

Übungen zur Vorlesung Kryptographie

## Blatt 2

**Aufgabe 5: (Einheitengruppen)**

- (a) Was sind die Elemente von  $Z_7^*$ ? Was sind jeweils ihre inversen Elemente? Was ist der Wert von  $\varphi(7)$ ?  
 (b) Was sind die Elemente von  $Z_{30}^*$ ? Was sind je ihre inversen Elemente? Was ist der Wert von  $\varphi(30)$ ?  
 (c) Bestimmen Sie alle Untergruppen von  $Z_7$  und  $Z_7^*$ .

**Aufgabe 6: (Mehr zu Einheitengruppen)***Diese Aufgabe bitte ohne Computer lösen!*

- (a) Berechnen Sie das inverse Element von 168 in  $Z_{503}^*$  und das inverse Element von 144 in  $Z_{233}^*$  von Hand mittels des erweiterten euklidischen Algorithmus.  
 (b) Bestimmen Sie alle  $n \in \mathbb{N}$ , so dass die jeweilige Einheitengruppe  $Z_n^*$  genau sechs Elemente hat. Begründen Sie, warum das wirklich alle sind!

**Aufgabe 7: (Euler-Fermat benutzen)***Diese Aufgabe bitte ohne Computer lösen!*

- (a) Berechnen Sie  $3^{1000003} \bmod 101$  von Hand.  
 (b) Berechnen Sie die letzten beiden Dezimalziffern von  $23^{1000005}$  von Hand.  
 (c) Zeigen Sie, dass  $a^p - a$  immer durch  $p$  teilbar ist, wenn  $p$  eine Primzahl ist und  $a \in \mathbb{N}$ .

**Aufgabe 8: (Gruppen, Ringe, Körper)**

- (a) Welche der folgenden fünf Objekte sind Gruppen, welche nicht? Falls nein, warum nicht? Falls ja, was ist jeweils das neutrale Element, und was das inverse Element zu einem Element  $x$ ?

$$(\mathbb{R}^+, \cdot), (\{-1, 0, 1\}, \cdot), (\{-1, 1\}, \cdot), \left(\left\{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right\}, +\right), \left(\left\{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right\}, \cdot\right).$$

Dabei ist  $\mathbb{R}^+$  die Menge der positiven reellen Zahlen ohne Null.

- (b) Welche der folgenden fünf Objekte sind Ringe, welche nicht? Und welche sind Körper, welche nicht? Falls nein, warum nicht?

$$(Z_6, +, \cdot), (Z_7, +, \cdot), (\{0, 1\}, \text{XOR}, \text{AND}), (\{0, 1\}, \text{AND}, \text{XOR}), \left(\left\{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right\}, +, \cdot\right)$$

---

Abgabe bis Mittwoch 22.4.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann    pbraukmann@techfak.de  
 Jonas Friemel        jfriemel+krypto@techfak.de