นิยาม ให้ a เป็นจำนวนเต็ม m เป็นจำนวนเต็มบวก จะใช้สัญลักษณ์ a mod m แทนเศษที่ได้จากการหาร a ด้วย m

ตัวอย่าง 3 mod 5 = 3 , -3 mod 5 = 2 , 17 mod 5 = 2,
-9 mod 4= 3 , 2001 mod 101 = 82

นิยาม ให้ $a , b \in Z$ $m \in Z^+$ จะเรียก a สมภาคกับ b มอดุโล m (a congruent to b modulo m) ถ้า $m \mid (a-b)$ จะใช้สัญลักษณ์แทนด้วย $a \equiv b \pmod m$

จะใช้สัญลักษณ์ $a \not\equiv b \pmod m$ แทน a ไม่สมภาคกับ b มอดุโล m

ตัวอย่าง $17 \equiv 5 \pmod 6$, $24 \not\equiv 14 \pmod 6$

ข้อสังเกตุ $a \equiv b \bmod m$ ก็ต่อเมื่อ $a \bmod m = b \bmod m$

ทฤษฎีบท ให้ $m \in Z^+$, $a, b \in Z$

$a \equiv b \bmod m$ ก็ต่อเมื่อ $a = b + km$ บาง k ที่เป็นจำนวนเต็ม

ทฤษฎีบท ให้ $m \in Z^+$, $a, b,c,d \in Z$ จะได้ว่า

1. $a \equiv a \pmod m$
2. ถ้า $a \equiv b \pmod m$ แล้ว $b \equiv a \bmod m$
3. ถ้า $a \equiv b \pmod m$ และ $b \equiv c \pmod m$ แล้ว $a \equiv c \pmod m$
4. ถ้า $a \equiv b \pmod m$ แล้ว $a + c \equiv b + c \pmod m$, $ac \equiv bc \pmod m$
5. ถ้า $a \equiv b \pmod m$ และ $c \equiv d \pmod m$ แล้ว
   $a + b \equiv c + d \pmod m$, $ab \equiv cd \bmod m$
6. ถ้า $a \equiv b \pmod m$ แล้ว $a^k \equiv b^k \bmod m$ ทุก $k \in Z^+$

ตัวอย่าง $7 \equiv 2 \bmod 5$, $11 \equiv 1 \pmod 5$ จะได้ว่า $18 = 7+11 \equiv 2 + 1 = 3 \pmod 5$
และ $77 = 7(11) \equiv 2(1) = 2 \pmod 5$

ตัวอย่าง จงแสดงว่า $15 \mid (17^{100} - 1)$

บทประยุกต์ ของ สมภาค

ตัวอย่าง การเลื่อกตัวเลขแบบสุ่มโดยวิธี สมภาคเชิงเส้น โดยการเลือกตัวเลข 4 ตัว คือ m, a, c,x_0 ซึ่ง $2 \le a < m$, $0 \le c < m$ และ $0 \le x_0 < m$.

แล้วจะสร้งตัวเลขลำดับ $\{ x_n \}$ ซึ่ง $0 \le x_n < m$ ทุก n จาก สมการ

$$x_{n+1} = a x_n + c \mod m$$

เช่น $m = 9, a = 7, c = 4 , x_0 = 3$

จะได้ว่า $x_1=7, x_2=8, x_3=6, x_4=1, x_5=2, x_6=0, x_7=4, x_8=5, x_9=3,\ldots$

ตัวอย่าง รหัส ซีซาร์ (Caesar cipher) กำหนดให้ ตัวอักษร A = 0 , B =1,…, Z = 25

ให้ $f(p) = p + 3 \mod 26$.

จงเปลี่ยนข้อความ " MEET YOU IN THE PARK " โดยรหัส ซีซาร์

ตัวอย่าง จงถอดข้อความ " WHQ" ที่ถูกเปลี่ยนโดยรหัสซีซาร์

ตัวอย่าง กำหนดให้ ตัวอักษร A = 0 , B =1,…, Z = 25

ให้ $f(p) = 7p+3 \mod 26$.

จงเปลี่ยนข้อความ " LOVE " โดย ใช้ฟังก์ชัน f .

สมภาคเชิงเส้น

นิยาม สมภาค ในรูปแบบ $ax \equiv b \bmod m$ เมื่อ $m \in Z^+$, $a, b \in Z$ และ x เป็นตัวแปร จะเรียกว่า สมภาคเชิงเส้น (Linear Congruences)

นิยาม จะเรียก จำนวนเต็ม x_0 ที่สอดคล้องในสมภาคเชิงเส้น $ax \equiv b \bmod m$ ว่าผลเฉลย (solution) ของสมภาคเชิงเส้น

ทฤษฎีบท ถ้า x_0 เป็นผลเฉลย ของสมภาคเชิงเส้น $ax \equiv b \bmod m$ และ $x_0 \equiv x_1$ แล้ว x_1 เป็นผลเฉลย ของสมภาคเชิงเส้นด้วย

ทฤษฎีบท ให้ $m \in Z^+$, $a, b \in Z$ และ $d = \gcd(a, m)$ แล้วจะได้ว่า สมภาคเชิงเส้น $ax \equiv b \bmod m$ มีผลเฉลย ก็ต่อเมื่อ $d \mid n$

ตัวอย่าง จงหาผลเฉลย (ถ้ามี) ของสมภาคเชิงเส้น $14x \equiv 13 \bmod 21$

ตัวอย่าง จงหาผลเฉลย (ถ้ามี) ของสมภาคเชิงเส้น $235x \equiv 54 \bmod 7$

ทฤษฎีบท ให้ $m, n \in Z^+$, $a, b \in Z$ และ $\gcd(m, n) = 1$ แล้วระบบสมภาคเชิงเส้น

$x \equiv a \bmod m$

$x \equiv b \bmod n$

มีผลเฉลยร่วมกันเพียงชุดเดียวมอดุโล mn

ทฤษฎีบท (Chiness Remainder Theory)

ให้ $m_1, m_2, \ldots, m_k \in Z^+$, $a_1, a_2, \ldots, a_k \in Z$ และ $\gcd(m_i, m_j) = 1$ ถ้า $i \neq j$ แล้วระบบสมภาคเชิงเส้น

$x \equiv a_1 \bmod m_1$

$x \equiv a_2 \bmod m_2$

$x \equiv a_k \bmod m_k$

มีผลเฉลยร่วมกันเพียงชุดเดียวมอดุโล $m_1 m_2 \ldots m_k$

ตัวอย่าง จงหาผลเฉลยของระบบสมภาคเชิงเส้น

$x \equiv 2 \mod 3$, $x \equiv 3 \mod 5$, $x \equiv 2 \mod 7$

ตัวอย่าง จงหาผลเฉลยของระบบสมภาคเชิงเส้น

$x \equiv 7 \mod 9$, $x \equiv 3 \mod 23$, $x \equiv 1 \mod 4$

การคำนวณ ตัวเลขที่มีค่ามาก

ให้ $m_1, m_2, .., m_n > 1$ เป็นจำนวนเฉพาะสัมพัทธ์ต่อกันทุกคู่ ($\gcd(m_i,m_j) = 1$ ถ้า $i \neq j$)

$m = m_1.m_2 .. m_n$ จะได้ว่า ทุกจำนวนเต็ม a ที่ $0 \leq a < m$

สามารถแทนได้ด้วย n-สิ่งอันดับ ($a \mod m_1$, $a \mod m_2$,..., $a \mod m_n$)

ตัวอย่าง ให้ $m_1 = 3$ และ $m_2 = 4$

ดังนั้นสามารถแทนตัวเลข ตั้งแต่ 0 ถึง 11 ได้ด้วยคู่อันดับต่อไปนี้

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)

ตัวอย่าง ให้ $m_1 = 99$, $m_2 = 98$, $m_3 = 97$ และ $m_4 = 95$

จงแทนตัวเลข 123684 และ 413456 ด้วย 4-สิ่งอันดับ

และถ้า 4ขสิ่งอันดับแทนได้ด้วย (65,2,51,10) จงหาค่าของตัวเลขนี้

รหัส RSA (RSA Encryption)

รหัส RSA สร้างโดยกลุ่ม นักวิจัย 3 คน คือ Rivert , Shamir and Adleman โดยการสร้างฟังก์ชั่นการแปลงรหัสเป็น

$$C = M^e \mod m$$

เมื่อ $m = p.g$ โดยที่ p , q เป็นจำนวนเฉพาะ $1 < e < (p-1)(q-1)$ และ $\gcd(e ,(p-1)(q-1)) = 1$

และ สามารถถอดรหัสเป็น

$$P = C^d \mod m$$

โดยต้องหาค่า d ที่ $d\,e \equiv 1 \mod (p-1)(q-1)$

ซึ่งในทางปฏิบัติแล้วการที่จะแปลงรหัสด้วยวิธีนี้เราต้องมีเครื่องคำนวณที่มีความสามารถในการคิดตัวเลขที่มีค่ามากได้เร็วดังตัวอย่าง

ตัวอย่าง จงแปลงรหัส ข้อความ STOP โดยใช้รหัส RSA เมื่อ p = 43 และ q = 59 และ เลือก e = 13

วิธีทำ จากข้อความ STOP แปลงเป็นตัวเลขได้ 18, 19, 14, 15

จัดกลุ่มตัวเลขเป็น 4 หลัก (แล้วแต่ข้อตกลงระหว่างผู้ส่งกับผู้รับ)ได้เป็น 1819 และ 1415

แปลงรหัสโดย $C = M^{13} \mod (43)(59) = 2537$

ได้เป็น $1819^{13} \mod 2537 = 2081$ และ $1415^{13} \mod 2537 = 2182$

ดังนั้นจะได้ตัวเลขที่ได้จากการแปลงรหัสเป็น 2081 2182 ซึ่งจะแปลงเป็นตัวอักษรต่อไป

ตัวอย่าง จงถอดรหัส RSA จากตัวอย่างที่แล้ว ที่แปลงมาจากข้อความแล้วได้ตัวเลข 0981 0461 โดยที่ผู้ส่งรหัส บอกค่า e =13 และ n = 2537

วิธีทำ จาก n = 2537 แยกตัวประกอบเป็นจำนวนเฉพาะ 2 ตัวคูณกันได้ 43 59

หา d ที่ทำให้ได้ว่า $d(13) \equiv 1 \mod (42)(58)$ ได้ d = 937

ถอดรหัส โดย $P = C^{937} \mod 2537$

ดังนั้น $0981^{937} \mod 2537 = 0704$ และ $0461^{937} \mod 2537 = 1115$

ซึ่งถอดเป็นข้อความได้เป็น HELP.

ดูเพิ่มเติมที่ http://www.orst.edu/dept/honors/makmur/index.html

และที่ http://www.rsasecurity.com/