Grundlagen und diskrete Mathematik
Übung 7

Abgabe: Keine Abgabe

Aufgabe 1

Zeichnen Sie die Verknüpfungstabellen der Multiplikation in $\mathbb{Z}/8$ und $\mathbb{Z}/7$. Diskutieren Sie auffällige unterschiede?

Lösung:

$\mathbb{Z}/7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$\mathbb{Z}/8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

In $\mathbb{Z}/7$ habe alle von $\bar{0}$ verschiedenen Elemente multiplikative Inverse (in jeder Spalte/Zeile ausser der 0-ten kommen Einsen vor). In $\mathbb{Z}/8$ ist dies nicht der Fall.

Aufgabe 2

Bestimmen Sie das multiplikative Inverse von $\overline{123}$ in $\mathbb{Z}/3211$.

Lösung: Euklidischer Algorithmus:

$$\begin{aligned} 3211 &= 26 \cdot 123 + 13 \\ 123 &= 9 \cdot 13 + 6 \\ 13 &= 2 \cdot 6 + 1 \end{aligned}$$

Rückwärts Einsetzen ergibt:

$$\begin{aligned} 1 &= 13 - 2 \cdot 6 \\ &= (3211 - 26 \cdot 123) - 2(123 - 9 \cdot 13) \\ &= (3211 - 26 \cdot 123) - 2(123 - 9 \cdot (3211 - 26 \cdot 123)) \\ &= 19 \cdot 3211 - 496 \cdot 123 \end{aligned}$$

somit ist das multiplikative Inverse von $\overline{123}$ in $\mathbb{Z}/3211$ die Restklasse $\overline{-496} = \overline{2715}$.

Aufgabe 3

Ihr Freund Karl hat die Buchstaben des Alphabets und weitere Zeichen nach folgendem Schema als Restklassen in $\mathbb{Z}/43$ codiert.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	:	-	(	)	.	,	0	1	2	3	4	5	6	7	8	9	a	b	c

20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u

38	39	40	41	42
v	w	x	y	z

Karl hat Ihnen eine Nachricht gesendet (siehe auch OLAT):

.-:pxc6p:zz: y46zv.,r)6.-:pxc6v.6n6svp,v: ny6pun)np,r)6v 6,ur6.,n)6,)rx6zrqvn6s)n puv.rb6sv).,6-:),)n4rq6o46yr: n)q6 vz:46v 6,ur6:)vtv ny6.,n)6,)rx6.r)vr.c6.-:px6ny.:6n–rn).6v 6,ur6n vzn,rq6.,n)6,)rx6.r)vr.c6n6,2:8-n),6r-v.:qr6:s6.,n)6,)rx76,ur6 r3,6tr r)n,v: c6rvtu,6:s6,ur6.,n)6,)rx6srn,0)r6svyz.c6n q6 0zr):0.6.,n)6,)rx6o::x.c6p:zvp.c6n q61vqr:6tnzr.b6v 6,ur6fddm6svyz6.,n)6,)rx6n q6v,.6fdeg6.r(0ry6.,n)6,)rx6v ,:6qn)x r..c6 vz:46)r-)v.rq6uv.6):yr6ny: t.vqr65npun)46(0v ,:c62u:6-yn4rq6n64:0 tr)c6ny,r) n,r80 v1r).r61r).v: 6:s6,ur6pun)np,r)c6n q6wnp:o6x:tn 6-yn4v t6.-:px6n.6n6puvyqb6.-:px6.r)1r.6no:n)q6,ur6.,n).uv-6r ,r)-)v.rc6n.6.pvr pr6:ssvpr)6n q6sv).,6:ssvpr)c6n q6yn,r)6n.6p:zzn qv t6:ssvpr)6:s6,2:6v,r)n,v: .6:s6,ur61r..ryb6.-:px.6zv3rq6u0zn 810ypn 6ur)v,ntr6.r)1r.6n.6n 6vz-:),n ,6-y:,6ryrzr ,6v 6zn 46:s6,ur6pun)np,r).6n–rn)n pr.b6ny: t62v,u6pn-,nv 6wnzr.6,b6xv)x6n q6q)b6yr: n)q6zpp:4c6ur6v.6: r6:s6,ur6,u)rr6pr ,)ny6pun)np,r).6v 6,ur6:)vtv ny6.,n)6,)rx6.r)vr.6n q6v,.6svyz.b6ns,r)6)r,v)v t6s):z6.,n)syrr,c6.-:px6.r)1r.6n.6n6srqr)n,v: 6nzon..nq:)c6p:,)vo0,v t6,:2n)q6,ur6qr,r ,r6or,2rr 6,ur6srqr)n,v: 6n q6,ur6xyv t: 6rz-v)rb6v 6uv.6yn,r)64rn).c6ur6.r)1r.6n.6srqr)n,v: 6nzon..nq:)6,:6,ur6):z0yn 6rz-v)r6n q6orp:zr.6v 1:y1rq6v 6,ur6vyy8sn,rq6n„rz-,6,:6.n1r6):z0y0.6s):z6n6.0-r) :1nb

Karl hat die Codierungsfunktion $c : \mathbb{Z}/43 \to \mathbb{Z}/43$ mit $c(x) = x + \overline{13}$ verwendet.

(a) Entschlüsseln Sie die Nachricht.

(b) Geben Sie die "Decodierungsfunktion" an.

(c) Ist es möglich die Nachricht durch mehrfache Anwendung der Codierungsfunktion zu decodieren? Begründen Sie Ihre Antwort.

Lösung:

b) $d : \mathbb{Z}/43 \to \mathbb{Z}/43$ mit $d(x) = x + \overline{30}$.

c) Ja, wenn man die Funktion c zum Beispiel $43 \cdot 13 = 559$ mal anwendet, bekommt man die ursprüngliche Nachricht.

Aufgabe 4

Zeigen Sie, dass folgende Aussagen für $n, x > 0$ äquivalent sind:

- $\bar{x}$ ist invertierbar in $\mathbb{Z}/n$.
- $ggT(x, n) = 1$.

Lösung:

$\Rightarrow$: Ist $\bar{x}$ in $\mathbb{Z}/n$ invertierbar, dann gibt es ein $y \in \{1, .., n-1\}$ mit der Eigenschaft $xy = 1 \mod n$. Es gilt somit:

$$\begin{aligned} & n|xy-1 \\ & \Rightarrow nk = xy - 1 && \text{für geeignetes } k \in \mathbb{Z} \\ & \Rightarrow 1 = xy - nk && \text{für geeignetes } k \in \mathbb{Z} \\ & \Rightarrow ggT(x,n) = 1 \end{aligned}$$

$\Leftarrow$: Ist $ggT(x,n) = 1$, dann gibt es Zahlen $a, b \in \mathbb{Z}$ mit $ax + bn = 1$. Somit gilt in $\mathbb{Z}/n$

$$\bar{1} = \overline{ax + bn} = \bar{a} \cdot \bar{x}.$$

Somit ist $\bar{a}$ in $\mathbb{Z}/n$ das Inverse von x.

Aufgabe 5

Lösen Sie folgendes System simultaner Kongruenzen mit dem in der Vorlesung behandelten Algorithmus. Geben Sie die gesamte Lösungsmenge an.

$$\begin{aligned} x &= 4 \mod 9 \\ x &= 5 \mod 11 \\ x &= 2 \mod 5 \end{aligned}$$

Lösung: Wir betrachten zuerst die Gleichungen

$$\begin{aligned} x &= 5 \mod 11 \\ x &= 2 \mod 5 \end{aligned}$$

Wir erhalten (notfalls mit dem euklidischen Algorithmus) $1 = 11 - 2 \cdot 5$ und somit mit dem Algorithmus aus der Vorlesung eine Lösung $x = 11 \cdot 2 - 2 \cdot 5 \cdot 5 = -28$. Wegen $-28 = 27 \mod 55$ erhalten wir als Gleichungssystem:

$$\begin{aligned} x &= 27 \mod 55 \\ x &= 4 \mod 9. \end{aligned}$$

Wir erhalten (notfalls mit dem euklidischen Algorithmus) $1 = 55 - 6 \cdot 9$ und somit mit dem Algorithmus aus der Vorlesung eine Lösung $x = 55 \cdot 4 - 6 \cdot 9 \cdot 27 = -1238$. Die Lösungsmenge des Systems ist also

$$[-1238]_{495} = [247]_{495}.$$