

Aufgabe 10: (6 Punkte)

- (a) Aus dem Satz von Euler und der Voraussetzung folgt, dass $a^{\varphi(n)} = 1 \pmod n$ ist. Daher gilt auch:

$$a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} = 1 \pmod n$$

Also gilt $a^{\varphi(n)-1} = a^{-1} \pmod n$. Deshalb kann das inverse Element zu a auch mittels Exponentiation berechnet werden.

Beispiel: Berechnung von $b := 5^{-1} \pmod{26}$.

Es gilt $\varphi(26) = \varphi(2 \cdot 13) = (2-1) \cdot (13-1) = 12$. Es folgt: $b = 5^{12-1} \pmod{26}$.

$$\begin{aligned} 5^2 &= 25 = -1 \pmod{26} \\ 5^4 &= (-1)^2 = 1 \pmod{26} \\ 5^8 &= 1^2 = 1 \pmod{26} \\ b = 5^{11} &= 5^8 \cdot 5^2 \cdot 5 = 1 \cdot (-1) \cdot 5 = -5 = 21 \pmod{26} \end{aligned}$$

Probe: $5 \cdot 21 = 105 = 4 \cdot 26 + 1 = 1 \pmod{26}$ ✓

- (b) Es gilt der Satz von Euler: $a^{\varphi(n)} = 1 \pmod n$. Division des Exponenten b durch $\varphi(n)$ mit Rest ergibt $b = k \cdot \varphi(n) + r$, also $r = b \pmod{\varphi(n)}$. Es folgt:

$$a^b = a^{k \cdot \varphi(n) + r} = \underbrace{\left(a^{\varphi(n)}\right)^k}_{=1 \pmod n} \cdot a^r = a^r = a^{b \pmod{\varphi(n)}} \pmod n$$

Die Aussage gilt nicht für Zahlen mit $\text{ggT}(a, n) \neq 1$. Gegenbeispiel: $a = 2, b = 6, n = 8, \varphi(8) = 4$. Aber:

$$2^6 = 64 = 0 \neq 4 = 2^2 = 2^{6 \pmod 4} \pmod 8$$

- (c) Zu zeigen: $p \neq q$ prim, $a < n = pq \implies \forall k \in \mathbb{N} : a^{k\varphi(n)+1} \pmod n = a$

1. Fall: $\text{ggT}(a, n) = 1$, dann gilt:

$$a^{k \cdot \varphi(n) + 1} = \underbrace{\left(a^{\varphi(n)}\right)^k}_{=1 \pmod n} \cdot a = a \pmod n$$

2. Fall: $d = \text{ggT}(a, n) \neq 1$. Aus der Wahl von a und n folgt: $d = p \vee d = q$. Sei o.B.d.A. $d = p$ (Fall $d = q$ analog). Damit gilt $q \nmid a$ bzw. $\text{ggT}(a, q) = 1$ und deshalb:

$$a^{k \cdot \varphi(n) + 1} = a^{k \cdot (p-1)(q-1) + 1} = \underbrace{\left(a^{q-1}\right)^{k \cdot (p-1)}}_{=1 \pmod q} \cdot a = a \pmod q$$

Weiterhin ist $a^{k \cdot \varphi(n) + 1} = 0 \pmod p$ wegen $p|a$. Deshalb bleibt noch die Bestimmung einer Lösung der simultanen Kongruenzen:

$$\begin{aligned} x &= a \pmod q \\ x &= 0 \pmod p \end{aligned}$$

Eine Lösung des Systems ist $x = a$, die nach dem Chinesischen Restsatz modulo $n = pq$ eindeutig ist. Also gilt auch in diesem Fall $a^{k \cdot \varphi(n) + 1} = a \pmod n$. q.e.d.