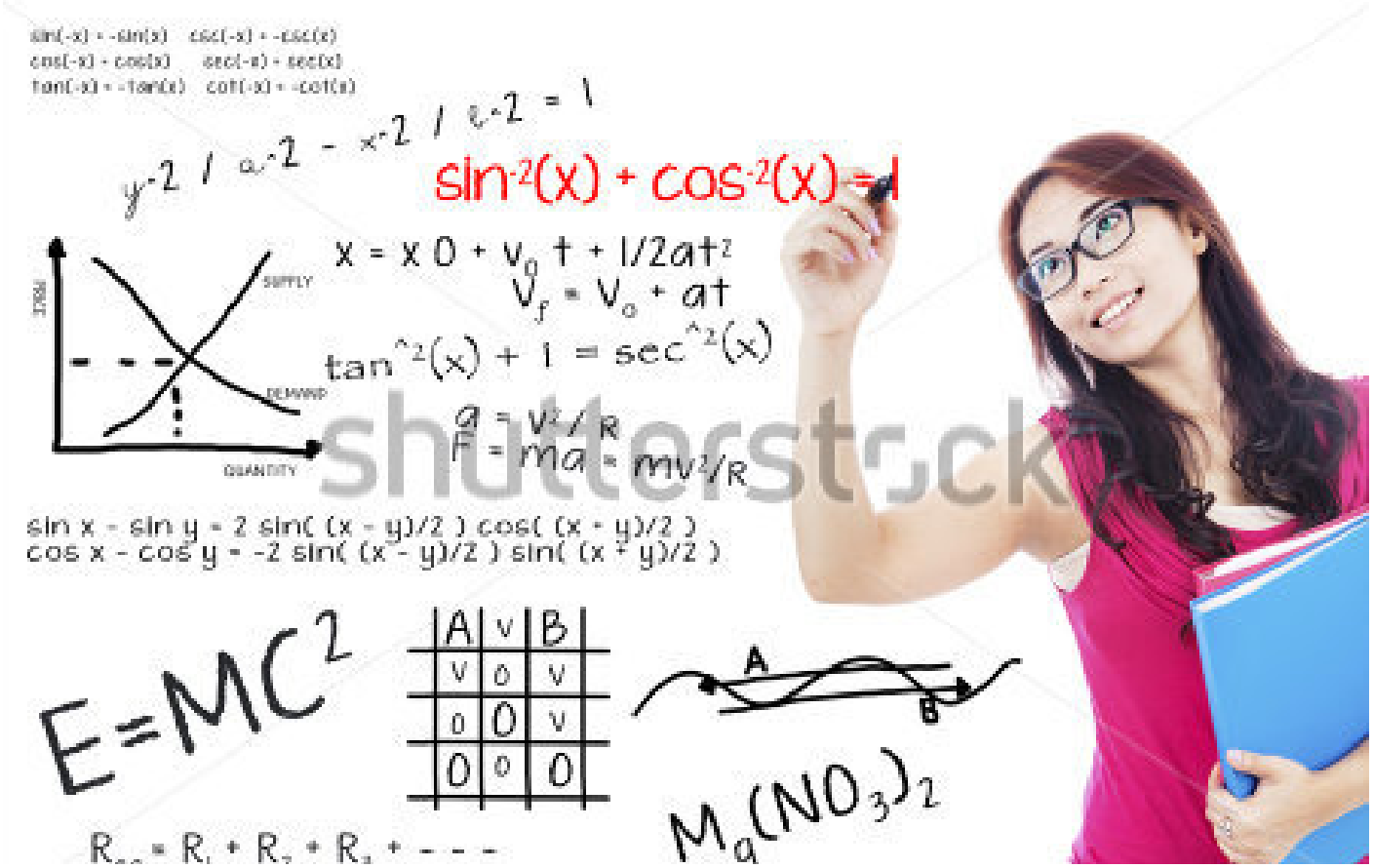
รศ. ดร. สมพร สูตินันท์โอภาส
ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยรามคำแหง / e-mail : sompornss@ru.ac.th

คณิตศาสตร์กับการสื่อสารอย่างปลอดภัย

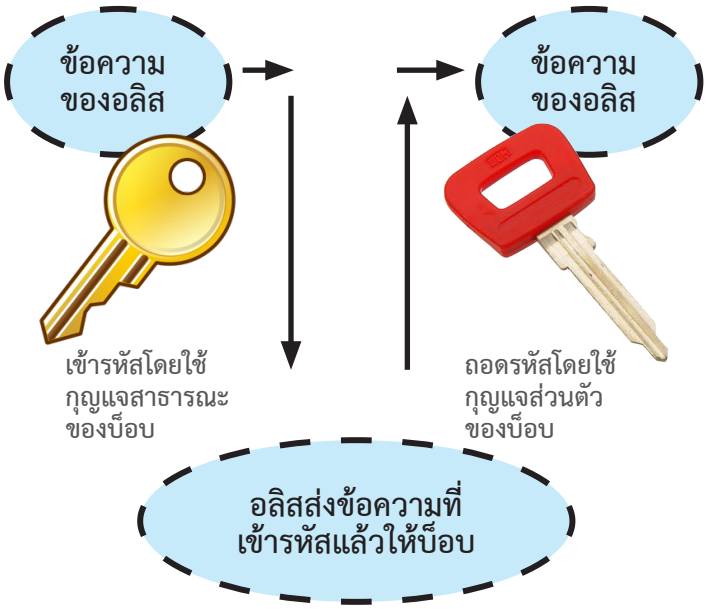


สาเหตุหนึ่งที่ทำให้นักเรียนจำนวนมากไม่ชอบวิชาคณิตศาสตร์ เป็นเพราะว่านักเรียนไม่ได้รับการกระตุ้นเพียงพอที่จะทำให้อยากเรียนคณิตศาสตร์ ครูมุ่งแต่สอนเนื้อหา ไม่มีเวลาพอที่จะชี้ให้เห็นถึงประโยชน์ของคณิตศาสตร์ ครูที่สอนคณิตศาสตร์ส่วนใหญ่มักจะได้ยินคำถามจากนักเรียนเสมอว่า “ทำไมต้องเรียนคณิตศาสตร์” หรือ “คณิตศาสตร์มีประโยชน์อย่างไร” และคำตอบที่เรามักได้ยินจนชินหู คือ “คณิตศาสตร์มีประโยชน์ต่อชีวิตประจำวัน” พร้อมทั้งยกตัวอย่างเช่น เราต้องใช้

คณิตศาสตร์ เมื่อเราไปตลาด ไปธนาคาร ไปเล่นกีฬา การเช่าซื้อรถหรือบ้าน หรือ แม้กระทั่งการทำอาหาร ล้วนต้องใช้ความรู้ทางคณิตศาสตร์ทั้งสิ้น ซึ่งเป็นประโยชน์ที่เป็นประจักษ์ของทุกคนอยู่แล้ว แต่นั่นเป็นเพียงประโยชน์ของคณิตศาสตร์พื้นฐานเท่านั้น คนส่วนใหญ่ยังมองไม่เห็นประโยชน์ของคณิตศาสตร์ระดับสูง ยกเว้นคนที่เลือกศึกษาต่อในระดับมหาวิทยาลัย โดยเฉพาะคนที่เลือกเรียนแพทย์ เรียนฟิสิกส์ คณิตศาสตร์ หรือ เศรษฐศาสตร์ เป็นต้น หารู้ไม่ว่าทุกคนได้สัมผัสกับคณิตศาสตร์ระดับสูงเป็นประจำโดยไม่รู้ตัว ถึงแม้นักเรียนจะไม่ชอบคณิตศาสตร์ หารู้ไม่ว่าเขาต้องใช้คณิตศาสตร์ขั้นสูงเป็นประจำ โดยเฉพาะเวลาไปกดเงินที่ตู้เอทีเอ็ม การใช้บัตรเครดิต หรือแม้กระทั่งการท่องเน็ต ปัจจุบันครูที่ดีต้องเป็นครูที่ชอบเรียนไม่ใช่ชอบสอนอย่างเดียว ครูที่ชอบสะสมบทประยุกต์ของคณิตศาสตร์ จะได้เปรียบครูอื่น ๆ ครูที่สอนให้เด็กรู้ถึงประโยชน์ของคณิตศาสตร์จะทำให้นักเรียนชอบคณิตศาสตร์มากขึ้น

ในยุคของเทคโนโลยี เป็นยุคที่โลกเราติดต่อเชื่อมโยงถึงกัน เป็นยุคที่คนส่วนใหญ่นิยมใช้บัตรเครดิต ต้องปกป้องและซ่อนข้อมูลลับของตัวเองจากผู้อื่น คณิตศาสตร์มีบทบาทสำคัญมากควบคู่ไปกับพัฒนาการทางคอมพิวเตอร์และการสื่อสาร ลองนึกภาพการสื่อสารระหว่างธนาคารกับลูกค้าที่ต้องการเบิกเงินจากตู้เอทีเอ็ม ธนาคารจะรู้ได้อย่างไรว่า คนที่มากดเงินจากตู้เอทีเอ็มคือคนที่ได้รับอนุญาตจากธนาคาร ลูกค้าจะต้องใส่รหัสผ่านที่ธนาคารกำหนดให้ ลูกค้าจะมั่นใจได้อย่างไรว่า ระหว่างส่งรหัสผ่านให้ธนาคารจะไม่มีใครแอบดูดข้อมูลระหว่างที่ข้อมูลเดินทางจากตู้เอทีเอ็มไปยังธนาคาร จึงจำเป็นต้องมีระบบรักษาความปลอดภัย ต้องมีระบบการเข้ารหัสและถอดรหัสเพื่อป้องกันไม่ให้มีใครแอบดูดข้อมูลระหว่างทางได้ หรือถ้าดูดข้อมูลไปได้ ก็ไม่สามารถถอดรหัสข้อมูลที่ส่งได้ วิทยาการรหัสลับ (cryptography) เป็นวิชาที่ศึกษาเกี่ยวกับการเข้ารหัสและถอดรหัส ไม่ให้ผู้ไม่หวังดีที่ดักขโมยข้อมูลหรือรหัสผ่านล่วงรู้ถึงข้อความหรือรหัสผ่านที่แท้จริงนั้นได้

สมมุติว่ามีคนสองคนชื่ออลิส (Alice) และบ็อบ (Bob) ซึ่งอยู่ห่างไกลกัน แต่ต้องการสื่อสารส่งข้อความลับถึงกัน ผ่านระบบสื่อสารสาธารณะ วิธีหนึ่งคืออลิสเขียนข้อความที่เป็นความลับนั้น เก็บใส่กล่อง ล็อกกุญแจ แล้วส่งไปให้บ็อบ ปัญหาคือบ็อบจะอ่านข้อความลับนั้นได้อย่างไร แสดงว่าอลิสต้องส่งลูกกุญแจตามไปด้วย ซึ่งย่อมไม่ปลอดภัย เพราะถ้ามีคนแอบขโมยลูกกุญแจไปได้ ก็สามารถจะไขกุญแจแล้วอ่านข้อความที่เป็นความลับได้



อลิส และบ็อบตกลงกันใหม่ว่า จะใช้ระบบสื่อสารที่ผู้รับและผู้ส่ง ถือกุญแจคนละชุด (แม่กุญแจและลูกกุญแจ) สมมุติว่าอลิสต้องการส่งข้อความลับให้บ็อบ อลิสขอให้บ็อบส่งกล่องเปล่าไปให้พร้อมทั้งแม่กุญแจที่ยังไม่กดล็อก โดยบ็อบเก็บลูกกุญแจไว้เอง เมื่ออลิสได้รับกล่อง อลิสใส่ข้อความลงในกล่อง กดล็อกกุญแจ แล้วส่งกลับไปให้บ็อบ บ็อบใช้ลูกกุญแจที่ตัวเองมีอยู่ปลดล็อก บ็อบก็สามารถอ่านข้อความได้ ในทำนองเดียวกัน ถ้าบ็อบต้องการตอบความลับกลับให้อลิส บ็อบจะต้องขอให้อลิสส่งกล่องเปล่า พร้อมแม่กุญแจของอลิสที่ยังไม่ปิดล็อกมาให้ บ็อบใส่ข้อความลงในกล่อง ปิดล็อก แล้วส่งกลับไปให้อลิส ระบบนี้ถือว่ามีความปลอดภัย เพราะไม่ต้องส่งลูกกุญแจให้กัน แต่ไม่สะดวก ถ้ามีคนจำนวนมากต้องการสื่อสารกัน ระบบที่สะดวกและปลอดภัยคือระบบที่แต่ละคนในระบบ ถือลูกกุญแจคนละสองดอก ดอกหนึ่งใช้สำหรับเข้ารหัส สามารถเปิดเผยให้สาธารณะรู้ได้ เรียกว่ากุญแจสาธารณะ (public key) ส่วนอีกดอกหนึ่งใช้สำหรับถอดรหัส ซึ่งต้องเก็บเป็นความลับ เรียกว่ากุญแจส่วนตัว (private key) ถ้าอลิสต้องการส่งข้อความให้บ็อบ อลิสจะต้องใช้กุญแจสาธารณะของบ็อบในการเข้ารหัสข้อความ แล้วส่งข้อความที่เข้ารหัสด้วยกุญแจสาธารณะของบ็อบไปให้บ็อบ บ็อบเป็นคนเดียวที่จะใช้กุญแจส่วนตัวของตนถอดรหัส และอ่านข้อความได้ โดยปกติกุญแจสาธารณะและกุญแจส่วนตัวจะสัมพันธ์กันในเชิงคณิตศาสตร์ ระบบที่จัดว่าเป็นระบบที่ปลอดภัยมาก ๆ ระบบหนึ่ง คือระบบที่อาศัยความยากของการหาจำนวน

เฉพาะสองจำนวนที่เป็นตัวประกอบของจำนวนเต็มจำนวนหนึ่งที่เลือก ในการสร้างและทำความเข้าใจระบบดังกล่าว จะต้องมีความรู้ทางคณิตศาสตร์ต่อไปนี้

พื้นฐานทางคณิตศาสตร์ที่ต้องใช้

คณิตศาสตร์ที่ต้องใช้ในการทำความเข้าใจเรื่องการเข้าและถอดรหัสลับที่จะกล่าวในที่นี้ ได้แก่ การหาตัวหารร่วมมากของจำนวนเต็มบวกสองจำนวน ความรู้เรื่องออยเลอร์ฟีฟังก์ชัน และความรู้เรื่องจำนวนเต็ม มอดุโล n พร้อมทั้งทฤษฎีบทที่เกี่ยวข้องบางทฤษฎี

ขั้นตอนวิธียุคลิด (Euclidean Algorithm) ถ้า x และ y เป็นจำนวนเต็มบวกสองจำนวนที่ไม่ใช่ 0 พร้อมกันแล้ว เราจะแทนตัวหารร่วมมากของ x และ y ด้วย gcd (x, y) เราอาจหาตัวหารร่วมมาก โดยใช้วิธีแยกตัวประกอบเหมือนที่เคยเรียนในระดับมัธยมก็ได้ เช่น การหาตัวหารร่วมมาก ของ 420 และ 90 เราแยกตัวประกอบของ 420 และ 90 ดังนี้

$$420 = 2^2 \times 3 \times 5 \times 7 \quad \text{และ}$$
$$90 = 2 \times 3^2 \times 5$$

ดังนั้น ตัวหารร่วมมากของ 420 และ 90 คือ $2 \times 3 \times 5 = 30$ กล่าวคือ gcd (90, 420) = 30 นอกเหนือจากวิธีการแยกตัวประกอบแล้ว ขั้นตอนวิธียุคลิดเป็นกระบวนการสำหรับหาตัวหารร่วมมากของจำนวนสองจำนวนที่ใช้ความรู้พื้นฐานเรื่องการหารยาว ในการหารยาวเราจะได้ผลหารและเศษ ใช้วิธีหารยาวซ้ำกันไปเรื่อย ๆ จนกว่าจะได้เศษเป็นศูนย์ ดังนี้

$x = q_1 y + r_1$ หาร x ด้วย y ได้ผลลัพธ์ q_1 และเศษ r_1
$y = q_2 r_1 + r_2$ หาร y ด้วย r_1 ได้ผลลัพธ์ q_2 และเศษ r_2
$r_1 = q_3 r_2 + r_3$ หาร r_1 ด้วย r_2 ได้ผลลัพธ์ q_3 และเศษ r_3
$\vdots$
$r_{t-2} = q_t r_{t-1} + r_t$ หาร r_{t-2} ด้วย r_{t-1} ได้ผลลัพธ์ q_t และเศษ r_t
$r_{t-1} = q_{t+1} r_t$ หาร r_{t-1} ด้วย r_t ได้ผลลัพธ์ q_{t+1} และเศษเป็นศูนย์

ในแต่ละขั้นตอน เราหารตัวหารในขั้นตอนก่อนหน้านั้นด้วยเศษ ซึ่งจะทำให้เศษมีค่าเล็กลงตามลำดับ ในที่สุดต้องมีค่าเป็นศูนย์ กล่าวคือ $y > r_1 > r_2 > r_3 > \ldots \geq 0$ ถ้า r_t เป็นเศษตัวสุดท้ายที่ไม่ใช่ศูนย์แล้ว gcd (x, y) = r_t เรียกขั้นตอนการหาตัวหารร่วมมาก โดยวิธีนี้ว่า ขั้นตอนวิธียุคลิด

ตัวอย่าง 1 **จงหา gcd (420, 90)**

(1) $420 = 4 \cdot 90 + 60$ หาร $x = 420$ ด้วย $y = 90$ ได้ผลลัพธ์ $q_1 = 4$ และเศษ $r_1 = 60$

(2) $90 = 1 \cdot 60 + 30$ หาร $y = 90$ ด้วย $r_1 = 60$ ได้ผลลัพธ์ $q_2 = 1$ และเศษ $r_2 = 30$

(3) $60 = 2 \cdot 30$ หาร $r_1 = 60$ ด้วย $r_2 = 30$ ได้ผลลัพธ์ $q_3 = 2$ และเศษ $r_3 = 0$

แสดงว่า gcd (420, 90) = 30 = r_2 ซึ่งเป็นเศษตัวสุดท้ายที่ไม่ใช่ศูนย์ ซึ่งตรงกับค่าที่หาได้ด้วยวิธีแยกตัวประกอบ

จากขั้นตอน (2) ข้างบนนี้ ถ้าเราเขียน 30 ใหม่ แล้วแทนค่าย้อนกลับขึ้นไปเรื่อยจะได้

$$\begin{aligned} 30 &= 90 - 1 \cdot 60 \\ &= 90 - 1 \cdot (420 - 4 \cdot 90) \\ &= 90 - 1 \cdot 420 + 4 \cdot 90 \\ &= (90 + 4 \cdot 90) - 1 \cdot 420 \\ &= (1 + 4) \cdot 90 - 1 \cdot 420 \\ &= 5 \cdot 90 - 1 \cdot 420 \end{aligned}$$

เราได้ $30 = 5 \cdot 90 - 1 \cdot 420$

ในกรณีทั่วไป ถ้า gcd (x, y) = d แล้ว เราสามารถเขียน d ในรูป ax + by = d โดยที่ a และ b คือจำนวนเต็มบางจำนวน เรียก d ที่เขียนในรูปแบบนี้ว่า รูปการรวมเชิงเส้นของ x และ y ในตัวอย่าง 1 จะเห็นว่า gcd (420, 90) = 30 และ $30 = 5 \cdot 90 - 1 \cdot 420$ ในที่นี้ a = 5 และ b = −1 ในกรณีเฉพาะ ถ้า gcd (x, y) = 1 แล้วเราย่อมหา a และ b ซึ่งทำให้ ax + by = 1 ได้เสมอ

ตัวอย่าง 2 **จงหา gcd (192, 7)**

(1) $192 = 27 \cdot 7 + 3$ หาร $x = 192$ ด้วย $y = 7$ ได้ผลลัพธ์ $q_1 = 27$ และเศษ $r_1 = 3$

(2) $7 = 2 \cdot 3 + 1$ หาร $y = 7$ ด้วย $r_1 = 3$ ได้ผลลัพธ์ $q_2 = 2$ และเศษ $r_2 = 1$

(3) $3 = 3 \cdot 1$ หาร $r_1 = 3$ ด้วย $r_2 = 1$ ได้ผลลัพธ์ $q_3 = 3$ และเศษ $r_3 = 0$

แสดงว่า gcd (192, 7) = 1 = r_2 ซึ่งเป็นเศษตัวสุดท้ายที่ไม่ใช่ศูนย์

จากขั้นตอน (2) ถ้าเราเขียน 1 ใหม่ แล้วแทนค่าย้อนกลับขึ้นไปเรื่อย ๆ จะได้

$$\begin{aligned} 1 &= 7 - 2\cdot 3 \\ &= 7 - 2(192 - 27\cdot 7) \\ &= 7 - 2\cdot 192 + 54\cdot 7 \\ &= (7 + 54\cdot 7) - 2\cdot 192 \\ &= (1 + 54)\cdot 7 - 2\cdot 192 \\ &= 55\cdot 7 - 2\cdot 192 \end{aligned}$$

จะเห็นว่า เราสามารถเขียน 1 ในรูปการรวมเชิงเส้นของ 192 และ 7 ได้คือ $1 = 55\cdot 7 - 2\cdot 192$

ออยเลอร์ฟีฟังก์ชัน (Euler ϕ-function)

สำหรับจำนวนเต็ม $n > 1$ ให้ $\Phi(n)$ แทนจำนวนสมาชิกในเซต $\{1, 2, \ldots, n-1\}$ ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ n กล่าวคือเป็นจำนวนของจำนวนเต็ม a ซึ่ง $1 \le a \le n$ และ $\gcd(a, n) = 1$ เช่น ถ้า $n = 8$ พิจารณาเซต $\{1, 2, 3, 4, 5, 6, 7\}$ จะพบว่า

$\gcd(1, 8) = \gcd(3, 8) = \gcd(5, 8) = \gcd(7, 8) = 1$

นั่นคือมี a เท่ากับ 1, 3, 5, และ 7 เพียง 4 จำนวนเท่านั้นที่เป็นจำนวนเฉพาะสัมพัทธ์กับ 8 ดังนั้น $\Phi(8) = 4$ เห็นได้ชัดว่า ถ้า p เป็นจำนวนเฉพาะแล้ว $\Phi(p) = p - 1$ เช่น $\Phi(11) = 10$ เพราะจำนวนเต็มทุกจำนวนในเซต $\{1, 2, \ldots, 10\}$ เป็นจำนวนเฉพาะสัมพัทธ์กับ 11 เรียก $\Phi(n)$ ว่า ออยเลอร์ฟีฟังก์ชัน ทฤษฎีบทที่สำคัญคือ ถ้า p และ q เป็นจำนวนเฉพาะแล้ว $\Phi(pq) = (p-1)(q-1)$ เช่น ถ้า $p = 13$ และ $q = 17$ แล้ว $\Phi(pq) = 12\cdot 16 = 192$ เป็นต้น

จำนวนเต็มมอดุโล n

ให้ a, b และ n เป็นจำนวนเต็มซึ่ง $n > 1$ ถ้า n หาร $a - b$ ได้ลงตัวแล้ว เราจะกล่าวว่า a คอนกรูเอน (congruence) กับ b มอดุโล n หรือเขียน $a \equiv b \pmod n$ เช่น

$2 \equiv 5 \pmod 3$ เพราะ 3 หาร $2 - 5 = -3$ ได้ลงตัว หรือ

$-7 \equiv 4 \pmod{11}$ เพราะ 11 หาร $-7 - 4 = -11$ ได้ลงตัว

เราสามารถพิสูจน์สมบัติ 2 ข้อ ต่อไปนี้ได้ไม่ยากนัก

1. ถ้า $a \equiv b \pmod n$ และ $b \equiv c \pmod n$ แล้ว $a \equiv c \pmod n$
2. ถ้า $a \equiv b \pmod n$ และ $c \equiv d \pmod n$ แล้ว $ac \equiv bc \pmod n$

จากสมบัติข้อ 2. ถ้าให้ $c = a$ และ $d = b$ เราได้ $a^2 \equiv b^2 \pmod n$ ในกรณีทั่วไป เราสรุปได้ว่า $a^k \equiv b^k \pmod n$ สำหรับ k ที่เป็นจำนวนเต็มบวกใด ๆ

ตัวอย่าง 3

เนื่องจาก $5^5 = 3125 \equiv 31 \pmod{221}$ และจากสมบัติข้อ 2. เราได้

$(5^5)^3 \equiv 31^3 \pmod{221}$ แต่

$31^3 = 29791 \equiv 177 \pmod{221}$

จากสมบัติข้อ 1. สรุปได้ว่า $(5^5)^3 \equiv 177 \bmod(221)$ จากสมบัติข้อ 2. เราได้

$5^{17} = (5^5)^3 \cdot 5^2 \equiv 177\cdot 25 \equiv 4425 \equiv 5 \pmod{221}$

ตัวอย่าง 4

จากสมบัติข้อ 1. และข้อ 2. เช่นกัน เราได้

$114^5 \equiv 173 \pmod{221}$ และ $114^{55} = (114^5)^{11} \equiv 173^{11} \equiv 75 \pmod{221}$

ในกรณีที่เลขชี้กำลังมีขนาดใหญ่มาก ๆ และใหญ่กว่า n ทฤษฎีบทของออยเลอร์มีประโยชน์ต่อการคำนวณเป็นอย่างยิ่ง

ทฤษฎีบทของออยเลอร์ (Euler's Theorem) ถ้า $\gcd(a, n) = 1$ แล้ว $a^{\Phi(n)} \equiv 1 \pmod n$

ดังนั้น ถ้า p เป็นจำนวนเฉพาะซึ่ง $\gcd(p, a) = 1$ แล้ว $a^{p-1} \equiv 1 \pmod p$ เพราะ $\Phi(p) = p - 1$

ตัวอย่าง 5

การคำนวณค่า $2^{43210} \pmod{101}$ เราทำได้ดังนี้

เนื่องจาก $\gcd(101, 2) = 1$ ดังนั้น $2^{100} \equiv 1 \pmod{101}$ และ $2^{43210} \equiv (2^{100})^{432}2^{10} \equiv 1^{432}2^{10} \equiv 1024 \equiv 14 \pmod{101}$

ขั้นตอนการสร้างระบบรักษาความปลอดภัย

สมมุติว่าอลิสต้องการส่งข้อความซึ่งแทนด้วยจำนวนเต็มบวก m ให้บ็อบ

1.บ็อบเลือกจำนวนเฉพาะสองจำนวนคือ p และ q แล้วหาผลคูณ n = pq

2.บ็อบเลือกเลขชี้กำลัง e ซึ่งสอดคล้องกับสมบัติ gcd (e, (p – 1)(q – 1)) = 1

3.บ็อบสามารถประกาศค่าของ n และ e ให้สาธารณะรู้ได้ แต่บ็อบต้องเก็บ p และ q ไว้เป็นความลับ ไม่ให้ใครล่วงรู้

4.อลิสเข้ารหัส m โดยคำนวณค่า $c \equiv m^e \pmod{n}$ แล้วส่ง c ไปให้บ็อบ

5.เนื่องจากบ็อบเป็นคนเดียวที่รู้ค่าของ p และ q บ็อบสามารถคำนวณค่า (p – 1)(q – 1) ได้โดยง่าย ซึ่งจะทำให้บ็อบสามารถหา d ที่สอดคล้องกับ $de \equiv 1 \pmod{(p-1)(q-1)}$ ได้ จะเห็นว่า p และ q เปรียบเสมือนกุญแจส่วนตัวที่ใช้สำหรับถอดรหัส ผู้ที่จะคำนวณค่า d ได้ จะต้องรู้ p และ q นั่นคือรู้ p – 1 และ q – 1

6.เมื่อบ็อบได้รับ c บ็อบทำการถอดรหัสโดยการคำนวณค่า c^d ดังนี้ เนื่องจาก $c = m^e$ ดังนั้น

$$c^d = (m^e)^d = m^{de} = m \bmod (p-1)(q-1)$$

เพราะ $de \equiv 1 \pmod{(p-1)(q-1)}$ จะเห็นว่า $c^d = m$ ซึ่งก็คือจำนวนเต็มบวกที่อลิสต้องการส่งให้บ็อบนั่นเอง

ตัวอย่าง 6

สมมุติว่า m = 75 แทนข้อความที่อลิสต้องการส่งให้บ็อบ

1.บ็อบเลือกจำนวนเฉพาะ p = 13 และ q = 17 ดังนั้น n = pq = 221 และ (p – 1)(q – 1) = 192

2.บ็อบเลือกเลขชี้กำลัง e = 7 ซึ่ง gcd (7, (p – 1)(q – 1)) = gcd (7, 192) = 1 ดูตัวอย่าง 2

3.บ็อบประกาศค่า n = 221 และ e = 7 ให้สาธารณะรวมทั้งอลิสรู้

4.อลิสเข้ารหัสข้อความ m โดยคำนวณค่า $c \equiv m^e \pmod{n}$ จะได้ $c \equiv 75^7 \equiv 114 \pmod{221}$ แล้วส่งค่า c = 114 ให้บ็อบ

5.เนื่องจากบ็อบรู้ค่า p และ q บ็อบสามารถคำนวณค่า (p – 1)(q – 1) = 192 แล้วใช้ความรู้เรื่องขั้นตอนวิธีของยุคลิดหาค่า d ที่สอดคล้องกับ $de \equiv 1 \bmod 192$ จากตัวอย่าง 2 จะเห็นว่า

$$1 = 55 \cdot 7 - 2 \cdot 192$$

ดังนั้น $1 \equiv 55 \cdot 7 \bmod 192$ เพราะ $2 \cdot 192 \equiv 0 \bmod 192$ แสดงว่า d = 55

6.บ็อบคำนวณค่า $c^d \pmod{n}$ จะได้

$c^d \equiv 114^{55} \equiv 75 \pmod{221}$ ดูตัวอย่าง 3

ซึ่งตรงกับจำนวนที่อลิสส่งให้บ็อบนั่นเอง

เห็นได้ชัดว่า ถ้ารู้ p และ q เราสามารถหา n = pq ได้โดยง่าย แต่ในทางกลับกัน ถ้ารู้ n จะหาจำนวนเฉพาะ p และ q ที่มีผลคูณเท่ากับ n ทำได้ยากมาก ซึ่งเป็นสาเหตุให้การถอดรหัสทำได้ยาก ส่วนการเข้ารหัสทำได้โดยง่าย

เพื่อให้การถอดรหัสทำได้ยาก ในทางปฏิบัติ จะเลือก p และ q ที่มีขนาดใหญ่ เช่น อาจเลือก p = 885320963 และ q = 238855417 ซึ่งจะทำให้ผลคูณ n = pq = 211463707796206571 และอาจเลือกเลขชี้กำลัง e = 9007 ซึ่ง gcd (9007, (p – 1)(q – 1)) = 1 เป็นต้น ซึ่งไม่สามารถคำนวณด้วยเครื่องคิดเลขปกติได้ ต้องอาศัยคอมพิวเตอร์ช่วย ถ้า n มีค่าใหญ่พอ การคำนวณด้วยคอมพิวเตอร์อาจต้องใช้เวลาถึงร้อยปี ซึ่งไม่คุ้มค่ากับความพยายามถอดรหัสข้อความ และข้อความนั้นก็อาจจะล้าสมัยแล้วก็ได้

ผู้อ่านคงสงสัยว่าทำไมคนสองคนที่สื่อสารกันต้องชื่ออลิสและบ็อบ ใช้ชื่ออื่นไม่ได้หรือ คำตอบก็คือได้ แต่เป็นที่รู้กันในวงการที่เกี่ยวกับการสื่อสารรหัสลับว่า เมื่อกล่าวถึงอลิส และบ็อบจะหมายถึงคนสองคนใด ๆ ที่ต้องการสื่อสารกัน เพียงเพื่อสะดวกต่อการอธิบายเท่านั้น ที่จริงแล้วยังมีอีกคนหนึ่งที่มีบทบาทสำคัญ คือ อีฟ(Eve) ซึ่งเป็นที่รู้กันว่าอีฟคือผู้ร้ายที่คอยดักขโมยข้อมูลระหว่างทาง

บรรณานุกรม

Trappe, Wade & Washington, Lawrence C. (2006). *Introduction to Cryptography with Coding Theory.* (2nd edition). New Jersey: Prentice-Hall.