RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt „Mathematische Grundlagen“ / 19. Oktober 2011

AUFGABE 1:
Sei G eine multiplikative Gruppe mit neutralem Element 1. Sei $a \in G$ beliebig. Zeigen Sie, dass $\langle a \rangle = \{a^1, a^2, \ldots, a^{\mathrm{ord}(a)}\}$ eine multiplikative Gruppe ist.

AUFGABE 2:
Seien $a, b, k, n, p \in \mathbb{N}$, p prim.
Zeigen Sie die folgenden Eigenschaften der Eulerschen φ-Funktion:

(a) $\varphi(p^k) = p^k(1 - \frac{1}{p})$

(b) $\varphi(ab) = \varphi(a)\varphi(b)$, falls $\gcd(a, b) = 1$.

Hinweis: Benutzen Sie den chinesischen Restesatz.

(c) $\varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$, falls $n = \prod_{p|n} p^{k_p}$ die Primfaktorzerlegung von n ist.

AUFGABE 3:
Sei G eine zyklische Gruppe. Zeigen Sie, dass es $\varphi(\mathrm{ord}(G))$ viele Generatoren in G gibt.

AUFGABE 4:
Zeigen Sie den verallgemeinerten Chinesischen Restsatz:
Seien $m_1, m_2, \ldots, m_n$ teilerfremde natürliche Zahlen. Es existiert genau eine Lösung $x \bmod m_1 m_2 \ldots m_n$ des Gleichungssystems

$$\left| \begin{array}{rcl} x & = & a_1 \bmod m_1 \\ x & = & a_2 \bmod m_2 \\ & \vdots & \\ x & = & a_n \bmod m_n \end{array} \right| .$$

Hinweis: Es gibt eine konstruktive Lösung in Analogie zu Satz 16 aus der Vorlesung. Alternativ kann man die Aussage per Induktionsbeweis zeigen.