Übungen zur Diskreten Mathematik (Master LAPSI)

WiSe 11/12 H.-J. Samaga und L. Selk **Blatt 9**

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 $c = 11$ (mit Probe).

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 $n = 4, 5, 33$.

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

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

d) Gesucht sind Primzahlen p und q mit $pq = 91$ und $\varphi(pq) = 72$.

28. Berechne möglichst einfach ohne Taschenrechner $(274 \cdot 97) \bmod 91$.
(Kann man im Kopf ausrechnen!)

29. Wahr oder falsch?

a) $2^5 \bmod 3 = 2^{5 \bmod 3} \bmod 3$.

b) $11^{16} \bmod 15 = 1$.

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 $pq = 45901$ und $\varphi(pq) = 45472$ (mit Herleitung).

21. Mit dem öffentlichen Schlüssel ($n = 13081$, $e = 173$) wird eine Nachricht m in den Geheimtext $c = me \bmod n$ verwandelt.

a) Bestimme den Geheimtext c zur Nachricht $m = 4301$.

b) Bestimme $\mathrm{ggT}\,(n, e)$.

c) Bestimme die Nachricht m zum Geheimtext $c = 1498$.

Abgabe der Übungsaufgaben : Dienstag, 20. Dezember, in den Übungen.