Ist p eine Primzahl, $\varphi(p) = p^0 \cdot (p-1) = p-1$

Klausurzettel

Monday, February 22, 2016 13:30

Relationen

Relationen: 2^{n^2}

anti/-symmetrisch: $2 \wedge \frac{n \cdot (n+1)}{2}$

Reflexiv: $2^{n^2 - n}$

Junktor | Mengenoperation

Junktor	Mengenoperation
$\neg A$	
$A \wedge B$	$M \cap N$
$A \vee B$	$M \cup N$
$A \veebar B$	$M \Delta N$
$A \wedge \neg B$	$M \setminus N$
$A \Rightarrow B$	$M < N$
$A \Leftrightarrow B$	$M = N$

Anzahl Abbildungen $A \to B$

Anzahl insgesamt: $|B|^{|A|}$

Injektiv: $\frac{|B|!}{(|B| - |A|)!}$

Bijektiv: $|B| = |A|$ muss gelten

$= A!$

Surjektiv: $\sum_{0 \le i \le k} (-1)^i \cdot \binom{k}{i} (k-i)^n$

Kombination

$\frac{n!}{(k!(n-k)!)}$ n = Gesamtlänge, k = Wahrscheinlichkeit / Anzahl einer Möglichkeit

Permutation

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 9 & 4 & 1 & 2 & 6 & 7 & 8 \end{pmatrix} \in S_9$

Zykelschreibweise: $(1,3,9,8,7,6,2,5,1)(4)$
$= (1,3,9,8,7,6,2,5)$

$\sigma^{-1} = (1,5,2,6,7,8,9,3)$

$\sigma = (1\,5)(5\,2)(2\,6)(6\,7)(7\,8)(8\,9)(9\,3)$

$sgn(\sigma) = (-1)^7 = -1$

(-1) "hoch" Anzahl der Tupel.

Algebraische Strukturen

Monoide:

Axiom 1: $(x \circ y) \circ z = x \circ (y \circ z)$

Axiom 2: $e \circ x = x = x \circ e$

Abelsch wenn gilt: $x \circ y = y \circ x$

Gruppe

$(G; \circ)$ muss Monoid sein

- alle Elemente sind invertierbar

Für alle $x \in G$ existiert $x' \in G$

Kartesisches Produkt

$A \times B$ $A = \{a, b, c\}$ $B = \{1, 2, 3\}$

$= \{(a_n, b_n) \mid a \in A, b \in B\}$

$= (x,1)\ (x,2)\ (x,3)$
$(y,1)\ (y,2)\ (y,3)$
$(z,1)\ (z,2)\ (z,3)$

$A \times B$

Ring

$(R; +; \cdot)$

(R_1) $(R; +)$ abelsche Gruppe

(R_2) $(R; \cdot)$ Monoid

(R_3) Distributivgesetz

$x \cdot (y+z) = (x \cdot y) + (x \cdot z)$

$(x+y) \cdot z = (x \cdot z) + (y \cdot z)$

kommutativer Ring wenn:

$(R4)$ $x \cdot y = y \cdot x$

Restklassen

$\bar{a}, \bar{b} \in \mathbb{Z}_n$

$\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

$\bar{9} \cdot x = b$ $\mathbb{Z}_{12}$

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$
$\bar{9} \cdot x$	$\bar{0}$	$\bar{9}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{9}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{9}$	$\bar{6}$	$\bar{3}$

Es gibt eine Lösung wenn $b = \bar{0}, \bar{3}, \bar{6}, \bar{9}$

$= \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}, \overline{10}, \overline{11}\}$ (Teilerfremd)

Inverse z.B. $\bar{4}^{-1}: \bar{4} \cdot \bar{x} = \bar{1}$

Tabelle

$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{8}$	$\bar{7}$	$\bar{2}$	$\bar{1}$

Anzahl Einheiten

$\#_n = \varphi(n)$

n	1	2	3	4	5	6	7
$\varphi(n)$	1	1	2	2	4	2	6

$ggT(m, n) = 1$

$\Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Für Primz. $\varphi(p^k) = p^0 (p-1)$

EulerFkt:

Bsp. $\varphi(51) = \varphi(3) \cdot \varphi(17) = (3-1) \cdot (17-1)$

1. Zahl Primfaktorzerlegung
2. In Formel einsetzen: $\varphi(m) \cdot \varphi(n) = (m-1) \cdot (n-1)$

Graphen

Eulertour: Alle Knoten haben geraden Grad
enthält jede Kante und endet wo er angefangen hat.

Eulerzug: End-/Anfangsknoten ungerade Anzahl an Kanten.
Jede Kante wird einmal besucht.

Brücke: Kante bei deren entfernen Wege unmöglich werden.

Kombinatorik

Ziehen von m aus n Kugeln

mit Reihenfolge:

mit Zurücklegen: n^m

ohne Zurücklegen: $\frac{n!}{(n-m!)}$

ohne Reihenfolge:

mit Zurücklegen: $\binom{n+m-1}{m} = \frac{(n+m-1)!}{(n-1)! \cdot m!}$

ohne Zurücklegen: $\binom{n}{m} = \frac{n!}{(n-1)! \cdot m!}$

Relationen (Formeln oben)

$R \subset M \times M \Rightarrow$ Relation auf M

(R) reflexiv, falls xRx für alle $x \in M$

(R') antireflexiv, falls nicht xRx für alle $x \in M$

(S) symmetrisch, $xRy \Rightarrow yRx$

(A) Antisymmetrisch, falls $(xRy \wedge yRx) \Rightarrow x = y$

(T) transitiv, falls $(xRy \wedge yRz) \Rightarrow xRz \Rightarrow x = y$

(partielle) Ordnung: (R) (A) (T) erfüllt

Totalordnung: $xRy \vee yRx \ \forall x, y \in M$

Äquivalenzrelation: (R) (S) (T) erfüllt

$\Rightarrow \{1, 2, 3\}$ = Partitionen = 5

Bäume

G ist kreisfrei / Wald wenn keine Kreise vorhanden.

- zusammenhängender Wald heißt Baum. Endknoten heißen Blätter
- Ein Graph ist dann ein Wald wenn jede Kante eine Brücke ist.

Erweiterter eukl. Algo.

$ggT(264, 385)$

$385 = 1 \cdot 264 + 121$
$264 = 2 \cdot 121 + 22$
$121 = 5 \cdot 22 + 11$
$22 = 2 \cdot 11 + 0$

Rückwärts einsetzen:

$11 = 121 - 5 \cdot 22$
$= 121 - 5 (264 - 2 \cdot 121)$
$= -5 \cdot 264 + 11 \cdot 121$
$= -5 \cdot 264 + 11 \cdot (385 - 1 \cdot 264)$
$= -5 \cdot 264 - 16 \cdot 264$
$\Rightarrow ggT(264, 385) = (-16) \cdot 264 + 11 \cdot 385$

Inverse $\bar{4}$ $n = 9$

$ggT(9, 4) = 1$

$9 = 2 \cdot 4 + 1 \Leftrightarrow 4 = 4 \cdot 1 + 0$

$1 = 1 \cdot 9 - 2 \cdot 4$
$\overset{+9}{=} -2 \cdot 4 \bmod 9 = 1$
$= 7 \cdot 4 \bmod 9 = 1$
$\Rightarrow \bar{4}^{-1} = \bar{7}$

Gleichung lösen $n = 246$ $a = 276$

$\bar{a} \cdot x = \overline{30}$

$\overline{276} \cdot x = \overline{30}$ in $\mathbb{Z}_{246}$

$ggT(276, 246) \Rightarrow 276 = 1 \cdot 246 + 30$
$246 = 8 \cdot 30 + 6$
$30 = 5 \cdot 6 + 0$

$6 = 246 - 8 \cdot 30$
$= 246 - 8 \cdot (276 - 1 \cdot 246)$
$= 9246 - 8 \cdot 276$

Berechnen von $c \Rightarrow \underset{ggT}{6}\, c = \underset{\text{aus Gleichung}}{30}$
$\Rightarrow c = 5$

Gleichung mal c

$5 \cdot 6 = 5 \cdot (-8) \cdot 276$
$30 = -40 \cdot 276$
$30 = \overset{+246}{206} \cdot 276$

$\Rightarrow \bar{a} \cdot \bar{x} = \overline{30}$
$276 \cdot 206 = 30$

• alle Elemente sind invertierbar
Für alle $x \in G$ existiert $x' \in G$
mit $x \circ x' = e = x' \circ x$
<u>Untergruppe</u> $\Rightarrow H \subseteq G$

$276 \cdot 206 = 30$