *ขั้นตอนวิธีการหาร*
ให้ a และ b เป็นจำนวนเต็ม ซึ่ง $b \neq 0$ จะได้ว่า มีจำนวนเต็ม q และ r คู่เดียวเท่านั้นที่ทำให้

$$a = bq + r \quad \text{โดยที่ } 0 \leq r < |b| \qquad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

หมายเหตุ จากขั้นตอนวิธีการหาร จะเรียก a ว่า **ตัวตั้ง**, เรียก b ว่า **ตัวหาร**, เรียก q ว่า **ผลหาร** และเรียก r ว่า **เศษที่เหลือจากการหาร a ด้วย b**

ตัวอย่าง 4.11 จงหาเศษ r จากการหาร

(1) 400 ด้วย 120 (2) 5 ด้วย 7

(3) 140 ด้วย –72 (4) –175 ด้วย 50

(5) –245 ด้วย –70

วิธีทำ

(1) เนื่องจาก $400 = 120(3) + 40$ ดังนั้น $r = 40$

(2) เนื่องจาก $5 = 7(0) + 5$ ดังนั้น $r = 5$

(3) เนื่องจาก $140 = -72(-1) + 68$ ดังนั้น $r = 68$

(4) เนื่องจาก $-175 = 50(-4) + 25$ ดังนั้น $r = 25$

(5) เนื่องจาก $-245 = -70(4) + 35$ ดังนั้น $r = 35$ □

ข้อสังเกต ทฤษฎีบท 4.5 เป็นทฤษฎีที่แสดงความสัมพันธ์ระหว่างตัวตั้ง ตัวหาร ผลหาร และเศษในรูป

ตัวตั้ง = ตัวหาร · ผลหาร + เศษ

โดยเศษที่เหลือจะมีค่ามากกว่าหรือเท่ากับ 0 แต่ต้องน้อยกว่าค่าสัมบูรณ์ของตัวหาร

ในกรณีเศษเป็น 0 จะได้ว่า a หาร b ลงตัว ดังนั้นจะเห็นว่าเมื่อหารจำนวนเต็ม a ใด ๆ ด้วย 2

จะได้ว่า r เป็น 0 หรือ 1

ถ้า $r = 0$ จะเรียก a ว่าเป็น **จำนวนคู่** และถ้า $r = 1$ จะเรียก a ว่าเป็น **จำนวนคี่**

ตัวหารร่วมมากและตัวคูณร่วมน้อย

พิจารณาจำนวนเต็มที่หารทั้ง a และ b ลงตัว ซึ่งเราเรียกว่า **ตัวหารร่วม** ดังตัวอย่างต่อไปนี้

ตัวอย่าง 4.12 จงหาเซตของตัวหารร่วมทั้งหมดของ 100 และ 152

วิธีทำ ให้ A และ B แทนเซตของตัวหารทั้งหมดของ 100 และ 152 ตามลำดับ ดังนั้นได้

$$A = \{-100, -50, -25, -20, -10, -5, -4, -2, -1, 1, 2, 4, 5, 10, 20, 25, 50, 100\}$$

และ $$B = \{-152, -76, -38, -19, -8, -4, -2, -1, 1, 2, 4, 8, 19, 38, 76, 152\}$$

เพราะฉะนั้น $A \cap B = \{-4, -2, -1, 1, 2, 4\}$

ดังนั้นเซตของตัวหารร่วมทั้งหมดของ 100 และ 152 คือ $\{-4, -2, -1, 1, 2, 4\}$ □

ข้อสังเกต กรณีที่ $a = 0$ และ $b = 0$ แล้วจะได้ว่าจำนวนเต็มทุกจำนวนที่ไม่เป็นศูนย์จะเป็นตัวหารร่วมของ a และ b ดังนั้นได้ว่า ตัวหารร่วมของ a และ b มีจำนวนไม่จำกัด

กรณีที่ $a \neq 0$ หรือ $b \neq 0$ แล้วตัวหารร่วมของ a และ b มีจำนวนจำกัด เนื่องจาก d เป็นตัวหารร่วมของ a และ b ก็ต่อเมื่อ $-d$ เป็นตัวหารร่วมของ a และ b

ดังนั้นจะพิจารณาหาตัวหารร่วมของ a และ b เฉพาะที่เป็นจำนวนเต็มบวกเท่านั้น และเป็นตัวหารร่วมที่มีค่ามากที่สุด ดังบทนิยามต่อไปนี้

บทนิยาม 4.4 ให้ a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกัน และ d เป็นจำนวนเต็มบวก จะกล่าวว่า d เป็น **ตัวหารร่วมมากของ a กับ b** ก็ต่อเมื่อ

1. $d \mid a$ และ $d \mid b$

และ 2. ถ้า c เป็นจำนวนเต็มบวกซึ่ง $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$

เขียนแทนตัวหารร่วมมากของ a และ b ด้วย (a, b) และเรียกย่อ ๆ ว่า **ห.ร.ม.**

นั่นคือ ห.ร.ม. หมายถึง ตัวหารร่วมของทั้ง a และ b ที่เป็นบวกซึ่งมีค่ามากที่สุดนั่นเอง

ตัวอย่าง 4.13 จงหา $(36, 48)$, $(17, 22)$ และ $(-8, 0)$

วิธีทำ ตัวหารร่วมที่เป็นบวกของ 36 และ 48 คือ 1, 2, 3, 4, 6, 12 ดังนั้นได้ $(36, 48) = 12$

ตัวหารร่วมที่เป็นบวกของ 17 และ 22 คือ 1 ดังนั้นได้ $(17, 22) = 1$

ตัวหารร่วมที่เป็นบวกของ -8 และ 0 คือ 1, 2, 4, 8 ดังนั้นได้ $(-8, 0) = 8$ □

ข้อสังเกต ถ้า a และ b เป็นจำนวนเต็มซึ่งเป็นศูนย์ไม่พร้อมกัน จะได้ว่า

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

ตัวอย่าง 4.14 จากข้อสังเกตข้างต้น จะได้ว่า

(1) $(12, 20) = 4$

(2) $(6, 15) = (6, -15) = (-6, 15) = (-6, -15) = (15, 6) = 3$

(3) $(-7, 0) = |-7| = 7$

(4) เนื่องจาก $-8 \mid 16$ ดังนั้น $(-8, 16) = |-8| = 8$

(5) เนื่องจาก $7 \mid 42$ และ $7 \mid 56$ ดังนั้น $7 \mid (42, 56)$ นั่นคือ $7 \mid 14$ □

ผลที่สำคัญอีกประการหนึ่งคือเราสามารถเขียน ห.ร.ม. ของ a และ b อยู่ในรูปการรวมเชิงเส้นของ a และ b ได้ นั่นคือ

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

สำหรับบางจำนวนเต็ม x และ y

ตัวอย่าง 4.15 เนื่องจาก $(1024, 364) = 4$ และ $4 = 1024(16) + 364(-45)$
ได้ว่ามีจำนวนเต็ม x และ y ซึ่งทำให้ $(1024, 364) = 1024x + 364y$
ในที่นี้ได้ $x = 16$ และ $y = -45$ □

สามารถสรุปเป็นทฤษฎีบทได้ดังนี้

ทฤษฎีบท 4.6 ถ้า $d = (a, b)$ จะได้ว่ามีจำนวนเต็ม x และ y ซึ่งทำให้ $d = ax + by$

ข้อสังเกต

1. ถ้า $d = (a, b)$ โดยที่ a และ b มีค่ามาก แล้วในการหา (a, b) จะทำได้ยากขึ้น นอกจากนั้นการหาจำนวนเต็ม x, y ที่ทำให้ $(a, b) = ax + by$ โดยการแทนค่า สำหรับ a, b ที่มีค่ามาก ๆ ก็จะทำได้ยากเช่นกัน เราจะหา (a, b) และหาจำนวนเต็ม x, y ที่ทำให้ $(a, b) = ax + by$ โดยใช้ขั้นตอนวิธีของยุคลิด ซึ่งจะกล่าวถึงในภายหลัง
2. เนื่องจาก $30 = 10(6) + 5(-6)$ จะเห็นว่า $30 \neq (10, 5)$, $30 \neq (10, -6)$, $30 \neq (6, 5)$ และ $30 \neq (6, -6)$ นั่นคือสรุปไม่ได้ว่า ถ้า $m = ax + by$ แล้ว $m = (a, b)$ เราเพียงแต่สรุป ได้ว่า $(a, b) \mid m$

ในกรณีที่ $(a, b) = 1$ จากทฤษฎีบท 4.6 เราสามารถเขียน ห.ร.ม. ของ a และ b อยู่ในรูปการรวมเชิงเส้นของ a และ b ได้ นั่นคือ $1 = ax + by$ สำหรับบางจำนวนเต็ม x และ y

ในทางกลับกัน ถ้า $1 = ax + by$ สำหรับบางจำนวนเต็ม x และ y ต้องการแสดงว่า $(a, b) = 1$ ดังนี้ สมมติว่า $(a, b) = d$ จะได้ว่า $d \mid a$ และ $d \mid b$ โดยทฤษฎีบท 4.1 ข้อ (ii) และ (iv) ได้ $d \mid ax$ และ $d \mid by$ ดังนั้น $d \mid (ax + by)$ จะได้ $d \mid 1$ นั่นคือ $d = 1$ แสดงว่า $(a, b) = 1$ สรุปเป็นทฤษฎีบทได้ดังนี้

ทฤษฎีบท 4.7 ให้ a และ b เป็นจำนวนเต็มซึ่งเป็นศูนย์ไม่พร้อมกัน จะได้ว่า $(a, b) = 1$ ก็ต่อเมื่อ มีจำนวนเต็ม x และ y ซึ่งทำให้ $ax + by = 1$

ตัวอย่าง 4.16

(1) เนื่องจาก $(5, 12) = 1$ โดยทฤษฎีบท 4.6 ได้ว่ามีจำนวนเต็ม x และ y ซึ่งทำให้

$$1 = 5x + 12y$$

เนื่องจาก $1 = 5(5) + 12(-2)$ ในที่นี้ได้ $x = 5$ และ $y = -2$

(2) เนื่องจาก $1 = 28(12) + 5(-67)$ โดยทฤษฎีบท 4.7 ได้ว่า

$$(28, 5) = (28, -67) = (12, 5) = (12, -67) = 1$$ □

บทนิยาม 4.5 ให้ a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกัน จะกล่าวว่า a และ b เป็น **จำนวนเฉพาะสัมพัทธ์** ก็ต่อเมื่อ $(a, b) = 1$

ตัวอย่าง 4.17 เนื่องจาก $(5, 12) = 1$ ดังนั้นได้ 5 และ 12 เป็นจำนวนเฉพาะสัมพัทธ์ □

ในการแก้ปัญหาโดยใช้ทฤษฎีบทเศษเหลือของจีน เราจำเป็นต้องใช้จำนวนเต็มบวกมากกว่าสองจำนวนโดยไม่มีสองจำนวนใด ๆ ที่ตัวหารร่วมซึ่งเป็นบวกมีค่ามากกว่า 1 ดังบทนิยามต่อไปนี้

บทนิยาม 4.6 จะกล่าวว่าจำนวนเต็ม $a_1, a_2, \ldots, a_n$ เป็น **จำนวนเฉพาะสัมพัทธ์เป็นคู่** ก็ต่อเมื่อ $(a_i, a_j) = 1$ โดยที่ $1 \leq i < j \leq n$

ตัวอย่าง 4.18 จงพิจารณาว่า 15, 17, 28 เป็นจำนวนเฉพาะสัมพัทธ์เป็นคู่หรือไม่

วิธีทำ เนื่องจาก $(15, 17) = 1$, $(15, 28) = 1$ และ $(17, 28) = 1$
ดังนั้นได้ 15, 17, 28 เป็นจำนวนเฉพาะสัมพัทธ์เป็นคู่ □

ตัวอย่าง 4.19 จงพิจารณาว่า 15, 20, 31, 43 เป็นจำนวนเฉพาะสัมพัทธ์เป็นคู่หรือไม่

วิธีทำ เนื่องจาก $(15, 20) = 5 \neq 1$ ดังนั้นได้ 15, 20, 31, 43 ไม่เป็นจำนวนเฉพาะสัมพัทธ์เป็นคู่ □

ยังมีวิธีการหาตัวหารร่วมมากของจำนวนเต็มสองจำนวน โดยวิธีการใช้รูปแบบบัญญัติของสองจำนวนนั้น ดังนี้คือ ให้ a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์และเขียนอยู่ในรูป

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad \text{และ} \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

โดยที่ $p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < \ldots < p_n$ และ a_i, b_i เป็นจำนวนเต็มที่ไม่เป็นลบทุกค่า $i = 1, 2, \ldots, n$
ดังนั้นได้

$$(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

โดยที่ $\min(x, y)$ แทนจำนวนที่มีค่าน้อยระหว่าง x และ y

ตัวอย่าง 4.20 จงหา $(600, 2420)$

วิธีทำ เนื่องจาก $600 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 11^0$ และ $2420 = 2^2 \cdot 3^0 \cdot 5^1 \cdot 11^2$
ดังนั้นได้

$$\begin{aligned}(600, 2420) &= 2^{\max(3,\,2)} \cdot 3^{\max(1,\,0)} \cdot 5^{\max(2,\,1)} \cdot 11^{\max(0,\,2)} \\ &= 2^2 \cdot 3^0 \cdot 5^1 \cdot 11^0 = 20\end{aligned}$$

□

ต่อไปจะกล่าวถึงตัวคูณร่วมของจำนวนเต็มบวก a และ b ที่เป็นจำนวนเต็มบวกที่มีค่าน้อยที่สุด ซึ่งเรียกว่า ตัวคูณร่วมน้อย และความสัมพันธ์ระหว่างตัวคูณร่วมน้อยกับตัวหารร่วมมากของ a และ b ดังนี้

บทนิยาม 4.7 ให้ a, b และ c เป็นจำนวนเต็มบวก จะกล่าวว่า c เป็น **ตัวคูณร่วมน้อยของ a กับ b** ก็ต่อเมื่อ
1. $a \mid c$ และ $b \mid c$

และ

2. ถ้าจำนวนเต็มบวก d ซึ่ง $a \mid d$ และ $b \mid d$ แล้ว $c \mid d$

เขียนแทนตัวคูณร่วมน้อยที่เป็นบวกของ a และ b ด้วย $[a, b]$ และเรียกย่อ ๆ ว่า **ค.ร.น.** นั่นคือ ค.ร.น. หมายถึง ตัวคูณร่วมของทั้ง a และ b ที่เป็นบวกซึ่งมีค่าน้อยที่สุดนั่นเอง

ตัวอย่าง 4.21 จงหา $[15, 20]$

วิธีทำ ตัวคูณร่วมของ 15 และ 20 คือ 60, 120, 180, ... ดังนั้นได้ $[15, 20] = 60$ □

ในทำนองเดียวกันกับการหาตัวหารร่วมมาก วิธีการหาตัวคูณร่วมน้อยของจำนวนเต็มสองจำนวน โดยวิธีการใช้รูปแบบบัญญัติของสองจำนวนนั้น ทำได้ดังนี้คือ ให้ a และ b เป็นจำนวนเต็มบวกและเขียนอยู่ในรูป

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad \text{และ} \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

โดยที่ $p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < \ldots < p_n$ และ a_i, b_i เป็นจำนวนเต็มที่ไม่เป็นลบทุกค่า $i = 1, 2, \ldots, n$
ดังนั้นได้

$$[a, b] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

โดยที่ $\max(x, y)$ แทนจำนวนที่มีค่ามากระหว่าง x และ y

ตัวอย่าง 4.22 จงหา $[2^3 \cdot 3^5 \cdot 7^2,\ 2^4 \cdot 3^3 \cdot 5^3]$

วิธีทำ $[2^3 \cdot 3^5 \cdot 7^2,\ 2^4 \cdot 3^3 \cdot 5^3] = 2^{\max(3,\,4)} \cdot 3^{\max(5,\,3)} \cdot 5^{\max(0,\,3)} \cdot 7^{\max(2,\,0)} = 2^4 \cdot 3^5 \cdot 5^3 \cdot 7^2$ □

พิจารณา $(24, 36) = 12$ และ $[24, 36] = 72$ จะสังเกตว่า

$$24 \cdot 36 = 864 = 12 \cdot 72 = (24, 36) \cdot [24, 36]$$

ทฤษฎีบทต่อไป แสดงความสัมพันธ์ระหว่างตัวหารร่วมมากและตัวคูณร่วมน้อยของจำนวนเต็มสองจำนวน ดังนี้

ทฤษฎีบท 4.8 ให้ a และ b เป็นจำนวนเต็มบวก จะได้ว่า $ab = (a, b)\,[a, b]$

คอนกรูเอนซ์

คาร์ล ฟรีดริค เกาส์ (Carl Friedrich Gauss) นักคณิตศาสตร์ชาวเยอรมันได้พัฒนาเกี่ยวกับแนวความคิดเรื่องคอนกรูเอนซ์นี้ ได้สร้างทฤษฎีบทที่สำคัญ ๆ ทางทฤษฎีจำนวนขึ้นหลายทฤษฎี ซึ่งเป็นประโยชน์อย่างมากในการนำไปประยุกต์ใช้ ในหัวข้อนี้จะกล่าวถึงบทนิยาม ทฤษฎีบท และการนำความรู้เรื่องคอนกรูเอนซ์ไปประยุกต์ใช้ในสาขาวิทยาการคอมพิวเตอร์

เกาส์, คาร์ล ฟรีดริค
ค.ศ. 1777 – 1855, เยอรมนี

ถ้าให้ a เป็นจำนวนเต็มและ m เป็นจำนวนเต็มบวก เขียน $a \bmod m$ แทนเศษที่ได้จากการหาร a ด้วย m จากขั้นตอนวิธีการหาร a ด้วย m จะได้ว่ามีจำนวนเต็ม q และ r เพียงคู่เดียวซึ่ง

$$a = mq + r \qquad \text{โดยที่ } 0 \le r < m$$

นั่นคือ $a \bmod m = r$

ตัวอย่าง 4.23 $3 \textbf{ mod } 5 = 3$, $40 \textbf{ mod } 9 = 4$, $2004 \textbf{ mod } 101 = 85$

$-4 \textbf{ mod } 5 = 1$ เพราะ $-4 = 5(-1) + 1$

$-142 \textbf{ mod } 9 = 2$ เพราะ $-142 = 9(-16) + 2$ □

ถ้าเศษที่ได้จากการหารจำนวนเต็มสองจำนวนด้วยจำนวนเต็มบวก m มีค่าเท่ากัน จะแทนด้วยสัญลักษณ์ดังบทนิยามต่อไปนี้

บทนิยาม 4.8 ให้ a และ b เป็นจำนวนเต็มใด ๆ และ m เป็นจำนวนเต็มบวก จะกล่าวว่า a **คอนกรูเอนซ์กับ** b **มอดุโล** m ถ้า $m \mid (a-b)$ เขียนแทนด้วย $a \equiv b \pmod{m}$ และเรียก m **ว่าโมดุลัส** และ $a \not\equiv b \pmod{m}$ แทน a **ไม่คอนกรูเอนซ์กับ** b **มอดุโล** m

ตัวอย่าง 4.24 จากบทนิยาม 4.8 จะได้ว่า $326 \equiv 151 \pmod{5}$ แต่ $24 \not\equiv 14 \pmod{6}$

และยังได้ว่า $326 = 151 + 5(36)$ □

ข้อสังเกต ให้ m เป็นจำนวนเต็มบวก a, b และ c เป็นจำนวนเต็ม จะได้ว่า

1. $a \equiv b \pmod{m}$ ก็ต่อเมื่อ $a \textbf{ mod } m = b \textbf{ mod } m$
2. $a \equiv b \pmod{m}$ ก็ต่อเมื่อ มีบางจำนวนเต็ม k ซึ่งทำให้ $a = mk + b$

นอกจากนี้ยังมีสมบัติของคอนกรูเอนซ์ที่สำคัญดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.9 ให้ m เป็นจำนวนเต็มบวก และ a, b, c และ d เป็นจำนวนเต็ม จะได้ว่า

(*i*) $a \equiv a \pmod{m}$

(*ii*) ถ้า $a \equiv b \pmod{m}$ แล้ว $b \equiv a \pmod{m}$

(*iii*) ถ้า $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$ แล้ว $a \equiv c \pmod{m}$

(*iv*) ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ แล้ว

$a + c \equiv b + d \pmod{m}$ และ $ac \equiv bd \pmod{m}$

(*v*) ถ้า $a \equiv b \pmod{m}$ แล้ว $a^n \equiv b^n \pmod{m}$ ทุกจำนวนเต็มบวก n

(*vi*) ถ้า $ac \equiv bc \pmod{m}$ และ $(c, m) = d$ แล้ว $a \equiv b \pmod{\frac{m}{d}}$

ตัวอย่าง 4.25 จงหาเศษที่ได้จากการหาร $13^{401} + 5$ ด้วย 10

วิธีทำ เนื่องจาก $13 \equiv 3 \pmod{10}$ โดยทฤษฎีบท 4.9 ข้อ (v) ได้ $13^4 \equiv 3^4 \pmod{10}$

เพราะว่า $3^4 \equiv 1 \pmod{10}$ โดยทฤษฎีบท 4.9 ข้อ (iii) ได้ $13^4 \equiv 1 \pmod{10}$

โดยทฤษฎีบท 4.9 ข้อ (v) ได้ $(13^4)^{100} \equiv 1^{100} \pmod{10}$

ดังนั้นได้ $13^{400} \equiv 1 \pmod{10}$

โดยทฤษฎีบท 4.9 ข้อ (iv) ได้ $13^{400} \cdot 13 \equiv 1 \cdot 13 \equiv 3 \pmod{10}$

แสดงว่า $13^{401} \equiv 3 \pmod{10}$

เนื่องจาก $5 \equiv 5 \pmod{10}$ โดยทฤษฎีบท 4.9 ข้อ (iv) ได้ $13^{401} + 5 \equiv 3 + 5 \equiv 8 \pmod{10}$

นั่นคือ $13^{401} + 5$ หารด้วย 10 เหลือเศษ 8 □

ตัวอย่าง 3.26 จงหา 2^{644} **mod** 645

วิธีทำ ต้องการหา a ซึ่ง $2^{644} \equiv a \pmod{645}$ โดยใช้ทฤษฎีบท 4.9 ดังนี้

เนื่องจาก $2^4 \equiv 16 \pmod{645}$ โดยทฤษฎีบท 4.9 ข้อ (v) ได้ $(2^4)^2 \equiv (16)^2 \equiv 256 \pmod{645}$

จะได้ $2^8 \equiv 256 \pmod{645}$ โดยทฤษฎีบท 4.9 ข้อ (v) ได้ $(2^8)^2 \equiv (256)^2 \pmod{645}$

เพราะว่า $(256)^2 = 65536 \equiv 391 \pmod{645}$

โดยทฤษฎีบท 4.9 ข้อ (iii) ได้ $2^{16} \equiv 391 \pmod{645}$

ในทำนองเดียวกันได้ $(2^{16})^2 = (391)^2 = 152881 \equiv 16 \pmod{645}$

ดังนั้นได้ $(2^{32})^2 \equiv (16)^2 \equiv 256 \pmod{645}$ เพราะฉะนั้น $(2^{64})^2 \equiv (256)^2 \equiv 391 \pmod{645}$

แสดงว่า $(2^{128})^2 \equiv (391)^2 \equiv 16 \pmod{645}$ ดังนั้น $(2^{256})^2 \equiv (16)^2 \equiv 256 \pmod{645}$

จะได้ว่า $2^{512} \equiv 256 \pmod{645}$

ดังนั้นได้ $2^{512} \cdot 2^{128} \equiv 256 \cdot 391 \pmod{645}$ เพราะฉะนั้น $2^{640} \equiv 100096 \equiv 121 \pmod{645}$

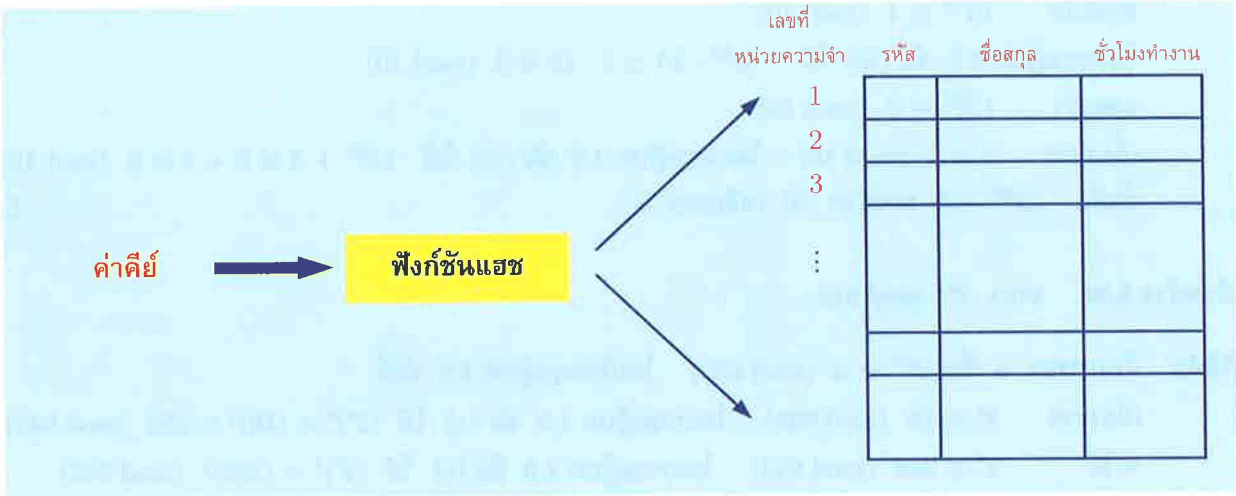
จะได้ว่า $2^{640} \cdot 2^4 \equiv 121 \cdot 2^4 \equiv 1936 \equiv 1 \pmod{645}$

นั่นคือ 2^{644} **mod** $645 = 1$ □

การประยุกต์ของคอนกรูเอนซ์

คอนกรูเอนซ์ได้ถูกนำไปประยุกต์ใช้กับงานในหลาย ๆ ด้าน แต่ในที่นี้จะกล่าวถึงการประยุกต์ใช้กับงานทางคอมพิวเตอร์ใน 3 เรื่อง คือ การเข้าถึงข้อมูลด้วยเทคนิคแฮชชิง การสร้างตัวเลขสุ่มแบบเทียม และการเข้ารหัสด้วยตัวเลขแบบมอดุโล

การเข้าถึงข้อมูลด้วยเทคนิคแฮชชิงเป็นกระบวนการเข้าถึงข้อมูลในแบบตรง โดยนำค่าคีย์ของรายการข้อมูลที่ต้องการ ผ่านเข้าไปในฟังก์ชันแฮช ซึ่งจะสร้างตัวเลขระบุตำแหน่งเลขที่หน่วยความจำที่สัมพันธ์กับรายการข้อมูลที่ต้องการภายในตารางแฮช ดังนั้นการทำแฮชชิงจึงประกอบด้วยสามส่วน คือ ส่วนการกำหนดค่าคีย์ที่นำมาใช้ ส่วนฟังก์ชันแฮช และส่วนตารางที่เก็บข้อมูล หรือเรียกอีกอย่างหนึ่งว่าตารางแฮช มีความสัมพันธ์ร่วมกันดังนี้



หากจะกล่าวถึงการประยุกต์ร่วมกันระหว่างคอนกรูเอนซ์กับกระบวนการเข้าถึงข้อมูลทางคอมพิวเตอร์ ก็จะพบได้จากการทำแฮชชิงที่ใช้เทคนิควิธีเศษที่เหลือจากการหาร

ถ้าให้ k แทน คีย์ จะได้ $h(k)$ แทนเลขที่หน่วยความจำ และ m เป็นขนาดของตารางแฮช ในทางปฏิบัติเราจะจัดเก็บโดยใช้ฟังก์ชันแฮชได้หลายรูปแบบ และฟังก์ชันแฮช h ฟังก์ชันหนึ่งที่นิยมใช้คือ

$$h(k) = k \ \mathbf{mod}\ m$$

ในการหาเลขที่หน่วยความจำที่ใช้เก็บข้อมูลกับปัญหาการกำหนดขนาดของตารางแฮชที่ใช้เก็บข้อมูล จำเป็นต้องมีสมบัติเป็นเลขจำนวนเฉพาะที่มีขนาดไม่น้อยกว่า 1.25 เท่าของจำนวนข้อมูลที่คาดว่าจะเกิดขึ้นทั้งหมดทั้งนี้เพื่อหลีกเลี่ยงปัญหาการใช้เลขที่หน่วยความจำเดียวกันของคีย์ที่ต่างกันหรือเรียกอีกอย่างหนึ่งว่าเกิดการชนกันหรือเกิดคอลลิชัน

ตัวอย่าง 4.27 สมมติว่าระบบประมวลผลของบริษัทแห่งหนึ่ง ต้องการเก็บข้อมูลรายการทำงานล่วงเวลาของพนักงานจำนวนไม่เกิน 100 คน โดยออกแบบการเข้าถึงรายการข้อมูลการทำงานล่วงเวลาของพนักงานด้วยวิธีการทำแฮชชิงในแบบดิวิชัน รีเมนเดอร์ ซึ่งใช้รหัสพนักงานที่ประกอบด้วยตัวเลขจำนวนเต็ม 5 หลัก เป็นคีย์สำหรับการเข้าถึงข้อมูล ปัญหาแรกที่พบก็คือ ผู้ออกแบบระบบควรต้องหาคำตอบว่าขนาดของตารางแฮชควรมีขนาดเท่าใดจึงจะเหมาะสม ซึ่งก็ไม่ใช่เรื่องยากที่จะหาคำตอบในเมื่อทราบว่าขนาดของตารางแฮชที่เหมาะสมควรมีค่าเป็นจำนวนเฉพาะที่มีขนาดไม่น้อยกว่า 1.25 เท่าของจำนวนข้อมูล 100 รายการ นั่นก็คือขนาดของตารางควรมีค่าเป็น 127 ซึ่งเป็นจำนวนเฉพาะ และถ้าพนักงานมีรหัสประจำตัว "40123" ถ้าต้องการบันทึกข้อมูล เขาควรบันทึกข้อมูลลงที่ตำแหน่งใดในตารางแฮช คำตอบนี้สามารถหาได้จากการแทน k ด้วย 40123 แล้วคำนวณหา $h(k)$ ได้ดังนี้

$$h(40123) = 40123 \ \mathbf{mod}\ 127 = 118$$

นั่นคือ ข้อมูลของพนักงานที่มีรหัสประจำตัว 40123 จะถูกจัดเก็บในเลขที่หน่วยความจำตำแหน่งที่ 118 นั่นเอง ในทำนองเดียวกัน

$$h(66893) = 66893 \ \mathbf{mod}\ 127 = 91$$

$$h(50918) = 50918 \ \mathbf{mod}\ 127 = 118$$

นั่นคือข้อมูลของพนักงานที่มีรหัสประจำตัว "66893" และ "50918" จะถูกจัดเก็บในเลขที่หน่วย

ความจำตำแหน่งที่ 91 และ 118 ตามลำดับ

จะสังเกตเห็นว่าข้อมูลของพนักงานสองคนที่มีรหัส "40123" และ "50918" ได้จัดเก็บในที่เดียวกัน นั่นคือเกิดคอลลิชันขึ้น ทั้งนี้เพราะว่าฟังก์ชันแฮชไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง ซึ่งในทางคอมพิวเตอร์ก็จะมีวิธีแก้ดังจะได้ศึกษาต่อไป □

ตัวอย่าง 4.28 ในการสร้างตัวเลขสุ่มโดยทั่วไปมักจะใช้เทคนิควิธีแบบจำลองทางคอมพิวเตอร์ ซึ่งมีหลายวิธีการและวิธีหนึ่งที่จะกล่าวถึง ก็คือการใช้คอนกรูเอนซ์ ซึ่งมีรายละเอียดดังต่อไปนี้

เราจะเลือกจำนวนเต็มมา 4 จำนวน คือ m, a, c และ x_0 โดยที่ m เป็นโมดุลัส, a เป็นตัวคูณ, c เป็นค่าที่เพิ่มขึ้น และ x_0 เป็นค่าเริ่มต้น เมื่อ $2 \leq a < m$, $2 \leq c < m$ และ $2 \leq x_0 < m$ แล้วสร้างลำดับ $\{x_n\}$ จากสมการ

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

ซึ่งจะได้ $\{x_n\}$ เป็นลำดับของจำนวนเต็มที่ไม่เป็นลบ โดยที่ $0 \leq x_n < m$ ทุก n

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

$$\begin{aligned}
x_1 &= (7x_0 + 4) \textbf{ mod } 9 = (7 \cdot 3 + 4) \textbf{ mod } 9 = 25 \textbf{ mod } 9 = 7 \\
x_2 &= (7x_1 + 4) \textbf{ mod } 9 = (7 \cdot 7 + 4) \textbf{ mod } 9 = 53 \textbf{ mod } 9 = 8 \\
x_3 &= (7x_2 + 4) \textbf{ mod } 9 = (7 \cdot 8 + 4) \textbf{ mod } 9 = 60 \textbf{ mod } 9 = 6 \\
x_4 &= (7x_3 + 4) \textbf{ mod } 9 = (7 \cdot 6 + 4) \textbf{ mod } 9 = 46 \textbf{ mod } 9 = 1 \\
x_5 &= (7x_4 + 4) \textbf{ mod } 9 = (7 \cdot 1 + 4) \textbf{ mod } 9 = 11 \textbf{ mod } 9 = 2 \\
x_6 &= (7x_5 + 4) \textbf{ mod } 9 = (7 \cdot 2 + 4) \textbf{ mod } 9 = 18 \textbf{ mod } 9 = 0 \\
x_7 &= (7x_6 + 4) \textbf{ mod } 9 = (7 \cdot 0 + 4) \textbf{ mod } 9 = 4 \textbf{ mod } 9 = 4 \\
x_8 &= (7x_7 + 4) \textbf{ mod } 9 = (7 \cdot 4 + 4) \textbf{ mod } 9 = 32 \textbf{ mod } 9 = 5 \\
x_9 &= (7x_8 + 4) \textbf{ mod } 9 = (7 \cdot 5 + 4) \textbf{ mod } 9 = 39 \textbf{ mod } 9 = 3 \\
&\vdots
\end{aligned}$$

เนื่องจาก $x_9 = x_0$ และพจน์หลังขึ้นอยู่กับพจน์ที่มาก่อนเพียงพจน์เดียว ดังนั้น เราจะได้ลำดับ

$$\mathbf{3, 7, 8, 6, 1, 2, 0, 4, 5}, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \ldots$$

ซึ่งลำดับที่ได้นี้มี 9 พจน์ที่ต่างกัน และจะซ้ำเดิมทุก ๆ 9 พจน์ เราเรียกตัวเลข 3, 7, 8, 6, 1, 2, 0, 4, 5 ว่า**ตัวก่อกำเนิด** □

การเข้ารหัสและการถอดรหัส

การเข้ารหัสเป็นกระบวนการหนึ่งในการรักษาความปลอดภัยของข้อมูล และวิธีการหนึ่งที่เก่าแก่และเป็นที่รู้จักกันดีก็คือ **การเข้ารหัสแบบซีซาร์** ที่คิดค้นโดยจูเลียสซีซาร์ เขาใช้วิธีการเลื่อนตัวอักษรแต่ละตัวถัดไปอีก 3 ตำแหน่ง

เช่นอักษร A เมื่อเข้ารหัสแล้วก็จะถูกเลื่อนไปเป็นอักษร D และตัวอักษร 3 ตัวสุดท้าย คือ X, Y และ Z จะเลื่อนไปเป็นตัวอักษร A, B และ C ตามลำดับ

วิธีการเข้ารหัสแบบซีซาร์จะกำหนดตัวเลขแทนตัวอักษร โดยให้ $A = 0,\ B = 1,\ \ldots,\ Z = 25$ เราจะเข้ารหัสโดยนิยามฟังก์ชัน f เป็นฟังก์ชันจากเซต $\{0, 1, 2, \ldots, 25\}$ ไปยังเซต $\{0, 1, 2, \ldots, 25\}$ นิยามโดย

$$f(p) = (p + 3) \textbf{ mod } 26$$

ตัวอย่าง 4.29 จงเข้ารหัสข้อความ "YESTERDAY" โดยรหัสแบบซีซาร์

วิธีทำ แทนตัวอักษรที่กำหนดด้วยตัวเลขได้ดังนี้

24 4 18 19 4 17 3 0 24

แล้วเข้ารหัสแบบซีซาร์ โดยแทนแต่ละจำนวน p ในฟังก์ชัน $f(p) = (p + 3) \textbf{ mod } 26$

ดังนั้นได้ 1 7 21 22 7 20 6 3 1

เมื่อแทนกลับเป็นตัวอักษร จะได้ข้อความที่เข้ารหัสแล้ว คือ "BHVWHUGDB" □

ข้อสังเกต ถ้าเข้ารหัสด้วยรหัสแบบซีซาร์ โดยใช้ฟังก์ชัน $f(p) = (p + 3) \textbf{ mod } 26$ แล้วเราสามารถถอดรหัสด้วยฟังก์ชัน $f^{-1}(p) = (p - 3) \textbf{ mod } 26$

นั่นคือ เราจะเลื่อนตัวอักษรกลับมา 3 ตำแหน่ง ดังตัวอย่าง

ตัวอย่าง 4.30 จงถอดรหัสข้อความ "WHQ" ที่ถูกส่งมาโดยใช้รหัสแบบซีซาร์

วิธีทำ แทนตัวอักษรที่กำหนดด้วยตัวเลขได้ดังนี้ คือ 22 7 16

แล้วถอดรหัสแบบซีซาร์ โดยแทนแต่ละจำนวน p ในฟังก์ชัน $f^{-1}(p) = (p - 3) \textbf{ mod } 26$

ดังนั้นได้ 19 4 13

เมื่อแทนกลับด้วยตัวอักษร จะได้ข้อความที่ถอดรหัสแล้ว คือ "TEN" □

จากสองตัวอย่างข้างต้นจะเห็นว่า การเข้ารหัสแบบซีซาร์นี้มีความปลอดภัยของข้อมูลน้อย ซึ่งในปัจจุบันนี้มีการพัฒนาการเข้ารหัสในแบบอื่นอีก เช่น การเข้ารหัสแบบ RSA หรือการเข้ารหัสแบบเชิงเส้นที่อยู่ในรูป

$$f(p) = (ap + b) \textbf{ mod } 26$$

โดยที่ a, b เป็นจำนวนเต็ม และ f เป็นฟังก์ชันสมนัยหนึ่งต่อหนึ่ง ดังตัวอย่าง

ตัวอย่าง 4.31 ให้ $A = 0,\ B = 1,\ \ldots,\ Z = 25$ และ $f(p) = (7p + 3) \textbf{ mod } 26$ จงเข้ารหัสข้อความ "LOVE" โดยใช้ฟังก์ชัน f

วิธีทำ แทนตัวอักษรที่กำหนดด้วยตัวเลขได้ คือ 11 14 21 4

เราเข้ารหัส โดยแทนจำนวนแต่ละจำนวน p ในฟังก์ชัน $f(p) = (7p + 3) \textbf{ mod } 26$

ดังนั้นได้

$$7(11) + 3 = 80 \textbf{ mod } 26 = 2$$

$$7(14) + 3 = 101 \ \mathbf{mod}\ 26 = 23$$
$$7(21) + 3 = 150 \ \mathbf{mod}\ 26 = 20$$
$$7(4) + 3 = 31 \ \mathbf{mod}\ 26 = 5$$

แปลงเป็นตัวอักษรจะได้ข้อความที่เข้ารหัสแล้ว คือ "CXUF" □

ยุคลิดแห่งอะเล็กซานเดรีย
ประมาณ 450 – 380 ปีก่อนคริสต์ศักราช, กรีซ

จำนวนเต็มและขั้นตอนวิธีของยุคลิด

ในหัวข้อที่ผ่านมานั้นได้ศึกษาขั้นตอนวิธีในการหาตัวประกอบที่เป็นจำนวนเฉพาะของจำนวนเต็ม ยังมีขั้นตอนวิธีหนึ่งที่สำคัญและเป็นขั้นตอนวิธีที่เก่าแก่ที่สุดในทางคณิตศาสตร์ ซึ่งคือ ขั้นตอนวิธีของยุคลิด เป็นขั้นตอนที่เราสามารถนำมาใช้หาตัวหารร่วมมากของจำนวนเต็มบวกสองจำนวน ใช้ในการเปลี่ยนจากเลขในฐานหนึ่งไปเป็นอีกฐานหนึ่ง หรือใช้ในการแก้ปัญหาที่ใช้ทฤษฎีบทเศษเหลือของจีน

ขั้นตอนวิธีของยุคลิด

ก่อนอื่นพิจารณาขั้นตอนดังต่อไปนี้

$$287 = 91(3) + 14$$
$$91 = 14(6) + 7$$
$$14 = 7(2)$$

จะได้ว่า $(14, 7) = 7, \quad (91, 7) = 7$ และ $(287, 91) = 7$

ทฤษฎีบท 4.10 ให้ a, b, q และ r เป็นจำนวนเต็มซึ่ง $b > 0$ และ

$$a = bq + r \quad \text{โดยที่ } 0 \le r < b$$

จะได้ว่า $(a, b) = (b, r)$

ทฤษฎีบท 4.11 *ขั้นตอนวิธีของยุคลิด*

ให้ a, b เป็นจำนวนเต็มบวก และ $q_1, q_2, \ldots, q_{n+1}, r_1, r_2, \ldots, r_n$ เป็นจำนวนเต็ม โดยที่

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b \\
b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

แล้วจะได้ว่า $(a, b) = r_n$

เราสามารถนำขั้นตอนวิธีของยุคลิดไปหา (a, b) และยังหาจำนวนเต็ม x และ y ที่ทำให้ $(a, b) = ax + by$ ได้ดังนี้

ตัวอย่าง 4.32 จงหา $(527, 3553)$ และหาจำนวนเต็ม x และ y ที่ทำให้ $(527, 3553) = 527x + 3553y$ โดยใช้ขั้นตอนวิธีของยุคลิด

วิธีทำ เนื่องจาก

$$\begin{aligned}
3553 &= 527(6) + 391 \\
527 &= 391(1) + 136 \\
391 &= 136(2) + 119 \\
136 &= 119(1) + 17 \\
119 &= 17(7)
\end{aligned}$$

ดังนั้นได้ $(527, 3553) = 17$

ต่อไปจะหาจำนวนเต็ม x และ y ที่ทำให้ $(a, b) = ax + by$ โดยการทำย้อนกลับ ดังนี้

$$\begin{aligned}
17 &= 136 - 119(1) \\
&= 136 - (391 - 136(2)) \\
&= 136(3) - 391 \\
&= (527 - 391)(3) - 391 \\
&= 527(3) - 391(4) \\
&= 527(3) - (3553 - 527(6))(4) \\
&= 527(27) + 3553(-4)
\end{aligned}$$

จะได้ว่า $x = 27$ และ $y = -4$ □

The input of a computer must be translated into a sequence of zeros and ones, and the output must be translated back again.

จำนวนที่เราใช้กันอยู่เป็นประจำจะเป็นจำนวนในระบบเลขฐาน 10 เช่น ใช้จำนวน 638 แทนจำนวน $6 \cdot 10^2 + 3 \cdot 10 + 8$ อย่างไรก็ตามในทางคอมพิวเตอร์เรายังใช้จำนวนที่อยู่ในเลขฐานอื่นอีก นอกจากเลขฐาน 10 เช่น เลขฐาน 2 หรือฐาน 8 หรือฐาน 16 โดยมีการใช้ในสองลักษณะ คือ ใช้ในระบบการคำนวณ และใช้สำหรับแทนตัวอักษรเพื่อทำให้เราเข้าใจ เช่น อักษร “A” จะถูกแทนด้วย 65 ในระบบเลขฐานสิบ หรือ $(01000001)_2$ ในระบบเลขฐานสอง ตามการแทนรหัสตัวอักษรของระบบแอสกี (ASCII) เป็นต้น ตัวอย่างและทฤษฎีบทที่จะกล่าวต่อไปจะทำให้เราสามารถเปลี่ยนจำนวนเต็มบวกที่อยู่ในเลขฐานหนึ่งไปเป็นอีกฐานหนึ่งได้ โดยจำนวนที่จะเป็นตัวฐานจะต้องเป็นจำนวนเต็มบวกที่มากกว่า 1 ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.12 ให้ b เป็นจำนวนเต็มบวกที่มากกว่า 1 จะได้ว่า ทุกจำนวนเต็มบวก a จะเขียนอยู่ในรูป

$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_2 b^2 + a_1 b + a_0 \qquad \ldots\ldots\ldots\ldots\ldots\ldots(*)$$

ได้เพียงแบบเดียวเท่านั้น

โดยที่ n เป็นจำนวนเต็มที่ไม่เป็นลบ และ a_i เป็นจำนวนเต็มซึ่ง $0 \leq a_i < b$ ทุกค่า $i = 0, 1, 2, \ldots, n$ เราเรียก $(*)$ ว่า **การเขียนจำนวนเต็ม a ในเลขฐาน b**

หมายเหตุ กรณีที่ $b = 10$ จะได้ว่า

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1(10) + a_0$$

โดยที่ $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ซึ่งจะเขียนแทน a ด้วย $a_n a_{n-1} \ldots a_2 a_1 a_0$ และเรียก a_i ว่า **เลขหลักของ a** ซึ่ง a_0 คือเลขหลักหน่วย, a_1 คือเลขหลักสิบ และ a_2 คือเลขหลักร้อย เป็นต้น เช่น

จำนวน 8963 เขียนได้ในรูป $8 \cdot 10^3 + 9 \cdot 10^2 + 6 \cdot 10 + 3$ ในกรณีนี้จะกล่าวว่า **เขียน a ในเลขฐานสิบ**

กรณีที่ $b = 2$ ก็จะเขียน a ได้ในทำนองเดียวกัน คือ

$$a = a_n 2^n + a_{n-1} 2^{n-1} + \cdots + a_2 2^2 + a_1(2) + a_0$$

โดยที่มีเลขหลัก a_i เพียงสองตัว คือ 0 หรือ 1 และเขียนแทน a ด้วย $(a_n a_{n-1} \ldots a_2 a_1 a_0)_2$

ในระบบคอมพิวเตอร์ จะใช้วิธีการแทนตัวเลขในระบบเลขฐานสองเป็นพื้นฐานในการคำนวณ และเพื่อให้ความสะดวกในการเขียนจำนวนที่มีค่ามาก ๆ ในรูปเลขฐานสองให้ง่ายขึ้นนั้น จึงนิยมเขียนแทนตัวเลขในระบบเลขฐานที่ใหญ่กว่า เช่น ระบบเลขฐานแปด หรือฐานสิบหก และจากความจริงที่พบว่าค่าของตัวเลขขึ้นอยู่กับหลักที่ตัวเลขนั้นถูกนำไปวาง เช่น $(368)_{10}$ ตัวเลข 3 จะมีค่าเป็น $3 \cdot 10^2$, ตัวเลข 6 จะมีค่าเป็น $6 \cdot 10^1$ และตัวเลข 8 มีค่าเป็น $8 \cdot 10^0$ ในระบบเลขฐานสองก็พิจารณาในทำนองเดียวกัน เช่น $(101)_2$ ตัวเลข 1 จะมีค่าเป็น $1 \cdot 2^2$, ตัวเลข 0 จะมีค่าเป็น $0 \cdot 2^1$ และตัวเลข 1 มีค่าเป็น $1 \cdot 2^0$ โดยเราสามารถนำทฤษฎีบท 4.12 มาใช้ในการเปลี่ยนจำนวนในที่อยู่ในระบบเลขฐานหนึ่งไปสู่จำนวนในระบบเลขอีกฐานหนึ่ง

ตัวอย่าง 4.33 จงเปลี่ยน $(101011011)_2$ เป็นเลขฐานสิบ

วิธีทำ จากโจทย์สามารถกระจายได้เป็น

$$\begin{aligned}(101011111)_2 &= 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 \\ &= 347\end{aligned}$$

□

ตัวอย่าง 4.34 จงเปลี่ยน 123 เป็นเลขฐานสอง

วิธีทำ เนื่องจาก

$$\begin{aligned}123 &= 2 \cdot 61 + 1 \\ 61 &= 2 \cdot 30 + 1 \\ 30 &= 2 \cdot 15 + 0 \\ 15 &= 2 \cdot 7 + 1 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1\end{aligned}$$

ดังนั้น 123 เขียนเป็นเลขฐานสอง คือ $(1111011)_2$ □

สำหรับกรณีทั่วไป เราจะได้ว่า

$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

ถ้า $b \leq 10$ เราใช้เลขหลัก $a_i = 0, 1, 2, \ldots, b-1$

เช่น $b = 8$ เราใช้ $0, 1, 2, 3, 4, 5, 6, 7$ เป็นเลขหลัก

ถ้า $b > 10$ เราใช้เลขหลัก $a_i = 0, 1, 2, \ldots, 9$ และตัวอักษรแทนเลขหลักที่เป็น $10, 11, \ldots, b-1$

สำหรับเลขในฐานสิบหกที่ใช้ในระบบคอมพิวเตอร์ จะต่างจากเลขในฐานสอง เนื่องจากเลขหลักที่ใช้จะเป็นตัวเลขและตัวอักษรร่วมกัน ดังนี้คือ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E และ F โดยที่ ตัวอักษร A ถึง F จะแทนเลขหลัก 10 ถึง 15 ในฐาน 16 ดังตัวอย่าง

ตัวอย่าง 4.35 จงเปลี่ยน $(2AE0F)_{16}$ เป็นเลขฐานสิบ

วิธีทำ จากโจทย์สามารถกระจายได้เป็น

$$\begin{aligned}(2AE0F)_{16} &= 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 15 \cdot 16^0 \\ &= 175631\end{aligned}$$

□

ตัวอย่าง 4.36 จงเปลี่ยน 12344 เป็นเลขฐานแปด

วิธีทำ เนื่องจาก

$$\begin{aligned}12344 &= 8 \cdot 1543 + 0 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3\end{aligned}$$

ดังนั้น 12344 เขียนเป็นเลขฐานแปด คือ $(30070)_8$ □

ตัวอย่าง 4.37 จงเปลี่ยน 177132 เป็นเลขฐานสิบหก

วิธีทำ เนื่องจาก

$$\begin{aligned}177132 &= 16 \cdot 11070 + 12 \\ 11070 &= 16 \cdot 691 + 14 \\ 691 &= 16 \cdot 43 + 3 \\ 43 &= 16 \cdot 2 + 11 \\ 2 &= 16 \cdot 0 + 2\end{aligned}$$

ดังนั้น 177132 เขียนเป็นเลขฐานสิบหก คือ $(2B3EC)_{16}$ □

ตารางเปรียบเทียบจำนวนในเลขฐานต่าง ๆ

ฐานสิบ	ฐานสอง	ฐานแปด	ฐานสิบหก
0	0	0	0
1	$(1)_2$	$(1)_8$	$(1)_{16}$
2	$(10)_2$	$(2)_8$	$(2)_{16}$
3	$(11)_2$	$(3)_8$	$(3)_{16}$
4	$(100)_2$	$(4)_8$	$(4)_{16}$
5	$(101)_2$	$(5)_8$	$(5)_{16}$
6	$(110)_2$	$(6)_8$	$(6)_{16}$
7	$(111)_2$	$(7)_8$	$(7)_{16}$
8	$(1000)_2$	$(10)_8$	$(8)_{16}$
9	$(1001)_2$	$(11)_8$	$(9)_{16}$
10	$(1010)_2$	$(12)_8$	$(A)_{16}$
11	$(1011)_2$	$(13)_8$	$(B)_{16}$
12	$(1100)_2$	$(14)_8$	$(C)_{16}$
13	$(1101)_2$	$(15)_8$	$(D)_{16}$
14	$(1110)_2$	$(16)_8$	$(E)_{16}$
15	$(1111)_2$	$(17)_8$	$(F)_{16}$
16	$(10000)_2$	$(20)_8$	$(10)_{16}$

การประยุกต์ของทฤษฎีจำนวน

ความรู้ทางทฤษฎีจำนวนมีการประยุกต์ใช้ได้มากมาย โดยเฉพาะในสาขาวิทยาการคอมพิวเตอร์ ดังได้กล่าวแล้ว ในหัวข้อนี้จะกล่าวถึงการประยุกต์ในสองแนวทาง คือ วิธีการคำนวณตัวเลขที่มีค่ามาก ๆ และการเข้ารหัสแบบ RSA ก่อนที่เราจะกล่าวถึงการประยุกต์เหล่านี้ จะขอกล่าวถึงความรู้ที่จะนำไปใช้ในเรื่องการแก้ระบบคอนกรูเอนซ์ที่มีมอดุโลเป็นจำนวนเฉพาะสัมพัทธ์เป็นคู่โดยใช้ทฤษฎีบทเศษเหลือของจีน ดังต่อไปนี้

คอนกรูเอนซ์เชิงเส้น

คอนกรูเอนซ์ที่อยู่ในรูป

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

โดยที่ m เป็นจำนวนเต็มบวก a, b เป็นจำนวนเต็มและ x เป็นตัวแปร จะเรียกคอนกรูเอนซ์นี้ว่า **คอนกรูเอนซ์เชิงเส้น** และเรียกจำนวนเต็ม x_0 ที่สอดคล้องกับ $ax \equiv b \pmod{m}$ ว่า **ผลเฉลย** ของคอนกรูเอนซ์เชิงเส้นนี้

การหาผลเฉลยของคอนกรูเอนซ์เชิงเส้น $ax \equiv b \pmod{m}$ ทำได้หลายวิธี วิธีหนึ่งคือ การแทนค่า x ด้วย $0, 1, 2, 3, \ldots, m-1$ ถ้า m เป็นจำนวนเต็มบวกที่มีค่าไม่มาก

ตัวอย่าง 4.38 จงหาผลเฉลยของคอนกรูเอนซ์เชิงเส้น $5x \equiv 2 \pmod{6}$

วิธีทำ แทนค่า x ด้วย $0, 1, 2, 3, 4$ และ 5

จะได้ว่า $5 \cdot 0 \not\equiv 2 \pmod{6}$, $5 \cdot 1 \not\equiv 2 \pmod{6}$, $5 \cdot 2 \not\equiv 2 \pmod{6}$,

$5 \cdot 3 \not\equiv 2 \pmod{6}$, $5 \cdot 4 \equiv 2 \pmod{6}$, $5 \cdot 5 \not\equiv 2 \pmod{6}$

ดังนั้นได้ ผลเฉลยของคอนกรูเอนซ์นี้ คือ $x \equiv 4 \pmod{6}$

ซึ่งหมายถึง จำนวนเต็ม $x \in \{\ldots, -14, -8, -2, 4, 10, 16, 22, 28, \ldots\}$

ทุกจำนวนก็จะเป็นผลเฉลยของคอนกรูเอนซ์เชิงเส้นที่กำหนดด้วย □

ข้อสังเกต ถ้า x_0 เป็นผลเฉลยของคอนกรูเอนซ์เชิงเส้น $ax \equiv b \pmod{m}$ แล้ว $x_1 = x_0 + km$ โดยที่ k เป็นจำนวนเต็ม จะเป็นผลเฉลยของคอนกรูเอนซ์เชิงเส้นนี้ด้วย

ตัวอย่าง 4.39 จงหาผลเฉลยของคอนกรูเอนซ์เชิงเส้น $2x \equiv 3 \pmod{4}$

วิธีทำ แทนค่า x ด้วย $0, 1, 2$ และ 3

จะได้ว่า $2 \cdot 0 \not\equiv 3 \pmod{4}$, $2 \cdot 1 \not\equiv 3 \pmod{4}$,

$2 \cdot 2 \not\equiv 3 \pmod{4}$ และ $2 \cdot 3 \not\equiv 3 \pmod{4}$

ดังนั้นได้ คอนกรูเอนซ์นี้ไม่มีผลเฉลย □

ตัวอย่าง 4.40 จงหาผลเฉลยของคอนกรูเอนซ์เชิงเส้น $2x \equiv 6 \pmod{8}$

วิธีทำ แทนค่า x ด้วย $0, 1, 2, 3, 4, 5, 6$ และ 7

จะได้ว่า $2 \cdot 3 \equiv 6 \pmod{8}$ และ $2 \cdot 7 \equiv 6 \pmod{8}$

แสดงว่า $x \equiv 3 \pmod{8}$ และ $x \equiv 7 \pmod{8}$ เป็นสองผลเฉลยที่ไม่คอนกรูเอนซ์กันของคอนกรูเอนซ์เชิงเส้นที่กำหนด □

จากทั้งสามตัวอย่างข้างต้นจะเห็นว่า คอนกรูเอนซ์เชิงเส้นที่กำหนดอาจจะมีหรือไม่มีผลเฉลยก็ได้ ในกรณีที่ m เป็นจำนวนเต็มบวกที่มีค่ามาก ๆ วิธีแทนค่าก็จะไม่สะดวก แต่ยังมีอีกวิธีหนึ่ง คือ โดยการใช้จำนวนเต็ม $\overline{a}$ ซึ่งทำให้ $a\overline{a} \equiv 1 \pmod{m}$ ถ้าจำนวนเต็ม $\overline{a}$ หาค่าได้ เราจะเรียกจำนวนเต็ม $\overline{a}$ นี้ว่า **ผกผันของ a มอดุโล m**

ตัวอย่าง 4.41 จงหาผกผันของ 7 และ 2 ในมอดุโล 4

วิธีทำ ต้องการหา $\overline{a}$ ซึ่งทำให้ $7\overline{a} \equiv 1 \pmod{4}$

โดยการแทนค่า $\overline{a}$ ด้วย $0, 1, 2$ และ 3 ได้

$$7 \cdot 0 \not\equiv 1 \pmod 4, \qquad 7 \cdot 1 \not\equiv 1 \pmod 4,$$
$$7 \cdot 2 \not\equiv 1 \pmod 4 \quad \text{และ} \quad 7 \cdot 3 \equiv 1 \pmod 4$$

นั่นคือ 3 เป็นผกผันของ 7 ในมอดุโล 4

ในทำนองเดียวกัน ต้องการหา $\overline{a}$ ซึ่งทำให้ $2\overline{a} \equiv 1 \pmod 4$

โดยการแทนค่า $\overline{a}$ ด้วย $0, 1, 2$ และ 3 ได้

$$2 \cdot 0 \not\equiv 1 \pmod 4, \qquad 2 \cdot 1 \not\equiv 1 \pmod 4,$$
$$2 \cdot 2 \not\equiv 1 \pmod 4 \quad \text{และ} \quad 2 \cdot 3 \not\equiv 1 \pmod 4$$

แสดงว่า ไม่มีผกผันของ 2 ในมอดุโล 4 □

สำหรับกรณีที่ a และ m มีค่ามาก การหาผกผันโดยการแทนค่านั้นจะไม่สะดวก เราสามารถนำขั้นตอนวิธีของยุคลิดมาประยุกต์ใช้ได้ และเราจะนำผกผันนี้ไปช่วยในการแก้คอนกรูเอนซ์เชิงเส้นดังจะกล่าวต่อไป จากตัวอย่าง 4.41 จะเห็นว่าผกผันไม่จำเป็นต้องหาค่าได้เสมอไป พิจารณา $(7, 4) = 1$ แต่ $(2, 4) \neq 1$ ทำให้เราได้ข้อสังเกตที่เป็นเงื่อนไขของการหาผกผันได้ ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.13 ถ้า a เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวกที่มากกว่า 1 ซึ่ง $(a, m) = 1$ แล้ว ผกผันของ a มอดุโล m จะหาค่าได้ และมีเพียงค่าเดียวเท่านั้นที่ไม่คอนกรูเอนซ์กันในมอดุโล m

ตัวอย่าง 4.42 จงหาผกผันของ 11 มอดุโล 60

วิธีทำ เนื่องจาก $(11, 60) = 1$ โดยทฤษฎีบท 4.13 ได้ว่า ผกผันของ 11 มอดุโล 60 หาค่าได้ จากขั้นตอนวิธีของยุคลิดได้ว่า

$$\begin{aligned} 60 &= 11(5) + 5 \\ 11 &= 5(2) + 1 \end{aligned}$$

ทำย้อนกลับได้ว่า

$$\begin{aligned} 1 &= 11 - 5(2) \\ &= 11 - [60 - 11(5)](2) \\ &= 11(11) + 60(-2) \end{aligned}$$

จากสมการ $11(11) + 60(-2) = 1$ จะได้ว่า $11(11) + 60(-2) \equiv 1 \pmod{60}$

เนื่องจาก $60(-2) \equiv 0 \pmod{60}$ ดังนั้นได้ $11(11) \equiv 1 \pmod{60}$

แสดงว่า 11 เป็นผกผันของ 11 มอดุโล 60 □

ตัวอย่าง 4.43 จงหาผลเฉลยของคอนกรูเอนซ์เชิงเส้น $11x \equiv 25 \pmod{60}$

วิธีทำ จากตัวอย่าง 4.42 ได้ว่า 11 เป็นผกผันของ 11 มอดุโล 60

คูณคอนกรูเอนซ์ที่กำหนดด้วย 11 ทั้งสองข้างได้

$$\begin{aligned} 11 \cdot 11x &\equiv 11 \cdot 25 \pmod{60} \\ 121x &\equiv 275 \pmod{60} \end{aligned}$$

เนื่องจาก $121 \equiv 1 \pmod{60}$ และ $275 \equiv 35 \pmod{60}$ ดังนั้น $x \equiv 35 \pmod{60}$

ตรวจสอบค่า x ที่ได้ว่าเป็นผลเฉลยของคอนกรูเอนซ์หรือไม่โดยการแทนค่า x ในคอนกรูเอนซ์ที่กำหนดได้ว่า

$$11x \equiv 11 \cdot 35 = 385 \equiv 25 \pmod{60}$$

ดังนั้นได้ $x \equiv 35 \pmod{60}$ เป็นผลเฉลยของคอนกรูเอนซ์ที่กำหนด □

ตัวอย่าง 4.44 จงหาผลเฉลยของคอนกรูเอนซ์เชิงเส้น $3x \equiv 4 \pmod{7}$

วิธีทำ เนื่องจาก $(3, 7) = 1$ โดยทฤษฎีบท 4.13 ได้ว่า ผกผันของ 3 มอดุโล 7 หาค่าได้ จากขั้นตอนวิธีของยุคลิดได้ว่า

$$7 = 3(2) + 1$$

$$3 = 1(3)$$

ทำย้อนกลับได้ว่า $1 = 7 - 3(2)$

จากสมการ $-2(3) + 7(1) = 1$ จะได้ว่า $-2(3) + 7(1) \equiv 1 \pmod{7}$

เนื่องจาก $7(1) \equiv 0 \pmod{7}$ ดังนั้นได้ $-2(3) \equiv 1 \pmod{7}$

แสดงว่า -2 เป็นผกผันของ 3 มอดุโล 7

คูณคอนกรูเอนซ์ที่กำหนดด้วย -2 ทั้งสองข้างได้

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}$$

$$-6x \equiv -8 \pmod{7}$$

เนื่องจาก $-6x \equiv x \pmod{7}$ และ $-8 \equiv 6 \pmod{7}$ ดังนั้น $x \equiv 6 \pmod{7}$

ตรวจสอบโดยการแทนค่า x ได้ $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7}$

นั่นคือ $x \equiv 6 \pmod{7}$ เป็นผลเฉลยของคอนกรูเอนซ์ที่กำหนด □

ทฤษฎีบทเศษเหลือของจีน

นักคณิตศาสตร์ชาวจีนชื่อ Sun – Tsu เขาถามปริศนาว่า “มีของอยู่จำนวนหนึ่งซึ่งเมื่อหารด้วย 3 จะเหลือเศษ 2 เมื่อหารด้วย 5 จะเหลือเศษ 3 และเมื่อหารด้วย 7 จะเหลือเศษ 2 จงหาจำนวนของสิ่งนั้น” ปริศนานี้สามารถเขียนอยู่ในรูประบบคอนกรูเอนซ์เชิงเส้นได้เป็น

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

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

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

จะเห็นว่าระบบคอนกรูเอนซ์เชิงเส้นนี้มีมอดุโลเป็นจำนวนเฉพาะสัมพัทธ์กันเป็นคู่ เราจะหาผลเฉลยของระบบคอนกรูเอนซ์เชิงเส้นนี้โดยใช้ทฤษฎีบทเศษเหลือของจีน ก่อนอื่นพิจารณาตัวอย่างต่อไปนี้

Sun – Tsu, จีน

ตัวอย่าง 4.45 จงหาผลเฉลยของระบบคอนกรูเอนซ์เชิงเส้น

$$\left.\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 7 \pmod 9 \end{aligned}\right\} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

วิธีทำ ในที่นี้ ได้ว่า $(5, 9) = 1$

ให้ $x = 5y + 9z$ โดยที่ y และ z เป็นจำนวนเต็ม แทนใน (1) ได้

$$5y + 9z \equiv 3 \pmod 5$$
$$5y + 9z \equiv 7 \pmod 9$$

เนื่องจาก $5y \equiv 0 \pmod 5$ และ $9z \equiv 0 \pmod 9$

ดังนั้นได้ $9z \equiv 3 \pmod 5$ และ $5y \equiv 7 \pmod 9$

เนื่องจาก $(5, 9) = 1$ โดยทฤษฎีบท 4.13 ได้ว่า 9 มีผกผันในมอดุโล 5 และ 5 มีผกผันในมอดุโล 9 จากขั้นตอนของยุคลิดได้ว่า 4 เป็นผกผันของ 9 มอดุโล 5 และ 2 เป็นผกผันของ 5 มอดุโล 9

นั่นคือ $9 \cdot 4 \equiv 1 \pmod 5$ และ $5 \cdot 2 \equiv 1 \pmod 9$

ให้ $y = 7 \cdot 2$ และ $z = 3 \cdot 4$

ดังนั้นได้ $9z = 9(3 \cdot 4) = (9 \cdot 4) \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod 5$

และ $5y = 5(7 \cdot 2) = (5 \cdot 2) \cdot 2 \equiv 1 \cdot 2 \equiv 7 \pmod 9$

ทำให้ได้ว่า $x = 5y + 9z = 5 \cdot 7 \cdot 2 + 9 \cdot 3 \cdot 4 = 178$ สอดคล้องกับระบบคอนกรูเอนซ์เชิงเส้น (1) โดยการตรวจคำตอบดังนี้

$$178 \equiv 3 \pmod 5$$
$$178 \equiv 7 \pmod 9$$

□

พิจารณาระบบคอนกรูเอนซ์ (1) ที่อยู่ในรูปทั่วไปเพื่อสร้างเป็นทฤษฎีบท ได้ดังนี้
จากตัวอย่าง 4.45 ให้ $a_1 = 3,\ a_2 = 7,\ m_1 = 5$ และ $m_2 = 9$
ดังนั้นจากระบบคอนกรูเอนซ์ (1) ได้ว่า

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}\right\} \quad \cdots\cdots\cdots\cdots\cdots\cdots(2)$$

เราจะพิจารณาเฉพาะกรณีที่ $(m_1, m_2) = 1$
ให้ $x = m_1y + m_2z$ โดยที่ y และ z เป็นจำนวนเต็ม แทนใน (2) ได้

$$m_1y + m_2z \equiv a_1 \pmod{m_1}$$
$$m_1y + m_2z \equiv a_2 \pmod{m_2}$$

เนื่องจาก $m_1y \equiv 0 \pmod{m_1}$ และ $m_2z \equiv 0 \pmod{m_2}$
ดังนั้นได้ $m_2z \equiv a_1 \pmod{m_1}$ และ $m_1y \equiv a_2 \pmod{m_2}$
เนื่องจาก $(m_1, m_2) = 1$ โดยทฤษฎีบท 4.13 ได้ว่า m_2 มีผกผันในมอดุโล m_1 ให้เป็น y_1 และ m_1 มีผกผันในมอดุโล m_2 ให้เป็น y_2
นั่นคือ $m_2y_1 \equiv 1 \pmod{m_1}$ และ $m_1y_2 \equiv 1 \pmod{m_2}$
ให้ $y = a_2y_2$ และ $z = a_1y_1$
ดังนั้นได้ $m_2z = m_2(a_1y_1) = (m_2y_1)a_1 \equiv 1 \cdot a_1 \equiv a_1 \pmod{m_1}$
และ $m_1y = m_1(a_2y_2) = (m_1y_2)a_2 \equiv 1 \cdot a_2 \equiv a_2 \pmod{m_2}$
ทำให้ได้ว่า $x = m_1y + m_2z = m_1a_2y_2 + m_2a_1y_1$ เป็นผลเฉลยของระบบคอนกรูเอนซ์เชิงเส้น (2)
ต่อไปจะแสดงว่าระบบคอนกรูเอนซ์เชิงเส้น (2) มีผลเฉลยเดียวในมอดุโล $m = m_1m_2$
สมมติว่า x' เป็นอีกผลเฉลยหนึ่งของ (2) ดังนั้นได้

$$x' \equiv a_1 \pmod{m_1}$$
$$x' \equiv a_2 \pmod{m_2}$$

แสดงว่า $x' \equiv x \pmod{m_1}$ และ $x' \equiv x \pmod{m_2}$
จะได้ว่า $m_1 \mid (x' - x)$ และ $m_2 \mid (x' - x)$
เนื่องจาก $(m_1, m_2) = 1$ จากแบบฝึกหัดบทที่ 4 ข้อ 2.4 ได้ $m_1m_2 \mid (x' - x)$
นั่นคือ $x' \equiv x \pmod{m_1m_2}$

ทำให้ได้ทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 4.14 ให้ m_1 และ m_2 เป็นจำนวนเต็มบวกซึ่ง $(m_1, m_2) = 1$ ซึ่ง a_1, a_2 เป็นจำนวนเต็ม และให้ y_1, y_2 เป็นจำนวนเต็มที่เป็นผลเฉลยของ

$$m_2y_1 \equiv 1 \pmod{m_1} \quad \text{และ} \quad m_1y_2 \equiv 1 \pmod{m_2}$$

จะได้ว่า ระบบคอนกรูเอนซ์เชิงเส้น

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

มีผลเฉลยร่วมกันเพียงตัวเดียว คือ $x = m_2a_1y_1 + m_1a_2y_2$ ในมอดุโล $m = m_1m_2$

ตัวอย่าง 4.46 จงหาผลเฉลยที่เป็นบวกค่าน้อยสุดของระบบคอนกรูเอนซ์เชิงเส้น

$$x \equiv 5 \pmod{7}$$
$$x \equiv 2 \pmod{9}$$

วิธีทำ ในที่นี้ให้ $m_1 = 7,\ m_2 = 9,\ a_1 = 5$ และ $a_2 = 2$

จะได้ว่า $(m_1, m_2) = (7, 9) = 1$ และ $m = m_1m_2 = 7 \cdot 9 = 63$

ต้องการหา y_1 และ y_2 ที่สอดคล้องกับคอนกรูเอนซ์ $9y_1 \equiv 1 \pmod{7}$ และ $7y_2 \equiv 1 \pmod{9}$

จะได้ -3 เป็นผกผันของ 9 ในมอดุโล 7 และ 4 เป็นผกผันของ 7 ในมอดุโล 9

ดังนั้นให้ $y_1 = -3$ และ $y_2 = 4$

โดยทฤษฎีบท 4.14 ได้ว่า $x = 9 \cdot 5 \cdot (-3) + 7 \cdot 2 \cdot 4 = -79$ เป็นผลเฉลยหนึ่ง

และ $-79 \equiv 47 \pmod{63}$

ดังนั้นได้ $x \equiv 47 \pmod{63}$ เป็นผลเฉลยที่เป็นบวกค่าน้อยสุดของระบบคอนกรูเอนซ์ที่กำหนด

สามารถตรวจคำตอบได้ดังนี้

$$47 \equiv 5 \pmod{7}$$
$$47 \equiv 2 \pmod{9}$$

□

ต่อไปจะกล่าวถึงการแก้ระบบคอนกรูเอนซ์เชิงเส้นที่มี n คอนกรูเอนซ์ โดยใช้ทฤษฎีบทเศษเหลือของจีนซึ่งเป็นกรณีทั่วไปของทฤษฎีบท 4.14 ดังนี้

ทฤษฎีบท 4.15 *ทฤษฎีบทเศษเหลือของจีน*

ให้ $m_1, m_2, \ldots, m_n$ เป็นจำนวนเต็มบวกซึ่ง $(m_i, m_j) = 1$ เมื่อ $i \neq j$ และ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มและให้ $m = m_1m_2 \cdots m_n$ และ $M_i = \dfrac{m}{m_i}$

สำหรับแต่ละ i ให้ y_i เป็นจำนวนเต็มที่เป็นผลเฉลยของ $M_iy \equiv 1 \pmod{m_i}$

จะได้ว่า ระบบคอนกรูเอนซ์เชิงเส้น

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

มีผลเฉลยร่วมกันเพียงตัวเดียว คือ $x = M_1a_1y_1 + M_2a_2y_2 + \cdots + M_na_ny_n$ ในมอดุโล m

ตัวอย่าง 4.47 จงหาผลเฉลยที่เป็นบวกค่าน้อยสุดของระบบคอนกรูเอนซ์เชิงเส้น

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

วิธีทำ ให้ $a_1 = 2,\ a_2 = 3,\ a_3 = 2,\ m_1 = 3,\ m_2 = 5$ และ $m_3 = 7$
เนื่องจาก $(3, 5) = (3, 7) = (5, 7) = 1$ โดยทฤษฎีบทเศษเหลือของจีน
ได้ว่าระบบคอนกรูเอนซ์เชิงเส้นมีผลเฉลยเดียวในมอดุโล $m = 3 \cdot 5 \cdot 7 = 105$
ให้ $M_1 = \dfrac{m}{m_1} = \dfrac{105}{3} = 35,\ M_2 = \dfrac{m}{m_2} = \dfrac{105}{5} = 21$
และ $M_3 = \dfrac{m}{m_3} = \dfrac{105}{7} = 15$
ต้องการหา $y_1,\ y_2$ และ y_3 ที่สอดคล้องกับคอนกรูเอนซ์

$$35y_1 \equiv 1 \pmod 3$$
$$21y_2 \equiv 1 \pmod 5$$
$$15y_3 \equiv 1 \pmod 7$$

จะได้ว่า $y_1 = 2,\ y_2 = 1$ และ $y_3 = 1$
โดยทฤษฎีบทเศษเหลือของจีน ได้ผลเฉลยคือ

$$x = M_1a_1y_1 + M_2a_2y_2 + M_3a_3y_3 = 35 \cdot 2 \cdot 2 + 21 \cdot 3 \cdot 1 + 15 \cdot 2 \cdot 1 = 233$$

และ $233 \equiv 23 \pmod{105}$
ดังนั้นได้ $x \equiv 23 \pmod{105}$ เป็นผลเฉลยที่เป็นบวกค่าน้อยสุดของระบบคอนกรูเอนซ์ที่กำหนด
สามารถตรวจคำตอบได้ดังนี้

$$23 \equiv 2 \pmod 3$$
$$23 \equiv 3 \pmod 5$$
$$23 \equiv 2 \pmod 7$$

□

การคำนวณตัวเลขที่มีค่ามาก

ให้ $m_1, m_2, \ldots, m_n$ เป็นจำนวนเต็มบวกที่มากกว่า 1 ซึ่ง $(m_i, m_j) = 1$ เมื่อ $i \neq j$ และ $m = m_1m_2 \cdots m_n$ โดยทฤษฎีบทเศษเหลือของจีนสามารถแสดงได้ว่า แต่ละจำนวนเต็ม a ที่ $0 \leq a < m$ สามารถแทนได้ด้วย n - สิ่งอันดับ ที่เป็นเศษเหลือจากการหาร m_i ได้แบบเดียวเท่านั้น นั่นคือเขียนแทน a ด้วย

$$(a \textbf{ mod } m_1,\ a \textbf{ mod } m_2,\ \ldots,\ a \textbf{ mod } m_n)$$

ตัวอย่าง 4.48 ให้ $m_1 = 3$ และ $m_2 = 4$
ดังนั้นสามารถแทนจำนวนตั้งแต่ 0 ถึง 11 ได้ด้วยคู่อันดับต่อไปนี้

$$\begin{array}{llll} 0 = (0, 0), & 1 = (1, 1), & 2 = (2, 2), & 3 = (0, 3), \\ 4 = (1, 0), & 5 = (2, 1), & 6 = (0, 2), & 7 = (1, 3), \\ 8 = (2, 0), & 9 = (0, 1), & 10 = (1, 2), & 11 = (2, 3) \end{array}$$

□

ในการคำนวณตัวเลขที่มีค่ามากเราจะเลือก $m_1, m_2, \ldots, m_n$ เป็นจำนวนเต็มบวกที่มากกว่า 1 ซึ่ง $(m_i, m_j) = 1$ เมื่อ $i \neq j$ และ $m = m_1 m_2 \cdots m_n$ ดังตัวอย่าง

ตัวอย่าง 4.49 ให้ $m_1 = 99,\ m_2 = 98,\ m_3 = 97$ และ $m_4 = 95$ เป็นจำนวนเฉพาะสัมพัทธ์เป็นคู่ โดยทฤษฎีบทเศษเหลือของจีนสามารถแสดงได้ว่า แต่ละจำนวนเต็ม a ซึ่ง $0 \leq a < m$ โดยที่ $m = 99 \cdot 98 \cdot 97 \cdot 95$ สามารถแทนได้ด้วย n – สิ่งอันดับที่เป็นเศษเหลือจากการหารด้วย m_i ได้แบบเดียวเท่านั้น เช่น

$a = 123{,}684$ สามารถเขียนแทนด้วย 4 – สิ่งอันดับ คือ

$$(123684 \textbf{ mod } 99,\ 123684 \textbf{ mod } 98,\ 123684 \textbf{ mod } 97,\ 123684 \textbf{ mod } 95)$$

ดังนั้นได้ $a = (33, 8, 9, 89)$

ในทำนองเดียวกันสามารถแทน $b = 413{,}456$ ด้วย 4 – สิ่งอันดับ คือ

$$(413456 \textbf{ mod } 99,\ 413456 \textbf{ mod } 98,\ 413456 \textbf{ mod } 97,\ 413456 \textbf{ mod } 95)$$

ดังนั้นได้ $b = (32, 92, 42, 16)$

ถ้าต้องการหา $a + b$ เราสามารถหาได้โดยการใช้ 4 – สิ่งอันดับ ดังนี้

$(33, 8, 9, 89) + (32, 92, 42, 16)$

$= (65 \textbf{ mod } 99,\ 100 \textbf{ mod } 98,\ 51 \textbf{ mod } 97,\ 105 \textbf{ mod } 95) = (65, 2, 51, 10)$

ถ้าต้องการหาว่าจำนวนใดที่แทนด้วย 4 – สิ่งอันดับนี้ เราหาได้โดยการหาผลเฉลยของระบบคอนกรูเอนซ์

$$x \equiv 65 \pmod{99}$$
$$x \equiv 2 \pmod{98}$$
$$x \equiv 51 \pmod{97}$$
$$x \equiv 10 \pmod{95}$$

โดยใช้ทฤษฎีบทเศษเหลือของจีนได้ผลเฉลยของระบบคอนกรูเอนซ์นี้ คือ 537,140

ซึ่งจะได้ผลลัพธ์เช่นเดียวกันกับ $123{,}684 + 413{,}456 = 537{,}140$ □

ก่อนจะกล่าวถึงการเข้ารหัสแบบ RSA จะกล่าวถึงความรู้ที่จะนำไปใช้ คือ การคำนวณจำนวนที่อยู่ในรูปเลขชี้กำลังโดยทฤษฎีบทของแฟร์มาต์

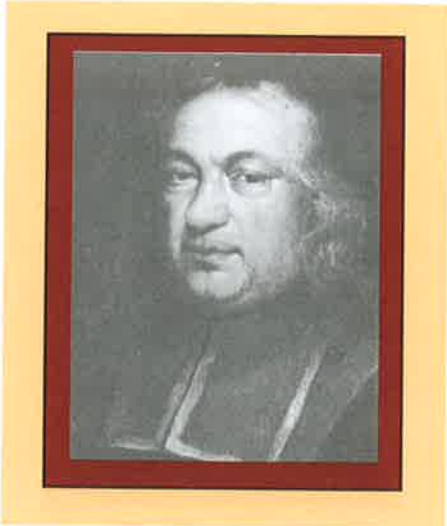
ทฤษฎีบท 4.16 *ทฤษฎีบทของแฟร์มาต์*

ถ้า p เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มซึ่ง $(a, p) = 1$ แล้วจะได้ว่า

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

และยังได้ว่า สำหรับจำนวนเต็ม a ใด ๆ

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



แฟร์มาต์, ปีแยร์ เดอ
ค.ศ. 1601 – 1665, ฝรั่งเศส

ตัวอย่าง 4.50 เนื่องจาก 101 เป็นจำนวนเฉพาะ และ $(2, 101) = 1$ จากทฤษฎีบทของแฟร์มาต์ได้

$$2^{100} \equiv 1 \pmod{101}$$

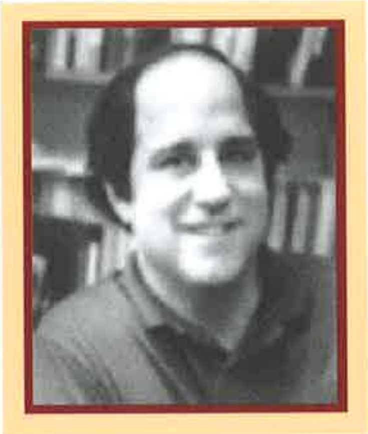
□

การเข้ารหัสแบบ RSA

ในปี ค.ศ. 1976 กลุ่มนักวิจัย 3 ท่าน คือ Ronald Rivest, Adi Shamir และ Leonard Adleman ได้วิจัยการเข้ารหัสแบบ RSA ซึ่งการเข้ารหัสแบบนี้จำเป็นต้องใช้ความรู้ในเรื่องของมอดุโล และการคำนวณค่าตัวเลขที่มีค่ามาก โดยการแปลงแต่ละตัวอักษรเป็นตัวเลขก่อนเหมือนกับการเข้ารหัสแบบซีซาร์ แล้วจึงแบ่งกลุ่มตัวเลขด้วยความยาวตามที่ต้องการ ซึ่งแต่ละกลุ่มของตัวเลขจะแทนกลุ่มของตัวอักษรแล้วจึงเข้ารหัส โดยการสร้างฟังก์ชันการแปลงรหัสเป็น

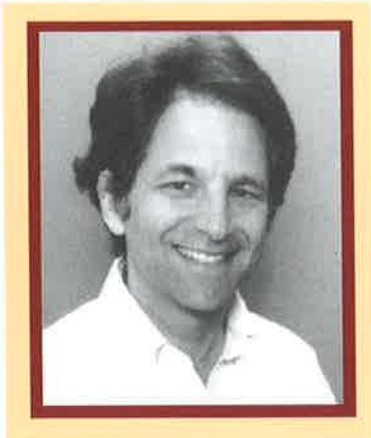
$$C = M^e \textbf{ mod } n \quad \text{เมื่อ} \quad n = pq$$

โดยที่ p และ q เป็นจำนวนเฉพาะซึ่ง $1 < e < (p-1)(q-1)$ และ $(e, (p-1)(q-1)) = 1$ ดังตัวอย่าง



Ronald Rivest
ค.ศ. 1948 – ปัจจุบัน,

Adi Shamir
ค.ศ. 1952 – ปัจจุบัน, อิสราเอล



Leonard Adleman
ค.ศ. 1945 – ปัจจุบัน, สหรัฐอเมริกา

ตัวอย่าง 4.51 จงแปลงข้อความ "STOP" โดยใช้รหัส RSA เมื่อ $p = 43$ และ $q = 59$ เลือก $e = 13$ และให้ $\mathrm{A} = 00, \mathrm{B} = 01, \mathrm{C} = 02, \ldots, \mathrm{Z} = 25$

วิธีทำ จะเห็นว่า $(e, (p-1)(q-1)) = (13, 42 \cdot 58) = 1$
จากข้อความ STOP แปลงเป็นตัวเลขได้

$$18,\ 19,\ 14,\ 15$$

แล้วจัดกลุ่มตัวเลขเป็น 4 หลัก (ขึ้นอยู่กับข้อตกลงระหว่างผู้ส่งกับผู้รับ) ได้เป็น

$$1819 \quad 1415$$

แปลงรหัสโดยใช้ $C = M^{13} \ \mathbf{mod}\ 43 \cdot 59$ หรือ $C = M^{13} \ \mathbf{mod}\ 2537$
ดังนั้นได้

$$1819^{13} \ \mathbf{mod}\ 2537 = 2081$$

และ $1415^{13} \ \mathbf{mod}\ 2537 = 2182$

ดังนั้นตัวเลขที่ได้จากการเข้ารหัสเป็น

$$2081 \quad 2182 \quad \text{หรือ} \quad 2003 \quad 2104$$

แล้วแปลงเป็นตัวอักษรได้เป็น "UDVE" □

การถอดรหัสแบบ RSA

เราสามารถถอดรหัสข้อความที่เข้ารหัส RSA ได้โดยผู้เข้ารหัสต้องบอกค่า e และ n เนื่องจาก $(e, (p-1)(q-1)) = 1$ ดังนั้นหาค่า d ซึ่งเป็นผกผันของ e ในมอดุโล $(p-1)(q-1)$ ได้ นั่นคือ

$$de \equiv 1 \pmod{(p-1)(q-1)}$$

จะมีจำนวนเต็ม k ซึ่ง $de = 1 + k(p-1)(q-1)$ ดังนั้นได้

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

ให้ $(M, p) = (M, q) = 1$ จากทฤษฎีบทของแฟร์มาต์ได้ว่า

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

ดังนั้น $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M \pmod{p}$

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

เนื่องจาก $(p, q) = 1$ จากทฤษฎีเศษเหลือของจีนได้ว่า

$$C^d \equiv M \pmod{pq}$$

นั่นคือ เราต้องหาค่า P ซึ่ง

$$P = C^d \textbf{ mod } pq$$

ตัวอย่างต่อไปจะแสดงการถอดรหัส RSA

ตัวอย่าง 4.52 ถ้าข้อความที่ได้รับคือ 0981 0461
แล้วจงถอดรหัส RSA โดยที่ผู้เข้ารหัสบอกค่า $e = 13$ และ $n = 2537$

วิธีทำ จาก $n = 2537$ แยกตัวประกอบเป็นจำนวนเฉพาะ 2 ตัวคูณกันได้ $n = 43 \cdot 59$
เราจะหาค่า d ที่เป็นผกผันของ $e = 13$ ในมอดุโล $42 \cdot 58$ นั่นคือหาค่า d ซึ่งทำให้

$$13d \equiv 1 \pmod{42 \cdot 58} \quad \text{หรือ} \quad 13d \equiv 1 \pmod{2436}$$

โดยการแก้คอนกรูเอนซ์เหมือนตัวอย่าง 4.42 จะได้ $d = 937$
ถอดรหัส โดยต้องหาค่า P ที่ทำให้

$$P = C^d \textbf{ mod } pq \quad \text{หรือ} \quad P = \mathrm{C}^{937} \textbf{ mod } 2537$$

โดยแทนค่า $C = 0918$ และ $C = 0461$
ดังนั้นได้ $0981^{937} \textbf{ mod } 2537 = 0704$ และ $0461^{937} \textbf{ mod } 2537 = 1115$
ข้อความที่ส่งมาคือ 0704 1115 ซึ่งถอดเป็นข้อความได้เป็น "HELP" □

แบบฝึกหัดบทที่ 4

1. จงพิจารณาว่า 13 หารจำนวนต่อไปนี้ลงตัวหรือไม่

   1.1 89 1.2 197 1.3 247 1.4 1261

2. สำหรับจำนวนเต็ม a, b และ c ใด ๆ จงพิสูจน์ว่า

   2.1 ถ้า $a \neq 0$ แล้ว $a \mid 0$ และ $a \mid a$

   2.2 $a \mid 1$ ก็ต่อเมื่อ $a = 1$ หรือ $a = -1$

   2.3 ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = b$ หรือ $a = -b$

   2.4 ถ้า $a \mid c$ และ $b \mid c$ โดยที่ $(a, b) = 1$ แล้ว $ab \mid c$

   2.5 ถ้า $a \mid bc$ และ $(a, b) = 1$ แล้ว $a \mid c$

   2.6 ถ้า $d = (a, b)$ แล้ว $(\frac{a}{d}, \frac{b}{d}) = 1$

3. จงพิจารณาว่าจำนวนต่อไปนี้เป็นจำนวนเฉพาะหรือเป็นจำนวนประกอบ

   3.1 53 3.2 79 3.3 101 3.4 163

4. จงพิจารณาว่าจำนวนต่อไปนี้เป็นจำนวนเฉพาะหรือเป็นจำนวนประกอบ

   4.1 43 4.2 89 4.3 1011 4.4 1347

5. จงหาผลหารและเศษเหลือของจำนวนที่กำหนด

   5.1 0 หารด้วย 12 5.2 -1 หารด้วย 4

   5.3 78 หารด้วย -13 5.4 -999 หารด้วย -23

6. จงหาผลหารและเศษเหลือของจำนวนที่กำหนด

   6.1 2 หารด้วย 7 6.2 -333 หารด้วย 33

   6.3 -7007 หารด้วย -89 6.4 2345678 หารด้วย 101

7. จงหาตัวประกอบที่เป็นจำนวนเฉพาะของจำนวนต่อไปนี้

   7.1 99 7.2 729 7.3 2222 7.4 505050

8. จงหาตัวประกอบที่เป็นจำนวนเฉพาะของจำนวนต่อไปนี้

   8.1 97 8.2 987 8.3 3333 8.4 808080

9. จงหาจำนวนเต็มบวกที่น้อยกว่า 24 และเป็นจำนวนเฉพาะสัมพัทธ์กับ 24

10. จงหาจำนวนเต็มบวกที่น้อยกว่า 35 และเป็นจำนวนเฉพาะสัมพัทธ์กับ 35

11. จงพิจารณาว่าจำนวนที่กำหนดในแต่ละข้อต่อไปนี้เป็นจำนวนเฉพาะสัมพัทธ์กันเป็นคู่หรือไม่

   11.1 17,35, 64 11.2 28, 33, 79

   11.3 19, 29, 39, 49 11.4 35, 46, 57, 681

12. จงพิจารณาว่าจำนวนที่กำหนดในแต่ละข้อต่อไปนี้เป็นจำนวนเฉพาะสัมพัทธ์กันเป็นคู่หรือไม่
    12.1 3, 5, 11 12.2 38, 43, 99
    12.3 22, 47, 89, 101 12.4 35, 46, 57, 681
13. จงแสดงว่า 3 หารผลคูณของจำนวนเต็มสามจำนวนที่เรียงติดกันได้ลงตัว
14. ให้ m เป็นจำนวนเต็มบวก จงแสดงว่า m หารผลคูณของจำนวนเต็ม m จำนวนที่เรียงติดกันได้ลงตัว
15. จำนวนนับตั้งแต่ 1 ถึง 200 มีทั้งหมดกี่จำนวน ซึ่งเมื่อหารด้วย 6 แล้วเหลือเศษ 2 และเมื่อหารด้วย 14 แล้วเหลือเศษ 10
16. จำนวนนับตั้งแต่ 1 ถึง 300 มีทั้งหมดกี่จำนวน ซึ่งเมื่อหารด้วย 7 แล้วเหลือเศษ 2 และเมื่อหารด้วย 11 แล้วเหลือเศษ 8
17. ให้ m เป็นจำนวนเต็มบวก และ a, b และ c เป็นจำนวนเต็ม จงพิสูจน์ว่า
    ถ้า $ac \equiv bc \pmod{m}$ แล้ว $a \equiv b \ (\text{mod } \dfrac{m}{(c,m)})$
18. จงแสดงว่า ถ้า $2^n - 1$ เป็นจำนวนเฉพาะ แล้ว n เป็นจำนวนเฉพาะ
    [**แนะนำ** ใช้ $2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$]
19. จงพิจารณาว่าจำนวนเต็มต่อไปนี้ จำนวนใดเป็นจำนวนเฉพาะ
    19.1 $2^7 - 1$ 19.2 $2^{11} - 1$ 19.3 $2^{21} - 1$
20. จงแสดงว่า ถ้า n และ k เป็นจำนวนเต็มบวก แล้วจะได้ว่า $\left\lceil \dfrac{n}{k} \right\rceil = \left\lfloor \dfrac{n-1}{k} \right\rfloor + 1$
21. จงหาตัวหารร่วมมากและตัวคูณร่วมน้อยของจำนวนเต็มแต่ละคู่ต่อไปนี้
    21.1 $2^3 \cdot 3^2 \cdot 5^7,\ 2^7 \cdot 3^3 \cdot 5^2$ 21.2 $3^3 \cdot 7^5 \cdot 11^2,\ 2^7 \cdot 3^4 \cdot 7^2$
    21.3 $41^3 \cdot 43^2 \cdot 53^7,\ 41^3 \cdot 43^2 \cdot 53^7$ 21.4 $3 \cdot 101,\ 0$
22. จงหาค่าจำนวนต่อไปนี้
    22.1 $23 \textbf{ mod } 3$ 22.2 $-99 \textbf{ mod } 13$ 22.3 $2^{340} \textbf{ mod } 341$
23. จงหาค่าจำนวนต่อไปนี้
    23.1 $13 \textbf{ mod } 3$ 23.2 $-97 \textbf{ mod } 11$ 23.3 $3^{340} \textbf{ mod } 341$
24. จงหาเลขโดดหลักท้ายของ 2^{350}
25. จงหาเลขโดดสองหลักท้ายของ 3^{400}
26. จงพิสูจน์ว่า $a \equiv b \pmod{m}$ ก็ต่อเมื่อ $a \textbf{ mod } m = b \textbf{ mod } m$
27. จงหาตำแหน่งในหน่วยความจำโดยใช้ฟังก์ชันแฮช $h(k) = k \textbf{ mod } 101$ ในการจัดเก็บเรคคอร์ดของนักศึกษาที่กำหนดให้ต่อไปนี้
    27.1 104567890 (65) 27.2 234056793 (100)
28. จงหาตำแหน่งในหน่วยความจำโดยใช้ฟังก์ชันแฮช $h(k) = k \textbf{ mod } 101$ ในการจัดเก็บเรคคอร์ดของนักศึกษาที่กำหนดให้ต่อไปนี้
    28.1 610235872 28.2 330126981
29. จงหาลำดับที่เกิดจากการสร้างตัวเลขสุ่มแบบเทียมโดยมีตัวก่อกำเนิดที่ได้จากคอนกรูเอนซ์เชิงเส้น

$$x_{n+1} = (5x_n + 1) \textbf{ mod } 7 \quad \text{เมื่อค่าเริ่มต้น } x_0 = 2$$

30. จงหาลำดับที่เกิดจากการสร้างตัวเลขสุ่มแบบเทียมโดยมีตัวก่อกำเนิดที่ได้จากคอนกรูเอนซ์เชิงเส้น

$$x_{n+1} = 4x_n \textbf{ mod } 11 \quad \text{เมื่อค่าเริ่มต้น } x_0 = 3$$

31. จงเข้ารหัสข้อความ "SEE YOU NEXT TIME" โดยใช้ฟังก์ชัน f ดังต่อไปนี้

31.1 $f(p) = (p+3) \bmod 26$ 31.2 $f(p) = (5p+7) \bmod 26$

32. จงเข้ารหัสข้อความ "TOMORROW" โดยใช้ฟังก์ชัน f ดังต่อไปนี้

32.1 $f(p) = (p+17) \bmod 26$ 32.2 $f(p) = (7p+3) \bmod 26$

33. จงถอดรหัสข้อความ "JR WR WKH SDUWB" ซึ่งถูกส่งมาโดยการเข้ารหัสแบบซีซาร์
34. จงถอดรหัสข้อความ "QHAW ZHHN" ซึ่งถูกส่งมาโดยการเข้ารหัสแบบซีซาร์
35. จงใช้ขั้นตอนวิธีของยุคลิดหาจำนวนเต็ม x และ y ที่ทำให้ $(a, b) = ax + by$ เมื่อ

35.1 $a = 18,\ b = 12$ 35.2 $a = 201,\ b = 111$

35.3 $a = 1331,\ b = 1001$ 35.4 $a = 9889,\ b = 6060$

35.5 $a = 53421,\ b = 12345$ 35.6 $a = 11111,\ b = 111111$

36. จงเปลี่ยนจำนวนที่กำหนดให้ในเลขฐานสิบเป็นจำนวนในเลขฐานสอง

36.1 123 36.2 4532 36.3 100632

37. จงเปลี่ยนจำนวนที่กำหนดให้ในเลขฐานสองเป็นจำนวนในเลขฐานสิบ

37.1 1 111 37.2 1 0101 0101 37.3 111 1100 0001 1111

38. จงเปลี่ยนจำนวนที่กำหนดให้ในเลขฐานสิบหกเป็นจำนวนในเลขฐานสอง

38.1 103F 38.2 ABBAB 38.3 BADFACED

39. จงเปลี่ยนจำนวนที่กำหนดให้ในเลขฐานสองเป็นจำนวนในเลขฐานสิบหก

39.1 1111 0111 39.2 1010 1010 1010 39.3 111 0111 0111 0111

40. จงเปลี่ยนจำนวนที่กำหนดให้ในเลขฐานแปดเป็นจำนวนในเลขฐานสอง

40.1 7345321 40.2 12345670 40.3 100063211

41. จงเปลี่ยนจำนวนที่กำหนดให้ในเลขฐานสองเป็นจำนวนในเลขฐานแปด

41.1 1011 1011 41.2 10 1011 1011 41.3 111 1111 1111

42. จงแสดงว่า 15 เป็นผกผันของ 7 ในมอดุโล 26
43. จงแสดงว่า 937 เป็นผกผันของ 13 ในมอดุโล 2436
44. จงหาผกผันของ 4 ในมอดุโล 9
45. จงหาผกผันของ 2 ในมอดุโล 17
46. จงหาผกผันของ 19 ในมอดุโล 141
47. จงหาผกผันของ 144 ในมอดุโล 233
48. จงหาผลเฉลยของคอนกรูเอนซ์เชิงเส้นต่อไปนี้

48.1 $4x \equiv 5 \pmod 9$ 48.2 $2x \equiv 7 \pmod{17}$

48.3 $10x \equiv 7 \pmod{13}$ 48.4 $8x \equiv 6 \pmod{11}$

49. ให้ a และ b เป็นจำนวนเต็ม $m_1, m_2, \ldots, m_n$ เป็นจำนวนเต็มบวกซึ่ง $(m_i, m_j) = 1$ เมื่อ $i \neq j$ และ $m = m_1 m_2 \cdots m_n$ จงแสดงว่า ถ้า $a \equiv b \pmod{m_i}$ ทุก $i = 1, 2, \ldots, n$ แล้วจะได้ว่า $a \equiv b \pmod m$

50. จงหาผลเฉลยทั้งหมดของระบบคอนกรูเอนซ์เชิงเส้นต่อไปนี้

50.1 $x \equiv 2 \pmod{3}$
$x \equiv 4 \pmod{5}$
$x \equiv 5 \pmod{11}$

50.2 $x \equiv 2 \pmod{3}$
$x \equiv 1 \pmod{4}$
$x \equiv 3 \pmod{5}$

50.3 $x \equiv 1 \pmod{2}$
$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{5}$
$x \equiv 4 \pmod{11}$

50.4 $x \equiv 5 \pmod{3}$
$x \equiv 2 \pmod{4}$
$x \equiv 8 \pmod{5}$
$x \equiv 4 \pmod{7}$

50.5* $x \equiv 5 \pmod{6}$
$x \equiv 3 \pmod{10}$
$x \equiv 8 \pmod{15}$

50.6 $x \equiv 7 \pmod{9}$
$x \equiv 4 \pmod{12}$
$x \equiv 16 \pmod{21}$

51. จงหาจำนวนเต็มที่หารด้วย 3, 4 และ 5 แล้วเหลือเศษ 2, 1 และ 2 ตามลำดับ

52. จงหาจำนวนเต็มที่หารด้วย 5 ลงตัว แต่เมื่อหารด้วย 3 แล้วเหลือเศษ 1

53. จงแสดงว่า $2^{340} \equiv 1 \pmod{11}$ โดยใช้ทฤษฎีบทของแฟร์มาต์ [**แนะนำ** $2^{340} = (2^{10})^{34}$]

54. จงแสดงว่า $2^{340} \equiv 1 \pmod{31}$ โดยใช้ทฤษฎีบทของแฟร์มาต์ [**แนะนำ** $2^{340} = (2^{5})^{68}$]

55. จงแสดงว่า $2^{340} \equiv 1 \pmod{341}$

56. จงใช้ทฤษฎีบทของแฟร์มาต์และทฤษฎีบทเศษเหลือของจีน เพื่อหาค่า

56.1 3^{302} **mod** 5, 3^{302} **mod** 7, 3^{302} **mod** 11 และ 3^{302} **mod** 385

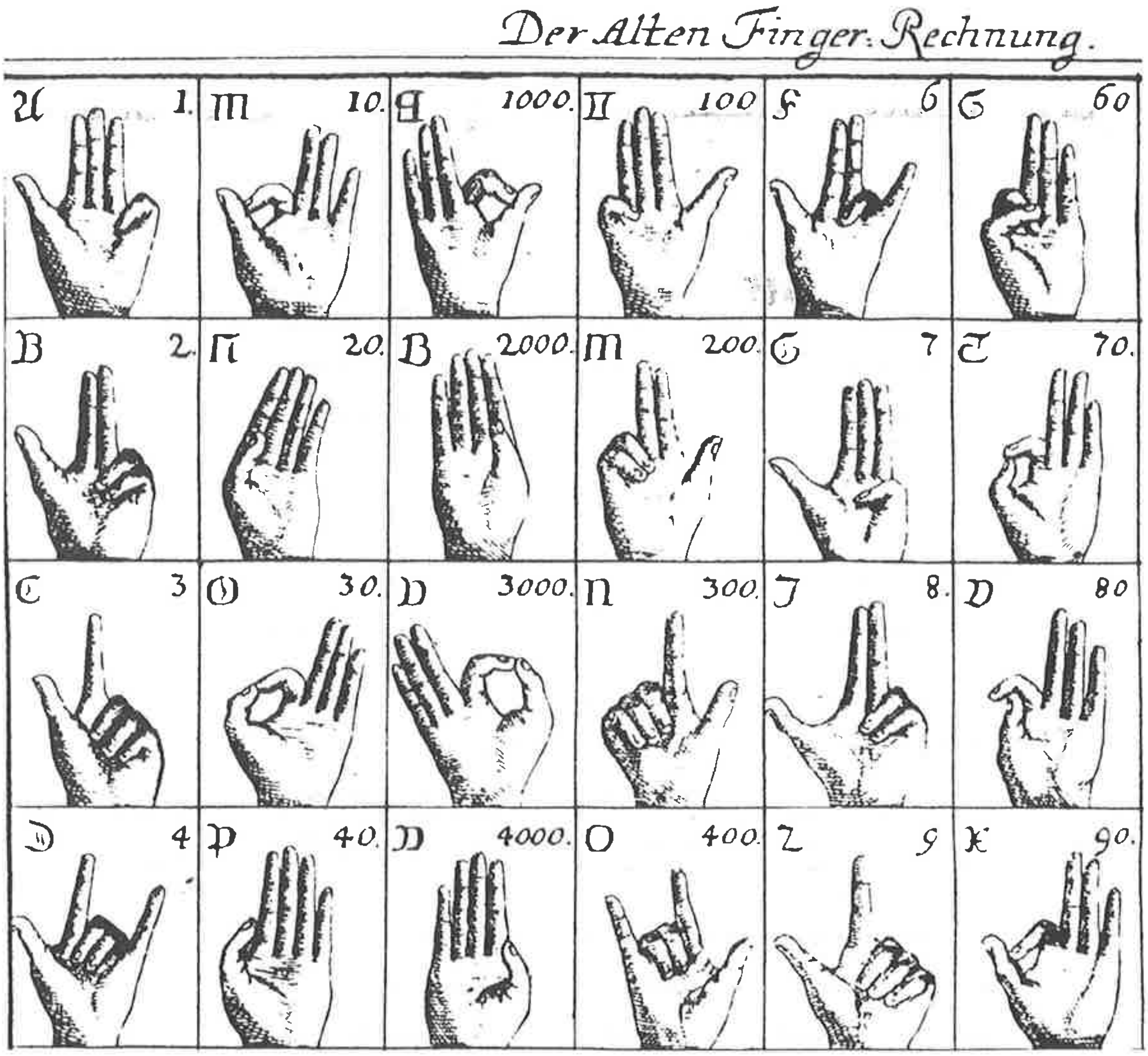
56.2 5^{2003} **mod** 7, 5^{2003} **mod** 11, 5^{2003} **mod** 13 และ 5^{2003} **mod** 1001

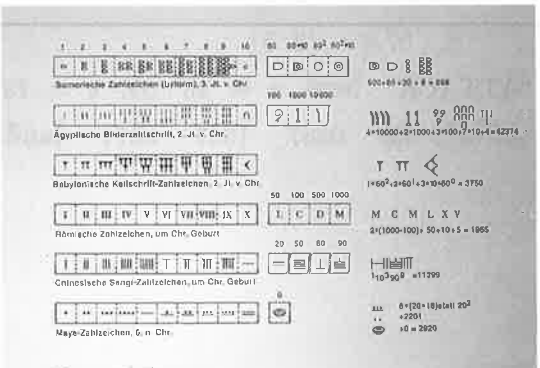
57. จงหา a ซึ่งเป็นจำนวนเต็มที่ไม่เป็นลบและน้อยกว่า 28 โดยเขียนอยู่ในรูป (a **mod** 4, a **mod** 7)

57.1	(0, 0)	57.2	(1, 0)	57.3	(1, 1)
57.4	(2, 1)	57.5	(2, 2)	57.6	(0, 3)
57.7	(2, 0)	57.8	(3, 5)	57.9	(3, 6)

58. จงเข้ารหัส RSA ข้อความ "ATTACK" โดยที่ $n = 43 \cdot 59$, $e = 13$

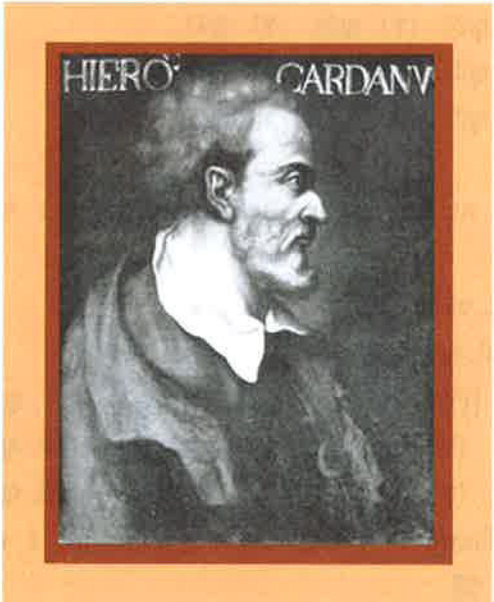
59. จงถอดรหัส RSA เมื่อข้อความที่ได้รับ คือ 0667 1947 0671 โดยที่ $n = 43 \cdot 59$, $e = 13$





Historische Ziffernsysteme.

คณิตศาสตร์เชิงการจัด



คาร์ดาโน, เจโรนิโม
ค.ศ. 1501 – 1576, อิตาลี

วิธีการนับ

หลักการนับเบื้องต้น

เรามักจะคุ้นเคยกับการนับจำนวนวิธีของการทำงานบางอย่าง หรือจำนวนวิธีที่เหตุการณ์บางอย่างจะเกิดขึ้น ตัวอย่างเช่น จำนวนวิธีที่จะจัดเรียงสิ่งของเพื่อตกแต่งสถานที่ จำนวนวิธีที่จะจัดคนกลุ่มหนึ่งเข้าที่พัก จำนวนวิธีที่จะจัดการแข่งขันของทีมนักกีฬา เป็นต้น หลักการนับเบื้องต้นจะช่วยให้การนับจำนวนวิธีของเหตุการณ์ต่างๆ ทำได้ง่ายและสะดวกรวดเร็วขึ้น หลักการนับเบื้องต้นจะประกอบด้วยหลักการคูณและหลักการบวกดังต่อไปนี้

หลักการคูณ

พิจารณาตัวอย่างต่อไปนี้

ตัวอย่าง 5.1 คนกลุ่มหนึ่งประกอบด้วยชาย 3 คน และหญิง 4 คน จงหาจำนวนวิธีที่จะเลือกตัวแทน 2 คน โดยที่เป็นชาย 1 คน และเป็นหญิง 1 คน

วิธีทำ สมมติชาย 3 คน คือ ช1, ช2, ช3
และหญิง 4 คน คือ ญ1, ญ2, ญ3, ญ4
จะเห็นว่ามีวิธีเลือกตัวแทนทั้งหมด 12 วิธี คือ

(ช1, ญ1), (ช1, ญ2), (ช1, ญ3), (ช1, ญ4),
(ช2, ญ1), (ช2, ญ2), (ช2, ญ3), (ช2, ญ4),
(ช3, ญ1), (ช3, ญ2), (ช3, ญ3), (ช3, ญ4) □

ข้อสังเกต ในการเลือกตัวแทน 2 คน โดยที่เป็นชาย 1 คน และเป็นหญิง 1 คน อาจคิดแบบผลคูณคาร์ทีเซียนของเซตสองเซตดังนี้

ให้ A = {ช1, ช2, ช3}
และ B = {ญ1, ญ2, ญ3, ญ4}
จะได้ $A \times B$ = {(ช1, ญ1), (ช1, ญ2), (ช1, ญ3), (ช1, ญ4),
(ช2, ญ1), (ช2, ญ2), (ช2, ญ3), (ช2, ญ4),
(ช3, ญ1), (ช3, ญ2), (ช3, ญ3), (ช3, ญ4)}

จำนวนวิธีในการเลือกตัวแทน 2 คนที่เป็นชาย 1 คน และหญิง 1 คน ก็คือจำนวนสมาชิกของ $A \times B$ ซึ่งเท่า $4 \cdot 3 = 12$ วิธี

หรืออาจคิดได้อีกวิธีหนึ่งดังนี้
มีวิธีเลือกชาย 1 คน ได้ 3 วิธี และในแต่ละวิธีเลือกหญิง 1 คน ได้อีก 4 วิธี
ดังนั้นจำนวนวิธีเลือกตัวแทนทั้งหมดเท่ากับ $4 \cdot 3 = 12$ วิธี

จากตัวอย่าง 5.1 เราสามารถสรุปหลักการคูณได้ดังนี้

กฎข้อ 1 ถ้าการทำงานอย่างหนึ่งประกอบด้วยการทำงาน 2 ชนิด โดยที่งานชนิดที่หนึ่งทำได้ n_1 วิธี และแต่ละวิธีในการทำงานชนิดที่หนึ่งมีวิธีทำงานงานชนิดที่สองได้ n_2 วิธี ดังนั้นจำนวนวิธีทั้งหมดของการทำงานนี้เท่ากับ $n_1 n_2$ วิธี

ตัวอย่าง 5.2 เรือโดยสารจากท่าช้างไปจังหวัดนนทบุรีมีทั้งหมด 20 ลำ จำนวนวิธีที่ชายคนหนึ่งจะเดินทางโดยเรือจากท่าช้างไปจังหวัดนนทบุรี และเดินทางกลับจากจังหวัดนนทบุรีมาที่ท่าช้างโดยที่ขากลับนั่งเรือคนละลำกับขาไป มีกี่วิธี

วิธีทำ เพราะว่าจำนวนวิธีที่จะเดินทางจากท่าช้างไปยังจังหวัดนนทบุรีเท่ากับ 20 วิธี
และจำนวนวิธีที่จะเดินทางจากจังหวัดนนทบุรีมายังท่าช้างเท่ากับ 19 วิธี
ดังนั้น จำนวนวิธีทั้งหมดที่จะเดินทางไปและกลับ เท่ากับ $20 \times 19 = 380$ วิธี □

ตัวอย่าง 5.3 จงหาจำนวนวิธีในการโยนเหรียญ 1 เหรียญ พร้อมกับทอดลูกเต๋า 1 ลูก

วิธีทำ ผลจากการโยนเหรียญ 1 เหรียญมี 2 วิธีคือ เกิดหน้า หัว ก้อย
ผลจากการทอดลูกเต๋า 1 ลูก มี 6 วิธี คือ เกิดแต้ม 1, 2, 3, 4, 5, 6
ดังนั้น จำนวนวิธีทั้งหมดเท่ากับ $2 \times 6 = 12$ วิธี □

ข้อสังเกต ในการโยนเหรียญ 1 เหรียญ และทอดลูกเต๋า 1 ลูก เป็นการกระทำที่เกิดขึ้นต่อเนื่องกันซึ่งจะทำอย่างใดก่อนหรือหลังจะมีจำนวนผลลัพท์ทั้งหมดเท่ากัน

อาศัยแนวคิดเช่นเดียวกับข้างต้นขยายไปสู่การนับจำนวนวิธีทั้งหมดของการทำงานที่ประกอบด้วยการทำงาน k อย่าง ได้ดังต่อไปนี้

กฎข้อ 2 ถ้างานอย่างแรกมีวิธีทำได้ n_1 วิธี
ในแต่ละวิธีที่เลือกทำงานอย่างแรกมีวิธีทำงานอย่างที่สองได้ n_2 วิธี
ในแต่ละวิธีที่เลือกทำงานอย่างที่สองมีวิธีทำงานอย่างที่สามได้ n_3 วิธี
⋮
ในแต่ละวิธีที่เลือกทำงานอย่างที่ $(k-1)$ มีวิธีทำงานอย่างที่ k ได้ n_k วิธี
ดังนั้น จำนวนวิธีทั้งหมดที่จะเลือกทำงาน k อย่างเท่ากับ $n_1 n_2 n_3 \cdots n_k$ วิธี

ตัวอย่าง 5.4 สถานีรถไฟแห่งหนึ่งมีชานชลาจอดรถไฟได้ทั้งหมด 7 ชานชลา ถ้ามีรถไฟเข้าจอด 4 ขบวน จะมีวิธีจัดรถไฟให้เข้าจอดในชานชลาได้กี่วิธี

วิธีทำ รถไฟขบวนที่ 1 เลือกจอดได้ 7 วิธี
รถไฟขบวนที่ 2 เลือกจอดได้ 6 วิธี
(เพราะรถไฟขบวนที่ 1 จอดไปแล้ว 1 ชานชลาจึงเหลือเพียง 6 ชานชลา)
รถไฟขบวนที่ 3 เลือกจอดได้ 5 วิธี
(เพราะรถไฟขบวนที่ 1 และ 2 จอดไปแล้ว 2 ชานชลาจึงเหลือเพียง 5 ชานชลา)
รถไฟขบวนที่ 4 เลือกจอดได้ 4 วิธี
(เพราะรถไฟขบวนที่ 1 – 3 เลือกจอดไปแล้ว 3 ชานชลาจึงเหลือเพียง 4 ชานชลา)
ดังนั้น รถไฟทั้ง 4 ขบวนจะเข้าจอดได้ $7 \times 6 \times 5 \times 4 = 840$ วิธี □

ตัวอย่าง 5.5 จำนวนเต็มคี่บวกสามหลักมีกี่จำนวนโดยที่แต่ละหลักมีตัวเลขไม่ซ้ำกัน

วิธีทำ ตัวเลขในหลักทั้งสามต่างก็เป็นสมาชิกของเซต $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

หลักร้อย หลักสิบ หลักหน่วย

ตัวเลขในหลักหน่วยเลือกได้ 5 วิธี (คือ $1, 3, 5, 7, 9$)
ตัวเลขในหลักร้อยเลือกได้ 8 วิธี (ต้องไม่ใช่ 0 และไม่ซ้ำกับตัวเลขในหลักหน่วย)
ตัวเลขในหลักสิบเลือกได้ 8 วิธี (ต้องไม่ใช่ 0 และไม่ซ้ำกับตัวเลขในหลักหน่วยและหลักร้อย)
ดังนั้น จำนวนเต็มคี่บวกสามหลักที่ต้องการมีทั้งสิ้น $5 \times 8 \times 8 = 320$ วิธี □

หลักการบวก

พิจารณาตัวอย่างต่อไปนี้

ตัวอย่าง 5.6 โรงเรียนแห่งหนึ่งมีครูคณิตศาสตร์ชาย 3 คนและหญิง 4 คน โดยในจำนวนนี้มีครูสองคนเป็นสามีภรรยากัน ซึ่งจะไปประชุมที่ต่างจังหวัดพร้อมกันเท่านั้น โรงเรียนแห่งนี้จะส่งครู 2 คน ที่เป็นชายหนึ่งคนและหญิงหนึ่งคนไปประชุมที่ต่างจังหวัดได้กี่วิธี

วิธีทำ การที่ครูสองคนจะไปประชุมที่ต่างจังหวัดแบ่งเป็น 2 วิธี คือ
วิธีที่ 1 ครูสองคนที่**เป็น**สามีภรรยากันไปประชุมได้ 1 วิธี
วิธีที่ 2 ครูสองคนที่**ไม่เป็น**สามีภรรยากันไปประชุมได้ 6 วิธี
ดังนั้น จำนวนวิธีส่งครูไปประชุมที่ต่างจังหวัด เท่ากับ $1 + 6 = 7$ วิธี □

กฎข้อ 3 ถ้าการทำงานอย่างหนึ่งประกอบด้วยวิธีทำงาน 2 วิธี แต่ละวิธีของการทำงานไม่เกิดซ้ำซ้อนกัน งานอย่างแรกทำได้ n_1 วิธี และงานอย่างที่สองทำได้ n_2 วิธี จำนวนวิธีที่จะทำงานนี้เท่ากับ $n_1 + n_2$ วิธี

ตัวอย่าง 5.7 จำนวนเต็มบวกสามหลักมีกี่จำนวนที่หารด้วย 5 ลงตัว และแต่ละหลักมีตัวเลขไม่ซ้ำกัน

วิธีทำ จำนวนเต็มบวกที่หารด้วย 5 ลงตัว แบ่งเป็นจำนวนเต็มที่ลงท้ายด้วย 0 และจำนวนเต็มที่ลงท้ายด้วย 5
วิธีที่ 1 ตัวเลขในหลักหน่วยเป็น 0 มี 1 วิธี
ตัวเลขในหลักร้อยเลือกได้ 9 วิธี (คือ $1, 2, 3, 4, 5, 6, 7, 8, 9$)
ตัวเลขในหลักสิบเลือกได้ 8 วิธี (ไม่ซ้ำกับหลักหน่วยและหลักร้อย)
ดังนั้น จำนวนเต็มบวกสามหลักที่ลงท้ายด้วย 0 มี $1 \times 9 \times 8 = 72$ วิธี
วิธีที่ 2 ตัวเลขในหลักหน่วยเป็น 5 มี 1 วิธี
ตัวเลขในหลักร้อยเลือกได้ 8 วิธี (ไม่ใช่เลข 0 และเลข 5)
ตัวเลขในหลักสิบเลือกได้ 8 วิธี (ไม่ซ้ำกับหลักหน่วยและหลักร้อย)

ดังนั้น จำนวนเต็มบวกสามหลักที่ลงท้ายด้วย 0 มี $1 \times 8 \times 8 = 64$ วิธี
เพราะฉะนั้น จำนวนเต็มสามหลักที่ต้องการมีทั้งหมด $72 + 64 = 136$ จำนวน □

จากตัวอย่างข้างต้น สรุปหลักการบวกในรูปทั่วไปดังนี้

กฎข้อ 4 ถ้าการทำงานอย่างหนึ่งประกอบด้วยวิธีทำงาน k วิธี แต่ละวิธีของการทำงานไม่เกิดซ้ำซ้อนกัน
วิธีที่ 1 มีวิธีการทำงาน n_1 วิธี
วิธีที่ 2 มีวิธีการทำงาน n_2 วิธี
$\vdots$
วิธีที่ k มีวิธีการทำงาน n_k วิธี
ดังนั้น จำนวนวิธีที่จะทำงานนี้เท่ากับ $n_1 + n_2 + \cdots + n_k$ วิธี

ตัวอย่าง 5.8 นายสง่ามีเพื่อน 4 คน ซึ่งเขาอาจจะเชิญเพื่อนมาทานอาหารด้วยกันหนึ่งคนหรือหลายคนก็ได้ เขามีวิธีเชิญเพื่อนทั้งหมดกี่วิธี

วิธีทำ วิธีที่ 1 เขาเชิญเพื่อนหนึ่งคน มี 4 วิธี
วิธีที่ 2 เขาเชิญเพื่อนสองคน มี 6 วิธี
วิธีที่ 3 เขาเชิญเพื่อนสามคน มี 4 วิธี
วิธีที่ 4 เขาเชิญเพื่อนสี่คน มี 1 วิธี
ดังนั้น จำนวนวิธีทั้งหมดที่นายสง่าจะเชิญเพื่อนเท่ากับ $4 + 6 + 4 + 1 = 15$ วิธี □

วิธีเรียงสับเปลี่ยน

บางครั้งเราต้องการทราบจำนวนวิธีที่เป็นไปได้ทั้งหมดของการจัดเรียงอันดับของสิ่งของ ดังตัวอย่างในการนำอักษร 3 ตัวคือ A, B และ C มาจัดเรียงใหม่ได้จำนวนวิธีการเรียงสับเปลี่ยนทั้งหมด 6 วิธีดังนี้

ABC BAC CAB
ACB BAC CBA

การจัดเรียงข้างต้นมีแนวคิดดังนี้
ตำแหน่งที่ 1 จะเป็นอักษร A, B หรือ C ก็ได้มีวิธีจัดได้ 3 วิธี
ตำแหน่งที่ 2 เหลืออักษรที่จะนำมาจัดเรียงเพียง 2 ตัวจึงจัดได้ 2 วิธี
ตำแหน่งที่ 3 เหลืออักษรเพียง 1 ตัวจึงจัดได้ 1 วิธี
ดังนั้น จำนวนวิธีทั้งหมดเท่ากับ $3 \times 2 \times 1 = 6$ วิธี
การจัดเรียงอันดับของตัวอักษร เช่นนี้เรียกว่า **วิธีเรียงสับเปลี่ยน**

แฟคทอเรียล

กำหนดให้ n เป็นจำนวนเต็มบวก **แฟคทอเรียล** n เขียนแทนด้วย $n!$ โดยที่

$$\begin{aligned} n! &= 1\cdot 2\cdot 3\cdots(n-1)\cdot n \\ &= n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 \end{aligned}$$

ข้อสังเกต 1. กำหนดให้ $0! = 1$ ดังนั้น สำหรับจำนวนเต็มบวก n,

$$n! = n(n-1)!$$

เช่น

$$\begin{aligned} 1! &= 1\cdot 0! &&= 1 \\ 2! &= 2\cdot 1! &&= 2 \\ 3! &= 3\cdot 2! &&= 6 \\ 4! &= 4\cdot 3! &&= 24 \\ 5! &= 5\cdot 4! &&= 120 \end{aligned}$$

2. ถ้า r เป็นจำนวนเต็มบวกซึ่ง $1 \leq r \leq n$ แล้ว

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

วิธีเรียงสับเปลี่ยนเป็นวิธีการเรียงอันดับของสิ่งของจำนวนจำกัดโดยถือเอาอันดับเป็นสำคัญ แบ่งเป็น 2 แบบ คือ วิธีเรียงสับเปลี่ยนเชิงเส้น และวิธีเรียงสับเปลี่ยนเชิงวงกลม

วิธีเรียงสับเปลี่ยนเชิงเส้น

เป็นการเรียงสับเปลี่ยนในแนวเส้นตรงหรือเส้นโค้งโดยที่ปลายทั้งสองข้างไม่บรรจบกัน

ก. วิธีเรียงสับเปลี่ยนเชิงเส้นของสิ่งที่แตกต่างกันทั้งหมด

ถ้ามีสิ่งของ n สิ่งแตกต่างกันทั้งหมด และต้องการนำมาเรียงสับเปลี่ยนในแนวเส้นตรงทั้ง n สิ่ง จำนวนวิธีเรียงสับเปลี่ยน หาได้ดังนี้

ตำแหน่งที่ 1	ตำแหน่งที่ 2	ตำแหน่งที่ 3		ตำแหน่งที่ n
			…	

ตำแหน่งที่ 1 จะวางของสิ่งใดใน n สิ่งก็ได้ มีวิธีจัดวางได้ n วิธี

ตำแหน่งที่ 2 สำหรับแต่ละวิธีที่วางของในตำแหน่งที่ 1 มีวิธีวางของในตำแหน่งที่ 2 ได้ $(n-1)$ วิธี

ตำแหน่งที่ 3 สำหรับแต่ละวิธีวางของในตำแหน่งที่ 1 และตำแหน่งที่ 2 จะมีวิธีวางของในตำแหน่งที่ 3 ได้ $(n-2)$ วิธี

$\vdots$

ตำแหน่งที่ n เหลือของอยู่สิ่งเดียวจึงมีวิธีวางของได้ 1 วิธี

ดังนั้น จำนวนวิธีเรียงสับเปลี่ยนสิ่งของทั้ง n สิ่งเท่ากับ $n(n-1)(n-2)\cdots 2\cdot 1 = n!$ วิธี

ตัวอย่าง 5.9 นำตัวอักษรจากคำว่า STAND มาจัดเรียงเป็นคำใหม่โดยไม่คำนึงถึงความหมาย ได้ทั้งหมดกี่คำ

วิธีทำ การจัดเรียงตัวอักษรให้ได้คำใหม่เป็นการสลับอักษรโดยถืออันดับเป็นสำคัญ และมีตัวอักษร 5 ตัวต่างกัน
ดังนั้น สร้างคำได้ทั้งหมด $5! = 120$ คำ □

ตัวอย่าง 5.10 จัดคน 7 คนยืนเรียงแถวเพื่อถ่ายรูป จะได้ภาพต่างกันกี่แบบ

วิธีทำ การจัดคน 7 คน ยืนเรียงแถว จะมีวิธีจัดที่ต่างกันทั้งหมด $7! = 5040$ วิธี
ดังนั้น จะได้ภาพที่ต่างกันทั้งหมด 5040 ภาพ □

ในทำนองเดียวกัน ถ้ามีของอยู่ n สิ่งแตกต่างกันทั้งหมด ต้องการนำมาจัดอันดับทีละ r สิ่ง โดยที่ $1 \leq r \leq n$ ตำแหน่งที่จะจัดเรียงจึงมีเพียง r ตำแหน่ง

ตำแหน่งที่ 1 ตำแหน่งที่ 2 ตำแหน่งที่ 3 … ตำแหน่งที่ r

ตำแหน่งที่ 1 มีวิธีวางของได้ n วิธี

ตำแหน่งที่ 2 มีวิธีวางของได้ $n-1$ วิธี

ตำแหน่งที่ 3 มีวิธีวางของได้ $n-2$ วิธี

$\vdots$

ตำแหน่งที่ r มีวิธีวางของได้ $n-(r-1) = n-r+1$ วิธี

ดังนั้น จำนวนวิธีจัดอันดับของ r สิ่งเท่ากับ $n(n-1)\cdots(n-r+1) = \dfrac{n!}{(n-r)!}$ วิธี

กฎข้อ 5 จำนวนวิธีเรียงสับเปลี่ยนของ n สิ่งซึ่งแตกต่างกันทั้งหมดแบบเชิงเส้นโดยจัดทีละ r สิ่ง เขียนแทนด้วย $P_{n,r}$ หาได้จาก

$$P_{n,r} = \frac{n!}{(n-r)!}$$

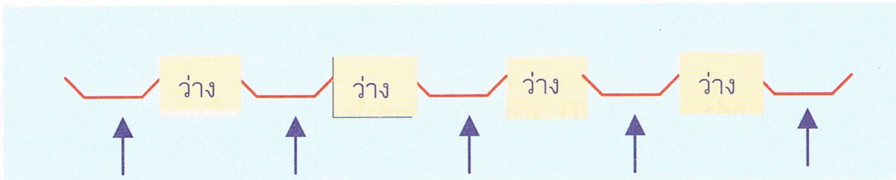
ข้อสังเกต $P_{n,n} = n!$

ตัวอย่าง 5.11 มีเก้าอี้ 7 ตัวเรียงกันเป็นแนวเส้นตรง มีคน 3 คน คือ ใหญ่, กลาง และเล็ก จงหาจำนวนวิธีจัดคนเหล่านี้นั่งเก้าอี้โดยที่

(1) คนทั้งสามนั่งไม่ติดกันเลย

(2) คนทั้งสามนั่งติดกันเสมอ

วิธีทำ (1) เนื่องจากคนทั้งสามไม่นั่งติดกันเลย ดังนั้นวางเก้าอี้ว่าง 4 ตัวก่อน และหลังจากนั้นให้คนทั้งสามนั่งแทรกระหว่างเก้าอี้ว่างดังรูป



มีที่ให้คนทั้งสามนั่งแทรกได้ 5 ที่แต่มีคนเพียง 3 คน

ดังนั้น จำนวนวิธีจัดคน 3 คนนั่งเก้าอี้ได้ $P_{5,3} = 60$ วิธี

(2) เนื่องจากคนทั้งสามต้องนั่งติดกันเสมอ ดังนั้นนับรวมเป็น 1 และนำมาแทรกระหว่างเก้าอี้ว่าง ซึ่งทำได้ $P_{5,1}$ วิธี

คนทั้งสามนั่งสลับกันตามตำแหน่งได้ 3! วิธี

ดังนั้น จำนวนวิธีจัดคน 3 คนนั่งเก้าอี้ได้ $3! \times P_{5,1} = 30$ วิธี □

ตัวอย่าง 5.12 จัดคน 5 คนยืนเรียงแถวถ่ายรูปทีละกี่คนก็ได้ จะได้ภาพกี่แบบ

วิธีทำ จัดคน 1 คน ถ่ายรูปได้ $P_{5,1}$ วิธี

จัดคน 2 คน ถ่ายรูปได้ $P_{5,2}$ วิธี

จัดคน 3 คน ถ่ายรูปได้ $P_{5,3}$ วิธี

จัดคน 4 คน ถ่ายรูปได้ $P_{5,4}$ วิธี

จัดคน 5 คน ถ่ายรูปได้ $P_{5,5}$ วิธี

ดังนั้น จะได้ภาพที่แตกต่างกัน $P_{5,1} + P_{5,2} + P_{5,3} + P_{5,4} + P_{5,5} = 325$ แบบ □

ตัวอย่าง 5.13 มีหนังสือต่างกันทั้งหมด 6 เล่ม ในจำนวนนี้มีหนังสือปกสีแดง 3 เล่ม จงหาจำนวนวิธีจัดหนังสือทั้ง 6 เล่ม บนชั้นโดยที่หนังสือเล่มแรกและเล่มสุดท้ายเป็นหนังสือปกสีแดง

วิธีทำ

หนังสือเล่มแรกและเล่มสุดท้ายเป็นหนังสือปกสีแดง จัดได้ $P_{3,2}$ วิธี

หนังสือตรงกลางมีทั้งหมด 4 เล่ม จัดวางได้ 4! วิธี

ดังนั้น จำนวนวิธีจัดหนังสือ 6 เล่มบนชั้นเท่ากับ $4! \times P_{3,2} = 144$ วิธี □

ข. วิธีเรียงสับเปลี่ยนเชิงเส้นของสิ่งที่ไม่แตกต่างกันทั้งหมด

ถ้ามีสิ่งของ n สิ่งแตกต่างกันทั้งหมด มีจำนวนวิธีจัดเรียงสับเปลี่ยนเชิงเส้นเท่ากับ $n!$ วิธี

สมมติให้ของ n สิ่งมี n_1 สิ่งเหมือนกันเป็นกลุ่มที่ 1 มี n_2 สิ่งเหมือนกันเป็นกลุ่มที่ 2 … และมี n_k สิ่งเหมือนกันเป็นกลุ่มที่ k โดยที่ $n_1 + n_2 + \cdots + n_k = n$ จำนวนวิธีเรียงสับเปลี่ยนจะน้อยลงไปคือในจำนวน $n!$ วิธีจะรวมวิธีเรียงสับเปลี่ยนที่ไม่แตกต่างกัน $n_1!$ วิธี สำหรับสิ่งของเหมือนกันของกลุ่มที่ 1 และ $n_2!$ วิธี สำหรับสิ่งของเหมือนกันของกลุ่มที่ 2 … และ $n_k!$ วิธี สำหรับสิ่งของเหมือนกันของกลุ่มที่ k

ดังนั้น วิธีเรียงสับเปลี่ยนที่สามารถเห็นความแตกต่างได้เท่ากับ

$$\frac{n!}{n_1!n_2!\cdots n_k!} \text{ วิธี}$$

ตัวอย่าง 5.14 มีลูกบอลขนาดเดียวกัน 9 ลูก เป็นสีแดง 5 ลูก และสีดำ 4 ลูก จะเรียงลูกบอลเป็นแนวตรงได้กี่วิธี โดยที่

(1) ลูกบอลที่อยู่หัวแถวและท้ายแถวมีสีเดียวกัน

(2) ลูกบอลที่อยู่หัวแถวและท้ายแถวมีสีต่างกัน

วิธีทำ (1) ลูกบอลที่อยู่หัวแถวและท้ายแถวจะเป็นสีแดงหรือสีดำก็ได้

<u>วิธีที่ 1</u> ถ้าลูกบอลหัวแถวและท้ายแถวเป็นสีแดง จะมีลูกบอลเหลือ 7 ลูก ที่เป็นสีแดง 3 ลูก และสีดำ 4 ลูก

จำนวนวิธีเรียงสับเปลี่ยนเท่ากับ $\frac{7!}{3!4!} = 35$ วิธี

<u>วิธีที่ 2</u> ถ้าลูกบอลหัวแถวและท้ายแถวเป็นสีดำจะมีลูกบอลเหลือ 7 ลูก ที่เป็นสีแดง 5 ลูก และสีดำ 2 ลูก

จำนวนวิธีเรียงสับเปลี่ยนเท่ากับ $\frac{7!}{5!2!} = 21$ วิธี

ดังนั้นจำนวนวิธีเรียงลูกบอลทั้ง 9 ลูกเป็นแนวตรงได้ $35 + 21 = 56$ วิธี

(2) เรียงลูกบอลทั้ง 9 ลูกที่เป็นสีแดง 5 ลูก และสีดำ 4 ลูกในแนวตรง

จำนวนเรียงสับเปลี่ยนเท่ากับ $\frac{9!}{5!4!} = 126$ วิธี

จำนวนวิธีเรียงสับเปลี่ยนโดยที่หัวแถวและท้ายแถวมีสีต่างกัน

= จำนวนวิธีเรียงสับเปลี่ยนทั้งหมด − จำนวนวิธีเรียงสับเปลี่ยนในข้อ (1)

$= 126 - 56 = 70$ วิธี □

ตัวอย่าง 5.15 ชายขี้เมาคนหนึ่งสามารถก้าวไปข้างหน้าหรือข้างหลังก็ได้ ถ้าเขาเดินทั้งหมด 15 ก้าว เขาจะมีวิธีเดินกี่วิธีที่เมื่อเดินครบ 15 ก้าวแล้วเขาอยู่ห่างจากจุดเริ่มต้นไปข้างหน้า 7 ก้าว

วิธีทำ สมมติเขาเดินไปข้างหน้า x ก้าว และเดินไปข้างหลัง y ก้าว

ดังนั้น $x + y = 15$ และ $x - y = 7$

เพราะฉะนั้น $x = 11$ และ $y = 4$

นั่นคือ เขาเดินไปข้างหน้า 11 ก้าว และถอยหลัง 4 ก้าว

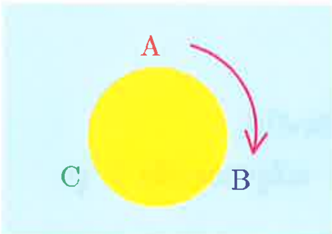
ดังนั้น จำนวนวิธีทั้งหมดที่เขาจะเดินได้เท่ากับ $\dfrac{15!}{11!4!} = 1365$ วิธี $\square$

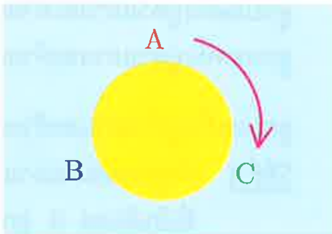
วิธีเรียงสับเปลี่ยนเชิงวงกลม

วิธีเรียงสับเปลี่ยนเชิงวงกลมจะต่างจากวิธีเรียงสับเปลี่ยนเชิงเส้น ทั้งนี้เพราะวิธีเรียงสับเปลี่ยนเชิงวงกลมไม่มีหัวแถวหรือท้ายแถว เช่น สมมติว่าจัดอักษร 3 ตัวคือ A, B และ C เรียงเป็นเชิงเส้นจะจัดได้ทั้งหมด $3! = 6$ วิธี คือ

ABC	BAC	CAB
ACB	BAC	CBA

แต่จัดอักษรทั้ง 3 ตัวเรียงเป็นวงกลมจะมีวิธีจัดเพียง 2 วิธีเท่านั้น ดังรูป





จะเห็นว่าการจัดเรียง ABC, BCA และ CAB ถือเป็นวิธีเดียวกัน และการจัดเรียง ACB, BAC และ CBA ก็ถือเป็นวิธีเดียวกัน ดังนั้น ถ้ากำหนดให้ A อยู่คงที่จะเหลืออักษรอีก 2 ตัว คือ B และ C ที่ต้องเรียงสับเปลี่ยนซึ่งมีวิธีจัดได้ $2!$ หรือ $(3-1)!$ วิธี อาศัยแนวคิดเช่นเดียวกันนี้ สามารถสรุปได้ดังต่อไปนี้

กฎข้อ 6 ถ้ามีของ n สิ่งแตกต่างกัน ทั้งหมดเมื่อนำมาจัดเรียงเป็นวงกลมกำหนดให้ของสิ่งหนึ่งอยู่คงที่ แล้วจัดของที่เหลือ $(n-1)$ สิ่ง เรียงสับเปลี่ยนจะได้จำนวนวิธีเท่ากับ $(n-1)!$ วิธี

ตัวอย่าง 5.16 มีผู้ชาย 3 คน และผู้หญิง 3 คนโดยที่มีชายและหญิงคู่หนึ่งเป็นสามีภรรยากัน จงหาจำนวนวิธีจัดคนทั้ง 6 คนนั่งรอบโต๊ะ เมื่อ

(1) สามีและภรรยานั่งติดกันเสมอ

(2) สามีและภรรยานั่งอยู่ตรงกันข้าม

(3) ไม่มีผู้ชาย 2 คนใดนั่งติดกัน

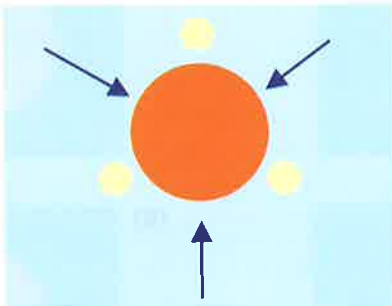
วิธีทำ (1)

สามีภรรยานั่งติดกันจะเหลือคนอีก 4 คน ถูกจัดเรียงสับเปลี่ยนได้ $4!$ วิธี
ขณะเดียวกันสามีภรรยาสลับที่กันได้ $2!$ วิธี
ดังนั้น จำนวนวิธีเรียงสับเปลี่ยนทั้งหมดเท่ากับ $4! \times 2! = 48$ วิธี

(2)

สามีภรรยานั่งอยู่ตรงกันข้ามนับเป็น 1 วิธี เหลือคนอีก 4 คน
ถูกจัดเรียงสับเปลี่ยนได้ $4! = 24$ วิธี

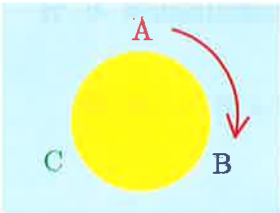
(3) เนื่องจากต้องการให้ผู้ชายทั้ง 3 คน นั่งไม่ติดกัน จึงต้องจัดให้ผู้หญิงทั้งหมดนั่งก่อน
หลังจากนั้นให้ผู้ชายนั่งแทรกระหว่างผู้หญิง ดังรูป

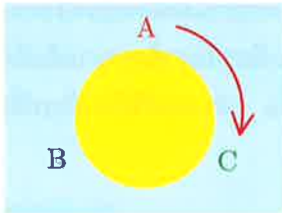


จัดผู้หญิง 3 คน นั่งรอบโต๊ะได้ $2!$ วิธี
จัดผู้ชายแทรกระหว่างผู้หญิงได้ $3!$ วิธี
ดังนั้น จำนวนวิธีจัดคนทั้งหมดนั่งรอบโต๊ะได้ $2! \times 3! = 12$ วิธี □

สังเกตว่าการจัดคนนั่งรอบโต๊ะ หรือการจัดตัวอักษรเป็นวงกลมเป็นการจัดเรียงสับเปลี่ยนที่มองได้ด้านเดียว แต่ก็มีการจัดเรียงสับเปลี่ยนสิ่งของเป็นวงกลมที่สามารถพลิกกลับอีกด้านหนึ่งได้ เช่น การร้อยพวงมาลัย การร้อยลูกปัดหรือพวงกุญแจ เป็นต้น

พิจารณาการเรียงตัวอักษร 3 ตัว A, B และ C เป็นวงกลมถ้ามองด้านเดียวจะมีการจัดเรียงได้ 2 แบบ

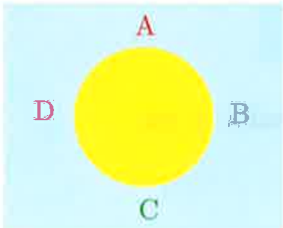




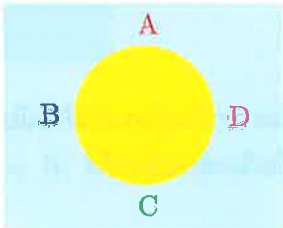
ถ้าพลิกอีกด้านหนึ่งการจัดเรียง ABC จะตรงกับการจัดเรียง ACB ดังนั้นจำนวนวิธีการจัดเรียงอักษรเป็นเพียงแบบเดียวเท่านั้น

ถ้าพิจารณาการเรียงตัวอักษร 4 ตัว A, B, C และ D เป็นวงกลมซึ่งเมื่อมองด้านเดียวจะมีการจัดเรียงได้ $3! = 6$ วิธี ดังรูป

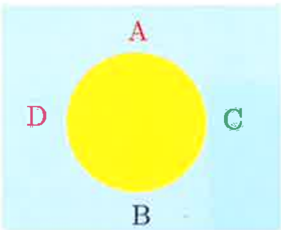
(1)



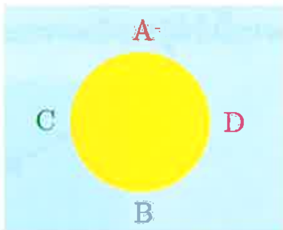
(2)



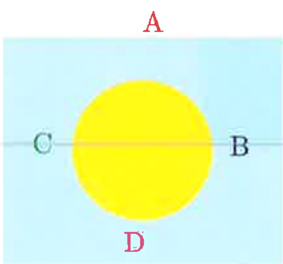
(3)



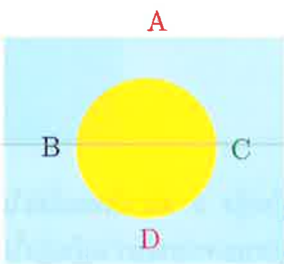
(4)



(5)



(6)



ถ้าพลิกอีกด้านหนึ่งการจัดเรียงแบบที่ (1) จะตรงกับแบบที่ (2) การจัดเรียงแบบที่ (3) จะตรงกับแบบที่ (4) และการจัดเรียงแบบที่ (5) จะตรงกับแบบที่ (6) สังเกตได้ว่าจำนวนวิธีเรียงสับเปลี่ยนเชิงวงกลมในลักษณะมีการพลิกกลับอีกด้านหนึ่ง เป็นครึ่งหนึ่งของจำนวนวิธีเรียงสับเปลี่ยนเชิงวงกลมแบบพลิกไม่ได้ดังนั้น

กฎข้อ 7 ถ้ามีของ n สิ่ง เมื่อ $n > 3$ แตกต่างกันทั้งหมดเมื่อนำมาจัดเรียงเป็นวงกลมในลักษณะมีการพลิกกลับอีกด้านหนึ่งได้ จะได้จำนวนวิธีเท่ากับ $(n-1)!/2$ วิธี

ตัวอย่าง 5.17 นำดอกกุหลาบ ดอกดาวเรือง และดอกไม้อื่น ๆ อีก 6 ชนิดมาร้อยเป็นพวงมาลัย โดยที่ดอกดาวเรืองและดอกกุหลาบอยู่ตรงกันข้ามเสมอ จะได้พวงมาลัยที่แตกต่างกันทั้งหมดกี่แบบ

วิธีทำ จำนวนวิธีจัดดอกกุหลาบและดอกดาวเรืองที่อยู่ตรงกันข้ามมี 1 วิธี ดอกไม้อื่น ๆ จัดเรียงกันได้ 6! วิธี ดังนั้น จำนวนวิธีเรียงสับเปลี่ยนเชิงวงกลมแบบพลิกกลับได้ เท่ากับ $\frac{1}{2} \times 6! \times 1 = 360$ วิธี □

วิธีจัดหมู่

สมมติว่าต้องการเลือกตัวแทนนักเรียน 2 คน จากผู้สมัคร 3 คน ซึ่งเหมือนกันกับการหาจำนวนสับเซตที่มีสมาชิก 2 ตัว ของเซตที่มีสมาชิก 3 ตัว

สมมติว่ามีเซต $A = \{a, b, c\}$ สับเซตของ A ที่มีสมาชิก 2 ตัวมีทั้งหมด 3 สับเซต คือ $\{a, b\}$, $\{a, c\}$ และ $\{b, c\}$ ทำนองเดียวกันในการเลือกตัวแทนนักเรียน 2 คนจากผู้สมัคร 3 คนจะมีวิธีเลือกทั้งหมด 3 วิธี วิธีหาสับเซตหรือวิธีเลือกตัวแทนนักเรียนดังกล่าว เรียกว่า **วิธีจัดหมู่**

สังเกตว่าสับเซตที่มีสมาชิก 2 ตัวของเซต A ข้างต้น อันดับของตัวอักษรในสับเซตไม่มีความสำคัญเพราะว่าเซตสองเซตเท่ากันก็ต่อเมื่อมีสมาชิกชุดเดียวกัน ดังนั้นวิธีจัดหมู่จะไม่คำนึงถึงอันดับของสิ่งของขณะที่การเรียงสับเปลี่ยนจะคำนึงถึงอันดับของสิ่งของ

จำนวนวิธีเรียงสับเปลี่ยนอักษร 2 ตัวจากอักษรทั้งหมด 3 ตัว มี $P_{3,2} = 6$ วิธี

จำนวนวิธีจัดหมู่อักษร 2 ตัว จากอักษรทั้งหมด 3 ตัว มี 3 วิธี

วิธีจัดหมู่ของสิ่งของที่แตกต่างกันทั้งหมด

ก. วิธีเลือกสิ่งของ r สิ่งจากสิ่งของที่ต่างกันทั้งหมด n สิ่ง เมื่อ $0 \le r \le n$

สมมติว่ามีสิ่งของ n สิ่งต่างกัน จะเลือกมาเพียง r สิ่ง เมื่อ $0 \le r \le n$
โดยทั่วไปถ้ามีของ n สิ่งแตกต่างกัน จำนวนวิธีเรียงสับเปลี่ยนสิ่งของคราวละ r สิ่ง เมื่อ $r \le n$ คือ

$$P_{n,r} = \frac{n!}{(n-r)!}$$

ให้ $C_{n,r}$ หรือ $\binom{n}{r}$ แทนจำนวนวิธีที่จะเลือกของ r สิ่งจากของ n สิ่ง

หมายเหตุ $\binom{n}{r}$ อ่านว่า "n เลือก r"

ในการเลือกสิ่งของ r สิ่งจากสิ่งของ n สิ่งไม่สนใจว่าของทั้ง r สิ่งนั้นเรียงกันอยู่อย่างไร จำนวนวิธีทั้งหมดเท่ากับ

$$C_{n,r} = \frac{P_{n,r}}{r!} = \frac{n!}{r!(n-r)!}$$

ข้อสังเกต 1. $\binom{n}{0} = \binom{n}{n} = 1$ และ $\binom{n}{1} = n$

2. $\binom{n}{r} = \binom{n}{n-r}$

3. $\binom{n}{r} = \dfrac{n(n-1)\cdots(n-r+1)}{r!}$

ตัวอย่าง 5.18 สมศรีต้องการเชิญเพื่อนสนิทซึ่งมี 10 คนมารับประทานอาหารด้วยกัน 6 คน ถ้าใน 10 คนนี้มี 2 คน เป็นพี่น้องกันจะเชิญมาต้องเชิญทั้งคู่ สมศรีจะมีวิธีเชิญเพื่อนได้กี่วิธี

วิธีทำ ถ้าสมศรีเชิญ 2 คน พี่น้องมาด้วยจะเชิญเพื่อนคนอื่นได้เพียง 4 คนจาก 8 คน

จำนวนวิธีเชิญเพื่อนเท่ากับ $\binom{8}{4} = 70$ วิธี

แต่ถ้าสมศรีไม่เชิญพี่น้อง 2 คนนั้นมาด้วยจะต้องเชิญเพื่อน 6 คน จาก 8 คน

จำนวนวิธีเชิญเพื่อนเท่ากับ $\binom{8}{6} = 28$ วิธี

ดังนั้น จำนวนวิธีเชิญเพื่อนทั้งหมดเท่ากับ $70 + 28 = 98$ วิธี □

ตัวอย่าง 5.19 กล่องใบหนึ่งบรรจุลูกบอลสีขาว 4 ลูก สีแดง 5 ลูก และสีเขียว 3 ลูก สุ่มหยิบลูกบอลมา 3 ลูก มีกี่วิธีที่จะได้ลูกบอลสีขาวอย่างน้อยหนึ่งลูก

วิธีทำ จำนวนวิธีหยิบลูกบอลสีขาว 1 ลูก และสีอื่น 2 ลูก เท่ากับ $\binom{4}{1}\binom{8}{2} = 112$ วิธี

จำนวนวิธีหยิบลูกบอลสีขาว 2 ลูก และสีอื่น 1 ลูก เท่ากับ $\binom{4}{2}\binom{8}{1} = 48$ วิธี

จำนวนวิธีหยิบลูกบอลสีขาว 3 ลูก เท่ากับ $\binom{4}{3} = 4$ วิธี

ดังนั้น จำนวนวิธีหยิบลูกบอลตามต้องการเท่ากับ $112 + 48 + 4 = 164$ วิธี □

ข้อสังเกต จำนวนวิธีหยิบลูกบอล 3 ลูกให้ได้สีขาวอย่างน้อยหนึ่งลูกเท่ากับ

จำนวนวิธีหยิบลูกบอล 3 ลูกจากกล่อง − จำนวนวิธีหยิบลูกบอล 3 ลูก ได้สีอื่นที่ไม่ใช่สีขาว

ดังนั้น จำนวนวิธีหยิบลูกบอลตามต้องการ $= \binom{12}{3} - \binom{8}{3}$

$= 220 - 56$

$= 164$ วิธี

ข. วิธีแบ่งสิ่งของที่แตกต่างกัน n สิ่งออกเป็น k กลุ่มโดยที่แต่ละกลุ่มมีสิ่งของไม่เท่ากัน

ถ้ามีตัวอักษร 3 ตัว a, b และ c ต้องการแบ่งเป็น 2 กลุ่ม โดยที่กลุ่มแรกมีอักษร 2 ตัว และกลุ่มที่สองมีอักษร 1 ตัว ทำได้ 3 วิธีคือ

{a, b} และ {c}
{a, c} และ {b}
{b, c} และ {a}

แนวคิดในการนับจำนวนวิธีคือเลือกตัวอักษร 2 ตัว เป็นกลุ่มแรกก่อนจะได้ว่าตัวอักษรที่เหลือจะเป็นตัวอักษรในกลุ่มที่สอง จำนวนวิธีการแบ่งกลุ่มเท่ากับ $\binom{3}{2} = 3$ วิธี

ข้อสังเกต ในการแบ่งตัวอักษร 3 ตัวออกเป็นสองกลุ่มอาจสลับเป็นเลือกตัวอักษร 1 ตัว เป็นกลุ่มแรกและตัวอักษรที่เหลือเป็นกลุ่มที่สอง

จำนวนวิธีการแบ่งกลุ่มเท่ากับ $\binom{3}{1} = 3$ วิธี

ถ้ามีสิ่งของแตกต่างกัน n สิ่ง ต้องการแบ่งเป็น 2 กลุ่ม ๆ ละ n_1 และ n_2 ตามลำดับ โดยที่ $n_1 \neq n_2$ และ $n_1 + n_2 = n$

จำนวนวิธีแบ่งกลุ่มเท่ากับ $\binom{n}{n_1} = \dfrac{n!}{n_1!(n-n_1)!} = \dfrac{n!}{n_1!n_2!}$ วิธี

ถ้ามีสิ่งของแตกต่างกัน n สิ่งต้องการแบ่งเป็น 3 กลุ่ม ๆ ละ n_1 และ n_2 ตามลำดับ โดยที่ $n_1 \neq n_2 \neq n_3$ และ $n_1 + n_2 + n_3 = n$

$$\text{จำนวนวิธีแบ่งกลุ่มเท่ากับ} \quad \binom{n}{n_1}\binom{n-n_1}{n_2} = \frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} = \frac{n!}{n_1!n_2!n_3!} \text{ วิธี}$$

ตัวอย่าง 5.20 จะแบ่งนักเรียน 12 คน ออกเป็นสองกลุ่ม ๆ ละ 5 คน และ 7 คน ได้กี่วิธี

วิธีทำ จำนวนวิธีแบ่งนักเรียนเท่ากับ $\dfrac{12!}{5!7!} = 792$ วิธี □

ตัวอย่าง 5.21 จะแบ่งคน 10 คน เข้าพักในห้อง 3 ห้อง โดยที่แต่ละห้องพักได้ 2 คน, 3 คน และ 5 คน ตามลำดับ

วิธีทำ จำนวนวิธีแบ่งคนเท่ากับ $\dfrac{10!}{2!3!5!} = 2520$ วิธี □

อาศัยแนวคิดข้างต้นขยายไปสู่กรณีทั่วไปได้ดังนี้

กฎข้อ 8 แบ่งสิ่งของแตกต่างกัน n สิ่งออกเป็น k กลุ่ม ๆ ละ $n_1, n_2, \ldots, n_k$ โดยที่ $n_1 \neq n_2 \neq \ldots = n_k$ และ $n_1 + n_2 + \cdots + n_k = n$

จำนวนวิธีการแบ่งกลุ่มเท่ากับ $\dfrac{n!}{n_1!n_2!\cdots n_k!}$ วิธี

ค. วิธีแบ่งสิ่งของแตกต่างกัน n สิ่งออกเป็น k กลุ่มโดยที่แต่ละกลุ่มมีจำนวนสิ่งของเท่ากัน

ถ้ามีตัวอักษร 4 ตัว a, b, c และ d ต้องการแบ่งเป็น 2 กลุ่ม โดยที่แต่ละกลุ่มมีอักษร 2 ตัว ถ้าเลือกตัวอักษร 2 ตัว เป็นกลุ่มแรกจะเหลือตัวอักษรอีก 2 ตัวเป็นกลุ่มที่สอง จะมีจำนวนวิธีเท่ากับ $\binom{4}{2} = 6$ วิธี ดังนี้

กลุ่มที่ 1	กลุ่มที่ 2
$\{a, b\}$	$\{c, d\}$
$\{a, c\}$	$\{b, d\}$
$\{a, d\}$	$\{b, c\}$
$\{b, c\}$	$\{a, d\}$
$\{b, d\}$	$\{a, c\}$
$\{c, d\}$	$\{a, b\}$

สังเกตว่ากลุ่มของตัวอักษรในกลุ่มที่ 1 และกลุ่มที่ 2 แต่ละชุดจะสลับกัน 2! วิธี (สลับที่ระหว่างกลุ่ม 2 กลุ่ม) ทำให้มีวิธีแบ่งกลุ่มซ้ำกันอยู่ 2! วิธี

ดังนั้น จำนวนวิธีแบ่งกลุ่มเท่ากับ $\dfrac{4!}{(2!)^2 2!} = \dfrac{6}{2!} = 3$ วิธี

ในทำนองเดียวกันแบ่งสิ่งของ n สิ่งออกเป็น k กลุ่ม ๆ ละ r สิ่งเท่า ๆ กัน

จำนวนวิธีการแบ่งกลุ่มเท่ากับ $\dfrac{n!}{(r!)^k k!}$ วิธี

ตัวอย่าง 5.19 จงหาจำนวนวิธีแบ่งดินสอสี 12 แท่งออกเป็น 3 กอง ๆ ละเท่า ๆ กัน

วิธีทำ แบ่งดินสอสี 12 แท่งเป็น 3 กอง จะต้องแบ่งกองละ 4 แท่ง

จำนวนวิธีแบ่งดินสอสีเท่ากับ $\dfrac{12!}{(4!)^3 3!} = 5775$ วิธี □

ตัวอย่าง 5.20 จงหาจำนวนวิธีจัดคน 6 คน ถ่ายรูปเป็น 2 แถว ๆ ละ 3 คน โดยที่คนที่อยู่แนวหน้านั่งเก้าอี้และคนที่อยู่แถวหลังยืนเรียงแถว

วิธีทำ แบ่งคน 6 คน เป็นสองกลุ่ม ๆ ละ 3 คน

จำนวนวิธีแบ่งกลุ่มเท่ากับ $\dfrac{6!}{(3!)^2 2!}$ วิธี

จัดคน 3 คนนั่งเรียงแถวได้ 3! วิธี

ดังนั้น จำนวนวิธีจัดคนถ่ายรูปเท่ากับ $\dfrac{6!}{(3!)^2 2!} \times 3! \times 3! \times 2! = 720$ วิธี □

สัมประสิทธิ์ทวินาม

พิจารณาการกระจายของ $(a+b)^n$ เมื่อ n เป็นจำนวนเต็มบวก

$$\begin{aligned}(a+b)^0 &= 1\\ (a+b)^1 &= a+b\\ (a+b)^2 &= a^2+2ab+b^2\\ (a+b)^3 &= a^3+3a^2b+3ab^2+b^3\\ (a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4\end{aligned}$$

การกระจายของ $(a+b)^n$ เมื่อ n เป็นจำนวนเต็มบวกที่ไม่มากนักทำได้โดยการคูณ $(a+b)$ เข้าด้วยกัน n ครั้งเช่น

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)(a+b)\\ &= (a+b)(a^2+2ab+b^2)\\ &= a^3+3a^2b+3ab^2+b^3\end{aligned}$$

แต่ถ้า n เป็นจำนวนที่มีค่ามาก ๆ จะพิจารณาได้จาก

$$(a+b)^n = (a+b)(a+b)(a+b)\cdots(a+b) \qquad (n \text{ วงเล็บ})$$

พจน์ที่ 1 ได้จากการนำ a จากทุกวงเล็บคูณกันได้ a^n

พจน์ที่ 2 ได้จากการนำ b จากหนึ่งวงเล็บคูณกับ a จาก $(n-1)$ วงเล็บที่เหลือ จะได้พจน์ $a^{n-1}b$ ซึ่งเกิดขึ้นได้ $\binom{n}{1}$ วิธี

พจน์ที่ 3 ได้จากการนำ b จากหนึ่งวงเล็บคูณกับ a จาก $(n-2)$ วงเล็บที่เหลือ จะได้พจน์ $a^{n-2}b^2$ ซึ่งเกิดขึ้นได้ $\binom{n}{2}$ วิธี

⋮

พจน์ที่ $n+1$ ได้จากการนำ b จากทุกวงเล็บคูณกัน จะได้ b^n

ดังนั้น

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

ข้อสังเกต 1. จำนวนพจน์จากการกระจาย $(a+b)^n$ มีทั้งหมด $n+1$ พจน์

2. ในการกระจาย $(a+b)^n$ เลขชี้กำลังของ a เริ่มจาก n แล้วลดลงทีละ 1 จนถึง 0

ส่วนเลขชี้กำลังของ b เริ่มจาก 0 เพิ่มขึ้นทีละ 1 จนถึง n

3. ในแต่ละพจน์ของการกระจาย $(a+b)^n$ ผลรวมของเลขชี้กำลังของ a และ b เท่ากับ n เสมอ
4. พจน์ที่ $r+1$ ของการกระจาย $(a+b)^n$ คือ $\binom{n}{r} a^{n-r}b^r$ เมื่อ $0 \leq r \leq n$

ตัวอย่าง 5.21 จงหาพจน์ที่ 4 ของการกระจาย $(x+2y)^{10}$

วิธีทำ พจน์ที่ 4 ของการกระจายคือ $\binom{10}{3} x^7(2y)^3$ □

ตัวอย่าง 5.22 จงหาพจน์ที่ไม่มี x ของการกระจาย $(2x^2+\frac{1}{x})^9$

วิธีทำ พจน์ที่ $r+1$ ของการกระจายคือ $\binom{9}{r}(2x^2)^{9-r}(\frac{1}{x})^r = \binom{9}{r}(2^{9-r})(x^{18-3r})$

ต้องการพจน์ที่มีกำลังของ x เท่ากับศูนย์ ดังนั้น $18-3r = 0$

นั่นคือ $r = 6$

ดังนั้น พจน์ที่ไม่มี x ของการกระจายคือ $\binom{9}{6}(2^{9-6}) = 672$ □

การทดลองสุ่มและแซมเปิลสเปซ

การทดลองสุ่ม หมายถึง การทดลองที่ทราบขอบเขตของผลลัพธ์แต่ไม่สามารถบอกได้อย่างถูกต้องแน่นอนว่าแต่ละครั้งที่ทำการทดลองเกิดผลลัพธ์ใด ตัวอย่างเช่น

1. โยนเหรียญต่างกัน 2 อัน 1 ครั้ง ถือว่าเป็นการทดลองสุ่ม เพราะสามารถบอกได้ว่าผลลัพธ์ที่จะเกิดขึ้นคือหน้า (หัว, หัว), (หัว, ก้อย), (ก้อย, หัว) หรือ (ก้อย, ก้อย)

2. การเลือกตัวอักษร 2 ตัว จากตัวอักษร 4 ตัว A B C และ D ก็เป็นการทดลองสุ่มเพราะสามารถบอกได้ว่าจะได้ตัวอักษร AB, AC, AD, BC, BD หรือ CD

แซมเปิลสเปซ คือเซตของผลลัพธ์ที่เป็นไปได้ทั้งหมดของการทดลองสุ่ม ตัวอย่างเช่น

1. โยนเหรียญต่างกัน 2 อัน 1 ครั้ง ให้ H แทนหน้าหัว และ T แทนหน้าก้อย จะได้
   แซมเปิลสเปซ $S = \{\text{HH, HT, TH, TT}\}$
2. การเลือกตัวอักษร 2 ตัว จากตัวอักษร 4 ตัว A B C และ D
   แซมเปิลสเปซ $S = \{\text{AB, AC, AD, BC, BD, CD}\}$

เหตุการณ์ คือ สับเซตของแซมเปิลสเปซ

ถ้าแซมเปิลสเปซของการทดลองสุ่มมีสมาชิก N ตัว จะได้ว่า จำนวนเหตุการณ์จะมีทั้งหมด 2^N เหตุการณ์ และจะเห็นว่าแซมเปิลสเปซ และ $\varnothing$ ต่างก็เป็นเหตุการณ์ด้วย

ตัวอย่าง 5.23 สุ่มครอบครัวที่มีบุตรสามคนมาครอบครัวหนึ่ง จงเขียนแซมเปิลสเปซ และเหตุการณ์ที่ครอบครัวนั้นมีบุตรชาย 2 คน

วิธีทำ ให้ ช แทนบุตรชาย

ญ แทนบุตรหญิง

จะได้ S = {ชชช, ชชญ, ชญช, ชญญ, ญชช, ญชญ, ญญช, ญญญ}

E = {ชชญ, ชญช, ญชช} □

ยูเนียนของเหตุการณ์

ถ้า E_1 และ E_2 เป็นเหตุการณ์สองเหตุการณ์

$E_1 \cup E_2$ คือ เหตุการณ์ที่ประกอบด้วยสมาชิกของเหตุการณ์ E_1 หรือเหตุการณ์ E_2 หรือทั้งสองเหตุการณ์

ตัวอย่าง 5.24 ในการทอดลูกเต๋า 1 ลูก 1 ครั้ง ถ้า E_1 เป็นเหตุการณ์ที่ลูกเต๋าขึ้นแต้มคี่ และ E_2 เป็นเหตุการณ์ที่ลูกเต๋าขึ้นแต้มที่เป็นจำนวนเฉพาะ จงหา $E_1 \cup E_2$

วิธีทำ แซมเปิลสเปซคือเซตของแต้มบนลูกเต๋า ดังนั้น

$$S = \{1, 2, 3, 4, 5, 6\}$$
$$E_1 = \{1, 3, 5\}$$
$$E_2 = \{2, 3, 5\}$$

ดังนั้น $E_1 \cup E_2 = \{1, 2, 3, 5\}$ ซึ่งคือเหตุการณ์ที่ได้แต้มลูกเต๋าเป็นเลขคี่ หรือ เป็นจำนวนเฉพาะ □

อินเตอร์เซกชันของเหตุการณ์

ถ้า E_1 และ E_2 เป็นเหตุการณ์สองเหตุการณ์

$E_1 \cap E_2$ คือ เหตุการณ์ที่ประกอบด้วยสมาชิกของเหตุการณ์ E_1 และเหตุการณ์ E_2

ตัวอย่าง 5.25 จงหา $E_1 \cap E_2$ จากตัวอย่าง 5.24

วิธีทำ $E_1 \cap E_2 = \{3, 5\}$ ซึ่งคือเหตุการณ์ที่ได้แต้มลูกเต๋าเป็นเลขคี่ และ เป็นจำนวนเฉพาะ □

เหตุการณ์ที่ไม่เกิดร่วมกัน

จะเรียกเหตุการณ์ E_1 และ E_2 ว่า **เหตุการณ์ที่ไม่เกิดร่วมกัน** ถ้า E_1 และ E_2 เป็นเหตุการณ์สองเหตุการณ์ที่ $E_1 \cap E_2 = \varnothing$

ตัวอย่าง 5.26 ให้ E_1 เป็นเหตุการณ์ที่ได้แต้มเป็นจำนวนคี่ ในการทอดลูกเต๋า 1 ลูก 1 ครั้ง และ E_2 เป็นเหตุการณ์ที่ได้แต้มมากกว่า 5 จงแสดงว่า E_1 และ E_2 ว่าเหตุการณ์ที่ไม่เกิดร่วมกัน

วิธีทำ เพราะว่า $E_1 = \{1, 3, 5\}$ และ $E_2 = \{6\}$ จะได้ว่า $E_1 \cap E_2 = \varnothing$
ดังนั้น E_1 และ E_2 ว่าเหตุการณ์ที่ไม่เกิดร่วมกัน □

คอมพลีเมนต์ของเหตุการณ์

ให้ S เป็นแซมเปิลสเปซ และ E เป็นเหตุการณ์

คอมพลีเมนต์ของเหตุการณ์ E เขียนแทนด้วย E' คือเหตุการณ์ที่ประกอบด้วยสมาชิกที่อยู่ในแซมเปิลสเปซ S แต่ไม่อยู่ในเหตุการณ์ E

ตัวอย่าง 5.27 ในการหยิบไพ่หนึ่งใบจากสำรับ ให้ E เป็นเหตุการณ์ที่ได้โพดำหรือโพแดง ดังนั้น

S = {โพดำ, โพแดง, ดอกจิก, ข้าวหลามตัด}

E = {โพดำ, โพแดง}

E' = {ดอกจิก, ข้าวหลามตัด} □

ความน่าจะเป็น

ถ้าในแซมเปิลสเปซ S มีสมาชิก N ตัวโดยที่สมาชิกแต่ละตัวมีโอกาสเกิดขึ้นได้เท่าๆ กัน และเหตุการณ์ E เป็นสับเซตของ S มีสมาชิก n ตัว **ความน่าจะเป็น**ที่จะเกิดเหตุการณ์ E เขียนแทนด้วย $P(E)$ โดยที่

$$P(E) = \frac{\text{จำนวนสมาชิกของเหตุการณ์ } E}{\text{จำนวนสมาชิกของแซมเปิลสเปซ } S} = \frac{n}{N}$$

ข้อสังเกต 1. ถ้า $P(E) = 0$ หมายความว่าเหตุการณ์ E ไม่มีโอกาสเกิดขึ้นเลย

2. ถ้า $P(E) = 1$ หมายความว่าเหตุการณ์ E จะเกิดขึ้นอย่างแน่นอน

สมบัติที่สำคัญของความน่าจะเป็น

1. ความน่าจะเป็นของเหตุการณ์ E ใดๆ จะมีค่าตั้งแต่ 0 ถึง 1
   นั่นคือ $0 \leq P(E) \leq 1$
2. $P(S) = 1$ และ $P(\varnothing) = 0$
3. ถ้า E_1 และ E_2 เป็นเหตุการณ์สองเหตุการณ์ จะได้
   $$P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)$$
4. ถ้า E_1 และ E_2 เป็นเหตุการณ์ที่ไม่เกิดร่วมกัน จะได้
   $$P(E_1 \cup E_2) = P(E_1) + P(E_2)$$
5. ถ้า E เป็นเหตุการณ์ใด ๆ จะได้
   $$P(E) + P(E') = 1$$

ตัวอย่าง 5.28 กล่องใบหนึ่งบรรจุหลอดไฟ 15 หลอด มีหลอดเสียอยู่ 5 หลอด สุ่มหยิบหลอดไฟมา 3 หลอด จากกล่องใบนี้ จงหาความน่าจะเป็นต่อไปนี้

(1) ได้หลอดไฟดีทั้งหมด

(2) ได้หลอดไฟเสีย 1 หลอด

(3) ได้หลอดไฟเสียอย่างน้อยหนึ่งหลอด

วิธีทำ จำนวนสมาชิกของแซมเปิลสเปซเท่ากับจำนวนวิธีหยิบหลอดไฟ 3 หลอดจากหลอดไฟทั้งหมด 15 หลอด

ดังนั้น $$N = \binom{15}{3} = \frac{15\times14\times13}{3!}$$

(1) ให้ E_1 เป็นเหตุการณ์ที่หยิบหลอดไฟได้หลอดดีทั้ง 3 หลอด

ให้ n_1 เป็นจำนวนสมาชิกของ E_1 ที่เท่ากับจำนวนวิธีหยิบหลอดไฟดี 3 หลอด จากหลอดไฟดีทั้งหมด 10 หลอด จะได้

$$n_1 = \binom{10}{3} = \frac{10\times9\times8}{3!}$$

ดังนั้น $$P(E_1) = \frac{n_1}{N} = \frac{10\times9\times8}{3!}\cdot\frac{3!}{15\times14\times13} = \frac{24}{91}$$

(2) ให้ E_2 เป็นเหตุการณ์ที่หยิบได้หลอดไฟเสีย 1 หลอด

ให้ n_2 เป็นจำนวนสมาชิกของ E_2 ที่เท่ากับจำนวนวิธีหยิบหลอดไฟเสีย 1 หลอดและได้หลอดไฟดี 2 หลอด จะได้

$$n_2 = \binom{5}{1}\binom{10}{2} = 5\cdot\frac{10\times9}{2!}$$

ดังนั้น $$P(E_2) = \frac{n_2}{N} = 5\cdot\frac{10\times9}{2!}\cdot\frac{3!}{15\times14\times13} = \frac{45}{91}$$

(3) ให้ E_3 เป็นเหตุการณ์ที่หยิบได้หลอดไฟเสียอย่างน้อย 1 หลอด

จะได้ E_3' เป็นเหตุการณ์ที่หยิบได้หลอดดีทั้งหมด

จาก $P(E_3) + P(E_3') = 1$

จะได้ $P(E_3) = 1 - P(E_3')$

จาก (1) จะได้ $P(E_3') = \dfrac{24}{91}$ ฉะนั้น $P(E_3) = 1 - \dfrac{24}{91} = \dfrac{67}{91}$ □

ตัวอย่าง 5.29 นักเรียนห้องหนึ่งมี 30 คน ประกอบด้วยนักเรียนชาย 10 คน นักเรียนหญิง 20 คน ครึ่งหนึ่งของนักเรียนชายและครึ่งหนึ่งของนักเรียนหญิงได้ระดับคะแนนสูงกว่า 2.5 ความน่าจะเป็นที่สุ่มเลือกนักเรียนมาคนหนึ่งที่เป็นนักเรียนชาย หรือได้ระดับคะแนนสูงกว่า 2.5 เป็นเท่าใด

วิธีทำ จำนวนสมาชิกของแซมเปิลสเปซเท่ากับจำนวนวิธีสุ่มเลือกนักเรียนหนึ่งคนจากนักเรียน 30 คน

ให้ E_1 เป็นเหตุการณ์ที่สุ่มเลือกนักเรียนหนึ่งคนได้นักเรียนชาย

และ E_2 เป็นเหตุการณ์ที่สุ่มเลือกนักเรียนหนึ่งคนได้นักเรียนที่มีระดับคะแนนสูงกว่า 2.5

จะได้ว่า $E_1 \cup E_2$ เป็นเหตุการณ์ที่เลือกนักเรียนมาหนึ่งคนเป็นนักเรียนชายหรือได้ระดับคะแนนสูงกว่า 2.5

และ $E_1 \cap E_2$ เป็นเหตุการณ์ที่เลือกนักเรียนมาหนึ่งคนเป็นนักเรียนชายและได้ระดับคะแนนสูงกว่า 2.5

ให้ n_1, n_2 และ n_3 เป็นจำนวนสมาชิกของ E_1, E_2 และ $E_1 \cap E_2$ ตามลำดับ

ดังนั้น $N = \binom{30}{1} = 30$

$$n_1 = \binom{10}{1} = 15 \quad \text{และ} \quad P(E_1) = \frac{10}{30} = \frac{1}{3}$$

$$n_2 = \binom{15}{1} = 15 \quad \text{และ} \quad P(E_2) = \frac{15}{30} = \frac{1}{2}$$

$$n_3 = \binom{5}{1} = 15 \quad \text{และ} \quad P(E_1 \cap E_2) = \frac{5}{30} = \frac{1}{6}$$

จาก $P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)$

จะได้ $P(E_1 \cup E_2) = \dfrac{1}{3} + \dfrac{1}{2} - \dfrac{1}{6} = \dfrac{2}{3}$ □

ความน่าจะเป็นแบบมีเงื่อนไข

ให้ A และ B เป็นเหตุการณ์โดยที่ $P(B) > 0$

$P(A \mid B)$ แทนความน่าจะเป็นที่จะเกิดเหตุการณ์ A เมื่อเหตุการณ์ B เกิดขึ้นแล้ว

ตัวอย่าง 5.30 ในการทอดลูกเต๋า 1 ลูก ทราบว่าจะเกิดแต้มคี่ จงหาความน่าจะเป็นที่จะได้แต้มน้อยกว่า 4

วิธีทำ ให้ B แทนเหตุการณ์ที่ลูกเต๋าเกิดแต้มคี่

และ A แทนเหตุการณ์ที่ลูกเต๋าเกิดแต้มน้อยกว่า 4

จะได้ $A \cap B$ แทนเหตุการณ์ที่ลูกเต๋าเกิดแต้มคี่และแต้มน้อยกว่า 4

ดังนั้น $B = \{1, 3, 5\}$, $A = \{1, 2, 3\}$ และ $A \cap B = \{1, 3\}$

ฉะนั้น $P(A \mid B) = \dfrac{2}{3}$ □

ตัวอย่าง 5.31 ในการโยนลูกเต๋า 2 ลูก 1 ครั้งแล้วลูกเต๋าขึ้นแต้มเหมือนกัน จงหาความน่าจะเป็นที่จะได้ผลรวมของแต้มเป็น 6

วิธีทำ ให้ B แทนเหตุการณ์ที่ลูกเต๋าขึ้นแต้มเหมือนกัน

และ A แทนเหตุการณ์ที่ลูกเต๋าขึ้นแต้มที่มีผลรวมเป็น 6

จะได้ $A \cap B$ แทนเหตุการณ์ที่ลูกเต๋าขึ้นแต้มเหมือนกันและมีผลรวมของแต้มเป็น 6

ดังนั้น $B = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$,

$A = \{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\}$

และ $A \cap B = \{(3, 3)\}$

ฉะนั้น $P(A \mid B) = \dfrac{1}{6}$ □

ข้อสังเกต ให้ $n(B)$ และ $n(A \cap B)$ แทนจำนวนสมาชิกของเหตุการณ์ B และ $A \cap B$ ตามลำดับ

$$P(A \mid B) = \frac{n(A \cap B)}{n(B)} = \frac{n(A \cap B)}{N} \cdot \frac{N}{n(B)}$$

ดังนั้น
$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}$$

และถ้า $P(B) = 0$ กำหนดให้ $P(A \mid B) = 0$

ตัวอย่าง 5.31 กล่องใบหนึ่งบรรจุลูกบอลสีขาว 3 ลูก และสีดำ 2 ลูก ถ้าหยิบลูกบอล 2 ครั้ง ๆ ละ 1 ลูก โดยที่หยิบครั้งแรกแล้วไม่ใส่คืน จงหาความน่าจะเป็นที่จะหยิบได้ลูกบอลสีดำทั้งสองลูก

วิธีทำ วิธีที่ 1 หยิบครั้งแรกมีวิธีเลือก 5 วิธี หยิบครั้งที่สองมีวิธีเลือก 4 วิธี

ดังนั้นวิธีเลือกทั้งหมดเท่ากับ $5 \times 4 = 20$ วิธี

หยิบลูกบอลสีดำครั้งแรกมี 2 วิธี ครั้งที่สองมี 1 วิธี

ดังนั้นวิธีเลือกทั้งหมดเท่ากับ $2 \times 1 = 2$ วิธี

จะได้ ความน่าจะเป็นที่จะหยิบลูกบอลสีดำทั้งคู่โดยหยิบครั้งแรกแล้วไม่ใส่คืนเท่ากับ $\dfrac{2}{20} = \dfrac{1}{10}$

วิธีที่ 2 ให้ B แทนเหตุการณ์ที่หยิบลูกบอลลูกแรกเป็นสีดำ

และ A แทนเหตุการณ์ที่หยิบลูกบอลลูกที่สองเป็นสีดำ

จะได้ $P(B) = \dfrac{2}{5}$ และ $P(A \mid B) = \dfrac{1}{4}$

จาก $P(A \mid B) = \dfrac{P(A \cap B)}{P(B)}$

ดังนั้น $P(A \cap B) = P(A \mid B) \cdot P(B) = \dfrac{1}{4} \cdot \dfrac{2}{5} = \dfrac{1}{10}$ □

ตัวอย่าง 5.32 ในการทอดลูกเต๋า 1 ลูกสองครั้ง จงหาความน่าจะเป็นที่ครั้งแรกเกิดแต้ม 2, 4 หรือ 6 และครั้งที่สองเกิดแต้ม 1, 2, 3 หรือ 4

วิธีทำ <u>วิธีที่ 1</u> จำนวนวิธีทั้งหมดที่เกิดแต้มจากการทอดลูกเต๋า 1 ลูก สองครั้งเท่ากับ $6 \times 6 = 36$ วิธี

จำนวนวิธีที่ครั้งแรกเกิดแต้ม 2, 4, 6 และครั้งที่สองเกิดแต้ม 1, 2, 3, 4

เท่ากับ $3 \times 4 = 12$ วิธี

ดังนั้น ความน่าจะเป็นที่ครั้งแรกเกิดแต้ม 2, 4, 6 และครั้งที่สองเกิดแต้ม 1, 2, 3, 4

เท่ากับ $\dfrac{12}{36} = \dfrac{1}{3}$

<u>วิธีที่ 2</u> ให้ B แทนเหตุการณ์ที่ทอดลูกเต๋าครั้งแรกเกิดแต้ม 2, 4 หรือ 6

และ A แทนเหตุการณ์ที่ทอดลูกเต๋าครั้งที่สองเกิดแต้ม 1, 2, 3, หรือ 4

จะได้ $P(B) = \dfrac{3}{6}$ และ $P(A \mid B) = P(A) = \dfrac{4}{6}$

ดังนั้น $P(A \cap B) = P(A \mid B) \cdot P(B) = \dfrac{4}{6} \cdot \dfrac{3}{6} = \dfrac{1}{3}$ □

ความน่าจะเป็นของเหตุการณ์ที่เป็นอิสระต่อกัน

จะเรียกเหตุการณ์ A และเหตุการณ์ B **เป็นอิสระต่อกัน** ก็ต่อเมื่อเหตุการณ์ A จะเกิดขึ้นไม่ว่าเหตุการณ์ B จะเกิดขึ้นหรือไม่ก็ตาม และจะได้ว่า

$$P(A \cap B) = P(A) \cdot P(B)$$

ตัวอย่าง 5.33 ในการทอดลูกเต๋าหนึ่งลูก 2 ครั้ง จงหาความน่าจะเป็นที่จะขึ้นแต้ม 3 อย่างน้อยหนึ่งครั้ง

วิธีทำ ให้ A แทนเหตุการณ์ที่ทอดลูกเต๋าครั้งแรกแล้วขึ้นแต้ม 3

และ B แทนเหตุการณ์ที่ทอดลูกเต๋าครั้งที่สองแล้วขึ้นแต้ม 3

จะได้ว่า $A \cap B$ แทนเหตุการณ์ที่ทอดลูกเต๋าครั้งแรกขึ้นแต้ม 3 และครั้งที่สองขึ้นแต้ม 3

และ $A \cup B$ แทนเหตุการณ์ที่ทอดลูกเต๋าหนึ่งลูก 2 ครั้งแล้วครั้งแรกขึ้นแต้ม 3 หรือครั้งที่สองขึ้นแต้ม 3

สังเกตว่า 1. แต้มที่จะเกิดจากการทอดลูกเต๋าทั้งสองครั้งเป็นอิสระต่อกัน

2. เหตุการณ์ที่ลูกเต๋าขึ้นแต้ม 3 อย่างน้อยหนึ่งครั้งจะตรงกับ $A \cup B$

เพราะว่า $P(A) = \dfrac{1}{6}$ และ $P(B) = \dfrac{1}{6}$

และเนื่องจากการทอดลูกเต๋าสองครั้งเป็นอิสระต่อกัน ดังนั้น

$$P(A \cap B) = P(A) \cdot P(B) = \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}$$

เพราะฉะนั้น
$$\begin{aligned} P(A \cup B) &= P(A) + P(B) - P(A \cap B) \\ &= \frac{1}{6} + \frac{1}{6} - \frac{1}{36} = \frac{11}{36} \end{aligned}$$ □

แบบฝึกหัดบทที่ 5

1. จงหาจำนวนวิธีเลือกสับเซต $\{a, b\}$ ของเซต $\{1, 2, 3, \ldots, 50\}$ โดยที่

   1.1 $|a - b| = 5$

   1.2 $|a - b| \leq 5$

2. มีนักเรียน 12 คน ในจำนวนนี้เป็นนักเรียนหญิง 5 คน จงหาจำนวนวิธีที่จะจัดแถวนักเรียนทั้ง 12 คน โดยที่

   2.1 นักเรียนหญิงทั้ง 5 คน ยืนติดกันเสมอ

   2.2 ไม่มีนักเรียนหญิง 2 คน ใดยืนติดกัน

   2.3 ระหว่างนักเรียนชาย 2 คน คือ สมชาย และสมศักดิ์ มีเพียงนักเรียนหญิงยืนอยู่ 3 คน

3. มีกี่วิธีที่จะสร้างคำที่ประกอบด้วยตัวอักษร 5 ตัว โดยไม่คำนึงถึงความหมาย โดยใช้ตัวอักษรจากเซต $\{A, B, C, D, E, F, G, H, I, J\}$ ตัวอักษรในแต่ละคำแตกต่างกันหมด
   ตัวอักษร A, B, C, D, E, F จะอยู่ในตำแหน่งที่ 1, ตำแหน่งที่ 3 หรือตำแหน่งที่ 4 เท่านั้น

4. จำนวนคี่ระหว่าง 3000 ถึง 8000 มีกี่จำนวนโดยที่แต่ละหลักมีตัวเลขต่างกัน

5. จงหาค่าของ $1{\cdot}1! + 2{\cdot}2! + 3{\cdot}3! + \cdots + n{\cdot}n!$ โดยที่ n เป็นจำนวนนับ

6. จงหาค่าของ $\dfrac{1}{(1+1)!} + \dfrac{2}{(2+1)!} + \cdots + \dfrac{n}{(n+1)!}$ โดยที่ n เป็นจำนวนนับ

7. จงหาจำนวนตัวหารที่เป็นจำนวนเต็มบวกของ 1040 และ 2030

8. จงหาจำนวนตัวหารที่เป็นจำนวนเต็มบวกของ n ซึ่งเป็นพหุคูณของ 3

   8.1 $n = 210$

   8.2 $n = 630$

   8.3 $n = 151200$

9. จงหาจำนวนวิธีที่จะเลือกนักเรียน 9 คน จากนักเรียน 15 คนที่ประกอบด้วยนักเรียนชาย 10 คน นักเรียนหญิง 5 คน โดยที่กลุ่มนักเรียนที่เลือกมาจะต้องมีนักเรียนหญิง 3 คน

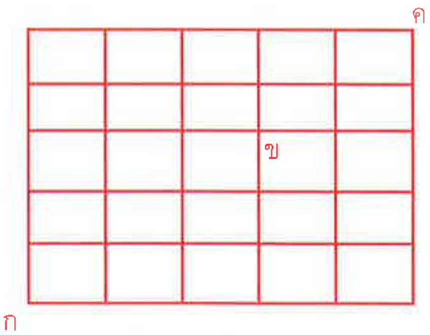
10. มีเก้าอี้ว่าง 10 ตัวจัดเรียงแถว จงหาจำนวนวิธีที่จะจัดเด็กนักเรียน 7 คน นั่งบนเก้าอี้โดยที่เก้าอี้ว่างแต่ละตัวไม่อยู่ติดกัน

11. มีกล่อง 8 กล่องวางเรียงเป็นแถว จงหาจำนวนวิธีที่จะนำลูกบอลต่างกัน 5 ลูก ใส่ลงกล่องโดยที่แต่ละกล่องใส่ลูกบอลได้เพียง 1 ลูกและกล่องว่างอยู่ติดกัน

12. กลุ่มของนักเรียน 20 คน ซึ่งรวมนักเรียนหญิง 3 คน g1, g2, g3 และนักเรียนชาย 4 คน b1, b2, b3, b4 อยู่ด้วย จงหาจำนวนวิธีที่จะจัดนักเรียนเป็น 2 แถวๆ ละ 10 คน โดยที่นักเรียนหญิง g1, g2, g3 อยู่แถวหน้า และนักเรียนชาย b1, b2, b3, b4 อยู่แถวหลัง

13. จงหาจำนวนวิธีที่จะจัดเด็กชาย 7 คน และเด็กหญิง 2 คน ยืนเรียงแถวโดยที่เด็กหญิงทั้ง 2 คน ถูกคั่นด้วยเด็กชาย 3 คน

14. มีนักเรียน 15 คน เป็นนักเรียนหญิง 3 คน จงหาจำนวนวิธีที่จะเลือกนักเรียน 7 คน โดยที่ต้องมีนักเรียนหญิงอย่างน้อย 1 คน และ
    14.1 เลือกมาเพื่อเป็นกรรมการนักเรียน
    14.2 เลือกมาเพื่อจัดเป็นแถว
15. ในการแข่งขันฟุตบอล มีทีมแข่งขัน 10 ทีมใน 10 ทีมนี้จับฉลากประกบคู่กันได้ 5 คู่ เพื่อแข่งขันในรอบแรกซึ่งจะมีขึ้นทุกวันจันทร์-ศุกร์โดยแข่งขันวันละคู่ จงหาจำนวนวิธีจัดการแข่งขัน
16. ระบายสี 6 สีต่างกันบนสี่เหลี่ยมลูกบาศก์หน้าเกลี้ยงหน้าละสีได้กี่วิธี
17. ระบายสี 5 สีต่างกันบนสี่เหลี่ยมลูกบาศก์หน้าเกลี้ยงโดยที่สีเดียวกันไม่อยู่ติดกันได้กี่วิธี
18. ระบายสี 5 สีต่างกันบนลูกเต๋าทุกหน้าหน้าละสีไม่ให้สีเดียวกันอยู่ติดกันได้กี่วิธี
19. นายจรต้องการขับรถจากเมือง ก. ไปยังเมือง ค. ถ้าเส้นที่ขีดเป็นรูปตารางคือเส้นทางเดินรถ และในการเดินทางนายจรจะมุ่งไปสองทิศคือ ทิศตะวันออกและทิศเหนือเท่านั้น ก่อนที่จะถึงเมือง ค. นายจรจะต้องแวะเติมน้ำมันที่จุด ข. เสียก่อน จงหาจำนวนวิธีทั้งหมดในการเดินทาง

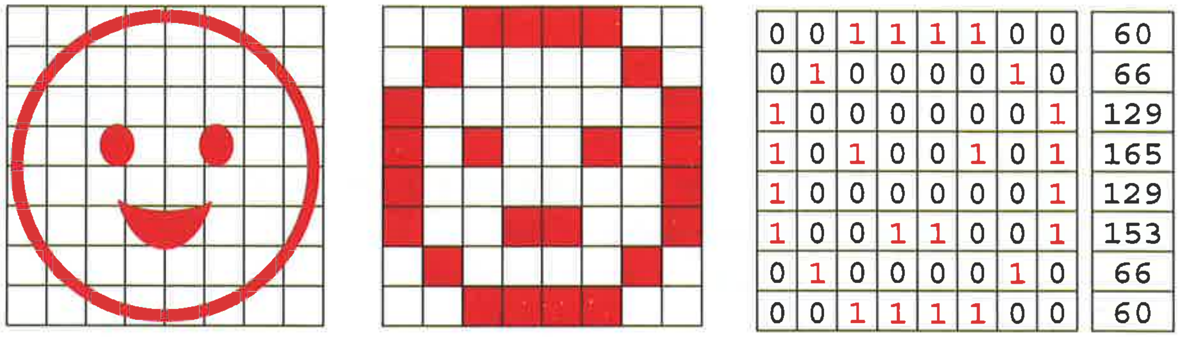


20. เส้นขนานชุดที่ 1 มี 5 เส้นตัดกับเส้นขนานอีกชุดหนึ่ง ซึ่งมี 10 เส้นจงหาจำนวนสี่เหลี่ยมด้านขนาน
21. จงหาจำนวนวิธีที่จะจัดสามีภรรยาจำนวน 5 คู่นั่งรอบโต๊ะกลมโดยที่
    21.1 คู่สามีภรรยานั่งติดกัน
    21.2 จัดให้นั่งครั้งละ 3 คู่ ชายและหญิงนั่งสลับกัน
    21.3 จัดให้นั่งครั้งละ 6 คน ชาย 3 คน หญิง 3 คน ชายและหญิงนั่งสลับกัน
22. มีครอบครัว 4 ครอบครัวแต่ละครอบครัวประกอบด้วย พ่อ แม่ และลูก 2 คน จงหาจำนวนวิธีจัดคนทั้งหมดนั่งรอบโต๊ะกลมโดยที่
    22.1 สมาชิกในครอบครัวเดียวกันนั่งติดกัน
    22.2 สมาชิกในครอบครัวเดียวกันนั่งติดกันและลูกทั้งสองคนนั่งติดกัน
    22.3 สมาชิกในครอบครัวเดียวกันนั่งติดกันและลูกทั้งสองคนนั่งตรงกลาง
23. จงหาค่าของ $C_{n,1} + 2C_{n,1} + 3C_{n,1} + \cdots + nC_{n,1}$
24. จงหาสัมประสิทธิ์ของ x^{18} จากการกระจาย $(x^2 + \frac{2}{x})^{12}$
25. ในการกระจาย $(a+b)^{10}$ ถ้าพจน์ที่ r มีสัมประสิทธิ์เป็น 210 แล้ว $C_{12,r}$ มีค่าเท่าใด
26. สัมประสิทธิ์ของพจน์ x ของผลบวก $1 + (1+x) + (1+x)^2 + \cdots + (1+x)^{15}$ เท่ากับเท่าใด
27. มีบัตร 10 ใบประกอบด้วยบัตรหมายเลข 1, 2, …, 10 สุ่มหยิบบัตร 2 ใบจากบัตรทั้ง 10 ใบนี้ จงหาความน่าจะเป็นของเหตุการณ์ต่อไปนี้
    27.1 หยิบบัตรพร้อมกัน 2 ใบให้ได้ผลบวกเป็นจำนวนคี่
    27.2 หยิบบัตรทีละใบโดยไม่ใส่กลับคืนให้ได้ผลบวกเป็นจำนวนคี่
    27.3 หยิบบัตรครั้งแรกบันทึกหมายเลขไว้และใส่กลับคืน แล้วหยิบบัตรครั้งที่สองให้ได้ผลบวกเป็นจำนวนคี่

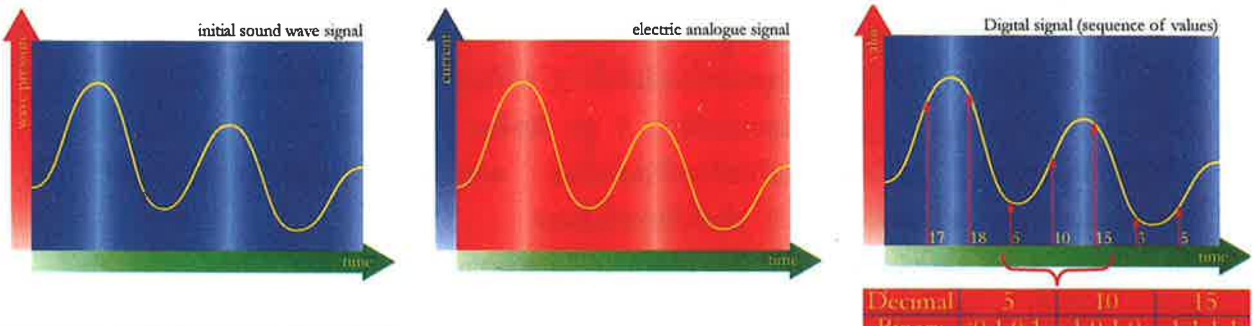
28. เลือกคน 2 คน จากสามีภรรยา 6 คู่ จงหาความน่าจะเป็นของเหตุการณ์ที่
    28.1 คนทั้งสองคนเป็นสามีภรรยากัน
    28.2 คนหนึ่งเป็นชายอีกคนหนึ่งเป็นหญิง
    28.3 คนทั้งสองไม่เป็นสามีภรรยากัน
29. ในการเลือกกรรมการ 3 คน จากชาย 4 คน และหญิง 5 คน จงหาความน่าจะเป็นที่จะได้กรรมการที่เป็นหญิงอย่างน้อย 2 คน
30. ข้อสอบฉบับหนึ่งมี 15 ข้อ ให้เลือกทำ 10 ข้อ โดยกำหนดให้เลือกทำ 4 ข้อจาก 5 ข้อแรก เด็กคนหนึ่งทำข้อสอบครบ 10 ข้อ จงหาความน่าจะเป็นที่เขาจะทำข้อ 1 ถึงข้อ 4
31. กล่องใบหนึ่งบรรจุลูกบอลสีขาว 4 ลูก และสีดำ 3 ลูก กล่องใบที่สองบรรจุลูกบอลสีขาว 3 ลูก และสีดำ 5 ลูก หยิบลูกบอล 1 ลูกจากกล่องใบที่หนึ่งและอีก 1 ลูกจากกล่องใบที่สอง จงหาความน่าจะเป็นที่หยิบได้ลูกบอลสีดำทั้ง 2 ลูก
32. เหรียญไม่เที่ยงตรงอันหนึ่ง เมื่อโยนเหรียญแล้วโอกาสที่เหรียญจะขึ้นหน้าหัวเป็น 3 เท่าของการขึ้นหน้าก้อย ถ้าโยนเหรียญนี้พร้อมกับทอดลูกเต๋าเที่ยงตรง 1 ลูก จงหาความน่าจะเป็นที่
    32.1 เหรียญขึ้นหน้าหัวและลูกเต๋าขึ้นแต้มคู่ในการโยนพร้อมๆ กัน 1 ครั้ง
    32.2 เหรียญขึ้นหน้าหัว 2 ครั้ง และลูกเต๋าขึ้นแต้มคี่ทั้ง 2 ครั้งในการโยนพร้อมๆ กัน 2 ครั้ง
33. ในตะกร้าใบหนึ่งมีลูกบอล 20 ลูก โดยมีลูกบอลสีขาว 5 ลูก สีเหลือง 4 ลูก สีเขียว 6 ลูก และสีแดง 5 ลูก ถ้าหยิบลูกบอลครั้งละ 1 ลูก โดยหยิบแล้วใส่คืนกลับลงไปใหม่ จงหาความน่าจะเป็นที่หยิบลูกบอลลูกที่ 1 เป็นสีขาวหรือสีเหลือง และหยิบลูกบอลลูกที่ 2 เป็นสีเขียวหรือสีแดง
34. ในการจัดชาย 5 คน และหญิง 4 คน เข้านั่งรอบโต๊ะกลม จงหาความน่าจะเป็นที่
    34.1 หญิงทั้ง 4 คนนั่งติดกัน
    34.2 ไม่มีหญิงสองคนใดนั่งติดกัน
35. ให้ A และ B เป็นเหตุการณ์ใด ๆ ภายใต้แซมเปิลสเปซเดียวกันโดยที่

    $$P(A \cup B) = \frac{3}{4},\ P(A') = \frac{2}{3} \text{ และ } P(A \cap B) = \frac{1}{4}$$

    จงหา $P(A \cap B') + P(A' \cap B)$
36. กล่องใบหนึ่งมีลูกหินสีน้ำเงิน 8 ลูก สีขาว 9 ลูก และสีแดง 3 ลูก
    36.1 ถ้าสุ่มหยิบลูกหิน 3 ลูกทีละลูกโดยไม่ใส่คืน จงหาความน่าจะเป็นที่ได้ลูกหินสีน้ำเงิน ขาว และแดงตามลำดับ
    36.2 ถ้าสุ่มหยิบลูกหิน 3 ลูก ทีละลูกโดยไม่ใส่คืน จงหาความน่าจะเป็นที่ไม่ได้ลูกหินสีน้ำเงินทั้ง 3 ครั้ง
37. ในการเลือกตั้งผู้แทนครั้งหนึ่ง พบว่าความน่าจะเป็นที่ผู้ชายมีภรรยาแล้วจะลงคะแนนเลือกตั้งเท่ากับ 0.4 สำหรับหญิงที่มีสามีแล้วความน่าจะเป็นจะลงคะแนนเลือกตั้งมีค่าเท่ากับ 0.3 แต่ถ้าทราบว่าสามีจะไปลงคะแนนความน่าจะเป็นก็จะเพิ่มขึ้นเป็น 0.7 จงหาความน่าจะเป็นที่สามีภรรยาคู่หนึ่งจะลงคะแนนเลือกตั้งทั้งคู่
38. ในการสุ่มหยิบใบดำใบแดงเพื่อรับทหารเกณฑ์ที่แห่งหนึ่ง มีใบแดงทั้งสิ้น 20 ใบ มีใบดำ 5 ใบ ถ้านายเด่นเป็นคนที่สามในการหยิบครั้งนี้ จงหาความน่าจะเป็นที่เขาจะสุ่มได้ใบดำ เมื่อ 2 คนแรกที่ได้หยิบไปแล้วมีเพียงคนเดียวที่หยิบได้ใบดำ (สุ่มแบบไม่ใส่คืน)

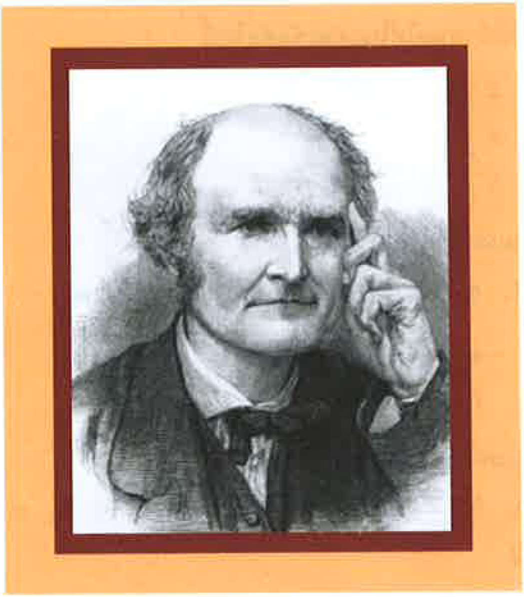


Pixel digitalization.



Analogue signals can be digitalized as a sequence of measured values.

เมทริกซ์



เคย์เลย์, อาร์เทอร์
ค.ศ. 1821 – 1895, อังกฤษ

ในบทนี้จะศึกษาถึงสมบัติพื้นฐาน การดำเนินการของเมทริกซ์ เมทริกซ์สลับเปลี่ยน เมทริกซ์ผกผันและดีเทอร์มิแนนต์ การเชื่อมโยงกันระหว่างเมทริกซ์กับความสัมพันธ์ สำหรับการพิสูจน์ทฤษฎีบทนั้นสามารถอ่านได้ในภาคผนวก

ความหมายของเมทริกซ์

ในหัวข้อนี้จะกล่าวถึงการเท่ากัน การบวก การลบ และการคูณของเมทริกซ์ เป็นต้น แต่ก่อนอื่นจะให้ความหมายของเมทริกซ์ก่อน ดังบทนิยามต่อไปนี้

บทนิยาม 6.1 **เมทริกซ์** หมายถึง การนำจำนวนจริงมาเขียนเรียงกันให้อยู่ในรูปสี่เหลี่ยมมุมฉากเป็นสองมิติ โดยอยู่ในแนวนอนที่เรียกว่า**แถว** และในแนวตั้งที่เรียกว่า**หลัก**

ถ้า A เป็นเมทริกซ์ เราจะเขียนแทน A ด้วย $[a_{ij}]$ เมื่อ a_{ij} เป็นจำนวนจริงใด ๆ ในแถวที่ i และหลักที่ j ของ A

จะกล่าวว่า A เป็นเมทริกซ์**ขนาด** $m \times n$ ถ้า A เป็นเมทริกซ์ที่มี m แถวและ n หลัก เขียนแทนขนาดของ A ด้วย $m \times n$

ตัวอย่าง 6.1 พิจารณาเมทริกซ์ที่กำหนดให้ในแต่ละข้อต่อไปนี้

(1) ให้ $A = \begin{bmatrix} 1 & 2 \\ 0 & 8 \\ 7 & 5 \end{bmatrix}$

จะได้ว่า A เป็นเมทริกซ์ที่มีขนาด 3×2

โดยที่ $a_{11} = 1,\ a_{12} = 2,\ a_{21} = 0,\ a_{22} = 8,\ a_{31} = 7$ และ $a_{32} = 5$

(2) ให้ $B = \begin{bmatrix} 5 & -4 & 1 & 0 \\ 3 & 7 & 10 & -2 \end{bmatrix}$

จะได้ว่า B เป็นเมทริกซ์ที่มีขนาด 2×4

โดยที่ $b_{11} = 5,\ b_{12} = -4,\ b_{13} = 1,\ b_{14} = 0,\ b_{21} = 3,\ b_{22} = 7,\ b_{23} = 10$ และ $b_{24} = -2$

(3) $C = \begin{bmatrix} 25 & 30 & 35 & 40 & 45 \\ -5 & 0 & 5 & 10 & 15 \\ -40 & -35 & -30 & -25 & -20 \\ 5 & 10 & 15 & 20 & 25 \\ 50 & 55 & 60 & 65 & 70 \end{bmatrix}$

จะได้ว่า C เป็นเมทริกซ์ที่มีขนาด 5×5

โดย $c_{11} = 25,\ c_{22} = 0,\ c_{33} = -30,\ c_{44} = 20$ และ $c_{55} = 70$ □

กรณีทั่วไป ถ้า A เป็นเมทริกซ์ขนาด $m \times n$ เขียนแทน A ด้วย $[a_{ij}]_{m\times n}$ เมื่อ a_{ij} เป็นจำนวนจริง โดยที่ $1 \le i \le m$ และ $1 \le j \le n$ นั่นคือ

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{bmatrix}$$

บทนิยาม 6.2 เรียกเมทริกซ์ที่มีแถวเดียวว่า **เมทริกซ์แถว** หรือ **เวกเตอร์แถว** และเรียกเมทริกซ์ที่มีหลักเดียวว่า **เมทริกซ์หลัก** หรือ **เวกเตอร์หลัก**

บทนิยาม 6.3 เมทริกซ์ที่มีจำนวนแถวเท่ากับจำนวนหลัก เรียกว่า **เมทริกซ์จัตุรัส** และเรียกมทริกซ์ที่ทุกจำนวนมีค่าเป็น 0 ว่า **เมทริกซ์ศูนย์** เขียนแทนด้วยสัญลักษณ์ $[0]$ หรือ $\mathbf{0}$

ตัวอย่าง 6.2 กำหนด $A = \begin{bmatrix} -3 & 7 & 11 & -5 \end{bmatrix}$, $B = \begin{bmatrix} 9 \\ 8 \\ 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 0 & 4 \\ 0 & 5 & -1 \end{bmatrix}$

และ $D = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$

จะได้ว่า A และ B เป็นเมทริกซ์แถวและเมทริกซ์หลัก ตามลำดับ
C เป็นเมทริกซ์จัตุรัส และ D เป็นเมทริกซ์ศูนย์ □

บทนิยาม 6.4 ให้ $A = [a_{ij}]$ และ $B = [b_{ij}]$ จะกล่าวว่า A และ B เป็น**เมทริกซ์ที่เท่ากัน** เขียนแทนด้วย $A = B$ ก็ต่อเมื่อ เมทริกซ์ทั้งสองมีขนาดเท่ากันและจำนวนในตำแหน่งที่ตรงกันเท่ากัน นั่นคือ $a_{ij} = b_{ij}$ ทุกค่า i และ j

ตัวอย่าง 6.3 กำหนด $A = \begin{bmatrix} 1 & 2 & -1 \\ 3 & 4 & 0 \end{bmatrix}$ และ $B = \begin{bmatrix} 1 & 2 & -1 \\ 3 & -4 & 0 \end{bmatrix}$

จะเห็นว่าเมทริกซ์ A และเมทริกซ์ B มีขนาดเท่ากันคือ 2×3 แต่ $A \neq B$
เพราะว่า $a_{23} = 4$ ขณะที่ $b_{23} = -4$ □

การดำเนินการบนเมทริกซ์

ในหัวข้อนี้จะกล่าวถึงการดำเนินการบนเมทริกซ์ เช่น การบวก การลบ และการคูณของเมทริกซ์ เป็นต้น นอกจากนี้ยังจะศึกษาถึงสมบัติต่าง ๆ ของเมทริกซ์ ดังต่อไปนี้

บทนิยาม 6.5 ให้ $A = [a_{ij}]$ และ $B = [b_{ij}]$ เป็นเมทริกซ์ขนาด $m \times n$ ผลบวกของ A และ B เขียนแทนด้วย $A + B$ มีค่าเท่ากับ $[a_{ij}+b_{ij}]$ และ $A + B$ มีขนาดเป็น $m \times n$

ตัวอย่าง 6.4 กำหนด $A = \begin{bmatrix} 2 & 1 & -2 \\ 0 & 4 & -1 \\ 3 & 5 & 6 \end{bmatrix}$ และ $B = \begin{bmatrix} -4 & 5 & 0 \\ 2 & 0 & 8 \\ -1 & 0 & 1 \end{bmatrix}$

จงหา $A + B$

วิธีทำ เนื่องจาก A และ B เป็นเมทริกซ์ที่มีขนาด 3×3 จะได้ว่า $A + B$ เป็นเมทริกซ์ที่มีขนาด 3×3 แล้ว

$$\begin{aligned} A + B &= \begin{bmatrix} 2 & 1 & -2 \\ 0 & 4 & -1 \\ 3 & 5 & 6 \end{bmatrix} + \begin{bmatrix} -4 & 5 & 0 \\ 2 & 0 & 8 \\ -1 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 2+(-4) & 1+5 & -2+0 \\ 0+2 & 4+0 & -1+8 \\ 3+(-1) & 5+0 & 6+1 \end{bmatrix} \\ &= \begin{bmatrix} -2 & 6 & -2 \\ 2 & 4 & 7 \\ 2 & 5 & 7 \end{bmatrix} \end{aligned}$$

□

บทนิยาม 6.6 กำหนด $A = [a_{ij}]$ เป็นเมทริกซ์ขนาด $m \times n$ ผลคูณของสเกลาร์ k และ A เขียนแทนด้วย kA หรือ Ak มีค่าเท่ากับ $[ka_{ij}]$ และมีขนาดเป็น $m \times n$ นั่นคือ

ถ้า $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$ แล้ว $kA = \begin{bmatrix} ka_{11} & ka_{12} & \cdots & ka_{1n} \\ ka_{21} & ka_{22} & \cdots & ka_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ ka_{m1} & ka_{m2} & \cdots & ka_{mn} \end{bmatrix}$

ตัวอย่าง 6.5 กำหนด $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix}$ และ $k_1 = -1,\ k_2 = 0$

จะได้ว่า $k_1A = \begin{bmatrix} -1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}$

และ $k_2A = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = [0]$ □

ต่อไปจะกล่าวถึงสมบัติพื้นฐานของเมทริกซ์ ดังนี้

ทฤษฎีบท 6.1 ให้ A, B และ C เป็นเมทริกซ์ขนาด $m \times n$ และ k_1 และ k_2 เป็นสเกลาร์ จะได้ว่า

(i) $(A + B) + C = A + (B + C)$
(ii) $A + B = B + A$
(iii) $A + \mathbf{0} = A = \mathbf{0} + A$
(iv) $A + (-A) = \mathbf{0} = (-A) + A$
(v) $k_1(A + B) = k_1A + k_1B$
(vi) $(k_1 + k_2)A = k_1A + k_2A$
(vii) $(k_1k_2)A = k_1(k_2A)$
(viii) $1A = A$

การดำเนินการบนเมทริกซ์ที่สำคัญและนำมาใช้บ่อย ๆ คือ การคูณกันระหว่างเมทริกซ์ โดยเมทริกซ์ทั้งสองต้องมีขนาดที่มีจำนวนหลักของเมทริกซ์แรกเท่ากับจำนวนแถวของเมทริกซ์ที่สอง ดังบทนิยามต่อไปนี้

บทนิยาม 6.7 ให้ $A = [a_{ij}]$ เป็นเมทริกซ์ขนาด $m \times k$ และ $B = [b_{ij}]$ เป็นเมทริกซ์ขนาด $k \times n$ **ผลคูณ**ของ A และ B เขียนแทนด้วย AB มีค่าเท่ากับ $[c_{ij}]$ ซึ่งเป็นเมทริกซ์ขนาด $m \times n$ โดยที่ c_{ij} มีค่าเท่ากับผลบวกของผลคูณของจำนวนในแถวที่ i ของ A และหลักที่ j ของ B นั่นคือ

ถ้า $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix}$ และ $B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix}$ แล้ว

$$AB = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \boxed{a_{i1} \quad a_{i2}} & \cdots & \boxed{a_{ik}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{i1} & c_{i2} & \cdots & \boxed{c_{ij}} & \cdots & c_{in} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{mn} \end{bmatrix}$$

โดยที่

$$\begin{aligned} c_{ij} &= a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} \\ &= \sum_{\ell=1}^{k} a_{i\ell}b_{\ell j} \qquad \text{เมื่อ } 1 \le i \le m \text{ และ } 1 \le j \le n \end{aligned}$$

ตัวอย่าง 6.6 กำหนด $A = \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 4 \\ 3 & 2 & -1 \\ -2 & 3 & 1 \end{bmatrix}$ และ $B = \begin{bmatrix} -4 & 0 \\ 5 & 2 \\ 1 & 0 \end{bmatrix}$ จงหา AB

วิธีทำ เนื่องจาก A เป็นเมทริกซ์ขนาด 4×3 และ B เป็นเมทริกซ์ขนาด 3×2
ดังนั้นได้จำนวนหลักของ A เท่ากับจำนวนแถวของ B
ทำให้สามารถหา AB ได้และเป็นเมทริกซ์ที่มีขนาด 4×2 ดังนี้

$$\begin{aligned} AB &= \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 4 \\ 3 & 2 & -1 \\ -2 & 3 & 1 \end{bmatrix} \begin{bmatrix} -4 & 0 \\ 5 & 2 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} (1)(-4)+(0)(5)+(-2)(1) & (1)(0)+(0)(2)+(-2)(0) \\ (0)(-4)+(1)(5)+(4)(1) & (0)(0)+(1)(2)+(4)(0) \\ (3)(-4)+(2)(5)+(-1)(1) & (3)(0)+(2)(2)+(-1)(0) \\ (-2)(-4)+(3)(5)+(1)(1) & (-2)(0)+(3)(2)+(1)(0) \end{bmatrix} \\ &= \begin{bmatrix} -6 & 0 \\ 9 & 2 \\ -3 & 4 \\ 24 & 6 \end{bmatrix} \end{aligned}$$

□

หมายเหตุ ตัวอย่าง 6.6 เราไม่สามารถหา BA เพราะว่าจำนวนหลักของ B ไม่เท่ากับจำนวนแถวของ A

ตัวอย่าง 6.7 กำหนด $A = \begin{bmatrix} 2 & 2 \\ 1 & 3 \\ 2 & 3 \end{bmatrix}$ และ $B = \begin{bmatrix} 2 & -4 & 5 \\ 2 & 1 & 0 \end{bmatrix}$ จงหา AB และ BA

วิธีทำ เนื่องจาก A เป็นเมทริกซ์ขนาด 3×2 และ B เป็นเมทริกซ์ขนาด 2×3
ดังนั้นจำนวนหลักของ A เท่ากับจำนวนแถวของ B และ จำนวนหลักของ B เท่ากับจำนวนแถวของ A
เพราะฉะนั้นสามารถหา AB และ BA ได้ตามลำดับ ดังนี้

$$AB = \begin{bmatrix} 2 & 2 \\ 1 & 3 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 2 & -4 & 5 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 8 & -6 & 10 \\ 8 & -1 & 5 \\ 10 & -5 & 10 \end{bmatrix}$$

$$BA = \begin{bmatrix} 2 & -4 & 5 \\ 2 & 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 1 & 3 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 10 & 11 \\ 5 & 6 \end{bmatrix}$$ □

ตัวอย่าง 6.8 กำหนด $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ และ $B = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}$ จงหา AB และ BA

วิธีทำ เนื่องจากเมทริกซ์ A และ B เป็นเมทริกซ์จัตุรัสที่มีขนาด 2×2 ดังนั้นสามารถหา AB และ BA ได้ดังนี้

$$AB = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 3 \\ -1 & 4 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 0 & -1 \end{bmatrix}$$ □

ข้อสังเกต
1. จากตัวอย่าง 6.7 และ 6.8 จะเห็นได้ว่า $AB \neq BA$
2. ถ้าเมทริกซ์ A มีขนาด $m \times n$ และเมทริกซ์ B มีขนาด $r \times s$ แล้ว AB จะหาค่าได้ก็ต่อเมื่อ $n = r$ และ BA จะหาค่าได้ก็ต่อเมื่อ $s = m$

ตัวอย่าง 6.9 กำหนด $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}$ และ $C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
จงหา $(AB)C$ และ $A(BC)$

วิธีทำ เนื่องจาก $AB = \begin{bmatrix} 0 & 3 \\ -1 & 4 \end{bmatrix}$ และ $BC = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}$

จะได้ $(AB)C = \begin{bmatrix} 0 & 3 \\ -1 & 4 \end{bmatrix}$

และ $A(BC) = \begin{bmatrix} 0 & 3 \\ -1 & 4 \end{bmatrix}$ □

จากตัวอย่าง 6.9 จะสังเกตเห็นว่า $(AB)C = A(BC)$ ทำให้เราได้ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 6.2 กำหนด A, B และ C เป็นเมทริกซ์ซึ่งสามารถหาผลบวกและผลคูณได้ และ k เป็นสเกลาร์ จะได้

(i) $A(BC) = (AB)C$

(ii) $A(B+C) = AB + AC$

(iii) $(A+B)C = AC + BC$

(iv) $k(AB) = (kA)B = A(kB)$

เมทริกซ์สลับเปลี่ยน

ในหัวข้อนี้จะกล่าวถึงเมทริกซ์ที่ได้จากการเปลี่ยนจากแถวเป็นหลักและเปลี่ยนจากหลักเป็นแถว ดังบทนิยามต่อไปนี้

บทนิยาม 6.8 ให้ $A = [a_{ij}]$ เป็นเมทริกซ์ขนาด $m \times n$ **เมทริกซ์สลับเปลี่ยน**ของ A เขียนแทนด้วย A^T คือเมทริกซ์ $[a_{ji}]$ ขนาด $n \times m$ ที่ได้จากการสลับแถวและหลักของ A
นั่นคือ ถ้า $A = [a_{ij}]$ และ $A^T = [b_{ij}]$ แล้ว $b_{ij} = a_{ji}$
เมื่อ $1 \leq i \leq m$ และ $1 \leq j \leq n$

ตัวอย่าง 6.10 กำหนด $A = \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ -1 & 3 \end{bmatrix}$ จงหา A^T

วิธีทำ เนื่องจาก A เป็นเมทริกซ์ที่มีขนาด 3×2 ดังนั้น A^T มีขนาด 2×3 และ

$$A^T = \begin{bmatrix} 3 & 2 & -1 \\ 2 & 1 & 3 \end{bmatrix}$$ □

ต่อไปจะกล่าวถึงสมบัติของเมทริกซ์สลับเปลี่ยน ดังนี้

ทฤษฎีบท 6.3 กำหนด A, B และ C เป็นเมทริกซ์ซึ่งสามารถหาผลบวกและผลคูณได้ และ k เป็นสเกลาร์ จะได้

(i) $(A+B)^T = A^T + B^T$

(ii) $(AB)^T = B^T A^T$

(iii) $(kA)^T = kA^T$

(iv) $(A^T)^T = A$

บทนิยาม 6.9 เมทริกซ์จัตุรัส A เป็น**เมทริกซ์สมมาตร** ก็ต่อเมื่อ $A = A^T$

ตัวอย่าง 6.11 เมทริกซ์ $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ และ $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 0 & 5 \\ 3 & 5 & -1 \end{bmatrix}$ เป็นเมทริกซ์สมมาตร □

ข้อสังเกต จะเห็นว่า $A = [a_{ij}]$ เป็นเมทริกซ์สมมาตรก็ต่อเมื่อ $a_{ij} = a_{ji}$ โดยที่ $1 \leq i, j \leq n$

เมทริกซ์เอกลักษณ์

บทนิยาม 6.10 **เมทริกซ์เอกลักษณ์อันดับ** n เขียนแทนด้วย $I_n = [\delta_{ij}]$ คือเมทริกซ์ขนาด $n \times n$ ที่มี

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

นั่นคือ
$$I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

ทฤษฎีบท 6.4 ถ้า A เป็นเมทริกซ์ขนาด $m \times n$ แล้ว $AI_n = I_m A = A$

เมทริกซ์ผกผันและดีเทอร์มิแนนต์

เมทริกซ์ที่จะกล่าวถึงในหัวข้อนี้จะเป็นเมทริกซ์จัตุรัสเท่านั้น โดยเราจะหาเมทริกซ์ผกผันและดีเทอร์มิแนนต์ของเมทริกซ์ที่กำหนด ดังบทนิยามต่อไปนี้

บทนิยาม 6.11 ถ้า A และ B เป็นเมทริกซ์ขนาด $n \times n$ ซึ่ง $AB = BA = I_n$ จะเรียก B ว่า **เมทริกซ์ผกผัน**ของ A เขียนแทน B ด้วย A^{-1} นั่นคือ $B = A^{-1}$ และเรียก A ว่า **เมทริกซ์ไม่เอกฐาน**

ตัวอย่าง 6.12 กำหนด $A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}$ และ $B = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$

จะได้ว่า $AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ และ $BA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

ดังนั้น A และ B เป็นเมทริกซ์ผกผันซึ่งกันและกัน □

บทนิยาม 6.12 ถ้า A เป็นเมทริกซ์ขนาด $n \times n$ **ดีเทอร์มิแนนต์**ของ A เขียนแทนด้วย $\det(A)$ หรือ $|A|$ นิยามโดย

1. ถ้า $A = [a_{11}]$ แล้ว $\det(A) = |a_{11}| = a_{11}$
2. ถ้า $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ แล้ว $\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$
3. ถ้า $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ แล้ว

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{32}a_{21} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{32}a_{23}$$

ตัวอย่าง 6.13 จงหาดีเทอร์มิแนนต์ของเมทริกซ์ในแต่ละข้อต่อไปนี้

(1) $A = [7]$ (2) $B = \begin{bmatrix} 2 & 1 \\ -4 & 6 \end{bmatrix}$

(3) $C = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 6 & -1 \\ 5 & 1 & 0 \end{bmatrix}$

วิธีทำ (1) $\det(A) = 7$

(2) $\det(B) = (2 \cdot 6) - (1 \cdot (-4)) = 16$

(3) $\det(C) = (2 \cdot 6 \cdot 0) + (1 \cdot (-1) \cdot 5) + (3 \cdot 1 \cdot 4)$
$- (3 \cdot 6 \cdot 5) - (1 \cdot 4 \cdot 0) - (2 \cdot 1 \cdot (-1))$
$= -81$ □

ทฤษฎีบท 6.5 ถ้า A และ B เป็นเมทริกซ์ขนาด $n \times n$ แล้ว $\det(AB) = \det(A)\det(B)$

ตัวอย่าง 6.14 กำหนด $A = \begin{bmatrix} 1 & 1 & 2 \\ 0 & -1 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ และ $B = \begin{bmatrix} -2 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$

จงแสดงว่า $\det(AB) = \det(A)\det(B)$

วิธีทำ $AB = \begin{bmatrix} -2+1+0 & 0+1+0 & 1+1-2 \\ 0-1+0 & 0-1+0 & 0-1-1 \\ -2+2+0 & 0+2+0 & 1+2+0 \end{bmatrix} = \begin{bmatrix} -1 & 1 & 0 \\ -1 & -1 & -2 \\ 0 & 2 & 3 \end{bmatrix}$

$$\begin{aligned} \det(AB) &= ((-1)\cdot(-1)\cdot 3) + (1\cdot(-2)\cdot 0) + (0\cdot 2\cdot(-1)) \\ &\quad - (0\cdot(-1)\cdot 0) - (1\cdot(-1)\cdot 3) - ((-1)\cdot 2\cdot(-2)) \\ &= 3 + 0 + 0 - 0 - (-3) - 4 \\ &= 2 \end{aligned}$$

$$\begin{aligned} \det(A) &= (1\cdot(-1)\cdot 0) + (1\cdot 1\cdot 1) + (2\cdot 2\cdot 0) \\ &\quad - (2\cdot(-1)\cdot 1) - (1\cdot 0\cdot 0) - (1\cdot 2\cdot 1) \\ &= 0 + 1 + 0 - (-2) - 0 - 2 \\ &= 1 \end{aligned}$$

$$\begin{aligned} \det(B) &= ((-2)\cdot 1\cdot(-1)) + (0\cdot 1\cdot 0) + (1\cdot 0\cdot 1) \\ &\quad - (1\cdot 1\cdot 0) - (0\cdot 1\cdot(-1)) - ((-2)\cdot 0\cdot 1) \\ &= 2 + 0 + 0 - 0 - 0 - 0 \\ &= 2 \end{aligned}$$

ดังนั้น $\det(AB) = \det(A)\det(B)$ □

ทฤษฎีบท 6.6 เมทริกซ์ A ขนาด 2×2 จะมีเมทริกซ์ผกผันก็ต่อเมื่อ $\det(A) \neq 0$ และ

ถ้า $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ แล้ว $A^{-1} = \dfrac{1}{\det(A)}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

ตัวอย่าง 6.15 กำหนด $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ จงหาเมทริกซ์ผกผันของ A

วิธีทำ เพราะว่า $\det(A) = (2\cdot 5) - (3\cdot 4) = -2 \neq 0$ แสดงว่าหา A^{-1} ได้ และ

$$A^{-1} = \frac{1}{-2}\begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} -2.5 & 1.5 \\ 2 & -1 \end{bmatrix}$$ □

เมทริกซ์กับความสัมพันธ์

เราสามารถแทนความสัมพันธ์ระหว่างเซตจำกัด 2 เซตได้หลายวิธี เช่น เขียนอยู่ในรูปคู่อันดับ หรือเขียนอยู่ในรูปตาราง เป็นต้น ในหัวข้อนี้จะกล่าวถึงการแทนความสัมพันธ์ที่กำหนดในรูปเมทริกซ์ $0-1$ มีวิธีการดังนี้

พิจารณาความสัมพันธ์ $r \subseteq A \times B$ เมื่อ A และ B เป็นเซตจำกัด

สมมติให้ $A = \{a_1, a_2, \ldots, a_m\}$ และ $B = \{b_1, b_2, \ldots, b_n\}$

ดังนั้น เมทริกซ์ $0-1$ ของความสัมพันธ์ r เขียนแทนด้วย $M_r = [m_{ij}]_{m\times n}$ นิยามโดย

$$m_{ij} = \begin{cases} 1, & (a_i, b_j) \in r \\ 0, & (a_i, b_j) \notin r \end{cases}$$

ตัวอย่าง 6.16 ให้ $A = \{1, 2, 3\}$, $B = \{1, 2\}$ และ r เป็นความสัมพันธ์จาก A ไป B
สมมติให้ $r = \{(a, b) \in A \times B \mid a < b\}$
จงเขียนแทน r ด้วยเมทริกซ์ $0-1$ M_r

วิธีทำ เนื่องจาก $r = \{(2, 1), (3, 1), (3, 2)\}$ จะได้เมทริกซ์ $0-1$ M_r คือ

$$M_r = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$$

นั่นคือ สมาชิก 1 ของ M_r หมายถึง คู่อันดับ $(2, 1)$, $(3, 1)$ และ $(3, 2)$ เป็นสมาชิกของ r
สมาชิก 0 ของ M_r หมายถึง คู่อันดับที่ไม่เป็นสมาชิกของ r □

ตัวอย่าง 6.17 ให้ $A = \{a_1, a_2, a_3\}$ และ $B = \{b_1, b_2, b_3, b_4, b_5\}$ จงหาความสัมพันธ์ r เมื่อ

$$M_r = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

วิธีทำ เนื่องจาก r ประกอบด้วยคู่อันดับ $(a_i, b_j) \in r$ เมื่อ $m_{ij} = 1$ ดังนั้นได้

$$r = \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}$$ □

ต่อไปจะกล่าวถึงการนำเมทริกซ์ $0-1$ ที่ใช้แทนความสัมพันธ์มาช่วยในการพิจารณาเรื่องของสมบัติสะท้อน สมบัติสมมาตรและสมบัติถ่ายทอด ถ้าเมทริกซ์ $0-1$ เป็นเมทริกซ์จัตุรัสขนาด $n \times n$ ได้ดังนี้

สมมติให้ $A = \{a_1, a_2, \ldots, a_n\}$ และ r เป็นความสัมพันธ์บน A จะได้ว่า
r มีสมบัติสะท้อน ก็ต่อเมื่อ $(a_i, a_i) \in r$ ทุก $i = 1, 2, 3, \ldots, n$

นั่นคือ ถ้าพิจารณาจากสมาชิกของเมทริกซ์ $0-1$ M_r แล้วจะได้ว่า

r มีสมบัติสะท้อน ก็ต่อเมื่อ $m_{ii} = 1$ ทุก $i = 1, 2, 3, \ldots, n$

หรือกล่าวได้อีกแบบว่า

r มีสมบัติสะท้อน ก็ต่อเมื่อ สมาชิกในแนวเส้นทแยงมุมหลักของเมทริกซ์ $0-1$ M_r เป็น 1

นั่นคือ

$$M_r = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

พิจารณาในทำนองเดียวกัน เนื่องจาก r เป็นความสัมพันธ์บน A จะได้ว่า

r มีสมบัติสมมาตร ก็ต่อเมื่อ ถ้า $(a_i, a_j) \in r$ แล้ว $(a_j, a_i) \in r$

นั่นคือ ถ้าพิจารณาจากสมาชิกของเมทริกซ์ $0-1$ M_r แล้วจะได้ว่า

r มีสมบัติสมมาตร ก็ต่อเมื่อ ถ้า $m_{ij} = 1$ แล้ว $m_{ji} = 1$

ทำให้ได้ว่า ถ้า $m_{ij} = 0$ แล้ว $m_{ji} = 0$ นั่นคือ

r มีสมบัติสมมาตร ก็ต่อเมื่อ $m_{ij} = m_{ji}$ ทุก $i, j = 1, 2, 3, \ldots, n$

หรือกล่าวได้อีกแบบว่า

r มีสมบัติสมมาตร ก็ต่อเมื่อ เมทริกซ์ $0-1$ M_r เป็นเมทริกซ์สมมาตร

นั่นคือ

$$M_r = \begin{bmatrix} & & 1 & 0 \\ 1 & & & \\ & & & \\ 0 & & & \end{bmatrix}$$

ตัวอย่าง 6.18 สมมติให้ความสัมพันธ์ r แทนด้วยเมทริกซ์

$$M_r = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

จงพิจารณาว่า r มีสมบัติสะท้อนและสมบัติสมมาตรหรือไม่

วิธีทำ r มีสมบัติสะท้อน เพราะว่าสมาชิกในแนวทแยงมุมหลักของเมทริกซ์ $0-1$ M_r เป็น 1 และ r มีสมบัติสมมาตร เพราะว่าเมทริกซ์ $0-1$ M_r เป็นเมทริกซ์สมมาตร □

ต่อไปจะกล่าวถึงการดำเนินการบูลีนระหว่างสมาชิกกับสมาชิก และระหว่างเมทริกซ์กับเมทริกซ์ ก่อนที่จะนำไปใช้ในการหายูเนียนและอินเตอร์เซกชันของความสัมพันธ์สองความสัมพันธ์ ดังต่อไปนี้

บทนิยาม 6.13 **การดำเนินการบูลีน** $\wedge$ และ $\vee$ นิยามโดย

$$a \wedge b = \begin{cases} 1, & a = b = 1 \\ 0, & \text{อื่น ๆ} \end{cases}$$

$$a \vee b = \begin{cases} 1, & a = 1 \vee b = 1 \\ 0, & \text{อื่น ๆ} \end{cases}$$

บทนิยาม 6.14 ให้ $A = [a_{ij}]$ และ $B = [b_{ij}]$ เป็นเมทริกซ์ $0-1$ ขนาด $m \times n$

เมทริกซ์หรือ ของ A และ B เขียนแทนด้วย $A \vee B$ นิยามโดย

$$A \vee B = [a_{ij} \vee b_{ij}]$$

เมทริกซ์และ ของ A และ B เขียนแทนด้วย $A \wedge B$ นิยามโดย

$$A \wedge B = [a_{ij} \wedge b_{ij}]$$

ตัวอย่าง 6.19 ให้ $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ และ $B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$

จงหา $A \vee B$ และ $A \wedge B$

วิธีทำ จากบทนิยาม 6.14 จะได้ว่า

$$A \vee B = \begin{bmatrix} 1\vee 0 & 0\vee 1 & 1\vee 0 \\ 0\vee 1 & 1\vee 1 & 1\vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$A \wedge B = \begin{bmatrix} 1\wedge 0 & 0\wedge 1 & 1\wedge 0 \\ 0\wedge 1 & 1\wedge 1 & 1\wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

□

ต่อไปจะนิยามผลคูณบูลีนของสองเมทริกซ์ดังนี้

บทนิยาม 6.15 ให้ $A = [a_{ij}]$ และ $B = [b_{ij}]$ เป็นเมทริกซ์ $0-1$

ผลคูณบูลีนของ A กับ B เขียนแทนด้วย $A \otimes B$ นิยามโดย

$$A \otimes B = [c_{ij}]_{m\times n}$$

โดยที่ $c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \ldots \vee (a_{ik} \wedge b_{kj})$

ข้อสังเกต การหาผลคูณบูลีนของเมทริกซ์ $0-1$ ของ A กับ B ก็เหมือนกับการหาผลคูณของเมทริกซ์ธรรมดา เพียงแต่แทนเครื่องหมายบวกด้วย "$\vee$" และแทนเครื่องหมายคูณด้วย "$\wedge$"

ตัวอย่าง 6.20 จงหา $A \otimes B$ เมื่อ

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{และ} \quad B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

วิธีทำ จากบทนิยาม 6.15 จะได้

$$A \otimes B = \begin{bmatrix} (1\wedge 1)\vee(0\wedge 0) & (1\wedge 1)\vee(0\wedge 1) & (1\wedge 0)\vee(0\wedge 1) \\ (0\wedge 1)\vee(1\wedge 0) & (0\wedge 1)\vee(1\wedge 1) & (0\wedge 0)\vee(1\wedge 1) \\ (1\wedge 1)\vee(1\wedge 0) & (1\wedge 1)\vee(1\wedge 1) & (1\wedge 0)\vee(1\wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1\vee 0 & 1\vee 0 & 0\vee 0 \\ 0\vee 0 & 0\vee 1 & 0\vee 1 \\ 1\vee 0 & 1\vee 1 & 0\vee 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

□

บทนิยาม 6.16 ให้ A เป็นเมทริกซ์จัตุรัส $0-1$ ขนาด $n \times n$ และ k เป็นจำนวนเต็มบวก นิยาม

$$A^k = A \otimes A \otimes \cdots \otimes A \quad (k \text{ ครั้ง})$$

และ

$$A^0 = I_n$$

ตัวอย่าง 6.21 ให้ $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$ จงหา A^5

วิธีทำ

$$A^2 = A \otimes A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$A^3 = A^2 \otimes A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

$$A^4 = A^3 \otimes A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$A^5 = A^4 \otimes A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$ □

ต่อไปจะนำการดำเนินการบูลีน มาใช้ในการหายูเนียนและอินเตอร์เซกชันของความสัมพันธ์สองความสัมพันธ์ ดังบทนิยามต่อไปนี้

บทนิยาม 6.17 ให้ r และ s เป็นความสัมพันธ์จากเซต A ไปเซต B กำหนด M_r และ M_s แทนเมทริกซ์ $0-1$ ของความสัมพันธ์ r และ s ตามลำดับ นิยาม

$$M_{r\cup s} = M_r \vee M_s \quad \text{และ} \quad M_{r\cap s} = M_r \wedge M_s$$

บทนิยาม 6.18 ให้ r เป็นความสัมพันธ์จากเซต A ไปเซต B และ s เป็นความสัมพันธ์จากเซต B ไปเซต C นิยาม

$$M_{s\circ r} = M_r \otimes M_s$$

ตัวอย่าง 6.22 ให้ r และ s เป็นความสัมพันธ์บนเซต A ซึ่งแทนด้วยเมทริกซ์ $0-1$ คือ

$$M_r = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{และ} \quad M_s = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

จงหาเมทริกซ์ $0-1$ ที่แทนความสัมพันธ์ $r \cup s$ และ $r \cap s$

วิธีทำ จากบทนิยาม 6.17 จะได้

$$M_{r\cup s} = M_r \vee M_s = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

และ $$M_{r\cap s} = M_r \wedge M_s = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$ □

ตัวอย่าง 6.23 ให้ r และ s เป็นความสัมพันธ์บนเซต A ซึ่งแทนด้วยเมทริกซ์ $0-1$ คือ

$$M_r = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \text{และ} \quad M_s = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

จงหาเมทริกซ์ $0-1$ ที่แทนความสัมพันธ์ $s \circ r$

วิธีทำ จากบทนิยาม 6.18 จะได้

$$M_{s \circ r} = M_r \otimes M_s = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

□

แบบฝึกหัดบทที่ 6

1. กำหนด $A = \begin{bmatrix} -2 & 3 & -1 \end{bmatrix}$ และ $B = \begin{bmatrix} 4 & -4 & 5 \end{bmatrix}$ จงหา

   1.1 $A + B$ และ $B + A$

   1.2 $A - B$ และ $B - A$

   1.3 $5A$ และ $-3B$

   1.4 AB และ BA

2. กำหนด $A = \begin{bmatrix} -1 \\ 1 \\ 4 \end{bmatrix}$ และ $B = \begin{bmatrix} 0 & 1 & 5 \end{bmatrix}$

   จงหา AB และ BA

3. จงหาค่าของ x, y, z และ w จากสมการ

$$\begin{bmatrix} x-y & 2w+z \\ x+y & z-w \end{bmatrix} = \begin{bmatrix} 5 & 4 \\ 3 & 1 \end{bmatrix}$$

4. กำหนด $A = \begin{bmatrix} 2 & -1 & 0 \\ 1 & 0 & 3 \end{bmatrix}$ และ $B = \begin{bmatrix} 1 & -4 & 0 & 1 \\ 2 & -1 & 3 & -1 \\ 4 & 0 & -2 & 0 \end{bmatrix}$

   จงหา AB และ BA (ถ้ามี)

5. กำหนด $A = \begin{bmatrix} 1 & 2 & 0 \\ 3 & -1 & 4 \end{bmatrix}$ จงหา

   5.1 $A + A^T$

   5.2 $3A^T - A$

   5.3 AA^T และ A^TA

6. กำหนด $A = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}$ และ $B = \begin{bmatrix} 5 & 0 \\ -6 & 7 \end{bmatrix}$ จงหา

   6.1 $(AB)^T$

   6.2 A^TB^T

   6.3 B^TA^T

7. กำหนด $A = \begin{bmatrix} 3 & 5 \\ 2 & 3 \end{bmatrix}$ และ $B = \begin{bmatrix} 3 & -5 \\ -2 & 3 \end{bmatrix}$

   จงหา AB และ BA

8. กำหนด $A = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}$ และ $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ จงหา

   8.1 A^2, A^3 และ A^4

   8.2 B^2, B^3 และ B^4

9. กำหนด $A = \begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix}$ และ $B = \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix}$

   จงแสดงว่า A และ B เป็นผกผันซึ่งกันและกัน

10. กำหนด $A = \begin{bmatrix} 5 & 3 \\ 4 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 2 & -3 \\ 1 & 3 \end{bmatrix}$ และ $C = \begin{bmatrix} -2 & 6 \\ 3 & -9 \end{bmatrix}$

    จงหาเมทริกซ์ผกผันของเมทริกซ์ทั้งสาม

11. จงพิสูจน์ทฤษฎีบทต่าง ๆ ต่อไปนี้

    11.1 ทฤษฎีบท 6.2 ข้อ (ii), (iii), (v), (vii) และ $(viii)$

    11.2 ทฤษฎีบท 6.3 ข้อ (iii) และ (v)

12. กำหนด A และ B เป็นเมทริกซ์ใด ๆ

    จงเขียนโปรแกรมเพื่อทำงานดังต่อไปนี้

    12.1 หาผลบวกของเมทริกซ์ A และ B

    12.2 หาผลต่างของเมทริกซ์ A และ B

    12.3 หาผลคูณของสเกลาร์ k กับเมทริกซ์ A

    12.4 หาผลคูณของเมทริกซ์ A และ B และหาผลคูณของเมทริกซ์ B และ A

    12.5 หาเมทริกซ์สลับเปลี่ยนของเมตริซ์ A

13. จงเขียนโปรแกรมเพื่อแสดงค่าสมาชิกทุกตัวในตำแหน่งแนวทแยงมุมของเมทริกซ์
14. กำหนดให้เมทริกซ์ประกอบด้วยสมาชิกที่มีค่า 0 และ 1

    จงเขียนโปรแกรมเพื่อเปลี่ยนค่าสมาชิกที่มีค่า 0 ให้เป็น 1 และสมาชิกที่มีค่า 1 ให้เป็น 0
15. จงเขียนโปรแกรมเพื่อสร้างเวกเตอร์แถวจากแถวที่ i และเวกเตอร์หลักจากหลักที่ j ของเมทริกซ์ที่มีขนาด $m \times n$ โดย $1 \leq i \leq m$ และ $1 \leq j \leq n$

ตัวบ่งปริมาณและตัวดำเนินการตรรกะ

ประโยคคณิตศาสตร์ที่พบทั่วไปประกอบด้วยตัวบ่งปริมาณ และตัวดำเนินการตรรกะในหลากหลายรูปแบบ

ตัวอย่าง 1 กำหนดให้เอกภพสัมพัทธ์เป็นเซตของจำนวนเต็ม

ให้ $N(x)$ แทน "x เป็นจำนวนเต็มบวกและศูนย์"

$E(x)$ แทน "x เป็นจำนวนคู่"

$O(x)$ แทน "x เป็นจำนวนคี่"

และ $P(x)$ แทน "x เป็นจำนวนเฉพาะ"

เราสามารถเขียนข้อความต่อไปนี้ในรูปประโยคสัญลักษณ์

	ข้อความ	ประโยคสัญลักษณ์
(1)	มีจำนวนเต็มที่เป็นจำนวนคู่	$\exists x[E(x)]$
(2)	จำนวนเต็มทุกจำนวนเป็นจำนวนคู่หรือจำนวนคี่	$\forall x[E(x) \vee O(x)]$
(3)	จำนวนเฉพาะทุกจำนวนเป็นจำนวนเต็มบวกและศูนย์	$\forall x[P(x) \rightarrow N(x)]$
(4)	จำนวนเฉพาะที่เป็นจำนวนคู่มีค่าเป็น 2	$\forall x[E(x) \wedge P(x)) \rightarrow x = 2]$
(5)	มีจำนวนเฉพาะเพียงจำนวนเดียวเท่านั้นที่เป็นจำนวนคู่	$\exists! x[E(x) \wedge P(x)]$
(6)	ถ้าจำนวนเต็มไม่เป็นจำนวนคู่แล้วจำนวนเต็มนั้นจะเป็นจำนวนคี่	$\forall x[\sim E(x) \rightarrow O(x)]$ □

ในประโยคคณิตศาสตร์ที่มีความซับซ้อน การใช้เครื่องหมายวงเล็บมีความสำคัญต่อการกำหนดขอบเขตของตัวบ่งปริมาณที่ใช้กำกับตัวแปร ทั้งนี้เพื่อให้ได้ความหมายของประโยคที่ถูกต้องและไม่คลุมเครือ

ตัวอย่าง 2 กำหนดให้เอกภพสัมพัทธ์เป็นเซตของจำนวนเต็ม

ให้ $P(x, y, z)$ แทน "$xy = z$"

เราสามารถเขียนแทนประโยคคณิตศาสตร์ต่อไปนี้ในรูปของประโยคสัญลักษณ์

(1) **ข้อความ** "สำหรับทุก x, ถ้า $x = 0$ แล้ว $xy = x$ สำหรับทุก y"

ประโยคสัญลักษณ์ $\forall x[x = 0 \rightarrow \forall y[P(x, y, x)]]$

$$a_3 = a_2 - a_1 = 2 - 5 = -3$$
$$a_4 = a_3 - a_2 = -3 - 2 = -5$$
$$a_5 = a_4 - a_3 = -5 + 3 = 2$$

□

ตัวอย่าง 2 กำหนดความสัมพันธ์เวียนเกิด $a_n = 2a_{n-1} - a_{n-2}$, $n = 2, 3, 4, \ldots$
จงแสดงว่า $\{a_n\}$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิดข้างต้นหรือไม่ เมื่อ

(1) $a_n = 3n$

(2) $a_n = 2^n$

(3) $a_n = 5$

วิธีทำ (1) สมมติว่า $a_n = 3n$ ทุก $n \in \mathbb{N}$ ดังนั้นสำหรับ $n \geq 2$ จะได้

$$2a_{n-1} - a_{n-2} = 2(3(n-1)) - 3(n-2) = 3n = a_n$$

นั่นคือ $\{a_n\}$ ที่ $a_n = 3n$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิดนี้

(2) สมมติว่า $a_n = 2^n$ ทุก $n \in \mathbb{N}$ ดังนั้น $a_0 = 1$, $a_1 = 2$ และ $a_2 = 4$ จะได้

$$2a_1 - a_0 = 2 \cdot 2 - 1 = 3 \neq a_2$$

นั่นคือ $\{a_n\}$ ที่ $a_n = 2^n$ ไม่เป็นผลเฉลยของความสัมพันธ์เวียนเกิดนี้

(3) สมมติว่า $a_n = 5$ ทุก $n \in \mathbb{N}$ ดังนั้นสำหรับ $n \geq 2$ จะได้

$$2a_{n-1} - a_{n-2} = 2 \cdot 5 - 5 = 5 = a_n$$

นั่นคือ $\{a_n\}$ ที่ $a_n = 5$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิดนี้ □

จะสังเกตได้ว่าการหาผลเฉลยที่เป็นลำดับของความสัมพันธ์เวียนเกิดจะต้องกำหนดเงื่อนไขเริ่มต้น แต่อย่างไรก็ตามในการหาผลเฉลยของความสัมพันธ์เวียนเกิดต้องอาศัยรูปแบบของความสัมพันธ์ ในเบื้องต้นจะพิจารณาการกำหนดรูปแบบของความสัมพันธ์เวียนเกิดและเงื่อนไขเริ่มต้นจากปัญหา ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3 จงเขียนความสัมพันธ์เวียนเกิดของเงินฝากในบัญชีในธนาคารที่ให้ดอกเบี้ยปีละ 2% (ดอกเบี้ยทบต้น) อยากทราบว่าเมื่อครบ n ปี จะมีเงินฝากในบัญชีเท่าไร เมื่อเริ่มฝากด้วยเงิน 20,000 บาท โดยไม่ถอนเงินจากบัญชีเลย พร้อมทั้งหาเงินฝากในบัญชีเมื่อครบปีที่ 3

วิธีทำ ให้ a_n เป็นจำนวนเงินในบัญชีเมื่อผ่านไป n ปี เมื่อ $a_0 = 20{,}000$

$$a_1 = 20000 + 0.02(20000)$$
$$a_2 = a_1 + 0.02a_0$$
$$\vdots$$
$$a_n = a_{n-1} + 0.02a_{n-1} = 1.02a_{n-1} \quad \text{สำหรับ } n \geq 1$$

เพราะฉะนั้น $a_3 = 1.02a_2$

เพราะว่า $a_1 = 20400$ และ $a_2 = 20808$ จะได้ $a_3 = 21224.16$ □

ตัวอย่าง 4 จงเขียนความสัมพันธ์เวียนเกิดของกระต่ายแรกเกิดเพศผู้และเพศเมียคู่หนึ่ง ถูกนำไปปล่อยไว้ที่เกาะแห่งหนึ่ง อยากทราบว่าจะมีกระต่ายทั้งหมดกี่คู่ เมื่อเวลาผ่านไป n เดือน โดยมีข้อสมมติว่าเมื่อกระต่ายทั้งสองมีอายุครบ 2 เดือน จึงสามารถให้กำเนิดกระต่ายเพศผู้ และเพศเมียอีก 1 คู่ และจุดเริ่มต้นบนเกาะยังไม่มีกระต่ายอยู่เลย

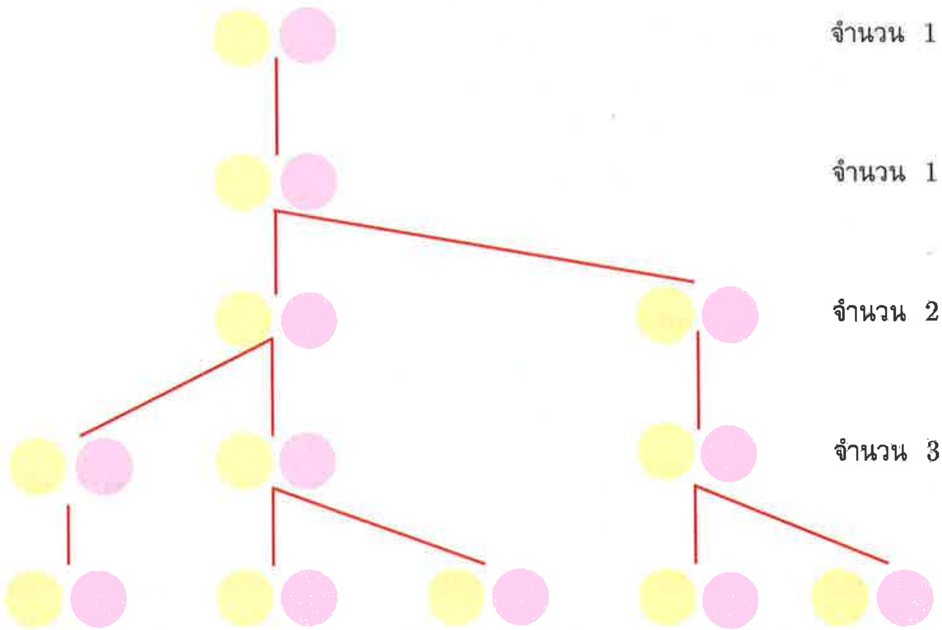
วิธีทำ ให้ a_n เป็นจำนวนกระต่าย (เป็นคู่) เมื่อครบเดือนที่ n โดยที่ $a_0 = 0,\ a_1 = 1$ และ $a_2 = 1$

เดือนที่ 1 จำนวน 1 คู่

เดือนที่ 2 จำนวน 1 คู่

เดือนที่ 3 จำนวน 2 คู่

เดือนที่ 4 จำนวน 3 คู่



เดือนที่ 5 จำนวน 5 คู่

จากรูปจะได้ $a_3 = 2 = a_2 + a_1,\ a_4 = 3 = a_3 + a_2,\ a_5 = 5 = a_4 + a_3,\ \ldots$

นั่นคือ $a_n = a_{n-1} - a_{n-2}$ สำหรับ $n \geq 2$ □

ตัวอย่าง 5 โรงงานผลิตรถตู้แห่งหนึ่งสามารถผลิตรถตู้ ได้มากกว่าเดิม 1 คันทุกๆ เดือน นั่นคือ เดือนที่ 1 ผลิตได้ 1 คัน เดือนที่ 2 ได้ 2 คันเป็นเช่นนี้ไปเรื่อยๆ จนถึงเดือนที่ n ผลิตได้ n คัน จงเขียนความสัมพันธ์เวียนเกิดที่บริษัทนี้จะผลิตรถตู้ได้ใน n เดือนแรก

วิธีทำ ให้ a_n เป็นจำนวนรถตู้ที่ผลิตได้ในเดือนที่ n เมื่อ $a_0 = 0$ และ $a_1 = 1$

จะได้ $a_2 = 1 + 2 = a_1 + 2,\ a_3 = 3 + 3 = a_2 + 3,\ \ldots$

ดังนั้น $a_n = a_{n-1} + n,\ n \geq 1$ □

ตัวอย่าง 6 จงเขียนความสัมพันธ์เวียนเกิดของจำนวนวิธีที่ชายคนหนึ่งจะขึ้นบันไดไปนมัสการรอยพระพุทธบาท จังหวัดสระบุรีจำนวน n ขั้น ถ้าในการก้าวขึ้นบันได 1 ครั้ง เขาอาจจะขึ้นบันไดได้ทีละ 1 ขั้น หรือ 2 ขั้น

วิธีทำ ให้ a_n เป็นจำนวนวิธีในการขึ้นบันได n ขั้น เมื่อ $a_1 = 1$ และ $a_2 = 2$
(จำนวนวิธีเป็น 2 เพราะ วิธีที่ 1 ขึ้นทีละขั้น วิธีที่ 2 ขึ้นครั้งเดียว 2 ขั้น)
ถ้าให้ขึ้นบันไดครั้งแรกเป็น 1 ขั้น จะเหลือบันไดจำนวน $n-1$ ขั้น
ซึ่งมีจำนวนวิธีในการขึ้นบันไดเป็น a_{n-1} วิธี
ถ้าให้ขึ้นบันไดครั้งแรกเป็น 2 ขั้น จะเหลือบันไดจำนวน $n-2$ ขั้น
ซึ่งมีจำนวนวิธีในการขึ้นบันไดเป็น a_{n-2} วิธี
โดยทั้งสองกรณีไม่มีวิธีขึ้นซ้ำกันเลย
ดังนั้น $a_n = a_{n-1} + a_{n-2}$ สำหรับ $n \geq 2$ □

ตัวอย่าง 7 เครื่องขายแสตมป์อัตโนมัติแห่งหนึ่งรับเฉพาะเหรียญ 1 บาท เหรียญ 5 บาท และเหรียญ 10 บาท เท่านั้น จงเขียนความสัมพันธ์เวียนเกิดของจำนวนวิธีที่จะหยอดเหรียญเงินทั้งหมด n บาท เพื่อซื้อแสตมป์จากตู้นี้ สมมติว่าจำนวนเหรียญแบบต่างๆ มีได้ไม่จำกัด

วิธีทำ ให้ a_n คือ จำนวนวิธีหยอดเหรียญเป็นจำนวนมูลค่า n บาท ถ้ามีเหรียญ 3 ชนิด คือ 1, 5 และ 10 วิธีการใส่เงินมีวิธีได้ 3 วิธีที่แตกต่างกัน
<u>วิธีที่ 1</u> หยอดเหรียญ 1 บาท ก่อน จะเหลือเงิน $n-1$ บาท ที่ต้องหยอดซึ่งมีจำนวนวิธีทั้งสิ้น a_{n-1}
<u>วิธีที่ 2</u> หยอดเหรียญ 5 บาท ก่อน จะเหลือเงิน $n-5$ บาท ที่ต้องหยอดซึ่งมีจำนวนวิธีทั้งสิ้น a_{n-5}
<u>วิธีที่ 3</u> หยอดเหรียญ 10 บาท ก่อน จะเหลือเงิน $n-10$ บาท ที่ต้องหยอดซึ่งมีจำนวนวิธีทั้งสิ้น a_{n-10}
แต่ละเหตุการณ์ไม่มีวิธีใดทำซ้ำกันเลย
ดังนั้น $a_n = a_{n-1} + a_{n-5} + a_{n-10}$ □

การหาผลเฉลยในหัวข้อนี้จะพิจารณาแค่เพียงเบื้องต้นเท่านั้น โดยพิจารณาจากความสัมพันธ์เวียนเกิดที่มีรูปแบบเฉพาะ ดังบทนิยามและทฤษฎีบทต่อไปนี้

บทนิยาม 2 กำหนดความสัมพันธ์เวียนเกิดของ $a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$ จะเรียกความสัมพันธ์นี้ว่าเป็น **ความสัมพันธ์เวียนเกิดอันดับที่ k** ก็ต่อเมื่อ a_n เขียนแทนด้วยพจน์ก่อนหน้าไกลสุดถึงตัวที่ a_{n-k}

ตัวอย่างเช่น ความสัมพันธ์เวียนเกิด $a_n = 2a_{n-1} - 3a_{n-3}$ เป็นความสัมพันธ์อันดับ 3
$a_n = 4a_{n-5} + n^2 + 1$ เป็นความสัมพันธ์อันดับ 5

การหาผลเฉลยของความสัมพันธ์เวียนเกิดอันดับหนึ่ง

ความสัมพันธ์เวียนเกิดอันดับหนึ่งในรูปทั่วไปคือ $a_n = f(a_{n-1})$ ผลเฉลยอาจทำได้โดยลองคำนวณค่าจากจำนวนในลำดับ แล้วสร้างความสัมพันธ์จากลำดับที่เกิดขึ้นซึ่งค่อนข้างยาก เพราะต้องอาศัยปุ่นัยเชิงคณิตศาสตร์เข้ามาช่วยในการตัดสินใจ

ในที่นี้จะศึกษาการหาผลเฉลยโดยใช้ความรู้ทางพีชคณิต โดยการกระจายพจน์ a_i ต่าง ๆ ในความสัมพันธ์ด้วยความสัมพันธ์ที่เขียนด้วยพจน์ก่อนหน้า ทำไปเรื่อย ๆ จนถึงค่าเริ่มต้นและใช้ความรู้ในการหาผลรวมหรือผลคูณ เพื่อให้อยู่ในพจน์ของ n

ตัวอย่าง 8 กำหนดความสัมพันธ์เวียนเกิดอันดับหนึ่ง

$$a_n = 2a_{n-1} + 1 \quad \text{เมื่อ} \quad a_0 = 0$$

จงหาผลเฉลย พร้อมทั้งหา a_8 ด้วย

วิธีทำ จาก

$$\begin{aligned}
a_n &= 2a_{n-1} + 1 \\
&= 2(2a_{n-1} + 1) + 1 \\
&= 2(2(2a_{n-2} + 1) + 1) + 1 \\
&\vdots \\
&= 2(2(2(\cdots(2a_0 + 1)\cdots) + 1) + 1) + 1 \\
&= 2^n a_0 + 2^{n-1} + 2^{n-2} + \cdots + 2^2 + 1 \\
&= 2^{n-1} + 2^{n-2} + \cdots + 2^1 + 1 \\
&= \frac{1(1-2^n)}{1-2} \\
&= 2^n - 1
\end{aligned}$$

ดังนั้น $a_n = 2^n - 1$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิดในพจน์ของ n

จะได้ $a_8 = 2^8 - 1 = 255$ □

ตัวอย่าง 9 จงหาผลเฉลยของความสัมพันธ์เวียนเกิด

$$a_n = a_{n-1} + n \quad \text{เมื่อ} \quad a_0 = 1$$

วิธีทำ จาก

$$\begin{aligned}
a_n &= a_{n-1} + n \\
&= (a_{n-2} + n - 1) + n \\
&= (a_{n-3} + n - 2) + n - 1 + n \\
&\vdots \\
&= (a_0 + 1) + 2 + \cdots + (n-1) + n \\
&= a_0 + \sum_{i=1}^{n} i \\
&= 1 + \frac{n(n+1)}{2}
\end{aligned}$$

$$= \frac{n^2+n+2}{2}$$

ดังนั้น $a_n = \dfrac{n^2+n+2}{2}$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิดในพจน์ของ n □

ตัวอย่าง 10 จงหาผลเฉลยของความสัมพันธ์เวียนเกิดของ

$p_n = (1.11)p_{n-1}$ เมื่อ $p_0 = 10,000$

วิธีทำ จาก

$$\begin{aligned} p_n &= (1.11)p_{n-1} \\ &= (1.11)((1.11)p_{n-2}) \\ &= (1.11)(1.11)((1.11)p_{n-3}) \\ &\vdots \\ &= (1.11)^n p_0 \end{aligned}$$

ดังนั้น $p_n = (1.11)^n p_0$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิดในพจน์ของ n □

ต่อไปจะพิจารณาการหาผลเฉลยของความสัมพันธ์เวียนเกิดที่มีอันดับมากกว่าหนึ่ง ซึ่งมีความยุ่งยากมากขึ้น โดยกำหนดลักษณะของความสัมพันธ์ให้อยู่ในรูปความสัมพันธ์เชิงเส้นดังบทนิยามและทฤษฎีบทต่อไปนี้

บทนิยาม 3 ความสัมพันธ์เวียนเกิดของ $a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$ เป็น**ความสัมพันธ์เวียนเกิดเชิงเส้น** ก็ต่อเมื่อ f เป็นฟังก์ชันเชิงเส้นของพจน์ก่อนหน้า

ตัวอย่างเช่น

ความสัมพันธ์เวียนเกิดเชิงเส้น	ความสัมพันธ์เวียนเกิดไม่เชิงเส้น
$a_n = 2a_{n-1} - 3a_{n-3} + 5$	$a_n = \dfrac{a_{n-1}}{2a_{n-2} - 3} + 4$
$a_n = 2a_{n-1} - 3a_{n-3} + n^2 + 1$	$a_n = 2a_{n-1}^2 - 3a_{n-3}$ เป็นต้น

บทนิยาม 4 ความสัมพันธ์เวียนเกิด $a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$ เป็น**ความสัมพันธ์เวียนเกิดเอกพันธุ์** ก็ต่อเมื่อ $f(0, 0, \ldots, 0) = 0$ หรือทุก ๆ พจน์ก่อนหน้าที่ไม่เป็นศูนย์ มีพจน์ a_i คูณอยู่ด้วย

ตัวอย่างเช่น $a_n = 2a_{n-1} - 3a_{n-3}$ เป็นความสัมพันธ์เวียนเกิดเอกพันธุ์
แต่ถ้า $a_n = 2a_{n-1} - 3a_{n-3} + n^2 + 1$ แล้วความสัมพันธ์เวียนเกิดนี้ไม่เป็นความสัมพันธ์เวียนเกิดเอกพันธุ์
เพราะ ถ้า $a_{n-1} = 0$ และ $a_{n-3} = 0$ แล้ว $a_n \neq 0$

หมายเหตุ สัมประสิทธิ์ที่คูณด้วยพจน์ a_i อาจจะเป็นค่าคงตัวหรือไม่ใช่ก็ได้ ตัวอย่างเช่น

$a_n = 2a_{n-1} - 3a_{n-3}$ เป็นความสัมพันธ์เวียนเกิดเอกพันธ์ที่สัมประสิทธิ์เป็นค่าคงตัว

แต่ $a_n = 2na_{n-1} - (3n^2 + 1)a_{n-3}$ เป็นความสัมพันธ์เวียนเกิดเอกพันธ์ที่สัมประสิทธิ์ไม่เป็นค่าคงตัว

ผลเฉลยของความสัมพันธ์เวียนเกิดเชิงเส้นเอกพันธุ์สัมประสิทธิ์เป็นค่าคงตัวอันดับ k

การหาผลเฉลยของความสัมพันธ์เวียนเกิดเชิงเส้นเอกพันธุ์สัมประสิทธิ์เป็นค่าคงตัวอันดับ k จะยุ่งยากกว่าอันดับหนึ่ง โดยพิจารณาความสัมพันธ์แทนด้วย

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$$

เมื่อ $c_1, c_2, \ldots, c_k \in \mathbb{R}$ ที่ $c_i \neq 0$ บาง $i \leq k$

สมมติให้รูปแบบผลเฉลยคือ $a_n = r^n,\ r \in \mathbb{R}$

แทน $a_n = r^n$ ในความสัมพันธ์เวียนเกิดจะได้

$$r^n = c_1r^{n-1} + c_2r^{n-2} + \cdots + c_kr^{n-k}$$

$$r^n \cdot r^{n-k} = c_1r^{k-1}r^{n-k} + c_2r^{k-2}r^{n-k} + \cdots + c_{k-1}rr^{n-k} + c_kr^{n-k}$$

หารตลอดด้วย r^{n-k} จะได้

$$r^k = c_1r^{k-1} + c_2r^{k-2} + \cdots + c_k$$

หรือ

$$r^k - c_1r^{k-1} - c_2r^{k-2} - \cdots - c_k = 0 \qquad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

เรียกสมการ (1) ว่า **สมการลักษณะของความสัมพันธ์เวียนเกิด** รากของสมการ (1) จะเป็นตัวกำหนดผลเฉลยของความสัมพันธ์เวียนเกิด เรียกรากของสมการ (1) ว่า **รากลักษณะ** ดังนั้น

$a_n = r^n$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิดเชิงเส้นเอกพันธุ์สัมประสิทธิ์เป็นค่าคงตัว ก็ต่อเมื่อ r เป็นรากของสมการลักษณะของความสัมพันธ์เวียนเกิดนี้

เนื่องจากรากลักษณะของความสัมพันธ์เวียนเกิดเชิงเส้นเอกพันธุ์สัมประสิทธิ์เป็นค่าคงตัวอันดับ k มีมากกว่าหนึ่งรากดังนั้นการพิจารณาผลเฉลยทั่วไปจะขึ้นกับรากดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 1 ให้ $c_1, c_2, \ldots, c_k$ เป็นจำนวนจริง สมมติสมการลักษณะ

$$r^k - c_1r^{k-1} - c_2r^{k-2} - \cdots - c_k = 0$$

มีรากลักษณะที่แตกต่างกัน k ราก คือ $r_1, r_2, \ldots, r_k$

แล้วลำดับ $\{a_n\}$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิด

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$$

ก็ต่อเมื่อ $a_n = \alpha_1r_1^n + \alpha_2r_2^n + \cdots + \alpha_kr_k^n$ สำหรับ $n = 1, 2, \ldots$

เมื่อ $\alpha_1, \alpha_2, \ldots, \alpha_k$ เป็นจำนวนจริง

ตัวอย่าง 11 กำหนดความสัมพันธ์เวียนเกิด

$$a_n = 2a_{n-1} + 3a_{n-2} \qquad \text{เมื่อ } a_0 = 1,\ a_1 = 1$$

จงหาผลเฉลยของความสัมพันธ์เวียนเกิด

วิธีทำ จากความสัมพันธ์เวียนเกิด

$a_n = 2a_{n-1} + 3a_{n-2}$ เป็นความสัมพันธ์เวียนเกิดเชิงเส้นเอกพันธุ์อันดับ 2

สมการลักษณะคือ $r^2 - 2r - 3 = 0$

รากลักษณะคือ $r = -1, 3$ เป็นรากแตกต่าง

ผลเฉลยทั่วไปคือ $a_n = \alpha_1(-1)^n + \alpha_2 3^n$

จากเงื่อนไขเริ่มต้น $a_0 = 1,\ a_1 = 1$ จะได้

$$a_0 = \alpha_1(-1)^0 + \alpha_2 3^0 \quad \Rightarrow \quad \alpha_1 + \alpha_2 = 1 \qquad \text{............(1)}$$

$$a_1 = \alpha_1(-1)^1 + \alpha_2 3^1 \quad \Rightarrow \quad -\alpha_1 + 3\alpha_2 = 1 \qquad \text{............(2)}$$

แก้สมการ (1) และ (2) เพื่อหาค่า α_1 และ α_2 จะได้ $\alpha_1 = \alpha_2 = \frac{1}{2}$

ดังนั้นผลเฉลยคือ $a_n = \frac{1}{2}(-1)^n + \frac{1}{2}3^n = \frac{1}{2}((-1)^n + 3^n),\ n \geq 2$ □

ตัวอย่าง 12 กำหนดความสัมพันธ์เวียนเกิด

$$a_n = 7a_{n-2} + 6a_{n-3} \qquad \text{เมื่อ } a_0 = 9,\ a_1 = 10,\ a_2 = 32$$

จงหาผลเฉลยของความสัมพันธ์เวียนเกิด

วิธีทำ จาก $a_n = 7a_{n-2} + 6a_{n-3}$ เป็นความสัมพันธ์เวียนเกิดเชิงเส้นเอกพันธุ์อันดับ 3

สมการลักษณะคือ $r^3 - 7r - 6 = 0$

รากลักษณะคือ $r = -1, -2, 3$

ผลเฉลยทั่วไปคือ $a_n = \alpha_1(-1)^n + \alpha_2(-2)^n + \alpha_3 3^n$

จากเงื่อนไขเริ่มต้น $a_0 = 9,\ a_1 = 10,\ a_2 = 32$ จะได้

$$\alpha_1 + \alpha_2 + \alpha_3 = 9 \qquad \text{............(1)}$$

$$\alpha_1 - 2\alpha_2 + 3\alpha_3 = 10 \qquad \text{............(2)}$$

$$\alpha_1 + 4\alpha_2 + 9\alpha_3 = 32 \qquad \text{............(3)}$$

จากสมการ (1) – (3) จะได้ $\alpha_1 = 8,\ \alpha_2 = -3$ และ $\alpha_3 = 4$

ดังนั้นผลเฉลยคือ $a_n = 8(-1)^n - 3(-2)^n + 4(3^n),\ n \geq 3$ □

ทฤษฎีบท 2 ให้ $c_1, c_2, \ldots, c_k$ เป็นจำนวนจริง สมมติสมการลักษณะ

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0$$

มีรากลักษณะที่ซ้ำกัน k ราก คือ $r_1 = r_2 = \ldots = r_k$

แล้วลำดับ $\{a_n\}$ เป็นผลเฉลยของความสัมพันธ์เวียนเกิด

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

ก็ต่อเมื่อ $a_n = (\alpha_1 + \alpha_2 n + \alpha_3 n^2 + \cdots + \alpha_k n^{k-1}) r_1^n$ สำหรับ $n = 1, 2, \ldots$

เมื่อ $\alpha_1, \alpha_2, \ldots, \alpha_k$ เป็นจำนวนจริง

ตัวอย่าง 13 จงหาผลเฉลยของความสัมพันธ์เวียนเกิด

$$a_n = 6a_{n-1} - 9a_{n-2} \qquad \text{เมื่อ } a_0 = 1,\ a_1 = 6$$

วิธีทำ จาก $a_n = 6a_{n-1} - 9a_{n-2}$ เป็นความสัมพันธ์เวียนเกิดเชิงเส้นเอกพันธุ์อันดับ 2

สมการลักษณะคือ $r^2 - 6r + 9 = 0$

รากลักษณะคือ $r = 3, 3$

ผลเฉลยทั่วไปคือ $a_n = \alpha_1 3^n + \alpha_2 n 3^n$

จากเงื่อนไขเริ่มต้น $a_0 = 1,\ a_1 = 6$ จะได้

$$\alpha_1 = 1 \qquad \text{............(1)}$$

$$3\alpha_1 + 3\alpha_2 = 6 \qquad \text{............(2)}$$

จากสมการ (1) และ (2) จะได้ $\alpha_1 = \alpha_2 = 1$

ดังนั้นผลเฉลยคือ $a_n = 3^n + n3^n = (1+n)3^n,\ n \geq 2$ □

ตัวอย่าง 14 กำหนดความสัมพันธ์เวียนเกิด

$$a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3} \quad \text{เมื่อ } a_0 = 1,\ a_1 = -2,\ a_2 = -1$$

จงหาผลเฉลยของความสัมพันธ์เวียนเกิด

วิธีทำ จาก $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ เป็นความสัมพันธ์เวียนเกิดเชิงเส้นเอกพันธุ์อันดับ 3

สมการลักษณะคือ $r^3 + 3r^2 + 3r + 1 = 0$

รากลักษณะคือ $r = -1, -1, -1$

ผลเฉลยทั่วไปคือ $a_n = \alpha_1(-1)^n + \alpha_2 n(-1)^n + \alpha_3 n^2(-1)^n$

จากเงื่อนไขเริ่มต้น $a_0 = 1,\ a_1 = -2,\ a_2 = -1$ จะได้

$$\alpha_1 = 1 \qquad \text{............(1)}$$

$$-\alpha_1 - \alpha_2 - \alpha_3 = -2 \qquad \text{............(2)}$$

$$\alpha_1 + 2\alpha_2 + 4\alpha_3 = -1 \qquad \text{............(3)}$$

จากสมการ (1) – (3) จะได้ $\alpha_1 = 1,\ \alpha_2 = 3$ และ $\alpha_3 = -2$

ดังนั้นผลเฉลยคือ $a_n = (1 + 3n - 2n^2)(-1)^n,\ n \geq 3$ □

ยุคลิดแห่งอะเล็กซานเดรีย
ประมาณ 450 – 380 ปีก่อนคริสต์ศักราช , กรีซ

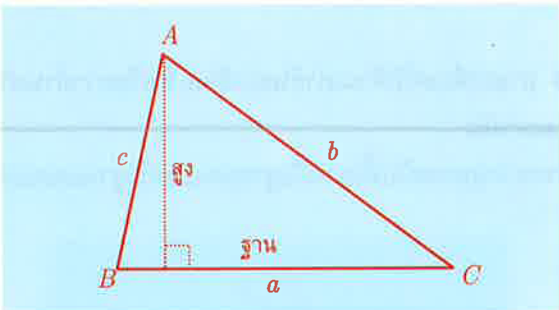
เรขาคณิตคำนวณเบื้องต้น

ในที่นี้จะเป็นการรวบรวมสูตรเกี่ยวกับการคำนวณของรูปทรงเรขาคณิตต่าง ๆ ซึ่งประกอบด้วยพื้นที่ของรูปเหลี่ยม พื้นที่ของวงกลม ปริมาตรของทรงกลม ปริมาตรของทรงกระบอก ปริมาตรของปริซึม ปริมาตรของรูปพีระมิด และเรขาคณิตในสองมิติเบื้องต้น

พื้นที่ของรูปเหลี่ยมและวงกลม

รูปสามเหลี่ยม

กำหนดให้รูปสามเหลี่ยม ABC มีด้านยาว a, b และ c หน่วย ดังรูป 1



รูป 1 สามหลี่ยมใด ๆ

ส่วนสูงของรูปสามเหลี่ยม คือ ความยาวของเส้นตรงที่ลากจากมุมยอดมาตั้งฉากกับฐาน
เส้นมัธยฐานของรูปสามเหลี่ยม คือ เส้นตรงที่ลากจากมุมยอดมายังจุดกึ่งกลางฐาน

$$\text{พื้นที่รูปสามเหลี่ยม} = \frac{1}{2} \times \text{ฐาน} \times \text{สูง}$$

หรือ พื้นที่รูปสามเหลี่ยม $= \sqrt{s(s-a)(s-b)(s-c)}$ เมื่อ $s = \dfrac{a+b+c}{2}$

ให้ R และ r เป็นรัศมีวงกลมที่ล้อมรอบและแนบในรูปสามเหลี่ยม ABC จะได้

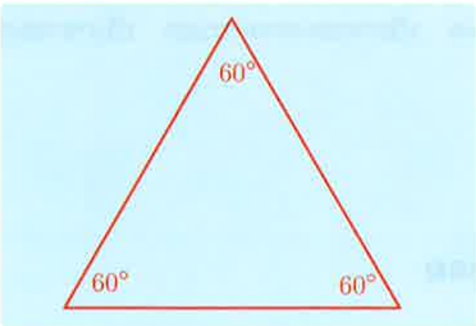
พื้นที่รูปสามเหลี่ยม $= \dfrac{abc}{4R} = rs$

รูปสามเหลี่ยมจำแนกตามสมบัติต่าง ๆ ดังนี้

1. **สามเหลี่ยมด้านเท่า** หมายถึง สามเหลี่ยมที่มีด้านเท่ากันทุกด้าน

จะได้ว่า *(i)* มุมเท่ากันทุกมุม แต่ละมุมเท่ากับ 60 องศา

(ii) เส้นมัธยฐานตั้งฉากกับฐาน



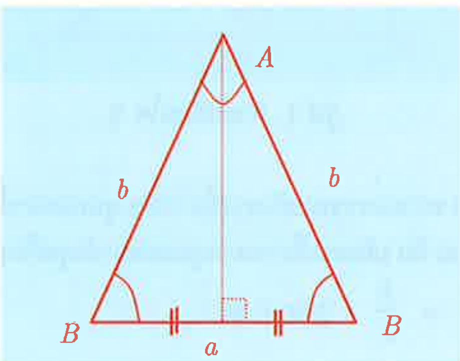
รูป 2 สามเหลี่ยมด้านเท่า

พื้นที่รูปสามเหลี่ยมด้านเท่า $= \dfrac{\sqrt{3}}{4} \times (\text{ด้าน})^2$

2. **สามเหลี่ยมหน้าจั่ว** หมายถึง สามเหลี่ยมที่มีด้านเท่ากันสองด้าน ซึ่งเรียกว่าด้านประกอบมุมยอด

จะได้ว่า *(i)* มุมที่ฐานเท่ากัน

(ii) เส้นที่ลากจากมุมยอดไปตั้งฉากกับฐานจะแบ่งครึ่งฐานและแบ่งครึ่งมุมยอดด้วย



รูป 3 สามเหลี่ยมหน้าจั่ว

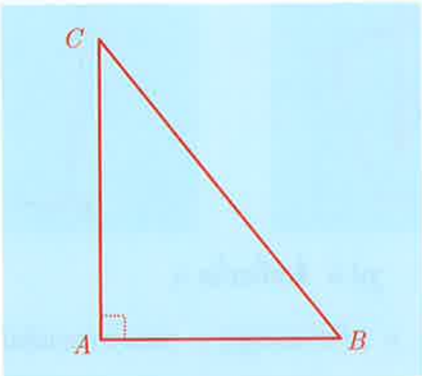
เรียกด้าน a ว่า **ฐาน** และเรียกด้าน b ว่า **ด้านประกอบมุมยอด**
เรียกมุม A ว่า **มุมยอด** และมุม B ว่า **มุมที่ฐาน**

$$\text{พื้นที่รูปสามเหลี่ยมหน้าจั่ว} = \frac{a}{4}\sqrt{4b^2 - a^2}$$

3. สามเหลี่ยมมุมฉาก หมายถึง สามเหลี่ยมที่มีมุมมุมหนึ่งเป็นมุมฉาก

จะได้ว่า ผลบวกของกำลังสองของด้านประกอบมุมฉากเท่ากับด้านตรงข้ามมุมฉากยกกำลังสอง จัตุรัสด้านตรงข้ามมุมฉาก เท่ากับ จัตุรัสบนด้านประกอบมุมฉากรวมกัน

หรือ ด้านตรงข้ามมุมฉากยกกำลังสอง เท่ากับ ผลบวกของกำลังสองของด้านประกอบมุมฉาก



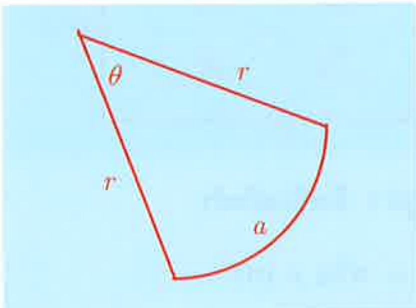
รูป 4 สามเหลี่ยมมุมฉาก

เรียกด้าน AB และ AC ว่า **ด้านประกอบมุมฉาก** และเรียกด้าน BC ว่า **ด้านประกอบมุมฉาก**

$$\text{พื้นที่ของรูปสามเหลี่ยมมุมฉาก} = \frac{1}{2} \times \text{ผลคูณของด้านประกอบมุมฉาก}$$

$$BC^2 = AB^2 + AC^2$$

4. สามเหลี่ยมฐานโค้ง หมายถึง สามเหลี่ยมที่มีจุดยอดอยู่ที่จุดศูนย์กลางของวงกลมและฐานเป็นส่วนของเส้นรอบวงของวงกลม



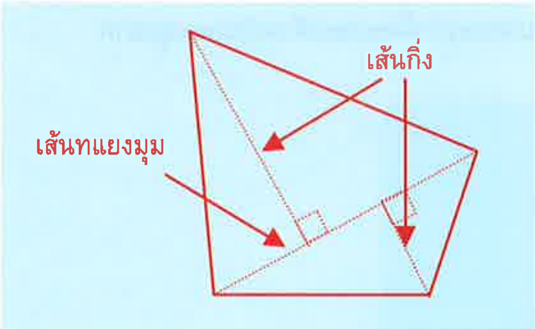
รูป 5 สามเหลี่ยมฐานโค้ง

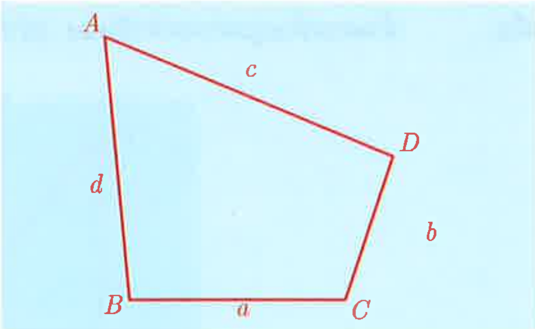
$$\text{พื้นที่รูปสามเหลี่ยมฐานโค้ง} = \frac{1}{2}ra$$

$$= \frac{1}{2}r^2\theta, \quad \text{เมื่อ } a = r\theta$$

รูปสี่เหลี่ยม

กำหนดให้รูปสามเหลี่ยม $ABCD$ มีด้านยาว a, b, c และ d หน่วย ดังรูป 7.6
เส้นทแยงมุม หมายถึง เส้นตรงที่ลากจุดมุมไปยังที่อยู่ตรงกันข้าม
เส้นกิ่ง หมายถึง เส้นตรงที่ลากจากมุมไปตั้งฉากกับเส้นทแยงมุม



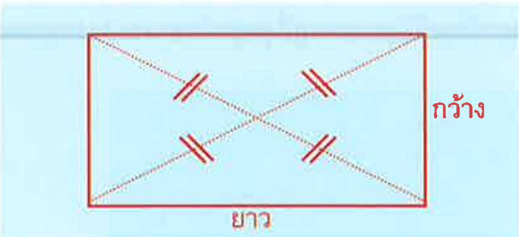


รูป 6 สี่เหลี่ยมใด ๆ

$$\text{พื้นที่รูปสี่เหลี่ยม} = \frac{1}{2} \times (\text{เส้นทแยงมุม}) \times (\text{ผลบวกของเส้นกิ่ง})$$

รูปสี่เหลี่ยมจำแนกตามสมบัติต่าง ๆ ดังนี้

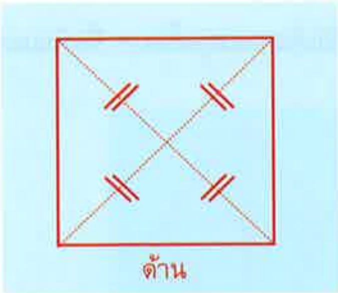
1. **สี่เหลี่ยมผืนผ้า** หมายถึง สี่เหลี่ยมที่มีมุมทุกมุมเป็นมุมฉาก
   จะได้ว่า เส้นทแยงมุมยาวเท่ากัน และแบ่งครึ่งซึ่งกันและกัน



รูป 7 สี่เหลี่ยมผืนผ้า

$$\text{พื้นที่รูปสี่เหลี่ยมผืนผ้า} = \text{กว้าง} \times \text{ยาว}$$

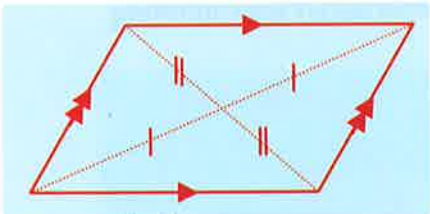
2. **สี่เหลี่ยมจัตุรัส** หมายถึง สี่เหลี่ยมที่มีมุมทุกมุมเป็นมุมฉาก และมีด้านเท่ากันทุกด้าน
   จะได้ว่า เส้นทแยงมุมยาวเท่ากัน ตั้งฉากและแบ่งครึ่งซึ่งกันและกัน



รูป 8 สี่เหลี่ยมจัตุรัส

$$\text{พื้นที่รูปสี่เหลี่ยมจัตุรัส} = (\text{ด้าน})^2$$

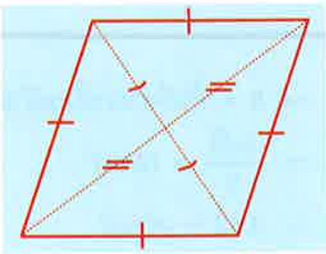
3. **สี่เหลี่ยมด้านขนาน** หมายถึง สี่เหลี่ยมที่มีด้านตรงข้ามขนานกันสองคู่
จะได้ว่า เส้นทแยงมุมแบ่งครึ่งซึ่งกันและกัน



รูป 9 สี่เหลี่ยมด้านขนาน

$$\text{พื้นที่รูปสี่เหลี่ยมด้านขนาน} = \text{ฐาน} \times \text{สูง}$$

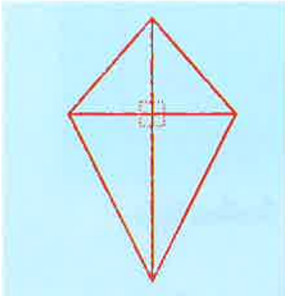
4. **สี่เหลี่ยมขนมเปียกปูน** หมายถึง สี่เหลี่ยมที่มีด้านเท่ากันทุกด้าน
จะได้ว่า เส้นทแยงมุมตั้งฉาก และแบ่งครึ่งซึ่งกันและกัน



รูป 10 สี่เหลี่ยมขนมเปียกปูน

$$\text{พื้นที่รูปสี่เหลี่ยมขนมเปียกปูน} = \text{ฐาน} \times \text{สูง} = \frac{1}{2} \times (\text{ผลคูณของเส้นทแยงมุม})$$

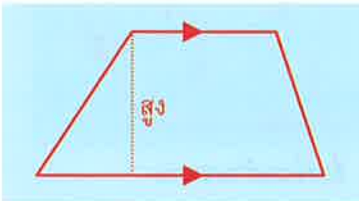
5. สี่เหลี่ยมรูปว่าว หมายถึง สี่เหลี่ยมที่มีเส้นทแยงมุมตั้งฉาก ซึ่งกันและกัน



รูป 11 สี่เหลี่ยมรูปว่าว

$$\text{พื้นที่รูปสี่เหลี่ยมรูปว่าว} = \frac{1}{2} \times (\text{ผลคูณของเส้นทแยงมุม})$$

6. สี่เหลี่ยมคางหมู หมายถึง สี่เหลี่ยมที่มีด้านตรงข้ามขนานกันหนึ่งคู่

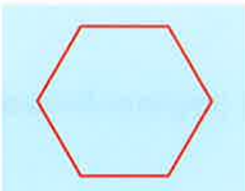


รูป 12 สี่เหลี่ยมคางหมู

$$\text{พื้นที่รูปสี่เหลี่ยมคางหมู} = \frac{1}{2} \times (\text{ผลบวกของด้านคู่ขนาน}) \times \text{สูง}$$

รูปหลายเหลี่ยมด้านเท่า

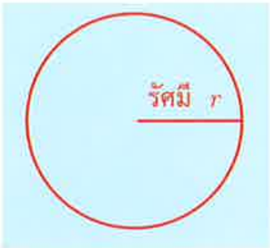
$$\begin{aligned}
\text{พื้นที่รูปหกเหลี่ยมด้านเท่า} &= 6 \times \text{พื้นที่สามเหลี่ยมด้านเท่า} \\
&= \frac{3\sqrt{3}}{2} \times (\text{ด้าน})^2 \\
\text{พื้นที่รูปแปดเหลี่ยมด้านเท่า} &= 4.82 \times (\text{ด้าน})^2
\end{aligned}$$



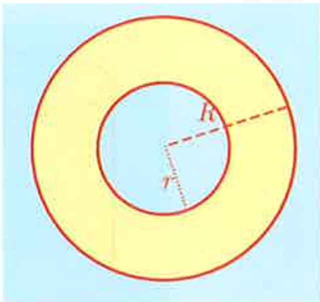
รูป 13 หกเหลี่ยมด้านเท่า

รูป 14 แปดเหลี่ยมด้านเท่า

รูปวงกลมและรูปวงแหวน



รูป 15 วงกลม



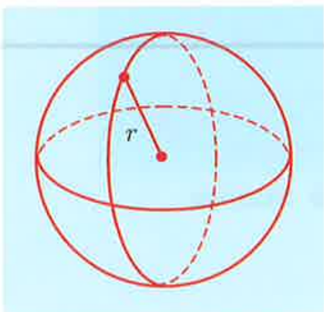
รูป 16 วงแหวน

เส้นรอบวงของวงกลม $= 2\pi r$
พื้นที่วงกลม $= \pi r^2$
พื้นที่วงแหวน $= \pi(R^2 - r^2)$
เมื่อ R เป็นรัศมีวงกลมวงนอก และ r เป็นรัศมีวงกลมวงใน

ปริมาตรและพื้นผิวของรูปทรงสามมิติ

รูปทรงกลม

เมื่อ r เป็นความยาวรัศมีของทรงกลม



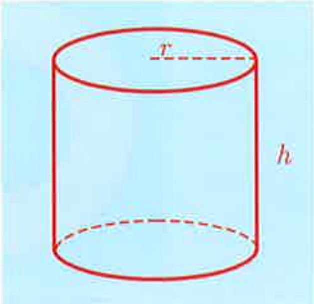
รูป 17 ทรงกลม

พื้นที่ผิวทรงกลม $= 4\pi r^2$

ปริมาตรทรงกลม $= \dfrac{4}{3}\pi r^3$

รูปทรงกระบอก

เมื่อ r เป็นความยาวรัศมี และ h เป็นความสูงของทรงกระบอก

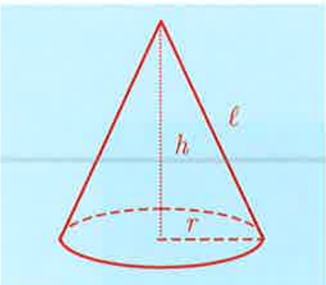


รูป 18 ทรงกระบอก

$$
\begin{aligned}
\text{พื้นที่ผิวข้าง} &= 2\pi rh \\
\text{พื้นที่ผิวทั้งหมด} &= 2\pi rh + 2\pi r^2 = 2\pi r(h+r) \\
\text{ปริมาตร} &= \pi r^2 h
\end{aligned}
$$

รูปกรวยกลมตรง

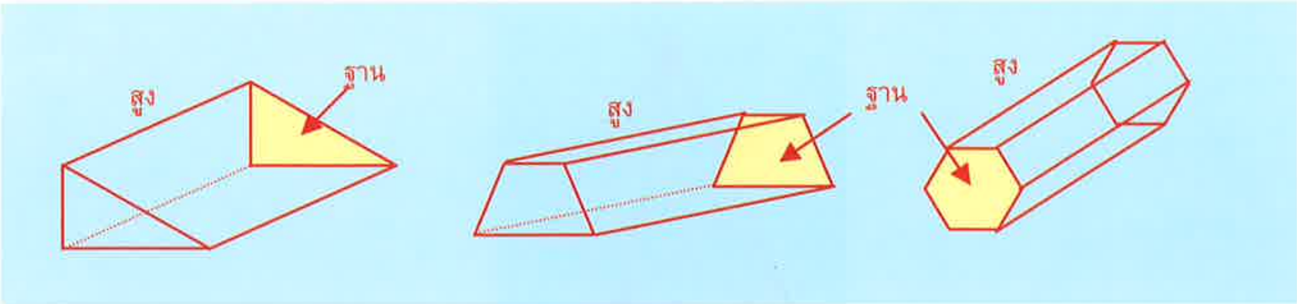
เมื่อ r เป็นความยาวรัศมี และ h เป็นความสูงของทรงกระบอก และ ℓ เป็นสูงเอียง



รูป 19 กรวยกลม

$$
\begin{aligned}
\text{พื้นที่ผิวข้าง} &= \pi r\ell \\
\text{พื้นที่ผิวทั้งหมด} &= \pi r\ell + \pi r^2 = \pi r(\ell + r) \\
\text{ปริมาตร} &= \frac{1}{3}\pi r^2 h \\
\ell &= \sqrt{h^2 + r^2}
\end{aligned}
$$

รูปปริซึม



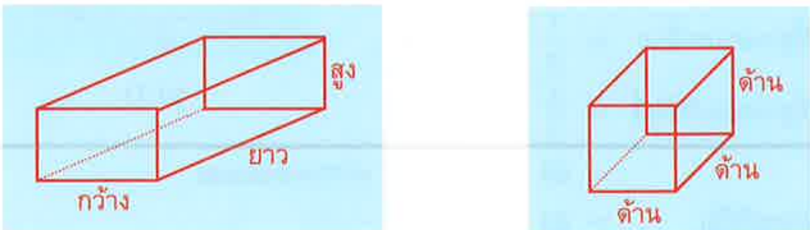
(1) ปริซึมฐานสามเหลี่ยมมุมฉาก (2) ปริซึมฐานสี่เหลี่ยมคางหมู (3) ปริซึมฐานหกเหลี่ยม

รูป 20 ปริซึม

พื้นที่ผิวข้าง	=	เส้นรอบฐาน × สูง
พื้นที่ผิวทั้งหมด	=	พื้นที่ผิวข้าง + 2(พื้นที่ฐาน)
ปริมาตร	=	พื้นที่ฐาน × สูง

รูปทรงสี่เหลี่ยมมุมฉาก

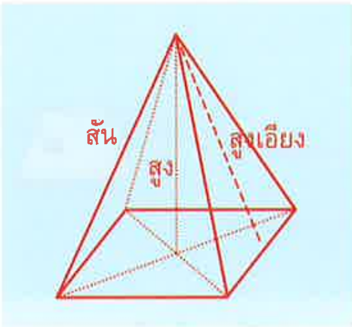
รูปทรงสี่เหลี่ยมมุมฉาก หมายถึง รูปปริซึมที่มีฐานเป็นสี่เหลี่ยมมุมฉาก



รูป 21 ทรงสี่เหลี่ยมมุมฉาก

ปริมาตรรูปทรงสี่เหลี่ยมผืนผ้า	=	กว้าง × ยาว × สูง
ปริมาตรรูปลูกบาศก์	=	(ด้าน)^3

รูปพีระมิด หรือ รูปกรวยเหลี่ยม



รูป 22 พีระมิดฐานสี่เหลี่ยม

พื้นที่ผิวข้าง $= \frac{1}{2} \times$ เส้นรอบฐาน $\times$ สูงเอียง

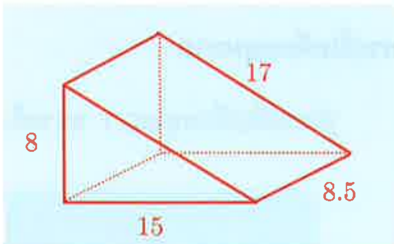
พื้นที่ผิวทั้งหมด $=$ พื้นที่ผิวข้าง $+$ พื้นที่ฐาน

ปริมาตร $= \frac{1}{3} \times$ พื้นที่ฐาน $\times$ สูง

ตัวอย่าง 1 ปริซึมฐานสามเหลี่ยมมุมฉากที่มีด้านที่ฐานยาว 8, 15 และ 17 เซนติเมตร ถ้าปริซึมนี้ยาว 8.5 เซนติเมตรจงหา

(1) ปริมาตรของปริซึม

(2) พื้นที่ผิวทั้งหมดของปริซึม



รูป 23

วิธีทำ (1) จาก ปริมาตร $=$ พื้นที่ฐาน $\times$ สูง

พื้นที่ฐานสามเหลี่ยม $= \frac{1}{2} \times$ ฐาน $\times$ สูง

จะได้ พื้นที่ฐานของปริซึมนี้ $= \frac{1}{2} \times 8 \times 15$

$= 60$ ตารางเซนติเมตร

ดังนั้น ปริมาตรปริซึม $= 60 \times 8.5$

$= 520$ ลูกบาศก์เซนติเมตร

(2) จาก พื้นที่ผิวทั้งหมดของปริซึม $=$ พื้นที่ผิวข้าง $+ 2$(พื้นที่ฐาน)

พื้นที่ผิวข้าง $=$ เส้นรอบฐาน $\times$ สูง

จะได้ พื้นที่ผิวข้างของปริซึม $= (8 + 15 + 17) + 8.5$

$= 340$ ตารางเซนติเมตร

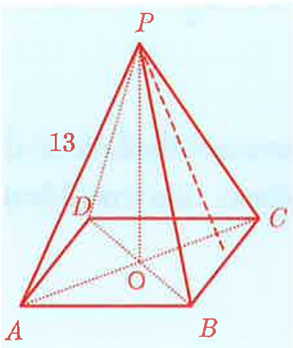
2(พื้นที่ฐาน) $= 2(\frac{1}{2} \times 8 \times 15)$

$= 340$ ตารางเซนติเมตร

ดังนั้น พื้นที่ผิวทั้งหมดของปริซึม $= 340 + 120 = 480$ ตารางเซนติเมตร □

ตัวอย่าง 2 จงหาปริมาตรของพีระมิดฐานสี่เหลี่ยมจัตุรัสมีเส้นทแยงมุมยาว 10 นิ้ว และสันของพีระมิดยาว 13 นิ้ว

วิธีทำ



รูป 24

จากรูป 24 ให้ สี่เหลียม $ABCD$ เป็นรูปสี่เหลี่ยมจัตุรัส และ OP เป็นความสูงของพีระมิด

ดังนั้น ΔAOP และ ΔABC เป็นรูปสามเหลี่ยมมุมฉาก

จะได้ $OP^2 = AP^2 - AO^2$

$= 13^2 - 5^2 = 144$

นั่นคือ $OP = 12$

จาก $AB^2 + BC^2 = AO^2$ และ $AB = AC$ จะได้

$$AB^2 = \frac{10^2}{2} = 50$$

ดังนั้น ปริมาตรของพีระมิด $= \frac{1}{3} \times AB^2 \times PO$

$= \frac{1}{3} \times 50 \times 12$

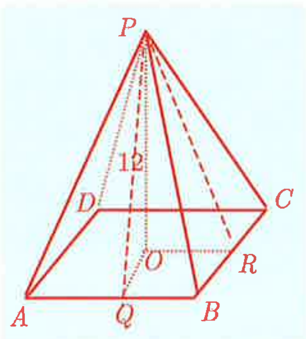
$= 200$ ลูกบาศก์นิ้ว □

ตัวอย่าง 3 จงหาพื้นที่ผิวทั้งหมดของพีระมิดฐานสี่เหลี่ยมผืนผ้า เมื่อฐานพีระมิดกว้าง 10 ฟุต ยาว 18 ฟุต และพีระมิดสูง 12 ฟุต

วิธีทำ กำหนดให้พีระมิดมีฐานเป็นรูปสี่เหลี่ยมผืนผ้า $ABCD$ สูง PO ดังรูป 25

จากรูป ให้ $AB = 18$, $BC = 10$ และ $PO = 12$

จะได้ $OR = 9$ และ $OQ = 5$



รูป 25

เนื่องจาก ΔPOR และ ΔPOQ เป็นรูปสามเหลี่ยมมุมฉาก

จะได้ $PR^2 = PO^2 + OR^2$

$= 12^2 + 9^2$

$= 225$

ดังนั้น $PR = 15$

และ $PQ^2 = PO^2 + OQ^2$

$= 12^2 + 5^2 = 169$

ดังนั้น $PQ = 13$

เนื่องจาก พื้นที่ผิวทั้งหมดของพีระมิด $=$ พื้นที่ฐาน $+$ พื้นที่ผิวข้าง

$$= (AB \cdot BC) + [2(\frac{1}{2} \cdot AB \cdot PQ) + 2(\frac{1}{2} \cdot BC \cdot PR)]$$

$$= (18 \cdot 10) + [2(\frac{1}{2} \cdot 18 \cdot 13) + 2(\frac{1}{2} \cdot 10 \cdot 15)]$$

$= 402$ ตารางฟุต □

ตัวอย่าง 4 ลวดทองแดงเส้นหนึ่งมีเส้นผ่าศูนย์กลาง 2 มิลลิเมตร พันรอบทรงกระบอกให้ปิดพื้นที่ผิวข้างโดยรอบ ถ้าทรงกระบอกมีเส้นผ่าศูนย์กลาง 10 เซนติเมตร ยาว 12 เซนติเมตร จงหาว่าต้องใช้ลวดยาวเท่าไร

วิธีทำ เพราะว่าจำนวนรอบที่พันทั้งหมด $= \dfrac{\text{ความสูงของทรงกระบอก}}{\text{เส้นผ่านศูนย์กลางของลวด}}$

$$= \frac{12}{2/10}$$

$$= \frac{12 \times 10}{2} = 60 \text{ รอบ}$$

ฉะนั้น ความยาวของลวดแต่ละรอบที่พันรอบทรงกระบอก $= 2\pi r$, r เป็นรัศมีของทรงกระบอก

$$= 2 \cdot \frac{22}{7} \cdot 5$$

$$= \frac{220}{7} \text{ เซนติเมตร}$$

ดังนั้น ความยาวของลวดทั้งหมด $=$ ความยาวลวดแต่ละรอบ $\times$ จำนวนรอบ

$$= \frac{220}{7} \times 60$$

$= 1885.71$ เซนติเมตร □

ตัวอย่าง 5 เหล็กแท่งหนึ่งหน้าตัดเป็นรูปหกเหลี่ยมด้านเท่า ยาวด้านละ 1.5 นิ้ว เหล็กแท่งยาว 16 ฟุต จงหาว่าเหล็กแท่งนี้มีปริมาตรกี่ลูกบาศก์นิ้ว

วิธีทำ พื้นที่รูปหกเหลี่ยมด้านเท่า $= \dfrac{3\sqrt{3}}{2} \times (\text{ด้าน})^2$

$$= \frac{3\sqrt{3}}{2} \times (\frac{3}{2})^2$$

$$= \frac{27\sqrt{3}}{8} \text{ ตารางนิ้ว}$$

ปริมาตรปริซึม $=$ พื้นที่ฐาน $\times$ สูง

ดังนั้น ปริมาตรแท่งเหล็ก $= \dfrac{27\sqrt{3}}{8} \times 16 \times 12$

$= 648\sqrt{3}$ ลูกบาศก์นิ้ว □

ตัวอย่าง 6 แท่งไม้รูปปริซึม มีหน้าตัดหัวท้ายเป็นรูปสี่เหลี่ยมด้านไม่เท่ามีความยาวด้านเป็น 3, 4.5, 5 และ 6 นิ้ว สูง 18 นิ้ว ถ้าพื้นที่หน้าตัดเท่ากับ 16 ตารางนิ้ว ต้องการทาสีไม้ให้ทั่ว ถ้าค่าทาสีตารางนิ้วละ 2 บาท จงหาว่าจะต้องเสียค่าทาสีเป็นเงินเท่าไร

วิธีทำ พื้นที่ผิวข้างของปริซึม = ความยาวเส้นรอบฐาน × สูง

$= (3 + 4.5 + 5 + 6) \times 18$

$= 333$ ตารางนิ้ว

พื้นที่หน้าตัดทั้ง 2 ด้าน $= 2 \times 16 = 32$ ตารางนิ้ว

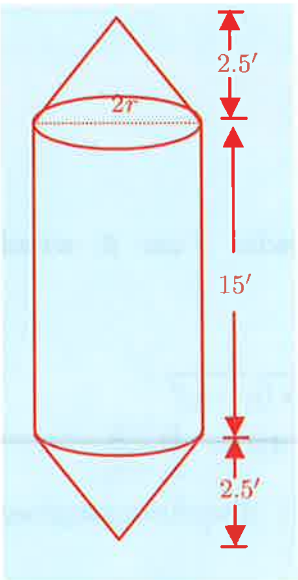
จะได้ พื้นที่ผิวทั้งหมด $= 333 + 32 = 365$ ตารางนิ้ว

เพราะว่าค่าทาสีตารางนิ้วละ 2 บาท

ดังนั้น ค่าทาสีทั้งหมดเป็นเงิน $= 365 \times 2 = 730$ บาท □

ตัวอย่าง 7 ถังน้ำใบหนึ่งรูปทรงกระบอกปลายทั้งสองข้างเป็นรูปกรวยมีขนาดเท่ากันทั้งสองปลาย ถ้าถังสูง 20 ฟุต และความยาวเฉพาะทรงกระบอก 15 ฟุต ถ้าถังใบนี้มีความจุ 308 ลูกบาศก์ฟุต จงหาความยาวของเส้นผ่าศูนย์กลางของรูปหน้าตัดทรงกระบอก

วิธีทำ



รูป 26

ให้ความยาวของเส้นผ่าศูนย์กลาง $= 2r$ ฟุต

ถังน้ำสูง 20 ฟุต ส่วนที่เป็นทรงกระบอกสูง 15 ฟุต

ดังนั้นกรวยแต่ละปลายของถัง สูง 2.5 ฟุต

ปริมาตรส่วนที่เป็นทรงกระบอก $= \pi r^2 h = 15\pi r^2$ ลูกบาศก์ฟุต

ปริมาตรส่วนที่เป็นกรวยทั้ง 2 ปลาย $= 2(\frac{1}{3}\pi r^2)2.5$

$= \frac{5}{3}\pi r^2$ ลูกบาศก์ฟุต

ถังน้ำมีความจุ 308 ลูกบาศก์ฟุต จะได้

$$15\pi r^2 + \frac{5}{3}\pi r^2 = 308$$

$$(15 + \frac{5}{3})\pi r^2 = 308$$

$$\frac{50}{3} \times \frac{22}{7} \times r^2 = 308$$

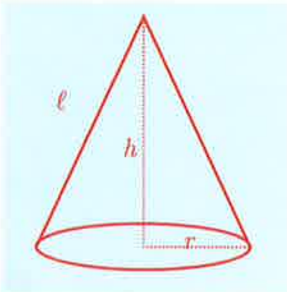
$$r^2 = 308 \times \frac{3}{50} \times \frac{7}{22} = 5.88$$

นั่นคือ $r = \sqrt{5.88} = 2.425$

ดังนั้น เส้นผ่านศูนย์กลางของรูปหน้าตัดทรงกระบอกเท่ากับ 4.85 ฟุต □

ตัวอย่าง 8 กรวยกลมตรงอันหนึ่ง มีความยาวเส้นรอบวงของปากกรวยเท่ากับ 44 นิ้ว ปริมาตรเท่ากับ 616 ลูกบาศก์นิ้ว จงหาพื้นที่ผิวข้างของกรวย

วิธีทำ



รูป 27

ความยาวเส้นรอบวงของปากกรวยเท่ากับ 44 นิ้ว

นั่นคือ $2\pi r = 44$

จะได้ $r = \dfrac{44}{2\pi} = 7$

ปริมาตรกรวยเท่ากับ 616 ลูกบาศก์นิ้ว

$$\pi r^2 h = 616$$

$$h = \frac{616}{\pi(7^2)} = 4$$

$$\ell = \sqrt{h^2 + r^2} = \sqrt{4^2 + 7^2} = 8.062$$

ดังนั้น พื้นที่ผิวข้างของกรวย $= \pi r \ell$

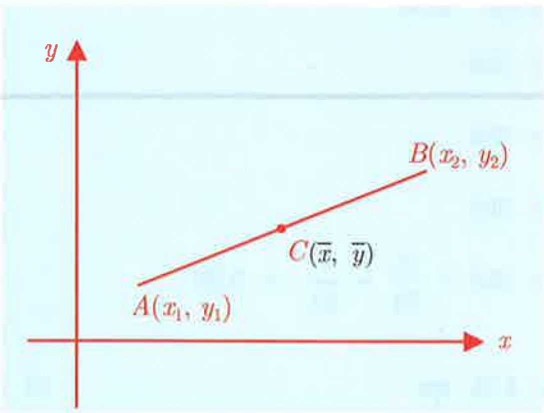
$$= \frac{22}{7} \times 7 \times 8.062$$

$= 177.364$ ตารางนิ้ว □

เรขาคณิตสองมิติเบื้องต้น

ระยะทาง จุดกึ่งกลาง และความชันของเส้นตรง

กำหนดให้ $A(x_1, y_1)$ และ $B(x_2, y_2)$ เป็นจุดสองจุดบนระนาบ **ระยะระหว่าง** A และ B, **ความชัน**ของเส้นตรง AB และ**จุดกึ่งกลาง**ของส่วนของเส้นตรง AB หาได้ดังนี้



รูป 28

ระยะ $AB = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$

ความชันของส่วนของเส้นตรง $AB = \dfrac{y_2 - y_1}{x_2 - x_1}$

ข้อสังเกต ให้จุด $C(\overline{x}, \overline{y})$ เป็นจุดกึ่งกลางของส่วนของเส้นตรง AB จะได้

$$\overline{x} = \frac{x_1 + x_2}{2}, \quad \overline{y} = \frac{y_1 + y_2}{2}$$

ถ้า $P_0(x_0, y_0)$ เป็นจุดบนส่วนของเส้นตรง AB ที่ทำให้ระยะ $AP : PB = m : n$ จะได้

$$x_0 = \frac{nx_1 + mx_2}{m + n}, \quad y_0 = \frac{ny_1 + my_2}{m + n}$$

เมื่อลากเส้นตั้งฉากจากจุด A ไปพบเส้นตรง PQ ที่จุด B จะเรียกจุด B ว่า**ภาพฉาย**ของจุด A บนเส้นตรง PQ

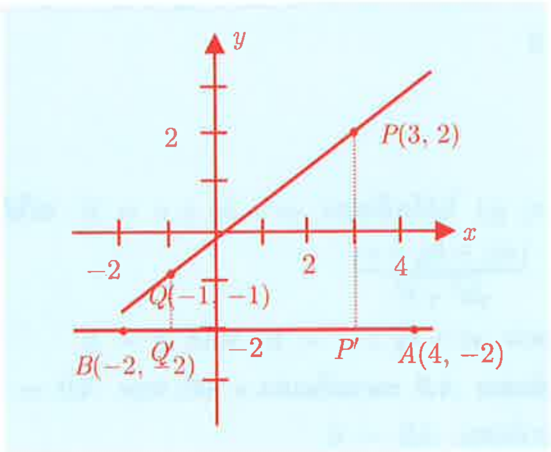
ตัวอย่าง 9 จงหาความยาวภาพฉายของส่วนของเส้นตรง $P(3, 2)$, $Q(-1, -1)$ บนเส้นตรงที่ผ่านจุด $A(4, -2)$ และจุด $B(-2, -2)$

วิธีทำ จากรูป 29 จะได้ว่า

ภาพฉายของจุด P บนเส้นตรง AB คือจุด $P'(3, -2)$

และ ภาพฉายของจุด Q บนเส้นตรง AB คือจุด $Q'(-1, -2)$

ดังนั้น ระยะ $P'Q' = 3 - (-1) = 4$



รูป 29

□

ตัวอย่าง 10 จงหาพิกัดของจุด C ซึ่งอยู่บนส่วนของเส้นตรง $A(-3, -8)$, $B(5, 10)$ ที่ทำให้ระยะ $AC : CB = 2 : 3$

วิธีทำ ให้พิกัดของจุด $C(x_0, y_0)$

จาก $x_0 = \dfrac{nx_1 + mx_2}{m+n}$, $y_0 = \dfrac{ny_1 + my_2}{m+n}$

จะได้ $x_0 = \dfrac{3(-3)+2(-8)}{2+3} = \dfrac{-9-16}{5} = -5$

และ $y_0 = \dfrac{3(5)+2(10)}{2+3} = \dfrac{15+20}{5} = 7$

ดังนั้น พิกัดของจุด C คือ $(-5, 7)$

□

สมการเส้นตรง

สมการเส้นตรงมีรูปทั่วไปเป็น $ax + by + c = 0$ เมื่อ a, b และ c เป็นค่าคงที่ โดยที่ a และ b ไม่เป็นศูนย์พร้อมกัน ถ้า $b \neq 0$ แล้วเส้นตรงจะมีความชันเท่ากับ $-\dfrac{b}{a}$ และตัดแกน y ที่จุด $(0, -\dfrac{c}{b})$

สมการเส้นตรงที่มีความชัน เท่ากับ m และผ่านจุด (x_1, y_1) คือ

$$y - y_1 = m(x - x_1)$$

สมการเส้นตรงที่ตัดแกน x ที่จุด $(a, 0)$ และตัดแกน y ที่จุด $(0, b)$ คือ

$$\frac{x}{a} + \frac{y}{b} = 1, \quad \text{เมื่อ } a \neq 0 \text{ และ } b \neq 0$$

เส้นตรงสองเส้นขนานกันจะมีความชันเท่ากัน

เส้นตรงสองเส้นตั้งฉากกัน ผลคูณของความชันของเส้นตรงมีค่าเท่ากับ -1

ข้อสังเกต เส้นตรง $ax + by + c_1 = 0$ จะขนานกับเส้นตรง $ax + by + c_2 = 0$
เส้นตรง $ax + by + c_1 = 0$ จะตั้งฉากกับเส้นตรง $bx - ay + c_3 = 0$
หรือ $-bx + ay + c_4 = 0$

ระยะระหว่างจุดกับเส้นตรง

ให้ d เป็นระยะตั้งฉากจากจุด (x_1, y_1) ไปยังเส้นตรง $ax + by + c = 0$ จะได้

$$d = \frac{|ax_1 + by_1 + c|}{\sqrt{a^2 + b^2}}$$

ข้อสังเกต
1. จุด (x_1, y_1) อยู่บนเส้นตรง $ax + by + c = 0$ จะได้ $d = 0$
2. จากรูป 28 ถ้าส่วนของเส้นตรง AB ขนานกันแกน x แล้ว ระยะ $AB = |x_1 - x_2|$ และความชันของส่วนของเส้นตรง $AB = 0$
3. จากรูป 28 ถ้าส่วนของเส้นตรง AB ขนานกันแกน y แล้ว ระยะ $AB = |y_1 - y_2|$ และความชันของส่วนของเส้นตรง AB หาค่าไม่ได้

ระยะระหว่างเส้นคู่ขนาน

ให้ $ax + by + c_1 = 0$ และ $ax + by + c_2 = 0$ เป็นเส้นตรงสองเส้นขนานกัน
d เป็นระยะระหว่างเส้นตรงทั้งสอง จะได้

$$d = \frac{|c_1 - c_2|}{\sqrt{a^2 + b^2}}$$

จุดตัดของเส้นตรง

ให้ $a_1x + b_1y = c_1$ และ $a_2x + b_2y = c_2$ เป็นเส้นตรงสองเส้นตัดกันที่จุด (x, y) จะได้

$$x = \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1} \quad \text{และ} \quad y = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1}$$

ตัวอย่าง 11 กำหนดจุด $A(1, 3)$, $B(-1, -2)$ และ $C(-3, 6)$ เป็นจุดยอดของรูปสามเหลี่ยม จงหา

(1) ความยาวเส้นมัธยฐาน AD

(2) ระยะตั้งฉากจากจุด A ไปยังด้าน BC

วิธีทำ (1) ให้จุด $D(\overline{x}, \overline{y})$ เป็นจุดกึ่งกลางของส่วนของด้าน BC จะได้

$$\overline{x} = \frac{-1+(-3)}{2} = -2 \text{ และ } \overline{y} = \frac{-2+6}{2} = 2$$

ดังนั้น $AD = \sqrt{(1-(-2))^2+(3-2)^2} = \sqrt{10}$

นั่นคือความยาวเส้นมัธยฐาน AD เท่ากับ $\sqrt{10}$

(2) ส่วนของเส้นตรง BC มีความชัน $= \dfrac{y_2-y_1}{x_2-x_1} = \dfrac{6-(-2)}{-3-(-1)} = -4$

สมการส่วนของเส้นตรง BC คือ

$$y+2 = -4(x+1)$$
$$4x+y+6 = 0$$

ระยะตั้งฉากจากจุด $A(1, 3)$ ไปยังด้าน BC คือ $\dfrac{|4(1)+1(3)+6|}{\sqrt{4^2+1^2}} = \dfrac{13}{\sqrt{17}}$ □

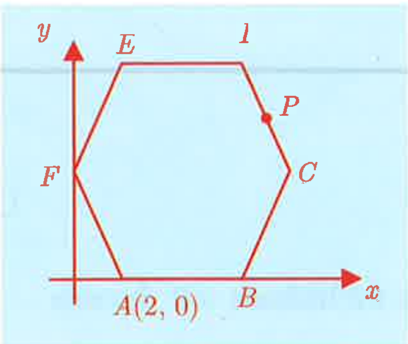
พื้นที่รูปหลายเหลี่ยม

ให้รูป n เหลี่ยมมีจุดยอดอยู่ที่จุด $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ เรียงลำดับกัน จะได้ว่า

$$\text{พื้นที่รูป } n \text{ เหลี่ยม} = \frac{1}{2}\begin{vmatrix} x_1 & x_2 & x_3 & \cdots & x_n & x_1 \\ y_1 & y_2 & y_3 & \cdots & y_n & y_1 \end{vmatrix}$$

$$= \frac{1}{2}[(x_1y_2 + x_2y_3 + x_3y_4 + \cdots + x_{n-1}y_n + x_ny_1) - (x_2y_1 + x_3y_2 + x_4y_3 + \cdots + x_ny_{n-1} + x_1y_n)]$$

ตัวอย่าง 12 $ABCDEF$ เป็นรูปหกเหลี่ยมด้านเท่า โดยมีจุด A, B อยู่บนแกน x และ P เป็นจุดกึ่งกลางด้าน CD ดังรูป 30 ถ้า จุด A มีพิกัด $(2, 0)$ แล้ว จงหาพิกัดของจุด P



รูป 30

วิธีทำ มุมภายในรูปหกเหลี่ยมด้านเท่ากางมุมละ 120 องศา

ดังนั้น มุม $OAF = 60$ องศา

ด้าน $AF = OA \sec 60^\circ = 4$

ระยะ $OF = OA \tan 60^\circ = 2\sqrt{3}$

เนื่องจาก ระยะ BD เป็น 2 เท่าระยะ OF

นั่นคือ ระยะ $BD = 4\sqrt{3}$

พิกัดจุด B เป็น $(6, 0)$, พิกัดจุด C เป็น $(8, 2\sqrt{3})$

และพิกัดจุด D เป็น $(6, 4\sqrt{3})$

ให้ $P(\overline{x}, \overline{y})$ เป็นจุดกึ่งกลาง CD ดังนั้น

$$\overline{x} = \frac{8+6}{2} = 7 \text{ และ } \overline{y} = \frac{2\sqrt{3}+4\sqrt{3}}{2} = 3\sqrt{3}$$

ดังนั้น จุด P มีพิกัดเป็น $(7, 3\sqrt{3})$ □

ตัวอย่าง 13 ให้ PQR เป็นรูปสามเหลี่ยมด้านเท่าที่มีจุด $P(3, 1)$ และ $Q(-1, 5)$ เป็นจุดยอด จงหาพื้นที่รูปสามเหลี่ยม PQR

วิธีทำ เนื่องจาก พื้นที่รูปสามเหลี่ยมด้านเท่า $= \dfrac{\sqrt{3}}{4} \times (\text{ด้าน})^2$

ความยาว $PQ = \sqrt{(3-(-1))^2+(1-5)^2} = \sqrt{32}$

จะได้ พื้นที่รูปสามเหลี่ยม $PQR = \dfrac{\sqrt{3}}{4} \times (\sqrt{32})^2 = 8\sqrt{3}$ ตารางหน่วย □

ตัวอย่าง 14 จงหาสมการของเส้นตรงที่ผ่านจุด $A(1, 5)$ และจุดที่เส้นตรง $x - y + 2 = 0$ ตัดกับเส้นตรง $2x + 3y - 6 = 0$

วิธีทำ ให้ $B(x, y)$ เป็นจุดตัดของเส้นตรง $x - y + 2 = 0$ และเส้นตรง $2x + 3y - 6 = 0$ จะได้

$$x = \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1} = \frac{(2)(3)-(-6)(-1)}{(1)(3)-(2)(-1)} = \frac{6-6}{3+2} = 0$$

และ $$y = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1} = \frac{(1)(-6)-(2)(2)}{(1)(3)-(2)(-1)} = \frac{-6-10}{3+2} = 2$$

ดังนั้น จุด B มีพิกัด $(0, 2)$

ความชันของส่วนของเส้นตรง AB คือ $\dfrac{y_2 - y_1}{x_2 - x_1} = \dfrac{2-5}{0-1} = 3$

สมการส่วนของเส้นตรง AB คือ
$$y - 5 = 3(x - 1)$$
$$3x - y + 2 = 0$$ □

ตัวอย่าง 15 กำหนดจุด A, B และ C มีพิกัดเป็น $(-1, 2)$, $(2, 3)$ และ $(a, 5)$ ตามลำดับ จงหาค่า a ที่ทำให้เส้นตรง AB ขนานกับเส้นตรง BC

วิธีทำ เส้นตรงขนานกันจะมีค่าความชันเท่ากัน

ดังนั้น $$\frac{3-2}{2-(-1)} = \frac{5-3}{a-2}$$
$$a - 2 = 6$$

ดังนั้น $a = 8$ □

ตัวอย่าง 16 กำหนด $A(1, -4)$, $B(-2, a)$ เป็นจุดสองจุด จงหาค่า a ที่ทำให้เส้นตรง AB ตั้งฉากกับเส้นตรง $2x - 3y = 4$

วิธีทำ จากสมการเส้นตรง $2x - 3y = 4$

จัดรูปสมการใหม่ได้เป็น $y = \dfrac{2}{3}x - \dfrac{4}{3}$

ดังนั้นเส้นตรงมีความชันเท่ากับ $\dfrac{2}{3}$

เส้นตรงตั้งฉากกันจะมีค่าผลคูณของความชันเท่ากับ -1

ดังนั้น
$$\begin{aligned} \frac{2}{3} \cdot \frac{a-(-4)}{-2-1} &= -1 \\ 2(a+4) &= 9 \\ 2a+8 &= 9 \\ a &= \frac{1}{2} \end{aligned}$$
□

ตัวอย่าง 17 จงหาว่าจุด $A(4, 1)$ อยู่ห่างจากเส้นตรงที่ผ่านจุด $P(2, 2)$ และ $Q(5, -2)$ เป็นระยะเท่าใด

วิธีทำ ความชันของเส้นตรงที่ผ่านจุด P และ Q คือ $\dfrac{-2-2}{5-2} = -\dfrac{4}{3}$

สมการเส้นตรงที่ผ่านจุด P และ Q คือ
$$\begin{aligned} y-2 &= -\frac{4}{3}(x-2) \\ 3y-6 &= -4x+16 \\ 4x+3y-22 &= 0 \end{aligned}$$

ระยะห่างจากจุด (x_1, y_1) ไปยังเส้นตรง $ax+by+c = 0$ คือ $\dfrac{|ax_1+by_1+c|}{\sqrt{a^2+b^2}}$

ระยะตั้งฉากจากจุด $A(4, 1)$ ให้ AB ตั้งฉากกับเส้นตรง $4x+3y-22 = 0$ คือ
$$\frac{|4(4)+3(1)-22|}{\sqrt{4^2+3^2}} = \frac{3}{5}$$

ดังนั้น จุด A อยู่ห่างจากเส้นตรง PQ เท่ากับ $\dfrac{3}{5}$ □

การพิสูจน์ทฤษฎีบท

การพิสูจน์ของทฤษฎีบทในบทที่ 2

ทฤษฎีบท 2.1 ให้ $\mathscr{U}$ เป็นเอกภพสัมพัทธ์ และ A เป็นเซต แล้ว $A \subseteq \mathscr{U}$

การพิสูจน์ เซต A จะเป็นสับเซตของ $\mathscr{U}$ ก็ต่อเมื่อ $x \in A \rightarrow x \in \mathscr{U}$
เนื่องจากผลนี้เป็นจริงเสมอ ดังนั้น $x \in A \rightarrow x \in \mathscr{U}$ เป็นจริงสำหรับทุก x
จากบทนิยาม 2.2 จะได้ว่า $A \subseteq \mathscr{U}$ □

ทฤษฎีบท 2.2 ให้ A และ B เป็นเซตใด ๆ
$A = B$ ก็ต่อเมื่อ $A \subseteq B$ และ $B \subseteq A$

การพิสูจน์ เราจะแบ่งการพิสูจน์เป็นสองตอนคือ

ตอนที่ 1 จะแสดงว่าถ้า $A = B$ แล้ว $A \subseteq B$ และ $B \subseteq A$
สมมติว่า $A = B$
จากบทนิยาม 2.1 จะได้ว่าสมาชิกทุกตัวของ A เป็นสมาชิกของ B
ดังนั้น จากบทนิยามของสับเซต จะได้ว่า $A = B \rightarrow A \subseteq B$ ....(1)
ในทำนองเดียวกัน จะได้ว่า $A = B \rightarrow B \subseteq A$ ....(2)
จาก (1) และ (2) จะได้ว่า $A = B \rightarrow [A \subseteq B \wedge B \subseteq A]$

ตอนที่ 2 จะแสดงว่าถ้า $A \subseteq B$ และ $B \subseteq A$ แล้ว $A = B$
สมมติว่า $A \subseteq B$ และ $B \subseteq A$ จากบทนิยาม 2.2 จะได้ว่า

$$A \subseteq B \rightarrow \forall x[x \in A \rightarrow x \in B]$$

และ $$B \subseteq A \rightarrow \forall x[x \in B \rightarrow x \in A]$$

ฉะนั้น

$$A \subseteq B \text{ และ } B \subseteq A \quad \to \quad \forall x[x \in A \to x \in B] \land \forall x[x \in B \to x \in A]$$
$$\to \quad A = B$$

จากตอนที่ 1 และตอนที่ 2 เราจึงสรุปได้ว่า $A = B \leftrightarrow \forall x[x \in A \leftrightarrow x \in B]$ □

ทฤษฎีบท 2.3 ให้ A, B และ C เป็นเซต
ถ้า $A \subseteq B$ และ $B \subseteq C$ แล้ว $A \subseteq C$

การพิสูจน์ ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$
สมมติว่า $A \subseteq B$ และ $B \subseteq C$
จาก $A \subseteq B$ จะได้ว่า $x \in A \to x \in B$
และ $B \subseteq C$ จะได้ว่า $x \in B \to x \in C$
ดังนั้น $x \in A \to x \in C$
นั่นคือ ถ้า $A \subseteq B$ และ $B \subseteq C$ แล้ว $A \subseteq C$ □

ทฤษฎีบท 2.4 ให้ A เป็นเซต แล้ว $\varnothing \subseteq A$

การพิสูจน์ ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$
จากบทนิยาม 2.2 เราจะได้ว่า $\varnothing \subseteq A \leftrightarrow \forall x[x \in \varnothing \to x \in A]$
และจากบทนิยาม 2.3 เราจะได้ว่า $x \in \varnothing$ เป็นเท็จเสมอ
ดังนั้น $\forall x[x \in \varnothing \to x \in A]$ เป็นจริง
ดังนั้น $\varnothing \subseteq A$ □

ทฤษฎีบท 2.5 ให้ A, B และ C เป็นเซตใด ๆ

สมบัติการสลับที่

(*i*) $A \cup B = B \cup A$

(*ii*) $A \cap B = B \cap A$

สมบัติการจัดกลุ่ม

(*iii*) $(A \cup B) \cup C = A \cup (B \cup C)$

(*iv*) $(A \cap B) \cap C = A \cap (B \cap C)$

สมบัติการกระจาย

(*v*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(*vi*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

การพิสูจน์ เราจะพิสูจน์เฉพาะ (*i*), (*iii*) และ (*v*) สำหรับการพิสูจน์ของที่เหลือจะมีวิธีการที่คล้ายคลึงกัน
ให้ A, B และ C เป็นเซตใด ๆ

(i) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in A \cup B \leftrightarrow x \in A \vee x \in B$ (บทนิยาม 2.5 ข้อ 1.)

$\leftrightarrow x \in B \vee x \in A$ (สมบัติการสลับที่ของ $\vee$)

$\leftrightarrow x \in B \cup A$ (บทนิยาม 2.5 ข้อ 1.)

ดังนั้น $\forall x[x \in A \cup B \leftrightarrow x \in B \cup A]$

นั่นคือ $A \cup B = B \cup A$

(iii) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in (A \cup B) \cup C \leftrightarrow x \in A \cup B \vee x \in C$ (บทนิยาม 2.5 ข้อ 1.)

$\leftrightarrow (x \in A \vee x \in B) \vee x \in C$ (บทนิยาม 2.5 ข้อ 1.)

$\leftrightarrow x \in A \vee (x \in B \vee x \in C)$ (สมบัติการจัดกลุ่มของ $\vee$)

$\leftrightarrow x \in A \vee x \in B \cup C$ (บทนิยาม 2.5 ข้อ 1.)

$\leftrightarrow x \in A \cup (B \cup C)$ (บทนิยาม 2.5 ข้อ 1.)

ดังนั้น $\forall x[x \in (A \cup B) \cup C \leftrightarrow x \in A \cup (B \cup C)]$

นั่นคือ $(A \cup B) \cup C = A \cup (B \cup C)$

(v) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in A \cup (B \cap C) \leftrightarrow x \in A \vee x \in B \cap C$ (บทนิยาม 2.5 ข้อ 1.)

$\leftrightarrow x \in A \vee (x \in B \wedge x \in C)$ (บทนิยาม 2.5 ข้อ 2.)

$\leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$

(สมบัติการกระจายของ $\wedge$ เหนือ $\vee$)

$\leftrightarrow x \in A \cup B \wedge x \in A \cup C$ (บทนิยาม 2.5 ข้อ 1.)

$\leftrightarrow x \in (A \cup B) \cap (A \cup C)$ (บทนิยาม 2.5 ข้อ 1.)

ดังนั้น $\forall x[x \in A \cup (B \cap C) \leftrightarrow x \in (A \cup B) \cap (A \cup C)]$

นั่นคือ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ □

ทฤษฎีบท 2.6 ให้ A, B และ C เป็นเซตใด ๆ

(i) $A \cup A = A$

(ii) $A \cap A = A$

(iii) $A \cup \varnothing = A$

(iv) $A \cap \varnothing = \varnothing$

(v) $A \cup \mathscr{U} = \mathscr{U}$

(vi) $A \cap \mathscr{U} = A$

(vii) $A - B \subseteq A$

$(viii)$ ถ้า $A \subseteq B$ และ $C \subseteq D$ แล้ว $A \cup C \subseteq B \cup D$

(ix) ถ้า $A \subseteq B$ และ $C \subseteq D$ แล้ว $A \cap C \subseteq B \cap D$

(x) $A \subseteq A \cup B$

(xi) $A \cap B \subseteq A$

(xii) ถ้า $A \subseteq B$ แล้ว $A \cup B = B$

$(xiii)$ ถ้า $A \subseteq B$ แล้ว $A \cap B = A$

(xiv) $A - \varnothing = A$

(xv) $A \cap (B - A) = \varnothing$

(xvi) $A \cup (B - A) = A \cup B$

$(xvii)$ $A - (B \cup C) = (A - B) \cap (A - C)$

$(xviii)$ $A - (B \cap C) = (A - B) \cup (A - C)$

การพิสูจน์ เราจะพิสูจน์เฉพาะ (i), (iv), (vii), (ix), $(xiii)$, (xiv) และ $(xviii)$

(i) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in A \cup A \leftrightarrow x \in A \vee x \in A$ (บทนิยาม 2.5 ข้อ 1.)

$\leftrightarrow x \in A$ (สมบัติการสะท้อนของ $\vee$)

ดังนั้น $A \cup A = A$

(iv) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in A \cap \varnothing \leftrightarrow x \in A \wedge x \in \varnothing$ (บทนิยาม 2.5 ข้อ 2.)

แต่ข้อความ $x \in \varnothing$ เป็นเท็จเสมอ ซึ่งทำให้ไม่มี x ใด ๆ ที่จะเป็นสมาชิกของ A เช่นกัน

ดังนั้น $A \cap \varnothing = \varnothing$ □

(vii) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in A - B \leftrightarrow x \in A \wedge x \notin B$ (บทนิยาม 2.5 ข้อ 2.)

$\rightarrow x \in A$ (สัจนิรันดร์ซิมพลิฟิเคชัน)

ดังนั้น $\forall x[x \in A - B \rightarrow x \in A]$

นั่นคือ $A - B \subseteq A$

(ix) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

สมมติว่า $A \subseteq B$ และ $C \subseteq D$

$x \in A \cap C \leftrightarrow x \in A \wedge x \in C$ (บทนิยาม 2.5 ข้อ 2.)

$\leftrightarrow x \in B \wedge x \in D$ (สมมติฐานข้างต้น)

$\leftrightarrow x \in B \cap D$ (บทนิยาม 2.5 ข้อ 2.)

นั่นคือ ถ้า $A \subseteq B$ และ $C \subseteq D$ แล้ว $A \cap C \subseteq B \cap D$

$(xiii)$ สมมติว่า $A \subseteq B$ จะพิสูจน์ว่า $A \cap B = A$

จาก (x) เราได้ว่า $A \cap B \subseteq A$

เพราะว่า $A \subseteq A$ และ $A \subseteq B$ จะได้โดย (ix) ว่า $A \cap A \subseteq A \cap B$

จาก (ii) จะได้ว่า $A \subseteq A \cap B$
ดังนั้น ถ้า $A \subseteq B$ แล้ว $A \cap B = A$

(xiv) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in A - \varnothing \leftrightarrow x \in A \wedge x \notin \varnothing$ (บทนิยาม 2.5 ข้อ 2.)

แต่ข้อความ $x \notin \varnothing$ เป็นจริงเสมอ

ดังนั้น $x \in A - \varnothing \leftrightarrow x \in A$

นั่นคือ $A - \varnothing = A$

$(xviii)$ ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in A - (B \cap C)$

$\leftrightarrow x \in A \wedge x \notin B \cap C$ (บทนิยาม 2.5 ข้อ 2.)

$\leftrightarrow x \in A \wedge \sim(x \in B \wedge x \in C)$ (บทนิยาม 2.5 ข้อ 2.)

$\leftrightarrow x \in A \wedge [\sim(x \in B) \vee \sim(x \in C)]$ (กฎเดอมอร์แกน)

$\leftrightarrow x \in A \wedge (x \notin B \vee x \notin C)$

$\leftrightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C)$

(สมบัติการกระจายของ $\wedge$ เหนือ $\vee$)

$\leftrightarrow x \in (A - B) \vee x \in (A - C)$ (บทนิยาม 2.5 ข้อ 2.)

$\leftrightarrow x \in (A - B) \cup (A - C)$ (บทนิยาม 2.5 ข้อ 1.)

ดังนั้น $A - (B \cap C) = (A - B) \cup (A - C)$ □

ทฤษฎีบท 2.7 ให้ $\mathscr{U}$ เป็นเอกภพสัมพัทธ์ และ A เป็นสับเซตของ $\mathscr{U}$

(i) $A \cup A' = \mathscr{U}$

(ii) $A \cap A' = \varnothing$

การพิสูจน์ (i)

$$A \cup A' = A \cup (\mathscr{U} - A) \quad \text{(บทนิยาม 2.7)}$$
$$= A \cup \mathscr{U} \quad \text{(ทฤษฎีบท 2.6 } (xvi))$$
$$= A \quad \text{(ทฤษฎีบท 2.6 } (v))$$

(ii) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$x \in A \cap A' \leftrightarrow x \in A \wedge x \in A'$ (บทนิยาม 2.5 ข้อ 2.)

$\leftrightarrow x \in A \wedge x \notin A$ (บทนิยาม 2.5 ข้อ 2.)

ซึ่งเกิดข้อขัดแย้ง

ดังนั้น $A \cap A' = \varnothing$ □

ทฤษฎีบท 2.9 ให้ A และ B เป็นเซตใด ๆ ซึ่ง $A \subseteq \mathscr{U}$ และ $B \subseteq \mathscr{U}$ จะได้ว่า
$B = A'$ ก็ต่อเมื่อ $A \cup B = \mathscr{U}$ และ $A \cap B = \varnothing$

การพิสูจน์ **ตอนที่ 1** จะพิสูจน์ว่า ถ้า $B = A'$ แล้ว $A \cup B = \mathscr{U}$ และ $A \cap B = \varnothing$
สมมติว่า $B = A'$ จะได้โดยทฤษฎีบท 2.7 ว่า
$A \cup B = A \cup A' = \mathscr{U}$ และ $A \cap B = A \cap A' = \varnothing$

ตอนที่ 2 จะพิสูจน์ว่า ถ้า $A \cup B = \mathscr{U}$ และ $A \cap B = \varnothing$ แล้ว $B = A'$
สมมติว่า $A \cup B = \mathscr{U}$ และ $A \cap B = \varnothing$

$$
\begin{aligned}
B &= \mathscr{U} \cap B && \text{(ทฤษฎีบท 2.6 } (vi)) \\
&= (A \cup A') \cap B && \text{(ทฤษฎีบท 2.7 } (i)) \\
&= (A \cap B) \cup (A' \cap B) && \text{(ทฤษฎีบท 2.5 สมบัติการกระจาย)} \\
&= \varnothing \cup (A' \cap B) && \text{(สมมติฐาน)} \\
&= (A \cap A') \cup (A' \cap B) && \text{(ทฤษฎีบท 2.7 } (ii)) \\
&= A' \cap (A \cup B) && \text{(ทฤษฎีบท 2.5 สมบัติการกระจาย)} \\
&= A' \cap \mathscr{U} && \text{(สมมติฐาน)} \\
&= A' && \text{(ทฤษฎีบท 2.6 } (vi))
\end{aligned}
$$

จากตอนที่ 1 และตอนที่ 2 เราจึงสรุปได้ว่า
$B = A'$ ก็ต่อเมื่อ $A \cup B = \mathscr{U}$ และ $A \cap B = \varnothing$ □

ทฤษฎีบท 2.11 *กฎเดอมอร์แกน*
ให้ A และ B เป็นเซตใด ๆ ซึ่ง $A \subseteq \mathscr{U}$ และ $B \subseteq \mathscr{U}$ จะได้ว่า
(i) $(A \cup B)' = A' \cap B'$
(ii) $(A \cap B)' = A' \cup B'$

การพิสูจน์ เราจะพิสูจน์เฉพาะ (i) สำหรับการพิสูจน์ของที่เหลือจะมีวิธีการที่คล้ายคลึงกัน
(i) ให้ x เป็นสมาชิกใด ๆ ในเซตเอกภพสัมพัทธ์ $\mathscr{U}$

$$
\begin{aligned}
x \in (A \cup B)' &\leftrightarrow x \notin A \cup B && \text{(บทนิยาม 2.7)} \\
&\leftrightarrow \sim(x \in A \cup B) && \\
&\leftrightarrow \sim(x \in A \vee x \in B) && \text{(บทนิยาม 2.5 ข้อ 1.)} \\
&\leftrightarrow x \notin A \wedge x \notin B && \text{(กฎเดอมอร์แกน)} \\
&\leftrightarrow x \in A' \wedge x \in B' && \text{(บทนิยาม 2.7)} \\
&\leftrightarrow x \in A' \cap B' && \text{(บทนิยาม 2.5 ข้อ 2.)}
\end{aligned}
$$

ดังนั้น $(A \cup B)' = A' \cap B'$

การพิสูจน์ของทฤษฎีบทในบทที่ 4

หลักการจัดอันดับดี

ทุก ๆ เซตย่อย S ของเซตของจำนวนเต็มบวกที่ไม่เป็นเซตว่าง แล้ว S จะมีสมาชิกค่าน้อยสุดเสมอ

ข้อสังเกต อาจกล่าวได้ว่า ถ้า $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ แล้ว S จะมีสมาชิก $r \in S$ ซึ่ง $r \leq a$ ทุกสมาชิก $a \in S$
โดยที่ $\mathbb{N}$ เป็นเซตของจำนวนเต็มบวก

หลักการอุปนัยเชิงคณิตศาสตร์วิธีที่ 1

ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก n

ถ้า (1) $P(1)$ เป็นจริง และ

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

จะได้ว่า $P(n)$ เป็นจริง ทุกจำนวนเต็มบวก n

หมายเหตุ เรียกข้อ (1) ว่า **ขั้นพื้นฐาน** และข้อ (2) ว่า **ขั้นอุปนัย**

หลักการอุปนัยเชิงคณิตศาสตร์วิธีที่ 2

ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก n

ถ้า (1) $P(1)$ เป็นจริง และ

(2) ทุกจำนวนเต็มบวก k ซึ่ง $k > 1$

ถ้า $P(1), P(2), \ldots, P(k)$ เป็นจริง แล้ว $P(k+1)$ เป็นจริง

จะได้ว่า $P(n)$ เป็นจริง ทุกจำนวนเต็มบวก n

ทฤษฎีบท 4.1 สำหรับจำนวนเต็ม a, b และ c ใด ๆ จะได้ว่า

(*i*) ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$

(*ii*) ถ้า $a \mid b$ แล้ว $a \mid bc$

(*iii*) ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$

(*iv*) ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (b+c)$

(*v*) ถ้า $a \mid (b+c)$ และ $a \mid b$ แล้ว $a \mid c$

การพิสูจน์ (*i*) สมมติให้ $a \mid b$ และ $b \mid c$
จะมีจำนวนเต็ม m และ n ซึ่ง $b = am$ และ $c = bn$
เนื่องจาก $c = bn = (am)n = a(mn)$ และ mn เป็นจำนวนเต็ม
ดังนั้น $a \mid c$

(ii) สมมติให้ $a \mid b$
จะมีจำนวนเต็ม m ซึ่ง $b = am$
เนื่องจาก $bc = (am)c = a(mc)$ และ mc เป็นจำนวนเต็ม
ดังนั้น $a \mid bc$

(iii) สมมติให้ $a \mid b$ และ $b \neq 0$
จะมีจำนวนเต็ม m ซึ่ง $b = am$
จาก $b \neq 0$ ดังนั้น $m \neq 0$ นั่นคือ $1 \leq |m|$
ดังนั้น $|a| \leq |a||m| = |am| = |b|$
นั่นคือ $|a| \leq |b|$

(iv) สมมติให้ $a \mid b$ และ $a \mid c$
จะมีจำนวนเต็ม m และ n ซึ่ง $b = am$ และ $c = an$
เนื่องจาก $b + c = am + an = a(m + n)$ และ $m + n$ เป็นจำนวนเต็ม
ดังนั้น $a \mid (b + c)$

(v) สมมติให้ $a \mid (b + c)$ และ $a \mid b$
จะมีจำนวนเต็ม m และ n ซึ่ง $b + c = am$ และ $b = an$
เนื่องจาก $c = (b + c) - b = am - an = \mathrm{a}(m - n)$
และ $m - n$ เป็นจำนวนเต็ม
ดังนั้น $a \mid c$ □

ทฤษฎีบท 4.2 *ทฤษฎีบทหลักมูลของเลขคณิต*
ทุกจำนวนเต็มบวก n ที่มากกว่า 1 จะได้ว่า n เป็นจำนวนเฉพาะหรือ n สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะได้เพียงแบบเดียวเท่านั้น โดยไม่คำนึงถึงตำแหน่งของจำนวนเฉพาะในผลคูณ

การพิสูจน์ จะแบ่งพิสูจน์เป็น 2 ตอนคือ

ตอนที่ 1 จะพิสูจน์ว่า n เป็นจำนวนเฉพาะหรือ n สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ โดยใช้หลักการอุปนัยเชิงคณิตศาสตร์วิธีที่ 2

ขั้นที่ 1 ถ้า $n = 2$ ได้ว่า n เป็นจำนวนเฉพาะ

ขั้นที่ 2 สมมติว่าทุกจำนวนเต็มบวกที่มากกว่า 1 แต่น้อยกว่า n แล้ว n เป็นจำนวนเฉพาะหรือ n สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ
ถ้า n เป็นจำนวนเฉพาะ จบการพิสูจน์
กรณีที่ n เป็นจำนวนประกอบ จะได้ว่ามีจำนวนเต็ม a และ b ที่ทำให้ $n = ab$ โดยที่ $1 < a, b < n$
โดยหลักการอุปนัยเชิงคณิตศาสตร์วิธีที่ 2 จะได้ว่าทั้ง a และ b เป็นจำนวนเฉพาะหรือสามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ

ดังนั้นได้ $n = ab$ สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ

ตอนที่ 2 จะแสดงว่า n สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะได้เพียงแบบเดียวเท่านั้น เมื่อไม่คำนึงถึงตำแหน่งของจำนวนเฉพาะในผลคูณ
สมมติให้ $n = p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$
โดยที่ p_i และ q_j เป็นจำนวนเฉพาะทุกค่า $i = 1, 2, \ldots, r,\ j = 1, 2, \ldots, s$
และ $p_1 \leq p_2 \leq \ldots \leq p_r,\ q_1 \leq q_2 \leq \ldots \leq q_s$
ต้องการแสดงว่า $r = s$ และ $p_i = q_i$ ทุกค่า i
เนื่องจาก $p_1 \mid q_1q_2 \cdots q_s$ จะได้ว่า $p_1 \mid q_i$ สำหรับบาง i
จะได้ว่า $p_1 = q_i$ ดังนั้น $p_1 \geq q_1$
ในทำนองเดียวกันสามารถพิสูจน์ได้ว่า $p_1 \leq q_1$ เพราะฉะนั้น $p_1 = q_1$
ดังนั้นได้ $p_2p_3 \cdots p_r = q_2q_3 \cdots q_s$
ในทำนองเดียวกันสามารถพิสูจน์ได้ว่า $p_2 = q_2,\ p_3 = q_3, \ldots$
ถ้า $r < s$ ได้ $1 = q_{r+1}q_{r+2} \cdots q_s$ ซึ่งเป็นไปไม่ได้
ถ้า $r > s$ ได้ $1 = p_{s+1}p_{s+2} \cdots p_r$ ซึ่งเป็นไปไม่ได้
ดังนั้นได้ $r = s$ และ $p_i = q_i$ ทุกค่า $i = 1, 2, \ldots, r$ □

ทฤษฎีบท 4.3 ถ้า n เป็นจำนวนประกอบที่มากกว่า 1 แล้ว n จะมีตัวหารที่เป็นจำนวนเฉพาะ p ซึ่ง $p \leq \sqrt{n}$

การพิสูจน์ ให้ n เป็นจำนวนประกอบที่มากกว่า 1
จะมีจำนวนเต็ม a และ b ซึ่ง $n = ab$ โดยที่ $1 < a \leq b < n$
ดังนั้นได้ $a \mid n$ และ $b \mid n$
เนื่องจาก $a \leq b$ ดังนั้น $a^2 \leq ab = n$ แสดงว่า $a \leq \sqrt{n}$
จากทฤษฎีบท 4.2 ได้ว่า a เป็นจำนวนเฉพาะหรือ a สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ
นั่นคือ n จะมีตัวหารที่เป็นจำนวนเฉพาะซึ่งน้อยกว่าหรือเท่ากับ $\sqrt{n}$ □

ทฤษฎีบท 4.4 จำนวนเฉพาะมีอยู่เป็นจำนวนอนันต์ตัว

การพิสูจน์ สมมติว่ามีจำนวนเฉพาะอยู่เป็นจำนวนจำกัด ให้เป็น $p_1, p_2, \ldots, p_n$ โดยที่ $p_1 < p_2 < \ldots < p_n$
สมมติว่า $N = p_1p_2 \cdots p_n + 1$
จะได้ว่า $N > p_n$ ดังนั้น N เป็นจำนวนประกอบ
จากทฤษฎีบท 4.2 ได้ว่า N สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ
แสดงว่ามี $p_i \in \{p_1, p_2, \ldots, p_n\}$ ซึ่ง $p_i \mid N$ เพราะฉะนั้น $p_i \mid (p_1p_2 \cdots p_n + 1)$
เนื่องจาก $p_i \mid p_1p_2 \cdots p_n$ ดังนั้น $p_i \mid 1$ ซึ่งเป็นไปไม่ได้
นั่นคือ จำนวนเฉพาะมีอยู่เป็นจำนวนอนันต์ตัว □

ทฤษฎีบท 4.5 ขั้นตอนวิธีการหาร

ให้ a และ b เป็นจำนวนเต็ม ซึ่ง $b \neq 0$ จะได้ว่า มีจำนวนเต็ม q และ r คู่เดียวเท่านั้นที่ทำให้

$$a = bq + r \qquad \text{โดยที่ } 0 \leq r < |b| \qquad \text{.........................(1)}$$

การพิสูจน์ จะแบ่งการพิสูจน์เป็นสองตอน คือ

ตอนที่ 1 จะพิสูจน์ว่า มีจำนวนเต็ม q และ r ที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < |b|$

ให้ $S = \{a - bx \mid x \in \mathbb{Z}$ และ $a - bx \geq 0\}$ โดยที่ $\mathbb{Z}$ แทนเซตของจำนวนเต็ม

จะพิสูจน์โดยใช้หลักการจัดอันดับดี โดยจะแสดงว่า $S \neq \varnothing$ ดังนี้

เนื่องจาก $b \neq 0$ ดังนั้น $b > 0$ หรือ $b < 0$

กรณีที่ $b > 0$ จะได้ $b \geq 1$ ดังนั้น $-|a|b \leq -|a|$

แต่ $-|a| \leq a$ ดังนั้น $-|a|b \leq a$ ดังนั้นได้ $a - (-|a|b) \geq 0$

จะได้ว่า $a - b(-|a|) \geq 0$ ดังนั้น $a - b(-|a|) \in S$ นั่นคือ $S \neq \varnothing$

กรณีที่ $b < 0$ สามารถพิสูจน์ได้ในทำนองเดียวกันได้ว่า $S \neq \varnothing$

ถ้า $0 \in S$ จะได้ว่ามี $q_1 \in \mathbb{Z}$ ซึ่ง $0 = a - bq_1$

ดังนั้นได้ $a = bq_1 + 0$ โดยที่ $0 \leq 0 < |b|$

นั่นคือ จะได้ $r = 0$

ถ้า $0 \notin S$ ดังนั้น $S \subseteq \mathbb{N}$

จากหลักการจัดอันดับดี จะได้ว่ามี S มีสมาชิกค่าน้อยสุดให้เป็น $r \in S$

จะมี $q \in \mathbb{Z}$ ซึ่ง $a - bq = r$ ดังนั้นได้ $a = bq + r$ โดยที่ $0 < r$

ต่อไปเราจะแสดงว่า $r < |b|$ จะพิสูจน์โดยวิธีหาข้อขัดแย้ง

สมมติว่า $r \geq |b|$

ดังนั้น $0 \leq r - |b| = (a - bq) - |b| = a - b(q \pm 1) \in S$

จึงเกิดข้อขัดแย้งในการเลือก r ที่เป็น 0 หรือเป็นจำนวนเต็มบวกที่น้อยที่สุดใน S

ดังนั้น $r < |b|$ นั่นคือ มี $q, r \in \mathbb{Z}$ ที่ทำให้

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

ตอนที่ 2 จะพิสูจน์ว่า มีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้นที่ทำให้

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

ให้ $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ ซึ่งทำให้

$$a = bq_1 + r_1 \qquad \text{โดยที่ } 0 \leq r_1 < |b|$$

และ $$a = bq_2 + r_2 \qquad \text{โดยที่ } 0 \leq r_2 < |b|$$

ดังนั้น $bq_1 + r_1 = bq_2 + r_2$ นั่นคือ $r_1 - r_2 = b(q_2 - q_1)$

จะได้ว่า $$|r_1 - r_2| = |b||q_1 - q_2| \qquad \text{.........................(2)}$$

แต่ทั้ง r_1 และ r_2 เป็นจำนวนเต็มที่อยู่ระหว่าง 0 กับ $|b|$ จึงส่งผลให้

$|r_1 - r_2| < |b|$

ดังนั้น $|b||q_1 - q_2| < |b|$ และจาก $b \neq 0$ จะได้ว่า $|q_1 - q_2| < 1$

แสดงว่า $0 \leq |q_1 - q_2| < 1$ แต่ $|q_1 - q_2|$ เป็นจำนวนเต็ม

ดังนั้น $|q_1 - q_2| = 0$

จะได้ว่า $q_1 = q_2$ ดังนั้นจาก (2) ได้ว่า $r_1 = r_2$

นั่นคือ มีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้นที่ทำให้

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

ทฤษฎีบท 4.6 ถ้า $d = (a, b)$ จะได้ว่ามีจำนวนเต็ม x และ y ซึ่งทำให้ $d = ax + by$

การพิสูจน์ ให้ $S = \{ax + by \mid x, y$ เป็นจำนวนเต็ม และ $ax + by > 0\}$

เนื่องจาก $a \neq 0$ หรือ $b \neq 0$ ดังนั้น $S \neq \varnothing$ และ $S \subseteq \mathbb{N}$

จากหลักการจัดอันดับดี จะได้ว่ามี S มีสมาชิกค่าน้อยสุดให้เป็น d

ดังนั้นมีจำนวนเต็ม x และ y ซึ่งทำให้ $d = ax + by$ ต่อไปจะแสดงว่า $d = (a, b)$

โดยขั้นตอนวิธีการหารได้ว่ามีจำนวนเต็ม q และ r ซึ่งทำให้

$$a = dq + r \quad \text{โดยที่ } 0 \leq r < d$$

ดังนั้น $a = (ax + by)q + r$ จะได้ว่า $r = a(1 - xq) + b(-yq)$

เนื่องจาก $0 \leq r < d$ และ d สมาชิกค่าน้อยสุดในเซต S จะได้ว่า $r \notin S$

แสดงว่า $r = 0$ นั่นคือ $d \mid a$

พิสูจน์ในทำนองเดียวกันได้ว่า $d \mid b$ ดังนั้นได้ d เป็นตัวหารร่วมของ a กับ b

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

นั่นคือ d เป็นตัวหารร่วมมากของ a กับ b และมีจำนวนเต็ม x และ y ซึ่ง

$$d = ax + by$$ □

ทฤษฎีบท 4.8 ให้ a และ b เป็นจำนวนเต็มบวก จะได้ว่า $ab = (a, b)\,[a, b]$

การพิสูจน์ ให้ $d = (a, b)$ และ $m = [a, b]$

เนื่องจาก $d \mid a$ และ $d \mid b$ จะมีจำนวนเต็ม x, y ซึ่ง $a = dx$ และ $b = dy$

จะได้ว่า $bx = (dy)x = (dx)y = ay = \dfrac{ab}{d}$

เนื่องจาก bx เป็นพหุคูณของ b และ ay เป็นพหุคูณของ a

ดังนั้น $\dfrac{ab}{d}$ เป็นตัวคูณร่วมของ a และ b นั่นคือ $m \leq \dfrac{ab}{d}$

จะได้ว่า $md \leq ab$

นั่นคือ $[a, b](a, b) \leq ab$ ....(1)

จะเห็นได้ชัดว่า $m \mid ab$ ดังนั้นจะมีจำนวนเต็ม s ที่ทำให้ $ab = ms$

และจาก $b \mid m$ จะมีจำนวนเต็ม t ที่ทำให้ $m = bt$
ดังนั้นได้ $ab = bst$ แสดงว่า $a = st$ ดังนั้น $s \mid a$
แสดงในทำนองเดียวกันได้ว่า $s \mid b$ นั่นคือ $s \leq d$ จะได้ $ms \leq md$
นั่นคือ $ab \leq [a, b](a, b)$ ....(2)
จาก (1) และ (2) สรุปได้ว่า $ab = [a, b](a, b)$ □

ทฤษฎีบท 4.9 ให้ m เป็นจำนวนเต็มบวก และ a, b, c และ d เป็นจำนวนเต็ม จะได้ว่า

(*i*) $a \equiv a \pmod{m}$

(*ii*) ถ้า $a \equiv b \pmod{m}$ แล้ว $b \equiv a \pmod{m}$

(*iii*) ถ้า $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$ แล้ว $a \equiv c \pmod{m}$

(*iv*) ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ แล้ว
$a + c \equiv b + d \pmod{m}$ และ $ac \equiv bd \pmod{m}$

(*v*) ถ้า $a \equiv b \pmod{m}$ แล้ว $a^n \equiv b^n \pmod{m}$ ทุกจำนวนเต็มบวก n

(*vi*) ถ้า $ac \equiv bc \pmod{m}$ และ $(c, m) = d$ แล้ว $a \equiv b \pmod{\frac{m}{d}}$

การพิสูจน์ (*i*) เนื่องจาก $m \mid (a - a)$ ดังนั้น $a \equiv a \pmod{m}$

(*ii*) สมมติให้ $a \equiv b \pmod{m}$
ดังนั้น $m \mid (a - b)$ จะมีจำนวนเต็ม k ที่ทำให้ $a - b = mk$
เพราะฉะนั้น $b - a = m(-k)$ นั่นคือ $m \mid (b - a)$ ดังนั้นได้ $b \equiv a \pmod{m}$

(*iii*) สมมติให้ $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$
จะได้ว่า $m \mid (a - b)$ และ $m \mid (b - c)$
จะมีจำนวนเต็ม k, n ที่ทำให้ $a - b = mk$ และ $b - c = mn$
ดังนั้น $a - c = (a - b) + (b - c) = m(k + n)$
นั่นคือ $a \equiv c \pmod{m}$

(*iv*) สมมติให้ $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$
จะมีจำนวนเต็ม k และ n ซึ่ง $a = b + mk$ และ $c = d + mn$
ดังนั้นได้ $a + c = (b + d) + m(k + n)$
และ $ac = (b + mk)(d + mn) = bd + m(bn + dk + kmn)$
นั่นคือ $a + c \equiv b + d \pmod{m}$ และ $ac \equiv bd \pmod{m}$

(*v*) สมมติให้ $a \equiv b \pmod{m}$
ต้องการแสดงว่า $a^n \equiv b^n \pmod{m}$ ทุกจำนวนเต็มบวก n
โดยใช้หลักการอุปนัยเชิงคณิตศาสตร์วิธีที่ 1
สมมติให้ $a^k \equiv b^k \pmod{m}$ เมื่อ k เป็นจำนวนเต็มบวก

จากข้อ (iv) ได้ว่า $a^k a \equiv b^k b \pmod{m}$ ดังนั้นได้ $a^{k+1} \equiv b^{k+1} \pmod{m}$
โดยหลักการอุปนัยเชิงคณิตศาสตร์วิธีที่ 1 ได้ว่า $a^n \equiv b^n \pmod{m}$ ทุกจำนวนเต็มบวก n

(vi) สมมติให้ $ac \equiv bc \pmod{m}$ และ $(c, m) = d$
จะมีจำนวนเต็ม k ที่ทำให้ $ac - bc = (a-b)c = mk$
ดังนั้น $(a-b)\dfrac{c}{d} = \dfrac{m}{d}k$
แสดงว่า $\dfrac{m}{d} \mid (a-b)\dfrac{c}{d}$
จากแบบฝึกหัดบทที่ 4 ข้อ 2.6 ได้ $(\dfrac{c}{d}, \dfrac{m}{d}) = 1$
จากแบบฝึกหัดบทที่ 4 ข้อ 2.5 ได้ $\dfrac{m}{d} \mid (a-b)$
นั่นคือ $a \equiv b \pmod{\dfrac{m}{d}}$ □

ทฤษฎีบท 4.10 ให้ a, b, q และ r เป็นจำนวนเต็มซึ่ง $b > 0$ และ

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

จะได้ว่า $(a, b) = (b, r)$

การพิสูจน์ ให้ $d = (a, b)$ และ $g = (b, r)$
จาก $d = (a, b)$ จะได้ $d \mid a$ และ $d \mid b$ ดังนั้น $d \mid r$
จาก $g = (b, r)$ จะได้ $d \mid g$
ในทำนองเดียวกัน จาก $g = (b, r)$ จะได้ $g \mid b$ และ $g \mid r$ ดังนั้น $g \mid a$
และจาก $d = (a, b)$ จะได้ $g \mid d$ ดังนั้น $d = g$
นั่นคือ $(a, b) = (b, r)$ □

ทฤษฎีบท 4.11 *ขั้นตอนวิธีของยุคลิด*

ให้ a, b เป็นจำนวนเต็มบวก และ $q_1, q_2, \ldots, q_{n+1}, r_1, r_2, \ldots, r_n$ เป็นจำนวนเต็ม โดยที่

$$\begin{aligned}
a &= bq_1 + r_1, & 0 &< r_1 < b \\
b &= r_1q_2 + r_2, & 0 &< r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, & 0 &< r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 &< r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

แล้วจะได้ว่า $(a, b) = r_n$

การพิสูจน์ จากทฤษฎีบท 4.10 ได้ว่า $(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n)$
เนื่องจาก $r_n \mid r_{n-1}$ ดังนั้นได้ $(r_{n-1}, r_n) = r_n$
นั่นคือ $(a, b) = r_n$ □

ทฤษฎีบท 4.13 ถ้า a เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวกที่มากกว่า 1 ซึ่ง $(a, m) = 1$ แล้ว อินเวอร์สของ a มอดุโล m จะหาค่าได้ และมีเพียงค่าเดียวเท่านั้นที่ไม่คอนกรูเอนซ์กันในมอดุโล m

การพิสูจน์ เนื่องจาก $(a, m) = 1$ จะมีจำนวนเต็ม x และ y ซึ่งทำให้ $1 = ax + my$
ดังนั้น $ax + my \equiv 1 \pmod{m}$
เนื่องจาก $my \equiv 0 \pmod{m}$ จะได้ว่า $ax \equiv 1 \pmod{m}$
นั่นคือ x เป็นอินเวอร์สของ a มอดุโล m
สมมติว่า x_1 เป็นอินเวอร์สอีกตัวหนึ่งของ a มอดุโล m ดังนั้น $ax_1 \equiv 1 \pmod{m}$
จะได้ว่า $ax_1 \equiv ax \pmod{m}$
เนื่องจาก $(a, m) = 1$ จากทฤษฎีบท 4.9 ข้อ (*vi*) ได้ $x_1 \equiv x \pmod{m}$
นั่นคือ อินเวอร์สของ a มีเพียงค่าเดียวเท่านั้นที่ไม่คอนกรูเอนซ์กันในมอดุโล m □

ทฤษฎีบท 4.15 *ทฤษฎีบทเศษเหลือของจีน*
ให้ $m_1, m_2, \ldots, m_n$ เป็นจำนวนเต็มบวกซึ่ง $(m_i, m_j) = 1$ เมื่อ $i \neq j$ และ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มและให้ $m = m_1 m_2 \cdots m_n$ และ $M_i = \dfrac{m}{m_i}$
สำหรับแต่ละ i ให้ y_i เป็นจำนวนเต็มที่เป็นผลเฉลยของ $M_i y \equiv 1 \pmod{m_i}$
จะได้ว่า ระบบคอนกรูเอนซ์เชิงเส้น

$$\left.\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv a_n \pmod{m_n} \end{array}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

มีผลเฉลยร่วมกันเพียงตัวเดียว คือ $x = M_1a_1y_1 + M_2a_2y_2 + \cdots + M_na_ny_n$ ในมอดุโล m

การพิสูจน์ เนื่องจาก $(m_i, m_j) = 1$ เมื่อ $i \neq j$ ดังนั้น $(M_i, m_i) = 1$ ทุก $i = 1, 2, \ldots, n$
สำหรับแต่ละ $i = 1, 2, \ldots, n$ จากทฤษฎีบท 4.12 ได้ว่า $M_i y \equiv 1 \pmod{m_i}$ มีผลเฉลยเดียวที่เป็นจำนวนเต็มให้เป็น y_i ดังนั้น $M_i y_i \equiv 1 \pmod{m_i}$
เพราะฉะนั้น $M_i a_i y_i \equiv a_i \pmod{m_i}$
เนื่องจากแต่ละ $i \neq j$ จะได้ M_j มี m_i เป็นตัวประกอบ ดังนั้นได้ $m_i \mid M_j$
จะได้ว่า $m_i \mid M_j a_j y_j$ แสดงว่า $M_j a_j y_j \equiv 0 \pmod{m_i}$
ดังนั้น $M_1a_1y_1 + M_2a_2y_2 + \cdots + M_na_ny_n \equiv a_i \pmod{m_i}$ ทุก $i = 1, 2, \ldots, n$
นั่นคือ $x = M_1a_1y_1 + M_2a_2y_2 + \cdots + M_na_ny_n$ เป็นผลเฉลยของระบบคอนกรูเอนซ์ (1)
เนื่องจาก $(m_i, m_j) = 1$ เมื่อ $i \neq j$ โดยแบบฝึกหัดบทที่ 4 ข้อ 49. ได้ $x_1 \equiv x \pmod{m}$
นั่นคือ $x = M_1a_1y_1 + M_2a_2y_2 + \cdots + M_na_ny_n$ เป็นผลเฉลยเดียวของระบบคอนกรูเอนซ์ (1)
□

การพิสูจน์ของทฤษฎีบทในบทที่ 6

ทฤษฎีบท 6.1 ให้ A, B และ C เป็นเมทริกซ์ขนาด $m \times n$ และ k_1 และ k_2 เป็นสเกลาร์ จะได้ว่า

(*i*) $(A+B)+C = A+(B+C)$

(*ii*) $A+B = B+A$

(*iii*) $A+\mathbf{0} = A = \mathbf{0}+A$

(*iv*) $A+(-A) = \mathbf{0} = (-A)+A$

(*v*) $k_1(A+B) = k_1A+k_1B$

(*vi*) $(k_1+k_2)A = k_1A+k_2A$

(*vii*) $(k_1k_2)A = k_1(k_2A)$

(*viii*) $1A = A$

การพิสูจน์ เราจะพิสูจน์เฉพาะ (*i*), (*iv*) และ (*vi*)

ให้ $A = [a_{ij}]$, $B = [b_{ij}]$ และ $C = [c_{ij}]$ เป็นเมทริกซ์ขนาด $m \times n$

(*i*)
$$
\begin{aligned}
(A+B)+C &= [(a_{ij}+b_{ij})+c_{ij}] && \text{(บทนิยาม 6.5)}\\
&= [a_{ij}+(b_{ij}+c_{ij})] && \text{(สมบัติการจัดกลุ่มของการบวก)}\\
&= A+(B+C) && \text{(บทนิยาม 6.5)}
\end{aligned}
$$

(*iv*) เพราะว่า $-A = (-1)A = [-a_{ij}]$ จะได้
$$
\begin{aligned}
A+(-A) &= [a_{ij}+(-a_{ij})] && \text{(บทนิยาม 6.5)}\\
&= [0]\\
&= \mathbf{0} && \text{(บทนิยาม 6.3)}
\end{aligned}
$$

(*vi*)
$$
\begin{aligned}
(k_1+k_2)A &= [(k_1+k_2)a_{ij}] && \text{(บทนิยาม 6.6)}\\
&= [k_1a_{ij}+k_2a_{ij}] && \text{(สมบัติการกระจายการคูณเหนือการบวก)}\\
&= [k_1a_{ij}]+[k_2a_{ij}] && \text{(บทนิยาม 6.5)}\\
&= k_1A+k_2A && \text{(บทนิยาม 6.6)}
\end{aligned}
$$
□

ทฤษฎีบท 6.2 กำหนด A, B และ C เป็นเมทริกซ์ซึ่งสามารถหาผลบวกและผลคูณได้ และ k เป็นสเกลาร์ จะได้

(*i*) $A(BC) = (AB)C$

(*ii*) $A(B+C) = AB+AC$

(*iii*) $(A+B)C = AC+BC$

(*iv*) $k(AB) = (kA)B = A(kB)$

การพิสูจน์ เราจะพิสูจน์เฉพาะ (*i*), (*ii*) และ (*iv*)

(*i*) ให้ $A = [a_{ij}]$, $B = [b_{jk}]$ และ $C = [c_{k\ell}]$ เมื่อ $i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, r$ และ $\ell = 1, 2, \ldots, s$

$$
\begin{aligned}
A(BC) &= [\sum_k [\sum_j a_{ij}b_{jk}]c_{k\ell}] && \text{(บทนิยาม 6.7)}\\
&= [\sum_k a_{ij}[\sum_j b_{jk}c_{k\ell}]] && \text{(สมบัติการจัดกลุ่มของการคูณ)}\\
&= (AB)C && \text{(บทนิยาม 6.7)}
\end{aligned}
$$

(ii) ให้ $A = [a_{ik}]$, $B = [b_{kj}]$ และ $C = [c_{kj}]$ เมื่อ $i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, r$ และ $j = 1, 2, \ldots, n$

$$
\begin{aligned}
A(B+C) &= A[b_{kj} + c_{kj}] && \text{(บทนิยาม 6.5)}\\
&= [\sum_k a_{ik}(b_{kj} + c_{kj})] && \text{(บทนิยาม 6.7)}\\
&= [\sum_k a_{ik}b_{kj} + \sum_k a_{ik}c_{kj}] && \text{(สมบัติการกระจายการคูณเหนือการบวก)}\\
&= [\sum_k a_{ik}b_{kj}] + [\sum_k a_{ik}c_{kj}] && \text{(บทนิยาม 6.5)}\\
&= AB + AC && \text{(บทนิยาม 6.7)}
\end{aligned}
$$

(iv) ให้ $A = [a_{i\ell}]$ และ $B = [b_{\ell j}]$ เมื่อ $i = 1, 2, \ldots, m$, $\ell = 1, 2, \ldots, r$ และ $j = 1, 2, \ldots, n$

$$
\begin{aligned}
k(AB) &= k[\sum_\ell a_{i\ell}b_{\ell k}] && \text{(บทนิยาม 6.7)}\\
&= [\sum_\ell (ka_{i\ell})b_{\ell k}] && \text{(สมบัติการจัดกลุ่มของการคูณ)}\\
&= (kA)B && \text{(บทนิยาม 6.7)}\\
k(AB) &= k[\sum_\ell a_{i\ell}b_{\ell k}] && \text{(บทนิยาม 6.7)}\\
&= [\sum_\ell a_{i\ell}(kb_{\ell k})] && \text{(สมบัติการจัดกลุ่มของการคูณ)}\\
&= A(kB) && \text{(บทนิยาม 6.7)}
\end{aligned}
$$

□

ทฤษฎีบท 6.3 กำหนด A, B และ C เป็นเมทริกซ์ซึ่งสามารถหาผลบวกและผลคูณได้ และ k เป็นสเกลาร์ จะได้

(i) $(A+B)^T = A^T + B^T$

(ii) $(AB)^T = B^TA^T$

(iii) $(kA)^T = kA^T$

(iv) $(A^T)^T = A$

การพิสูจน์ *(i)* ให้ $A = [a_{ij}]$ และ $B = [b_{ij}]$ เมื่อ $i = 1, 2, \ldots, m$ และ $j = 1, 2, \ldots, n$

$$
\begin{aligned}
(A+B)^T &= [a_{ij} + b_{ij}]^T && \text{(บทนิยาม 6.5)}\\
&= [a_{ji} + b_{ji}] && \text{(บทนิยาม 6.8)}\\
&= [a_{ji}] + [b_{ji}] && \text{(บทนิยาม 6.5)}\\
&= A^T + B^T && \text{(บทนิยาม 6.8)}
\end{aligned}
$$

(ii) ให้ $A = [a_{ik}]$ และ $B = [b_{kj}]$ เมื่อ $i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, r$ และ $j = 1, 2, \ldots, n$

$$
\begin{aligned}
(AB)^T &= [\sum_k a_{ik}b_{kj}]^T && \text{(บทนิยาม 6.7)}\\
&= [\sum_k a_{ki}b_{jk}] && \text{(บทนิยาม 6.8)}\\
&= [\sum_k b_{jk}a_{ki}] && \text{(สมบัติการสลับที่การคูณ)}\\
&= [\sum_k b_{kj}a_{ik}]^T && \text{(บทนิยาม 6.8)}\\
&= B^TA^T && \text{(บทนิยาม 6.7)}
\end{aligned}
$$

(iii) ให้ $A = [a_{ij}]$ เมื่อ $i = 1, 2, \ldots, m$ และ $j = 1, 2, \ldots, n$

$$
\begin{aligned}
(kA)^T &= [ka_{ij}]^T && \text{(บทนิยาม 6.6)}\\
&= [ka_{ji}] && \text{(บทนิยาม 6.8)}\\
&= k[a_{ji}] && \text{(บทนิยาม 6.6)}\\
&= kA^T && \text{(บทนิยาม 6.8)}
\end{aligned}
$$

(iv) ให้ $A = [a_{ij}]$ เมื่อ $i = 1, 2, \ldots, m$ และ $j = 1, 2, \ldots, n$

$$
\begin{aligned}
(A^T)^T &= [[a_{ij}]^T]^T &&\\
&= [a_{ji}]^T && \text{(บทนิยาม 6.8)}\\
&= [a_{ij}] && \text{(บทนิยาม 6.8)}\\
&= A && \text{(บทนิยาม 6.8)}
\end{aligned}
$$

□

ทฤษฎีบท 6.4 ถ้า A เป็นเมทริกซ์ขนาด $m \times n$ แล้ว $AI_n = I_mA = A$

การพิสูจน์ ให้ $A = [a_{ij}]$ เมื่อ $i, \ell = 1, 2, \ldots, m$ และ $k, j = 1, 2, \ldots, n$

$$
\begin{aligned}
AI_n &= [\sum_k a_{ik}\delta_{kj}] && \text{(บทนิยาม 6.7)}\\
&= [a_{ij}] &&\\
&= A &&
\end{aligned}
$$

$$
\begin{aligned}
I_mA &= [\sum_\ell \delta_{i\ell}a_{\ell k}] && \text{(บทนิยาม 6.7)}\\
&= [a_{ij}] &&\\
&= A &&
\end{aligned}
$$

บรรณานุกรม

ภาษาไทย

1. สถาบันการสอนวิทยาศาสตร์และเทคโนโลยี. **คณิตศาสตร์ ค 016 ระดับมัธยมศึกษาตอนปลาย.** กรุงเทพฯ : โรงพิมพ์คุรุสภา ลาดพร้าว, 2536.
2. สถาบันการสอนวิทยาศาสตร์และเทคโนโลยี. **คณิตศาสตร์ ค 012 ระดับมัธยมศึกษาตอนปลาย.** พิมพ์ครั้งที่ 7 กรุงเทพฯ : โรงพิมพ์คุรุสภา ลาดพร้าว, 2541.
3. สมาคมคณิตศาสตร์แห่งประเทศไทย ในพระบรมราชูปถัมภ์. **เสริมประสบการณ์คณิตศาสตร์ ระดับมัธยมปลาย เล่มที่ 5.** กรุงเทพฯ : พิทักษ์การพิมพ์, 2529.
4. หมวดวิชาคณิตศาสตร์ โรงเรียนเตรียมอุดมศึกษา, **โจทย์เสริมทักษะคณิตศาสตร์ รายวิชา ค 015 – ค 016.** กรุงเทพฯ : โรงเรียนเตรียมอุดมศึกษา, 2540.
5. อัจฉรา หาญชูวงศ์. **เอกสารเสริมความรู้วิชาคณิตศาสตร์ เรื่อง ทฤษฎีจำนวน.** สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. กรุงเทพฯ : สำนักพัฒนาธุรกิจ, 2544.

ภาษาอังกฤษ

1. ARITHMEUM rechnen einst und heute in the Research Institute for Discrete Mathematics. Lennestrasse 2, Bonn, 1999.
2. H.S Hall and F.H. Stevens, A School Geometry part I-VI, Macmillan and Co.Ltd., London, 1955
3. Howard. Anton, **Calculus (A New Horizon)**, 6th ed, John Wiley & Sons, Inc., New York, 1999.
4. http://www-history.mcs.st-andrews.ac.uk.
5. Johnonbaugh. Richard, **Discrete Mathematics**, 5th ed, Prentice Hall, 2001.
6. Redmond, Don. **An Introduction to Number Theory**, Marcel Dekker, Inc. New York, 1996.
7. Rosen. Kenneth H., **Discrete Mathematics and Its Applications**, 5th ed, McGraw-Hill , 2003.

ดัชนี

บัญชีสัญลักษณ์

สัญลักษณ์	ความหมาย
$\sim$	นิเสธ 3
$\wedge$	และ 3
$\vee$	หรือ 3
$\oplus$	เอกซ์คลูซีฟออร์ 4
$\rightarrow$	ถ้า...แล้ว... 4
$\leftrightarrow$	...ก็ต่อเมื่อ... 5
$\forall$	ตัวบ่งปริมาณสำหรับทุกตัว 11
$\exists$	ตัวบ่งปริมาณสำหรับตัวมีจริง 11
$\exists!$	มีเพียงค่าเดียวเท่านั้น 12
$\in$	เป็นสมาชิกของ 15
$\notin$	ไม่เป็นสมาชิกของ 15
$n(A),\ \lvert A\rvert$	จำนวนสมาชิกของ A 17
$A \subseteq B$	A เป็นสับเซตของ B 18
$A \subset B$	A เป็นสับเซตแท้ของ B 18
$A \nsubseteq B$	A ไม่เป็นสับเซตของ B 18
$\varnothing$	เซตว่าง 19
$A \cup B$	ยูเนียนของ A และ B 21
$A \cap B$	อินเตอร์เซกชันของ A และ B 21
$A - B$	ผลต่างของ A และ B 21
A'	คอมพลีเมนต์ของ A 23
$A \times B$	ผลคูณคาร์ทีเซียนของ A และ B 32
r^{-1}	ความสัมพันธ์ผกผันของ r 34
$s \circ r$	ความสัมพันธ์ประกอบของ r และ s 36

คอมพิวเตอร์
ISBN 974 - 92235 - 2 - 7.
9 789749 223529
C 112
5500 250.00 บาท

มูลนิธิส่งเสริมโอลิมปิกวิชาการและพัฒนามาตรฐานวิทยาศาสตร์ศึกษา
ในพระอุปถัมภ์สมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์
สำนักงานตั้งอยู่ในบริเวณ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ถนนพญาไท ปทุมวัน กทม. 10330
โทร. 0-2252-8916, 0-2252-8917, แฟกซ์. 0-2252-8917