

## 7. Übungsblatt zur Vorlesung Kryptologie

### Übung 1

- Welche Elemente hat  $\mathbb{Z}_{20}^\times$  bzw.  $\mathbb{Z}_{30}^\times$ ?
- Bestimmen Sie  $\phi(20)$  und  $\phi(30)$  einerseits durch Abzählen der Elemente und andererseits mit Hilfe von Satz 7.3 des Skripts.

### Übung 2

- Was besagt der Satz von Euler für  $m = 9$  und  $a = 5$ ?
- Was besagt der kleine Satz von Fermat für  $p = 23$  und  $a = 5$ ?

### Übung 3

Bestimmen Sie die folgenden Werte. Nutzen Sie - wo möglich - den Satz von Euler bzw. den kleinen Satz von Fermat!

- $8^{50} \bmod 17$ ,
- $8^{50} \bmod 15$ ,
- $5^{36} \bmod 18$ ,
- $12^{19} \bmod 18$ ,
- $9^{25} \bmod 15$ .

### Übung 4

- Seien  $p$  und  $q$  zwei verschiedene Primzahlen.  
Zeigen Sie  $\phi(pq) = (p-1) \cdot (q-1)$ , indem Sie die Anzahl der Elemente aus  $\mathbb{Z}_{pq}$  bestimmen, die *nicht* in  $\mathbb{Z}_{pq}^\times$  liegen.
- Bestimmen Sie  $\phi(p^k)$  mit einer Primzahl  $p$  und  $k \in \mathbb{N}$ , einerseits indem Sie Satz 7.3 anwenden und andererseits, indem Sie (auf elementarem Weg) die Anzahl der Elemente aus  $\mathbb{Z}_{p^k}^\times$  bestimmen.