Reimund Albers, Einführung in die Mathematik I, WiSe 04/05

Übung 4 Lösungsskizzen

1a) R_5

$\cdot \bmod 5$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

R_6

$\cdot \bmod 6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

b) R_5: Alle Restklassen tauchen in jeder Zeile auf außer in der Zeile für $\bar{0}$

R_6: Alle Restklassen tauchen nur in den Zeilen für $\bar{1}$ und $\bar{5}$ auf

c) in R_5 $\quad \bar{a} \cdot \bar{b} = \bar{0} \iff \bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$

in R_6 $\quad \bar{a} \cdot \bar{b} = \bar{0}$ gilt für $\bar{a} = 0$ u. $\bar{b}$ beliebig, $\bar{b} = \bar{0}$ und $\bar{a}$ beliebig, $\bar{2} \cdot \bar{3} = 0$, $\bar{3} \cdot \bar{2} = 0$, $\bar{3} \cdot \bar{4} = \bar{0}$, $\bar{4} \cdot \bar{3} = \bar{0}$

d) R_5 hat keine Nullteiler

R_6 hat $\bar{2}$, $\bar{3}$ und $\bar{4}$ als Nullteiler

e) R_7 hat auch keine Nullteiler

f) R_5 u. R_7 keine Nullteiler: Vermutung ist, dass keine Nullteiler bei ungeraden Modulu auftauchen.

R_9

$\cdot$ mod 9	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$					

also ist $\bar{3}$ Nullteiler in R_9

Die Vermutung mit den ungeraden Modulu ist falsch!

...... Ergebnis $\bar{a} \neq \bar{0}$ ist Nullteiler in R_n

$\Leftrightarrow$ a und n haben einen gemeinsamen Teiler größer als 1

Hausübung

2. a) „ist Teiler von"

Reflexivität: a ist Teiler von a stimmt

Symmetrie: $a \mid b \Rightarrow b \mid a$ stimmt nicht, denn

$2 \mid 12$ aber $12 \nmid 2$

Transitivität: $a \mid b$ und $b \mid c \Rightarrow a \mid c$ stimmt

denn
$$\left.\begin{array}{l} a \mid b \Rightarrow b = k_a \cdot a \\ b \mid c \Rightarrow c = k_b \cdot b \end{array}\right\} c = k_b \cdot k_a \cdot a \Rightarrow a \mid c$$

Also ist „ist Teiler von" <u>keine</u> Äquivalenzrelation

b) „a AGP b"

Reflexivität: a AGP a stimmt

Symmetrie: a AGP b $\Rightarrow$ b AGP a stimmt

Wenn a mit b Aufgaben abgibt, dann auch b mit a.

Transitivität: a AGP b und b AGP c $\Rightarrow$ a AGP c stimmt

Wenn a mit b Aufgaben abgibt und b mit c, dann muss auch a mit c Aufgaben abgeben

2 b) (Forts) Also ist „ist AGP von" eine Äquivalenzrelation.

c) „a GP b"

Reflexivität: a GP a stimmt

Symmetrie: a GP b ⇒ b GP a stimmt

Wenn a mit b in einer Arbeitsgruppe ist, ist auch b mit a in einer

Transitivität: a GP b und b GP c ⇒ a GP c muss nicht stimmen. Denn die Arbeitsgruppen in denen a und b sind ~~mi~~ und b und c müssen nicht übereinstimmen. Dann müssen a und c nicht in einer Arbeitsgruppe sein.

3 a)

+ mod 5	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

b)

+ mod m	$\overline{0}$	$\overline{1}$	$\overline{2}$	....	$\overline{m-2}$	$\overline{m-1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	....	$\overline{m-2}$	$\overline{m-1}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	....	$\overline{m-1}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	....	$\overline{0}$	$\overline{1}$
....	. . .	. . .	. . .	$\ddots$	$\vdots$	$\vdots$
$\overline{m-2}$	$\overline{m-2}$	$\overline{m-1}$	$\overline{0}$	...	$\overline{m-4}$	$\overline{m-3}$
$\overline{m-1}$	$\overline{m-1}$	$\overline{0}$	$\overline{1}$	...	$\overline{m-3}$	$\overline{m-2}$

Oben links beginnt es immer mit $\overline{0}$. Die erste Zeile und Spalte wiederholt den Rand.

3b) Forts.

Die letzte Spalte beginnt oben mit $\overline{m-1}$, darunter steht $\overline{0}$, dann erhöht sich der Restklassenrepräsentant um 1 bis $m-2$.
In schrägen Linien von links unten nach rechts oben stehen die gleichen Restklassen. Diese so verlaufende Diagonale wird von $\overline{m-1}$ gebildet.
Die ganze Tabelle ist symmetrisch zur Diagonalen von links oben nach rechts unten.

4 a) i) $3^6 = 729 = 104 \cdot 7 + 1$ also $3^6 \equiv 1 \mod 7$

ii) $5^6 = 15625 = 2232 \cdot 7 + 1$ also $5^6 \equiv 1 \mod 7$

iii) $3^{10} = 59049 = 5368 \cdot 11 + 1$ also $3^{10} \equiv 1 \mod 11$

iv) $4^{12} = 16777216$ = Division durch 13 liefert kein brauchbares Ergebnis

also

$4^6 = 4096 = 315 \cdot 13 + 1$ also $4^6 \equiv 1 \mod 13$

$\Rightarrow 4^{12} = 4^6 \cdot 4^6 \equiv 1 \cdot 1 = 1 \mod 13$

v) 5^{12}: Ich berechne $5^4 = 625 = 48 \cdot 13 + 1$

also $5^4 \equiv 1 \mod 13$

$\Rightarrow 5^{12} = 5^4 \cdot 5^4 \cdot 5^4 \equiv 1 \cdot 1 \cdot 1 = 1 \mod 13$

b) Vermutung: $a^{m-1} \equiv 1 \mod m$ für $a, m \in \mathbb{N}$

oder besser: für $m \in \mathbb{N}$, $1 \leq a < m$

c) Nach der Vermutung in b) müsste gelten:
$7^{10} \equiv 1 \mod 11$. Überprüfung (notwendig, denn die Aussage in b) ist ja nur eine Vermutung)

$7^{\cancel{10}5} = 16807 = 1527 \cdot 11 + 10$

also $7^5 \equiv 10 \equiv -1 \mod 11$

$\Rightarrow 7^{10} = 7^5 \cdot 7^5 \equiv (-1) \cdot (-1) = 1 \mod 11$

4 c) (Forts)

Dann gilt für jede Potenz von 7^{10}:

$(7^{10})^n \equiv 1 \mod 11$, $n \in \mathbb{N}$

Nun zerlege ich 7^{112} in $7^{11 \cdot 10 + 2} = (7^{10})^{11} \cdot 7^2$

Gesetze der Potenzrechnung

$$(7^{10})^{11} \cdot 7^2 \equiv 1^{11} \cdot 49 \mod 11$$

$$\equiv 5 \mod 11$$

$$\underline{\underline{7^{112} \equiv 5 \mod 11}}$$