



Hausübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 1 / 17. April 2008 / Abgabe bis 2. Mai 2008, 12 Uhr, in den Kasten
auf NA 02

AUFGABE 1 (4 Punkte):

Sei $n \in \mathbb{N}$. Zeigen Sie, dass gilt:

$$\mathbb{Z}_n \text{ Körper} \Leftrightarrow n \text{ prim.}$$

AUFGABE 2 (6 Punkte):

(a) Sei $N \in \mathbb{N}$ und $x \in \mathbb{Z}_N^*$ mit $\text{ord}(x) = k \in \mathbb{N}$. Zeigen Sie, dass mit $a, b \in \mathbb{Z}$ gilt:

$$x^a \equiv x^b \pmod{N} \Leftrightarrow a \equiv b \pmod{k}.$$

(b) Seien $a, b \in \mathbb{Z}$ mit $a \equiv b \pmod{\varphi(N)}$. Zeigen Sie, dass dann für alle $x \in \mathbb{Z}_N^*$ gilt:

$$x^a \equiv x^b \pmod{N}.$$

(c) Berechnen Sie $5^{2222211} \pmod{19}$.

(d) Bestimmen Sie das Inverse zu $5^{2222225} \pmod{19}$.

AUFGABE 3 (2 Punkte):

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

AUFGABE 4 (4 Punkte):

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 $\text{ggT}(a, b) = 1$.

(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 5 (4 Punkte):

Zeigen Sie den verallgemeinerten Chinesischen Restsatz:

Seien $m_1, m_2, \dots, m_n$ teilerfremde natürliche Zahlen. Es existiert genau eine Lösung $x \bmod m_1 m_2 \dots m_n$ des Gleichungssystems

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