Aufgaben

Aufgabe 1. Sind die folgenden Gruppen G zyklisch ? Wenn ja, berechnen Sie eine primitive Wurzel, wenn nein, berechnen Sie $\exp(G)$.

a. $(\mathbb{Z}/25\mathbb{Z})^\times$,

b. $(\mathbb{Z}/50\mathbb{Z})^\times$,

c. $(\mathbb{Z}/33\mathbb{Z})^\times$,

d. $(\mathbb{Z}/1024\mathbb{Z})^\times$.

Aufgabe 2. Es sei $p \neq 2$ eine Primzahl. Zeigen Sie :

a.
$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0,$$

b.
$$\sum_{k=1}^{p-1} k \left(\frac{k}{p}\right) = 0,$$

falls $p \equiv 1 \bmod 4$.

Folgende Übungen nutzen das RSA-Verfahren (§7 der Vorlesung) und die unten abgedruckte Tabelle, die jedem Buchstaben eine zweistellige Zahl zuordnet.

Aufgabe 3. Diese Übung sollte am besten zu zweit (A und B) gemacht werden.

a. A : Berechnen Sie für die Primzahlen 59 und 97 einen öffentlichen und den zugehörigen privaten Schlüssel. Geben Sie B den öffentlichen Schlüssel.

b. B : Wählen Sie ein Wort mit 4 Buchstaben und wandeln sie es in zwei 4-stellige Zahlen um.

c. B : Verschlüssen Sie diese Zahlen mit dem öffentlischen Schlüssel und geben Sie A die verschlüsselte Nachricht.

d. A : Entschlüssen Sie die Nachricht von B.

Aufgabe 4. Dr. N hat Dr. V das Geheimnis für einen großen Erfolg in der EZT-Klausur gesendet :

$$1385,\ 1550,\ 670.$$

Es war natürlich durch RSA verschlüsselt, und zwar mit dem öffentlichen Schlüssel $(2623, 11)$. Können Sie es hacken ?

Die Blätter sollen bis Donnerstag, den 27.11. um 14.15 Uhr in die dafür vorgesehenen Einwurfkästen im Foyer des Mathematischen Instituts abgegeben werden.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35