1 Logik

semantische Äquivalenz — verschiedene Syntax, aber Wahrheitstabelle gleich

DNF, KNF

A	B	
1	0	1
1	1	1
0	0	0
0	1	0

DNF: $(A \wedge B) \vee (A \wedge \neg B)$ 1-Zeilen

KNF: $(A \vee B) \wedge (A \vee \neg B)$ 0-Zeilen

Resolution (KNF)

$$\begin{array}{llll} A \vee B, & A \to B, & B \to C & \models C \quad \equiv \\ (A \vee B) & \wedge (A \to B) & \wedge (B \to C) & \wedge \neg C \equiv \\ (A \vee B) & \wedge (\neg A \vee B) & \wedge (\neg B \vee C) & \wedge \neg C \\ \{A, B\} & \{\neg A, C\} & \{\neg B, C\} & \{\neg C\} \end{array}$$

Hornformeln

Eine Hornformel hat höchstens ein positives Literal

DB
- Fakten
  - A $\{A\}$
  - B $\{B\}$
- Regeln
  - $A \wedge B \to C$ $\{\neg A, \neg B, C)$
  - $B \wedge C \to D$ $\{\neg B, \neg C, D)$

Abfrage: Gilt E? $\neg E \cup DB$ unerfüllbar (Resolution)

Quantoren

$$\begin{array}{lcl} \neg \forall x(P(x)) & \equiv & \exists x(\neg P(x)) \\ \neg \forall x(P(x) \wedge Q(x)) & \equiv & \forall x(P(x)) \wedge \forall y(Q(y)) \\ \neg \exists (P(x) \vee Q(x)) & \equiv & \exists x(P(x)) \vee \exists y(Q(y)) \end{array}$$

ABER:

$$\forall x(P(x) \vee Q(x)) \not\equiv \forall x(P(x)) \vee \forall y(Q(y))$$

Bsp: P = gerade Zahlen; Q = ungerade Zahlen

$$\exists x(P(x) \wedge Q(x)) \not\equiv \exists x(P(x)) \wedge \exists y(Q(y))$$

$$\begin{array}{lcl} \forall x \forall y P(x,y) & \equiv & \forall y \forall x P(x,y) \\ \exists x \exists y P(x,y) & \equiv & \exists y \exists x P(x,y) \end{array}$$

ABER:

$$\forall x \exists y P(x,y) \not\equiv \exists y \forall x P(x,y) \quad \text{ausser } x = y$$

2 Mengenlehre

Mengen	$A \subset B \ :\Leftrightarrow \forall x(x \in A \rightarrow x \in B)$	$A = B \ :\Leftrightarrow (A \subset B) \wedge (B \subset A)$
	$A \cup B \ : \{x \vert x \in A \vee x \in B$	$A \cap B \ : \{x \vert x \in A \wedge x \in B\}$
	$A \setminus B \ : \{x \in A \wedge x \notin B\}$	$A \triangle B \ : \{x \in A \oplus x \in B\}$
Potenzmenge P	Menge aller Teilmengen	$P(\{a,b\}) = \{\varnothing, \{a\}, \{b\}, \{a,b\}\}$
	$\vert P\vert = 2^{\vert A\vert}$	$\vert P(\{a,b\})\vert = 4 = 2^2$
Komplementärmenge	$\bar{A} := U \setminus A$	Achtung! $\bar{\varnothing}$ existiert nicht!

3 Relationen

Eigenschaften	reflexiv:	$\forall a \in A : (a,a) \in R$(Relation)
	Bsp: $3 \mid 3$ wahr, $\leqslant, =, \mid, \subset, \equiv_m$ Gegenbsp: $3 < 3$ falsch, $<, >, \neq, \nmid, \in$	
	anti-reflexiv:	$\forall a \in A : (a,a) \notin R$
	Symmetrie:	$\forall a,b \in A : (a,b) \in R \Leftrightarrow (b,a) \in R$
	Bsp: $=, \equiv_m$	
	Anti-Symmetrie:	$\forall a,b \in A : (a,b) \in R \wedge (b,a) \in R \Rightarrow a = b$
	Bsp: $\leqslant, <, =$	
	transitiv:	$\forall a,b,c \in A : (a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R$
	Bsp: $\leqslant, <, =, \equiv_m$ Gegenbsp: $\neq, \notin$	
ÄquivalenzR ($\sim$)	reflexiv, symmetrisch, transitiv ($\forall a \in A : a \sim a$) etc. (s.o.)	
	Äq.rel. partitionieren Grundmenge (Bell-Zahlen)	
	Äq.rel. sind disjunkt oder identisch	
	Alle Elemente einer Äq.rel sind miteinander verbunden	
	Bsp: $\equiv_m, =$	
OrdnungsR (OR)	reflexiv (anti-reflexiv), anti-symmetrisch, transitiv	
	Bsp: $\leqslant$ auf $\mathbb{N}, \mathbb{Z}, \mathbb{R}$; $\mid$ auf $\mathbb{N}$	
	OR heisst wohlgeordnet, falls $\forall$ nichtleere Teilmengen $\exists$ kleinstes Element	
	Bsp: $(\mathbb{N}, \leqslant)$; Gegenbsp:$(\mathbb{Z}, \leqslant)$	
Hassediagramm	Darstellung endlicher Partialordnungen (Teilbarkeit)	
	Kante in gleiche Richtung: mit gleichem Faktor multipliziert	
	kgV: nächsthöherer gemeinsamer Knoten, ggT: nächsttieferer gem. Knoten	

4 Kombinatorik

Urnenmodell

	geordnet			ungeordnet			
mit Zurückl.	A	$(1,1)$	$(1,2)$	$(1,3)$	B	$(1,1)$	$(1,2)$	$(1,3)$
		$(2,1)$	$(2,2)$	$(2,3)$			$(2,2)$	$(2,3)$
		$(3,1)$	$(3,2)$	$(3,3)$				$(3,3)$
ohne Zurückl.	C		$(1,2)$	$(1,3)$	D	$(1,2)$	$(1,3)$	
		$(2,1)$		$(2,3)$			$(2,3)$	
		$(3,1)$	$(3,2)$					

n Kugeln, k Ziehungen

$A : n^k \quad B : \binom{n+k-1}{k} \quad C : \frac{n!}{(n-k)!} \quad D : \binom{n}{k}$

Inklusion-Exklusion

$|A \cup B| = |A| + |B| - |A \cap B|$

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

$|A_1 \cup ... \cup A_n| = \sum |A_i| - \sum |A_i \cap A_j| + -... + (-1)^{n+1}|A_1 \cap ... \cap A_n|$

Schubfachprinzip

Werden n Objekte auf $k < n$ Schubfächer verteilt,
so gibt es ein Schubfach, das mind. 2, resp. $\left\lceil \frac{n}{k} \right\rceil$ Objekte enthält

Bsp: Von 100 Leuten sind mind. $\left\lceil \frac{100}{12} \right\rceil = 9$ im gleichen Monat geboren.

Doppeltes Abzählen

$|S| = \sum_{a \in A} m_a = \sum_{b \in B} n_b \qquad S = A \times B$

		Airport		
		1	2	3
Airline	a	1	1	0
	b	0	1	1

m_a Summe der Zeilen = Summe der angeflogenen Airports einer Airline

n_b Summe der Spalten = Summe anfliegenden Airlines eines Airports

S = Flugverbindungen

a fliegt zum Airport 1 und 2; Airport 2 wird von a und b angeflogen

Binomialkoeffizient

$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ Pascal-$\triangle$

$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$ Spez.fälle: x=y=1; x=-1, y=1

Vandermonde-Identität

Kugeln in Gruppen unterteilen

$\binom{n}{k} = \sum_{t=0}^{k} \binom{r}{t} \cdot \binom{n-r}{k-t}$ Bsp: $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k} \cdot \binom{n}{n-k}$

Permutationen

$$\begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix}^{-1}=\begin{pmatrix}3&4&5&2&1\\1&2&3&4&5\end{pmatrix}$$

Zyklendarstellung: $(1,3,5)\circ(2,4)$

benötigte Perm. bis zur Identität = kgV(Einzelzyklen)

Perm. einer n-Menge = $n!$

fixpunktfreie Perm. = $\frac{n!}{e}$

Stirling △ 1.Art

$S1_{n,k} = S1_{n-1,k-1} + (n-1)\cdot S1_{n-1,k}$

$S1_{n,k}$ =# Permutationen von n Elementen mit genau k Zyklen

$n=0:$			1		
$n=1:$		0		1	
$n=2:$	0		1		1
$n=3:$	0	2		3	1
$n=4:$	0	6	11	6	1

Stirling △ 2.Art

$S2_{n,k} = S2_{n-1,k-1} + k\cdot S2_{n-1,k}$

$S2_{n,k}$ =# Partitionen einer n-Menge in k-Mengen

$n=0:$			1		
$n=1:$		0		1	
$n=2:$	0		1		1
$n=3:$	0	1		3	1
$n=4:$	0	1	7	6	1

Bell-Zahlen

$B_n = \sum_{k=0}^{n} S_{n,k}$ Summe einer Zeile des Stirling △ 2.Art

B_n =# Äq.rel auf einer n-Menge

$P_{n,k}$

$P_{n,k} = \sum_{i=1}^{k} P_{n-k,i}$

$P_{n,k}$ =# ungeordnete Partitionen von $n \in \mathbb{N}$ durch k positive Summanden

Bsp: n = 4, k = 2: $4 = 1{+}3 = 2{+}2 \Rightarrow P_{4,2} = 2$

$n=0:$			1	0	0
$n=1:$		1		0	0
$n=2:$	1		1	0	0
$n=3:$	1	1		1	0
$n=4:$	1	2	1	1	0

geordnete Partitionen von $n \in \mathbb{N}$ durch k positive Summanden = $\binom{n-1}{k-1}$

Rekursionsgleichung $f_n = f_{n-1} + f_{n-2} \quad f_0 = 0; f_1 = 1$

Ansatz: $f_n = \lambda^n \Rightarrow \lambda^n = \lambda^{n-1} + \lambda^{n-2}$

$\underbrace{(\lambda^2 - \lambda - 1)}_{\text{char. Polynom}} \cdot \lambda^{n-2} = 0 \Rightarrow \lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$

Lsg: $f_n = a \cdot \lambda_1^n + b \cdot \lambda_2^n$

Lsg. bei mehrfachen Nst: $f_n = a \cdot \lambda_1^n + b \cdot n \cdot \lambda_1^n + c \cdot n^2 \cdot \lambda_1^n$

Anfangsbedingungen einsetzen:

$0 = a \cdot 1 + b \cdot \Rightarrow a = -b$

$1 = a \cdot \lambda_1 - a \cdot \lambda_2 \Rightarrow 1 = a(\lambda_1 - \lambda_2)$

$a = \frac{1}{\sqrt{5}}; b = -\frac{1}{\sqrt{5}}$

$$f_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

5 Graphentheorie

Graph $G = (V, E)$ V = Knoten, E = Kanten

$\sum_i \deg(v_i) = 2|E|$

Kreis Sei $(v_i, ..., v_l)$ paarweise verschiedene Knoten, $l \geqslant 3$

G Kreis $:\forall i = 1, ..., l-1 : (v_i, v_{i+1}) \in E \wedge (v_l, v_1) \in E$

zsh. G zusammenhängend. $:\forall u, v \in V \exists$u-v-Pfad

$G = (V, E)$ hat mind. $|V| - |E|$ Zsh.komp.

G zsh. $\Rightarrow |V| - |E| \leqslant 1$

Teilgraph $H = (V', E')$ Teilgraph von $G = (V, E) : V' \subset V \wedge E' \subset E \wedge E' \subset V' \times V'$

Brücke $e \in E$ Brücke: $G' = (V, E \setminus e)$ hat eine Zsh.komp. mehr als $G = (V, E,)$

Baum kreislos, zsh., $|V| \geqslant 2$, mind. 2 Blätter

G ist ein Baum

$\Leftrightarrow$ G ist zsh. $\wedge |V| = |E| + 1$

$\Leftrightarrow$ G ist kreislos $\wedge |V| = |E| + 1$

$\Leftrightarrow$ G ist zsh. $\wedge$ jede Kante ist Brücke

$\Leftrightarrow$ G ist maximal kreislos (zusätzl. Kante ergibt Kreis)

$\Leftrightarrow$ $\forall u, v \in V \exists!$ u-v-Pfad $\quad \exists$: zsh., !: Kreislosigkeit

Spannbaum Sei $G = (V, E)$ Baum. $H = (V, E')$ Spannbaum: H Baum $\wedge E' \subset E$

Kanten im Spannbaum $= |V| - 1$

K_n K_n: vollständiger Graph # Kanten im $K_n = \binom{n}{2} = \frac{n(n-1)}{2}$

Cayley # Spannbäume im $K_n = n^{n-2}$

C_n C_n: Kreis(Zyklen) der Länge $n, n \geqslant 3$

$M_{m,n}$ $M_{m,n}$: Gittergraph, Meshgraph

$K_{m,n}$ $K_{m,n}$: vollst. bipartiter (zweifärbbarer) Graph

Q_d Q_d: d-dim. Hyperkubus

$V = 0, 1^d \quad u, v \in E :\Leftrightarrow d_H(u, v) = 1 \quad d_H$: Hammingdistanz

$|E| = 2^{d-1} \cdot d \quad |V| = 2^d$

Eulertour	Kreis, der jede Kante genau einmal enthält
	Ein zsh. Graph hat eine *geschlossene* Eulertour gdw. alle Knotengrade gerade sind.
	Bsp: K_n für n ungerade, Q_d für d gerade
	Ein zsh. Graph hat eine *offene* Eulertour gdw. zwei Knotengrade ungerade sind
Hamiltonkreis	Kreis, der jeden Knoten genau einmal enthält
	$M_{m,n}$ hamiltonsch, falls $m \cdot n$ gerade und $n \geqslant 2$
	Q_d hamiltonsch für $d \geqslant 2$
	$G = (V, E)$ mit $\deg(V) \geqslant \frac{\lvert V\rvert}{2} \forall v \wedge \lvert V\rvert \geqslant 3 \Rightarrow G$ hamiltonsch
Planare Graphen	$G = (V, E)$ planar, wenn er ohne Kantenüberschneidung gezeichnet werden kann.
	G planar, zsh. $\Rightarrow \lvert V\rvert + f - \lvert E\rvert = 2$
	G teilt die Ebene in f Gebiete
	G planar, $\lvert V\rvert \geqslant 3 \Rightarrow \lvert E\rvert \leqslant 3\lvert V\rvert - 6 \wedge \overline{\deg(v)} < 6$
	G planar, bipartit $\Rightarrow \lvert E\rvert \leqslant 2\lvert V\rvert - 4 \wedge \overline{\deg(v)} < 4$
	Achtung: Die Umkehrrichtung gilt jeweils nicht!
	Nicht planar sind (vollständige Liste nach Kuratowski):
	$K_5, K_{3,3}$ $K_6, K_{3,4}, K_{4,4}, ...$
	Graphen, die den K_5 oder $K_{3,3}$ als Teilgraph enthalten
	Unterteilte Graphen von K_5 oder $K_{3,3}$
	Graphen, die diese unterteilte Graphen als Teilgraph enthalten
Knotenfärbbarkeit	$G = (V, E)$ zsh. $\lvert V\rvert \geqslant 2$, zweifärbbar = bipartit ($\chi(G) = 2$)
	gdw er keinen Kreis ungerader Länge enthält
	$G = (V, E)$planar $\Rightarrow \chi(G) \leqslant 4$
	$\chi(K_n) = n$ $\chi(K_{m,n}) = 2$ $\chi(M_{m,n}) = 2$
	$\chi(Q_d) = 2$ $\chi(\text{Baum}) = 2$ $\chi(C_n) = \begin{cases} 2 & n \text{ gerade} \\ 3 & n \text{ ungerade} \end{cases}$

6 Zahlentheorie

Teilbarkeit	$a \mid b \Leftrightarrow \exists n : a \cdot n = b \Leftrightarrow$ b ist Vielfaches von $a \Rightarrow b > a$
Euklid.Restsatz	$a = q \cdot m + r$
Rest	$r =: R_m(a)$
Modulare Arithmetik	$a = b + q \cdot m \Leftrightarrow a \equiv_m b \Leftrightarrow m \mid (a - b)$ $\equiv_m$ ist Äquivalenzrelation
"Resttheoreme"	$R_m(a + b) = R_m(R_m(a) + R_m(b))$
	$R_m(a \cdot b) = R_m(R_m(a) \cdot R_m(b))$
	$R_m(a^b) = R_m(R_m(a)^b)$
Beispiel	$R_7(2011^{2011}) = R_7(R_7(2011)^{2011}) = R_7(2^{2011}) = R_7(2^{3 \cdot Q+1}) = R_7(2^{3 \cdot Q} \cdot 2) =$
	$R_7(R_7(8^Q) \cdot R_7(2)) = R_7(R_7(8)^Q \cdot 2) = R_7(1^Q \cdot 2) = 2$

Ideal (=ggT)	$(a, b) = \{x \cdot a + y \cdot b \mid a, b, x, y \in \mathbb{Z}\}$
	$\forall a_i \in \mathbb{Z}\ \exists d \in \mathbb{Z} : (a_1, ..., a_n) = \{z \cdot d \mid z \in \mathbb{Z}\} = d\mathbb{Z}$

ggT,kgV

d heisst ggT von a und b, falls:	l heisst kgV von a und b, falls:
$d \mid a$	$a \mid l$
$d \mid b$	$b \mid l$
$c \mid a \wedge c \mid b \Rightarrow c \mid d$	$a \mid m \wedge b \mid m \Rightarrow l \mid m$
$\text{ggT}(a, b) = \lvert d \rvert = (a, b)$	$a \cdot b = \text{kgV} \cdot \text{ggT}$

Erw.Euklid.Algo (EEA)

$\text{ggT}(24, 9)$		24	9
	24	1	0
	9	0	1
$24 \mod 9 = 24 - \mathbf{2} \cdot 9 =$	6	$1 - \mathbf{2} \cdot 0 = 1$	$0 - \mathbf{2} \cdot 1 = -2$
$9 - \mathit{1} \cdot 6$	3	$0 - \mathit{1} \cdot 1 = -1$	$1 - \mathit{1} \cdot -2 = 3$
$6 - 2 \cdot 3$	0	$1 - 2 \cdot (-1) = 3$	$-2 - 2 \cdot 3 = -8$

$\text{ggT}(24, 9) = 3 = -24 + 3 \cdot 9$

Multiplikative Inverse	$a \cdot \underline{\underline{x}} \equiv_b 1$
	Nur vorhanden, falls ggT(a,b) = 1

Beispiel (mit EEA)

$57^{-1} \equiv_{128}?$		128	57
	128	1	0
	57	0	1
2	14	1	-2
4	1	-4	$\underline{\underline{9}}$

$-4 \cdot 128 + 9 \cdot 57 = 1 \Rightarrow \underline{\underline{9}} \cdot 57 \equiv_{128} 1$

Chin. Restsatz (CRS)

$$\left.\begin{array}{l} x \equiv_3 1 \\ x \equiv_4 3 \\ x \equiv_5 3 \end{array}\right| \begin{array}{llll} m_1 = 3 & a_1 = 1 & M = 3 \cdot 4 \cdot 5 = 60 \\ m_2 = 4 & a_2 = 3 \\ m_3 = 5 & a_3 = 3 \end{array}$$

$$M_i = \frac{M}{m_i}: \quad M_1 = 20,\ M_2 = 15,\ M_3 = 12$$

$M_i N_i \equiv_{m_i} 1$ erraten:

$$20 \cdot N_1 \equiv_3 1 \to N_1 = 2$$
$$15 \cdot N_2 \equiv_3 1 \to N_2 = 3$$
$$12 \cdot N_3 \equiv_3 1 \to N_3 = 3$$

$$\tilde{x} = R_M\left(\sum_{i=1}^{r} a_i M_i N_i\right)$$

$$\tilde{x} = R_{60}(1 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3) = R_{60}(40 + 135 + 108) = R_{60}(283) = 43$$

$$x = \tilde{x}(\mod 60)$$

Umwandlung in ein reguläres CRS-System aus CRS-System mit nicht teilerfremden Moduli

$$\left.\begin{array}{l} z \equiv_6 1 \\ z \equiv_{10} 3 \\ z \equiv_{75} 28 \end{array}\right\} \begin{array}{l} \left.\begin{array}{l} z \equiv_2 1 \\ z \equiv_3 1 \end{array}\right\} z \equiv_6 1 \\ z \equiv_{25} 3 \end{array} \Rightarrow \left|\begin{array}{l} z \equiv_6 1 \\ z \equiv_{25} 3 \end{array}\right| z = 103(\mod 150)$$

$$\left\{\begin{array}{ll} z \equiv_2 1 & \\ z \equiv_3 1 & \\ z \equiv_2 3 & = z \equiv_2 1 \\ z \equiv_5 3 & \\ z \equiv_3 28 & = z \equiv_3 1 \\ z \equiv_{25} 28 & = z \equiv_{25} 3 \end{array}\right.$$

7 Algebra

Gruppe (G,$*$)	Assoziativität	$\forall a, b, c \in G : (a * b) * c = a * (b * c)$
	Neutrales Element	$\exists e : a * e = e * = a \forall a$
	Inverses	$\forall a \exists b : a * b = b * a = e$
Geometrische Gruppen	Rotationen, Ähnlichkeitstrafos, Translationen, Spiegelungen	
Symmetriegruppe s_n	Spiegelungen und Rotationen am n-Eck $\quad \lvert s_n \rvert = 2n$	
Untegruppen	$H \subset G$ falls H bzgl. $*$ selbst eine Gruppe ist	
Lagrange	$\lvert H \rvert \mid \lvert G \rvert$	
	Falls G Untergruppen hat, so sind diese paarweise disjunkt	
Produkt von Gruppen	$\mathbb{Z}_{15}^* = \left\{\binom{1}{1}, \binom{2}{1}, \binom{3}{1}, \binom{4}{1}, \binom{1}{2}, \binom{2}{2}, \binom{3}{2}, \binom{4}{2}\right\} = \{1,2,3,4\} \times \{1,2\} = \mathbb{Z}_5^* \times \mathbb{Z}_3^*$	
	$\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$	
	$\mathbb{Z}_m = \mathbb{Z}_p \times \mathbb{Z}_q \quad$ falls $m = p \cdot q$	
Endliche Gruppen	$\mathbb{Z}_p \quad \mathbb{Z}_{p-1}^* \quad p$ prim	
Ordnung endl. Gruppen	$\text{ord}(a) := \min\{i > 0 \mid a^i = e\}$	
	$\text{ord}(a) \mid \lvert G \rvert \quad a^{\lvert G \rvert} = e$	

Zyklische endl. Gruppen

G heisst zyklisch, falls $\exists g \in G : \text{ord}(g) = |G|$

$G = \{g^0, g^1, g^2, ..., g^{|G|-1}\}$

g heisst Generator von G, $G =< g >$

$|G|$ prim $\Rightarrow G$ zyklisch $\Rightarrow G$ abelsch

$|G|$ prim $\Rightarrow$ jedes $g \neq e$ ist Generator

Beispiel

$\mathbb{Z}_p^*$

φ-Funktion

$\mathbb{Z}_m^* := \{a \in \mathbb{Z}_m | \text{ggT}(a, m) = 1\}$

$\varphi(m) = |\mathbb{Z}_m^*|$ "Anzahl teilerfremde Zahlen von m"

$\varphi(m) = \prod_{i=1}^{r}(p_i - 1) \cdot p_i^{e_i - 1}$ $m = \prod_{i=1}^{r} p_i^{e_i}$ Primfaktorzerlegung

$\varphi(p) = p - 1$

Beispiel

$|\mathbb{Z}_{45}^*|$ $45 = 3^2 \cdot 5^1 \Rightarrow p_1 = 3, e_1 = 2; p_2 = 5, e_2 = 1$

$\varphi(45) = (3-1) \cdot 3^{2-1} \cdot (5-1) \cdot 5^{1-1} = 2 \cdot 3 \cdot 4 = 24$

Satz von Fermat-Euler

$\forall m \geqslant 2 \; \forall a : \text{ggT}(a, m) = 1$

$a^{\varphi(m)} \equiv_m 1$

$a^{p-1} \equiv_p 1$

Diskreter Logarithmus

$R_p(a^x) \leftrightarrow x \xleftrightarrow{isomorph} \mathbb{Z}_p^*$

$x \rightarrow R_p(a^x)$ einfach

$R_p(a^x) \rightarrow x$ schwierig, lösbar z.B. mit Babystep-Giantstep

Babystep-Giantstep Algo

Eingabe: zykl.endl.Gruppe G, Generator g, Gruppenelement a

Ausgabe: $x = \log_g a$

$m := \left\lceil \sqrt{|G|} \right\rceil$

$\forall j \in \{0, ..., m-1\}$ berechne g^j und speichere (j, g^j) in der Tabelle T

$\forall i \in \{0, ..., m-1\}$ berechne $a \cdot \left(g^{-m}\right)^i$ und suche den Wert in T

Falls gefunden, gib $im + j$ aus

Beispiel

$R_{29}(11^x) = 3$ $G = 29, g = 11, a = 3$

$|G| = \varphi(29) = 28 \Rightarrow m := \left\lceil \sqrt{28} \right\rceil = 6$

j	0	1	2	3	4	5
11^j	1	11	5	26	25	14

$11^{-6} = 11^{28-6} = 13$

i	0	1	2
$3 \cdot 13^i$	3	10	14

$i = 2, j = 5 \Rightarrow x = 2 \cdot 6 + 5 = 17$

Körper (K,+,·)

$(K, +)$ abelsche Gruppe bzgl. Addition mit NE 0

$(K^*, \cdot)$ abelsche Gruppe bzgl. Multiplikation mit NE 1

$\forall a, b, c \in K : \ a \cdot (b + c) = a \cdot b + a \cdot c$

Endliche Körper

$(\mathbb{Z}_p, +, \cdot) =: GF(m)$

p prim, $n \in \mathbb{N} \Rightarrow \exists!$ endlicher Körper mit p^n Elementen, genannt $GF(p^n)$

Werden Zeilen oder Spalten eines GF vertauscht,

so ist es immer noch der gleiche (isomorphe) GF

Beispiele

$GF(2)$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$GF(4) = GF(2^2)$

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

irreduzible Polynome

Analogon zu Primzahlen

Polynom hat Nullstellen $\Rightarrow$ Nicht irreduzibel

Für Polynome mit Grad $\leqslant 3$ gilt obiges in beide Richtungen.

iP über GF(2)

Grad 1: $x, \ x + 1$

Grad 2: $x^2 + x + 1$

Grad 3: $x^3 + x + 1, \ x^3 + x^2 + 1$

Grad 4: $x^4 + x^3 + 1, \ x^4 + x + 1, \ x^4 + x^3 + x^2 + x + 1$

Elemente des $GF(2^3)$

Elemente des $GF(2) : 0, 1$

Nimm ein irreduzibles Polynom, z.B. $P = x^3 + x + 1 = 0$

Alle Polynome, die strikt kleiner sind als das Primpolynom, sind $\in GF(2^3) \Rightarrow 0, 1, x, x$

Teilbarkeit

$a(x) \mid b(x) \Leftrightarrow \exists n(x) : a \cdot n(x) = b \Rightarrow \deg(b) \geqslant \deg(a)$

Euklid.Restsatz

$a(x) = q(x) \cdot m(x) + r(x)$

Rest

$r(x) =: R_{m(x)}(a(x))$

Modulare Arithmetik

$a(x) = b(x) + q(x) \cdot m(x) \Leftrightarrow a(x) \equiv_{m(x)} b(x) \Leftrightarrow m(x) \mid (a(x) - b(x))$

Multiplikative Inverse

$a(x) \cdot \underline{\underline{z(x)}} \equiv_{m(x)} 1$

Beispiel (mit EEA)

$x^{-1} \equiv_{x^2+x+1}$		$x^2 + x + 1$	x
	$x^2 + x + 1$	1	0
	x	0	1
$x + 1$	1	1	$\underline{\underline{x + 1}}$

$(x + 1) \cdot x + x^2 + x + 1 \equiv_{x^2+x+1} 1 \Rightarrow \underline{\underline{x + 1}} \cdot x \equiv_{x^2+x+1} 1$

RSA

Alice	Eve	Bob
$p, q :=$ prim		$m :=$ Nachricht $\quad m \leqslant n$
$\rightarrow n = p \cdot q$		
$\rightarrow f = \varphi(n) = (p-1)(q-1)$		
$e := \mathrm{ggT}(e, f) = 1$	$\overset{n,e}{\Longrightarrow}$	$c = R_n(m^e)$
$\rightarrow d = q \cdot f + e^{-1}$	$\overset{c}{\Longleftarrow}$	
$\rightarrow m = R_n(c^d)$		

Angriffspunkte

1. Finde $n = p \cdot q$, berechne d und m wie Alice
2. $c = R_n(m^e)$ durchprobieren

Diffie-Hellman

Alice	Eve	Bob
	Einwegfkt: $x \mapsto R_p(g^x)$	
$p :=$ prim, $g :=$ Generator	$\overset{p,g}{\Longrightarrow}$	
$x :=$ geheim $\in \{0, ..., p-2\}$	$\overset{R_p(g^x)}{\Longrightarrow}$	
	$\overset{R_p(g^y)}{\Longleftarrow}$	$y :=$ geheim $\in \{0, ..., p-2\}$
$\rightarrow K_{AB} = R_p\left((g^y)^x\right)$		$\rightarrow K_{BA} = R_p\left((g^x)^y\right)$

$K_{AB} = K_{BA}$ ist der gemeinsame Schlüssel