**Prof. Dr. Rudolf Mathar, Dr. Michael Reyer**

# Tutorial 1

Friday, April 12, 2019

**Problem 1.** *(Dividers)* Let $a$, $b$, $c$, $d \in \mathbb{Z}$. The integer $a$ divides $b$, if and only if there exists a $k \in \mathbb{Z}$ such that $a \cdot k = b$. This property is denoted by $a \mid b$. Prove the following implications.

**a)** $a \mid b$ and $b \mid c \quad \Rightarrow \quad a \mid c$.

**b)** $a \mid b$ and $c \mid d \quad \Rightarrow \quad (ac) \mid (bd)$.

**c)** $a \mid b$ and $a \mid c \quad \Rightarrow \quad a \mid (xb + yc) \;\; \forall\, x, y \in \mathbb{Z}$.

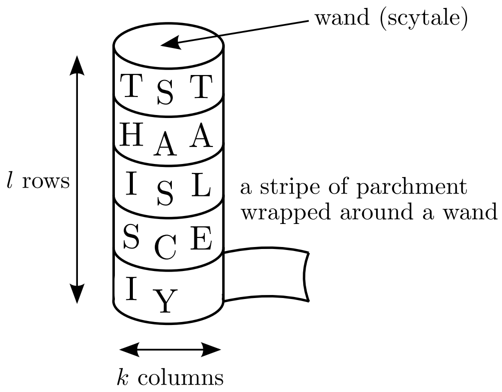
**Problem 2.** *(GCD Multiplicativity)* Let $a, b, m \in \mathbb{Z}$ and $\gcd(a, b)$ the greatest common divisor of $a$ and $b$.

**a)** Show the following.

$$\gcd(a, b) = 1 \Longrightarrow \gcd(ab, m) = \gcd(a, m)\gcd(b, m)$$

**b)** Show that the reverse direction does not hold true.

**Problem 3.** *(Scytale)* For the encryption with an ancient Scytale, a parchment is wrapped around a wand such that there are $l \in \mathbb{N}$ rows and $k \in \mathbb{N}$ columns, cf. the conceptual figure. The letters of the plaintext $\boldsymbol{m} = (m_1, m_2, \ldots, m_{kl})$ are written columnwise on the parchment. After unwrapping, the cryptogram is given on the stripe of parchment.




**a)** Give the entries $\pi(i)$ for $i \in \{1, 2, l, l+1, (k-1)l+1, kl-1, kl\}$ for the permutation

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

which describes the encryption scheme of the Scytale with $l$ rows and $k$ columns.