UNIVERSITÄT DES SAARLANDES

Fachrichtung Mathematik
Prof. Dr. Simon Brandhorst
Dr. Tobias Columbus

Elementare Zahlentheorie

Übungsblatt 12

Aufgabe 1 (2 Punkte)
Es seien $N \in \mathbb{N}$ sowie $a_1, a_2 \in (\mathbb{Z}/N\mathbb{Z})^\times$ und $b_1, b_2 \in \mathbb{Z}/N\mathbb{Z}$. Zeigen Sie, dass die Hintereinanderausführung der zwei affinen Verschlüsselungsfunktionen $E_1(x) = a_1x + b_1$ und $E_2(x) = a_2x + b_2$ wieder eine affine Verschlüsselungsfunktion ist.

In den folgenden beiden Aufgaben identifizieren wir Buchstaben A, B, C, ... mit ihrer Position im Alphabet modulo 26. So haben wir zum Beispiel die Entsprechungen $A \leftrightarrow 0$, $B \leftrightarrow 1$ und $C \leftrightarrow 2$.

Aufgabe 2 (2 Punkte)
Die Nachricht „`OXQABMFDM`“ wurde mit einer Caesar-Chiffre verschlüsselt. Bestimmen Sie den Klartext unter der Annahme, dass „`A`“ der häufigste Buchstabe in der ursprünglichen Nachricht ist.

Aufgabe 3 (4 Punkte)
Die Nachricht „`NIIP IOJB COJOQS`“ wurde mit einer affinen Chiffre $E\colon \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$ verschlüsselt.

(a) Entschlüsseln Sie die Nachricht mit Hilfe der Information, dass $E(\mathtt{S}) = \mathtt{I}$ und $E(\mathtt{H}) = \mathtt{J}$.

(b) Hätten Sie die Nachricht auch mit Hilfe der Information, dass $E(\mathtt{S}) = \mathtt{I}$ und $E(\mathtt{M}) = \mathtt{S}$ entschlüsseln können?

Aufgabe 4 (4 Punkte)
Es sei $n \in \mathbb{N}$. Ein Element $\zeta \in (\mathbb{Z}/n\mathbb{Z})^\times$ heißt *primitive Wurzel modulo* n, wenn es für alle $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ ein $k \in \mathbb{N}$ gibt, so dass $\zeta^k = a$. Es sei nun ζ eine solche primitive Wurzel modulo n.

(a) Zeigen Sie, dass $\zeta^k = \zeta^l$ genau dann, wenn $k \equiv l \mod \varphi(n)$.

(b) Zeigen Sie, dass ζ^m genau dann eine primitive Wurzel modulo n ist, wenn $\mathrm{ggT}(m, \varphi(n)) = 1$.

(c) Zeigen Sie, dass es modulo n entweder keine oder genau $\varphi(\varphi(n))$ primitive Wurzeln gibt.

Aufgabe 5 (4 Punkte)
Es sei p eine ungerade Primzahl.

(a) Zeigen Sie, dass es eine primitive Wurzel in $\mathbb{Z}/2p\mathbb{Z}$ gibt.

(b) Bestimmen Sie für $p = 19$ explizit eine primitive Wurzel modulo $38 = 2 \cdot 19$.

Abgabe bis spätestens Montag, den 01. 07. 2019, um 12:00 Uhr. Werfen Sie Ihre Lösungsvorschläge in die dafür vorgesehenen Einwurfkästen vor dem Zeichensaal in Gebäude E 2 5. Abgabe zu zweit ist möglich. Bitte geben Sie Ihren Namen, Ihre Matrikelnummer und Ihre Übungsgruppe and!