Reimund Albers, Arithmetik als Prozess, WiSe 06/07

Übung 4 Lösungsskizzen

1a) R_5

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

R_6

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

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

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

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

in R_6 $\quad \overline{a} \cdot \overline{b} = \overline{0}$ gilt für $\overline{a} = 0$ u. $\overline{b}$ beliebig,

$\overline{b} = \overline{0}$ und $\overline{a}$ beliebig, $\overline{2} \cdot \overline{3} = 0$, $\overline{3} \cdot \overline{2} = 0$,

$\overline{3} \cdot \overline{4} = \overline{0}$, $\overline{4} \cdot \overline{3} = \overline{0}$

d) R_5 hat keine Nullteiler

R_6 hat $\overline{2}$, $\overline{3}$ und $\overline{4}$ 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

HAUSÜBUNGEN

2a) „a AGP b"

Reflexivität a AGP a stimmt (Einergruppe)

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

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

stimmt: a, b, c bilden eine Dreiergruppe [soll nicht sein]

Also: „AGP" ist eine Äquivalenzrelation

c) Die Grundmenge sind alle StudentInnen, die Übungen zur Arithm. abgeben. Die Äquivalenzklassen sind die ~~Übungsz~~, Aufgabengruppen.

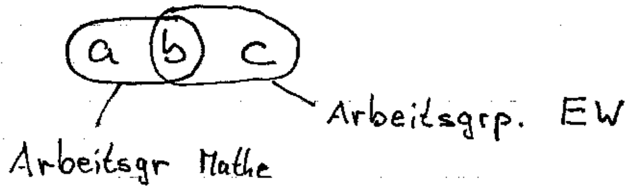
b) „ a GP b"

Reflexivität: $a \, GP \, a$ stimmt

Symmetrie: $a \, GP \, b \Rightarrow b \, GP \, a$ stimmt

Transitivität $a \, GP \, b$ und $b \, GP \, c \not\Rightarrow a \, GP \, c$

denn:



a und c müssen nicht in einer Gruppe sein

3. $a \equiv b \mod m$ heißt: $a = k_a \cdot m + r_1$ $\quad b = k_b m + r_1$

$c \equiv d \mod m$ heißt: $c = k_c m + r_2$ $\quad d = k_d m + r_2$

Dann ist

$$a \cdot c = (k_a m + r_1)(k_c m + r_2) = k_a k_c m^2 + k_a m r_2 + k_c m r_1 + r_1 r_2$$

$$= m \underbrace{(k_a k_c m + k_a r_2 + k_c r_1)}_{\in \mathbb{N}} + r_1 r_2$$

also ist $a \cdot c \equiv r_1 \cdot r_2 \mod m$

Ebenso gilt

$$b \cdot d = (k_b m + r_1)(k_d m + r_2) = m(k_b k_d m + k_b r_2 + k_d r_1) + r_1 r_2$$

also ist $b \cdot d \equiv r_1 \cdot r_2 \mod m$

$\Rightarrow a \cdot c \equiv b \cdot d \mod m$ (Transitivität von $\equiv$)

q.e.d.

4 $\quad 3^1 \equiv 3 \mod 7 \qquad 3^2 \equiv 2 \mod 7 \qquad 3^3 \equiv 6 \mod 7$

$3^4 \equiv 4 \mod 7 \qquad 3^5 \equiv 5 \mod 7 \qquad 3^6 \equiv 1 \mod 7$

$3^7 \equiv 3 \mod 7 \qquad 3^8 \equiv 2 \mod 7 \qquad 3^9 \equiv 6 \mod 7$

a) $3^6 \equiv 1 \mod 7$ danach wiederholen sich die Reste periodisch. Nimmt der Exponent um 6 zu, ist der Rest gleich.

b) Formal $3^n \equiv 3^{n+6} \mod 7$

und fortgesetzt $3^n \equiv 3^{n+6\cdot k}$ $k \in \mathbb{N}$

c) Man muss 253 in „6-er Päckchen" aufteilen

→ teilen mit Rest $253 = 42 \cdot 6 + 1$

also $3^{253} = 3^{42\cdot 6+1} = (3^6)^{42} \cdot 3 \equiv 1^{42} \cdot 3 = 3 \mod 7$

Also: $3^{253} \equiv 3 \mod 7$

d) Bei gegebener Modulzahl m gibt es immer nur m verschiedene Reste beim Teilen. Also kann man im günstigsten Fall den Potenzen $k^1, k^2, \dots, k^m$ verschiedene Reste zuordnen. Spätestens für die Potenz k^{m+1} muss der Rest x_{m+1} eine Zahl sein, die schon einmal vorgekommen ist. Diese Argumentation nennt man Schubfachprinzip

5. a) In der Multiplikationstafel für $m = 11$ ist die Rechnung für „unten rechts" $\overline{10} \cdot \overline{10} = \overline{1}$, denn $10 \cdot 10 = 100 = 9 \cdot 11 + 1$

$m = 18$: $17 \cdot 17 = 289 = 16 \cdot 18 + 1$ also $\overline{17} \cdot \overline{17} = \overline{1}$

$m = 74$: $73 \cdot 73 = 5329 = 72 \cdot 74 + 1$ also $\overline{73} \cdot \overline{73} = \overline{1}$

b) Allgemein ist also immer $(m-1)\cdot(m-1)$ zu berechnen und dann der Rest beim Teilen durch m

c) Also ist allgemein die Rechnung „unten rechts" $\overline{m-1} \cdot \overline{m-1}$ und die Behauptung ist, dass für jede Modulzahl m stets $\overline{1}$ heraus kommt

Formal: $\forall_{\substack{m \in \mathbb{N} \\ m \geq 2}} : \overline{m-1} \cdot \overline{m-1} = \overline{1}$

d) $(n-1)(n-1) = n^2 - 2n + 1$

$= n(n-2) + 1$

Also ist $(n-1)^2 \equiv 1 \mod n$