Übungsblatt 1

Abgabe der schriftlichen Lösungen am 2. 11. 2017 bis 13.10 Uhr

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 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 $x \in \{0, \ldots, m-1\}$ der Kongruenzgleichung

$$ax \equiv_m b$$

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

Aufgabe 6 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 $0 \leq r < |b|$.

Aufgabe 7 ***mündlich, rechenintensiv***
(*keine Besprechung in der Übung; Fragen über Moodle*) Bereiten Sie in der Programmiersprache, die Sie im Semester nutzen wollen, Algorithmen für zunächst folgende Aufgabenstellungen vor: Multiplikation, Addition und Inversenbildung in Restklassenringen sowie Matrixmultiplikation und Addition über Restklassenringen; naive Primzahltests für kleine Zahlen inkl. Faktorisierung; Sie dürfen bereits fertige Pakete nutzen, sollten aber wissen, wie sie diese notfalls erweitern können (z.B. um Determinantenberechnung, Polynome über $\mathbb{Z}_p$, p prim).