Übungen zur Diskreten Mathematik (Lehramt GM/So)

WiSe 06/07 W. Huang und H.-J. Samaga **Blatt 7**

A: Präsenzaufgaben und Verständnisfragen

26. Mit dem öffentlichen Schlüssel ($n = 31,\ e = 13$) wird eine Nachricht m in den Geheimtext $c = me \bmod n$ verwandelt. Gesucht sind der Geheimtext zur Nachricht $m = 10$, der geheime Schlüssel d und die Nachricht zum Geheimtext $c = 11$.

27. Zur Eulerschen φ–Funktion: $\mathbb{N} \to \mathbb{N},\ \varphi(n) := |\{1 \le k \le n \mid \mathrm{ggT}(k, n) = 1\}|$:

a) Gesucht ist $\varphi(n)$ für $n = 1, 2, 3, 4, 5$.

b) Gesucht ist $\varphi(27)$.

c) Gesucht ist $\varphi(p^3)$ für eine Primzahl p.

28. Berechne möglichst einfach $274 \cdot 97 \bmod 91$ und $11^{17} \bmod 15$.

29. Wahr oder falsch? $2^5 \bmod 3 = 2^{5 \bmod 3} \bmod 3$.

B: Übungsaufgaben

20. Zur Eulerschen φ–Funktion: $\mathbb{N} \to \mathbb{N},\ \varphi(n) := |\{1 \le k \le n \mid \mathrm{ggT}(k, n) = 1\}|$:

a) Gesucht sind vier verschiedene $n \in \mathbb{N}$ mit $\varphi(n) = 6$.

b) Gesucht sind $\varphi(2048)$ und $\varphi(7^4)$.

c) Gesucht sind Primzahlen p und q mit $pq = 14803$ und $\varphi(pq) = 14560$.

21. Mit dem öffentlichen Schlüssel ($n = 65,\ e = 11$) wird eine Nachricht m in den Geheimtext $c = m^e \bmod n$ verwandelt.

a) Bestimme den Geheimtext c zur Nachricht $m = 2$.

b) Bestimme einen zugehörigen geheimen Schlüssel d.

c) Bestimme die Nachricht m zum Geheimtext $c = 2$.

22. Beweise oder widerlege:

a) $12^{512} - 1$ ist durch 4147 teilbar.

b) $28^{121} \bmod 143 = 28$.

Abgabe der Übungsaufgaben : Dienstag, 12. Dezember 06, in den Übungen.