Review Exercise Cryptography
- Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

06.03.2012

Solution to Exercise 5.

Claim: For $a, b \in \mathbb{N}$, it holds that $\varphi(ab) = \varphi(a)\varphi(b)$ if $\gcd(a, b) = 1$.

Remark: $\gcd(a, b) = 1 \Rightarrow \gcd(ab, m) = \gcd(a, m) \cdot \gcd(b, m)$.

It further holds that:

$$\begin{aligned} & \gcd(a, m) \cdot \gcd(b, m) = 1 \\ \Leftrightarrow \quad & \gcd(a, m) = 1 \wedge \gcd(b, m) = 1. \end{aligned}$$

The (multiplicative) totient (Euler-phi) function is:

$$\varphi(n) = |\mathbb{Z}_n^*| = |\{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}|.$$

Consider the following sets:

$$\begin{aligned} \mathbb{Z}_a^* &= \{x \in \mathbb{Z}_a \mid \gcd(x, a) = 1\}, & \varphi(a) &= |\mathbb{Z}_a^*|, \\ \mathbb{Z}_b^* &= \{x \in \mathbb{Z}_b \mid \gcd(x, b) = 1\}, & \varphi(b) &= |\mathbb{Z}_b^*|, \\ \mathbb{Z}_{ab}^* &= \{x \in \mathbb{Z}_{ab} \mid \gcd(x, ab) = 1\}, & \varphi(ab) &= |\mathbb{Z}_a^* \times \mathbb{Z}_b^*|. \end{aligned}$$

For $n = ab$, we may use the remark and compute:

$$\begin{aligned} \varphi(ab) &= |\mathbb{Z}_{ab}^*| \\ &= |\{x \in \mathbb{Z}_{ab} \mid \gcd(x, ab) = 1\}| \\ &= |\{x \in \mathbb{Z}_{ab} \mid \gcd(x, a) \cdot \gcd(x, b) = 1\}| \\ &= |\{x \in \mathbb{Z}_{ab} \mid \gcd(x, a) = 1 \wedge \gcd(x, b) = 1\}| \\ &\leq |\{x \in \mathbb{Z}_a \mid \gcd(x, a) = 1\}| \cdot |\{y \in \mathbb{Z}_b \mid \gcd(y, b) = 1\}| \\ &= |\mathbb{Z}_a^*| \cdot |\mathbb{Z}_b^*|. \end{aligned}$$

Since $\gcd(a, b) = 1$, we can use the *Chinese Remainder Theorem*:

$$\begin{aligned} f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b, \\ f(x) = (x \mod a, x \mod b). \end{aligned}$$

It follows that $f(x) = f(y) \Leftrightarrow x = y$ and $x \neq y \Leftrightarrow f(x) \neq f(y)$ hold and thus:

$$|\mathbb{Z}_{ab}^*| \geq |\mathbb{Z}_b^*| \cdot |\mathbb{Z}_b^*|.$$

Thus we can conclude that equality holds:

$$\varphi(ab) = |\mathbb{Z}_{ab}^*| = |\mathbb{Z}_a^*| \cdot |\mathbb{Z}_b^*| = \varphi(a)\varphi(b). \quad \square$$