บทที่ 2

วิชาทฤษฎีจำนวน

วิชาทฤษฎีจำนวนที่ศึกษาในเริ่มแรกเป็นวิชาที่เกี่ยวข้องกับการศึกษาสมบัติของจำนวนธรรมชาติ ได้แก่ 1, 2, 3, 4, ... ซึ่งมีอีกชื่อว่า จำนวนนับ หรือจำนวนเต็มบวก ในยุคต้นของกรีก ถ้ากล่าวถึงจำนวนจะหมายถึงจำนวนเต็มบวก ในปัจจุบันคำว่าจำนวนเต็มจะหมายถึง จำนวนเต็มบวก ศูนย์ และจำนวนเต็มลบ

ตัวอย่างของสมบัติของจำนวนเต็มที่ศึกษาในยุคแรก

1. จำนวนเต็มบวกจะหารด้วย 3 ลงตัวก็ต่อเมื่อผลบวกของเลขโดดทุกตัวรวมกันแล้วหารด้วย 3 ลงตัว เช่น 9852 หารด้วย 3 ลงตัว เพราะ 9 + 8 + 5 + 2 = 24 ซึ่งหารด้วย 3 ลงตัว
2. สมการ $X^2 + Y^2 = Z^2$ มีคำตอบเป็นจำนวนเต็มบวกมากมายนับไม่ถ้วน 3, 4, 5 เป็นคำตอบชุดหนึ่ง เพราะ $3^2 + 4^2 = 5^2$ แต่สมการ $X^3 + Y^3 = Z^3$ และ $X^4 + Y^4 = Z^4$ ไม่มีคำตอบเป็นจำนวนเต็มบวก
3. มีจำนวนเฉพาะมากมายนับไม่ถ้วน ลำดับของจำนวนเฉพาะ ได้แก่ 2, 3, 5, 7, 11, 13, 17, ...

มีข้อความบางข้อความในทฤษฎีจำนวนที่ไม่อาจพิสูจน์ได้จนถึงปัจจุบัน เช่น สมการ $X^n + Y^n = Z^n$ ไม่มีคำตอบเป็นจำนวนเต็มบวกเมื่อ n มีค่ามากกว่า 2 แต่แฟร์มาต์ (Fermat, Pierre de ค.ศ. 1601 - 1665) อ้างว่าพิสูจน์ได้ แต่ไม่มีใครพบการพิสูจน์นี้เลย และยังไม่พบข้อหักล้างหรือพิสูจน์ได้ จึงยังคงไม่ใช้เป็นทฤษฎีบท

บ่อยครั้งที่พบว่าความรู้ในทฤษฎีจำนวนได้จากการสังเกตทดลองหลายๆ ครั้ง แล้วสรุปเป็นข้อคาดเดา (Conjecture) จากนั้นภายหลังจึงพยายามพิสูจน์ข้อคาดเดา เช่น เมื่อสังเกตจำนวนธรรมชาติตั้งแต่ 1 – 1000 สามารถเขียนเป็นผลบวกของกำลังสองของจำนวนเต็มที่ไม่ใช่จำนวนลบสี่จำนวนได้ เช่น

$1000 = 30^2 + 10^2 + 0^2 + 0^2$

$999 = 30^2 + 9^2 + 3^2 + 3^2$

จึงตั้งข้อคาดเดาได้ว่าจำนวนธรรมชาติทุกตัวน่าจะทำเช่นนั้นได้ ซึ่งข้อคาดเดานี้ภายหลังได้รับการพิสูจน์ว่าจริงเป็นครั้งแรกโดยลากรองจ์ (Joseph Louis Lagrange ค.ศ. 1736 - 1813) นักคณิตศาสตร์ชาวฝรั่งเศส

วิธีการสังเกตจากตัวอย่างจำนวนหนึ่ง แล้วตั้งข้อคาดเดานี้ ในบางครั้งอาจได้ข้อคาดเดาที่ผิดเช่น การสังเกตว่าเมื่อแทนค่า n = 1, 2, 3, ... , 40 ใน $n^2 - n + 41$ พบว่าผลออกมาเป็น 41, 43, 47, 53, ..., 1601 ซึ่งเป็นจำนวนเฉพาะทั้งหมด เราอาจด่วนสรุปได้ว่า การแทนค่าตัวแปรดังกล่าวด้วยค่า n = 1, 2, 3, ... ได้ค่าเป็นจำนวนเฉพาะหมดทุกค่า ซึ่งเป็นข้อสรุปที่ผิด เพราะถ้าแทนค่าด้วย n = 41 คำตอบที่ได้ก็ไม่ใช่จำนวนเฉพาะ

การตั้งข้อคาดเดาจากการสังเกตและการทดลองในวิชาทฤษฎีจำนวนนี้จะมีทั้งถูกและผิด และดูเหมือนว่าผู้ตั้งข้อคาดเดาอาจทำงานน้อยกว่าผู้พยายามพิสูจน์ข้อคาดเดานั้น แต่วิธีการดังกล่าวก็เป็นวิธีสำคัญในการค้นพบความรู้ในรูปแบบทั่วไปและเป็นประโยชน์ต่อการทดสอบข้อคาดเดา อีกทั้งยังมีประโยชน์ต่อการทำความเข้าใจทฤษฎีบทต่างๆ อันจำเป็นสำหรับผู้ศึกษาหาความรู้ในสาขาวิชานี้ที่จะต้องทดลองกับตัวเลขเพื่อทำความเข้าใจก่อนที่จะพิสูจน์

วิชาทฤษฎีจำนวนไม่เพียงแต่จะเป็นวิชาที่เป็นระบบ แต่ยังเป็นวิชาที่สนุก เพลิดเพลิน มีเนื้อหาที่เป็นคณิตศาสตร์นันทนาการ รวมทั้งยังมีความประหลาดมหัศจรรย์ มีปัญหาน่าฉงน ท้าทายความคิด ซึ่งหากได้ศึกษาวิชาทฤษฎีจำนวนอย่างมีระบบแล้ว จะช่วยในการแก้ปัญหาท้าความคิดเหล่านั้นได้เป็นอย่างดี

วิชาทฤษฎีจำนวนยังเกี่ยวข้องผูกพันกับคณิตศาสตร์แขนงอื่นๆ เช่น พีชคณิตนามธรรม พีชคณิตเชิงเส้น วิชาเชิงวิธีจัดหมู่ การวิเคราะห์เรขาคณิตและโทโพโลยี ผลที่ได้จากการศึกษาวิชาทฤษฎีจำนวนคือวิธีการพิสูจน์ที่มีแนวคิดและหลักการที่เป็นพื้นฐานสำคัญของการพิสูจน์ในวิชาคณิตศาสตร์สองหลักการคือ หลักการเป็นอันดับดีแล้วและหลักการอุปนัยเชิงคณิตศาสตร์ ซึ่งทั้งสองหลักการนี้สมมูลกัน กล่าวคือ สามารถพิสูจน์หลักการอันใดอันหนึ่งได้หากยอมรับหลักการอีกอันหนึ่ง

2.1 ประวัติความเป็นมาของวิชาทฤษฎีจำนวน

เป็นที่ยอมรับกันว่า ปีทาโกรัส (Pythagoras 580 – 496 ปีก่อนคริสต์ศักราช) และบรรดาศิษย์เป็นผู้ริเริ่มในการพัฒนาวิชาทฤษฎีจำนวน ปีทาโกรัสและบรรดาศิษย์เชื่อว่ากุญแจดอกสำคัญที่จะใช้อธิบายสิ่งต่างๆ ในจักรวาลได้คือ จำนวน แนวคิดของคนกลุ่มนี้ยึดปรัชญาว่า ทุกสิ่งทุกอย่างคือจำนวน

การศึกษาจำนวนในสมัยของปีทาโกรัสได้นำความมหัศจรรย์ของจำนวนไปผูกพันกับความเชื่อโชคลาง โหราศาสตร์และโชคชะตาราศีต่างๆ เช่น จำนวนมิตรภาพคู่แรกที่เชื่อว่าพบในสมัยของปีทาโกรัสคือ 284 และ 220 โดยที่สองจำนวนนี้มีคุณสมบัติพิเศษคือตัวหารแท้ของจำนวนหนึ่งมีผลบวกเท่ากับอีกจำนวนหนึ่ง เช่น ตัวหารแท้ของ 284 ได้แก่ 1, 2, 4, 71 และ 142 มีผลบวก

เป็น 220 และตัวหารแท้ของ 220 ได้แก่ 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 และ 110 มีผลบวกเป็น 284 ผู้ที่เชื่อโชคลางจะจารึกตัวเลขลงในเครื่องลางของขลัง โดยเชื่อว่าคนคู่ใดห้อยของขลังที่จารึกตัวเลขดังกล่าวจะเป็นมิตรแท้ต่อกัน ต่อมาผู้ที่พบจำนวนมิตรภาพคู่ที่สองคือ แฟร์มาต์ พบ 17,296 กับ 18,416 ในปี ค.ศ. 1636 จากนั้นต่อมาก็มีผู้พบจำนวนมิตรภาพเพิ่มมากขึ้นเรื่อยๆ

ตัวอย่างเกี่ยวกับความเชื่อถือในความมหัศจรรย์ของจำนวนคือ จำนวนสมบูรณ์ ซึ่งมีคุณสมบัติพิเศษคือจำนวนดังกล่าวจะมีค่าเท่ากับผลบวกของตัวหารแท้ทั้งหมดของจำนวนนั้น เช่น 6 เป็นจำนวนสมบูรณ์ เพราะมี 1, 2, 3 เป็นตัวหารแท้ และ 6 = 1 + 2 + 3 ในสมัยนั้นเชื่อว่าพระเจ้าสร้างโลก และสามารถสร้างเสร็จใน 6 วัน จึงถือว่า 6 เป็นจำนวนสมบูรณ์ จนถึงปี ค.ศ. 1952 มีการพบจำนวนสมบูรณ์รวม 12 จำนวน ทุกจำนวนเป็นจำนวนคู่ สามจำนวนแรกคือ 6, 28 และ 496 ซึ่งในหนังสืออิลิเมนต์(Element) ของยูคลิด ประมาณ 300 ปีก่อนคริสต์ศักราชมีการพิสูจน์ว่า ถ้า $2^n - 1$ เป็นจำนวนเฉพาะแล้ว $2^{n-1}(2^n - 1)$ จะเป็นจำนวนสมบูรณ์ เมื่อ n เป็นจำนวนเต็มบวก

การศึกษาเกี่ยวกับวิชาทฤษฎีจำนวนมีหลักฐานที่เด่นชัดในสมัยของกรีกประมาณ 300 ปีก่อนคริสต์ศักราช ปรากฏในหนังสืออิลิเมนต์ของยูคลิด ประมาณ 450 – 380 ปีก่อนคริสต์ศักราช มีอยู่ 13 เล่ม เล่มที่ 7, 8 และ 9 มีเนื้อหาเกี่ยวกับวิชาทฤษฎีจำนวน เนื้อหาที่รู้จักกันดีในปัจจุบัน ได้แก่ จำนวนคี่ จำนวนคู่ จำนวนเฉพาะ ตัวหารร่วมมาก ตัวคูณร่วมน้อย รวมทั้งทฤษฎีบทขั้นตอนวิธีของยูคลิดและทฤษฎีบทที่กล่าวถึงจำนวนเฉพาะว่ามีมากมายนับไม่ถ้วน

นักคณิตศาสตร์ที่ได้รับขนานนามว่า บิดาแห่งวิชาทฤษฎีจำนวน คือ แฟร์มาต์

2.2 จำนวนเต็ม

เซตของจำนวนเต็มแทนด้วยสัญลักษณ์ I เป็นเซตที่ประกอบด้วยสมาชิก ดังนี้ $I = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$ การศึกษาสมบัติของจำนวนเต็มกับการบวก การลบ การคูณ อาจศึกษาได้หลายแนวทาง แนวทางหนึ่งเริ่มจากจำนวนจริง แล้วสร้างจำนวนเต็มบวกโดยอาศัยเซตเชิงอุปนัย อีกแนวทางหนึ่งเริ่มจากจำนวนนับแล้วสร้างจำนวนเต็มจากจำนวนนับ ซึ่งจะได้ผลสรุปทั้งสองแบบว่าเซตของจำนวนเต็มกับการบวก การลบและการคูณ มีคุณสมบัติเบื้องต้นดังต่อไปนี้

2.2.1 สมบัติปิด $a + b \in I$ และ $a * b \in I$

2.2.2 สมบัติการเปลี่ยนกลุ่ม

$(a + b) + c = a + (b + c)$ และ $(a * b) * c = a * (b * c)$

2.2.3 สมบัติการมีเอกลักษณ์

มี $\acute{a} \in I$ ซึ่ง $\acute{a} + a = a + \acute{a} = a$ และ มี $\acute{a} \in I$ ซึ่ง $\acute{a} * a = a * \acute{a} = a$

2.2.4 สมบัติการมีอินเวอร์ส $-a + a = 0$ และ $a * a^{-1} = a^{-1} * a = 1$ เมื่อ $a \neq 0$

2.2.5 สมบัติการสลับที่ $a + b = b + a$ และ $a * b = b * a$

2.2.6 สมบัติการแจกแจง $a * (b + c) = a * b + a * c$

2.2.7 สมบัติการตัดออก ถ้า $a + b = c + b$ แล้ว $a = c$ และ ถ้า $a * b = c * b$ และ b ไม่เท่ากับ 0 แล้ว $a = c$

2.2.8 สมบัติเกี่ยวกับการลบ $a - b = a + (-b)$ และ สำหรับ a, b ทุกตัวที่ $a, b \in I$ จะได้ว่า $a - b \in I$

2.3 ทฤษฎีจำนวนในชุดโปรแกรมทฤษฎีจำนวน

ในชุดโปรแกรมทฤษฎีจำนวนนี้ได้นำเนื้อหาจากวิชาทฤษฎีจำนวนบางส่วนมาพัฒนาเป็นโปรแกรมที่ช่วยในการคำนวณ ดังต่อไปนี้

(1) การหาตัวหารร่วมมากโดยวิธีของยูคลิด (Euclidean Algorithm) และการหาตัวหารร่วมมากด้วยวิธีเศษเหลือน้อยที่สุด (Least Remainder Algorithm)

(2) การหาจำนวนเฉพาะ

(3) การหาค่าฟังก์ชั่นฟี(ϕ), เทา(τ)และซิกม่า(σ)

(4) การแยกตัวประกอบของจำนวนต่างๆ

(5) การแยกตัวประกอบโดยวิธีของโพลาร์ด(Polard Rho Factorization)

(6) การแยกตัวประกอบโดยวิธีของแฟร์มาต์ (Fermat Factorization)

(6) สมการไดโอแฟนไทน์(Diophantine)

(7) ระบบคอนกรูเอนซ์ (Congruence) และ Round Robin Tournament

(8) การเปลี่ยนจำนวนตรรกยะเป็นเศษส่วนต่อเนื่องจำกัด

(9) การเปลี่ยนเศษส่วนต่อเนื่องจำกัดเป็นจำนวนตรรกยะ

(10) การเปลี่ยนเศษส่วนต่อเนื่องอนันต์เป็นจำนวนอตรรกยะ

(11) การเปลี่ยนจำนวนอตรรกยะเป็นเศษส่วนต่อเนื่องอนันต์

(12) การแยกตัวประกอบโดยการใช้เศษส่วนต่อเนื่อง

(13) การเข้ารหัสแบบซีซ่า (Caesar Encryption)

(14) การเข้ารหัสแบบบล็อค (Block Encryption)

(15) การเข้ารหัสแบบแอฟไฟน์ (Affine Encryption)

(16) การเข้ารหัสแบบแนบแสค (Knapsack Encryption)

(17) การเข้ารหัสแบบอาร์เอสเอ (RSA Encryption)

(18) Elliptic Curve และ Quadratic Residue

2.3.1 ตัวหารร่วมมากและขั้นตอนวิธีของยูคลิด

ในหัวข้อนี้จะกล่าวถึงบทนิยามของตัวหารร่วมมากของจำนวนเต็มบวกสองจำนวน ตัวหารร่วมมากของจำนวนเต็มบวกมากกว่าสองจำนวน

บทนิยามที่ 1 ให้ a และ b เป็นจำนวนเต็มที่ $a \neq 0$ เราจะกล่าวว่า a หาร b ลงตัว (a divides b) ถ้ามีจำนวนเต็ม c ซึ่ง $b = ac$ และเราเรียก a ว่า ตัวหาร(divisor) หรือตัวประกอบ (factor) ของ b

ถ้า a หาร b ลงตัว เขียนแทนด้วย $a \mid b$ และถ้า a หาร b ไม่ลงตัว เขียนแทนด้วย $a \nmid b$

ทฤษฎีบทที่ 1 ถ้า a, b และ c เป็นจำนวนเต็มที่ $a, b \neq 0$ และ $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$

ทฤษฎีบทที่ 2 ถ้า a, b, m และ n เป็นจำนวนเต็มบวก และถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid (ma + nb)$

ทฤษฎีบทที่ 3 ถ้า a, b เป็นจำนวนเต็ม ซึ่ง $b > 0$ แล้ว จะมีจำนวน q และ r เพียงชุดเดียว ซึ่ง $a = bq + r$ โดยที่ $0 \leq r < b$

จากทฤษฎีบทนี้เราเรียก q ว่าผลลัพธ์ (quotient) และเรียก r ว่า เศษเหลือ (remainder) และเรียก a ว่า ตัวถูกหาร (dividend) และเรียกเรา b ว่า ตัวหาร (divisor)

ถ้า a และ b เป็นจำนวนเต็มซึ่งไม่เป็น 0 ทั้งคู่แล้ว เซตของตัวหารของ a และ b เป็นเซตที่จำกัดซึ่งบรรจุ 1 และ –1 เราจะให้ความสนใจกับตัวหารของจำนวนเต็มสองจำนวนตัวอื่นที่ไม่ใช่ 1 และ –1

บทนิยามที่ 2 ตัวหารร่วมมาก (greatest common divisors) ของจำนวนเต็มสองจำนวน a และ b ซึ่งไม่เป็น 0 พร้อมกัน คือจำนวนเต็มที่ใหญ่ที่สุดที่หารทั้ง a และ b ลงตัว ตัวหารร่วมมากของ a และ b แทนด้วยสัญลักษณ์ (a, b)

บทนิยามที่ 3 จำนวนเต็ม a และ b เรียกว่าเป็นจำนวนเฉพาะสัมพัทธ์กัน (relatively prime) ถ้า $(a, b) = 1$

เราจะสังเกตได้ว่าตัวหารทั้งหมดของ –a เมื่อ a>0 จะเหมือนกับตัวหารทั้งหมดของ a ซึ่งจะทำให้ได้ว่า (a, b) = (|a|, |b|) โดยที่ |a| แทนค่าสัมบูรณ์ของ a และ (a, 0) = a = (0, a) ดังนั้นเราจะกล่าวถึงการหาตัวหารร่วมมากของจำนวนเต็มบวกเท่านั้น

ทฤษฎีบทที่ 4 **ให้** a, b **และ** c เป็นจำนวนเต็มบวก ซึ่ง (a, b) = d แล้ว

(1) (a/d, b/d) = 1

(2) (a+cb, b) = (a, b)

ตัวหารร่วมมากของจำนวนเต็มบวก a และ b สามารถที่จะเขียนเป็นผลบวกเชิงเส้นของ a และ b ได้

การหาตัวหารร่วมมากของจำนวนเต็มบวกสองจำนวนโดยหาตัวหารร่วมทั้งหมดก่อนแล้วเลือกตัวหารร่วมที่มีค่ามากที่สุดนั้นไม่สะดวกอย่างยิ่งในทางปฏิบัติ โดยเฉพาะอย่างยิ่งเมื่อตัวเลขมีค่ามากๆ วิธีที่มีประสิทธิภาพมากกว่าคือ การใช้ขั้นตอนวิธีของยูคลิด (Euclidean Algorithm) ซึ่งเป็นผลจากการใช้ Division Algorithm ในทฤษฎีบทที่ 3 ซ้ำๆ กันอย่างต่อเนื่องเป็นจำนวนครั้งที่จำกัด วิธีการดังกล่าวนี้ยูคลิดได้เขียนไว้ในหนังสืออิลิเมนต์เล่มที่ 7 แม้จะมีหลักฐานยืนยันว่า วิธีการดังกล่าวเป็นที่ทราบกันก่อนสมัยยูคลิด แต่เพื่อเป็นเกียรติกับยูคลิดที่ได้รวบรวมไว้ในสมัยต่อมาจึงยังคงเรียกว่าขั้นตอนวิธีของยูคลิด

ทฤษฎีบทที่ 5 ถ้า a และ b เป็นจำนวนเต็มและ a = bq + r โดยที่ q และ r เป็นจำนวนเต็มแล้ว (a, b) = (b, r)

ทฤษฎีบทที่ 6 **ให้** $r_0 = a$ และ $r_1 = b$ เป็นจำนวนเต็มบวกซึ่ง $a \geq b > 0$ ถ้าปรับปรุง Division algorithm เป็น $r_i = r_{j+1} q_{j+1} + r_{j+2}$ โดยที่ $0 < r_{j+2} < r_{j+1}$ สำหรับ j = 1, 2, ..., n-2 และ $r_{n+1} = 0$ แล้ว (a, b) = r_n ซึ่งเป็นจำนวนเศษเหลือที่ไม่เป็นศูนย์ตัวสุดท้าย จากทฤษฎีบทนี้ทำให้เราเห็นว่าตัวหารร่วมมากของ a และ b เป็นเศษเหลือที่มากกว่าศูนย์ตัวสุดท้าย

ตัวอย่าง จงหา (252 , 198) โดยใช้ขั้นตอนวิธีของยูคลิด

252 = 1 . 198 + 54

198 = 3 . 54 + 36

54 = 1 . 36 + 18

$36 = 2 \cdot 18$

ดังนั้น $(252, 198) = 18$

การหาตัวหารร่วมมากของสองจำนวนที่มีขนาดไม่ใหญ่มากนั้นอาจจะยังไม่เห็นถึงประสิทธิภาพของขั้นตอนวิธีของยูคลิด แต่หากเป็นการหาตัวหารร่วมมากของสองจำนวนที่มีขนาดใหญ่มากๆ จะเห็นถึงประสิทธิภาพของขั้นตอนวิธีนี้ ดังตัวอย่างต่อไปนี้

ตัวอย่าง จงหาตัวหารร่วมมากของ 1,160,718,174 และ 316,258,250

1,160,718,174 = 3 x 316,258,250 + 211,943,424

316,258,250 = 1 x 211,943,424 + 104,314,826

211,943,424 = 2 x 104,314,826 + 3,313,772

104,314,826 = 31 x 3,313,772 + 1,587,894

3,313,772 = 2 x 1,587,894 + 137,984

1,587,894 = 11 x 137,984 + 70,070

137,984 = 1 x 70,070 + 67,914

70,070 = 1 x 67,914 + 2,156

67,914 = 31 x 2,156 + 1,078

2,156 = 2 x 1,078 + 0

ดังนั้นตัวหารร่วมมากระหว่าง 1,160,718,174 และ 316,258,250 คือ 1,078

2.3.2 ขั้นตอนวิธีเศษเหลือน้อยที่สุด (Least – Remainder Algorithm)

จากการปรับปรุงขบวนการขั้นตอนในการหาตัวหารร่วมมากโดยให้ a และ b เป็นจำนวนเต็มบวก แล้วจะมีจำนวนเต็มบวก q, r และ e เพียงชุดเดียวที่ $a = bq + er$ โดยที่ $e = 1$ หรือ -1 และ $-b/2 < er < b/2$ เราสามารถกำหนดขบวนการที่แตกต่างจากขั้นตอนวิธีของยูคลิด ซึ่งเราเรียกว่า ขั้นตอนวิธีเศษเหลือน้อยที่สุด

ทฤษฎีบทที่ 7 (Least – Remainder Algorithm) ให้ $r_0 = a$ และ $r_1 = b$ เป็นจำนวนเต็มบวกซึ่ง $a \geq b > 0$ ถ้าปรับปรุง Division algorithm เป็น $r_j = r_{j+1} q_{j+1} + e r_{j+2}$ โดยที่ $0 \leq r_{j+2} < r_{j+1}/2$ และ $e = 1$ หรือ -1 สำหรับ $j = 1, 2, \ldots, n-2$ และ $r_{n+1} = 0$ แล้ว $(a, b) = r_n$ ซึ่งเป็นจำนวนเศษเหลือที่ไม่เป็นศูนย์ตัวสุดท้าย เราสามารถสรุปได้ว่ามีเศษ

เหลือที่เป็นศูนย์ได้เพราะว่าลำดับของเศษเหลือเป็นลำดับลด กล่าวคือ $a = r_0 > r_1 > r_2 > \ldots \geq 0$ จากขั้นตอนวิธีดังกล่าวข้างต้นจะได้ว่า

(1) $(a, b) = (r_0, r_1) = (r_1, er_2) = (|r_1|, |er_2|) = (r_1, r_2)$

(2) $(r_1, r_2) = (r_2, er_3) = (|r_2|, |er_3|) = (r_2, r_3)$

ทำไปเช่นนี้จนกระทั่งเหลือเศษเหลือเป็นศูนย์เราจะได้ว่า

$(a, b) = (r_0, r_1) = (r_1, r_2) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n$

จากทฤษฎีบทนี้ทำให้เห็นว่าตัวหารร่วมมากของ a และ b เป็นเศษเหลือที่ไม่เป็นศูนย์ตัวสุดท้ายเช่นเดียวกับขั้นตอนวิธีของยูคลิด

ตัวอย่าง การหาตัวหารร่วมมากระหว่าง 384 และ 226

STEP 1 $384 = 2 \times 226 + (-1) \times 68$

STEP 2 $226 = 3 \times 68 + 1 \times 22$

STEP 3 $68 = 3 \times 22 + 1 \times 2$

STEP 4 $22 = 11 \times 2 + (-1) \times 0$

ดังนั้นตัวหารร่วมมากคือ 2

เราจะเปรียบเทียบการหาตัวหารร่วมมากของจำนวนเต็มสองจำนวนของวิธีการทั้งสองวิธีว่าวิธีการใดมีประสิทธิภาพมากกว่ากันดังตัวอย่างต่อไปนี้ เราจะทำการหาตัวหารร่วมมากของ 5,321,684 และ 2,348,567

วิธีการของยูคลิด

$5321684 = 2348567(2) + 624550$

$2348567 = 624550(3) + 474917$

$624550 = 474917(1) + 149633$

$474917 = 149633(3) + 26018$

$149633 = 26018(5) + 19543$

$26018 = 19543(1) + 6475$

$19543 = 6475(3) + 118$

$6475 = 118(54) + 103$

$118 = 103(1) + 15$

$103 = 15(6) + 13$

15 = 13(1) + 2

13 = 2(6) + 1

2 = 1(2) + 0

ดังนั้นตัวหารร่วมมากเท่ากับ 1

วิธีการเศษเหลือน้อยที่สุด

5321684 =2 x2348567 + 1 x624550

2348567 =4 x624550 + (-1) x149633

624550 =4 x149633 + 1 x26018

149633 =6 x26018 + (-1) x6475

26018 =4 x6475 + 1 x118

6475 =55 x118 + (-1) x15

118 =8 x15 + (-1) x2

15 =7 x2 + 1 x1

2 =2 x1 + (-1) x0

ดังนั้นตัวหารร่วมมากคือ 1

2.3.3 การทำย้อนกลับ

ขั้นตอนวิธีดังกล่าวทั้งสองวิธีนั้นสามารถใช้ประโยชน์จากการหาตัวหารร่วมมากของจำนวนเต็มบวกสองจำนวนมาเขียนเป็นผลบวกเชิงเส้นของจำนวนทั้งสอง โดยในที่นี้ขอกล่าวถึงการทำย้อนกลับของขั้นตอนวิธีของยูคลิด ก่อนอื่นเราดูการหาค่าตัวหารร่วมมากของ 252 และ 198 ดังนี้

ตัวอย่าง จงหา (252 , 198) โดยใช้ขั้นตอนวิธีของยูคลิด

252 = 1 . 198 + 54 ... ขั้นตอนที่ 1

198 = 3 . 54 + 36 ... ขั้นตอนที่ 2

54 = 1 . 36 + 18 ... ขั้นตอนที่ 3

36 = 2 . 18 ... ขั้นตอนที่ 4

ดังนั้น (252, 198) = 18

และในการทำย้อนกลับจากระบบสมการ

18 = 54 - 1 . 36 ... จากขั้นตอนที่ 3

= 54 - 1(198 - 3 . 54) ... จากขั้นตอนที่ 2

$= 4 \cdot 54 - 1 \cdot 198$

$= 4(252 - 1 \cdot 198) - 1 \cdot 198$ ... จากขั้นตอนที่ 1

$= 4 \cdot 252 - 4 \cdot 198 - 1 \cdot 198$

$= 4 \cdot 252 - 5 \cdot 198$

$= (4)(252) + (-5)(198)$

พบว่าสามารถเขียนเป็นผลบวกเชิงเส้นของ 252 และ 198 ได้เสมอซึ่งจากผลลัพธ์ที่ได้ จะเห็นว่า d = (a, b) จะเป็นผลบวกเชิงเส้นของ a และ b ซึ่งเปรียบเหมือนลำดับของสมการที่เกิดในขั้นตอนวิธีของยูคลิดซึ่งสมการแรกที่ได้นั้นคือ

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

ซึ่งจะได้ (a, b) เขียนเป็นผลบวกเชิงเส้นของ r_{n-2} และ r_{n-1} และต่อไปจะได้ว่า

$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-2}$$

ดังนั้น $(a, b) = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-2}) q_{n-1}$

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

เราเขียน (a, b) เป็นผลบวกเชิงเส้นของ r_{n-3} และ r_{n-2} เราจะทำการย้อนกลับไปจนพบว่า (a, b) สามารถเขียนเป็นผลบวกเชิงเส้นของ $r_0 = a$ และ $r_1 = b$

ทฤษฎีบทที่ 8 ให้ a และ b เป็นจำนวนเต็มบวกแล้ว

$(a, b) = s_n a + t_n b$ สำหรับ $n = 1, 2, 3, \ldots$ เมื่อ s_n และ t_n คือพจน์ที่ n ของลำดับซึ่งนิยามโดย $s_0 = 1$, $t_0 = 0$ และ $s_1 = 0$, $t_1 = 1$ และ

$$s_j = s_{j-2} - q_{j-1} s_{j-1} \quad , \quad t_j = t_{j-2} - q_{j-1} t_{j-1} \text{ สำหรับ } j = 2, 3, 4, \ldots, n$$

2.3.4 จำนวนเฉพาะ

จำนวนเฉพาะคือจำนวนเต็มที่มากกว่า 1 ที่หารลงตัวด้วย 1 หรือตัวมันเองเท่านั้น และจำนวนเต็มที่มากกว่า 1 ที่ไม่ใช่จำนวนเฉพาะ เราเรียกว่า จำนวนประกอบ

จำนวนเฉพาะคู่ มีเพียง 1 จำนวนคือ 2

จำนวนเฉพาะคี่ มีจำนวนนับไม่ถ้วน เช่น 3, 5, 7, 11, 13, ...

โดยที่ 0 และ 1 ไม่ใช่ทั้งจำนวนเฉพาะและจำนวนประกอบ

ดังนั้นอาจกล่าวได้ว่ามีจำนวนเฉพาะเป็นจำนวนอนันต์

ในหนังสือบางเล่ม ถ้า p เป็นจำนวนเฉพาะแล้วจะให้ -p เป็นจำนวนเฉพาะด้วย ดังนั้นจึงนิยามว่า p เป็นจำนวนเฉพาะก็ต่อเมื่อ p ไม่เท่ากับ 0, 1, -1 และ p จะมีตัวหารเพียง 4 ตัวคือ 1, -1, p, -p

ถ้า p เป็นจำนวนเฉพาะและ p หาร ab ลงตัว แล้ว p หาร a ลงตัวหรือ p หาร b ลงตัว โดยที่เราจะเรียกการเขียนจำนวนเต็มบวกในรูปผลคูณของจำนวนเฉพาะโดยที่ไม่คำนึงถึงลำดับการเขียนจำนวนเฉพาะแต่ละตัวว่าการแยกตัวประกอบ และจะสามารถเขียนได้เพียงชุดเดียวเท่านั้น

ตัวอย่าง จงตรวจดูว่า 323 เป็นจำนวนเฉพาะหรือไม่

17 < รากที่สองของ 323 < 18

จำนวนเฉพาะที่น้อยกว่ารากที่สองของ 323 คือ 2, 3, 5, 7, 11, 13, 17

ทดลองนำแต่ละตัวไปหาร 323 พบว่า 17 หาร 323 ได้ลงตัว

ได้ 323 = 17 x 19

ดังนั้น 323 เป็นจำนวนประกอบ

ตัวอย่าง จงตรวจดูว่า 811 เป็นจำนวนเฉพาะหรือไม่

28 < รากที่สองของ 811 < 29

จำนวนเฉพาะที่น้อยกว่ารากที่สองของ 811 คือ 2,3,5,7,11,13,17,19,23

ทดลองนำแต่ละตัวไปหาร 811 พบว่าไม่มีจำนวนใดหาร 811 ได้ลงตัว

ดังนั้น 811 เป็นจำนวนเฉพาะ

2.3.5 ฟังก์ชันทางทฤษฎีจำนวน

ฟังก์ชั่นทางทฤษฎีจำนวนคือฟังก์ชั่นที่มีโดเมนเป็นเซตของจำนวนเต็มบวก ซึ่งฟังก์ชั่นทางทฤษฎีจำนวนที่ได้จัดทำไว้ในชุดโปรแกรมทางทฤษฎีจำนวนมี 3 ฟังก์ชั่น คือ τ, σ และ ϕ

นิยาม ถ้า n เป็นจำนวนเต็มบวก แล้ว

$\tau(n)$ คือจำนวนตัวหารที่เป็นบวกของ n

$\sigma(n)$ คือผลบวกของตัวหารที่เป็นบวกของ n

$\phi(n)$ คือจำนวนของจำนวนเต็มบวกที่น้อยกว่าหรือเท่ากับ n และเป็นจำนวนเฉพาะสัมพัทธ์กับ n

ตารางข้างล่างเป็นค่าของ $\tau(n)$, $\sigma(n)$ และ $\phi(n)$ เมื่อ $1 \leq n \leq 12$

ตาราง 2.1 แสดงค่าฟังก์ชันทางทฤษฎีจำนวนเมื่อค่า N มีค่าตั้งแต่ 1 ถึง 12

N	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6
$\sigma(n)$	1	3	4	7	6	12	8	15	15	18	12	28
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

ทฤษฎีบท ให้ n เป็นจำนวนเต็มบวกที่มากกว่า 1 และถ้า $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

เมื่อ $p_1 p_2 \dots p_r$ เป็นจำนวนเฉพาะที่แตกต่างกัน

และ $k_1, k_2, \dots, k_r$ เป็นจำนวนเต็มบวก แล้ว

$\tau(n) = (k_1+1)(k_2+1) \dots (k_r+1)$

$$\sigma(n) = \left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{k_2+1}-1}{p_2-1}\right) \dots \left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)$$

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \dots \left(1-\frac{1}{p_r}\right)$$

ตัวอย่าง ให้ $n = 360 = 2^3 \cdot 3^2 \cdot 5$

ดังนั้น $\tau(n) = (3+1)(2+1)(1+1)$

$= 4 \cdot 3 \cdot 2 = 24$

$$\sigma(n) = \left(\frac{2^4-1}{2-1}\right)\left(\frac{3^3-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)$$

$$= 15 \cdot \frac{26}{2} \cdot \frac{24}{4}$$

$= 15 \cdot 13 \cdot 6$

$= 1170$

$$\phi(n) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 360\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) \quad = 96$$

2.3.6 **การแยกตัวประกอบโดยวิธีของแฟร์มาต์(Fermat Factorization)และการแยกตัวประกอบโดยวิธีของโพลาร์ด(Polard Rho Factorization)**

จำนวนเต็มบวกทุกจำนวนที่มากกว่าหนึ่งสามารถเขียนให้อยู่ในรูปของผลคูณของจำนวนเฉพาะมากกว่าหรือเท่ากับ 2 จำนวนได้ เรียกการเขียนจำนวนเต็มบวกใดๆในรูปผลคูณของจำนวนเฉพาะว่า"การแยกตัวประกอบ"

ถ้ามีจำนวนใดจำนวนหนึ่งเป็นจำนวนประกอบแล้ว จำนวนดังกล่าวจะมีตัวประกอบที่เป็นจำนวนเฉพาะที่ไม่ใหญ่เกินรากที่สองของจำนวนนั้น

ตัวอย่าง จงตรวจดูว่า 323 เป็นสามารถแยกตัวประกอบได้หรือไม่

17 < รากที่สองของ 323 < 18

จำนวนเฉพาะที่น้อยกว่ารากที่สองของ 323 คือ 2, 3, 5, 7, 11, 13, 17

ทดลองนำแต่ละตัวไปหาร 323 พบว่า 17 หาร 323 ได้ลงตัว

ได้ 323 = 17 x 19

ดังนั้น 323 เป็นจำนวนประกอบ

จำนวนแฟร์มาต์และการแยกตัวประกอบโดยวิธีแฟร์มาต์

จากที่เราทราบแล้วว่าจำนวนเต็มบวกทุกจำนวนสามารถแยกตัวประกอบเป็นผลคูณของจำนวนเฉพาะได้เพียงวิธีเดียว ในวิธีการแยกตัวประกอบของจำนวนเต็มบวก n จะมีตัวประกอบเป็นจำนวนเฉพาะที่ไม่เกินรากที่สองของ n ดังนั้นหากเราหาร n ด้วยจำนวนเฉพาะ 2, 3, 5, ... ตามลำดับที่ไม่เกินรากที่สองของ n ถ้าจำนวนเฉพาะ p_1 หาร n ลงตัวแล้ว p_1 เป็นตัวประกอบของ n เราเก็บ p_1 ไว้แล้วแยกตัวประกอบของผลหารระหว่าง n และ p_1 ตามวิธีดังกล่าวเช่นนี้เรื่อยๆ เราก็จะได้จำนวนเฉพาะที่เป็นตัวประกอบของ n ดังตัวอย่าง

ให้ n = 42833 พบว่า 2, 3, 5 หาร n ไม่ลงตัว แต่ 7 หารลงตัว ดังนั้น 7 เป็นตัวประกอบเฉพาะของ n

n = 42833 = 7 . 6119 (n1 = 6119)

ทดลองหาร 6119 ด้วย 7 ปรากฏว่าหารไม่ลงตัว ทดลองหารด้วย 11, 13, 17, 19, 23 ก็หารไม่ลงตัว แต่ 29 หารลงตัว

ดังนั้น 6119 = 29 . 211

หรือ 42833 = 7 . 29 . 211

วิธีดังกล่าวเป็นวิธีที่ใช้เวลามาก ถ้า n เป็นจำนวนที่ใหญ่มากๆ วิธีการแยกตัวประกอบของจำนวนเต็มบวกที่น่าสนใจและสะดวกคือ Fermat Factorization Method ผู้คิดค้นคือ แฟร์มาต์ ในศตวรรษที่ 17 โดยตั้งอยู่บนบทตั้งที่ว่า ให้ n เป็นจำนวนเต็มบวกคี่ แล้ว n จะเป็นผลคูณของจำนวนเต็ม 2 จำนวนก็ต่อเมื่อ สมการ $n = x^2 - y^2$ มีคำตอบของ x, y เป็นจำนวนเต็ม

วิธีของแฟร์มาต์ใช้ได้อย่างมีประสิทธิภาพ ถ้า n มีตัวประกอบที่มีขนาดไม่ต่างกันมาก แฟร์มาต์ได้คิดวิธีนี้ขึ้นเพื่อแยกตัวประกอบของ n = 2,027,651,281 ซึ่งได้ 2,027,651,281 = 44,021 . 46,061

โดยพิจารณาจากลำดับ 11 พจน์แล้ว ถ้าใช้วิธีหารด้วยจำนวนเฉพาะที่น้อยกว่ารากที่สองของ n = 44021 แล้วต้องใช้จำนวนครั้งของการหารถึง 4,850 ครั้ง ข้อดีวิธีของแฟร์มาต์อีกข้อคือเราไม่จำเป็นต้องทราบจำนวนเฉพาะทุกจำนวนที่น้อยกว่ารากที่สองของ n

ตัวอย่าง จงใช้วิธีแฟร์มาต์ แยกตัวประกอบของ 6077 และ 119143

$77 < \sqrt{6077} < 78$

$78^2 - 6077 = 7$

$79^2 - 6077 = 164$

$80^2 - 6077 = 323$

$81^2 - 6077 = 484 = 22^2$

ดังนั้นจะได้ว่า $6077 = 81^2 - 22^2$

$= (81 + 22)(81 - 22) = 103 . 59$

$345 < \sqrt{119143} < 346$

$346^2 - 119143 = 573$

$347^2 - 119143 = 1266$

$348^2 - 119143 = 1961$

$349^2 - 119143 = 2658$

$350^2 - 119143 = 3357$

$351^2 - 119143 = 4058$

$352^2 - 119143 = 4761 = 69^2$

ดังนั้นจะได้ว่า $119143 = 352^2 - 69^2$

$= (352 + 69)(352 - 69)$

$= 421 . 283$

วิธีการของแฟร์มาต์บางครั้งอาจต้องใช้หลายขั้นตอนกว่าจะพบผลต่างที่เป็นจำนวนกำลังสองสมบูรณ์

การแยกตัวประกอบโดยวิธีของโพลาร์ด(Pollard Rho Factorization)

ให้ m เป็นจำนวนเต็มที่คาดว่ามี p เป็นตัวประกอบเฉพาะ และถ้าสุ่มเลือกจำนวนเต็มบวกที่ต่างๆ กัน k จำนวน

$u_0, u_1, u_2, \ldots, u_k \leq \sqrt{m}$

ซึ่ง $u_j \not\equiv u_i \pmod m$ $\quad 0 \leq i < j$

แต่ $u_j \equiv u_i \pmod p$ $\quad 0 \leq i < j$

จากคอนกรูเอนซ์ทั้งสอง จะได้ว่า $m \nmid (u_j - u_i)$ แต่ $p \mid (u_j - u_i)$

ถ้า $(u_j - u_i , m) > 1$ แล้ว $(u_j - u_i , m)$ เป็นตัวประกอบของ m แต่ในความเป็นจริงแล้วเราต้องการหาตัวประกอบของ m เราจึงยังไม่ทราบตัวประกอบเฉพาะ p ถึงแม้ว่าเราอาจสุ่มได้ลำดับ $u_0, u_1, u_2, \ldots, u_k$ แล้วก็ตาม แต่เราไม่ทราบว่า u_j , u_i ชุดใดที่ทำให้ $(u_j - u_i , m) > 1$ เราจึงต้องสุ่มเลือก u_j , u_i จากลำดับ $u_0, u_1, u_2, \ldots, u_k$ ซึ่งมีถึง $\binom{k+1}{2}$ วิธี และแต่ละคู่ u_j , u_i ที่เลือกได้ต้องใช้ขั้นตอนวิธีของยูคลิดหา $(u_j - u_i , m)$ ซึ่งทั้งสองส่วนนี้ต้องใช้เวลามาก ดังนั้น นักคณิตศาสตร์ชื่อ Pollard ได้คิดวิธีลัดเพื่อสร้าง $u_0, u_1, u_2, \ldots, u_k$ และคิดวิธีลัดเพื่อเลือก u_j , u_i ที่สามารถทำให้ $(u_j - u_i , m) > 1$ ได้เร็วขึ้น ซึ่งมีขั้นตอนดังนี้

1. เลือก u_0
2. เลือกพหุนาม f(x) ที่มีกำลังสูงกว่าหนึ่งและมีสัมประสิทธิ์เป็นจำนวนเต็ม โดยมากมักเลือก $f(x) = x^2 + c$ $(c \neq 0, -2)$

3. คำนวณหา u_i จากความสัมพันธ์ $u_{i+1} = f(u_i) \pmod m$ โดยมีเงื่อนไขว่า $0 < u_{i+1} < m$ ในขั้นตอนนี้จะได้ลำดับของจำนวนเต็มบวก $u_0, u_1, u_2, \ldots, u_k$

ถ้า $u_j \equiv u_i \pmod d$ สำหรับจำนวนเต็มบวก d บางค่า แล้ว $u_{j+1} \equiv u_{i+1} \pmod d$ เพราะว่า $f(u_j) \equiv u_{i+1} \pmod d$ และ $f(u_j) \equiv u_{j+1} \pmod d$ ดังนั้นลำดับ $u_0, u_1, u_2, \ldots, u_i, u_{i+1}, \ldots, u_j, u_{j+1}, \ldots, u_k$ เป็นลำดับที่มีคาบและความยาวคาบเป็น j - i ดังนั้น $u_t \equiv u_s \pmod d$ ได้ เมื่อ $t \equiv s \pmod{j-i}$ ทุก $s, t \geq i$

ดังนั้น $t - s = (j-i)\,k$, สำหรับจำนวนเต็มบวก k บางค่า ในกรณีเฉพาะถ้าเลือก k=1 , s = j - i นั่นคือเลือกให้ s เป็นพหุคูณของ j - i ที่เล็กที่สุดได้ t = 2s ดังนั้น $u_{2s} \equiv u_s \pmod d$

4. หา $(u_{2s} - u_s, m)$ เมื่อ $s = 1, 2, 3, \ldots, k \leq \sqrt{m}$ จนกว่าเราจะพบว่า $(u_{2s} - u_s, m) > 1$ ซึ่งจะได้ว่า $(u_{2s} - u_s, m)$ ที่ได้นี้เป็นตัวประกอบของ m

ตัวอย่าง ให้ m =8051 จงแยกตัวประกอบของ m

เลือก u_0 =2 และให้ $f(x) = x^2 + 1$

ใช้สูตร $u_{i+1} = f(u_i) \pmod{8051}$ ได้ลำดับ u_i ต่อไปนี้

$u_1 = 5$, $u_2 = 26$, $u_3 = 677$, $u_4 = 7474$, $u_5 = 2839$, $u_6 = 871$, $u_7 = 848$, ...

หา $(u_{2s} - u_s, 8051)$, s = 1, 2, 3, ... ได้

$(u_2 - u_1, 8051) = (26 - 5, 8051) = (21, 8051) = 1$

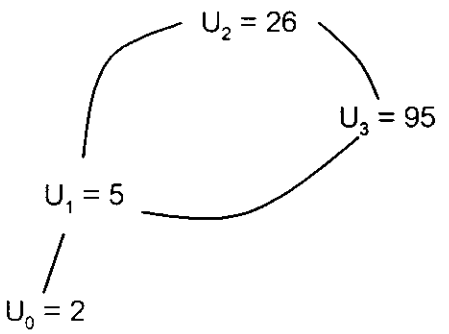
$(u_4 - u_2, 8051) = (7474 - 26, 8051) = (7448, 8051) = 1$

$(u_6 - u_3, 8051) = (871 - 677, 8051) = (194, 8051) = 97$

ดังนั้น 97 เป็นตัวประกอบของ 8051

จากลำดับ $u_0, u_1, u_2, u_3, u_4, u_5, u_6$ หรือ 2, 5, 26, 677, 7474, 2839, 871ถ้าลดขนาดของ u_i ด้วยมอดูโล 97 แล้ว จะได้ลำดับของเลขเป็น 2, 5, 26, 95, 5,

26, 95 และพบว่า $u_4 \equiv u_1 \pmod{97}$ และ $u_5 \equiv u_2 \pmod{97}$ แสดงว่าลำดับที่ได้นี้เป็นลำดับที่มีความยาวคาบเท่ากับ 3 โดยเริ่มที่ u_1 และเมื่อนำตัวเลขในลำดับที่มีการลดขนาดด้วยมอดูโล 97 มาเขียนเป็นแผนภาพจะได้รูปเป็นตัวอักษร ρ ซึ่งเป็นอักษรในภาษากรีก



วิธีการแยกตัวประกอบของจำนวนประกอบด้วยวิธีนี้ J.M. Pollard ได้คิดขึ้นในปี 1975 และเรียกว่าวิธี Pollard - ρ โดยวิธีนี้จะใช้ได้ผลดีเมื่อทราบมาก่อนว่า m เป็นจำนวนประกอบ และตัวประกอบที่ได้จากวิธีนี้อาจไม่เป็นจำนวนเฉพาะ หรือถ้าเป็นจำนวนเฉพาะ ก็อาจจะไม่เป็นจำนวนเฉพาะที่เล็กที่สุดของ m ก็ได้ และบางครั้งเมื่อใช้วิธีนี้โดยการหา $(u_{2s} - u_s, m)$, $s = 1, 2, \ldots$ ไปเรื่อยๆ อาจจะได้ว่า $(u_{2s} - u_s, m) = m$ ก็ได้ ถ้าเป็นเช่นนี้ให้เปลี่ยน u_0 หรือเปลี่ยนฟังก์ชั่น $f(x) = x^2 + c$ โดยเปลี่ยนค่า c แต่ควรหลีกเลี่ยงค่า 0 และ –2

ตัวอย่าง ให้ m =36,287 จงแยกตัวประกอบของ m

เลือก $u_0 = 1$ และให้ $f(x) = x^2 + 1$

ใช้สูตร $u_{i+1} = f(u_i) \pmod{36,287}$ ได้ลำดับ u_i ต่อไปนี้

$u_1 = 2$, $u_2 = 5$, $u_3 = 26$, $u_4 = 677$, $u_5 = 22886$, $u_6 = 2439$, $u_7 = 33941$, $u_8 = 24380$, $u_9 = 3341$, $u_{10} = 22173$, $u_{11} = 25652$, $u_{12} = 26652$, $u_{13} = 29425$, $u_{14} = 22806$,...

หา $(u_{2s} - u_s, 36287)$, $s = 1, 2, 3, \ldots$ ได้

$(u_2 - u_1, 36287) = (3, 36287) = 1$

$(u_4 - u_2, 36287) = (672, 36287) = 1$

$(u_6 - u_3, 36287) = (2413, 36287) = 1$

$(u_8 - u_4, 36287) = (23703, 36287) = 1$

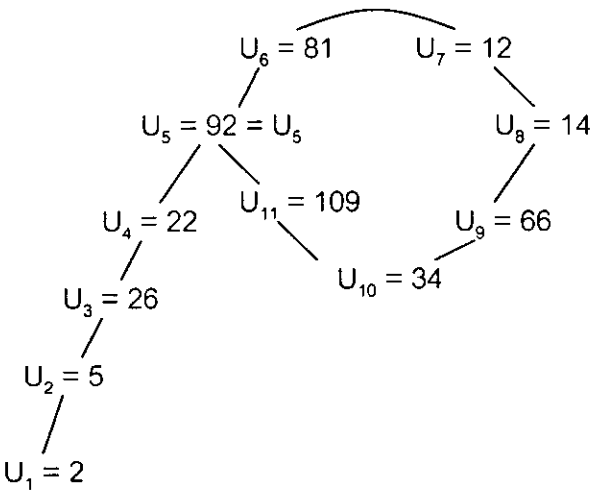
$(u_{10} - u_5, 36287) = (35574, 36287) = 1$

$(u_{12} - u_6, 36287) = (24213, 36287) = 1$

$(u_{14} - u_7, 36287) = (25152, 36287) = 131$

ดังนั้น 131 เป็นตัวประกอบของ 36287 และตัวประกอบที่เหลือคือ 277 นั่นคือ 36287 = 131 . 277

จากลำดับ u_0, u1, u_2, u_3, u_4, u_5, ... , u_{14} ถ้าลดขนาดของ u_i มอดูโล 131 แล้ว จะได้ลำดับของเลขเป็น 2, 5, 26, 22, 92, 81, 12, 14, 66, 34, 109, 92, 81, 12 และพบว่า $u_{12} \equiv u_5 \pmod{131}$ แสดงว่าลำดับที่ได้นี้เป็นลำดับที่มีความยาวคาบเท่ากับ 7 โดยเริ่มที่ u_5 และเมื่อนำตัวเลขในลำดับที่มีการลดขนาดมอดูโล 97 มาเขียนเป็นแผนภาพจะได้รูปเป็นตัวอักษร ρ



2.3.7 สมการไดโอแฟนไทน์เชิงเส้น

สมการไดโอแฟนไทน์เชิงเส้นคือสมการที่มีตัวแปรมากกว่าหรือเท่ากับหนึ่งจำนวนที่มีคำตอบเป็นจำนวนเต็ม สมการไดโอแฟนไทน์แบบเชิงเส้นง่ายที่สุดซึ่งมีตัวแปร 2 ตัว จะอยู่ในรูปแบบ

ax + by = c เมื่อทั้ง a , b และ c เป็นจำนวนเต็ม และทั้ง a และ b เป็นศูนย์พร้อมกันไม่ได้

สมการไดโอแฟนไทน์โดยปกติมักเกิดขึ้นกับปัญหาโจทย์ (Word Problem) ดังเช่นสตรีคนหนึ่งต้องการส่งของทางไปรษณีย์ ปรากฏว่าต้องเสียค่าส่ง 83

เซนต์ แต่แสตมป์ที่มีขายอยู่นั้นมีเพียงชนิด 6 เซนต์และ 15 เซนต์ สตรีผู้นี้ต้องซื้อแสตมป์แต่ละชนิดกี่ดวงจึงพอจะติดบนพัสดุ

สมมุติให้ x แทนจำนวนแสตมป์ดวงละ 6 เซนต์

y แทนจำนวนแสตมป์ดวงละ 15 เซนต์

สมการที่สร้างได้คือ $6x + 15y = 83$ ..... (1)

การหาคำตอบของสมการไดโอแฟนไทน์ $ax + by = c$ อย่างที่กล่าวมาคือการหาจำนวนเต็ม x, y ที่ทำให้สมการเป็นจริง

สมการไดโอแฟนไทน์อาจมีคำตอบได้มากกว่าหรือเท่ากับหนึ่งชุด หรืออาจไม่มีคำตอบเลยก็ได้เช่น $3x + 6y = 18$ มีคำตอบมากกว่าหนึ่งชุด

$2x + 10y = 17$ จะไม่มีคำตอบ

เงื่อนไขที่ทำให้สมการ $ax + by = c$ มีคำตอบหรือไม่มีคำตอบเป็นไปตามทฤษฎีบทต่อไปนี้

ทฤษฎีบท สมการ $ax + by = c$ มีคำตอบก็ต่อเมื่อ d หาร c ลงตัวเมื่อ d คือตัวหารร่วมมากของ a และ b และถ้า x_0 และ y_0 เป็นคำตอบเฉพาะชุดหนึ่งของสมการไดโอแฟนไทน์แล้ว คำตอบทุกชุดของสมการซึ่งเป็นคำตอบที่มีจำนวนนับไม่ถ้วนจะอยู่ในรูป

$x = x_0 + (b/d)\, n$, $y = y_0 - (a/d)\, n$ เมื่อ n เป็นจำนวนเต็ม

ตัวอย่าง จากสมการไดโอแฟนไทน์ $172x + 20y = 1000$

สามารถหาตัวหารร่วมมากระหว่าง 172 และ 20 ได้เท่ากับ 4 และ 4 หาร 1000 ลงตัว ดังนั้นสมการไดโอแฟนไทน์นี้มีคำตอบ

จากการทำขบวนการย้อนกลับจากขั้นตอนวิธีของยูคลิด

$4 = 20 + (-2) \times 8$

$4 = 2 \times 172 + (-17) \times 20$

จะได้คำตอบเฉพาะชุดแรกคือ $x_0 = 2$, $y_0 = -17$

ดังนั้นคำตอบในรูปทั่วไปคือ

$x = 2 + 5k$

$y = -17 - 43k$ เมื่อ k เป็นจำนวนเต็ม

2.3.8 **ระบบคอนกรูเอนซ์** (Congruence)

คอนกรูเอนซ์เป็นเรื่องที่มีเนื้อหาเกี่ยวกับการหารจำนวนเต็มอีกรูปแบบหนึ่ง คอนกรูเอนซ์เป็นรากฐานสำคัญในการศึกษาวิชาทฤษฎีจำนวน สัญลักษณ์เกี่ยวกับคอนกรูเอนซ์ ใช้สะดวก สามารถพิสูจน์ทฤษฎีบทต่างๆ ได้ง่ายขึ้น

ความรู้เกี่ยวกับคอนกรูเอนซ์ปรากฏครั้งแรกในหนังสือ Disquisitions Arithmeticae ของเกาส์ นักคณิตศาสตร์ชาวเยอรมันเมื่อปี ค.ศ. 1801 เป็นผลงานล้ำค่าและเรียบเรียงได้อย่างเหมาะสมในขณะที่เกาส์มีอายุเพียง 24 ปี เกาส์ได้ชื่อว่าเป็นผู้พัฒนาวิชานี้จนเป็นสาขาหนึ่งของคณิตศาสตร์

เกาส์เป็นนักคณิตศาสตร์ที่รอบรู้ในสาขาต่างๆ ของคณิตศาสตร์เกือบทุกแขนง มีผลงานทางคณิตศาสตร์เกือบทุกเรื่อง คำกล่าวที่ท่านแสดงให้เห็นถึงความสำคัญของคณิตศาสตร์คือ " คณิตศาสตร์เป็นราชินีของวิทยาศาสตร์ และทฤษฎีจำนวนเป็นราชินีของคณิตศาสตร์ "

คอนกรูเอนซ์

ให้ m เป็นจำนวนเต็มบวก a , b เป็นจำนวนเต็ม

ถ้า m หาร a - b ลงตัว กล่าวว่า a คอนกรูเอนซ์กับ b มอดูโล m

เขียนแทนด้วย $a \equiv b \pmod{m}$

บทนิยาม ให้ a, b เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก ถ้า $n|(a-b)$ หรือ $kn = a-b$ สำหรับจำนวนเต็ม k บางจำนวน เรากล่าวว่า a คอนกรูเอนซ์กับ b มอดูโล n และเขียนแทนด้วยสัญลักษณ์ $a \equiv b \pmod{n}$ และถ้า $n \nmid (a-b)$ เราจะกล่าวว่า a ไม่คอนกรูเอนซ์กับ b มอดูโล n และเขียนแทนด้วยสัญลักษณ์ $a \not\equiv b \pmod{n}$ และเรียก n ว่ามอดูลัส (modulus)

ตัวอย่าง $3 | (3 - 0)$ ดังนั้น $3 \equiv 0 \pmod{3}$

$3 | (5 - 2)$ ดังนั้น $5 \equiv 2 \pmod{3}$

$3 | (-2 - 1)$ ดังนั้น $-2 \equiv 1 \pmod{3}$

$3 | (-2 - (-5))$ ดังนั้น $-2 \equiv -5 \pmod{3}$

ข้อสังเกต 1. จำนวนเต็มสองจำนวนใดๆ จะคอนกรูเอนซ์มอดูโล 1 เสมอ ดังนั้นจึงไม่มีอะไรน่าสนใจ จึงไม่พิจารณามอดูโล 1 ต่อไปนี้จะกล่าวถึงมอดูโล n ที่มากกว่า 1

2. จำนวนเต็มสองจำนวนใดๆ จะคอนกรูเอนซ์มอดูโล 2 ก็ต่อเมื่อจำนวนทั้งสองนั้นเป็นจำนวนคู่หรือจำนวนทั้งสองเป็นจำนวนคี่

ทฤษฎีบท ให้ n เป็นจำนวนเต็มที่มากกว่า 1 และให้ a, b, c, dเป็นจำนวนเต็ม

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n} \rightarrow a \equiv c \pmod{n}$
4. $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n} \rightarrow a+c \equiv b+d \pmod{n}$
5. $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n} \rightarrow ac \equiv bd \pmod{n}$
6. $a \equiv b \pmod{n} \rightarrow a+c \equiv b+c \pmod{n}$
7. $a \equiv b \pmod{n} \rightarrow ac \equiv bc \pmod{n}$
8. $a \equiv b \pmod{n} \rightarrow a^k \equiv b^k \pmod{n}$ เมื่อ k เป็นจำนวนเต็มบวก
9. $ac \equiv bc \pmod{n}$ และ $(c, n) = d \rightarrow a \equiv b \pmod{\frac{n}{d}}$
10. $ac \equiv bc \pmod{p}$ และ p เป็นจำนวนเฉพาะ และ $p \nmid c \rightarrow a \equiv b \pmod{p}$
11. $ac \equiv bc \pmod{n}$ และ $(c, n) = 1 \rightarrow a \equiv b \pmod{n}$

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

$2^5 \equiv -9 \pmod{41}$

$(2^5)^4 \equiv (-9)^4 \pmod{41}$

$2^{20} \equiv (81)(81) \pmod{41}$ แต่ $81 \equiv -1 \pmod{41}$

ดังนั้น $(81)(81) \equiv (-1)(-1) \pmod{41} \equiv 1 \pmod{41}$

เพราะฉะนั้น $2^{20} \equiv 1 \pmod{41}$

เพราะฉะนั้น $41 \mid 2^{20} - 1$

คอนกรูเอนซ์เชิงเส้น

ถ้า a, b เป็นจำนวนเต็ม สมการ ax = b มีรากเป็นจำนวนเต็มก็ต่อเมื่อ a|b จำนวนเต็ม x_0 ใดๆ ที่สอดคล้องกับคอนกรูเอนซ์เชิงเส้น $ax \equiv b \pmod{n}$ เราเรียกว่า **ราก หรือคำตอบ หรือผลเฉลยของคอนกรูเอนซ์**

ตัวอย่าง จากคอนกรูเอนซ์ $3x \equiv 1 \pmod{4}$ จะพบว่า 3 และ 7 เป็นคำตอบหรือรากของคอนกรูเอนซ์

ทฤษฎีบท ให้ (a, n) = d คอนกรูเอนซ์เชิงเส้น $ax \equiv b \pmod{n}$ มีรากก็ต่อเมื่อ d | b และถ้า d | b แล้วคอนกรูเอนซ์เชิงเส้นนี้มีรากอยู่ d รากที่ไม่คอนกรูเอนซ์กันหรือแตกต่างกันภายใต้มอดูโล n โดยที่ถ้า x_0 เป็นรากหนึ่งที่เรียกว่ารากเฉพาะ แล้วรากทั่วไปของคอนกรูเอนซ์เชิงเส้น จะอยู่ในรูป

$$x = x_0 + \frac{n}{d}k \pmod{n}, \text{ เมื่อ } k \text{ เป็นจำนวนเต็ม}$$

ตัวอย่าง จากคอนกรูเอนซ์เชิงเส้น $14x \equiv 13 \pmod{21}$ จะไม่มีรากหรือผลเฉลย เพราะว่า (14, 21) = 7 แต่ $7 \nmid 13$

ตัวอย่าง จากคอนกรูเอนซ์เชิงเส้น $9x \equiv 15 \pmod{21}$ มีรากเพราะว่า (9, 21) = 3 และ 3 | 15 และคอนกรูเอนซ์นี้จะมีราก 3รากที่ไม่คอนกรูเอนซ์กัน ซึ่งหาได้จาก

$9x \equiv 15 \pmod{21}$ เมื่อหารตลอดด้วย 3

จะได้เป็น $3x \equiv 5 \pmod{7}$

เลือกจำนวนเต็มที่น้อยกว่าหรือเท่ากับ 7 แทนในคอนกรูเอนซ์ข้างต้น ถ้าจำนวนเต็มใดทำให้คอนกรูเอนซ์เป็นจริงแสดงว่าค่านั้นเป็น x_0 ซึ่งจะมีเพียงคำตอบเดียว ในที่นี้คือ 4 ดังนั้น $x_0 = 4$ ซึ่งเป็นรากเฉพาะ และรากทั้งสามที่ต่างกันของคอนกรูเอนซ์นี้คือ $x \equiv 4, 4 + \frac{21}{3}, 4 + 2(\frac{21}{3}) \pmod{21}$

หรือเขียนรากในรูปทั่วไปคือ

$x \equiv 4 + \frac{21}{3}k \pmod{21}$ เมื่อ k เป็นจำนวนเต็ม

หรือ $x \equiv 4 + 7k \pmod{21}$ เมื่อ k เป็นจำนวนเต็ม

Round – Robin Tournament

Round – Robin Tournament เป็นการประยุกต์ใช้ระบบคอนกรูเอนซ์มาช่วยในการจัดตารางการแข่งขันของผู้เข้าแข่งขันที่มีจำนวนทีม n ทีม โดยมีเงื่อนไขว่าแต่ละทีมจะพบกันหนึ่งครั้งตลอดการแข่งขัน ผู้คิดค้นคือ Freund โดยการใช้ระบบคอนกรูเอนซ์ช่วยจัดเป็นตารางและทุกทีมต้องพบกันหมด โดยรูปแบบของตารางเป็นรอบๆ โดยแต่ละรอบจะแสดงรายละเอียดว่าทีมใดพบทีมใดบ้าง การจัดตารางนี้จะไม่มีปัญหาหากจำนวนทีม n เป็นจำนวนคู่ แต่หากจำนวนทีม n เป็นจำนวนคี่แล้ว ในแต่ละรอบจะมีทีมหนึ่งที่ไม่มีคู่แข่งขัน ซึ่งการแก้ปัญหาจุดนี้จะมีการเพิ่มชื่อทีมที่ไม่มีตัวตนเข้าไปอีกหนึ่งทีม ซึ่งจะทำให้จำนวนทีมเป็นจำนวนคู่

การจัดจะเริ่มด้วยการให้หมายเลขทีมต่างๆ เป็น 1, 2, 3, ... n-1, n สร้างตารางโดยรอบที่ k จะจัดทีม I พบกับทีม j ,$I \neq j$ และ $I, j \neq n$ เมื่อ $I + j \equiv k(\text{mod } n-1)$ และถ้า $I + j \equiv 2I \equiv k(\text{mod } n-1)$, $(I \neq j)$ แล้วให้ I พบกับทีม n ในรอบที่ k และหาก n เป็นทีมที่ไม่มีตัวตน ให้เขียน Bye ลงในตาราง ซึ่งกรณี $I + j \equiv 2I \equiv k \ (\text{mod } n-1)$ นี้เกิดขึ้นแน่นอนในแต่ละรอบทั้งนี้เนื่องจากคอนกรูเอนซ์

$2x \equiv k \ (\text{mod } n-1)$

ซึ่งเมื่อ $(2, n-1) = 1$ จะมีคำตอบ x เพียงหนึ่งคำตอบเมื่อ $1 \leq x \leq n-1$ และแต่ละทีมจะพบกันเพียงครั้งเดียวตลอดการแข่งขันเท่านั้น

ตัวอย่าง การสร้างตาราง Round-Robin Tournament สำหรับการแข่งขันครั้งหนึ่ง ซึ่งมีจำนวนทีม 5 ทีม

ให้หมายเลขทีมกับทีมทั้งห้า เป็น 1, 2, 3, 4, 5 และเนื่องจากจำนวนทีมเป็นจำนวนคี่ ดังนั้นเพิ่มทีมสมมุติขึ้นมาอีกหนึ่งทีมเป็นทีมที่ 6

จากคอนกรูเอนซ์ $I + j \equiv k \ (\text{mod } 5)$ ถ้า $k = 1$ ในรอบที่หนึ่ง จะได้

$1 + j \equiv 1 \ (\text{mod } 5)$ ได้ $j = 5$ นั่นคือ ทีมที่ 1 พบกับทีมที่ 5 ในรอบที่หนึ่ง

$2 + j \equiv 1 \ (\text{mod } 5)$ ได้ $j = 4$ นั่นคือ ทีมที่ 2 พบกับทีมที่ 4 ในรอบที่หนึ่ง

$3 + j \equiv 1 \ (\text{mod } 5)$ ได้ $j = 3$ ทำให้ $2j \equiv 1 \ (\text{mod } 5)$ ดังนั้นให้ทีมที่ 3 พบกับทีมที่ 6 แต่เนื่องจากทีมที่ 6 เป็นทีมสมมุติ ไม่มีตัวตน จึงเขียน Bye ลงในตาราง จากที่ทราบว่าทีมที่ 1 พบทีมที่ 5 ดังในในตารางช่องของทีมที่ 5 จึงพบกับทีมที่ 1

และเมื่อ k = 2, 3, 4, 5 จะสามารถทำได้ทำนองเดียวกันกับข้างต้น และได้ตารางดังต่อไปนี้

Team / *Round*	1	2	3	4	5
1	5	4	Bye	2	1
2	Bye	5	4	3	2
3	2	1	5	Bye	3
4	3	Bye	1	5	4
5	4	3	2	1	Bye

ตาราง 2.2 Round – Robin Tournament จำนวน 5 ทีม

2.3.9 เศษส่วนต่อเนื่อง

เศษส่วนต่อเนื่องจำกัดอย่างง่าย (Simple Finite Continued Fraction) คือเศษส่วนที่เขียนอยู่ในรูปต่อไปนี้

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\mathrm{O} \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

โดยที่ a_0 เป็นจำนวนจริง และ $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนจริงบวก มีชื่อเรียกว่าตัวส่วนย่อย (Partial denominators) ซึ่งนิยมเขียนเศษส่วนต่อเนื่องในรูปแบบดังกล่าวด้วย $[a_0; a_1, a_2, a_3, \ldots, a_n]$ หรือ $<a_0; a_1, a_2, a_3, \ldots, a_n>$ ถ้า $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเต็มบวกจะเรียก $[a_0; a_1, a_2, a_3, \ldots, a_n]$ ว่าเศษส่วนต่อเนื่องจำกัดอย่างง่าย (Finite simple continued fraction)

เศษส่วนต่อเนื่องจำกัดอย่างง่ายทุกจำนวนสามารถแปลงให้เป็นจำนวนตรรกยะได้ ในทางกลับกัน จำนวนตรรกยะก็สามารถแปลงให้เป็นเศษส่วนต่อเนื่องจำกัดอย่างง่ายได้เช่นกัน

ตัวอย่าง การเขียนเศษส่วนต่อเนื่อง [2; 3, 5] ให้อยู่ในรูป $\frac{a}{b}$

$$[2; 3, 5] = 2 + \frac{1}{3+\frac{1}{5}} = 2 + \frac{1}{\frac{16}{5}} = 2 + \frac{5}{16} = \frac{37}{16}$$

ตัวอย่าง การเขียน $\frac{5}{13}$ ในรูปเศษส่วนต่อเนื่องจำกัดอย่างง่าย

$$\frac{5}{13} = 0 + \frac{1}{\frac{13}{5}} = 0 + \frac{1}{2+\frac{3}{5}} = 0 + \frac{1}{2+\frac{1}{\frac{5}{3}}}$$

$$= 0 + \frac{1}{2+\frac{1}{1+\frac{2}{3}}} = 0 + \frac{1}{2+\frac{1}{1+\frac{1}{\frac{3}{2}}}}$$

$$= 0 + \frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}}$$

$$= [0; 2, 1, 1, 2]$$

การแปลงจำนวนตรรกยะเป็นเศษส่วนต่อเนื่องจำกัดอย่างง่ายนั้น ต้องอาศัยขั้นตอนวิธีของยูคลิดดังต่อไปนี้

ให้ $\frac{a}{b}$ เมื่อ a, b เป็นจำนวนเต็ม และ b > 0 จากขั้นตอนวิธีการหาร (Division Algorithm) จะได้สมการ

$a = ba_0 + r_1 \qquad 0 < r_1 < b$

$b = r_1a_1 + r_2 \qquad 0 < r_2 < r_1$

$r_1 = r_2a_2 + r_3 \qquad 0 < r_3 < r_2$

$\vdots$

$r_{n-2} = r_{n-1}a_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$

$r_{n-1} = r_na_n$

จะเห็นว่า $r_1, r_2, r_3, \dots, r_n$ และ $a_1, a_2, a_3, \dots, a_n$ เป็นจำนวนเต็มบวก จากสมการข้างต้น จะได้

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}}$$

$$\frac{b}{r_1} = a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}}$$

$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2} = a_2 + \frac{1}{\frac{r_2}{r_3}}$$

$$\vdots$$

$$\frac{r_{n-2}}{r_{n-1}} = a_{n-1} + \frac{r_n}{r_{n-1}} = a_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}}$$

$$\frac{r_{n-1}}{r_n} = a_n$$

จะได้

$$\frac{a}{b} = a_0 + \frac{1}{\frac{b}{r_1}}$$

$$= a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}}$$

$$= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\frac{r_2}{r_3}}}}$$

$$\vdots$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

และเขียนในรูปสัญลักษณ์ได้เป็น $[a_0; a_1, a_2, a_3, \ldots, a_n]$

ตัวอย่าง การเขียน $\frac{19}{51}$ ในรูปเศษส่วนต่อเนื่องจำกัดอย่างง่าย

ในขั้นต้นหากใช้ขั้นตอนวิธีของยูคลิด

$51 = 2 \cdot 19 + 13$ **หรือ** $\frac{51}{19} = 2 + \frac{13}{19}$

$19 = 1 \cdot 13 + 6$ **หรือ** $\frac{19}{13} = 1 + \frac{6}{13}$

$13 = 2 \cdot 6 + 1$ **หรือ** $\frac{13}{6} = 2 + \frac{1}{6}$

$6 = 6 \cdot 1 + 0$ **หรือ** $\frac{6}{6} = 1$

ซึ่งเมื่อแปลงเป็นเศษส่วนต่อเนื่อง จะได้

$$\frac{19}{51} = \frac{1}{51/19} = \frac{1}{2+\frac{13}{19}}$$

$$= \frac{1}{2+\frac{1}{\frac{19}{13}}}$$

$$= \frac{1}{2+\frac{1}{1+\frac{6}{13}}}$$

$$= \frac{1}{2+\frac{1}{1+\frac{1}{\frac{13}{6}}}}$$

$$= \frac{1}{2+\frac{1}{1+\frac{1}{2+\frac{1}{6}}}}$$

เขียนในรูปอย่างง่ายได้เป็น $[0; 2, 1, 2, 6]$

ข้อสังเกต a_0 จะเป็นศูนย์เมื่อเศษส่วนต่อเนื่องนั้นมีค่าเป็นบวกที่น้อยกว่า 1

จากเศษส่วนต่อเนื่องจำกัดอย่างง่ายที่มีขนาดใหญ่ ถ้าต้องการแปลงเป็นจำนวนตรรกยะ โดยใช้การคำนวณแบบเศษส่วนซ้อนดังตัวอย่างจะใช้เวลามากในการคำนวณ และยุ่งยาก จึงมีวิธีอีกวิธีหนึ่งที่อาศัยคอนเวอร์เจนต์ที่ k ซึ่งนิยามดังนี้

บทนิยาม1 ให้ $[a_0; a_1, a_2, a_3, \dots, a_n]$ เป็นเศษส่วนต่อเนื่องจำกัดอย่างง่าย กำหนด $c_0 = [a_0]$ และ $c_k = [a_0; a_1, a_2, a_3, \dots, a_k]$ ซึ่ง $0 \leq k \leq n$ เรียก c_k ว่าคอนเวอร์เจนต์ที่ k (k^{th} convergent)

ตัวอย่าง จงหา c_0, c_1, c_2, c_3, c_4 ของเศษส่วนต่อเนื่อง [0; 3, 2, 1, 5]

$c_0 = [0]$

$c_1 = [0; 3] = 0 + \frac{1}{3} = \frac{1}{3}$

$c_2 = [0; 3, 2] = 0 + \cfrac{1}{3+\frac{1}{2}} = \frac{2}{7}$

$c_3 = [0; 3, 2, 1] = 0 + \cfrac{1}{3+\cfrac{1}{2+\frac{1}{1}}} = \frac{3}{10}$

$c_4 = [0; 3, 2, 1, 5] = 0 + \cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{1+\frac{1}{5}}}} = \frac{17}{57}$

ทฤษฎีบท1 จากเศษส่วนต่อเนื่องจำกัดอย่างง่าย $[a_0; a_1, a_2, a_3, \dots, a_n]$ จะได้ว่า

$c_k = \frac{p_k}{q_k}$, $0 \leq k \leq n$

เมื่อ $p_0 = a_0$, $q_0 = 1$

$p_1 = q_1 p_0 + q_0$, $q_1 = a_1$

และ $p_k = a_k p_{k-1} + a_{k-2}$, $q_k = a_k q_{k-1} + q_{k-2}$ เมื่อ $k = 2, 3, \dots, n$

ตัวอย่าง จงหา c_k เมื่อ $k = 0, 1, 2, 3$ สำหรับเศษส่วนต่อเนื่อง [3; 1, 2, 3]

$p_0 = a_0 = 3$

$p_1 = a_1 p_0 + 1 \qquad = 1 \times 3 + 1 \qquad = 4$

$p_2 = a_2p_1 + p_0 \quad = 2 \times 4 + 3 \quad = 11$

$p_3 = a_3p_2 + p_1 \quad = 3 \times 11 + 4 \quad = 37$

$q_0 = 1$

$q_1 = a_1 \quad = 1$

$q_2 = a_2q_1 + q_0 \quad = 2 \times 1 + 1 \quad = 3$

$q_3 = a_3q_2 + q_1 \quad = 3 \times 3 + 1 \quad = 10$

$$c_0 = \frac{p_0}{q_0} \quad = 3$$

$$c_1 = \frac{p_1}{q_1} \quad = 4$$

$$c_2 = \frac{p_2}{q_2} \quad = \frac{11}{3}$$

$$c_3 = \frac{p_3}{q_3} \quad = \frac{37}{10}$$

เพื่อให้เกิดความสะดวกในการคำนวณหาจำนวนตรรกยะจาก c_k โดยใช้สูตรจากทฤษฎีบทดังกล่าวข้างต้น เราอาจจะสร้างตารางช่วยในการหา p_k, q_k ดังตัวอย่างต่อไปนี้

ตัวอย่าง จากเศษส่วนต่อเนื่องในตัวอย่างข้างต้น สามารถสร้างตารางได้ดังนี้

n	0	1	2	3
a_n	3	1	2	3
p_n	3	4	11	37
q_n	1	1	3	10

ตัวอย่าง จากเศษส่วนต่อเนื่องจำกัดอย่างง่าย [3; 1, 1, 2, 5, 4, 8] สามารถสร้างตารางได้ดังนี้

n	0	1	2	3	4	5	6
A_n	3	1	1	2	5	4	8
p_n	3	4	7	18	97	406	3345
q_n	1	1	2	5	27	113	931

$$c_0 = \frac{p_0}{q_0} \qquad = 3$$

$$c_1 = \frac{p_1}{q_1} \qquad = 4$$

$$c_2 = \frac{p_2}{q_2} \qquad = \frac{7}{2}$$

$$c_3 = \frac{p_3}{q_3} \qquad = \frac{18}{5}$$

$$c_4 = \frac{p_4}{q_4} \qquad = \frac{97}{27}$$

$$c_5 = \frac{p_5}{q_5} \qquad = \frac{406}{113}$$

$$c_6 = \frac{p_6}{q_6} \qquad = \frac{3345}{931}$$

เศษส่วนต่อเนื่องอนันต์ คือ ลิมิตของเศษส่วนต่อเนื่องจำกัด ดังบทนิยามต่อไปนี้

บทนิยาม 2 ถ้า a_0 เป็นจำนวนจริง $a_1, a_2, \ldots$ เป็นจำนวนจริงบวก แล้วเศษส่วน

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \mathrm{O} + \cfrac{1}{a_{n-1} + \mathrm{O}}}}$$

เราเรียกว่า เศษส่วนต่อเนื่องอนันต์ แทนด้วย $[a_0; a_1, a_2, \ldots]$ และถ้า a_0 เป็นจำนวนเต็ม $a_1, a_2, a_3, \ldots$ เป็นจำนวนเต็มบวก แล้ว $[a_0; a_1, a_2, \ldots]$ เป็นเศษส่วนต่อเนื่องอนันต์อย่างง่าย

ทฤษฎีบท 2 $[a_0; a_1, a_2, \ldots]$ เป็นจำนวนอตรรกยะ

ตัวอย่าง จงหาค่าของเศษส่วนต่อเนื่องอนันต์ [3; 6 , 1 , 4 , 1 , 4 , ...]

วิธีทำ ให้ x = [3; 6 , 1 , 4 , 1 , 4 , ...]

และ y = [1; 4 , 1 , 4 , 1 , 4 , ...]

$$y = 1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{4 + _{O}}}} \quad = \quad 1 + \cfrac{1}{4 + \cfrac{1}{y}}$$

$$y = 1 + \cfrac{1}{\cfrac{4y+1}{y}} \qquad = 1 + \frac{y}{4y+1} \qquad = \frac{5y+1}{4y+1}$$

$$4y^2 + y = 5y + 1$$

$$4y^2 - 4y - 1 = 0$$

$$y = \frac{1+\sqrt{2}}{2} \qquad , y > 0$$

$$x = 3 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{4 + _{O}}}} \qquad = 3 + \cfrac{1}{6 + \cfrac{1}{y}} \qquad = 3 + \cfrac{1}{6 + \cfrac{1}{\cfrac{1+\sqrt{2}}{2}}}$$

$$= 3 + \cfrac{1}{6 + \cfrac{2}{1+\sqrt{2}}}$$

$$= 3 + \cfrac{1}{\cfrac{6+6\sqrt{2}+2}{1+\sqrt{2}}} \qquad = 3 + \frac{1+\sqrt{2}}{8+6\sqrt{2}} \quad = \frac{24+18\sqrt{2}+1+\sqrt{2}}{8+6\sqrt{2}}$$

$$= \frac{25+19\sqrt{2}}{8+6\sqrt{2}} \cdot \frac{8-6\sqrt{2}}{8-6\sqrt{2}}$$

$$= \frac{14-\sqrt{2}}{4}$$ เป็นจำนวนอตรรกยะ

ทฤษฎีบท 3 ให้ $\alpha = \alpha_0$ เป็นจำนวนอตรรกยะ และถ้านิยามลำดับ $a_0, a_1, a_2, \ldots$ ด้วยสูตร

$$a_k = [\alpha_k] \quad \text{และ} \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \text{ สำหรับ k = 0, 1, 2, 3, ...}$$

แล้ว $\alpha = [a_0; a_1, a_2, \ldots]$

ตัวอย่าง ให้ $\alpha = \sqrt{6}$ จงแปลง α เป็นเศษส่วนต่อเนื่องอนันต์แบบง่าย

จาก $a_k = [\alpha_k]$, $\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$, $k = 0,1,2,\ldots..$

ให้ $\alpha_0 = \alpha = \sqrt{6}$ ได้

$$a_0 = [\alpha_0] = [\sqrt{6}] = 2 \qquad \alpha_1 = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2}$$

$$a_1 = [\alpha_1] = [\frac{\sqrt{6}+2}{2}] = 2 \qquad \alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\frac{\sqrt{6}+2}{2}-2} = \sqrt{6}+2$$

$$a_2 = [\sqrt{6}+2] = 4 \qquad \alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{(\sqrt{6}+2)-4} = \frac{\sqrt{6}+2}{2} = \alpha_1$$

$$\therefore \alpha_3 = \alpha_1, a_3 = a_1$$

$$\alpha_4 = \alpha_2, a_4 = a_2$$

M

$$\therefore \sqrt{6} = [2;2,4,2,4,....]$$

บทนิยาม 3 เรากล่าวว่า $[a_0;a_1,a_2,...]$ เป็นเศษส่วนต่อเนื่องอนันต์ที่มี คาบ (periodic continued fraction) ถ้ามีจำนวนเต็ม N,k ที่ $a_n = a_{n+k}$ ทุกจำนวนเต็มบวก n ที่ $n \geq N$ นั่นคือ

$$[a_0;a_1,a_2,...] = [a_0;a_1,a_2,...,a_{N-1},a_N,a_{N+1},...,a_{N+k-1},a_N,a_{N+1},...]$$

ซึ่งจะแทนสัญลักษณ์ $[a_0;a_1,a_2,...,a_{N-1},\overline{a_N,...,a_{N+k-1}}]$

เช่น $[1;2,4,2,4,2;4,...] = [1;\overline{2,4}]$ เป็นเศษส่วนต่อเนื่องอนันต์ที่มีคาบ

บทนิยาม 4 เราจะกล่าวว่า จำนวนจริง α เป็น quadratic irrational ถ้า

1. α เป็นจำนวนอตรรกยะ และ
2. α เป็นรากของสมการ $Ax^2 + Bx + C = 0$ $\quad A,B,C \in I$ และ $A \neq 0$

ตัวอย่าง $\alpha = 2+\sqrt{3}$ เป็น Quadratic irrational เพราะว่า α เป็นจำนวนอตรรกยะ และ α เป็นรากของสมการกำลังสอง

$$x^2 - 4x + 1 = 0$$

ทฤษฎีบท 4 เศษส่วนต่อเนื่องอนันต์ของจำนวนอตรรกยะเป็นเศษส่วนต่อเนื่องอนันต์ที่มีคาบก็ต่อเมื่อจำนวนอตรรกยะนั้นเป็นจำนวน Quadratic irrational

ทฤษฎีบท 5 ถ้า α เป็น Quadratic irrational แล้วเราสามารถเขียน α ในรูป $\alpha = \frac{P+\sqrt{d}}{Q}$ โดยที่ P,Q,d เป็นจำนวนเต็มที่ $Q \neq 0, d > 0$ และ d ไม่เป็นจำนวนกำลังสองสมบูรณ์ และ $Q \mid d - P^2$

ตัวอย่าง ให้ $\alpha = \frac{5+\sqrt{3}}{3}$

ถ้าคูณ α ด้วย $\frac{3}{3}$ ได้

$\alpha = \frac{15+\sqrt{27}}{9}$

ถ้าให้ P = 15, d = 27และ Q = 9

แล้วจะได้ว่า $Q \mid d - P^2$

ทฤษฎีบท 6 ให้ α เป็น Quadratic irrational ที่มี P_0, Q_0, d เป็นจำนวนเต็มที่ $Q_0 \neq 0, d > 0$ และ d ไม่เป็นจำนวนกำลังสองสมบูรณ์ และ $Q_0 \mid (d - P_0^2)$ และนิยาม α_k , P_{k+1} ดังนี้

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k} \qquad , a_k = [\alpha_k]$$

$$P_{k+1} = a_k Q_k - P_k \qquad , Q_{k+1} = \frac{d - P^2{}_{k+1}}{Q_k}, k = 0,1,2,.....$$

แล้วจะได้ว่า $\alpha = [a_0; a_1, a_2, ...]$

ตัวอย่าง ให้ $\alpha = \frac{3+\sqrt{7}}{2}$ จงแปลง α เป็นเศษส่วนต่อเนื่องอนันต์แบบง่าย

จากทฤษฎีบทที่ 5 จะได้ว่า α เป็น Quadratic irrational ดังนั้นเราสามารถแปลง α เป็นเศษส่วนต่อเนื่องอนันต์ โดยใช้ทฤษฎีบทที่ 6 ดังนี้

$$\alpha = \frac{3+\sqrt{7}}{2} = \frac{6+\sqrt{28}}{4}$$

$P_0 = 6, Q_0 = 4$ และ $d = 28$, $\alpha_0 = \frac{6+\sqrt{28}}{4}$ และ $a_0 = [\alpha_0] = 2$

จากนั้นใช้สูตรจากบทนิยามในทฤษฎีบท 6

$$P_{k+1} = a_k Q_k - P_k \qquad \alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$$

$$Q_{k+1}=\frac{d-P^2_{k+1}}{Q_k} \qquad a_k=[\alpha_k] \qquad ,k= 0,1,2,.....$$

ซึ่งได้ดังนี้

$$P_1=2\cdot 4-6=2 \qquad \alpha_1=\frac{2+\sqrt{28}}{6}$$

$$Q_1=\frac{28-2^2}{4}=6 \qquad a_1=\left[\frac{2+\sqrt{28}}{6}\right]=1$$

$$P_2=1\cdot 6-2=4 \qquad \alpha_2=\frac{4+\sqrt{28}}{2}$$

$$Q_2=\frac{28-4^2}{6}=2 \qquad a_2=\left[\frac{4+\sqrt{28}}{2}\right]=4$$

$$P_3=4\cdot 2-4=4 \qquad \alpha_3=\frac{4+\sqrt{28}}{6}$$

$$Q_3=\frac{28-4^2}{2}=6 \qquad a_3=\left[\frac{4+\sqrt{28}}{6}\right]=1$$

$$P_4=1\cdot 6-4=2 \qquad \alpha_4=\frac{2+\sqrt{28}}{4}$$

$$Q_4=\frac{28-2^2}{6}=4 \qquad a_4=\left[\frac{2+\sqrt{28}}{4}\right]=1$$

$$P_5=1\cdot 4-2=2 \qquad \alpha_5=\frac{2+\sqrt{28}}{6}$$

$$Q_5=\frac{28-2^2}{4}=6 \qquad a_5=\left[\frac{2+\sqrt{28}}{6}\right]=1=a_1$$

เราจะเห็นว่า $P_5=P_1$ และ $Q_5=Q_1$

ดังนั้น $a_5=a_1$, $a_6=a_2$, $a_7=a_3$,.....

$$\therefore \frac{3+\sqrt{7}}{2}=[2;1,4,1,1,1,4,1,1,1,4,1,1,.....]=[2;\overline{1,4,1,1}]$$

2.3.10 การเข้ารหัส

การเข้ารหัสและการถอดรหัสลับมีมาตั้งแต่สมัยจูเลียต ซีซาร์ โดยมีการนำระบบคอนกรูเอนซ์จากทฤษฎีจำนวนมาช่วย ได้มีการพัฒนาและใช้งานเรื่อยๆ มาจนถึงปี 1970 ได้มีการนำคอมพิวเตอร์มาช่วย ทำให้การเข้าและถอดรหัสมีประสิทธิ

ภาพมากขึ้น ทำงานได้เร็วขึ้น สามารถป้องกันการลักลอบถอดรหัสได้ดีขึ้น มีการใช้การเข้าและถอดรหัสเพื่อผลประโยชน์ของกลุ่มคนอย่างแพร่หลาย

หลักการทั่วไปของระบบรหัสลับ

ข้อความลับที่เป็นตัวอักษร ในเบื้องต้นจะถูกเปลี่ยนเป็นข้อความลับที่เป็นตัวเลข ถ้าเป็นอักษรภาษาอังกฤษโดยทั่วไปจะถูกเปลี่ยนตามดังแสดงต่อไปนี้

A = 0	B = 1	C = 2	D = 3	E = 4	F = 5	G = 6
H = 7	I = 8	J = 9	K = 10	L = 11	M = 12	N = 13
O = 14	P = 15	Q = 16	R = 17	S = 18	T = 19	U = 20
V = 21	W = 22	X = 23	Y = 24	Z = 25		

จากนั้นจึงเข้ารหัสกับข้อความลับที่เป็นตัวเลข (P) ด้วยฟังก์ชั่นเข้ารหัสที่เป็นฟังก์ชั่นชนิด 1-1 จากเซต {0,1,2,...,25} ไปทั่วถึงเซต {0,1,2,...,25} และตัวแปรในฟังก์ชั่นเข้ารหัสเรียกว่า "กุญแจเข้ารหัส"

ให้ฟังก์ชั่นเข้ารหัสเป็น Ek และ k เป็นกุญแจเข้ารหัส ข้อความที่ได้จากการเข้ารหัสคือ $Ek(P) \equiv C \pmod{26}$ เราเรียก C ว่ารหัสลับ ขั้นตอนนี้เรียกว่า การเข้ารหัสลับ จากนั้นผู้ส่งจะส่งรหัสลับที่เป็นตัวเลข หรืออาจเปลี่ยนเป็นตัวอักษรโดยใช้ตารางข้างต้นแล้วจึงส่งให้ผู้รับโดยสื่อชนิดใดชนิดหนึ่ง

เมื่อผู้รับได้รับรหัสลับ (C) จะทำการถอดรหัสด้วยฟังก์ชั่นผกผันของ Ek ซึ่งให้ Dk เป็นฟังก์ชั่นผกผันดังกล่าวและ k เป็นกุญแจถอดรหัส และ $Dk(C) \equiv P \pmod{26}$ เรียกว่าการถอดรหัสลับ

ดังแสดงตามแผนภาพ

P ---- Ek ----> C ---- Media ----> C ---- Dk ----> P

ชนิดของระบบรหัสลับ

1. Symmetric Cryptosystem เป็นระบบที่การเข้ารหัสและการถอดรหัสใช้กุญแจตัวเดียวกันในการเข้าและถอดรหัส

2. Asymmetric Cryptosystem เป็นระบบที่การเข้ารหัสและการถอดรหัสใช้กุญแจคนละตัวกัน ดังนั้นเราจึงสามารถประกาศกุญแจการเข้ารหัสให้ทราบโดยทั่วไปได้ จึงเรียกระบบนี้อีกชื่อว่า Public-Key Cryptosystem

ระบบรหัสลับแบบซีซ่าร์หรือระบบรหัสลับแบบเลื่อน(Caesar Encryption)

ระบบรหัสลับแบบซีซ่าร์หรือระบบรหัสลับแบบเลื่อนเป็นระบบรหัสลับแบบ Symmetric มีมาตั้งแต่สมัยจูเลียต ซีซาร์ โดยมีขั้นตอนคือแปลงข้อความที่จะเข้ารหัสเป็นตัวเลขก่อน จากนั้นจึงนำมาเข้ารหัสกับกุญแจ b ดังนี้

$Ek(P) \equiv (P + b) \bmod 26 \equiv C \pmod{26}$

จากนั้นจึงส่ง C ไปให้แก่ผู้รับ

และการถอดรหัสก็สามารถทำโดย

$Dk(C) \equiv (C - b) \bmod 26 \equiv P \pmod{26}$

ตัวอย่าง จงเข้ารหัสลับข้อความ MESSAGE โดยใช้ระบบรหัสลับแบบเลื่อน มีกุญแจในการเข้ารหัสคือ 3

อักษรในข้อความลับเมื่อเปลี่ยนเป็นตัวเลขคือ

P : 12 4 18 18 0 6 4

เมื่อผ่านฟังก์ชั่นเข้ารหัสจะได้รหัสลับคือ

C : 15 7 21 21 3 9 7

และแปลงกลับเป็นตัวอักษรก่อนส่งไปได้เป็น PHVVDJH

ตัวอย่าง จงถอดรหัสข้อความ HMFSNPF โดยใช้ระบบรหัสลับแบบเลื่อน มีกุญแจในการถอดรหัสคือ 5

อักษรในข้อความลับเมื่อเปลี่ยนเป็นตัวเลขคือ

C : 7 12 5 18 13 15 5

เมื่อผ่านฟังก์ชั่นถอดรหัสจะได้ข้อความคือ

P : 2 7 0 13 8 10 0

และแปลงกลับเป็นตัวอักษรก่อนส่งไปได้เป็น CHANIKA

ระบบรหัสลับแบบแอฟไฟน์ (Affine Encryption)

ระบบรหัสลับแบบแอฟไฟน์เป็นระบบรหัสลับแบบ Symmetric โดยมีขั้นตอนคือแปลงข้อความที่จะเข้ารหัสเป็นตัวเลขก่อน จากนั้นจึงนำมาเข้ารหัสกับกุญแจ (a,b) ดังนี้

$$Ek(P) \equiv (aP + b) \bmod 26 \equiv C \pmod{26}$$

จากนั้นจึงส่ง C ไปให้แก่ผู้รับ

และการถอดรหัสก็สามารถทำโดย

$$Dk(C) \equiv @(C - b) \pmod{26} \equiv P \pmod{26}$$ เมื่อ @ เป็นผกผันกับ a (mod 26)

ตัวอย่าง จงเข้ารหัสลับข้อความ MONEY โดยใช้ระบบรหัสลับแบบแอฟไฟน์ มีกุญแจในการเข้ารหัสคือ (7,10)

อักษรในข้อความลับเมื่อเปลี่ยนเป็นตัวเลขคือ

P : 12 14 13 4 24

เมื่อผ่านฟังก์ชั่นเข้ารหัสจะได้รหัสลับคือ

C : 16 4 23 12 22

และแปลงกลับเป็นตัวอักษรก่อนส่งไปได้เป็น QEXMW

การเข้ารหัสลับแบบบล็อค(Block Encryption)

การเข้ารหัสตัวอักษรทีละตัวตามแบบที่กล่าวมาแล้วข้างต้นทั้งสองระบบทำให้สามารถใช้ความถี่ของตัวอักษรที่ใช้ในแต่ละภาษานั้นนำไปหากุญแจในการถอดรหัสได้ และทำให้รหัสลับที่ได้นั้นไม่ยาก ดังนั้นเพื่อป้องกันการแกะรหัสหรือทำให้การแกะรหัสนั้นมีความยุ่งยากมากยิ่งขึ้น จะเข้ารหัสอีกแบบเรียกว่า ระบบการเข้ารหัสแบบบล็อค ด้วยการแบ่งข้อความที่จะเข้ารหัสนั้นเป็นบล็อคๆ แต่ละบล็อคมีจำนวนตัวอักษรเท่ากัน แล้วเข้ารหัสกับบล็อคแต่ละบล็อค โดยใช้เมตริกซ์จัตุรัสที่มีสมาชิกเป็นจำนวนเต็มมอดูโล 26

ถ้าแต่ละบล็อคมีตัวอักษร 2 ตัวก็ใช้เมตริกซ์ 2x2 แต่หากแต่ละบล็อคมีตัวอักษร n ตัวก็ใช้เมตริกซ์ nxn ($n \geq 2$) และเมตริกซ์นั้นต้องมีอินเวอร์สการคูณมอดูโล 26 คือ (det A, 26) = 1

ขั้นตอนการเข้ารหัสแบบบล็อค

1. จัดตัวอักษรแต่ละข้อความเป็นบล็อคๆ ถ้าจำนวนตัวอักษรในบล็อคสุดท้ายไม่เต็มบล็อคให้เติมอักษรที่ได้ตกลงกันไว้ เช่น X ลงไปให้จนจำนวนตัวอักษรเต็มบล็อค
2. เปลี่ยนตัวอักษรแต่ละตัวในบล็อคเป็นตัวเลขโดยใช้ตารางที่กล่าวมาข้างต้น
3. สมมุติในกรณีนี้ใช้บล็อคละสองตัวอักษร แต่ละคู่ของตัวอักษรสมมุติเป็น p_1p_2 นำมาเขียนเป็น column vector

$$p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

4. เลือกเมตริกซ์ A_{2x2} ที่มีสมาชิกเป็นจำนวนเต็มมอดูโล 26 และเป็นเมตริกซ์ที่มีอินเวอร์สการคูณมอดูโล 26 คือ (det A, 26) = 1
5. เข้ารหัส P ด้วยฟังก์ชั่นเข้ารหัส E_k ที่มีกุญแจเข้ารหัส A

$C \equiv E_k(P) \equiv AP \pmod{26}$

จากนั้นอาจเปลี่ยนรหัสลับ C ซึ่งเป็น column vector $\begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$ เป็นรหัสลับ

การถอดรหัสลับแบบบล็อค

ทฤษฎีบท ถ้าฟังก์ชั่นการเข้ารหัส E_k มีสูตรเป็น

$C \equiv E_k(P) \equiv AP \pmod{26}$

เมื่อ A เป็นเมตริกซ์ nxn ที่ (det A, 26) = 1 และ P เป็นเมตริกซ์ nx1แล้ว ฟังก์ชั่นถอดรหัส D_k มีสูตรดังนี้

$P \equiv D_k(C) \equiv \overline{A}C \pmod{26}$

เมื่อ $\overline{A}$ เป็นเมตริกซ์อินเวอร์สของ A มอดูโล 26

ตัวอย่าง จงเข้ารหัสข้อความ THE GOLD โดยใช้ระบบรหัสลับแบบบล็อค โดยใช้เมตริกซ์ $\begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix}$ เป็นกุญแจเข้ารหัส

จาก THE GOLD แยกเป็นบล็อค TH EG OL DX

เปลี่ยนเป็นตัวเลขได้ 19 7 4 6 14 11 3 23

เข้ารหัสด้วยฟังก์ชั่น P : $\begin{bmatrix}19\\7\end{bmatrix}\begin{bmatrix}4\\6\end{bmatrix}\begin{bmatrix}14\\11\end{bmatrix}\begin{bmatrix}3\\23\end{bmatrix}$

C $\equiv$ AP (mod 26) ดังนี้

$$C:\begin{bmatrix}c_1 & c_3 & c_5 & c_7\\ c_2 & c_4 & c_6 & c_8\end{bmatrix}\equiv\begin{bmatrix}5 & 17\\ 4 & 15\end{bmatrix}\begin{bmatrix}19 & 4 & 14 & 3\\ 7 & 6 & 11 & 23\end{bmatrix}(\mathrm{mod}\,26)$$

$$\equiv\begin{bmatrix}6 & 18 & 23 & 16\\ 25 & 2 & 13 & 19\end{bmatrix}(\mathrm{mod}\ 26)$$

C : 6 25 18 2 23 13 16 19

ซึ่งสามารถเปลี่ยนเป็นตัวอักษรได้เป็น GZSCXNQT

ตัวอย่าง จงถอดรหัสข้อความ BPQFJNBW โดยใช้ระบบรหัสลับแบบบล็อค โดยมีเมตริกซ์ $\begin{bmatrix}3 & 10\\ 9 & 7\end{bmatrix}$ เป็นกุญแจรหัส

เริ่มต้นด้วยการหา $\overline{A}$ จาก det A = 21 – 90 = -69 $\equiv$ 9 (mod 26)

ถ้าให้ det A = ∇ = 9 เราหา $\overline{\nabla}$ ที่ $\nabla\overline{\nabla}\equiv\overline{\nabla}\nabla\equiv 1$ (mod 26)

จาก $9\overline{\nabla}\equiv 1$ (mod 26) จะได้ $\overline{\nabla}$ = 3

ดังนั้น $\overline{A}\equiv\overline{\nabla}\begin{bmatrix}7 & -10\\ -9 & 3\end{bmatrix}\equiv 3\begin{bmatrix}7 & -10\\ -9 & 3\end{bmatrix}\equiv\begin{bmatrix}21 & -4\\ -1 & 9\end{bmatrix}(\mathrm{mod}\ 26)$

แบ่งรหัสที่ได้มาเป็นคู่ๆ ได้เป็น BP QF JN BW และเปลี่ยนรหัสแต่ละคู่เป็นตัวเลขและเขียนเป็นเวกเตอร์หลัก

$$C:\begin{bmatrix}1\\15\end{bmatrix}\begin{bmatrix}16\\5\end{bmatrix}\begin{bmatrix}9\\13\end{bmatrix}\begin{bmatrix}1\\12\end{bmatrix}$$

$$P:\begin{bmatrix}p_1 & p_3 & p_5 & p_7\\ p_2 & p_4 & p_6 & p_8\end{bmatrix}\equiv\begin{bmatrix}21 & -4\\ -1 & 9\end{bmatrix}\begin{bmatrix}1 & 16 & 9 & 3\\ 15 & 5 & 13 & 12\end{bmatrix}(\mathrm{mod}\,26)$$

$$\equiv\begin{bmatrix}13 & 4 & 7 & 25\\ 4 & 3 & 4 & 3\end{bmatrix}(\mathrm{mod}\,26)$$

ดังนั้นจะได้ข้อความคือ NEEDHEZD

การเข้ารหัสแบบ Knapsack

การเข้ารหัสแบบ Knapsack เป็นการเข้ารหัสแบบ Asymmetric Cryptosystem การเข้ารหัสแบบแนบแสคมีหลักการเบื้องต้นดังนี้

กำหนดเซตของจำนวนเต็ม { a_0, a_1, ... , a_n } และจำนวนเต็ม s ที่ a_0+ a_1+ ... + a_n >s ต้องหาสับเซตที่ทำให้ผลบวกของสมาชิกทุกตัวในสับเซตนั้นเท่ากับ s พอดี

ตัวอย่าง กำหนด A = { 2, 3, 4, 7, 11, 13, 16 } หาสับเซตของ A ที่ทำให้ผลบวกสมาชิกเท่ากับ 8 และ 18

ไม่มีสับเซตใดที่ผลบวกเท่ากับ 8

แต่มี 4 สับเซตที่ผลบวกเท่ากับ 18 คือ { 2, 16 } , { 7, 11 } , { 2, 3, 13 } , { 3, 4, 11 }

ปัญหาต่อมาคือการหาเซต $\overline{X}$ = { x_0, x_1, ... , x_n } ที่ x_i =0 หรือ 1 ที่ s = $\sum_{i=0}^{n} a_i x_i$ เมื่อ { a_0, a_1, ... , a_n } เป็นลำดับสมาชิกใน A

ในการหาไม่จำเป็นต้องหาได้เสมอ แต่หาก A เป็นเซตลำดับ Super increasing ที่ $a_n > a_{n-1} + a_{n-2} + \dots + a_1 + a_0$ ให้ $X_n = \begin{cases} 1, a_n \le s \\ 0, a_n > s \end{cases}$ แล้วทำจนจบจากข้างหลังมาข้างหน้าแทน s แต่ละตัวด้วย $s - a_n x_n$

ตัวอย่าง (3, 7, 17, 30, 59) หา $\overline{X}$ = { x_0, x_1, ... , x_4 } ที่รวม s = 83

$a_4 = 59 < 83$ ดังนั้น $x_4 = 1$

$a_3 = 30 > 24$ ดังนั้น $x_3 = 0$

$a_2 = 17 < 24$ ดังนั้น $x_2 = 1$

$a_1 = 7 = 7$ ดังนั้น $x_1 = 1$

$a_0 = 3 > 0$ ดังนั้น $x_0 = 0$

ดังนั้นจะได้ $\overline{X}$ = { 0, 1, 1, 0, 1 }

ซึ่ง Merkle และ Hellman ซึ่งเป็นนักคณิตศาสตร์ได้ใช้ความจริงที่ว่าปัญหาแนบแสคโดยทั่วไปจะไม่สามารถหาคำตอบได้ แต่หากสมาชิกใน A เป็นลำดับ Super increasing แล้วจะสามารถแก้ปัญหาได้โดยง่าย มาสร้างระบบรหัสลับ

การเข้ารหัสและถอดรหัส Knapsack

การเข้ารหัสและถอดรหัส Knapsack มีหลักการดังนี้

1. เปลี่ยนตัวอักษรแต่ละตัวไปเป็นตัวเลขฐานสอง ความยาว n+1
2. สร้างลำดับ Super Increasing ($a_0, a_1, \ldots, a_n$)
3. เลือก m ที่ $m > 2a_n$
4. เลือก w ที่ $(w, m) = 1$
5. สร้าง w' ที่ $ww' \equiv 1 \pmod{m}$
6. สร้าง ($b_0, b_1, \ldots, b_n$) โดยให้ $b_i \equiv a_i w \pmod{m}$, I=0, 1, ..., n และใช้ ($b_0, b_1, \ldots, b_n$) เป็น Public Key
7. การเข้ารหัสก็คือสร้าง $c = b_0x_0 + b_1x_1 + \ldots + b_nx_n$ เป็นตัวเลขชุดหนึ่งที่พร้อมส่ง
8. ในขั้นตอนการถอดรหัสก็เช่นเดียงกันกับที่กล่าวมาข้างต้น เพียงแต่ใช้กุญแจถอดรหัสคือ (w', m) ซึ่งได้จาก

$$w'c \equiv w'(b_0x_0 + b_1x_1 + \ldots + b_nx_n) \pmod{m}$$

$$\equiv (w'b_0)x_0 + (w'b_1)x_1 + \ldots + (w'b_n)x_n \pmod{m}$$

$$\equiv (w'wa_0)x_0 + (w'wa_1)x_1 + \ldots + (w'wa_n)x_n \pmod{m}$$

$$c' \equiv a_0x_0 + a_1x_1 + \ldots + a_nx_n \pmod{m}$$

ตัวอย่าง กำหนด k = (111, 27, 49, 66, 95) จงเข้ารหัสข้อความ KNAP

แปลงข้อความแต่ละตัวอักษรเป็นเลขฐานสอง

P : 01010 01101 00000 01111

จาก 01010 จะได้เป็น 111(0) + 27(1) + 49(0) + 66(1) + 95(0) = 93

จาก 01101 จะได้เป็น 111(0) + 27(1) + 49(1) + 66(0) + 95(1) = 171

จาก 00000 จะได้เป็น 111(0) + 27(0) + 49(0) + 66(0) + 95(0) = 0

จาก 01111 จะได้เป็น 111(0) + 27(1) + 49(1) + 66(1) + 95(1) = 237

ดังนั้น C : 93 171 0 237

ตัวอย่าง จากตัวอย่างข้างต้น ให้ถอดรหัสเมื่อกุญแจถอดรหัสคือ (116, 37)

กุญแจถอดรหัส (m, w) คือ (116, 37)

ในที่นี้จะแสดงวิธีการถอดรหัสเพียงตัวเดียวคือ 93

ดังนั้นหา w' ได้ $37w' \equiv 1 \pmod{116}$

จะได้ $w' = 69$

จาก $w'c \equiv 69(93) \pmod{116}$

จะได้ $c' \equiv 37 \pmod{116}$

$37 \equiv a_0x_0 + a_1x_1 + \ldots + a_4x_4 \pmod{116}$

จาก $b_i \equiv a_iw \pmod{116}$

$w'b_i \equiv a_i \pmod{116}$

$a_0 \equiv 111(69) \equiv 3 \pmod{116}$

$a_1 \equiv 27(69) \equiv 7 \pmod{116}$

$a_2 \equiv 49(69) \equiv 17 \pmod{116}$

$a_3 \equiv 66(69) \equiv 30 \pmod{116}$

$a_4 \equiv 95(69) \equiv 59 \pmod{116}$

ดังนั้นจะได้ลำดับ Super Increasing คือ { 3, 7, 17, 30, 59 }

ดังนั้นจะได้ว่า $37 \equiv 3x_0 + 7x_1 + 17x_2 + 30x_3 + 59x_4 \pmod{116}$

และจะได้ตัวแรกคือ P : 01010 ซึ่งคือตัวอักษร K ของข้อความต้นฉบับ

การเข้ารหัสแบบ RSA

การเข้ารหัสแบบ RSA เป็นการเข้ารหัสแบบ Asymmetric Cryptosystem ซึ่งได้ถูกเสนอขึ้นในปี ค.ศ. 1970 โดย Rivest, Shamir และ Adleman มีพื้นฐานอยู่บน Modular Exponentiation มีหลักการเบื้องต้นดังนี้

1. ค่ากุญแจในการเข้ารหัสอยู่ในรูปแบบ (e, n)
2. ค่าของ e เป็นค่าของ exponent และค่าของ n เป็น modulus
3. ค่าของ n เป็นผลคูณของจำนวนเฉพาะขนาดใหญ่สองจำนวน $n = pq$ และ $(e, \phi(n)) = 1$
4. ในการเข้ารหัสข้อมูลเริ่มต้นด้วยการแปลงตัวอักษรต่างๆ ให้อยู่ในรูปตัวเลขดังตารางข้างต้นที่ได้เสนอมาแล้ว
5. จากนั้นจึงสร้างบล็อคของตัวเลขที่มีจำนวนหลักเป็นเลขคู่ ซึ่งมีวิธีการคำนวณคือ $E(P) = C \equiv P^e \pmod{n}$, $0 < C < n$ ซึ่งจะได้ผล

การคำนวณเป็นชุดของบล็อคตัวเลขที่ใช้ส่งเป็นข้อความที่เข้ารหัสเรียบร้อยแล้ว

6. ในการถอดรหัสข้อความจำเป็นต้องมีความรู้เกี่ยวกับการคำนวณหา d ซึ่งเป็นอินเวอร์สของ e (mod $\phi(n)$) ดังนี้

$$D(C) \equiv C^d = (P^e)^d = P^{ed} = P^{k\phi(n)+1} \pmod{n}$$

$$\equiv (P^{\phi(n)})^k P \equiv P \pmod{n}$$

7. เมื่อ $ed = k\phi(n) + 1$ สำหรับจำนวนเต็มบางจำนวน k เพราะว่า $ed \equiv 1 \pmod{\phi(n)}$ และโดยทฤษฎีบทของออยเลอร์ จะได้ว่า $P^{\phi(n)} \equiv 1 \pmod{n}$ เมื่อ $(P, n) = 1$ จะได้ว่า (d, n) เป็นกุญแจในการถอดรหัส

ตัวอย่าง ในการเข้ารหัสแบบ RSA กำหนดให้จำนวนเฉพาะทั้งสองคือ 43 และ 59 จะได้ $n = pq = 43 \cdot 59 = 2537$ และให้ $e = 13$ ซึ่งจะได้ $(e, \phi(n)) = (13, 42 \cdot 58) = 1$ และข้อความในการเข้ารหัสคือ PUBLIC KEY CRYPTOGRAPHY

เริ่มต้นด้วยการแปลงตัวอักษรเป็นตัวเลขและจัดกลุ่มตัวเลขที่ได้เป็นบล็อคตัวเลขความยาวเท่ากับ 4 หลัก จะได้เป็น

1520 0111 0802 1004 2402 1724 1519 1406 1700 1507 2423

ในกรณีตัวอย่างนี้มีการเติมตัวอักษร X = 23 ลงในบล็อคสุดท้ายเพื่อจัดกลุ่มบล็อคสุดท้ายให้เต็ม

จากนั้นจึงเปลี่ยน plaintext ที่ได้เป็น ciphertext ตามสมภาค

$$C \equiv P^{13} \pmod{2537}$$

ซึ่งยกตัวอย่างบล็อคแรกจะได้

$$C \equiv (1520)^{13} \pmod{2537} \equiv 95 \pmod{2537}$$

เมื่อคำนวณหมดทุกบล็อคแล้วจะได้

0095 1648 1410 1299 0811 2333 2132 0370 1185 1457 1084

ซึ่งก็คือ ciphertext ที่จะใช้ส่งไปให้ผู้รับ

ต่อมาคือขั้นตอนในการถอดรหัส เริ่มแรกต้องหาอินเวอร์สของ e = 13 (mod $\phi(2537)) = \phi(43 \cdot 59) = 42 \cdot 58 = 2436$ เมื่อใช้ทฤษฎีบทของออยเลอร์ จะได้ d = 937 เป็นอินเวอร์สของ 13 (mod 2436)

ในการถอดรหัสจะใช้สมภาค

$$P \equiv C^{937} \pmod{2537}, 0 \leq P \leq 2537$$

ซึ่งเมื่อถอดรหัสบล็อคต่างๆ ของ ciphertext จะได้ดังต่อไปนี้

$$P \equiv 95^{937} \pmod{2537} \equiv 1520 \pmod{2537}$$

$$P \equiv 1648^{937} \pmod{2537} \equiv 111 \pmod{2537}$$

$$P \equiv 1410^{937} \pmod{2537} \equiv 802 \pmod{2537}$$

$$P \equiv 1299^{937} \pmod{2537} \equiv 1004 \pmod{2537}$$

$$P \equiv 811^{937} \pmod{2537} \equiv 2402 \pmod{2537}$$

$$P \equiv 2333^{937} \pmod{2537} \equiv 1724 \pmod{2537}$$

$$P \equiv 2132^{937} \pmod{2537} \equiv 1519 \pmod{2537}$$

$$P \equiv 370^{937} \pmod{2537} \equiv 1406 \pmod{2537}$$

$$P \equiv 1185^{937} \pmod{2537} \equiv 1700 \pmod{2537}$$

$$P \equiv 1457^{937} \pmod{2537} \equiv 1507 \pmod{2537}$$

$$P \equiv 1084^{937} \pmod{2537} \equiv 2423 \pmod{2537}$$

ซึ่งก็จะได้กลับมาเป็น plaintext เดิม

2.3.11 Elliptic Curve and Quadratic Residue

Elliptic Curve คือ เซตของจุด (x, y) บนระนาบที่สอดคล้องกับสมการ $y^2 = x^3 + ax + b$ เมื่อ a, b เป็นจำนวนจริงใดๆ

$Z_p = \{ n \in Z \mid 0 \leq n < p$ และ p เป็นจำนวนเฉพาะ $\}$

เช่น $Z_7 = \{ 1, 2, 3, 4, 5, 6 \}$

บทนิยาม กำหนดให้ $P(x_p, y_p)$ เป็นจุดบน Elliptic Curve แล้ว $-P$ คือจุด $-P(x_p, -y_p)$ เป็น จุดสะท้อนของ P

การบวกสองจุดใดๆ บน Elliptic Curve

กำหนดให้ $P(x_p, y_p)$ และ $Q(x_q, y_q)$ เป็นจุดบน Elliptic Curve แล้ว $P + Q = R$ เมื่อ $R(x_r, y_r)$ คือ จุดสะท้อนของจุดที่เกิดจากการลากเส้นตรงผ่านจุด P และ Q ไปตัดยัง Elliptic Curve เมื่อ $P \neq Q$ และ $P \neq -P$

การบวกจุด P กับจุด -P

ให้ $P(x_p, y_p)$ เป็นจุดบน Elliptic Curve เมื่อ $P(x_p, y_p)$ และ $-P(x_p, -y_p)$ ผลบวกจะได้จากการลากเส้นตรงต่อจุดทั้งสองจุดตามที่ได้อธิบายข้างต้น แต่ผลลัพธ์การตัดครั้งนี้ เส้นตรงดังกล่าวไม่ตัด Elliptic Curve เลย ดังนั้นจึงได้กำหนดจุด Point at Infinity เป็นผลบวกของจุดทั้งสองจุดในกรณีนี้

การบวกจุด P กับจุด P เมื่อจุด P ไม่อยู่บนแกน X

กำหนดจุด $P(x_p, y_p)$ เป็นจุดบน Elliptic Curve โดยที่ $y_p \neq 0$ ผลบวกทำได้โดยลากเส้นสัมผัส Elliptic Curve ที่จุด P เส้นสัมผัสนี้จะตัด Elliptic Curve ที่จุดอีกจุดหนึ่ง –R ซึ่งเป็นจุดสะท้อนของจุดที่เป็นผลลัพธ์ R ของการบวกครั้งนี้ และจะได้ว่า $P + P = 2P$

การบวกจุด P กับจุด P เมื่อจุด P อยู่บนแกน X

กำหนดจุด $P(x_p, y_p)$ เป็นจุดบน Elliptic Curve โดยที่ $y_p = 0$ จะได้ผลลัพธ์การบวกเป็นจุด Point at Infinity เพราะเส้นสัมผัสจุดจะขนานกับแกน Y จึงไม่มีโอกาสตัด Elliptic Curve ดังนั้น $P + P = 2P = 0$

การบวกสองจุดใดๆ บน Elliptic Curve **เชิงพีชคณิต** แบ่งเป็นสองลักษณะ

1. การบวกจุด P และจุด Q เมื่อ $P \neq Q$ และ $P \neq -P$

   กำหนดให้ $P(x_p, y_p)$ และ $Q(x_q, y_q)$ แล้ว $P + Q = R$ เมื่อ $R(x_r, y_r)$ โดยที่

   $x_r = s^2 - x_p - x_r$ และ $y_r = -y_p + s(x_p - x_r)$

   เมื่อ $s = \dfrac{y_q - y_p}{x_q - x_p}$

2. การบวกจุด P กับจุด P เมื่อจุด P ไม่อยู่บนแกน X

กำหนดจุด $P(x_p, y_p)$ โดยที่ $y_p \neq 0$ การบวกในกรณีนี้จะได้ $P + P = 2P = R(x_r, y_r)$ โดยที่

$x_r = s^2 - 2x_p$ และ $y_r = -y_p + s(x_p - x_r)$

เมื่อ $s = \frac{3x_p^2 + a}{2y_p}$

Elliptic Curve บน Z_p

ในส่วนนี้กำหนดให้ p เป็นจำนวนเฉพาะที่มากกว่าหรือเท่ากับ 3 จะได้ Elliptic Curve $y^2 = x^3 + ax + b$ บน Z_p คือ เซตของจุด (x, y) ใดๆ ที่ $(x, y) \in Z_p \times Z_p$ และจะสอดคล้องกับสมภาค $y^2 \equiv x^3 + ax + b \pmod p$ และ $a, b \in Z_p$

การบวกสองจุดใดๆ ของ Elliptic Curve บน Z_p มีสองลักษณะดังนี้

1. การบวกจุด P และจุด Q เมื่อ $P \neq Q$ และ $P \neq -P$

กำหนดให้ $P(x_p, y_p)$ และ $Q(x_q, y_q)$ แล้ว $P + Q = R$ เมื่อ $R(x_r, y_r)$ โดยที่

$x_r \equiv s^2 - x_p - x_r \pmod p$ และ $y_r \equiv -y_p + s(x_p - x_r) \pmod p$

เมื่อ $s \equiv \frac{y_q - y_p}{x_q - x_p} \pmod p$

2. การบวกจุด P กับจุด P เมื่อจุด P ไม่อยู่บนแกน X

กำหนดจุด $P(x_p, y_p)$ โดยที่ $y_p \neq 0$ การบวกในกรณีนี้จะได้ $P + P = 2P = R(x_r, y_r)$ โดยที่

$x_r \equiv s^2 - 2x_p \pmod p$ และ $y_r \equiv -y_p + s(x_p - x_r) \pmod p$

เมื่อ $s \equiv \frac{3x_p^2 + a}{2y_p} \pmod p$

Quadratic Residue

บทนิยาม จากสมภาค $y^2 \equiv a \pmod p$ เมื่อ $a \in Z_p$

ถ้า $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ แล้ว $y^2 \equiv a \pmod p$ จะมีผลเฉลย และผลเฉลยจะมีค่า $y \equiv \pm a^{\frac{p+1}{4}} \pmod p$ เมื่อ $p = 4k + 3$

และถ้า $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ แล้ว $y^2 \equiv a \pmod p$ จะไม่มีผลเฉลย

ตัวอย่าง กำหนด $y^2 \equiv x^3 + x + 1 \pmod{17}$

X	$x^3 + x + 1 \pmod{17}$	$y^2 \equiv a \pmod{17}$	Y
0	1	หาได้	16, 1
1	3	หาไม่ได้	
2	11	หาไม่ได้	
3	14	หาไม่ได้	
4	1	หาได้	16, 1
5	12	หาไม่ได้	
6	2	หาได้	11, 6
7	11	หาไม่ได้	
8	11	หาไม่ได้	
9	8	หาได้	12, 5
10	8	หาได้	12, 5
11	0	หาไม่ได้	
12	7	หาไม่ได้	
13	1	หาได้	16, 1
14	5	หาไม่ได้	
15	8	หาได้	12, 5
16	16	หาได้	13, 4

ตาราง 2.3 ผลเฉลยของ $y^2 \equiv x^3 + x + 1 \pmod{17}$

Generator

Generator คือจุด P(x, y) ใดๆ ที่ $(x, y) \in Z_p \times Z_p$ ที่ เมื่อบวกกับตัวมันเองเรื่อยๆ แล้วจะได้จุดใหม่ที่ไม่ซ้ำกับจุดเดิม $P \neq 2P \neq 3P \neq \ldots \neq nP$ เมื่อ n เป็นจำนวนจุดทั้งหมดที่หาได้ และจุดคำตอบยังคงเป็น $(x, y) \in Z_p \times Z_p$

ตัวอย่าง จาก $y^2 \equiv x^3 + x + 3 \pmod{17}$

จะได้จุดที่เป็นคำตอบคือ (2,9), (2,8), (3,13), (3,4), (6,15), (6,2), (7,9), (7,8), (8,9), (8,8), (11,11), (11,6), (12,14), (12,3), (16,16), (16,1)

ทดสอบว่าจุด P(2, 9) เป็น generator หรือไม่

P : (2,9) 2P : (12,14)

3P : (16,1) 4P : (8,9)

5P : (7,8) 6P : (6,2)

7P : (11,11) 8P : (3,4)

9P : (3,13) 10P : (11,6)

11P : (6,15) 12P : (7,9)

13P : (8,8) 14P : (16,16)

15P : (12,3) 16P : (2,8)

ดังจะเห็นได้ว่า จุด P(2,9) เมื่อบวกตัวมันเองไปเรื่อยๆ จะได้จุดที่อยู่ในเซตของจุดคำตอบที่ไม่ซ้ำกันเลย ดังนั้น P(2,9) เป็น Generator

และเมื่อทดสอบด้วยวิธีดังกล่าวกับจุดที่เหลือจนหมดจะพบว่าสำหรับสมภาคดังกล่าวนี้จุดคำตอบทุกจุดสามารถเป็น generator ได้หมด