

Tutorial-I & II (Mathematical Background)

1. Consider the groups $G_1 = \langle \mathbb{Z}_6, + \rangle$ and $G_2 = \langle \mathbb{Z}_{10}^*, \times \rangle$

(i) Draw Group Operation table

(ii) Find the cyclic groups can be made from G_1 and G_2

2. List all subgroups of $\mathbb{Z}_9$ and $\mathbb{Z}_{13}^*$

3. Find the all primitive root of $\mathbb{Z}_{18}^*$.

4. Find the solution to the simultaneous equations using CRT.

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

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

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

Hint : Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \dots \times m_k$, where m_i represents modulo of different equation which are relatively prime. This is the common modulus.

2. Find $M_1 = M/m_1, M_2 = M/m_2, \dots, M_k = M/m_k$.

3. Find the multiplicative inverse of $M_1, M_2, \dots, M_k$ using the corresponding moduli $(m_1, m_2, \dots, m_k)$. Call the inverses $M_1^{-1}, M_2^{-1}, \dots, M_k^{-1}$.

4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \dots + a_k \times M_k \times M_k^{-1}) \pmod{M}$$