Übungsblatt 6 - Musterlösung

Technische Hochschule Mittelhessen, Fachbereich MNI, Diskrete Mathematik, Prof. Dr. B. Just

Aufgabe 1

a.)

	x	y	
20	1	0	
12	0	1	diese Zeile $\lfloor \frac{20}{12} \rfloor = 1$ mal von vorheriger abziehen
8	1	−1	diese Zeile $\lfloor \frac{12}{8} \rfloor = 1$ mal von vorheriger abziehen
4	−1	2	diese Zeile $\lfloor \frac{8}{4} \rfloor = 2$ mal von vorheriger abziehen
0	3	−5	

b.) $\mathrm{ggT}(20, 12) = 4 = -1 \cdot 20 + 2 \cdot 12$, also $x = -1$, $y = 2$.

c.)

	x	y	
53	1	0	
41	0	1	diese Zeile $\lfloor \frac{53}{41} \rfloor = 1$ mal von vorheriger abziehen
12	1	−1	diese Zeile $\lfloor \frac{41}{12} \rfloor = 3$ mal von vorheriger abziehen
5	−3	4	diese Zeile $\lfloor \frac{12}{5} \rfloor = 2$ mal von vorheriger abziehen
2	7	−9	diese Zeile $\lfloor \frac{5}{2} \rfloor = 2$ mal von vorheriger abziehen
1	−17	22	diese Zeile $\lfloor \frac{2}{1} \rfloor = 2$ mal von vorheriger abziehen
0	41	−53	

d.) $\mathrm{ggT}(53, 41) = 1 = -17 \cdot 53 + 22 \cdot 41$, also $x = -17$, $y = 22$.

e.) „$\Longrightarrow$“: Sei $\mathrm{ggt}(a, m) \neq 1$, also $\mathrm{ggt}(a, m) > 1$.

Der ggT teilt a und m, also teilt er für alle $a^{-1}, q \in \mathbb{Z}$ auch $a \cdot a^{-1} + q \cdot m$.

Somit ist $|a \cdot a^{-1} + q \cdot m|$ entweder Null, oder echt größer als 1, also nicht 1.

„$\Longleftarrow$“: Ist $\mathrm{ggt}(a, m) = 1$, so findet der erweiterte Euklidische Algorithmus $a^{-1}, q \in \mathbb{Z}$ mit $a \cdot a^{-1} + q \cdot m = 1$, also ist die Gleichung lösbar. Q.e.d.

Aufgabe 2

a.) Anwendung des erweiterten Euklidischen Algorithmus liefert:

	x	y	
11	1	0	
2	0	1	obere Zeile $-\lfloor \frac{11}{2} \rfloor = 5$ mal diese Zeile
1	1	−5	

Also ist $1 \cdot 11 - 5 \cdot 2 = 1$, somit $-5 \equiv 6 \equiv 2^{-1} \bmod 11$ (denn $2 \cdot 6 \equiv 1 \bmod 11$).

b.) Anwendung des erweiterten Euklidischen Algorithmus liefert:

	x	y	
15	1	0	
7	0	1	obere Zeile $-\lfloor \frac{15}{7} \rfloor = 2$ mal diese Zeile
1	1	−2	

Also ist $1 \cdot 15 - 2 \cdot 7 = 1$, somit $-2 \equiv 13 \equiv 7^{-1} \bmod 15$.
(Tatsächlich ist $13 \cdot 7 = 91 = 6 \cdot 15 + 1 \equiv 1 \bmod 15$).

c.) Anwendung des Euklidischen Algorithmus liefert:

	x	y	
111	1	0	
101	0	1	obere Zeile $-\lfloor \frac{111}{101} \rfloor = 1$ mal diese Zeile
10	1	−1	obere Zeile $-\lfloor \frac{101}{10} \rfloor = 10$ mal diese Zeile
1	−10	11	

Also ist $-10 \cdot 111 + 11 \cdot 101 = 1$, somit $11 \equiv 101^{-1} \bmod 101$.
(Tatsächlich ist $11 \cdot 101 = 1111 = 10 \cdot 111 + 1 \equiv 1 \bmod 111$).

d.) $\mathrm{ggT}(3, 11) = 1 \Rightarrow$ Es gibt ein multiplikatives Inverses von 3 mod 11.

e.) $\mathrm{ggT}(14, 21) = 7 \neq 1 \Rightarrow$ Es gibt kein multiplikatives Inverses von 14 mod 21.

f.) $\mathrm{ggT}(100, 200) = 100 \neq 1 \Rightarrow$ Es gibt kein multiplikatives Inverses von 100 mod 200.

Aufgabe 3

a.) $(\mathbb{Z}/m\mathbb{Z}, +)$ ist eine Gruppe, denn:

i.) Die Addition mod m zweier Zahlen aus $\{0, 1, ..., m-1\}$
gibt wieder eine Zahl in $\{0, 1, ...m-1\}$.

ii.) Die Assoziativität gilt:
Für $a, b, c \in \{0, ..., m-1\}$ ist $(a+b)+c \equiv a+(b+c) \bmod m$, weil die Assoziativität in $\mathbb{Z}$ gilt.

iii.) Das neutrale Element ist 0:
Für $a \in \mathbb{Z}$ ist $a+0 = 0+a = a$ und damit für $a \in \{0, ..., m-1\}$ stets $a+0 \equiv 0+a \equiv a \bmod m$.

iv.) Inverse Elemente:
Für $a \in \{0, ..., m-1\}$ ist $m-a \in \{0, ..., m-1\}$ das inverse Element, denn $a+(m-a) \equiv m \equiv 0 \bmod m$.

Die Gruppe ist kommutativ und endlich mit m Elementen.

b.) (gerade Zahlen in $\mathbb{Z}$, $+$) ist eine Gruppe, denn:

i.) Die Addition zweier gerader Zahlen ist wieder eine gerade Zahl.

ii.) Die Assoziativität gilt, weil sie in ganz $\mathbb{Z}$ gilt.

iii.) Das neutrale Element ist 0, wie in $\mathbb{Z}$, und 0 ist gerade, also enthalten.

iv.) Ist a eine gerade Zahl, so ist $-a$ ebenfalls eine gerade Zahl, also sind inverse Elemente enthalten.

Die Gruppe ist kommutativ und unendlich.

c.) $(G, \circ)$ ist keine Gruppe, denn kein Wort hat ein Inverses. Durch Hintereinanderhängen werden die Worte länger, und es wird niemals das leere Wort erzeugt, welches Länge 0 hat.

d.) $(G,\circ)$ ist eine Gruppe, denn:

i.) Das Hintereinanderhängen zweier Worte mit Buchstaben a,b,c ist wieder ein Wort mit Buchstaben a,b,c.

ii.) Das Assoziativgesetz gilt:
Sind w_1, w_2, w_3 Worte aus G, so ist $(w_1 \circ w_2) \circ w_3 = w_1 \circ (w_2 \circ w_3)$ das Wort, das durch Hintereinanderschreiben aller Buchstaben aus w_1, w_2, w_3 (in dieser Reihenfolge) entsteht.

iii.) Das leere Wort l ist das neutrale Element:
Es erfüllt für jedes Wort $w \in G$ die Gleichungen $w \cdot l = l \cdot w = w$.

iv.) Inverse Elemente:
Für $w \in G$ ist w^{-1} das Wort, welches aus den Buchstaben in umgekehrter Reihenfolge entsteht. Dann gilt: $w \cdot w^{-1} = w^{-1} \cdot w = l$ (leeres Wort).
Beispiel: $w = abcbb, w^{-1} = bbcba$
$\Rightarrow w \cdot w^{-1} = abcb\underbrace{bb}_{=l}bcba = abc\underbrace{bb}_{=l}cba = ab\underbrace{cc}_{=l}ba = a\underbrace{bb}_{=l}a = aa = l.$
und $w^{-1} \cdot w = \underbrace{bb}_{=l}\underbrace{cb}\underbrace{aa}_{=l}\underbrace{bc}\underbrace{bb}_{=l} = c\underbrace{bb}_{=l}c = cc = l.$

Die Gruppe ist nicht kommutativ und nicht endlich.

e.) $(\mathbb{C}, +, \cdot)$ ist ein Körper, denn:

1.) $(\mathbb{C}, +)$ ist eine Gruppe, denn:

i.) Die Summe zweier komplexer Zahlen ist wieder eine komplexe Zahl.

ii.) Das Assoziativgesetz gilt in $\mathbb{C}$ für die Addition.

iii.) $0 = 0 + 0i$ ist das neutrale Element; für jede komplexe Zahl z ist $z + 0 = 0 + z = z$.

iv.) Zu $a + bi \in \mathbb{C}$ ist $-a - bi$ das additive inverse Element, denn es ist
$a + bi + (-a - bi) = 0$.

2.) $(\mathbb{C} \setminus \{0\}, \cdot)$ ist eine Gruppe, denn:

i.) Das Produkt zweier komplexer Zahlen ist wieder eine komplexe Zahl.

ii.) Das Assoziativgesetz gilt in $\mathbb{C}$ für die Multiplikation.

iii.) $1 = 1 + 0i$ ist das neutrale Element; für jede komplexe Zahl z ist $z \cdot 1 = 1 \cdot z = z$.

iv.) Zu $a + bi \in \mathbb{C}$ ist $\frac{a-bi}{a^2+b^2}$ das multiplikative inverse Element, denn es ist (siehe Vorlesung)

$$(a + bi) \cdot \frac{a - bi}{a^2 + b^2} = 1.$$

3.) Für $x_1 = a_1 + b_1 i,\ x_2 = a_2 + b_2 i,\ x_3 = a_3 + b_3 i \in \mathbb{C}$ gilt das Distributivgesetz:
$x_1 \cdot (x_2 + x_3) = (a_1 + b_1 i) \cdot (a_2 + a_3 + b_2 i + b_3 i) = (a_1 + b_1 i) \cdot (a_2 + b_2 i) + (a_1 + b_1 i) \cdot (a_3 + b_3 i) = x_1 \cdot x_2 + x_1 \cdot x_3$.

f.) $(\{0, 1, 2\}, +)$ ist ein Körper, denn:

1.) $(\{0, 1, 2\}, +)$ mit der Addition mod 3 ist eine (kommutative) Gruppe, wie in Teil a. der Aufgabe gezeigt wurde.

2.) $(\{1, 2\}, \cdot)$ mit der Multiplikation mod 3 ist eine Gruppe, denn:

i.) Das Produkt mod 3 zweier Zahlen aus $\{1, 2\}$ ist wieder in $\{1, 2\}$, denn
$1 \cdot 1 \equiv 1 \cdot 2 \equiv 2 \cdot 1 \equiv 2 \cdot 2 \equiv 1 \bmod 3$.

ii.) Das Assoziativgesetz gilt für die Multiplikation in $\mathbb{Z}$, also auch für die Multiplikation mod 3 .

iii.) 1 ist das neutrale Element, denn für jedes $a \in \{1,2\}$ ist $a \cdot 1 \equiv 1 \cdot a \equiv 1 \bmod 3$.

iv.) Das inverse Element für 1 ist 1, und das inverse Element für 2 ist 2, denn $1 \cdot 1 \equiv 2 \cdot 2 \equiv 1 \bmod 3$.

3.) Das Distributivgesetz gilt, denn:
Für $a, b, c \in \{0,1,2\}$ ist $a \cdot (b+c) \equiv (a \cdot b + a \cdot c) \bmod 3$, weil man mod-Rechnung und Addition/Multiplikation in $\mathbb{Z}$ vertauschen darf.

Anmerkung: $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ mit der Modulo-Rechnung ist für jede Primzahl p ein Körper - wer will, überzeugt sich davon ;-).

Aufgabe 4

a.) Die Anzahl der Elemente in $\mathbb{Z}/12\mathbb{Z} = \{0, ..., 11\}$ ist 12.
$\underbrace{3 + 3 + ... + 3}_{12mal} \equiv 12 \cdot 3 \equiv 36 \equiv 0 \bmod 12$.

b.) Die zu 5 teilerfremden Zahlen in $\{0,1,2,3,4\}$ sind $\{1,2,3,4\}$, also ist die Anzahl der Elemente in $\mathbb{Z}/5\mathbb{Z}^*$ genau 4.
Es ist $4 \cdot 4 \cdot 4 \cdot 4 \equiv 16 \cdot 16 \equiv 1 \cdot 1 \equiv 1 \bmod 5$.

c.) Die zu 17 teilerfremden Zahlen in $\{0,1,...,16\}$ sind $\{1,2,...,16\}$, also ist die Anzahl der Elemente in $\mathbb{Z}/17\mathbb{Z}^*$ genau 16.
Es ist $\underbrace{13 \cdot 13 \cdot 13 \cdot ... \cdot 13}_{16mal} \equiv \underbrace{169 \cdot ... \cdot 169}_{8mal}$
$\equiv 16^8 \bmod 17$ (weil $169 \equiv 16 \bmod 17$)
$\equiv (-1)^8 \bmod 17 \equiv 1 \bmod 17$.

d.) Die zu 21 teilerfremden Zahlen in $\{0,1,...,20\}$ sind $\{1,2,4,5,8,10,11,13,16,17,19,20\}$, also genau 12 Zahlen.
Es ist $5^{12} \equiv 25^6 \equiv 4^6 \equiv 256 \cdot 16 \equiv 4 \cdot 16 \equiv 64 \equiv 1 \bmod 21$

Anmerkung: Allgemein ist für zwei Primzahlen p und q die Anzahl der Elemente in $\mathbb{Z}/p \cdot q\mathbb{Z}^*$ stets $(p-1) \cdot (q-1)$.

e.) Die Zahl der Elemente in G ist 4.
Das neutrale Element ist die Drehung um 0°.
Dreht man 4 mal hintereinander um 270°, so hat man insgesamt um 4·270° = 1080° = 3·360° gedreht.
Jede Ecke wird also wieder in sich überführt.