Mathematisches Institut
Georg-August-Universität Göttingen
Prof. Dr. E. Viada, Dr. V. Cantoral

Lösungen zu Übungsblatt 12.

Aufgabe 1 (10 Punkte)**.** Bestimmen Sie alle erzeugenden Elemente von $(\mathbb{Z}/17\mathbb{Z})^*$ und von $(\mathbb{Z}/19\mathbb{Z})^*$.

Lösung zu Aufgabe 1. (4 Punkte) Die multiplikative Gruppen $(\mathbb{Z}/17\mathbb{Z})^*$ und $(\mathbb{Z}/19\mathbb{Z})^*$ sind zyklischen. Insbesonderes gibt es $\varphi(17-1) = 8$ erzeugende Elemente in $(\mathbb{Z}/17\mathbb{Z})^*$ und $\varphi(19-1) = 6$ erzeugende Elemente in $(\mathbb{Z}/19\mathbb{Z})^*$. Welche sind es? Wir testen modulo 17 und 19:

- (3 Punkte) Da wir wissen, dass es genau 8 euzeugende Elemente in $(\mathbb{Z}/17\mathbb{Z})^*$ gibt, haben wir mit $\{\bar{3}, \bar{5}, \bar{6}, \bar{7}, \overline{10}, \overline{11}, \overline{12}, \overline{14}\}$ alle erzeugende Elemente von $(\mathbb{Z}/17\mathbb{Z})^*$ gefunden.
- (3 Punkte) Da wir wissen, dass es genau 6 euzeugende Elemente in $(\mathbb{Z}/19\mathbb{Z})^*$ gibt, haben wir mit $\{\bar{2}, \bar{3}, \overline{10}, \overline{13}, \overline{14}, \overline{15}\}$ alle erzeugende Elemente von $(\mathbb{Z}/19\mathbb{Z})^*$ gefunden.

Aufgabe 2 (10 Punkte)**.** Was lässt sich jeweils mithilfe der gegebenen Kongruenz und des kleinen Fermatschen Satzes über die Primalität des Modulus sagen?

(i) $5^{277} \equiv 5 \mod 277$ und $17^{277} \equiv 17 \mod 277$

(ii) $2^{1105} \equiv 2 \mod 1105$, $3^{1104} \equiv 1 \mod 1105$ und $7^{1105} \equiv 7 \mod 1105$

(iii) $4^{8911} \equiv 4 \mod 8911$, $11^{8891} \equiv 11 \mod 8911$ und $134^{8910} \equiv 134 \mod 8911$

Lösung zu Aufgabe 2. Hierfür brauchen wir nur zu wissen:

- Gilt $a^n \equiv a \mod n$ bzw. $a^{n1} \equiv 1 \mod n$, so ist n Pseodoprim bzgl. a.
- Gibt es eine Zahl a, sodass n nicht Pseodoprim bzgl. a ist, so ist n nicht prim.

Damit können wir die Aussagen direkt aus den Gleichungen ablesen:

(i) (2 Punkte) 277 ist Pseodoprim bzgl. 5 und bzgl. 17. (Wir wissen nicht, ob 277 prim ist.)

(ii) (4 Punkte) 1105 ist Pseodoprim bzgl. 2, 3 und 7. (Wir wissen nicht, ob 1105 prim ist.)

(iii) (4 Punkte) 8911 ist Pseodoprim bzgl. 4 und 11, jedoch nicht Pseodoprim bzgl. 134. Insbesondere ist 8911 nicht prim.

Aufgabe 3 (10 Punkte)**.** Die folgende Chiffre wurde mit einer Vigenère-Verschlüsselung verschlüsselt. Folgen Sie dem Beispiel 6.7 auf Seite 166 und verwenden Sie die Schlüssel "krypt", um den Originaltext zu finden.

OAD CUEZDCUEAJ YME VHU EZWUYATF CUL RARIYYKBXUQLDD

Lösung zu Aufgabe 3. Als Schlüssel wählen wir krypt, was dem Element $(\overline{11}, \overline{18}, \overline{25}, \overline{16}, \overline{20})$ entspricht. Erhalten wir nun die Nachricht

$$OADCUEZDCUEAJYMEVHUEZWUYATFCULRARIYYKBXUQLDD$$

und kennen wir den Schlüssel "krypt", so können wir auf gleiche Weise den Klartext erzeugen: Wir fassen die Buchstabenfolgen OADCUEZDCUEAJYMEVHUEZWUYATFCULRARIYYKBXUQLDD und kryptkryptkryptkryptkryptkryptkryptkryptkryptkryp als Elemente in $(\mathbb{Z}/26\mathbb{Z})^{44}$ auf und berechnen

$$\begin{aligned} &OADCUEZDCUEAJYMEVHUEZWUYATFCULRARIYYKBXUQLDD \\ &\quad -kryptkryptkryptkryptkryptkryptkryptkryptkryptkryp \\ &\quad = diemathematikistdiekoeniginderwissenschaften \end{aligned}$$

Daher lautet der Originaltext (10 Punkte):

Aufgabe 4 (10 Punkte)**.** Umgekehrt kodieren Sie mit dem Schlüssel „dima“ den folgenden Satz:

Wir muessen wissen, wir werden wissen.

Wo finden wir dieses Zitat in Göttingen?

Lösung zu Aufgabe 4. Zuerst identifizieren wir jeden Buchstaben des Alphabets mit einer Äquivalenzklasse in $\mathbb{Z}/26\mathbb{Z}$.

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Als Schlüssel wählen wir "dima", was dem Element $(\bar{4}, \bar{9}, \overline{13}, \bar{1}) \in (\mathbb{Z}/26\mathbb{Z})^4$ entspricht (die Schlüssellänge ist 4). Dann haben wir Folgendes

$$\begin{array}{c} \text{Schlüssel: } d\,i\,m\,a\;d\,i\,m\,a\,d\,i\,m\,a\,d\,i\,m\,a\,d\,i\,m\,a\,d\,i\,m\,a\,d\,i\,m \\ \text{Klartext: } w\,i\,r\,m\,u\,e\,s\,s\,e\,n\,w\,i\,s\,s\,e\,n\;w\,i\,r\;w\,e\,r\;d\,e\,n\,w\,i\,s\,s\,e\,n \\ \hline \text{Chiffre: } a\,r\,e\,n\,y\,n\,f\,t\,i\,w\,j\,j\,w\,b\,r\,o\,a\,r\,e\,x\,i\,a\,q\,f\,r\,f\,v\,t\,w\,n\,a \end{array}$$

Zum Beispiel erhalten wir den Buchstaben a, der der Äquivalenzklasse $\bar{1}$ entspricht, indem wir die Äquivalenzklasse von w, die $\overline{23}$ ist, mit der von d, die $\bar{4}$ ist, addieren. Als Ergebnis erhalten wir $\overline{27}$, was mit 1 modulo 26 kongruent ist. Wir erhalten daher den folgenden Satz (10 Punkte):

Are nynftiw jjwbro are xiaqfr fvtwna.

Das Motto "Wir müssen wissen, wir werden wissen."findet sich auch als Epitaph auf Hilbert Grabstein.