

Musterlösung zum  
7. Übungsblatt zur Vorlesung  
Kryptologie

## Übung 1

$$\begin{aligned} \text{a) } \mathbb{Z}_{20}^{\times} &= \{1, 3, 7, 9, 11, 13, 17, 19\} \\ \mathbb{Z}_{30}^{\times} &= \{1, 7, 11, 13, 17, 19, 23, 29\} \end{aligned}$$

b) Aufzählen der Elemente ergibt:  $\phi(20) = |\mathbb{Z}_{20}^{\times}| = 8$  und  $\phi(30) = |\mathbb{Z}_{30}^{\times}| = 8$ , andererseits ergibt sich mit der Primfaktorzerlegung von  $20 = 2^2 \cdot 5$  und  $30 = 2 \cdot 3 \cdot 5$ :

$$\begin{aligned} \phi(20) &= 20 \cdot \frac{2-1}{2} \cdot \frac{5-1}{5} = 20 \cdot \frac{1}{2} \cdot \frac{4}{5} = 8, \\ \phi(30) &= 30 \cdot \frac{2-1}{2} \cdot \frac{3-1}{3} \cdot \frac{5-1}{5} = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8. \end{aligned}$$

## Übung 2

a) Da  $\gcd(5, 9) = 1$  ist, folgt:

$$5^{\phi(9)} = 5^6 = 1 \pmod{9}.$$

b) Da  $p = 23$  eine Primzahl ist, und  $a = 5 \in \mathbb{Z}_{23} \setminus \{0\}$ , folgt:

$$5^{23-1} = 5^{22} = 1 \pmod{23}.$$

## Übung 3

a) Da 17 eine Primzahl ist, folgt mit  $8^{16} = 1 \pmod{17}$ :

$$8^{50} = 8^{16 \cdot 3} \cdot 8^2 = 1 \cdot 8^2 = 64 = 13 \pmod{17}.$$

b) Da  $\gcd(8, 15) = 1$  und  $\phi(15) = 8$ , folgt:

$$8^{50} = 8^{8 \cdot 6} \cdot 8^2 = 1 \cdot 8^2 = 4 \pmod{15}.$$

c) Da  $\gcd(5, 18) = 1$  und  $\phi(18) = 6$ , folgt:

$$5^{36} = 5^{6 \cdot 6} = 1 \pmod{18}.$$

d) Da  $12 = 2^2 \cdot 3$  und  $18 = 2 \cdot 3^2$ , ist  $12^2$  durch 18 teilbar, also  $12^2 = 0 \pmod{18}$ . Damit gilt:

$$12^{19} = 12^{2+17} = 12^2 \cdot 12^{17} = 0 \cdot 12^{17} = 0 \pmod{18}.$$

e) Schnelle Exponentiation ergibt:

$$9^2 = 6 \pmod{15}$$

$$9^4 = 6^2 = 6 \pmod{15}$$

$$9^8 = 6^2 = 6 \pmod{15}$$

$$9^{16} = 6^2 = 6 \pmod{15}$$

$$\Rightarrow 9^{25} = 9^{16} \cdot 9^8 \cdot 9 = 6 \cdot 9 = 54 = 9 \pmod{15}.$$

## Übung 4

a) Die Zahlen, die nicht teilerfremd zu  $p \cdot q$  sind, sind die Null und alle Vielfache von  $p$  und  $q$ :  $kp$  und  $lq$ ,  $k, l \in \mathbb{N}$ . Für  $k \geq q$  und für  $l \geq p$  liegen  $kp$  und  $lq$  nicht mehr in  $\mathbb{Z}_{pq}$ . Für  $k < q$  und für  $l < p$  sind  $kp$  und  $lq$  alle verschieden, da  $p$  und  $q$  zwei verschiedene Primzahlen sind.

Damit ergibt sich:

$$\begin{aligned} \phi(pq) &= p \cdot q - |\{a \in \mathbb{Z}_{pq} \mid \gcd(a, pq) \neq 1\}| \\ &= p \cdot q - |\{0, p, 2p, 3p, \dots, (q-1)p, q, 2q, 3q, \dots, (p-1)q\}| \\ &= p \cdot q - (1 + (q-1) + (p-1)) \\ &= p \cdot q - q - p + 1 \\ &= (p-1)(q-1). \end{aligned}$$

b) 1.  $\phi(p^k) = p^k \cdot \frac{(p-1)}{p} = p^{k-1} \cdot (p-1).$

2. Die Zahlen, die nicht teilerfremd zu  $p^k$  sind, sind die Null und alle Vielfache von  $p$ :  $kp$ ,  $k \in \mathbb{N}$ . Für  $k \geq p^{k-1}$  liegt  $kp$  nicht mehr in  $\mathbb{Z}_{p^k}$ . Damit ergibt sich:

$$\begin{aligned} \phi(p^k) &= p^k - |\{a \in \mathbb{Z}_{p^k} \mid \gcd(a, p^k) \neq 1\}| \\ &= p^k - |\{0, p, 2p, 3p, \dots, (p^{k-1} - 1) \cdot p\}| \\ &= p^k - p^{k-1} \\ &= p^{k-1} \cdot (p-1). \end{aligned}$$