S. Wewers, S. Wilke

Kryptographie, SS 06

Lösung 2

Aufgabe 1.

Wegen $a_0 = a_1 = 1 > 0$ folgt induktiv $a_n > 0$ und damit auch $a_{n+1} = a_n + a_{n-1} > a_n$ für alle $n \in \mathbb{Z}$. Daraus folgt insbesondere $a_{n-1} = a_{n+1} \bmod a_n$. Für den ggT gilt somit: $\mathrm{ggT}(a_{n+1}, a_n) = \mathrm{ggT}(a_{n+1} \bmod a_n, a_n) = \mathrm{ggT}(a_{n-1}, a_n) = \mathrm{ggT}(a_n, a_{n-1})$. Induktiv folgt also $\mathrm{ggT}(a_{n+1}, a_n) = \mathrm{ggT}(a_1, a_0) = \mathrm{ggT}(1, 1) = 0$.

Aufgabe 2.

(a) Folgt direkt mit der Identität: $a^{n+1} - b^{n+1} = (a-b) \cdot \sum\limits_{k=0}^{n} a^k b^{n-k}$

(b) Zunächst gilt nach (a): $a^k - 1 = (a-1) \cdot \sum\limits_{j=0}^{k-1} a^j$. Falls $a > 2$, so ist $a - 1 > 1$. Wegen $k \geqslant 2$ ist $a^k > a$, also ist $1 < a - 1 < a^k - 1$ ein nicht-trivialer Teiler von $a^k - 1$; also ist $a^k - 1$ zusammengesetzt.
Sei nun $k = p \cdot q$ zusammengesetzt, $1 < p < k$, so gilt:

$$a^{pq} - 1 = (a^p - 1) \cdot \sum_{j=0}^{q-1} a^{pj}.$$

Nun ist aber $1 < a^p - 1 < a^k - 1$ ein nicht-trivialer Teiler von $a^k - 1$; also ist $a^k - 1$ zusammengesetzt.

Aufgabe 3.

Sei $n = p \cdot q$ zusammengesetzt mit $1 < p, q < n$. Zu zeigen: $n \mid (n-1)!$
Wir betrachten zwei Fälle:

(i) Sei $p \neq q$. Dann kommen p, q im Produkt $(n-1)! = \prod_{k=1}^{n-1} k$ vor; also gilt $p, q \mid (n-1)!$, also auch $n = p \cdot q \mid (n-1)!$

(ii) Sei $p = q$, dann ist $p > 2$. Damit gilt: $1 < 2p < p^2 = n$. Dann kommen aber p und $2p$ im Produkt $(n-1)! = \prod_{k=1}^{n-1} k$ vor; also gilt $2 \cdot n = 2p \cdot p \mid (n-1)!$; also insbesondere auch $n \mid (n-1)!$

Aufgabe 4.

(a) Es ist $10 \equiv 1 \pmod 9$, also ist $10^{99} \equiv 1^{99} \equiv 1 \pmod 9$ bzw. $10^{99} \bmod 9 = 1$. Analog ist $10 \equiv -1 \pmod{11}$ und daher $10^{99} \equiv (-1)^{99} \equiv -1 \equiv 10 \pmod{11}$ bzw. $10^{99} \bmod 11 = 10$.

(b) Es ist $7^2 \equiv 49 \equiv -1 \pmod{10}$, und damit ist $7^{1000} \equiv (7^2)^{500} \equiv (-1)^{500} \equiv 1 \pmod{10}$; also ist die letzte Ziffer eine 1.

(c) Zunächst ist $13^2 \equiv 169 \equiv -14 \pmod{61}$. Damit ist $13^3 \equiv -14 \cdot 13 \equiv -182 \equiv 1 \pmod{61}$. Also ist $13^{47} \equiv 13^2 \cdot (13^3)^{15} \equiv -14 \cdot 1^{15} \equiv -14 \equiv 47 \pmod{61}$, bzw. $13^{47} \bmod 61 = 47$.