COMP 2711 Discrete Mathematical Tools for Computer Science
2022 Fall Semester – Tutorial 8

Question 1: Find the inverse of 15 mod 26.

Solution : First find $\gcd(26, 15)$:

$$\begin{aligned} 26 &= 15 \cdot 1 + 11 \\ 15 &= 11 \cdot 1 + 4 \\ 11 &= 4 \cdot 2 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

So, $\gcd(26, 15) = 1$.

Rewriting:

$$\begin{aligned} 11 &= 26 - 15 \cdot 1 \\ 4 &= 15 - 11 \cdot 1 \\ 3 &= 11 - 4 \cdot 2 \\ 1 &= 4 - 3 \cdot 1 \end{aligned}$$

Substituting:

$$\begin{aligned} 1 &= 4 - (11 - 4 \cdot 2) \cdot 1 \\ &= 4 \cdot 3 - 11 \cdot 1 \\ &= (15 - 11 \cdot 1) \cdot 3 - 11 \cdot 1 \\ &= 15 \cdot 3 - 11 \cdot 4 \\ &= 15 \cdot 3 - (26 - 15 \cdot 1) \cdot 4 \\ &= 15 \cdot 7 - 26 \cdot 4 \end{aligned}$$

Therefore, the linear combination is $1 = 15 \cdot 7 + 26 \cdot -4$. Multiplicative inverse of 15 modulo 26 is $7 \bmod 26 = 7$.

Verify:
$7 \cdot 15 \equiv 1 \pmod{26}$.

Question 2: Show that the following equation has no solution

$$16 \cdot_{46} x = 3$$

Solution : If there was such an x then $16x = 46q + 3$ for some q.
Then $3 = 16x - 46q = 2(8x - 23q)$
Since 2 does not divide 3, this is impossible.

Question 3: Solve each of these congruences using the results $19 \cdot 52 \equiv 1 \pmod{141}$, $55 \cdot 34 \equiv 1 \pmod{89}$ and $89 \cdot 73 \equiv 1 \pmod{232}$.

(a) $19x \equiv 4 \pmod{141}$

(b) $55x \equiv 34 \pmod{89}$

(c) $89x \equiv 2 \pmod{232}$

Solution : (a) An inverse of 19 modulo 141 is 52.
$19^{-1} \cdot 19 \cdot x \equiv 19^{-1} \cdot 4 \pmod{141}$.
$x \equiv 52 \cdot 4 \equiv 67 \pmod{141}$

(b) 88

(c) 146

Question 4: Find a solution x in Z_{143} that satisfies the following system of equations,

$$\begin{aligned} x &\equiv 4 \pmod{13} \\ x &\equiv 8 \pmod{11}. \end{aligned}$$

Solution : Given a system of equations:

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

The solution $x \equiv a \cdot n \cdot n^{-1} + b \cdot m \cdot m^{-1} \pmod{mn}$.

Because 13 and 11 are relatively prime, the Chinese Remainder Theorem tells us that there is a unique solution in Z_{143}. By the extended GCD algorithm, we have $13 \cdot 6 \equiv 1 \pmod{11}$ and $11 \cdot 6 \equiv 1 \pmod{13}$.

Hence, $x = 4 \cdot 11 \cdot 6 + 8 \cdot 13 \cdot 6 = 888 \equiv 30 \pmod{143}$.