Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 1
- Proposed Solution -

Friday, April 20, 2018

Solution of Problem 1

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

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

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

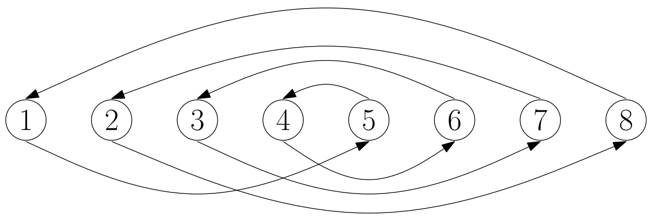
Solution of Problem 2

a)
- Try to identify common bigrams and trigrams.
  e.g. ch, th, nd, st, sh, sp, etc.
  e.g. the, ing, and.
- Check phrases with not so frequent letters like x, v, q.
- Try to guess words directly, e.g. *difficult* here.
- Apply the assumed permutation to the other blocks.

Ciphertext is

THISEXRE CISEISNO TDIFFICU LTEITHER

b) Permutation graph is



Therefore,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 6 & 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 1 & 4 & 3 & 2 \end{pmatrix}$$

Solution of Problem 3

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 factorization:

$$a = \prod_{i=1}^{k_a} p_i^{t_i} = a_1 \cdot a_2 \cdot \ldots \cdot a_{k_a}$$

$$b = \prod_{j=1}^{k_b} p_j^{l_j} = b_1 \cdot b_2 \cdot \ldots \cdot b_{k_b}$$

By assumption we have:

$$\gcd(a, b) = \gcd(\prod_{i=1}^{k_a} p_i^{t_i}, \prod_{i=1}^{k_b} p_j^{l_j}) \stackrel{!}{=} 1$$

Thus those two products have no common divisor greater than 1.

Write m in terms of its prime factorization:

$$m = \prod_{r=1}^{k_r} p_r^{v_r} = m_1 \cdot m_2 \cdot \ldots \cdot m_{k_r}$$

The greatest common divisor of interest here yields:

$$\gcd(ab, m) = \gcd(\prod_{i=1}^{k_a} p_i^{t_i} \cdot \prod_{i=1}^{k_b} p_j^{l_j}, \prod_{r=1}^{k_r} p_r^{v_r})$$

The element m can have common divisors with either a or b, but the divisors are only common with one of the factors respectively, since $\gcd(a, b) = 1$.

We cross out all prime factors on both sides in the argument of $\gcd(ab, m)$ that are not common. On the left side of the argument, there will be $\gcd(a, m)$ common factors between a and m (first product) and $\gcd(b, m)$ common factors between b and m (second product). This provides the $\gcd(ab, m)$ factors in total.

Hence, we may write $\gcd(ab, m) = \gcd(a, m) \cdot \gcd(b, m)$ as a multiplicative product if $\gcd(a, b) = 1$.