# VU Discrete Mathematics

## Exercises for 18th November 2025

**31)** Which of the following mappings is well-defined?

a) $f : \mathbb{Z}_m \to \mathbb{Z}_m$, $\overline{x} \mapsto \overline{x^2}$,

b) $g : \mathbb{Z}_m \to \mathbb{Z}_m$, $\overline{x} \mapsto \overline{2^x}$.

**32)** Use the Chinese remainder theorem to solve the following system of congruence relations:

$$7x \equiv 8\ (24), \qquad 12x \equiv 4\ (28), \qquad 9x \equiv 3\ (15).$$

**33)** Let $(m, e) = (3233, 49)$ be a public RSA key. Compute the private key $(m, d)$.
Use the public key to encrypt the string „`COMPUTER`“. To this end, decompose the string into blocks of length 2 and, afterwards, apply the mapping `A` $\mapsto 01$, `B` $\mapsto 02, \ldots,$ `Z` $\mapsto 26$ letter by letter.

**34)** Let $(m, e)$ and $(m, d)$ be Bob's public and private RSA key, respectively. Suppose that Eve wants Bob to sign the message $A$, but Bob refuses to do so. But Eve gets Bob to sign another message $A'$ and uses the signed message $(A', \sigma')$. How can Eve use this idea to get message $A$ signed with Bob's signature?

Hint: Pick a random integer $R$ and consider the message $A' = R^e A \mod m$

**35)** Let $\varphi$ denote Euler's totient function. Prove that the identity

$$\varphi(m \cdot n) = \varphi(m)\varphi(n)\frac{\gcd(m,n)}{\varphi(\gcd(m,n))}$$

holds for all $m, n \in \mathbb{N}^+$.

**36)** Let $A_{d,n} = \{x \mid 1 \leq x \leq n \text{ and } \gcd(x,n) = d\}$

(a) Show that $\bigcup_{d|n} A_{d,n} = \{1, 2, \ldots, n\}$.

(b) Show that $|A_{d,n}| = |A_{1,n/d}|$. Hint: First show that $\gcd(k,n) = d$ if and only if $\gcd\left(\frac{k}{d}, \frac{n}{d}\right) = 1$ and use this to construct a bijection.

(c) Use (a) and (b) to show that

$$\sum_{d|n} \varphi(d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$$

where $\varphi$ denotes Euler's totient function.