Übungsblatt 1

Abgabe für die mündlichen Aufgaben bis 27. 04. 2020 und für die schriftliche Aufgabe bis 04. 05. 2020

Aufgabe 1 ***mündlich***
Der Kryptotext `BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD` wurde durch eine additive Chiffre generiert. Entschlüsseln Sie ihn.

Aufgabe 2 Berechnen Sie: ***mündlich***

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

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

Aufgabe 3 ***mündlich***
Bestimmen Sie alle echt involutorischen Schlüssel k (d. h. E_k ist echt involutorisch) der additiven Chiffre über einem Alphabet mit $m = 26$ Zeichen. Wieviele solche Schlüssel gibt es in Abhängigkeit von m?

Aufgabe 4 ***mündlich***
Bestimmen Sie die Schlüsselzahl der affinen Chiffre für die Modulwerte $m = 30, 100$ und 343.

Aufgabe 5 ***mündlich***
Bestimmen Sie die Anzahl der Lösungen $x \in \{0, \ldots, m-1\}$ der Kongruenzgleichung

$$ax \equiv_m b$$

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

Aufgabe 6 ***mündlich***
Sei $(R, +, \cdot, 0, 1)$ ein Ring mit Eins. Zeigen Sie, dass die Multiplikation auf der Menge $R^* = \{a \in R \mid \exists b \in R : ab = 1 = ba\}$ aller Einheiten von R eine Gruppe $(R^*, \cdot, 1)$ bildet.

Aufgabe 7 ***mündlich***
Ver- und entschlüsseln Sie den Text `DREIEINS` mittels einer

(a) additiven Chiffre mit dem Schlüssel $k = 13$,

(b) affinen Chiffre mit dem Schlüssel $k = (17, 6)$.

Aufgabe 8 ***mündlich***
Sei $k = (b, c)$ ein Schlüssel der affinen Chiffre mit m Zeichen. Zeigen Sie, dass E_k genau dann involutorisch ist, wenn $b^2 \equiv_m 1$ und $c(b+1) \equiv_m 0$ gilt.

Aufgabe 9 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 $0 \leq r < |b|$.