# Tutorial 1

**P1** $a \mid b \iff \exists k \in \mathbb{Z} \quad a \cdot k = b$

a) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

$a \mid b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a$

$b \mid c \Rightarrow \exists k_2 \in \mathbb{Z} : c = k_2 \cdot b$

$\Rightarrow c = \underbrace{k_2 \cdot k_1}_{k} \cdot a \Rightarrow \exists k \in \mathbb{Z} : c = k \cdot a \Rightarrow a \mid c$

b) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

$a \mid b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a$

$c \mid d \Rightarrow \exists k_2 \in \mathbb{Z} : d = k_2 \cdot c$

$\Rightarrow b \cdot d = \underbrace{k_1 \cdot k_2}_{k} \cdot a \cdot c \Rightarrow \exists k \in \mathbb{Z} : bd = k \cdot a \cdot c \Rightarrow ac \mid b \cdot d$

c) $a \mid b \wedge a \mid c \Rightarrow a \mid (\lambda \cdot b + \gamma \cdot c) \quad \forall \lambda, \gamma \in \mathbb{Z}$

$a \mid b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a \Rightarrow \forall \lambda \in \mathbb{Z} \quad \lambda \cdot b = \lambda \cdot k_1 \cdot a$

$a \mid c \Rightarrow \exists k_2 \in \mathbb{Z} : c = k_2 \cdot a \Rightarrow \forall \gamma \in \mathbb{Z} \quad \gamma \cdot c = \gamma \cdot k_2 \cdot a$

$\Rightarrow \lambda \cdot b + \gamma \cdot c = \lambda \cdot k_1 \cdot a + \gamma \cdot k_2 \cdot a = \underbrace{(\lambda \cdot k_1 + \gamma \cdot k_2)}_{k} \cdot a$

$\Rightarrow \exists k : \lambda \cdot b + \gamma \cdot c = k \cdot a \Rightarrow a \mid (\lambda \cdot b + \gamma \cdot c)$ ✓

P2] $a, b, m \in \mathbb{Z}$ ; $gcd(a,b)$ : greatest common divisor of $a, b$

a) $gcd(a,b) = 1 \Rightarrow gcd(a \cdot b, m) = gcd(a,m) \cdot gcd(b,m)$

Solution: Write a and b in terms of their prime factorization

$$a = \prod_{i=1}^{k_a} p_i^{t_i} \qquad [\, t_i \in \mathbb{N},\ p_i \text{ prime},\ p_i \neq p_j\ \forall i \neq j \,]$$

$$b = \prod_{j=1}^{k_b} q_j^{u_j}$$

We know $gcd(a,b) = 1 \Rightarrow \forall i,j : p_i \neq q_j$

Represent m as

$$m = \prod_{i=1}^{k_a} p_i^{\hat{t}_i} \prod_{j=1}^{k_b} q_j^{\hat{u}_j} \prod_{l=1}^{k_m} r_l^{v_l} \qquad [\, \hat{t}_i, \hat{u}_j \in \mathbb{N}_0,\ r_l \neq p_i,\ r_l \neq q_j \,]$$

$$gcd(ab, m) = gcd\left( \prod_{i=1}^{k_a} p_i^{t_i} \cdot \prod_{j=1}^{k_b} q_j^{u_j} \ /\ \prod_{i=1}^{k_a} p_i^{\hat{t}_i} \prod_{j=1}^{k_b} q_j^{\hat{u}_j} \cdot \prod_{l=1}^{k_m} r_l^{v_l} \right)$$

$$= \prod_{i=1}^{k_a} p_i^{t_i'} \prod_{j=1}^{k_b} q_j^{u_j'} = gcd(a,m) \cdot gcd(b,m) \quad \checkmark$$

$t_i' = \min\{t_i, \hat{t}_i\}\ \forall i$

$u_j' = \min\{u_j, \hat{u}_j\}\ \forall j$

b) Let $a = b = 2$, $m = 4$

$gcd(a \cdot b, m) = gcd(4,4) = 4 = gcd(a,m) \cdot gcd(b,m) = 2 \cdot 2 = 4$ ✓

But $gcd(a,b) = gcd(2,2) = 2$

P3| Have a look at the following representation of the message:

$$\left(\begin{array}{cccc|cccc} m_1 & m_{\ell+1} & \dots & m_{(k-1)\ell+1} & 1 & 2 & \dots & k \\ m_2 & \vdots & & \vdots & k+1 & \dots & & 2k \\ \vdots & \vdots & & m_{k\cdot\ell-1} & \vdots & & & \\ m_\ell & & & m_{k\ell} & & & & (\ell-1)\cdot k \\ & & & & (\ell-1)\cdot k+1 & \dots & & \underbrace{k\cdot\ell}_{\sim} \end{array}\right)$$

From this encryption the Scytale may be described as permutation $\pi$

$$\pi = \begin{pmatrix} 1 & 2 & \dots & \ell & \ell+1 & \dots & (k-1)\ell+1 & \dots & k\cdot\ell-1 & k\ell \\ 1 & k+1 & & (\ell-1)\cdot k+1 & 2 & \dots & k & \dots & (\ell-1)\cdot k & k\ell \end{pmatrix}$$