Mathe Tutorium 29.10.13

(16) $R \subset \mathbb{R}^2 \times \mathbb{R}^2$

$((a,b),(c,d)) \in R \Leftrightarrow a \cdot d = b \cdot c$

Wann ist R eine Äquivalenzrelation

3 Dinge prüfen: Reflexivität, Symmetrie, Transitivität
$(x \sim x)$ $(x \sim y \Rightarrow y \sim x)$ $(x \sim y$ und $y \sim z \Rightarrow x \sim z)$

Reflexivität

$(x \sim x)$

$((a,b),(a,b)) \in R$

weil

$a \cdot b = b \cdot a$ ✓

Symmetrie

$(x \sim y \Rightarrow y \sim x)$

$((a,b),(c,d)) \in R$

$\Leftrightarrow a \cdot d = b \cdot c$

$\Leftrightarrow c \cdot b = d \cdot a$

$\Leftrightarrow ((c,d),(a,b))$ ✓

Transitivität

$(x \sim y$ und $y \sim z \Rightarrow x \sim z)$

$((a,b),(c,d)) \in R \Leftrightarrow a \cdot d = b \cdot c$

$((c,d),(e,f)) \in R \Leftrightarrow c \cdot f = d \cdot e$

zu zeigen

$((a,b),(e,f))$ also $a \cdot f = b \cdot e$

Das gilt immer denn

$b = \frac{a \cdot d}{c}$, $f = \frac{d \cdot e}{c}$

und $a \cdot f = a \cdot \frac{d \cdot e}{c}$

$b \cdot e = \frac{a \cdot d}{c} \cdot e$

Wichtige Relationen:

1) Äquivalenzrelation

2) Ordnungen-Relationen

"$\leq$" etwa $1 \leq 2 \leq 3 \leq 4 \leq \ldots$

- reflexiv
- antisymmetrisch $a \leq b,\ b \leq a \Rightarrow a = b$

"$<$" etwa $1 < 2 < 3 < 4 < \ldots$

- asymmetrisch

(17)

$R_1 = \{(a,b), (a,c)\}$

$R_2 = \{(b,d), (c,a)\}$

$R_1 \circ R_2 = ?$ $\{(c,b), (c,c)\}$ ← von R_2 nach R_1

$R_2 \circ R_1 = ?$ $\{(a,a), (a,d)\}$ ← von R_1 nach R_2

R_1	a	b	c	d
a	0	1	1	0
b	0	0	0	0
c	0	0	0	0
d	0	0	0	0

R_2	a	b	c	d
a	0	0	0	0
b	0	0	0	1
c	1	0	0	0
d	0	0	0	0

Matrizenrechnung geht aber auch! siehe:

$$\begin{pmatrix} 0&1&1&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix} \cdot \begin{pmatrix} 0&0&0&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&0&0&0 \end{pmatrix} = \begin{pmatrix} a & & & d \\ a\ 1&0&0&1 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix}$$

$\{(a,a), (a,d)\}$

$$\begin{pmatrix} 0000 \\ 0001 \\ 1000 \\ 0000 \end{pmatrix} \cdot \begin{pmatrix} 0110 \\ 0000 \\ 0000 \\ 0000 \end{pmatrix} = \begin{pmatrix} 0000 \\ 0000 \\ 0110 \\ 0000 \end{pmatrix} = \{(c,b),(c,c)\}$$

(R_2 · R_1 = b c)

Matrizenrechnung:
Zeile mal Spalte

Rechnen mit Restklassen

$\boxed{a \equiv b \mod m}$, wenn $a-b$ durch m teilbar ist.

etwa $a \equiv 3 \mod 7$

für welche "a" ist das erfüllt?

erfüllt für $a = \ldots, -11, -4, 3, 10, 17, 24$

also für alle Zahlen die beim Teilen durch 7 den Rest 3 lassen

$3 = 0 \cdot 7 + 3$ $\qquad$ $-4 = -1 \cdot 7 + 3$

$10 = 1 \cdot 7 + 3$ $\qquad$ $-11 = -2 \cdot 7 + 3$

$17 = 2 \cdot 7 + 3$ $\qquad$ oder auch negativ $\qquad$ $-18 = -3 \cdot 7 + 3$

$24 = 3 \cdot 7 + 3$ $\qquad$ $-25 = -4 \cdot 7 + 3$

Restklasse $R_3 = \{\ldots, -11, -4, \underline{3}, 10, 17, 24, \ldots\}$

Weitere Restklassen

$R_0 = \{\ldots -14, -7, \underline{0}, \underline{7}, 14, 21, 28, \ldots\}$

$R_1 = \{\ldots, -13, -6, \underline{1}, 8, 15, 22, 29, \ldots\}$

$R_2 = \{\ldots -12, -5, \underline{2}, 9, 16, 23, \ldots\}$

$R_4 = \{\ldots -10, -3, \underline{4}, 11, 18, 25, \ldots\}$

$R_5 = \{\ldots -9, -2, \underline{5}, 12, 19, 26, \ldots\}$

$R_6 = \{\ldots, -8, -1, \underline{6}, 13, 20, 27, \ldots\}$

↑ Kleinste reelle Zahl ist Index

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

← $m = 7$

·	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

← m = 7

Multiplikation wichtig für Verschlüsselungen (Caesar-Chiffre und RSA-Verfahren)

m = 2

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

m = 3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

m = 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

m = 5

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

m = 6

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $a \cdot b = 0$ wenn $a \neq 0, b \neq 0$
  passiert, wenn m keine Primzahl
- a, b heißen Nullteiler
- sind nicht schön
- deshalb benutzt man zum Verschlüsseln in der Kryptographie gerne Primzahlen als Modul m

Weil => Verschlüsseln mit Multiplikation, Entschlüsseln mit Umkehrung, spricht Division. Teilen durch 0 ist aber uncool. Ich weiß nicht, ob vorher Inhalt "a" oder "b" wenn $a \cdot b = 0$.

Division

$\frac{a}{b} = a \cdot b^{-1}$

b^{-1} ist die Zahl mit
$b \cdot b^{-1} = 1$

etwa in $\mathbb{Z}_7$
$1^{-1} = 1$, weil $1 \cdot 1 = 1$
$2^{-1} = 4$, weil $2 \cdot 4 = 1$
$3^{-1} = 5$, weil $3 \cdot 5 = 1$
$4^{-1} = 2$, weil $4 \cdot 2 = 1$
$5^{-1} = 3$, weil $5 \cdot 3 = 1$
$6^{-1} = 6$, weil $6 \cdot 6 = 1$

·	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

$6 = -1$

allgemeine Inverse b^{-1} über Euklidischen Algorithmus