Übungsblatt 1

Abgabe der schriftlichen Lösungen bis 05.05.2022, 24 Uhr

Aufgabe 1 ***mündlich***

Der Kryptotext `beeakfydjxuqyhyjiqryhtyjiqfbqduyjiikfuhcqd` wurde durch eine additive Chiffre über dem lateinischen Alphabet 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 $m = 26$, 30, 100, 343 und 1225.

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` über dem lateinischen Alphabet mittels einer

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

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

Aufgabe 8 ***mündlich***

(a) 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.

(b) Bestimmen Sie alle involutorischen und alle echt involutorischen Schlüssel der affinen Chiffre für $m = 2, 3, 5, 13, 15, 26$.

Aufgabe 9 ***10 Punkte***

(a) Zeigen Sie, dass es für jedes Zahlenpaar $a, b \in \mathbb{Z}$ mit $b \neq 0$ genau ein Paar $d, r \in \mathbb{Z}$ mit $a = bd + r$ und $0 \leq r < |b|$ gibt.

(b) Bestimmen Sie für primes $p \geq 2$ alle Lösungen der Kongruenz $x^2 \equiv_p 1$.