6. Übungsblatt (19.12.2007)

1. Es sei p eine Primzahl.
   a) Zeigen Sie für $a \in \mathbb{Z}$, daß $a^2 \equiv 1 \bmod p$ genau dann, wenn $a \equiv 1 \bmod p$ oder wenn $a \equiv p-1 \bmod p$.
   b) Folgern Sie aus a), daß $(p-2)! \equiv 1 \bmod p$ und infolgedessen $(p-1)! \equiv p-1 \bmod p$. (Anmerkung: Letzteres ist der sogenannte Satz von Wilson.)

2. Zeigen Sie für $n = 561$, daß für alle $a \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$ stets $a^{n-1} \equiv 1 \bmod n$ gilt. (Anmerkung: Wenn eine Zahl $n > 1$ diese Bedingung erfüllt und wenn n nicht prim ist, so nennt man n eine Carmichael-Zahl.)
   (Hinweis: Primfaktorzerlegung von n, Übungsaufgabe 4.5, Kleiner Satz von Fermat und Chinesischer Restsatz)

3. Berechnen Sie mittels des Kleinen Satzes von Fermat und modularem Potenzieren in $\mathbb{Z}_{29}$ die (multiplikative) Inverse der Restklasse [18].

4. Unter Verwendung Ihres öffentlichen RSA-Schlüssels $(n, k) = (91, 5)$ senden wir Ihnen die folgende, verschlüsselte Nachricht: 68, 47, 78, 28, 62, 10, 39, 78, 70, 39, 78, 15.
   Bestimmen Sie Ihren privaten Schlüssel l, dechiffrieren Sie damit unsere Nachricht und interpretieren Sie anschließend die Ergebniswerte als ASCII-Code.

5. Für die Sicherheit des RSA-Verfahren ist es wichtig, daß auch die Zahl m geheim bleibt. Zeigen Sie: Wenn man das Produkt $n = pq$ kennt, wobei p und q zwei verschiedene, unbekannte Primzahlen sind, und wenn man auch die Zahl $m = (p-1)(q-1)$ kennt, dann kann man die beiden Primzahlen p und q berechnen.
   Berechnen Sie p und q, wenn $n = 6499$ und $m = 6336$ bekannt sind.

SCHÖNE WEIHNACHTSFEIERTAGE SOWIE -FERIEN UND ALLES GUTE FÜR 2008!

Die Übungsblätter gibt es auch online via

http://www.mathematik.uni-kassel.de/∼compmath/lehre/ds2/ds2.html