

## Übungsblatt 1

### Aufgabe 1

*mündlich*

Der Kryptotext **BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD** wurde durch eine additive Chiffre generiert. Entschlüsseln Sie ihn.

### Aufgabe 2

 Berechnen Sie:

*mündlich*

(a)  $\text{ggT}(26, 81)$ ,

(b)  $26^{-1} \bmod 81$ .

### Aufgabe 3

*mündlich*

Bestimmen Sie alle involutorischen Schlüssel  $k$  (d. h.  $E_k$  ist involutorisch) der additiven Chiffre über einem Alphabet mit  $m = 26$  Zeichen.

### Aufgabe 4

*mündlich*

Bestimmen Sie die Schlüsselzahl der affinen Chiffre für die Modulwerte  $m = 30, 100$  und  $1225$ .

### Aufgabe 5

*mündlich*

Bestimmen Sie die Anzahl der Lösungen  $x \in \{0, \dots, m-1\}$  der Kongruenzgleichung

$$ax \equiv_m b$$

in Abhängigkeit von  $\text{ggT}(a, m)$  und  $b$ . Betrachten Sie zunächst den Fall  $b = 0$ .

### Aufgabe 6

 Zeigen Sie.

**10 Punkte**

Seien  $a, b \in \mathbb{Z}$  mit  $b \neq 0$ . Dann gibt es genau ein Paar  $d, r$  von ganzen Zahlen mit  $a = bd + r$  und  $0 \leq r < |b|$ .