Übungen zur Diskreten Mathematik (Master LAPSI)

WiSe 11/12 H.-J. Samaga und L. Selk **Blatt 10**

A: Präsenzaufgaben und Verständnisfragen

30. Berechne ohne Einsatz eines Taschenrechners $(274 \cdot 97) \bmod 91$ und $6^9 \bmod 7$.
(Kann man jeweils im Kopf ausrechnen!)

31. Es geht in dieser Aufgabe um Modulares Rechnen. Ergänze die fehlenden Rechenschritte (mit Erklärung) und führe die Rechnung zu Ende:

$$82^{16} \bmod 20 \;=\; (4 \cdot 20 + 2)^{16} \bmod 20 \;=\; 2^{16} \bmod 20 \;=\; (16 \bmod 20)^4 \bmod 20 \;=\; \cdots$$

32. Der öffentliche Schlüssel zum RSA – Algorithmus sei $(n = 143, e = 37)$. Gesucht ist der geheime Schlüssel d.

33. Wahr oder falsch?

a) $2^5 \bmod 3 = 2^{5 \bmod 3} \bmod 3$ b) $11^{16} \bmod 15 = 1$.

B: Übungsaufgaben

22. Berechne ohne den Einsatz eines Taschenrechners mit Angabe der Rechenschritte
$54^{16} \bmod 55$, $3^{334} \bmod 26$, $2^{269} \bmod 19$, $3^{333} \bmod 15$

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

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

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

Bei dieser Aufgabe sind alle Hilfsmittel wie Taschenrechner, Einsatz von MuPad usw. erlaubt.

Abgabe der Übungsaufgaben: Dienstag, 10. Januar, in den Übungen.

C: Eine Knobelaufgabe für lange Weihnachtsabende:

Zerlege ein Quadrat in möglichst wenige spitzwinklige Dreiecke (jeder Winkel muss kleiner als 90 Grad sein.)

D: Eine Knobelaufgabe für Silvester:

In wieviele Teile kann man einen Berliner (gemeint ist das zu Silvester beliebte Naschwerk) mit n ebenen Schnitten maximal teilen? (Es sind Schnitte in beliebiger Richtung zugelassen.)
Wem das Problem zu räumlich ist: In wieviele Teile kann man eine (zweidimensionale) Pizza mit n geraden Schnitten maximal teilen? (Es sind Schnitte in beliebiger Richtung zugelassen.)

Wir wünschen allen Studierenden ein besinnliches Weihnachtsfest und ein erfolgreiches Jahr 2012!