Übungen zur Kryptologie 1 Wintersemester 05/06

Johannes Köbler/Olaf Beyersdorff

Übungsblatt 12

Aufgabe 45 (schriftlich, 10 Punkte)

a) Zeigen Sie, dass für jedes $a \in \mathbb{Z}_m^*$ ein $k > 0$ existiert mit $a^k \equiv 1 \pmod{m}$.

b) Sei nun $\mathrm{ord}_m(a) = k$. Zeigen Sie, dass die Menge

$$\{a^0 \bmod m, a^1 \bmod m, a^2 \bmod m, \ldots\}$$

eine Untergruppe von $\mathbb{Z}_m^*$ mit genau k Elementen bildet. Folgern Sie $k|\varphi(m)$.

c) Zeigen Sie $a^i \equiv_m a^j$ genau dann, wenn $i \equiv_{\mathrm{ord}_m(a)} j$.

Aufgabe 46 (mündlich)

Sei a ein Element von $\mathbb{Z}_m^*$ der Ordnung $\mathrm{ord}_m(a) = k$. Zeigen Sie

$$\mathrm{ord}_m(a^i) = \frac{k}{\mathrm{ggT}(k, i)}.$$

Aufgabe 47 (mündlich)

Seien $m_1, \ldots, m_{n+1} \in \mathbb{N}$. Sei $g_i =\mathrm{ggT}(m_i, m_{n+1})$, $i = 1, \ldots, n$. Zeigen Sie

$$\mathrm{kgV}(g_1, \ldots, g_n) = \mathrm{ggT}(\mathrm{kgV}(m_1, \ldots, m_n), m_{n+1}).$$

Aufgabe 48 (mündlich)

Zeigen Sie, dass das System von linearen Kongruenzen

$$x \equiv a_i \pmod{m_i} \quad i = 1, \ldots n$$

genau dann lösbar ist, wenn $\mathrm{ggT}(m_i, m_j)|(a_i - a_j)$ für alle Paare (i, j) mit $1 \leq i < j \leq n$. Zeigen Sie: wenn eine Lösung existiert, dann ist sie eindeutig modulo $\mathrm{kgV}(m_1, m_2, \ldots, m_n)$.

Hinweis: Führen Sie einen Induktionsbeweis und verwenden Sie Aufgabe 44.