Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 1
- Proposed Solution -

Friday, April 12, 2019

Solution of Problem 1

It holds $a \mid b \Leftrightarrow \exists k \in \mathbb{Z}$ with $ak = b$.

a) Show that from $a \mid b$ and $b \mid c$ it follows that $a \mid c$.
$a \mid b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a$
$b \mid c \Rightarrow \exists k_2 \in \mathbb{Z} : c = k_2 \cdot b$
$\Rightarrow c = k_1 \cdot k_2 \cdot a$
$\Rightarrow k = k_1 \cdot k_2$
$\Rightarrow \exists k \in \mathbb{Z} : c = k \cdot a$
$\Rightarrow a \mid c$

b) Show that from $a \mid b$ and $c \mid d$ it follows that $(ac) \mid (bd)$.
$a \mid b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a$
$c \mid d \Rightarrow \exists k_2 \in \mathbb{Z} : d = k_2 \cdot c$
$\Rightarrow b \cdot d = k_1 \cdot a \cdot k_2 \cdot c$
$\Rightarrow k = k_1 \cdot k_2$
$\Rightarrow \exists k \in \mathbb{Z} : b \cdot d = k \cdot a \cdot c$
$\Rightarrow (a \cdot c) \mid (b \cdot d)$

c) Show that from $a \mid b$ and $a \mid c$ it follows that $a \mid (xb + yc) \;\; \forall\, x, y \in \mathbb{Z}$.
$a \mid b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a$
$\Rightarrow x \in \mathbb{Z}, x \cdot b = xk_1 \cdot a$
$a \mid c \Rightarrow \exists k_2 \in \mathbb{Z} : c = k_2 \cdot a$
$\Rightarrow y \in \mathbb{Z}, y \cdot c = yk_2 \cdot a$
$xb + yc = xk_1 \cdot a + yk_2 \cdot a = (xk_1 + yk_2)a$
$\Rightarrow k = xk_1 + yk_2$
$\Rightarrow \exists k \in \mathbb{Z} : (xb + yc) = k \cdot a$
$\Rightarrow a \mid (xb + yc)$

Solution of Problem 2

a) Let $a, b, m \in \mathbb{Z}$. Show that if $\gcd(a, b) = 1$, then $\gcd(ab, m) = \gcd(a, m)\gcd(b, m)$.
Solution:

Write a and b in terms of their prime factorizations, $t_i, u_j \in \mathbb{N}$.

$$a = \prod_{i=1}^{k_a} p_i^{t_i}$$

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

By assumption we have $\gcd(a, b) = 1$, which means that for all indices i, j it hold $p_i \neq q_j$. Thus, those two products have no common divisor greater than 1.

Write m in terms of its prime factorization, though we add the prime factors of a, b. Hence, in this representaion the exponents $\hat{t}_i$ and $\hat{u}_j$ might be zero, but $v_l \in \mathbb{N}$.

$$m = \prod_{i=1}^{k_a} p_i^{\hat{t}_i} \prod_{j=1}^{k_b} q_j^{\hat{u}_j} \prod_{l=1}^{k_m} r_l^{v_l}$$

Moreover, the primes r_l shall be unequal to all the primes occuring in the prime factorization of a and b. Hence, the representation is unique.

The greatest common divisor of interest here yields:

$$\begin{aligned} \gcd(ab, m) &= \gcd\left(\prod_{i=1}^{k_a} p_i^{t_i} \cdot \prod_{j=1}^{k_b} q_j^{u_j}, \prod_{i=1}^{k_a} p_i^{\hat{t}_i} \prod_{j=1}^{k_b} q_j^{\hat{u}_j} \prod_{l=1}^{k_m} r_l^{v_l}\right) \\ &= \prod_{i=1}^{k_a} p_i^{t'_i} \prod_{j=1}^{k_b} q_j^{u'_j} = \gcd(a, m) \gcd(b, m), \end{aligned}$$

where

$$\begin{aligned} t'_i &= \min\{t_i, \hat{t}_i\}, \\ u'_j &= \min\{u_j, \hat{u}_j\}. \end{aligned}$$

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

$\gcd(ab, m) = \gcd(4, 4) = \gcd(2, 4) \gcd(2, 4) = 4 = \gcd(a, m) \gcd(b, m)$, but obviously $\gcd(a, b) = 2$.

Solution of Problem 3

It is helpful to organize the plaintext $\boldsymbol{m} = (m_1, m_2, m_3, ..., m_{kl})$ in a matrix with l rows and k columns as shown on the left hand side. The second matrix on the right hand side describes the mapping of the positions to the ciphertext.

$$\begin{array}{cccc|cccc} m_1 & m_{l+1} & \cdots & m_{(k-1)l+1} & 1 & 2 & \cdots & k \\ m_2 & \cdots & \cdots & \vdots & k+1 & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & \vdots & \vdots & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & m_{kl-1} & \vdots & \cdots & \cdots & (l-1)k \\ m_l & \cdots & \cdots & m_{kl} & (l-1)k+1 & \cdots & \cdots & kl \end{array}$$

From this the encryption of the Scytale is described by a permutation $\boldsymbol{\pi}$ with:

$$\boldsymbol{\pi} = \begin{pmatrix} 1 & 2 & \dots & l & l+1 & \dots & (k-1)l+1 & \dots & kl-1 & kl \\ 1 & k+1 & \dots & (l-1)k+1 & 2 & \dots & k & \dots & (l-1)k & kl \end{pmatrix}$$