

Inhaltsverzeichnis

<u>Inhaltsverzeichnis</u>	1
<u>Grundlagen</u>	10
Mathematische Zeichen.....	10
Zahlenmenge	10
<u>Logik und Beweise</u>	12
Logik (Aussagelogik/Propositionale Logik).....	12
Term	12
Aussage (Propositionen)	12
Prioritäten von Logischen Operatoren	12
Verknüpfung von Aussagen	12
Negation , die nicht-Verknüpfung (\neg)	12
UND -Verknüpfung = Konjunktion (\wedge)	13
ODER -Verknüpfung = Disjunktion (\vee)	13
XOR -Verknüpfung (\oplus).....	13
Implikation (Subjunktion) (\rightarrow).....	14
Bikonditional (Bijunktion) (\Leftrightarrow)	14
Tautologie und Widerspruch (T / F).....	14
Propositionale Äquivalenzen	15
Logische Äquivalenzen	15
Logische Äquivalenzgesetze	15
Beispiel Absorption ($p \vee (p \wedge q)$).....	16
Prädikat (=Aussageform) und Quantoren	16
Quantoren.....	17
Allquantor (\forall)	17
Existenzquantor (\exists).....	17
Verschachtelte Quantoren.....	17
Beweismethoden	17
Ausdrücke.....	17
Mathematische Ausdrücke (gerade/ungerade Zahl)	17
1. Durchrechnen aller Möglichkeiten	18
2. Gegenbeispiel finden	18
Direkte Beweis	18
Indirekter Beweis (durch Kontraposition).....	18
Indirekter Beweis (Durch Kontradiktion oder Widerspruchsbeweis).....	19
<u>Mengen, Funktionen, Folgen & Reihen</u>	19
Mengenlehre.....	19

Bekannte Mengen ($\mathbb{N}, \mathbb{Z}, \mathbb{Z}+, \mathbb{R}, \mathbb{C}$)	20
Spezielle Mengen	20
Teilmenge (\subset)	20
Leere Menge (\emptyset)	20
Kardinalität ($ A $) - Anzahl Elemente	20
Potenzmenge (2^S)	20
Gleiche Mengen ($=$)	20
Gleichmächtige Menge ($ A = B $)	20
Kreuzprodukt (x)	20
Mengenoperationen	20
Komplement (A)	20
Durchschnitt (\cap)	21
Vereinigung (\cup)	21
Differenz ($-$)	21
Zusammenfassung der Regeln	21
Funktionen ($f(x)$)	21
Einführung	21
Schreibweise	21
Definitionsbereich (x)	21
Wertebereich = Bildbereich = Bildmenge (y)	21
Weitere Funktionen	21
Mehrdimensionale Funktionen	21
Stückweise Definition von (reellen) Funktionen	22
Spezielle Funktionen / Funktionseigenschaften	22
Wurzelziehen ($DB \geq 0$)	22
Injektive Funktion (Auf jedes Y zeigt höchstens ein X)	22
Surjektive Funktion (Jedes Y hat min. ein X)	22
Bijektive Funktion (Injektiv und Sujektiv = Jedes Y genau ein X)	22
Der Graph der Funktion	23
Zusammengesetzte Funktionen	23
Die Umkehrfunktion	23
Die ceiling- und die floor-Funktion (Aufrund- / Abrundfunktion)	24
Folgen	24
Einige spezielle Folgen	24
Eine wichtige Überlegung	24
Arithmetische Folge (Differenz Konstant)	24
Geometrische Folge (Quotient Konstant)	24
Funktionale Darstellung der geometrischen folge GF	25

Reihen	25
Summenzeichen	25
Produktzeichen	25
Definitionen	25
Rekursive Darstellung einer Reihe	26
Formeln für arithmetische Reihe	26
Formeln für geometrische Reihe	26
<u>Komplexe Matrizen</u>	27
Algorithmen	27
Eigenschaften	27
Wachstum von Funktionen (Big O-Notation)	27
Definition	27
Funktionen nach Größen ($n!$, 2^n , n^2 , $n\log n$, n , $\log n$, 1)	27
Wachstum von Polynomen (=Mehrgliedriger Term)	28
Wachstum von weiteren Funktionen (Log- & Potenz-Gesetze)	29
Fakultät	29
Logarithmus	29
Allgemeine (Graphische) Betrachtung	29
Zahlen und Division	29
Einführung	29
Teilbarkeit ($a b \rightarrow a$ teilt b)	30
Definition	30
Primzahlen	30
Definition	30
Fundamentalsatz der Arithmetik	30
Primfaktorzerlegung	30
Mersenne Primzahlen	30
Anzahl Primzahlen errechnen	30
ggT und kgV	31
Modulare Arithmetik (Modulo)	31
Eigenschaften	31
Kongruent (\equiv)	31
Addition und Subtraktion	31
Modulo von negativer Zahl	31
Multiplikation	32
Restklasse	32
Der euklidische Algorithmus	32
Matrizen	33

Einführung.....	33
Definition (Matrix)	33
Rechnen mit Matrizen.....	34
Addition & Subtraktion	34
Multiplikation mit Zahl (Zahl mal Matrix)	34
Wichtige Eigenschaften.....	34
Matrizenmultiplikation (Matrix mal Matrix).....	35
Transponierte Matrix (A^T)	36
Eigenschaften (symmetrisch, antisymmetrisch, Einheitsmatrix I_n).....	36
Die inverse Matrix (A^{-1})	37
Rechenregeln / Formeln für Matrizen	37
Lösen von Matrizengleichungen	38
Vorgehen bei Matrizengleichungen.....	38
Null-eins Matrizen.....	39
Oder- und Und-Verknüpfung	39
Definition ($\vee = \text{oder}$, $\wedge = \text{und}$)	39
Boolsches Produkt.....	39
Eigenschaften.....	39
R-te Boolesche Potenz	40
Definition.....	40
<u>Begründungen, Induktionsbeweise, Rekursive Funktionen & Algorithmen, Inferenzregeln</u>	41
Mathematische Induktion (beweisen durch Induktionsschritt)	41
Bekannte Beweismethoden	41
Der Induktionsbeweis	41
Rekursiv definierte Funktionen.....	43
Definition.....	43
Rekursive/induktive vs. Funktionale/explizite Darstellung.....	43
Rekursive Algorithmen.....	44
Definition.....	44
Rekursiv vs. Iterativ.....	44
Turm von Hanoi.....	44
Schlussregeln/Inferenzregeln	45
Begriffe	45
Grundlagen.....	45
Verschiedene Regeln (Alles Tautologien)	45
Schlussregel Schreibweise (\therefore).....	45
Modus ponens (Inferenzregel/Abtrennungsregel = Grundform des direkten Beweises)	46
Modus tollens (Aufhebender Modus).....	46

Hypothetischer Syllogismus	46
Disjunktiver Syllogismus.....	47
Addition.....	47
Simplifikation	47
Konjunktion	47
Resolution	47
Prüfungsaufgabe	48
Beispiel zu den Schlussregeln (Um welche Schlussregel handelt es sich?)	48
Anwendungen der Schlussregeln.....	48
Schlussregeln – Denkfehler (Nicht alle Prämissen sind Tautologien).....	48
Schlussregeln für quantifizierte Aussagen	48
<u>Kombinatorik – Counting (Permutation, Kombination, Variation)</u>	49
Grundlegende Zählprinzipien.....	49
Anzahl Teilmengen ($ A $)	49
Produktregel (unabhängige Wahl, ohne wegnehmen).....	49
Produktregel & kartesisches Produkt von Mengen	49
Summenregel (entweder oder)	50
Summenregel & Vereinigung von Mengen.....	50
Das Einschluss-/Ausschlussprinzip (Anzahl Lösungen)	51
Das Schubfachprinzip (Finden von (mindestens) einer Zahl, welche ...).....	51
Definition.....	51
Zahlen finden, welche nur aus Einsen & Nullen besteht	51
Formel	52
Permutation und Kombination	53
Permutation ($P(n,n) / P(n,r) = \text{geordnete Auswahl}$)	53
Definition.....	53
Anzahl n-Permutationen einer Menge	53
Anzahl r-Permutationen(Variation) einer Menge	53
Kombination ($C(n,r) = \text{ungeordnete Auswahl}$)	53
Definition.....	53
Anzahl r-Kombinationen einer Menge n (Reihenfolge egal = Kombination)	54
Prüfungsaufgabe – Lotto.....	54
Verallgemeinerte Permutationen und Kombinationen	55
r-Permutationen (Variation, geordnet) mit Wiederholung (mehrmals das gleiche Element/Wert).....	55
r-Kombinationen(ungeordnet) mit Wiederholung (mehrmals das gleiche Element/Wert).....	55
Permutationen nicht unterscheidbarer Objekte	56
Binomialkoeffizienten (für α – reelle Zahlen (nicht \mathbb{N})).....	56
Definition.....	56

Pascal'sche Dreieck & Binomialkoeffiziente (Zahl vor x^2 herausfinden).....	57
Entscheidungsbaum Kombinatorik	58
.....	58
<u>Diskrete Wahrscheinlichkeit 1 & 2</u>	59
Laplace'sche Wahrscheinlichkeit	59
Grundlagen der Wahrscheinlichkeitstheorie	59
Grundbegriffe (Stichprobenraum, Ereignisse, etc.)	59
Unendlicher Stichproberaum.....	60
2 Unterscheidbare Würfel	60
2 nicht unterscheidbare Würfel.....	60
Mengenlehre vs. Wahrscheinlichkeit.....	61
Zusammenstellung der Gemeinsamkeiten(\subseteq =Teilmenge, \cap =und(Schnittmenge), \cup =oder,usw.)	61
Wahrscheinlichkeit; Axiome von Kolmogorov	62
Definition.....	62
Annahmen/Regeln/Formeln	62
Gleichverteilung	62
Wichtige Regeln im Detail	63
Wahrscheinlichkeit des Gegenereignisses(höchstens/mindestens eine ...)	63
Additionssatz.....	63
Mehrstufige Experimente – Baumdiagramm – Entscheidungsbäume	64
Wahrscheinlichkeit einer Vereinigung mehrerer Mengen	65
Vertiefung der Wahrscheinlichkeitstheorie.....	65
Wahrscheinlichkeit von Ereignissen	65
Definition.....	65
Unabhängige Ereignisse und bedingte Wahrscheinlichkeit.....	66
Unabhängige Ereignisse	66
Bedingt Wahrscheinlichkeit (mit Voraussetzung)	66
Satz von Bayes.....	68
Satz der totalen Wahrscheinlichkeit	68
Prüfungsbeispiel – Satz der Totalen Wahrscheinlichkeit	69
Satz von Bayes (mit $P(B A)$ zu $P(A B)$)	69
Multiplikationssatz für beliebige zwei Ergebnisse ($P(A \cap B)$ berechnen für Additionssatz).....	70
Multiplikationssatz.....	70
Wahrscheinlichkeitsverteilungen, Verteilungsfunktion.....	71
Wahrscheinlichkeitsverteilung.....	71
Berechnung des Erwartungswertes $E[X]$ der Zufallsvariablen X	71
Berechnung der Varianz $Var[x]$ der Zufallsvariablen X (Volatilität)	71
Berechnungsmethode 1	71

Berechnungsmethode 2	71
Einführung und Definitionen (Begriffe)	72
Verteilungen ohne Modelle	72
Die diskrete Gleichverteilung (Alle Wsk. sind gleich).....	73
Die Bernoulli-Verteilung (Einmal ziehen, mit zwei Mögliche Ausgänge mit unter. Wsk.).....	73
Die Binomialverteilung (Ziehen mit zurücklegen).....	73
Die hypergeometrische Verteilung (Ziehen ohne zurücklegen - wegnehmen)	74
Die Poisson-Verteilung (μ , mittlere/erwartete Anzahl, Durchschnittl. /min, /m ² – Anzahl E in Zeitraum)	74
Anwendung 1	74
Anwendung 2:	75
Strategie bei Verteilmodell-Aufgaben (Wsk von Teilmenge mit best. Eigenschaft).....	76
Zusammenfassung der diskreten Verteilungen	76
Zufallsvariablen (X – Wert einem Ergebnis zuordnen)	77
Definition.....	77
Wahrscheinlichkeitsverteilung einer Zufallsvariable ($p(X = r)$)	77
Erwartungswert von Zufallsvariablen ($E[X]$, «erwartete Gewinn», «Durchschnitt»,...)	78
Definition.....	78
Weitere Anwendungen.....	78
Rechnen mit dem Erwartungswert	78
Unabhängige Zufallsvariablen.....	79
Varianz von Zufallsvariablen	79
Formelzusammenstellung von $E[X]$ und $Var[X]$ von unseren Modellen	79
<u>Fortgeschrittene Zähltechnik</u>	80
Abkürzungen	80
Einführung von Rekursionsbeziehungen	80
Rekursive Gleichung.....	80
Explizite/Funktionale Gleichung	80
Beispiel Fibonacci-Folge	80
Zielformulierung.....	80
Definition der Rekursionsbeziehung	80
Lösen von Rekursionsbeziehungen RB.....	81
Begriffe	81
Lineare Rekursionsbeziehung	81
Lösen von linearen Rekursionsbeziehungen (Allgemeines Vorgehen)	81
1. Lösen der homogenen Rekursionsbeziehung	81
2. Bestimmen einer partikulären Lösung der inhomogenen Rekursionsbeziehung	84
3. Summe von Schritt 1 und 2 berechnen.....	85
Beispiele zum Lösen von linearen Rekursionsbeziehungen	85

Homogene , lineare RB vom Grad $k = 1$	85
Inhomogene , lineare RB vom Grad $k = 1$	86
Homogene , lineare RB vom Grad $k = 2$ und $D > 0$	87
Inhomogene , lineare RB vom Grad $k = 2$ und $D > 0$	88
Homogene , lineare RB vom Grad $k = 2$ und $D = 0$	89
Inhomogene , lineare RB vom Grad $k = 2$ und $D = 0$	90
Homogene/Inhomogene , lineare RB vom Grad $k = 2$ und $D < 0$	91
Erzeugende Funktionen	91
Repetition Polynom n-ten Grades	91
Definition.....	91
Anwendung: Anzahl Lösungen in den natürlichen Zahlen von Ungleichungen.....	92
Weiteres Beispiel (Wieviele Arten verteilen, wenn mindestens & maximal).....	93
Erweitertes Ein-/Ausschlussprinzip.....	93
Mengenvereinigung	93
Definition Ein-/Ausschlussprinzip	93
Derangement	94
Anwendung (Anzahl Mglk. Etwas aufzuteilen ohne zweimal etwas an denselben Ort zu tun).....	94
Zahlentheorie	95
Mod n Operation und Euklidischer Algorithmus	95
Division mit Rest (Dividend, Divisor, Quotient, $R_n(a)$).....	95
Kongruenz mod n (Beide Zahlen haben denselben Rest bei Division durch n, (\equiv)).....	95
Der Euklidische Algorithmus (ggT)	96
Vorgehen/Algorithmus	96
Eigenschaften des ggT(a,b)	96
Diophantische Gleichungen	96
Lösen von linearen Diophanischen Gleichungen	96
Satz von Bezout.....	96
Das Inverse mod N (Kehrwert).....	97
Das additive Inverse mod N ($(a + b) \text{ mod } N$).....	97
Multiplikative Inverse mod N ($(a * b) \text{ mod } N$)	97
Das "gezielte Durchprobieren" um multiplikatives Inverses welches 1 ergibt zu bekommen.....	97
Wann existiert das multiplikative inverse der Zahl $x \text{ mod } N$?	98
Das Inverse mod N & der erweiterte Euklidische Algorithmus.....	98
Der erweiterte Euklidische Algorithmus ($x \& y$ finden, sodass $n_1 * x + n_2 * y = 1$)	99
Beispiel Prüfungsaufgabe (Finden Sie $x, y \in \mathbb{Z}$ mit $963 \cdot x + 218 \cdot y = 1$)	100
Der Chinesische Restsatz	101
Definition.....	101
Vorgehensweise anhand von einem Beispiel	102

Eulerische ϕ -Funktion («Phi» - Teilerfremde natürliche Zahlen kleiner n)	103
Definition.....	103
Anwendungsregeln / Ausrechnen von teilerfremden Zahlen.....	103
Primzahlen	104
Definition und Eigenschaften.....	104
Der kleine Satz von Fermat ($m^p \bmod p$ – Potenz in Moduloberechnung)	104
Der kleine Satz von Fermat & der Chinesische Restsatz (Große Potenzen modulo schnell rechnen).....	105
Prüfungsbeispiel – Satz von Fermat und Chinesischer Restsatz	105
Verteilung der Primzahlen	106
Mersenne-Primzahlen.....	106
Rechnen in Restesystemen	107
Relationen und Äquivalenzrelationen (Reflexiv, Symmetrisch, Transitiv)	107
Restklassen ($\bmod n$).....	108
Modulare Rechenoperationen.....	108
Addition und Multiplikation $\bmod n$ (\oplus_n, \odot_n).....	108
Square and Multiply (SAM-Algorithmus)	110
Nullteiler.....	111
Definition Nullteiler.....	111
Inverse Elemente	111
Inverse berechnen mit dem kleinen Fermat (Nur wenn $n = \text{Primzahl}$).....	112
Primitive Elemente.....	113
Einwegfunktionen	114
Definition.....	114
Modulare Quadratwurzel.....	114
Schulbuchversion der Diffie-Hellman Schlüsselverteilung	115
Übersicht und Definitionen.....	115
Symmetrische Verschlüsselung.....	115
Asymmetrische Verschlüsselung.....	115

Grundlagen

Mathematische Zeichen

Zeichen	Bedeutung	Beispiel	
\in	„Ist Element von ...“	$-2 \in \mathbb{Z}$	
\notin	„Ist nicht Element von ...“	$-2 \notin \mathbb{N}$	
\exists	„Es existiert ...“	$\exists a, b, c \in \mathbb{N}$ so, dass $a^2 + b^2 = c^2$	
\nexists	„Es existiert nicht (keine) ...“	$\nexists a, b \in \mathbb{R}$ so, dass $ a + b > a + b $	
\forall	„Für alle ...“	$\forall a \in \mathbb{R}$ gilt $ a \geq 0$	
\setminus	„Ohne ...“	$\mathbb{R} \setminus \{0\}$ heisst „die reellen Zahlen ohne die Null“	
$ $	„Für die gilt“	$\{x \in \mathbb{R} \mid x > 0\}$ „ x aus \mathbb{R} , für die gilt $x > 0$ “	
$ $	Betrag	$ -4 = 4$	
Σ	Summe		
\prod	Produkt		
!	Fakultät		
\approx	„ungefähr“	$1/3 \approx 0,333$	
\neq	„nicht gleich“	$1/3 \neq 0,333$	
\equiv	„äquivalent“, „gleichwertig“	$\neg(A \vee B) \equiv \neg A \wedge \neg B$	
∞	„unendlich“		
\vee	oder, OR	$A \vee B$ (A oder B)	
\wedge	und, AND	$A \wedge B$ (A und B)	
\neg	nicht, NOT	$\neg A$ (nicht A)	
$<$	„kleiner“	$3 < 4$	
$>$	„grösser“	$-5 > -6$	
\leq	„kleiner oder gleich“	$3 \leq 4; 3 \leq 3$	
\geq	„grösser oder gleich“	$-5 \geq -6; -5 \geq -5$	
$] [$	„offenes Intervall“	$]a; b[= \{x \mid a < x \wedge x < b\}$ $= \{x \mid a < x < b\}$	Alle Zahlen zwischen a und b, <u>exkl.</u> a und b
$[]$	„abgeschlossenes Intervall“	$[a; b] = \{x \mid a \leq x \wedge x \leq b\}$ $= \{x \mid a \leq x \leq b\}$	Alle Zahlen zwischen a und b, <u>inkl.</u> a und b
$[[$	„links abgeschlossenes, rechts offenes Intervall“	$[a; b[= \{x \mid a \leq x \wedge x < b\}$ $= \{x \mid a \leq x < b\}$	Alle Zahlen zwischen a und b, <u>inkl.</u> a, <u>exkl.</u> b
$]]$	„links offenes, rechts abge- schlossenes Intervall“	$]a; b] = \{x \mid a < x \wedge x \leq b\}$ $= \{x \mid a < x \leq b\}$	Alle Zahlen zwischen a und b, <u>exkl.</u> a, <u>inkl.</u> b

Bemerkung:

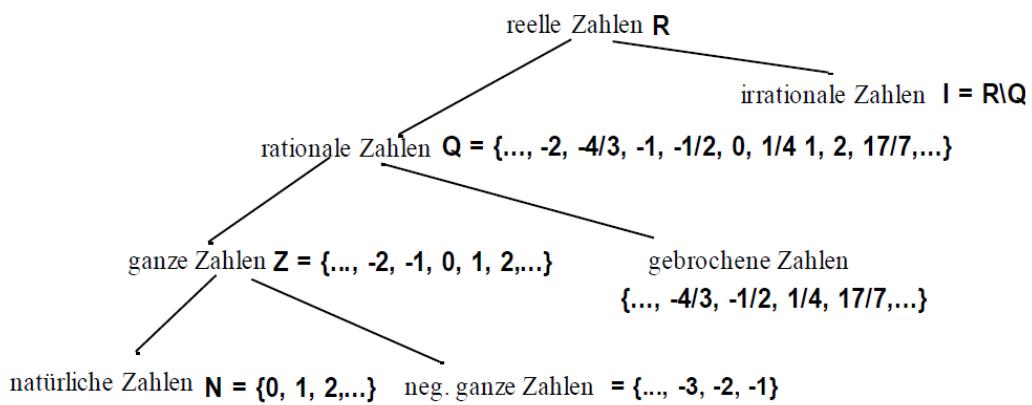
Falls die Grenzen der Intervalle $-\infty$ oder ∞ sind, dann werden die offenen Intervalle gebraucht:

$]-\infty; b]$ $[a; \infty[$ $]-\infty; \infty[$

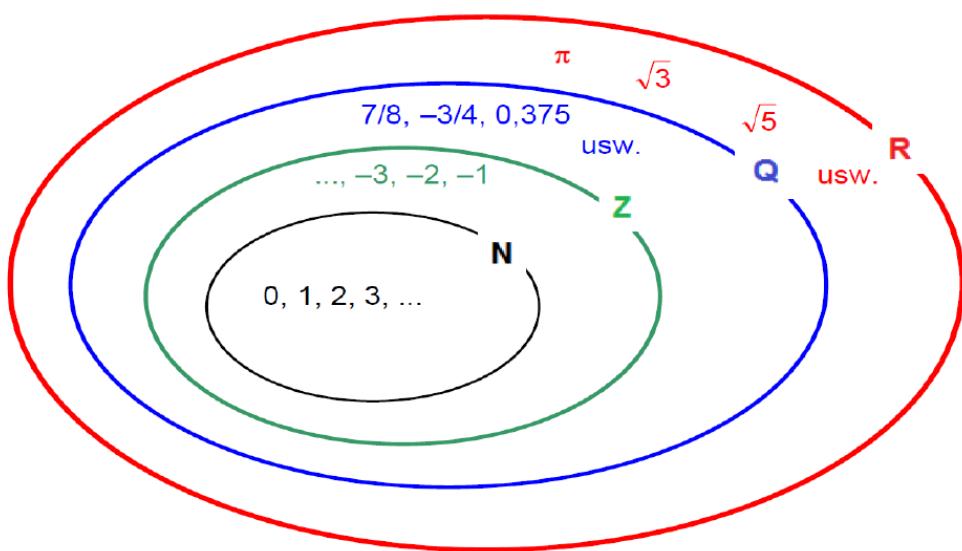
- * Die Zahl Null wird aus der Zahlenmenge ausgeschlossen. $\mathbb{N}^* \{1, 2, 3, \dots\}$
- + Es sind nur die positiven Zahlen und die Null zu nehmen. $\mathbb{Z}_+ \{0, 1, 2, 3, \dots\}$
- Es sind nur die negativen Zahlen und die Null zu nehmen. $\mathbb{Z}_- \{\dots, -3, -2, -1, 0\}$

Zahlenmenge

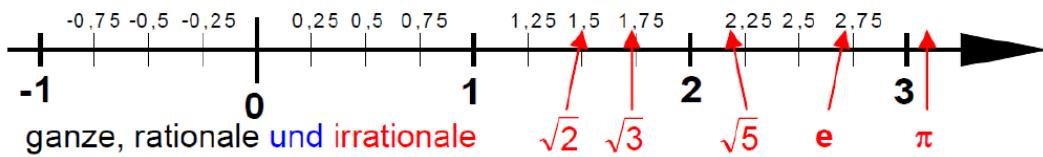
Die reellen Zahlen als Baumdiagramm:



Die reellen Zahlen als Zwiebeldiagramm:



Darstellung auf der Zahlengerade:



Beispiele von rationalen (= „als Bruch darstellbare“) Zahlen: $\frac{2}{3}, \frac{17}{6}, \frac{4}{1} = 4, \frac{3}{1} = 3$

Beispiele von Zahlen, die nicht rational sind: $\pi, \sqrt{2}$, usw.

Logik und Beweise

Logik (Aussagelogik/Propositionale Logik)

Term

Ein Term ist eine sinnvolle **Zusammensetzung von Zahlen, Variablen, Operationszeichen und Klammern**. Ein Term hat **keinen Wahrheitsgehalt**, ist also **weder wahr noch falsch**.

Beispiel: $4, x, -a, |z|, \sqrt{a}$

Speziell: $T(a,b)$ ist ein Term, der die Variablen a und b enthält.

Aussage (Propositionen)

Eine Aussage (Proposition) **beschreibt** durch Worte oder Zeichen **einen Sachverhalt**. Eine Aussage ist **entweder wahr(w,t,1) oder falsch(f,f,0)**.

Beispiel: $2 + 5 = 7$ (wahr) ; 19 ist eine Primzahl (wahr) ; Mozart war ein Mathematiker (falsch)

Keine Aussagen

Wie spät ist es? $x + 1 = 2$ (Aussageform, je nach x -Wert wahr oder falsch) ; Dieser Satz ist falsch.

Begründung: Dem Sachverhalt kann **nicht entweder wahr oder falsch zugeordnet werden**.

Prioritäten von Logischen Operatoren

Operator	Priorität
\neg	1
\wedge	2
\vee	2
\rightarrow	3
\leftrightarrow	3

Verknüpfung von Aussagen

Auf wie viele Arten kann man zwei Aussagen verknüpfen?

Es gibt 16 mögliche binäre Verknüpfungen

p	q	Widerspruch						\oplus		\wedge	\leftrightarrow		\rightarrow		\vee	Tautologie	
1	1	0			0	0	0	0	0	0	1	1	1	1	1	1	1
1	0	0			0	0	0	1	1	1	1	0	0	0	1	1	
0	1	0			0	1	1	0	0	1	1	0	0	1	0	1	
0	0	0			1	0	1	0	1	0	1	0	1	0	1	1	

Negation, die nicht-Verknüpfung (\neg)

Definition

Ist p eine Proposition, dann ist die Proposition „Es ist nicht der Fall, dass p gilt“ die Negation von p ; man schreibt $\neg p$ und liest „nicht p “.

Wahrheitstabelle

Die „NICHT“-Verknüpfung (Negation, NOT)

p	$\neg p$	$\neg(\neg p) = p$
1	0	1
0	1	0

Der Eingang wird invertiert, d.h. aus einer 0 wird eine 1 und umgekehrt.

in Worten: $\neg p$ = „Nicht p “

Regel: $\neg(\neg p) = p$ (Analog Mengenlehre $\bar{\bar{A}} = A$)

UND-Verknüpfung = Konjunktion (\wedge)**Definition (Konjunktion – UND-Verknüpfung)**

Die Propositionen $p \wedge q$ (gelesen: "p und q") heisst **Konjunktion** der Propositionen p und q, falls diese genau dann wahr ist, wenn p und q wahr sind; andernfalls ist sie falsch.

Wahrheitstabelle**Die „UND“-Verknüpfung (Konjunktion, AND)**

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Der Ausgang ist nur 1 wenn beide Eingänge 1 sind.

in Worten: \wedge = „UND“ resp. „AND“

Regel: $p \wedge q = q \wedge p$ (KG)
 $(p \wedge q) \wedge r = p \wedge (q \wedge r)$ (AG)

Bemerkung

Analogie zur Mengenlehre: Seien A und B Mengen, dann wird der **Durchschnitt** der Mengen A und B wie folgt definiert.

Der **Durchschnitt** zweier Mengen A und B ist diejenige Menge, die die Elemente von A und von B enthält.

Mathematisch: $A \cap B = \{x \mid x \in A \wedge x \in B\}$

ODER-Verknüpfung = Disjunktion (\vee)**Definition (Disjunktion)**

Die Propositionen $p \vee q$ (gelesen: "p oder q") heisst **Disjunktion** der Propositionen p und q falls diese wahr ist, wenn mindestens eine der Propositionen p oder q wahr ist; andernfalls ist sie falsch.

Wahrheitstabelle**Die „ODER“-Verknüpfung (Disjunktion, OR)**

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Der Ausgang ist 1 wenn mindestens ein Eingang 1 ist.

in Worten: \vee = „ODER“ resp. „OR“

Regel: $p \vee q = q \vee p$ (KG)
 $(p \vee q) \vee r = p \vee (q \vee r)$ (AG)

Bemerkung

Analogie zur Mengenlehre: Seien A und B Mengen, dann wird die **Vereinigung** der Mengen A und B wie folgt definiert.

Die **Vereinigung** zweier Mengen A und B ist diejenige Menge, die die Elemente von A oder von B enthält.

Mathematisch: $A \cup B = \{x \mid x \in A \vee x \in B\}$

XOR-Verknüpfung (\oplus)**Definition (XOR)**

Die Propositionen $p \oplus q$ (gelesen: "p exor q") heisst **XOR-Verknüpfung** der Propositionen p und q, falls diese genau dann wahr ist, wenn genau eine der Propositionen p oder q wahr ist (aber nicht beide gleichzeitig); ansonsten ist sie falsch.

Wahrheitstabelle**Die „XOR“-Verknüpfung (exclusive OR, entweder oder, Addition mod 2)**

p	q	$p \oplus q$
1	1	0
1	0	1
0	1	1
0	0	0

Der Ausgang ist 0 genau dann wenn beide Eingänge gleich sind. Resp. der Ausgang ist 1 genau dann wenn beide Eingänge unterschiedlich sind.

in Worten: \oplus = „XOR“

Regel: $p \oplus q = q \oplus p$ (KG)
 $(p \oplus q) \oplus r = p \oplus (q \oplus r)$ (AG)

Implikation (Subjunktion) (\rightarrow)**Definition**

Die **Implikation** $p \rightarrow q$ (gelesen "p impliziert q" oder "falls p, dann q") ist diejenige Proposition, die genau dann falsch ist, wenn p wahr und q falsch ist; anderenfalls ist die Implikation wahr. p heißt auch **Hypothese** und q **Konklusion**.

Wir werden weiter hinten noch zeigen, dass gilt: $p \rightarrow q \equiv \neg q \rightarrow \neg p$ resp. $p \rightarrow q \equiv \neg p \vee q$

Wahrheitstabelle**Die „Implikation“ („Wenn dann“, Subjunktion)**

p	q	$p \rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Die Implikation $p \rightarrow q$ ist nur dann falsch, wenn die Hypothese p wahr, die Konklusion q aber falsch ist. In allen anderen Fällen ist sie wahr.

Oder kurz: „Aus Falschem folgt alles“.

Die Implikation $p \rightarrow q$ kann auch so interpretiert werden:

- wenn p, dann q
- schon wenn p, dann q
- p ist eine hinreichende Bedingung für q
- eine hinreichende Bedingung für q ist p
- p ist hinreichend für q
- p nur wenn q
- eine notwendige Bedingung für p ist q
- q ist eine notwendige Bedingung für p
- q folgt aus p
- p impliziert q
- Beim Programmieren if p then q

Bikonditional (Bijunktion) (\leftrightarrow)**Definition**

Das **Bikonditional** $p \leftrightarrow q$ (gelesen "p genau dann, wenn q") ist diejenige Proposition, die wahr ist, wenn p und q die selben Wahrheitswerte haben und sonst falsch.

Wahrheitstabelle**Die „Bijunktion“ („genau dann wenn“, Bikonditional)**

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Die Bijunktion $p \leftrightarrow q$ ist genau dann wahr, beide Propositionen den gleichen Wahrheitsgehalt haben.

Beispiel

Ein Dreieck ABC mit den Seitenlängen a, b und c ist rechtwinklig $\Leftrightarrow c^2 = a^2 + b^2$

Tautologie und Widerspruch (T / F)**Definition (Tautologie, Widerspruch)**

Eine zusammengesetzte Aussage, die immer wahr (falsch) ist heißt **Tautologie** (Kontradiktion oder **Widerspruch**).

Wahrheitstabelle**Die Tautologie („immer wahr“)**

p	q	$p \top q$
1	1	1
1	0	1
0	1	1
0	0	1

Der Widerspruch (Kontradiktion, „immer falsch“)

p	q	$p \perp q$
1	1	0
1	0	0
0	1	0
0	0	0

Propositionale Äquivalenzen

Logische Äquivalenzen

Definition (Logische Äquivalenz)

Die Aussagen p und q heißen logisch äquivalent, falls $p \leftrightarrow q$ eine Tautologie ist. Man schreibt dann $p \Leftrightarrow q$ (oder auch $p \equiv q$ bzw. $p \sim q$).

Beweisen durch Umformen, oder aufzeigen in Wahrheitstabelle.

Beispiel

Mit $p = \neg(a \vee b)$ und $q = \neg a \wedge \neg b$ gilt: $p \equiv q$ resp. $\neg(a \vee b) \equiv \neg a \wedge \neg b$.

Beweis für Äquivalenz

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

Logische Äquivalenzgesetze

TABLE 6 Logical Equivalences.

Equivalence	Name
$p \wedge T \equiv p$	Identity laws
$p \vee F \equiv p$	
$p \vee T \equiv T$	Domination laws
$p \wedge F \equiv F$	
$p \vee p \equiv p$	Idempotent laws
$p \wedge p \equiv p$	
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$	Commutative laws
$p \wedge q \equiv q \wedge p$	
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive laws
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ <i>& wird zu V</i>	De Morgan's laws
$\neg(p \vee q) \equiv \neg p \wedge \neg q$ <i>& V zu &</i>	
$p \vee (p \wedge q) \equiv p$	Absorption laws
$p \wedge (p \vee q) \equiv p$	
$p \vee \neg p \equiv T$	Negation laws
$p \wedge \neg p \equiv F$	

TABLE 7 Logical Equivalences Involving Conditional Statements.

$p \rightarrow q \equiv \neg p \vee q$
$p \rightarrow q \equiv \neg q \rightarrow \neg p$
$p \vee q \equiv \neg p \rightarrow q$
$p \wedge q \equiv \neg(p \rightarrow \neg q)$
$\neg(p \rightarrow q) \equiv p \wedge \neg q$
$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

TABLE 8 Logical Equivalences Involving Biconditional Statements.

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

WICHTIG BEISPIEL AUF NÄCHSTER SEITE!!!

$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Verwendetes Gesetz
$\equiv [(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	$A \rightarrow B \equiv \neg A \vee B$
$\equiv \neg[(p \vee q) \wedge (\neg p \vee r)] \vee (q \vee r)$	De Morgan auf den Ausdruck in [...]
$\equiv [\neg(p \vee q) \vee \neg(\neg p \vee r)] \vee (q \vee r)$	Je de Morgan in den 2 Ausdrücken (...) in [...]
$\equiv [(\neg p \wedge \neg q) \vee (p \wedge \neg r)] \vee (q \vee r)$	Ohne [...] und ohne letzte (...) geschrieben.
$\equiv (\neg p \wedge \neg q) \vee (p \wedge \neg r) \vee q \vee r$	AG und KG auf V angewandt und neue [...] gesetzt.
$\equiv [(\neg p \wedge \neg q) \vee q] \vee [(p \wedge \neg r) \vee r]$	Beide [...] mit DG auseinander genommen.
$\equiv [(\neg p \vee q) \wedge (\neg q \vee q)] \vee [(p \vee r) \wedge (r \vee \neg r)]$	$(\neg q \vee q)$ und $(r \vee \neg r)$ sind Tautologien
$\equiv [(\neg p \vee q) \wedge T] \vee [(p \vee r) \wedge T]$	$T \wedge A \equiv A$ und [...] weggelassen.
$\equiv (\neg p \vee q) \vee (p \vee r)$	AG und KG auf V angewandt und neue (...) gesetzt.
$\equiv (\neg p \vee p) \vee (q \vee r)$	$(\neg p \vee p)$ ist eine Tautologie
$\equiv T \vee (q \vee r)$	$T \vee A \equiv T$
$\equiv T$	

Beispiel Absorption ($p \vee (p \wedge q)$)

Example (Absorption)

Zeige mit Hilfe einer Wahrheitstabelle, dass das Absorptionsgesetz $p \vee (p \wedge q) \equiv p$ gilt!

p	q	$p \wedge q$	$p \vee (p \wedge q)$
w	w	w	w
w	f	f	w
f	w	f	f
f	f	f	f

Analytisch hat man

$$\begin{aligned}
 p \vee (p \wedge q) &\equiv (p \wedge T) \vee (p \wedge q) && \text{Identität} \\
 &\equiv p \wedge (T \vee q) && \text{Distributiv 2} \\
 &\equiv p \wedge T && \text{Dominanz} \\
 &\equiv p && \text{Identität}
 \end{aligned}$$

Infolge dualer Symmetrie gilt auch $p \wedge (p \vee q) \equiv p$.

Prädikat (=Aussageform) und Quantoren

Example

Falls eine Folge von Wörtern bei geeigneter Wahl einer oder mehrerer Variablen zu einer Aussage wird, dann spricht man von einem Prädikat. Beispiel:

$P(x) = "x > 3"$

Prädikate enthalten mind. eine Variable (hier x); sie haben aber nur dann einen eindeutigen Wahrheitswert, wenn man für diese Variable einen bestimmten Wert einsetzt. Man kann also nach den Wahrheitswerten von $P(4)$ und $P(2)$ fragen.Lösung: $P(4) = "4 > 3"$ ist wahr, während $P(2) = "2 > 3"$ falsch ist.Man nennt die Aussage $P(x)$ auch den Wert der propositionalen Funktion P für x . Wenn es keine „=“/“<“/“>“-Zeichen hat ist es keine Aussage.Achtung: Sobald „Für alle“ (\forall) oder „es existiert“ (\exists) steht ist es eine Aussage und deshalb keine Aussageform, da sie eben entweder wahr oder falsch ist.

Quantoren

Zeichen	Bedeutung	Beispiel
\exists	„Es existiert ...“	$\exists a, b, c \in \mathbb{N}$ so, dass $a^2 + b^2 = c^2$
$\nexists \equiv \neg \exists$	„Es existiert nicht (keine) ...“	$\nexists a, b \in \mathbb{R}$ so, dass $ a + b > a + b $
$\exists!$	„Es existiert genau ein ...“	$\exists! x \in \mathbb{R}$, so dass $3x + 2 = 6$
\forall	„Für alle ...“	$\forall a \in \mathbb{R}$ gilt $ a \geq 0$
$\neg \forall$	„Nicht für alle...“	$\neg \forall a \in \mathbb{R}$ gilt $ a > 1$

Allquantor (\forall)

Ist $P(x)$ wahr für alle x aus einer bestimmten Universalmenge, dann schreibt man $\forall x P(x)$ und liest: „für alle x gilt $P(x)$ “.

Beispiel: $P(x): x + 1 > x \Rightarrow \forall x P(x)$ (d.h. Für alle x existiert ein $P(x)$ resp. ein y)

Existenzquantor (\exists)

Ist $P(x)$ wahr für mindestens ein x aus einer bestimmten Universalmenge, dann schreibt man $\exists x P(x)$ und liest: „es existiert ein x für welches $P(x)$ wahr ist“.

Beispiel: $P(x): x^2 - 1 < 0 \Rightarrow \exists x P(x)$ (d.h. Für mind. ein x gibt es ein $P(x)$ resp. ein y , Bsp. $x = 0$)

ACHTUNG: Es **existiert genau ein x** wird mit $!$ bezeichnet. $\exists! x P(x)$

Verschachtelte Quantoren

Wichtiger Nachtrag	Ausdruck	Negation	Bemerkung
	=	\neq	Und umgekehrt
	$>$	\leq	Und umgekehrt
	$<$	\geq	Und umgekehrt
	Gerade Zahl	Ungerade Zahl	Nur in \mathbb{Z} oder \mathbb{N}
	Gerade Zahl	Nicht gerade Zahl	in \mathbb{R} , \mathbb{Q} usw.
	Primzahl	Nicht Primzahl oder zusammengesetzte Zahl	Nur in $\mathbb{N} \setminus \{0; 1\}$ 0 und 1 sind weder Prim noch zusammengesetzt.

Beispiel:

	w/f	Grund/Resultat
$\forall x \exists y(xy = 1)$ in $\mathbb{R} \setminus \{0\}$ oder $\mathbb{Q} \setminus \{0\}$	1	Die Aussage ist wahr, weil es zu jedem x in $\mathbb{R} \setminus \{0\}$ oder $\mathbb{Q} \setminus \{0\}$ ein y gibt, nämlich $y = 1/x$. Man könnte sogar $\forall x \exists! y(xy = 1)$ schreiben, aber das wollen wir nicht.
$\forall x \exists y(xy = 1)$ in $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ oder \mathbb{N}	0	Die Aussage ist falsch, weil es in \mathbb{R} resp. \mathbb{Q} , genau ein Element gibt, wo es kein solches y gibt, nämlich für $x = 0$ In \mathbb{Z} resp. \mathbb{N} ist die Aussage falsch, weil außer für $x = 1$ resp. $x = -1$ kein y gibt, so dass die Aussage wahr wird.

Beweismethoden

Ausdrücke

- **Theorem:** Eine Aussage, von der man zeigen kann, dass sie wahr ist.
- **Axiome/Postulate:** Können in Aussagen enthalten sein und sind grundlegende Annahmen, welche dementsprechend nicht bewiesen werden müssen.
- **Lemma/Hilfssatz:** Einfacher Satz, der in Beweisen von komplizierteren Sätzen verwendet wird
- **Korollar:** Einfache Folgerung eines Satzes.

Mathematische Ausdrücke (gerade/ungerade Zahl)

- Sei $m \in \mathbb{Z}$ eine **gerade Zahl**, dann hat sie die Form $m = 2n$ mit $n \in \mathbb{Z}$.
- Resp. umgekehrt: $\forall n \in \mathbb{Z}$ gilt $m = 2n$ ist eine gerade ganze Zahl
- Sei $m \in \mathbb{Z}$ eine **ungerade Zahl**, dann hat sie die Form $m = 2n + 1$ resp. $m = 2n - 1$ mit $n \in \mathbb{Z}$.
- Resp. umgekehrt: $\forall n \in \mathbb{Z}$ gilt $m = 2n + 1$ resp. $m = 2n - 1$ ist eine ungerade ganze Zahl.
- Innerhalb der ganzen Zahlen ist „nicht gerade“ äquivalent zu „ungerade“, resp. „nicht ungerade“ ist äquivalent zu „gerade“. Dies gilt aber in anderen Zahlenbereichen wie \mathbb{R} oder \mathbb{Q} nicht!!

1. Durchrechnen aller Möglichkeiten

Meist nicht effizient und oft unmöglich. Jedoch bei gewissen Fällen mit der Wahrheitstabelle möglich.

a	b	$a \vee b$	$\neg(a \vee b)$		$\neg a$	$\neg b$	$\neg a \wedge \neg b$
1	1	1	0		0	0	0
1	0	1	0		0	1	0
0	1	1	0		1	0	0
0	0	0	1		1	1	1

2. Gegenbeispiel finden

Wird verwendet, um zu beweisen, dass eine Regel **nicht stimmt**.

Direkte Beweis

Der direkte Beweis **wenn p dann q** , oder eben die **Implikation $p \rightarrow q$** gründet darauf, dass **aufgrund der Richtigkeit von p die Richtigkeit von q folgt**. Wir erinnern uns **aber**, dass **aus Falschem alles folgt** ($0 \rightarrow 1$, also ist der Teil vor dem « \rightarrow » 0, dann ist der Teil nach dem « \rightarrow » immer 1).

Beim direkten Beweis wird aber **$p \wedge (p \rightarrow q)$** bewiesen. Nicht nur $p \rightarrow q$. Das heisst es werden nur die Fälle betrachtet, wo p wahr ist.

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$
1	1	1	1
1	0	0	0
0	1	1	0
0	0	1	0

Beispiel:

Behauptung: Die Summe einer geraden und einer ungeraden ganzen Zahl ist eine ungerade ganze Zahl.

Beweis:

Wir schreiben die Voraussetzung (direkte Annahme) „x ist eine gerade und y ist eine ungerade ganze Zahl“ zunächst um.

Also $x = 2n$ mit $n \in \mathbb{Z}$ und $y = \underbrace{2m+1}_{\text{ungerade Zahl}}$ mit $m \in \mathbb{Z}$.

Daher folgt:

$z = x + y = 2n + 2m + 1 = 2(m + n) + 1$; d.h. die Summe z ist von der Form $z = 2t + 1$, mit $t = n + m$. Da die Summe von zwei ganzen Zahlen (n & m) wieder eine ganze Zahl ist, ist $z = 2t + 1$ eine ungerade ganze Zahl.

Indirekter Beweis (durch Kontraposition)

Beruhrt auf der logisch äquivalenten Aussage $(p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$ und dass wir die Implikation $(\neg q \rightarrow \neg p)$ wiederum direkt beweisen. Also es ist ein **direkter Beweis der Kontraposition**.

Beispiel:

Behauptung: Alle Primzahlen grösser 2 sind ungerade.

Behauptung Umformulierung: Gegeben sei $a > 2$, dann gilt: Ist a eine Primzahl $\Rightarrow a$ ist ungerade.

D.h. wir haben etwas in der **Form: $p \rightarrow q$, mit $p = \text{„}a \text{ ist eine Primzahl}\text{“}$ und $q = \text{„}a \text{ ist ungerade}\text{“}$** .

Behauptung Kontraposition: Gegeben sei $a > 2$, dann gilt: Ist a gerade $\Rightarrow a$ ist keine Primzahl.

Beweis:

Wenn **a gerade** ist, dann **können wir schreiben** $a = 2 \cdot r$ und **damit enthält a neben den Faktoren 1 und a auch den Faktor 2** und damit ist a **per Definition keine Primzahl** q.e.d.

Beispiel 2:

Behauptung: Gegeben sei n eine natürliche Zahl, dann gilt: $3n + 2$ ist ungerade $\Leftrightarrow n$ ist ungerade.

Beweis:

„**n ungerade**“ heisst ja, dass es eine natürliche Zahl k gibt, so dass **n = 2k + 1**. Dann gilt: $3n + 2 = 3(2k + 1) + 2 = 6k + 3 + 2 = (6k + 4) + 1 = 2(3k + 1) + 1 = 2t + 1$

Somit ist **$3n + 2 = 2t + 1$** für eine natürliche Zahl t, da **$3n + 2$ die Form $2t + 1$** (gerade + ungerade = ungerade) **hat, ist $3n + 2$ ungerade**.

Indirekter Beweis (Durch Kontradiktion oder Widerspruchsbeweis)

Um die Aussage p zu beweisen nimmt man an $\neg p$ sei wahr und führt diese Aussage durch logisches Schliessen auf einen Widerspruch. Somit muss $\neg p$ falsch und damit p wahr sein.

Beispiel

Behauptung: Für alle positiven Zahlen a, b gilt: $\frac{a+b}{2} \geq \sqrt{ab}$

Gegenteil: $\frac{a+b}{2} > \sqrt{ab}$, also: $\frac{a+b}{2} < \sqrt{ab}$

$\Rightarrow a + b < 2\sqrt{ab}$

$\Rightarrow (a + b)^2 < 4ab$ Quadrieren, hier kommt nun die Voraussetzung, $a, b \geq 0$ zum Zuge.

$\Rightarrow a^2 + 2ab + b^2 < 4ab$

$\Rightarrow a^2 - 2ab + b^2 < 0$

$\Rightarrow (a - b)^2 < 0$ Widerspruch, denn ein Quadrat ist immer positiv.

Also ist die Annahme falsch, dass $\frac{a+b}{2} < \sqrt{ab}$ und damit muss gelten $\frac{a+b}{2} \geq \sqrt{ab}$.

Beispiel 2

Kurze Repetition zu den rationalen Zahlen \mathbb{Q} . $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \right\}$.

Satz: $\sqrt{2}$ ist keine rationale Zahl (also irrational), d.h. $\sqrt{2} \notin \mathbb{Q}$

Beweis durch Widerspruch, wir nehmen an, es gilt: $\sqrt{2} \in \mathbb{Q}$ und führen dann einen Widerspruch herbei.

Also: $\sqrt{2} = \frac{p}{q}$ wobei p/q ein gekürzter Bruch ist, d.h. p und q seien teilerfremd, d.h. $\text{gg}(p, q) = 1$.

Durch Quadrieren folgt: $2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2$ (*) und somit ist p^2 eine gerade Zahl.

Denn q ist nach Voraussetzung eine natürliche Zahl, damit ist q^2 ebenfalls eine natürliche Zahl und damit ist $2q^2$ eine gerade natürliche Zahl und somit ist $p^2 = 2q^2$ eine gerade Zahl.

Nun haben wir aber vorhin gezeigt, dass aus n^2 gerade folgt, dass n auch gerade sein muss.

D.h. da p^2 gerade ist, folgt dass p auch gerade ist. D.h. es gilt $p = 2k$ für ein $k \in \mathbb{Z}$

Nun müssen wir noch zeigen, dass q auch gerade ist.

$p = 2k$ in (*) eingesetzt ergibt: $2q^2 = p^2 = (2k)^2 = 4k^2 \Rightarrow q^2 = 2k^2$

Und damit ist $q^2 = 2k^2$ gerade und somit muss auch q auch gerade sein – aus demselben Grund wie vorhin.

Wenn aber beide Zahlen gerade sind, haben sie (zumindest) den gemeinsamen Faktor 2.

Das ist aber ein Widerspruch zur Annahme, dass p und q teilerfremd sind. Somit ist die Annahme falsch und somit ist der Satz $\sqrt{2} \notin \mathbb{Q}$ bewiesen.

Mengen, Funktionen, Folgen & Reihen

Mengenlehre

Definition

Eine **Menge** ist eine ungeordnete Zusammenfassung wohldefinierter, **unterscheidbarer Objekte**, genannt **Elemente**, zu einem Ganzen.

Für irgend ein Objekt x gilt dann bezüglich der Menge A entweder $x \in A$ oder dann $x \notin A$.

Bsp. Menge aller natürlichen Zahlen kleiner 101

$A = \{0, 1, 2, \dots, 99, 100\}$ oder $A = \{n \in \mathbb{N} : n \leq 100\} = \{n \mid n \in \mathbb{N} \wedge n \leq 100\}$ («|» - pipe, heisst **für die gilt**)

Bekannte Mengen ($\mathbb{N}, \mathbb{Z}, \mathbb{Z}^+, \mathbb{R}, \mathbb{C}$)

Example

Einige bekannte Mengen sind:

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$,	Menge der natürlichen
$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$	Menge der ganzen Zahlen
$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$	Menge der positiven ganzen Zahlen
$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z} \wedge q \in \mathbb{N} \setminus \{0\} \right\}$	Menge der Brüche
\mathbb{R}	Menge der reellen Zahlen
\mathbb{C}	Menge der komplexen Zahlen (siehe IMATH)

Es braucht \mathbb{R} , denn die Gleichung $x^2 = 2$ hat in \mathbb{Q} keine Lösung. Analog braucht es \mathbb{C} , denn die Gleichung $x^2 = -1$ hat in \mathbb{R} keine Lösung.

Spezielle Mengen

Teilmenge (\subset)

A ist **Teilmenge** von B, geschrieben $A \subset B$, genau dann, wenn
 $\forall x(x \in A \rightarrow x \in B)$: Es gilt $A \subset A$!

Leere Menge (\emptyset)

Für jede Menge A gilt: $\emptyset \subset A$.

Kardinalität ($|A|$) - Anzahl Elemente

Ist S eine endliche Menge, dann bezeichnet $|S|$ die **Kardinalität** (Anzahl Elemente) von S. Eine nicht endliche Menge heisst unendliche Menge.

Potenzmenge (2^S)

Die Potenzmenge P(S) oder 2^S der Menge S besteht aus der Menge aller Teilmengen $A \subset S$.

Bsp. Potenzmenge von M = {1,2,3}.

-> $P(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2,3\}, \{1,2\}, \{1,3\}, \{2,3\}\}$

Gleiche Mengen (=)

$A = B$, falls A dieselben Elemente wie B enthält.

Gleichmächtige Menge ($|A|=|B|$)

Zwei Mengen A und B heissen **gleichmächtig**, wenn sie die **gleiche Anzahl Elemente** haben, d.h. $|A| = |B|$.

Achtung $|A|$ bedeutet **nicht Betrag**.

Kreuzprodukt (x)

xt: (oder **kartesisches Produkt**) zweier Mengen A und B, bezeichnet mit $A \times B$ ist die Menge aller geordneten Paare (a, b) , wobei $a \in A$ und $b \in B$, d.h.
 $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

Bsp. $A \times B$ und $B \times A$, falls $A = \{1,2,3\}$ und $B = \{a,b\}$ (**Achtung** $A \times B$ nicht gleich $B \times A$, Kommutativgesetz gilt nicht)

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

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

Mengenoperationen

Komplement (\overline{A})

Komplement von A bezüglich/in M heisst. Alle Elemente der Menge M ohne die Elemente der Menge A.

Also: Komplementärmenge $L = M \setminus A$ oder $A^c = \overline{A} = \{m \in M : m \notin A\}$

Bsp. $A = \{a,b,c\}$, $M = \{a,b,c,d,e,f\}$

$\overline{A} = \{d,e,f\}$

Durchschnitt (\cap)

Elemente welche in A und in B vorhanden sind.

$$A \cap B = \{ m \in M \mid \underbrace{m \in A \wedge m \in B}_{\text{und}} \}$$

Vereinigung (\cup)

Alle Element von A plus alle Elemente von B.

$$A \cup B = \{ m \in M \mid \underbrace{m \in A \vee m \in B}_{\text{oder}} \}$$

Differenz (-)

$B - A$ ist gleich alle Elemente von B minus die Elemente von A. Auch $B \setminus A$.

$$B - A = \{ m \in M \mid \underbrace{m \in B \wedge m \notin A}_{\text{und}} \}$$

Zusammenfassung der Regeln

$A \cup B = B \cup A$	Kommutativgesetz
$A \cap B = B \cap A$	Kommutativgesetz
$A \cup (B \cup C) = (A \cup B) \cup C$	Assoziativgesetz
$A \cap (B \cap C) = (A \cap B) \cap C$	Assoziativgesetz
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributivgesetz
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributivgesetz
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's Gesetz
$\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's Gesetz.

Die duale Rechenregel (jeweils auf den Zeilen 2, 4, 6 und 8, erhält man, indem man \cap und \cup vertauscht und \emptyset mit der Universalmenge M (falls diese vorkommen).

Funktionen ($f(x)$)Einführung

Jedem x-Wert darf nur ein y-Wert zugeordnet werden. Sobald einem x-Wert zwei oder mehrere y-Werte zugeordnet sind, ist es keine Funktion.

Schreibweise

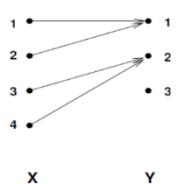
$X \rightarrow f(x)$ oder $f: X \rightarrow Y$ $f = \text{Funktion}, f(x) = \text{Wert der Funktion } f \text{ an der Stelle } x.$

Definitionsbereich (x)

Alle Punkte an denen gemessen wird. Ein x kann nur einem y zugeordnet werden. Bsp. Person -> Eine Grösse.

Wertebereich = Bildbereich = Bildmenge (y)

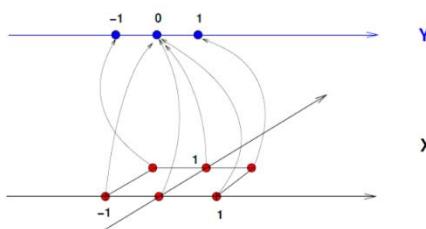
Resultate/Werte an den Punkten x. Ein y kann mehrere x haben. Bsp. Eine Grösse -> mehrere Personen.

Bsp. Bildmenge

→ Damit ist die Bildmenge von f: $f(X) \subset Y = \{1; 2\}$

Weitere FunktionenMehrdimensionale Funktionen

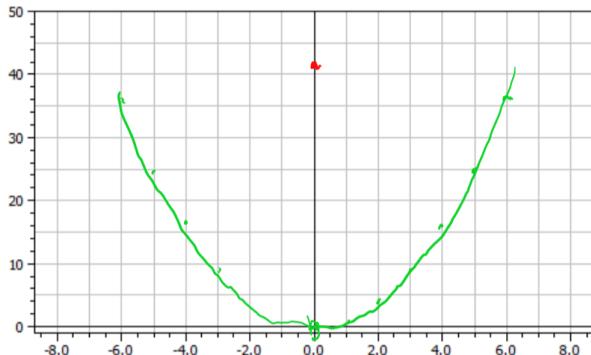
$X = \mathbb{R} \times \mathbb{R}$ und $Y = \mathbb{R}$



Stückweise Definition von (reellen) Funktionen

$$g: \mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto g(x) = \begin{cases} x^2 & \text{für } x \neq 0 \\ 42 & \text{für } x = 0 \end{cases}$$



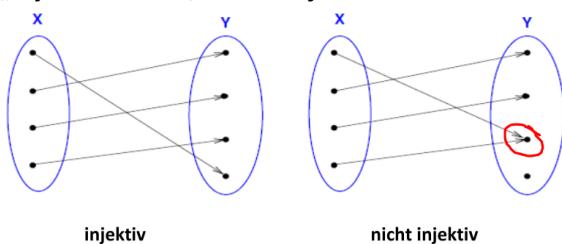
Spezielle Funktionen / Funktionseigenschaften

Wurzelziehen ($DB \geq 0$)

$f(x) = \sqrt{x} \rightarrow \sqrt{9} = 3 \text{ und nicht } \{3, -3\}$. Denn $3^2 = (-3)^2 = 9$.

Injektive Funktion (Auf jedes Y zeigt höchstens ein X)

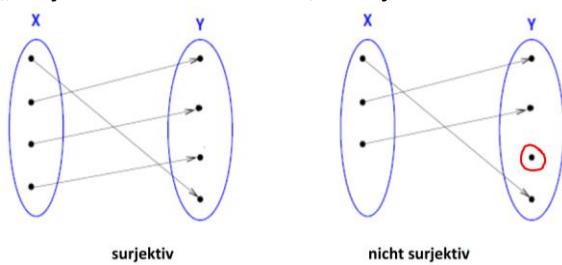
„Injektiv“ heisst, dass auf jedes Element in Y höchstens ein Pfeil zeigt.



Surjektive Funktion (Jedes Y hat min. ein X)

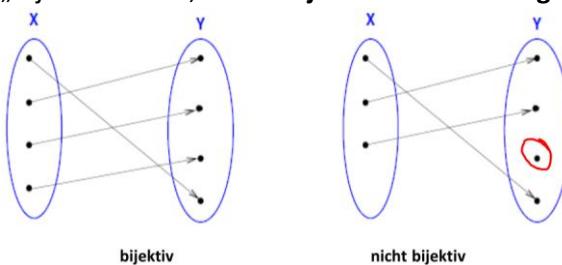
„Surjektiv“ heisst, dass auf jedes Element in Y mindestens ein Pfeil zeigt.

„Surjektiv“ bedeutet auch, dass jedes Y als Funktionswert vorkommt, d.h. $f(X) = Y = WB$.



Bijektive Funktion (Injektiv und Sujektiv = Jedes Y genau ein X)

„Bijektiv“ heisst, dass auf jedes Element in Y genau ein Pfeil zeigt.

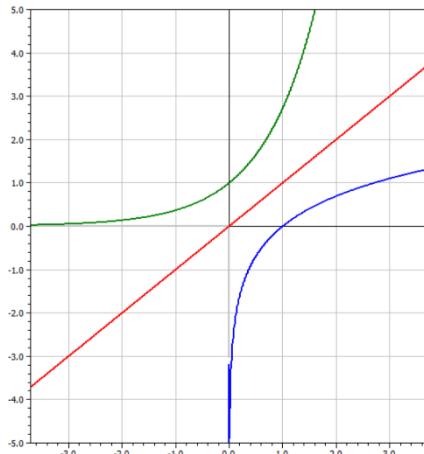


Der Graph der Funktion

$$y = f(x) = e^x$$

$$y = g(x) = x$$

$$y = h(x) = \ln x$$



Zusammengesetzte Funktionen

Es sei $f(x) = x^2$ und $g(x) = \log_{10} x = \lg x$

Quadrieren, dann logarithmieren	Logarithmieren, dann quadrieren
$g(f(x)) = (g \circ f)(x) = \lg x^2$	$f(g(x)) = (f \circ g)(x) = (\lg x)^2$

1. Die Verkettung $f \circ g$ liest man von rechts nach links: „Zuerst g dann f “.
2. „ \circ “ ist das Zeichen für die Verkettung, $f \circ g$ liest man „ f Ring g “.
3. Die Reihenfolge ist wichtig!!
4. Eine Anwendung ist die Kettenregel beim Ableiten von Funktionen. Siehe dazu Ihr Analysismodul.

Bsp. Es sei $f(x) = x^2$ und $g(x) = 3x$

Das Hintereinander Ausführen von zwei Funktionen können wir nun wie folgt schreiben:

- I) $r(x) = (f \circ g)(x) = f(g(x)) = f(3x) = (3x)^2$. Dabei bedeutet hier, dass g die innere und f die äußere Funktion ist. D.h. zuerst $3x$ rechnen, dann das Resultat Quadrieren. Vereinfacht man das Ganze, dann erhält man $r(x) = 9x^2$.
- II) $s(x) = (g \circ f)(x) = g(f(x)) = g(x^2) = 3 \cdot (x^2)$. Dabei bedeutet hier, dass f die innere und g die äußere Funktion ist. D.h. zuerst Quadrieren, dann das Resultat mal 3 rechnen. Vereinfacht man das Ganze, dann erhält man $s(x) = 3x^2$.
- III) Somit ist auch sofort ersichtlich, dass $f(g(x)) \neq g(f(x))$ ist.

Die Umkehrfunktion

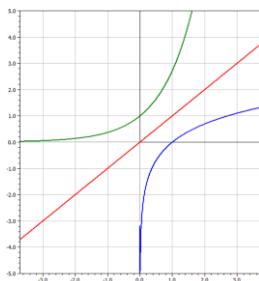
Wir betrachten eine **bijektive Funktion f** , d.h. insbesondere, dass zu **jedem y des Wertebereichs von f genau ein x des Definitionsbereiches von f mit der Eigenschaft $y = f(x)$ existiert. Somit können wir die Umkehrfunktion f^{-1} von f definieren, die jedem Element y des Wertebereichs von f dieses eindeutig bestimmte Element x zuordnet.**

Bsp. $f(x) = e^x$

1. Auflösen von $y = f(x)$ in $x = f^{-1}(y)$

$$f(x) = e^x \rightarrow x = \ln(y) \quad \rightarrow \text{noch die gleiche Punktemenge}$$

2. Variablentausch $x \leftarrow \rightarrow y \quad \rightarrow$ ergibt die neue Punktemenge $y = f^{-1}(x) = h(x) = \ln(x)$



Beispiel 3.20 = Fortsetzung der Aufgabe 3.9:

Wir hatten $y = f(x) = \frac{3x+4}{x+2}$ und $x = f^{-1}(y) = \frac{4-2y}{y-3}$

Es gilt:

$$\begin{aligned} f^{-1}(f(x)) &= \frac{4-2f(x)}{f(x)-3} = \frac{4-2 \cdot \frac{3x+4}{x+2}}{\frac{3x+4}{x+2}-3} = \frac{4-\frac{6x+8}{x+2}}{\frac{3x+4}{x+2}-3} = \frac{\frac{4(x+2)}{x+2}-\frac{6x+8}{x+2}}{\frac{3x+4}{x+2}-\frac{3(x+2)}{x+2}} \\ &= \frac{\frac{4x+8-(6x+8)}{x+2}}{\frac{3x+4-3(x+2)}{x+2}} = \frac{\frac{4x+8-6x-8}{x+2}}{\frac{3x+4-3x-6}{x+2}} = \frac{4x+8-6x-8}{3x+4-3x-6} = \frac{-2x}{-2} = x \end{aligned}$$

Die ceiling- und die floor-Funktion (Aufrund- / Abrundfunktion)

Ceiling-Funktion $\lceil \cdot \rceil: \mathbb{R} \rightarrow \mathbb{Z}, x \mapsto \lceil x \rceil = \min\{n \in \mathbb{Z} \mid x \leq n\}$

→ nächst grösste ganze Zahl.

Bsp.: $\lceil 4.5 \rceil = 5, \lceil 25/6 \rceil = 5$ (weil $25/6 = 4.166$)



Floor-Funktion $\lfloor \cdot \rfloor: \mathbb{R} \rightarrow \mathbb{Z}, x \mapsto \lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}$

→ nächst kleinere ganze Zahl.

Bsp.: $\lfloor 4.5 \rfloor = 4, \lfloor 5.99 \rfloor = 5, \lfloor 6/3 \rfloor = 2$



Folgen

Zahlenfolgen sind **Elemente einer Zahlenmenge**, welche in einer **bestimmten Reihenfolge angeordnet** sind. D.h. Die Reihenfolge ist sehr wichtig.

Typische Form: $a_k = a_1 + ? \cdot 5$ (Bsp. das unterschied gleich 5)

Einige spezielle Folgen

Folge	Folgeglieder $\{a_k\} = (a_k) = a_1, a_2, a_3, \dots$	Folgeglieder $\{a_k\} = (a_k) = a_0, a_1, a_2, a_3, \dots$
(n)	$= (1, 2, 3, 4, 5, 6, \dots)$	$= (0, 1, 2, 3, 4, 5, 6, \dots)$
(n^2)	$= (1, 4, 9, 16, 25, 36, \dots)$	$= (0, 1, 4, 9, 16, 25, 36, \dots)$
(n^3)	$= (1, 8, 27, 64, 125, 216, \dots)$	$= (0, 1, 8, 27, 64, 125, 216, \dots)$
(n^4)	$= (1, 16, 81, 256, 625, 1296, \dots)$	$= (0, 1, 16, 81, 256, 625, 1296, \dots)$
(2^n)	$= (2, 4, 8, 16, 32, 64, \dots)$	$= (1, 2, 4, 8, 16, 32, 64, \dots)$
(3^n)	$= (3, 9, 27, 81, 243, 729, \dots)$	$= (1, 3, 9, 27, 81, 243, 729, \dots)$
$(n!)$	$= (1, 2, 6, 24, 120, 720, 5040, \dots)$	$= (0, 1, 2, 6, 24, 120, 720, 5040, \dots)$

Folge	das k-te Glied bei a_1, \dots	das k-te Glied bei a_0, \dots
(a) $(a_k) = (0, 1, 2, 3, 4, \dots)$	$a_k = k - 1$	$a_k = k$
(b) $(b_k) = (1, -2, 3, -4, 5, -6, \dots)$	$b_k = (-1)^{k+1} \cdot k$	$b_k = (-1)^k \cdot (k+1)$
(c) $(c_k) = (1, 4, 9, 16, 25, 36, 49, \dots)$	$c_k = k^2$	$c_k = (c_{k-1} + 1)^2$
(d) $(d_k) = \left(1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \frac{1}{64}, \dots\right)$	$d_k = \frac{1}{2^{k-1}}$	$d_k = \frac{1}{2^k}$

Bei **alternierenden Folgen** (wie bei b), d.h. das **Vorzeichen wechselt stetig**. Wird immer der gleiche Trick angewandt.

Multiplizieren zweier Terme wobei **einer negativ** ist und eine **Potenz** hat.

$$\rightarrow (-1)^k \text{ oder } (-1)^{k+1}$$

Eine wichtige Überlegung

Es gibt **nicht immer** eine Formel für das **k-te Glied**.

Arithmetische Folge (Differenz Konstant)

Für eine arithmetische Folge gilt: $a_{k+1} - a_k = d = \text{konstant}$.

Kennt man das k-Glied, dann kann man das Folgeglied leicht berechnen.

Nachteil: Berechnung von hohen Gliedern wie a_{10000} ausser a_{9999} wäre gegeben.

Bsp. $a_1 = 9; a_2 = 14; a_3 = 19$ → $d = 5$ & $a_1 = 9$

Geometrische Folge (Quotient Konstant)

Für eine geometrische Folge gilt: $\frac{a_{k+1}}{a_k} = q = \text{konstant}$.

Kennt man das k-Glied, dann kann man das Folgeglied leicht berechnen.

Nachteil: Berechnung von hohen Gliedern wie a_{10000} ausser a_{9999} wäre gegeben.

Funktionale Darstellung der geometrischen folge GF

- Sei $\{a_k\} = (a_k) = a_0, a_1, a_2, a_3, \dots$ eine GF mit Quotient q, dann gilt: $a_n = a_0 \cdot q^n$
- Sei $\{a_k\} = (a_k) = a_1, a_2, a_3, \dots$ eine GF mit Quotient q, dann gilt: $a_n = a_1 \cdot q^{n-1}$
- Sei $\{a_k\} = (a_k) = a_2, a_3, a_4, \dots$ eine AF mit Differenz d, dann gilt: $a_n = a_2 \cdot d^{n-2}$ $a_n = a_{n-1} + d$
resp. $a_n = a_1 + (n-1) * d$

Bsp. $a_1 = 8; a_2 = 12; a_3 = 18; a_4 = 27; a_5 = 40,5$

$$\text{Berechne } a_{12}: \rightarrow q = \frac{12}{8} = \frac{3}{2} \rightarrow a_{12} = 8 \cdot \left(\frac{3}{2}\right)^{11} = 691.98 \quad (a_n = a_1 \cdot q^{n-1})$$

Reihen

Summenzeichen

$$\sum_{i=m}^n a_i = a_m + a_{m+1} + a_{m+2} + a_{m+3} + \dots + a_n$$

für $n, m \in \mathbb{Z}$ und $n \geq m$

\underline{n} Summationsobergrenze
 \underline{m} Summationsuntergrenze
 \underline{i} Summationsindex:
 i erhöht sich beim nachfolgenden Summanden um 1
 i beginnt bei der Summationsuntergrenze m
 i endet mit der Summationsobergrenze n

Bsp.

$$\sum_{k=1}^4 (2k - 1) = \left(2 \cdot \sum_{k=1}^1 - 1\right) + \left(2 \cdot \sum_{k=2}^2 - 1\right) + \left(2 \cdot \sum_{k=3}^3 - 1\right) + \left(2 \cdot \sum_{k=4}^4 - 1\right) = 1 + 3 + 5 + 7 = 16$$

Produktzeichen

$$\prod_{i=m}^n a_i = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot a_{m+3} \cdot \dots \cdot a_n$$

für $n, m \in \mathbb{Z}$ und $n \geq m$

\underline{n} Summationsobergrenze
 \underline{m} Summationsuntergrenze
 \underline{i} Summationsindex:
 i erhöht sich beim nachfolgenden Summanden um 1
 i beginnt bei der Summationsuntergrenze m
 i endet mit der Summationsobergrenze n

Bsp.

$$\prod_{r=5}^8 \frac{r}{r+2} = \frac{5}{5+2} \cdot \frac{6}{6+2} \cdot \frac{7}{7+2} \cdot \frac{8}{8+2} = \frac{5}{7} \cdot \frac{6}{8} \cdot \frac{7}{9} \cdot \frac{8}{10} = \frac{1680}{5040} = \frac{1}{3}$$

Fakultät (Anwendung von Produktzeichen)

$$n! = \begin{cases} 1 \cdot 2 \cdot 3 \cdot \dots \cdot n = \prod_{i=1}^n i & \text{für } n > 0, n \in \mathbb{N} \\ 1 & \text{für } n = 0 \end{cases}$$

gesprochen: "n Fakultät"

→ Achtung: $0! = 1$

Bsp.

$$3! \cdot 5! = (3 \cdot 2 \cdot 1) \cdot (5 \cdot 4 \cdot 3 \cdot 2 \cdot 1) = 720$$

Definitionen

Eine Reihe ist die Summe der Glieder einer Folge. Sie entsteht aus einer arithmetischen bzw. geometrischen Folge.

- Die neue Folge $\{s_n\}$ mit $s_i = a_1 + a_2 + a_3 + \dots + a_i$ resp. $\{s_n\}$ mit $s_i = a_0 + a_1 + a_2 + \dots + a_i$ heisst Reihe.
- Entsteht die Reihe aus einer arithmetischen Zahlenfolge, so heisst sie arithmetische Reihe.
- Entsteht die Reihe aus einer geometrischen Zahlenfolge, so heisst sie geometrische Reihe.

Beispiel 5.4:

$$\begin{aligned} S_2 &= a_1 + a_2 = 1+2 = 3 \\ S_3 &= a_1 + a_2 + a_3 = 1+2+3 = 6 \end{aligned}$$

Folge	Folge $\{a_k\} = (a_k) = a_1, a_2, a_3, \dots$	Reihe $\{s_k\} = (s_k) = s_1, s_2, s_3, \dots$
	$s_1 = a_1$	$s_1 = a_1$
(n)	$= (1, 2, 3, 4, 5, 6, \dots)$	$= (1, 3, 6, 10, 15, 21, \dots)$
(n^2)	$= (1, 4, 9, 16, 25, 36, \dots)$	$= (1, 5, 19, 30, 55, 91, \dots)$
(n^3)	$= (1, 8, 27, 64, 125, 216, \dots)$	$= (1, 9, 36, 100, 225, 441, \dots)$
(n^4)	$= (1, 16, 81, 256, 625, 1296, \dots)$	$= (1, 17, 98, 354, 979, 2275, \dots)$
(2^n)	$= (2, 4, 8, 16, 32, 64, \dots)$	$= (2, 6, 14, 30, 62, 126, \dots)$
(3^n)	$= (3, 9, 27, 81, 243, 729, \dots)$	$= (3, 12, 39, 120, 363, 1029, \dots)$
$(n!)$	$= (1, 2, 6, 24, 120, 720, 5040, \dots)$	$= (1, 3, 9, 33, 153, 873, 5913, \dots)$

Rekursive Darstellung einer Reihe

$$S_{n+1} = S_n + a_{n+1}$$

Formeln für arithmetische Reihe

Mit a_1 :

Sei $\{a_k\} = (a_k) = a_1, a_2, a_3, \dots$ eine AF mit Differenz d , dann gilt: $a_n = a_1 + (n - 1) \cdot d$

$$\textcircled{A} \quad s_n = \sum_{i=1}^n a_i = \frac{n}{2}(a_1 + a_n) \quad (*)$$

Oder

$$s_n = \sum_{i=1}^n a_i = \frac{n}{2}(a_1 + a_1 + (n - 1)d) = \frac{n}{2}(2a_1 + (n - 1) \cdot d) = na_1 + \frac{n(n - 1)}{2}d$$

Mit a_0 :

Sei $\{a_k\} = (a_k) = a_0, a_1, a_2, a_3, \dots$ eine AF mit Differenz d , dann gilt: $a_n = a_0 + n \cdot d$ und

$$s_n = \sum_{i=0}^n a_i = \frac{n+1}{2}(a_0 + a_n)$$

Oder

$$s_n = \sum_{i=0}^n a_i = \frac{n+1}{2}(2a_0 + n \cdot d) = (n+1)a_0 + \frac{n(n+1)}{2} \cdot d$$

Bsp. alle Zahlen von 1 – 100 zusammenzählen

Es ist ja eine AF mit $a_1 = 1$ und $d = 1$, also

$$\textcircled{B} \quad s_{100} = \sum_{i=1}^{100} a_i = \frac{100}{2}(1 + 100) = 50 \cdot 101 = 5050$$

$$\textcircled{C} \quad s_{100} = \sum_{i=1}^{100} a_i = \frac{100}{2}(2 \cdot 1 + (100 - 1) \cdot 1) = 50(2 + 99) = 5050$$

$$\textcircled{D} \quad s_{100} = \sum_{i=1}^{100} a_i = 100 \cdot 1 + \frac{100(100 - 1)}{2} \cdot 1 = 100 + \frac{100 \cdot 99}{2} = 5050$$

Formeln für geometrische Reihe

Mit a_1 :

Sei $\{a_k\} = (a_k) = a_1, a_2, a_3, \dots$ eine GF mit Quotient q , dann gilt: $a_n = a_1 \cdot q^{n-1}$ und

$$s_n = \sum_{i=1}^n a_i = a_1 \cdot \frac{1 - q^n}{1 - q} = \textcircled{a_1} \cdot \frac{q^n - 1}{q - 1} \quad \text{für } q \neq 1 \quad (**)$$

$$s_n = \sum_{i=1}^n a_i = n \cdot a_1 \quad \text{für } q = 1$$

Mit a_0 :

Sei $\{a_k\} = (a_k) = a_0, a_1, a_2, a_3, \dots$ eine GF mit Quotient q , dann gilt: $a_n = a_0 \cdot q^n$

$$s_n = \sum_{i=0}^n a_i = a_0 \cdot \frac{1 - q^{n+1}}{1 - q} = \textcircled{a_0} \cdot \frac{q^{n+1} - 1}{q - 1} \quad \text{für } q \neq 1$$

$$s_n = \sum_{i=0}^n a_i = (n + 1) \cdot a_0 \quad \text{für } q = 1$$

Komplexe Matrizen

Algorithmen

Ein Algorithmus ist eine **endliche Menge von präzisen Instruktionen** mit deren Hilfe eine Berechnung ausgeführt oder ein Problem gelöst wird.

Bsp. Euklidischer Algorithmus um den ggT zu berechnen.

Eigenschaften

- Einen genau spezifizierten Input und daraus berechneten Output
- Die Instruktionen sind präzise, korrekt für jeden möglichen Input und in endlicher Zeit durchführbar.

Wachstum von Funktionen (Big O-Notation)

Definition

Seien f und g Funktion von \mathbb{Z} oder (\mathbb{R}) nach \mathbb{R} . Dann sagt man " $f(x)$ ist $\mathcal{O}(g(x))$ ", falls es Konstanten C und k gibt, so dass gilt:

$|f(x)| \leq C|g(x)|, \forall x > k$ Lies: " $f(x)$ ist gross-O von $g(x)$ "; man schreibt: $f(x) \in \mathcal{O}(g(x))$.

Die Konstanten **C** und **k** heissen Zeugen.

C: Summe aller Konstanten. (Bsp. $2x^2 + 3x + 1 = |2| + |3| + |1| = 6$)

k: $O(?)$ gilt für alle x grösser als **k** = $\forall x > k$

Bsp. $2x^2 - 3x + 1$

1. Zuerst bestimmen welcher Term der am schnellst wachsende ist. Hier **x^2** .
2. Alle anderen Terms als **x^2** darstellen und **k** bestimmen. Wobei **k** bestimmt, ab welchem Wert die Terme (3x und 1) kleiner als der schnellstwachsende Term sind(x^2).
 - a. $3 \cdot 0 > 0^2, 3 \cdot 1 > 1^2, 3 \cdot 2 > 2^2, 3 \cdot 3 \leq 3^2 \rightarrow$ Sobald $x > 3$ ist $\rightarrow k = 3$.
 - b. Wenn $x > 3$ ist, dann gilt auch für den zweiten Term, 1, $1 \leq 3^2$.
3. Alle BeträgenKoeffizienten zusammenzählen
 - a. $2 + 3 + 1 = 6 \rightarrow C = 6$
4. Resultat bestimmen. $\rightarrow f(x) \in \mathcal{O}(x^2)$, mit Zeugen $C = 6$ und $k = 3$.

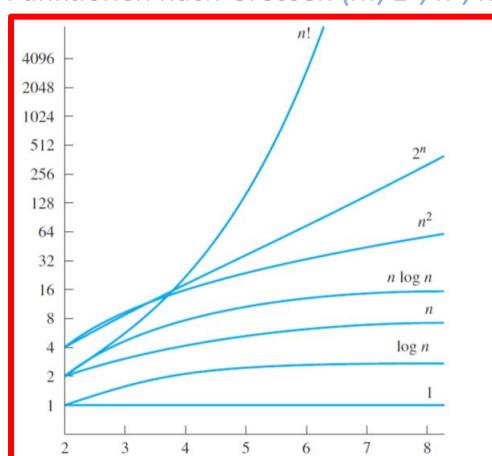
Bsp. $f(x) = 2^x$

$\rightarrow f(x) \in \mathcal{O}(2^x)$, mit Zeugen $C = 1$ und $k = 0$, denn $|f(x)| = |2^x| \leq 1 \cdot |2^x| \forall x > 0$

Bsp. $f(x) = 2^{x+1}$

$\rightarrow f(x) \in \mathcal{O}(2^x)$, mit Zeugen $C = 2$ und $k = 0$, denn $2^{x+1} = 2^1 \cdot 2^x \rightarrow |f(x)| = 2 \cdot |2^x| \leq 2 \cdot |2^x| \forall x > 0$

Funktionen nach Größen ($n!$, 2^n , n^2 , $n \log n$, n , $\log n$, 1)



Dabei nennt man:

- $\mathcal{O}(1)$ constant
- $\mathcal{O}(\log(n))$ logarithmic
- $\mathcal{O}(n)$ linear
- $\mathcal{O}(n \cdot \log(n)) = \mathcal{O}(\log(n^n))$ ploylogarithmic
- $\mathcal{O}(n^2)$ quadratic
- $\mathcal{O}(n^c)$ polynomial
- $\mathcal{O}(2^n)$ (gilt auch für $\mathcal{O}(e^n)$) exponential
- $\mathcal{O}(n!)$ (gilt auch für $\mathcal{O}(n^n)$) factorial

Wachstum von Polynomen (=Mehrgliedriger Term)

Bsp.: Wir zeigen, dass $f(x) = x^2 + 2x + 1$ ist $\mathcal{O}(x^2)$, d.h. $f(x) \in \mathcal{O}(x^2)$.

Lösung: Wir betrachten nur reelle Zahlen x mit $x > 1$. Für diese Zahlen gilt auch $x^2 > x$ und $x^2 > 1$ und weiterhin (da f in diesem Bereich nur positive Werte annehmen kann):

$$|x^2 + 2x + 1| = x^2 + 2x + 1 \leq x^2 + 2x^2 + x^2 = 4x^2$$

Schnellst wachsender Term

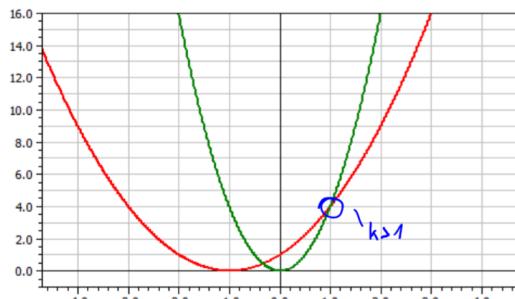
Die anderen Terme mit x^2 abschätzen

Insgesamt haben wir also gezeigt: Für alle $x > 1$ gilt

$$|x^2 + 2x + 1| \leq 4|x^2|$$

also $f(x) = x^2 + 2x + 1$ ist $\mathcal{O}(x^2)$ mit den Zeugen $k = 1$ und $C = 4$.

Anhand der Graphik mit $f(x) = x^2 + 2x + 1$ und $g(x) = 4x^2$ sehen wir, dass $g(x)$ ab $k = 1$ schneller als $f(x)$ wächst.



→ Wir benötigen unbedingt den Zeugen $k = 1$, denn die Abschätzung $x < x^2$ gilt (für positive, reelle Zahlen) nur für $x > 1$.

Für $x = 1$ ist $x = x^2$ und für $0 < x < 1$ gilt $x > x^2$, z.B. $0,5 > 0,25 = 0,25$

- I) Funktionen der Form $y = f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, mit $a_n \neq 0$ und $n \in \mathbb{N}$, heißen **Polynome n-ten Grades**.
- II) Kurzschreibweise: $y = f(x) = \sum_{k=0}^n a_k \cdot x^k$
- III) Die höchste Potenz heißt „Grad“ des Polynoms.
- IV) Die Koeffizienten $a_k \in \mathbb{R}$ sind beliebige, aber feste reelle Zahlen.

→ Polynom n-ten Grades wächst $\mathcal{O}(x^n)$. Berechnung von C. D.h. es kann immer mit der grössten Potenz abgeschätzt werden.

→ Für die Zeugen gilt: **k = 1** (immer bei Polynom n-ten Grades) und **C = Summe der Beträge (+) der Koeffizienten**.

Bsp. $x^2 + 2x + 1$

$$1 \cdot x^2 + 2 \cdot x + 1 \rightarrow 1 \cdot x^2 + 2 \cdot x^2 + 1 \cdot x^2 (2x < x^2 \text{ wenn } k > 1) \rightarrow 4x^2$$

Oder:

$$f(x) = x^2 + 2x + 1 = x^2 \left(1 + 2 \cdot \frac{1}{x} + \frac{1}{x^2} \right) \leq x^2 (1 + 2 + 1) = 4x^2$$

x^2 ausklammern

Die Abschätzungen $\frac{1}{x} \leq 1$ und $\frac{1}{x^2} \leq 1$ gelten jeweils für $x > 1$ und damit ist – wir vorher $k = 1$ und $C = 4$

Bsp. Polynom 3-ten Grades

$$y = f(x) = x^3 + 2x^2 - 13x + 10$$

$$C = \sum_{k=0}^n |a_k| = |1| + |2| + |-13| + |10| = 1 + 2 + 13 + 10 = 26$$

Wachstum von weiteren Funktionen (Log- & Potenz-Gesetze)

Potenzgesetze	Logarithmengesetze
$a^r \cdot a^s = a^{r+s}$	$\log_a(u \cdot v) = \log_a(u) + \log_a(v)$
$\frac{a^r}{a^s} = a^{r-s}$	$\log_a\left(\frac{u}{v}\right) = \log_a(u) - \log_a(v)$
$(a^r)^s = (a^s)^r = a^{rs}$	$\log_a(u^v) = v \cdot \log_a(u)$

Fakultät

$n!:$ Abgeschätzt ist $f(n) = n! \in \mathcal{O}(n^n)$, mit Zeugen $C = 1$ und $k = 1$.

Logarithmus

$\log n!:$ Abgeschätzt ist $f(n) = \log n! \in \mathcal{O}(n \cdot \log n)$, mit Zeugen $C = 1$ und $k = 1$.

$$\log n! \approx \log \left[\sqrt{2\pi n} \cdot \left(\frac{n}{e} \right)^n \right]$$

Bsp. $f(n) = 3n \cdot \log(n!) + (n^2 + 3) \cdot \log n$

$$\begin{aligned} |f(n)| &= |3n \log(n!) + (n^2 + 3) \log n| \\ &= 3n \cdot \underbrace{\log(n!)}_{\leq n \log(n), \forall n > 1} + \underbrace{(n^2 + 3)}_{\leq 4n^2, \forall n > 1} \log n \\ &\leq 3n^2 \cdot \log(n) + 4n^2 \log(n) \quad \text{falls } n > 1 \\ &= 7n^2 \log(n) \quad \text{falls } n > 1 \end{aligned}$$

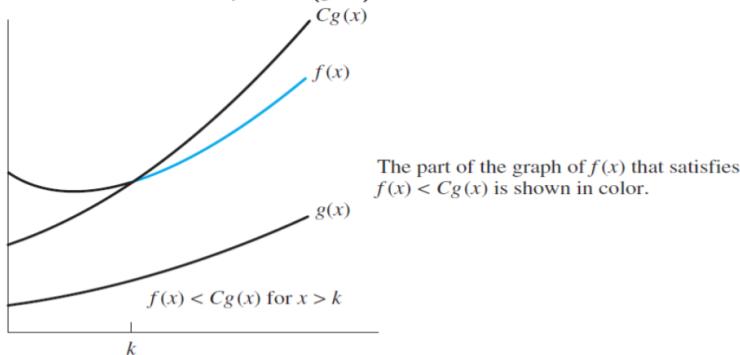
Also ist $f(n) \in \mathcal{O}(n^2 \log n)$ mit den Zeugen $C = 7$ und $k = 1$.

*(Eine solche Aufgabe könnte an der Prüfung kommen)

Allgemeine (Graphische) Betrachtung

Nun betrachten wir nochmals die graphische Interpretation von $|f(x)| \leq C \cdot |g(x)| \forall x > k$.

Aus KR, p.208, Figure 2 The $f(x)$ is $\mathcal{O}(g(x))$.



Zahlen und Division

Einführung

Typische Abschätzungen in der Informatik.

$$2^{10} = 1024 \approx 1000 = 10^3 \Rightarrow 2^{10} \approx 10^3$$

Damit kann man schnelle Abschätzungen machen für einen Schlüssel mit 256 Bit Länge

$$2^{256} = 2^{10 \cdot 25,6} = (2^{10})^{25,6} \approx 10^3^{25,6} = 10^{3 \cdot 25,6} \approx 10^{77}, \text{ was ungefähr der Anzahl der Atome im Weltall bedeutet.}$$

Teilbarkeit ($a|b \rightarrow a \text{ teilt } b$)

Definition

Falls $a, b \in \mathbb{Z}$ mit $a \neq 0$ dann sagt man: a teilt b , falls $\exists c \ (b = ac)$ in der Universalmenge \mathbb{Z} . Dann ist a ein Faktor von b und b ein Vielfaches von a . Man schreibt dann $a|b$ und andernfalls $a \nmid b$.

Falls $a, b, c \in \mathbb{Z}$, dann gilt:

- (a) $a|b \wedge a|c \rightarrow a|(b+c)$,
- (b) $a|b \rightarrow \forall c (a|bc)$,
- (c) $a|b \wedge b|c \rightarrow a|c$.

Beispiel 5.3:

- (a) Es sei $a = 2, b = 4$ und $c = 8$:
- (b) Es sei $a = 2, b = 4$ und c beliebig, z.B. $c = 7$:
- (c) Es sei $a = 2, b = 4$ und $c = 8$:

$$2|4 \wedge 2|8 \Rightarrow 2|(4+8), \text{ d.h. } 2|12.$$

$$2|4 \Rightarrow 2|4c, \text{ z.B. } 2|28.$$

$$2|4 \wedge 4|8 \Rightarrow 2|8.$$

Primzahlen

Definition

Eine positive Zahl $n \in \mathbb{Z}$ grösser als 1 heisst Primzahl, wenn sie lediglich die Faktoren 1 und n hat. Andernfalls heisst die Zahl zusammengesetzt: in diesem Fall gilt: $\exists a (a|n \wedge (1 < a < n))$.

Falls n eine zusammengesetzte Zahl ist, dann hat n (mind.) einen Primzahlteiler kleiner gleich \sqrt{n} .

Fundamentalsatz der Arithmetik

Jede natürliche Zahl $n \geq 2$ kann (eindeutig) als Produkt von Primzahlen geschrieben werden.

$$744776409 = 3 \cdot 13^3 \cdot 17^3 \cdot 23$$

Primfaktorzerlegung

Zahl durch kleinste Primzahl Teilen, falls es dabei keinen Rest gibt, diesen nehmen und wieder durch die kleinste Primzahl teilen. Falls es einen Rest geben sollte, dann die nächst höhere Primzahl wählen und durch diese Teilen, usw.

Mit TR: Factor() → Menu:3:2

Mersenne Primzahlen

Primzahlen der Form $M_n = 2^p - 1$ wobei p eine Primzahl ist, heissen Mersenne Primes.

Anzahl Primzahlen errechnen

Dazu gibt es zunächst die Abschätzung $\pi(x)$ für die Anzahl der Primzahlen kleiner als x :

$$\pi(x) \approx \frac{x}{\ln(x)}$$

Grösstmögliche n -stellige Zahl = $10^n - 1$.

Bsp. Anzahl Primzahlen bis 100-Stellen

$$\text{Es gibt } \pi(x = 10^{100}) \approx \frac{10^{100}}{\ln(10^{100})} \approx \frac{10^{100}}{100 \cdot \ln(10)} \approx \frac{10^{98} \cdot 10^{99}}{10^2 \cdot \ln(10)} \approx \frac{10^{98}}{\ln(10)} \approx \frac{1}{\ln(10)} \cdot 10^{99} \approx 0.43 \cdot 10^{99} = \underline{\underline{4.3 \cdot 10^{97}}} \text{ Primzahlen}$$

Bsp. Anzahl 100-stellige Primzahlen

Anzahl aller Primzahlen bis 100 Stellen – Anzahl aller Primzahlen bis 99 Stellen.

$$\text{Es gibt } \pi(x = 10^{100}) - \pi(x = 10^{99}) \approx \frac{10^{100}}{\ln(10^{100})} - \frac{10^{99}}{\ln(10^{99})} \approx 4.3 \cdot 10^{97} - 4.4 \cdot 10^{96} \approx 4.3 \cdot 10^{97} - 0.44 \cdot 10^{97} \approx 3.9 \cdot 10^{97} \text{ 100-stellige Primzahlen.}$$

ggT und kgV

Der ggT(18; 48) wird wie folgt berechnet:

$$18 = 2 \cdot 3 \cdot 3$$

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$$

Und somit ist $ggT(18; 48) = 2 \cdot 3 = 6$

Das $kgV(18, 48) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 144$

$$ggT(18, 48) \cdot kgV(18, 48) = 6 \cdot 144 = 864 = 18 \cdot 48$$

ggT: → **Mit TR**: Menu:2:5 → **gcd(x,y)**

kgV: → **Mit TR**: Menu:2:4 → **lcm(x,y)**

Formel ggT und kgV gegenseitig berechnen:

$$ggT(a, b) \cdot kgV(a, b) = a \cdot b \Rightarrow kgV(a, b) = \frac{a \cdot b}{ggT(a, b)}$$

Modulare Arithmetik (Modulo)

Die **mod N** Operation ist nichts anderes als die **Angabe eines Restes bei einer Ganzzahldivision durch N**.

→ **Nur der Rest interessiert** uns.

Bsp. 13 mod 5

$13 \text{ mod } 5 = 3$, da $13 : 5 = 2 \text{ Rest } 3$

Eigenschaften

- Für eine ganze Zahl a gilt: $a \text{ mod } N \in \{0; 1; 2; \dots; N - 1\}$
- **Mod N ist eine Äquivalenzrelation**, im Sinne dass **zwei ganze Zahlen äquivalent mod N sind, wenn sie den gleichen Rest mod N haben**. So sind **13** und **38 äquivalent mod 5**: $13 \equiv 38 \equiv 3 \text{ mod } 5$.

Kongruent (\equiv)

Sei $m \in \mathbb{N}$. Dann nennt man zwei ganze Zahlen a und b **kongruent modulo m**, falls $m|(a - b)$ d.h. a und b liegen ein Vielfaches von m auseinander. Man schreibt dann $a \equiv b \text{ mod } m$ und sagt: "a ist kongruent zu b modulo m".

→ Beide Zahlen a & b modulo n ergeben das gleicher Ergebnis. → \equiv bedeutet **kongruent**

Bsp.

$$13 \equiv 1 \text{ mod } 4 \text{ denn } 4|(13 - 1)$$

$$13 \equiv 1 \text{ mod } 3 \text{ denn } 3|(13 - 1)$$

$$13 \not\equiv 1 \text{ mod } 5 \text{ denn } 5 \nmid (13 - 1)$$

Addition und Subtraktion

$$(a + b) \text{ mod } N = (a \text{ mod } N + b \text{ mod } N) \text{ mod } N$$

$$(a - b) \text{ mod } N = (a \text{ mod } N - b \text{ mod } N) \text{ mod } N$$

Bsp.

$$1. (13 + 49) \text{ mod } 5 \equiv 62 \text{ mod } 5 \equiv 2$$

$$2. (13 + 49) \text{ mod } 5 \equiv (13 \text{ mod } 5 + 49 \text{ mod } 5) \text{ mod } 5 \equiv (3+4) \text{ mod } 5 \equiv 2$$

Modulo von negativer Zahl

1. Die negative Zahl mit der beim Modulo zu teilende Zahl addieren bis sie positiv wird.
2. Danach den modulo machen.

Bsp.

$$1. (-13) \text{ mod } 5 \equiv (-13 + 3 \cdot 5) \text{ mod } 5 \equiv 2 \text{ mod } 5 \equiv 2$$

$$2. (13 - 49) \text{ mod } 5 \equiv -36 \text{ mod } 5 \equiv (-36 + 8 \cdot 5) \equiv 4 \text{ mod } 5 \equiv 4$$

Multiplikation

$$(a * b) \bmod N = (a \bmod N * b \bmod N) \bmod N$$

Bsp.

$$1. (13 * 49) \bmod 5 \equiv 637 \bmod 5 \equiv 2$$

$$2. (13 * 49) \bmod 5 \equiv (13 \bmod 5 * 49 \bmod 5) \bmod 5 \equiv (3 * 4) \bmod 5 \equiv 12 \bmod 5 \equiv 2$$

Bsp. $8^9 \bmod 11$ ohne Taschenrechner

$$\begin{aligned} 8^9 \bmod 11 &\equiv (8^2 * 8^2 * 8^2 * 8^2 * 8) \bmod 11 \equiv \left(\underbrace{8^2 \bmod 11}_{=9} * \dots * 8^2 \bmod 11 * 8 \right) \bmod 11 \\ &\equiv (9 * 9 * 9 * 9 * 8) \bmod 11 \equiv (81 * 81 * 8) \bmod 11 \equiv (4 * 4 * 8) \bmod 11 \equiv (16 * 8) \bmod 11 \equiv 5 \\ &\equiv (16 * 8) \bmod 11 \equiv (5 * 8) \bmod 11 \equiv (40) \bmod 11 \equiv 7 \end{aligned}$$

Restklasse

Die Restklasse ist die Menge aller Zahlen, welche denselben Rest modulo N haben.

Bsp. fünf Restklassen modulo 5

$\{\dots, -15, -10, -5, 0, 5, 10, \dots\}$... alle Zahlen mit Rest 0 modulo 5
$\{\dots, -14, -9, -4, 1, 6, 11, \dots\}$... alle Zahlen mit Rest 1 modulo 5
$\{\dots, -13, -8, -3, 2, 7, 12, \dots\}$... alle Zahlen mit Rest 2 modulo 5
$\{\dots, -12, -7, -2, 3, 8, 13, \dots\}$... alle Zahlen mit Rest 3 modulo 5
$\{\dots, -11, -6, -1, 4, 9, 14, \dots\}$... alle Zahlen mit Rest 4 modulo 5

Der euklidische Algorithmus

Berechnen vom ggT

Berechne den ggT(67, 24)	Berechne den ggT(201, 72)
$67 = 2 \cdot 24 + 19$	$201 = 2 \cdot 72 + 57$
$24 = 1 \cdot 19 + 5$	$72 = 1 \cdot 57 + 15$
$19 = 3 \cdot 5 + 4$	$57 = 3 \cdot 15 + 12$
$5 = 1 \cdot 4 + 1$	$15 = 1 \cdot 12 + 3$
$4 = 4 \cdot 1 + 0$	$12 = 4 \cdot 3 + 0$

→ Aufwand/Laufzeit vom Euklid Algorithmus ist $O(\log n)$, mit $n = \max(a,b)$. D.h. auch für grosse Zahlen schnell.

Matrizen

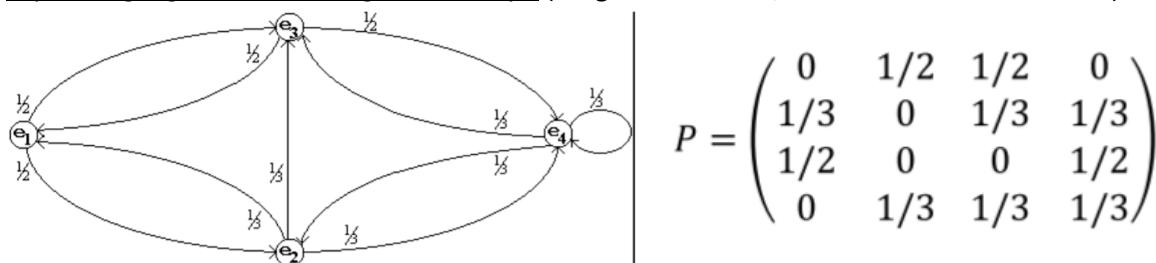
Einführung

Gegeben seien zwei lineare Gleichungen mit zwei Unbekannten.

$$\begin{array}{l} \text{(I)} \quad a_{11}x + a_{12}y = c_1 \\ \text{(II)} \quad a_{21}x + a_{22}y = c_2 \end{array} \quad | \quad A \cdot X = C$$

Man nennt die Zahlen a_{11}, a_{12}, a_{21} und a_{22} Koeffizienten und c_1 und c_2 Konstanten.

Bsp. Übergangsmatrix P zu folgendem Graph (Wege eines Käfers, stehenbleiben darf er nicht)



Definition (Matrix)

Eine $m \times n$ -Matrix ist eine rechteckige Anordnung von Zahlen in m Zeilen (Reihen) und n Spalten. Für eine quadratische Matrix gilt $m = n$.

$$A = \begin{bmatrix} \text{Zeile 1} & [a_{11} & a_{12} & \cdots & a_{1n}] \\ \vdots & a_{21} & a_{22} & \cdots & a_{2n} \\ \text{Zeile m} & a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \quad \begin{matrix} a_{mn} \\ \text{Zeile} \\ \text{Spalte} \end{matrix}$$

Man schreibt kurz auch $A = [a_{ij}]$. Spalte 1 Spalte n

Bsp. von oben

Wir identifizieren von der obigen allgemeinen Definition und von $P = \begin{pmatrix} 0 & 1/2 & 1/2 & 0 \\ 1/3 & 0 & 1/3 & 1/3 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/3 & 1/3 & 1/3 \end{pmatrix}$

- Anzahl Spalten: $n = 4$
- Anzahl Zeilen: $m = 4$
- Die Diagonale: Alle Elemente a_{ii}
- Die Elemente $(2,2) = a_{22} = 0$; $(1,2) = a_{12} = 1/2$; $(2,1) = a_{21} = 1/3$
- Element (Zeile, Spalte)

Bsp.

Gegeben sind die Matrizen mit reellen Elementen

$$A = \begin{pmatrix} 3 & 2 \\ 5 & -1 \\ 0 & 7 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 4 \\ 0 & -3 \end{pmatrix}, \quad C = \begin{pmatrix} 7 & 5 & -2 \end{pmatrix}, \quad D = \begin{pmatrix} 6 \\ -3 \end{pmatrix}$$

- $A = (3,2)$ -Matrix; $B = (2,2)$ -Matrix; $C = (1,3)$ -Matrix; $D = (2,1)$ -Matrix
- $a_{21}=5$; $b_{12}=4$, $c_{11}=7$

Rechnen mit Matrizen

Addition & Subtraktion

Zwei $m \times n$ -Matrizen $A = [a_{ij}]$ und $B = [b_{ij}]$ werden addiert, indem man entsprechende Glieder der Matrix addiert:

$$A + B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{bmatrix}$$

→ **Matrizen A und B müssen die gleiche Dimension haben.** D.h. beide gleiche viele Spalten und Zeilen.

Bsp.

Es sei $A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$ und $B = \begin{bmatrix} -2 & 1 \\ 2 & -4 \end{bmatrix}$

$$A + B = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} + \begin{bmatrix} -2 & 1 \\ 2 & -4 \end{bmatrix} = \begin{bmatrix} 1+(-2) & 2+1 \\ 3+2 & 1+(-4) \end{bmatrix} = \begin{bmatrix} -1 & 3 \\ 5 & -3 \end{bmatrix}$$

$$A - B = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} - \begin{bmatrix} -2 & 1 \\ 2 & -4 \end{bmatrix} = \begin{bmatrix} 1-(-2) & 2-1 \\ 3-2 & 1-(-4) \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 1 & 5 \end{bmatrix}$$

Multiplikation mit Zahl (Zahl mal Matrix)

Eine $m \times n$ -Matrizen $A = [a_{ij}]$ wird mit einer Zahl $\alpha \in \mathbb{R}$ multipliziert, indem man jedes Matrixelement mit dieser Zahl multipliziert:

$$\alpha A = \begin{bmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \cdots & \alpha a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \cdots & \alpha a_{mn} \end{bmatrix}$$

Bsp.

Es sei $A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$ und $\alpha = 3$ resp. $\alpha = -1$

$$3A = 3 \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 3 \cdot 1 & 3 \cdot 2 \\ 3 \cdot 3 & 3 \cdot 1 \end{bmatrix} = \begin{bmatrix} 3 & 6 \\ 9 & 3 \end{bmatrix}$$

$$(-1)A = (-1) \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -2 \\ -3 & -1 \end{bmatrix}$$

Achtung: $2A + 2B = 2(A+B)$ → Zuerst A + B rechnen und dann die erhaltene Matrix mal 2.

Wichtige Eigenschaften

- Durch die Matrixaddition wird zwei $m \times n$ -Matrizen wieder eine $m \times n$ -Matrix zugeordnet.
- Die **Nullmatrix** (d.h. die Matrix mit lauter Nullen) ist das **Neutralelement** der Matrixaddition: $A + 0 = 0 + A = A$.
- Das Negative einer Matrix A ist die Matrix, bei der jedes Matrixelement mit -1 multipliziert wurde: $A = (a_{ij}) \rightarrow -A = (-a_{ij})$. Man nennt $-A$ das **Invers von A** bezüglich Addition.
- Man kann leicht nachrechnen, dass (bezüglich Addition von Matrizen) das **Assoziativgesetz**, $A + (B + C) = (A + B) + C$, gilt.
- Ebenso leicht kann man zeigen, dass (bezüglich Addition von Matrizen) das **Kommutativgesetz**, $A + B = B + A$, gilt.
- Damit bildet die Menge der $m \times n$ -Matrizen zusammen mit der Matrixaddition eine kommutative Gruppe.

Begriff Gruppe bezüglich einer Operation

Der Begriff „Gruppe“ bez. einer Operation bedeutet, dass

- Die Operation abgeschlossen ist (d.h. das Resultat ist auch Element der Gruppe). In diesem Fall bedeutet es, dass die Addition zweier $m \times n$ – Matrizen wieder eine $m \times n$ -Matrix ist.
- Es ein Neutralelement NE gibt, in diesem Fall ist die $m \times n$ -Nullmatrix das Neutralelement.
- Es ein inverses Element IE zur Matrix A gibt, in diesem Fall ist es $-A = (-1)A$.
- Das Assoziativgesetz AG gilt.

Gilt zusätzlich noch das Kommutativgesetz KG, dann nennt man es eine **kommutative Gruppe**.

Matrizenmultiplikation (Matrix mal Matrix)

Das Produkt der $m \times k$ Matrix $A = [a_{ij}]$ und der $k \times n$ Matrix $B = [b_{ij}]$ ist eine $m \times n$ Matrix, definiert durch d.h. #Spalte von A = #Zeile von B

$$AB = [c_{ij}] \text{ wobei } c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj} = \sum_{l=1}^k a_{il}b_{lj}$$

c_{ij} ist das Skalarprodukt des i-ten Zeilenvektors von A mit dem j-ten Spaltenvektor von B.

→ Neue Matrix: **Anzahl Zeile der ersten mal Anzahl Spalte der Zweiten → Neue Dimension**. (#Spalte von A muss gleich #Zeile von B sein. (2,3)-Matrix = (2 Zeilen, 3 Spalten)-Matrix

A sei 2×3 – Matrix, B sei 3×4 – Matrix, dann ist $A \cdot B$ eine 2×4 – Matrix.

A sei 2×3 – Matrix, B sei 3×1 – Matrix, dann ist $A \cdot B$ eine 2×1 – Matrix.

A sei 3×2 – Matrix, B sei 3×4 – Matrix, dann ist $A \cdot B$ nicht definiert, da die „grünen“ Werte nicht übereinstimmen.

A sei 3×5 – Matrix, B sei 5×2 – Matrix, dann ist $A \cdot B$ eine 3×2 – Matrix, aber $B \cdot A$ ist nicht definiert. **Folgerung:** Das Matrizenprodukt ist nicht kommutativ.

Multiplikations-Regel

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \rightarrow a_{11} * b_{11} + a_{12} * b_{21} + a_{13} * b_{31}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \rightarrow a_{21} * b_{11} + a_{22} * b_{21} + a_{23} * b_{31}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \rightarrow a_{11} * b_{12} + a_{12} * b_{22} + a_{13} * b_{32}$$

$$\rightarrow a_{21} * b_{12} + a_{22} * b_{22} + a_{23} * b_{32}$$

...

→ 1. Zeile * 1. Spalte, 2. Zeile * 1. Spalte, 1. Zeile * 2. Spalte, 2. Zeile * 2. Spalte, ...

Bsp.

$$\begin{aligned} \text{Es sei } A &= \begin{bmatrix} 2 & -1 \\ 4 & 1 \end{bmatrix} \text{ und } B = \begin{bmatrix} 1 & 3 & -4 \\ -1 & 2 & 3 \end{bmatrix}, \text{ dann ist } A \cdot B = \begin{bmatrix} 2 & -1 \\ 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 & -4 \\ -1 & 2 & 3 \end{bmatrix} = \\ &= \begin{bmatrix} 2 \cdot 1 + (-1) \cdot (-1) & 2 \cdot 3 + (-1) \cdot 2 & 2 \cdot (-4) + (-1) \cdot 3 \\ 4 \cdot 1 + 1 \cdot (-1) & 4 \cdot 3 + 1 \cdot 2 & 4 \cdot (-4) + 1 \cdot 3 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 4 & -11 \\ 3 & 14 & -13 \end{bmatrix} \end{aligned}$$

Beispiel 7.8: Es sei $A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$ und $B = \begin{bmatrix} -2 & 1 \\ 2 & -4 \end{bmatrix}$

$$A \cdot B = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} -2 & 1 \\ 2 & -4 \end{bmatrix} = \begin{bmatrix} 1 \cdot (-2) + 2 \cdot 2 & 1 \cdot 1 + 2 \cdot (-4) \\ 3 \cdot (-2) + 1 \cdot 2 & 3 \cdot 1 + 1 \cdot (-4) \end{bmatrix} = \begin{bmatrix} 2 & -7 \\ -4 & -1 \end{bmatrix}$$

Transponierte Matrix (A^T)

Die transponierte Matrix A^T der $m \times n$ -Matrix $A = [a_{ij}]$ ergibt sich durch Vertauschen von Zeilen und Spalten, d.h.

Element (1,2) wird zu (2,1); (3,2) wird zu (2,3)

Falls $A^T = [b_{ij}]$ dann gilt $b_{ij} = a_{ji}$ für $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$.

→ Ist A eine $(m*n)$ -Matrix, dann wird A^T eine $(n*m)$ -Matrix.

Berechnung

Koordinaten/Positionswerte einer Zahl tauschen. Zeile 1, Spalte 2 wird zu Spalte 1, Zeile 2.

Bsp.

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \Rightarrow A^T = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$$

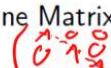
→ Position **(1,2) = 2** wird zu **(2,1)** und Position **(2,1) = 3** wird zu **(1,2)**

$$B = \begin{bmatrix} -2 & 1 & 3 \\ 2 & -4 & -2 \end{bmatrix} \Rightarrow B^T = \begin{bmatrix} -2 & 2 \\ 1 & -4 \\ 3 & -2 \end{bmatrix}$$

→ **(1,3) = 3** wird zu **(3,1)**, also 3.Zeile & 1. Spalte, usw.

Mit TR: Zuerst Matrix eingeben, dann **Menu:7:2** (Transpose)

Eigenschaften (symmetrisch, antisymmetrisch, Einheitsmatrix I_n)

- Eine Matrix A heisst **symmetrisch**, falls $A^T = A$.
- Eine Matrix A heisst **antisymmetrisch**, falls $A^T = -A$.
- Eine symmetrische oder antisymmetrische Matrix ist quadratisch!
- Die n-dimensionale **Einheitsmatrix I_n** ist eine Matrix bei der alle Elemente auf der Diagonalen Eins und alle anderen Null sind. 
- Ist A eine $n \times n$ -Matrix, dann kann man deren **k-te Potenz** rekursiv definieren durch:
 $A^0 = I_n$ und $A^n = A A^{n-1}$, $n = 1, 2, \dots$

Bsp.

$$A \text{ ist symmetrisch: } A = \begin{bmatrix} a & c \\ c & d \end{bmatrix}$$

$$A \text{ ist antisymmetrisch (notwendige Bedingung, dass in der Diagonalen Nullen sind: } A = \begin{bmatrix} 0 & -c \\ c & 0 \end{bmatrix}$$

Bsp. 2.

Gegeben sind

$$A = \begin{pmatrix} 2 & 3 & -4 \\ 0 & 1 & 5 \\ 0 & 0 & 8 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 9 & -2 & 6 \end{pmatrix}, C = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 3 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Um was für spezielle Matrizen handelt es sich?

- Alle 4 Matrizen sind zunächst einmal quadratische Matrizen
- A ist eine obere, B ist eine untere Dreiecksmatrix, C ist eine Diagonalmatrix und I ist die $(2,2)$ -Einheitsmatrix.

Die inverse Matrix (A^{-1})

Die inverse Matrix A^{-1} der (quadratischen) $n \times n$ -Matrix $A = [a_{ij}]$ hat die Eigenschaft

$$A^{-1} \cdot A = A \cdot A^{-1} = I_n.$$

Allgemeine Formel für (2,2)-Matrizen:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ und } a \cdot d - b \cdot c \neq 0 \Rightarrow A^{-1} = \frac{1}{a \cdot d - b \cdot c} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

1. Überprüfen ob die Determinante (TR: Menu:7:3) $a*d - b*c \neq 0$ ist. Wenn ja dann weiterfahren, falls nein → inverse Matrix existiert nicht.
2. Formel anwenden

Mit TR: Zuerst Matrix eingeben, dann $\wedge -1$ (also hoch -1 eingeben)

Bsp.

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \Rightarrow A^{-1} = \frac{1}{1 \cdot 1 - 3 \cdot 2} \cdot \begin{bmatrix} 1 & -2 \\ -3 & 1 \end{bmatrix} = -\frac{1}{5} \cdot \begin{bmatrix} 1 & -2 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -\frac{1}{5} & \frac{2}{5} \\ \frac{3}{5} & -\frac{1}{5} \end{bmatrix}$$

Kontrolle:

$$A \cdot A^{-1} = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \cdot \frac{1}{1 \cdot 1 - 2 \cdot 3} \cdot \begin{bmatrix} 1 & -2 \\ -3 & 1 \end{bmatrix} = -\frac{1}{5} \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 \\ -3 & 1 \end{bmatrix} = -\frac{1}{5} \begin{bmatrix} -5 & 0 \\ 0 & -5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Achtung:

$$B = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \Rightarrow 1 \cdot 2 - 1 \cdot 2 = 0 \Rightarrow B^{-1} \text{ ex. nicht}$$

Rechenregeln / Formeln für Matrizen

- | | | |
|--|--|-------------------------|
| 1a. $A + B = B + A$ | 1b. Im Allg.: $AB \neq BA$ | $A^0 = E$ |
| 2a. $(A + B) + C = A + (B + C)$ | 2b. $(AB)C = A(BC)$ | $A^{-p} = (A^{-1})^p$ |
| 3a. $A + 0 = A$ | 3b. <u>$AI = IA = A$</u> , (A quadr.) | $A^{p+q} = A^p A^q$ |
| 4. $AB = 0 \quad \nRightarrow \quad A = 0 \text{ oder } B = 0$ | | $A \cdot 0 = 0A = 0$ |
| 5. $AB = AC \quad \nRightarrow \quad B = C$ | | $0 = \text{Nullmatrix}$ |
| 6. $\lambda(A + B) = \lambda A + \lambda B \quad \lambda \in \mathbb{R}$ | | |
| 7. $A(B + C) = AB + AC$ | | |
| < 8. $(A + B)C = AC + BC$ | | |
| 9. $(A^{-1})^{-1} = A$ | | |
| 10. $(AB)^{-1} = B^{-1}A^{-1}$ | | |
| 11. $(A^T)^T = A$ | | |
| 12. $(A + B)^T = A^T + B^T$ | | |
| 13. $(AB)^T = B^T A^T$ | | |
| 14. $(A^{-1})^T = (A^T)^{-1}$ | | |

Für $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ mit $ad - bc \neq 0$ gilt $A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Lösen von Matrizengleichungen

Vorgehen bei Matrizengleichungen

1. Grundsätzlich gleich wie bei normalen Gleichungen. **Auf beiden Seiten das Gleiche tun.**
2. Man kann **auf** beiden Seiten **Matrizen addieren und subtrahieren**. Auch mit **Skalaren(Zahl)dividieren**.
3. **Achtung beim multiplizieren von Matrizen.** Auf **beiden Seiten muss die Multiplikation entweder ganz links oder ganz rechts machen**. Da die Reihenfolge wichtig ist.
4. Wir können **nicht mit einer Matrix dividieren**. Dafür muss auf **beiden Seiten mit der Inversen Matrix multipliziert** (am richtigen Ort) werden.

Wichtig: Es gilt zwar $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{A}^{-1} \cdot \mathbf{A}$, $\mathbf{I} \cdot \mathbf{A} = \mathbf{A} \cdot \mathbf{I}$ & $\mathbf{I} \cdot \mathbf{A}^{-1} = \mathbf{A}^{-1} \cdot \mathbf{I}$ aber i.a. ist $\mathbf{B} \cdot \mathbf{A}^{-1} \neq \mathbf{A}^{-1} \cdot \mathbf{B}$

Bsp. #1

Gegeben seien die Matrizen: $\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 4 & 0 \\ 1 & 3 \end{bmatrix}$

Wir suchen eine Matrix $\mathbf{X} = \begin{bmatrix} x_1 & x_3 \\ x_2 & x_4 \end{bmatrix}$ so, dass die Gleichung $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$ erfüllt ist.

Wir multiplizieren beide Seiten der Gleichung von links mit \mathbf{A}^{-1}

$$(\mathbf{A}^{-1} \cdot \mathbf{A}) \cdot \mathbf{X} = (\mathbf{A}^{-1} \cdot \mathbf{B})$$

Mit $\mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{I}$ (Einheitsmatrix) erhalten wir

$$\underbrace{\mathbf{A}^{-1} \cdot \mathbf{A}}_{=\mathbf{I}} \cdot \mathbf{X} = \mathbf{A}^{-1} \cdot \mathbf{B} \Rightarrow \mathbf{I} \cdot \mathbf{X} = \mathbf{A}^{-1} \cdot \mathbf{B} \Rightarrow \underline{\underline{\mathbf{X} = \mathbf{A}^{-1} \cdot \mathbf{B}}}$$

Da eine Matrix (X) mal die Einheitsmatrix (I) die Matrix (X) ergibt. ($\mathbf{A}^* \mathbf{I} = \mathbf{A}$)

Nun noch die Zahlen einsetzen. \mathbf{A}^{-1} wird mit der inversen Formel von der vorherigen Unterkapitel berechnet.

$$\mathbf{X} = \begin{bmatrix} -2 & 1 \\ 1,5 & -0,5 \end{bmatrix} \cdot \begin{bmatrix} 4 & 0 \\ 1 & 3 \end{bmatrix} = \underline{\underline{\begin{bmatrix} -7 & 3 \\ 5,5 & -1,5 \end{bmatrix}}}$$

Bsp. #2

Gegeben seien die Matrizen: $\mathbf{A} = \begin{bmatrix} 4 & 0 \\ -2 & 5 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} -1 & 2 \\ -2 & 3 \end{bmatrix}$

Wir suchen eine Matrix $\mathbf{X} = \begin{bmatrix} x_1 & x_3 \\ x_2 & x_4 \end{bmatrix}$ so, dass die Gleichung $\mathbf{X}^T \cdot \mathbf{A} = \mathbf{B}$ erfüllt ist.

Wir multiplizieren beide Seiten der Gleichung von rechts mit \mathbf{A}^{-1}

$$\mathbf{X}^T \cdot (\mathbf{A} \cdot \mathbf{A}^{-1}) = (\mathbf{B} \cdot \mathbf{A}^{-1})$$

Mit $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{I}$ (Einheitsmatrix) erhalten wir

$$\mathbf{X}^T \cdot \underbrace{\mathbf{A} \cdot \mathbf{A}^{-1}}_{=\mathbf{I}} = \mathbf{B} \cdot \mathbf{A}^{-1} \Rightarrow \mathbf{X}^T \cdot \mathbf{I} = \mathbf{X}^T = \mathbf{B} \cdot \mathbf{A}^{-1}$$

$$\mathbf{X} = (\mathbf{X}^T)^T = (\mathbf{B} \cdot \mathbf{A}^{-1})^T \Rightarrow \underline{\underline{\mathbf{X} = (\mathbf{A}^{-1})^T \cdot \mathbf{B}^T}}$$

Nun noch die Zahlen eingesetzt: $\mathbf{A}^{-1} = \frac{1}{20} \begin{bmatrix} 5 & 0 \\ 2 & 4 \end{bmatrix} \Rightarrow (\mathbf{A}^{-1})^T = \frac{1}{20} \begin{bmatrix} 5 & 2 \\ 0 & 4 \end{bmatrix}$

$$\mathbf{X} = \frac{1}{20} \begin{bmatrix} 5 & 2 \\ 0 & 4 \end{bmatrix} \cdot \begin{bmatrix} -1 & -2 \\ +2 & 3 \end{bmatrix} = \frac{1}{20} \begin{bmatrix} -1 & -4 \\ 8 & 12 \end{bmatrix} \xrightarrow{*} \text{da } \mathbf{B}^T$$

Bsp. #3 Prüfungsaufgabe

Beweisen Sie die Regel $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$

Die Regel $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$ ist bewiesen, wenn wir zeigen können, dass $(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = I$ gilt.

$$(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = A \cdot (B \cdot B^{-1}) \cdot A^{-1} = A \cdot I \cdot A^{-1} = A \cdot A^{-1} = I$$

Dabei wurde in der ersten Umformung das AG der Matrizenmultiplikation angewandt.

Weitere Beispiele in 3-Kompl-Matrizen Seite 39.

Bsp. X, sodass $B \cdot X = A \cdot X + B$ erfüllt ist. Oder X, sodass $B \cdot X = X + A$ erfüllt ist.

Null-eins Matrizen**Oder- und Und-Verknüpfung**

Null-Eins (Zero-One) Matrizen werden z.B. in der Graphentheorie verwendet.

Definition (\vee = oder, \wedge = und)

Die **Oder- und die Und-verknüpfung zweier $m \times n$ -Matrizen A und B** wird definiert durch

$$A \vee B = [a_{ij} \vee b_{ij}] \quad \text{und} \quad A \wedge B = [a_{ij} \wedge b_{ij}]$$

wobei \vee und \wedge für die boolschen Oder- und Und-Operationen stehen.

Bsp.

$$A \vee B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$A \wedge B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \wedge \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Boolsches Produkt

Das **boolsche Produkt** der $m \times n$ -Matrix $A = [a_{ij}]$ mit der $n \times p$ -Matrix $B = [b_{ij}]$ wird definiert durch

$$A \odot B = [c_{ij}] \text{ wobei } c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \dots \vee (a_{in} \wedge b_{nj}),$$

mit $1 \leq i \leq m$ und $1 \leq j \leq p$.

Eigenschaften

- Sei A eine $(m \times n)$ und B eine $(n \times p)$ Matrix, dann gilt $A \cdot B$ resp. $A \odot B$ ist eine $(m \times p)$ -Matrix
- Wenn $p \neq m$ kann in diesen Fällen $B \cdot A$ resp. $B \odot A$ nicht berechnet werden.
- Es ist nun A eine (3×2) und B eine (2×3) , dann ist $A \odot B$ eine (3×3) -Matrix
- Steht mindestens einmal $(1 \wedge 1)$, dann ist dieses Element **1** in der Endmatrix, egal, was sonst dort steht.

Bsp.

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad B = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Wie lautet das boolsche Produkt der folgenden Matrizen:

$$A \odot B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Achtung: In diesem Beispiel ist $p = m = 3$, wäre es $B \cdot A$, dann wäre $B \odot A$ eine (2×2) -Matrix.

R-te Boolesche Potenz

Definition

Die **r-te boolsche Potenz** der quadratischen $n \times n$ -Matrix A ist definiert durch:

$$A^{[r]} = \underbrace{A \odot A \odot \cdots \odot A}_{r \text{ Faktoren}} \quad \text{wobei } A^{[0]} = 1_n \text{ verwendet wird.}$$

Bsp.

$$\text{Wie lautet die 2-te boolsche Potenz der folgenden Matrix: } A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

$$A^{[2]} = A \odot A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Errechnet wäre das so:

$$(a_{11} \wedge b_{11}) \vee (a_{12} \wedge b_{21}) \vee (a_{13} \wedge b_{31}) \quad (a_{11} \wedge b_{12}) \vee (a_{12} \wedge b_{22}) \vee (a_{13} \wedge b_{32}) \quad (a_{11} \wedge b_{13}) \vee (a_{12} \wedge b_{23}) \vee (a_{13} \wedge b_{33})$$

$$(a_{21} \wedge b_{11}) \vee (a_{22} \wedge b_{21}) \vee (a_{23} \wedge b_{31}) \quad (a_{21} \wedge b_{12}) \vee (a_{22} \wedge b_{22}) \vee (a_{23} \wedge b_{32}) \quad (a_{21} \wedge b_{13}) \vee (a_{22} \wedge b_{23}) \vee (a_{23} \wedge b_{33})$$

$$(a_{31} \wedge b_{11}) \vee (a_{32} \wedge b_{21}) \vee (a_{33} \wedge b_{31}) \quad (a_{31} \wedge b_{12}) \vee (a_{32} \wedge b_{22}) \vee (a_{33} \wedge b_{32}) \quad (a_{31} \wedge b_{13}) \vee (a_{32} \wedge b_{23}) \vee (a_{33} \wedge b_{33})$$

 \rightarrow

$$(0 \wedge 0) \vee (0 \wedge 1) \vee (1 \wedge 1) \quad (0 \wedge 0) \vee (0 \wedge 0) \vee (1 \wedge 1) \quad (0 \wedge 1) \vee (0 \wedge 0) \vee (1 \wedge 0)$$

$$(1 \wedge 0) \vee (0 \wedge 1) \vee (0 \wedge 1) \quad (1 \wedge 0) \vee (0 \wedge 0) \vee (0 \wedge 1) \quad (1 \wedge 1) \vee (0 \wedge 0) \vee (0 \wedge 0)$$

$$(1 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 1) \quad (1 \wedge 0) \vee (1 \wedge 0) \vee (0 \wedge 1) \quad (1 \wedge 1) \vee (1 \wedge 0) \vee (0 \wedge 0)$$

 \rightarrow

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Begründungen, Induktionsbeweise, Rekursive Funktionen & Algorithmen, Inferenzregeln

Mathematische Induktion (beweisen durch Induktionsschritt)

Bekannte Beweismethoden

- **Direkter Beweis:** Man zeigt, dass $p \rightarrow q$ wahr ist, indem zeigt, dass aus $p = \text{WAHR}$ sofort $q = \text{WAHR}$ folgt, d.h. die Kombination $p = \text{WAHR}$ und $q = \text{FALSCH}$ kommt nicht vor (Beweis: n ungerade, sofort n^2 ungerade folgt).
- **Beweis durch Kontraposition:** Es handelt sich um einen indirekten Beweis bei welchem man verwendet, dass $p \rightarrow q$ äquivalent zur Kontraposition $\neg q \rightarrow \neg p$ ist (siehe Beweis, dass mit $3n + 2$ ungerade, auch n ungerade ist).
- **Beweis durch Widerspruch:** Wir möchten zeigen, dass p wahr ist (z.B. $p = \sqrt{2} \notin \mathbb{Q}$). Nehmen wir an, wir finden einen Widerspruch q so, dass $\neg q \rightarrow \neg p$ wahr ist (z.B. $\sqrt{2} \in \mathbb{Q} \rightarrow f$). Weil q falsch ist, aber $\neg q \rightarrow \neg p$ wahr, muss notwendigerweise $\neg p$ falsch sein (Wahrheitstabelle!), d.h. p muss wahr sein (Siehe Beweis, dass $\sqrt{2} \notin \mathbb{Q}$).

p	$\neg p$	q	$\neg p \rightarrow q$
f	w	f	f
w	f	f	w

Der Induktionsbeweis

Der Induktionsbeweis besteht aus **zwei Schritten**:

1. **Induktionsverankerung:** Es wird **gezeigt**, dass $P(n)$ für eine **bestimmte Zahl wahr** ist. Bsp. $P(1)$.
2. **Induktionsschritt:** Es wird **gezeigt**, dass die **Implikation** $P(n) \rightarrow P(n+1)$ **wahr ist** $\forall n \geq 1$.
3. **Beweis des Induktionsschritts:** Beweise, dass unter Annahme der Induktionsvoraussetzung $P(n)$ die Induktionsbehauptung $P(n+1)$ wahr ist.

Bsp. #1

$$\sum_{k=1}^n k^2 = 1^2 + 2^2 + 3^2 + \dots + n^2 = 1 + 4 + 9 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad (**)$$

Schritt 1 – Induktionsverankerung (Formel für bestimmter Wert (Bsp. 1) wahr):

$$\sum_{k=1}^1 k^2 = 1^2 = 1 \quad \text{resp. } \frac{1 \cdot (1+1)(2 \cdot 1+1)}{6} = \frac{6}{6} = 1$$

→ Formel ist für 1 wahr. Da sowohl die Summenformel als auch die (**) Formel 1 ergeben.

Schritt 2 – Induktionsschritt (Formel gilt für $n+1$, also n durch $n+1$ ersetzen):

$$\begin{aligned} \sum_{k=1}^{n+1} k^2 &= 1^2 + \dots + n^2 + (n+1)^2 = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

Das ist nun auf einem anderen Weg zu zeigen. Sprich Formel von Schritt 1 plus zusätzlichen Rechenschritt für **$n+1$** .

$$\begin{aligned} \sum_{k=1}^{n+1} k^2 &= \left(\sum_{k=1}^n k^2 \right) + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \\ &= \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} = \frac{(n+1)[n(2n+1) + 6(n+1)]}{6} = \\ &= \frac{(n+1)[2n^2 + 7n + 6]}{6} = \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

→ Resultat ist dasselbe wie von Schritt 2.
Also ist der Induktionsschritt richtig und die Formel bewiesen.

Bsp. #2

Beweisen Sie: $\forall n \in \mathbb{N}$ gilt: $m = 2^n \cdot 2^n - 1 = 2^{2n} - 1$ ist durch 3 teilbar.

Schritt 1 – Induktionsverankerung (Formel für bestimmter Wert (Bsp. 1) wahr):

$$n = 1: 2^1 \cdot 2^1 - 1 = 3 \text{ ist durch 3 teilbar.}$$

Schritt 2 – Induktionsschritt (Formel gilt für $n + 1$, also n durch $n + 1$ ersetzen):

$$\begin{aligned} 2^{n+1} \cdot 2^{n+1} - 1 &= 2 \cdot 2^n \cdot 2 \cdot 2^n - 1 = 4 \cdot 2^n \cdot 2^n - 1 = 4 \cdot 2^n \cdot 2^n - 4 + 4 - 1 \\ &= 4 \cdot (2^n \cdot 2^n - 1) + 4 - 1 = 4 \cdot \underbrace{(2^n \cdot 2^n - 1)}_{\text{nach Vor.durch 3 teilbar, } \rightarrow \text{also } 3 \cdot (\text{durch 3 Teil})} + 3 = 4 \cdot 3 \cdot k + 3 = 3(4k + 1) \end{aligned}$$

$3 \cdot (4k + 1)$ ist ein Vielfaches von 3 und somit durch 3 teilbar und damit ist die Behauptung bewiesen.

Bsp. #3 Mit Index Null

Beweisen Sie:

$$\forall n \in \mathbb{N} \text{ gilt: } s_{n-1} = \sum_{i=0}^{n-1} 7^i = 7^0 + 7^1 + 7^2 + \dots + 7^{n-1} = \frac{7^n - 1}{7 - 1}$$

Achtung: Es ist nicht s_n sondern s_{n-1} , d.h. n muss auf der rechten Seite $n + 1$ sein. (Bsp. wäre $n = 0$, also $s_{n-1} = 0$ und entsprechend $n = n + 1$, also $0 + 1$, also 1. Somit würde recht 7^1 stehen.)

Schritt 1 – Induktionsverankerung (Hier mit 0, Achtung s_{n-1} , entsprechend **n um eins erhöhen**):

$$s_0 = \sum_{i=0}^0 7^0 = \underline{\underline{1}} \quad \text{und} \quad s_0 = \frac{7^0 - 1}{7 - 1} = \frac{6}{6} = \underline{\underline{1}}$$

Schritt 2 – Induktionsschritt (Formel gilt für $n - 1$, also n durch $n - 1$ ersetzen, s_{n-1} wird zu s_n & 7^n wird zu 7^{n+1}):

$$s_n = \sum_{i=1}^n 7^i = \frac{7^{n+1} - 1}{7 - 1}$$

$$\begin{aligned} s_n &= \sum_{i=0}^n 7^i = \left(\sum_{i=0}^{n-1} 7^i \right) + 7^n = \left(\frac{7^n - 1}{7 - 1} \right) + 7^n = \frac{7^n - 1}{6} + \frac{6 \cdot 7^n}{6} = \frac{7^n - 1 + 6 \cdot 7^n}{6} \\ &= \frac{7 \cdot 7^n - 1}{6} = \frac{7^{n+1} - 1}{6} = \underline{\underline{\frac{7^{n+1} - 1}{7 - 1}}} \end{aligned}$$

Bsp. #4 alte Prüfungsaufgabe

Beweisen Sie, dass $\forall m \in \mathbb{N}$ gilt: $m^3 + 8m + 6$ ist durch 3 teilbar.

Schritt 1 – Induktionsverankerung (Formel für bestimmter Wert (Bsp. 1) wahr):

$$n = 1: 1^3 + 8 \cdot 1 + 6 = 15 \rightarrow \text{durch 3 teilbar. Also OK.}$$

Schritt 2 – Induktionsschritt (Formel gilt für $n + 1$, also m durch $m + 1$ ersetzen):

$$(m + 1)^3 + 8(m + 1) + 6 = m^3 + 3m^2 + 3m + 1 + 8m + 8 + 6 = m^3 + 3m^2 + 11m + 15 = m^3 + 8m + 6 + 3m^2 + 3m + 9$$

$$= (m^3 + 8m + 6) + 3(m^2 + m + 3) = (m^3 + 8m + 6) + 3 \cdot k \rightarrow \text{bewiesen. Da } (m^3 + 8m + 6) \text{ gemäss Vorgabe durch drei teilbar ist und der nächste Term } 3 \cdot k \text{ auch durch drei teilbar ist.}$$

Weitere Beispiele im [4-Reason-Ind-Bew](#) Seite 9. – 15. (Bsp. Bernoulli-Ungleichung: $(1 + b)^n \geq 1 + nb$)

Rekursiv definierte Funktionen

Definition

Ist f eine Funktion mit Definitionsbereich $D(f) = \mathbb{Z}^+ \cup \{0\}$, für die $f(0)$ definiert ist und für die eine Vorschrift existiert, die den Wert $f(k)$ aus $f(k-1), f(k-2), \dots, f(1), f(0)$ berechnet, dann wird diese Definition rekursive oder induktive Definition genannt.

Rekursive/induktive vs. Funktionale/explizite Darstellung

Es sei $\{a_k\} = (a_k) = a_1, a_2, a_3, \dots$ eine arithmetische Folge(AF) mit Differenz d , dann gilt:

- Rekursivs/induktive Darstellung: $a_n = a_{n-1} + d$
- Funktionale/explizite Darstellung: $a_n = a_1 + (n - 1) \cdot d$

Sei $\{a_k\} = (a_k) = a_1, a_2, a_3, \dots$ eine geometrische Folge(GF) mit Quotient q , dann gilt:

- Rekursivs/induktive Darstellung: $a_n = a_{n-1} \cdot q$
- Funktionale/explizite Darstellung: $a_n = a_1 \cdot q^{n-1}$

Bsp. Fibonacci-Zahlen

Wir berechnen die ersten Glieder der Fibonacci f_0, f_1, f_2, \dots , welche rekursiv definiert ist durch

$$f_0 = 0 \text{ und } f_1 = 1 \quad (\text{Anfangsbedingungen})$$

$$f_k = f_{k-1} + f_{k-2}, \text{ für } k = 2, 3, 4, \dots \quad (\text{Rekursionsgleichung})$$

Achtung: Da f_0 und f_1 die Anfangsbedingung sind und in der Rekursionsgleichung f_{k-2} ist. Muss das erste Glied f_{k-2} die kleinste Zahl (Anfangsbedingung) also f_0 entsprechen. Somit ist das erste Glied f_2 , welches bestimmt werden kann.

$$\textcircled{f}_2 = f_1 + f_0 = 1 + 0 = 1$$

$$f_3 = f_2 + f_1 = 1 + 1 = 2$$

$$f_4 = f_3 + f_2 = 2 + 1 = 3$$

$$f_5 = f_4 + f_3 = 3 + 2 = 5$$

Die funktionale Darstellung der Fibonacci-Folge lautet wie folgt:

$$f_k = \frac{\sqrt{5}}{5} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^k - \left(\frac{1 - \sqrt{5}}{2} \right)^k \right]$$

Also für $f_5 \rightarrow k = 5$ eingesetzt ergibt: 5. (gleiches Resultat wie oben)

Weitere Beispiele im [4-Reason-Ind-Bew Seite 16](#).

Rekursive Algorithmen

Definition

Ein Algorithmus heisst **rekursiv**, wenn er ein Problem löst, indem er dazu ein (oder mehrere) gleiche, aber kleinere Probleme löst.

Rekursiv vs. Iterativ

In der folgenden Gegenüberstellung sei die Inputeingabe n immer eine natürliche (= Integer) Zahl. Die folgende Gegenüberstellung soll den Unterschied zwischen „iterativ“ und „rekursiv“ aufzeigen. Die Pseudoprogramme erheben nicht den Anspruch, dass sie so in der Art direkt lauffähig sind.

Aufgabenstellung	Iterativ, n eine Integer Zahl	Rekursiv, die Funktionen rufen sich immer wieder selber auf, n eine Integer Zahl
Fakultät(n) = $n!$	<pre> Fact := 1 For i = 1 bis n do Fact := Fact*i return Fact </pre>	<pre> Funktion factoriel(n) If n = 0 then return 1 Else return n*factoriel(n - 1) </pre>
Beispiel für $n = 4$	$ \begin{aligned} &1 \\ &1 \cdot 2 = 2 \\ &1 \cdot 2 \cdot 3 = 6 \\ &1 \cdot 2 \cdot 3 \cdot 4 = 24 \end{aligned} $	$ \begin{aligned} &4 \cdot \text{factoriel}(3) \\ &4 \cdot 3 \cdot \text{factoriel}(2) \\ &4 \cdot 3 \cdot 2 \cdot \text{factoriel}(1) \end{aligned} $
a^n	<pre> Potz := 1 For i = 1 bis n do Potz := Potz*a return Potz </pre>	<pre> Funktion Potz(a, n) If n = 0 then return 1 Else return a*Potz(a, n - 1) </pre>
Beispiel für $n = 4$	$ \begin{aligned} &a \\ &a*a \\ &a*a*a \\ &a*a*a*a \end{aligned} $	$ \begin{aligned} &a * \text{Potz}(a, 3) \\ &a * a * \text{Potz}(a, 2) \\ &a * a * a * \text{Potz}(a, 1) \\ &a * a * a * a * \text{Potz}(a, 0) \end{aligned} $

Turm von Hanoi

Für n = Höhe des Turmes gilt folgende Formel für die Anzahl Züge um den Turm von links nach rechts zu bringen:

$$H(n) = 2^n - 1$$

Schlussregeln/Inferenzregeln

Begriffe

Für p (wahr) und $p \rightarrow q$ (wahr), gilt q (wird) wahr.

- **Prämissen:** sind **Voraussetzungen**, die **wahr sein müssen**. (Hier p und $p \rightarrow q$, sind beides Prämissen)
- **Konklusion:** ist die **Folgerung** (Hier q) und zwar **aufgrund wahrer Voraussetzungen**.
- Ein **Argument** ist eine **Folge von Aussagen**, die mit einer **Folgerung (Konklusion)** enden.
- **Gültig heisst**, dass die **Folgerung (Konklusion)** aus der **Wahrheit der vorhergehenden Aussagen (den Prämissen) des Arguments folgt**.

Wertetabelle dazu:

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$
1	1	1	1
1	0	0	0
0	1	1	0
0	0	1	0

Grundlagen

In der **Logik** der „**Schlussregeln**“ oder des „**Schliessens**“ gilt der **folgende Grundsatz**:

- **Aus wahren Voraussetzungen (Prämissen) werden wahre Schlussfolgerungen gezogen.**

Oder anders ausgedrückt:

- Es kann **niemals der Fall eintreten, dass eine falsche Schlussfolgerung aus wahren Voraussetzungen gezogen wird.**

Wir werden immer **von wahren Prämissen ausgehen**.

Bsp. Wir wollen zeigen, dass $[p \wedge (p \rightarrow q)] \rightarrow q$ eine Tautologie ist.

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$[p \wedge (p \rightarrow q)] \rightarrow q$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

Letzte drei Zeilen: «**Aus falschem folgt alles**». Hinterste Spalte **alles «1»**, also ist es eine **Tautologie**.

Achtung: Tautologie bedeutet hier **nicht**, dass **q immer wahr** ist, sondern dass die **Formel « $[p \wedge (p \rightarrow q)] \rightarrow q$ » immer wahr**, also **gültig** ist.

Kann auch mit logisch äquivalenten Umformung gezeigt werden (Siehe Kapitel «[logische Äquivalenzgesetze](#)»):

$$\begin{aligned} [p \wedge (p \rightarrow q)] \rightarrow q &\equiv [p \wedge (\neg p \vee q)] \rightarrow q \equiv [(p \wedge \neg p) \vee (\neg p \wedge q)] \rightarrow q \equiv [\mathbf{F} \vee (\neg p \wedge q)] \rightarrow q \\ &\equiv [\neg p \wedge q] \rightarrow q \equiv \neg[\neg p \wedge q] \vee q \equiv [\neg \neg p \vee \neg q] \vee q \equiv [p \vee \neg q] \vee q \equiv p \cdot \vee (\neg q \vee q) \equiv p \vee \mathbf{T} \equiv \mathbf{T} \end{aligned}$$

Verschiedene Regeln (Alles Tautologien)

Schlussregel Schreibweise (\therefore)

Schlussregeln können in dieser Form beschrieben werden und es bedeutet folgendes:

Seien also

- p = "Sie haben ein aktuelles Passwort"
- q = "Sie können sich ins Netzwerk einloggen"

Dann kann man das Argument in folgender Form schreiben

$$\begin{array}{c} p \rightarrow q \\ p \\ \hline \therefore q \end{array} \quad \left. \begin{array}{l} \text{Prämissen (sind wahr)} \\ \text{Folgerung (demzufolge)} \end{array} \right\}$$

Das Symbol \therefore steht für "demzufolge" oder "folglich".

Modus ponens (Inferenzregel/Abtrennungsregel = Grundform des direkten Beweises)

$$\frac{p \quad p \rightarrow q}{\therefore q}$$

Tautologie : $[p \wedge (p \rightarrow q)] \rightarrow q$

Bsp.

- p die Aussage „den Spinat auf fressen“.
- q die Aussage „es gibt ein Dessert“.
- $p \rightarrow q$ die Aussage „Wenn du den Spinat aufisst, dann gibt es einen Dessert“.

Folgerung: q «Der Spinat wurde aufgegessen und es gibt ein Dessert»

Modus tollens (Aufhebender Modus)

$$\frac{\neg q \quad p \rightarrow q}{\therefore \neg p}$$

Tautologie : $[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$

Bsp.

Wir nehmen die Aussagen von unserem Einführungsbeispiel:

- p die Aussage „den Spinat auf fressen“.
- q die Aussage „es gibt ein Dessert“.
- $p \rightarrow q$ ist die Aussage „Wenn du den Spinat aufisst, so gibt es ein Dessert“.

Es sei nun $\neg q$ (es gibt also kein Dessert) und $p \rightarrow q$ wahr, dann folgt, dass $\neg p$ wahr ist. D.h. die Folgerung ist, dass das Kind den Spinat nicht aufgegessen hat. Was für konsequente Eltern!!

Folgerung: $\neg p$ „Das Kind hat den Spinat nicht aufgegessen“.

Wertetabelle dazu:

p	q	$\neg q$	$p \rightarrow q$	$\neg q \wedge (p \rightarrow q)$
1	1	0	1	0
1	0	1	0	0
0	1	0	1	0
0	0	1	1	1

Wir wissen, dass $\neg q$ und $p \rightarrow q$ wahr sind (**also 1**). Oben in der Tabelle abgelesen bedeutet dies, dass p = 0 und somit $\neg p = 1$ ist.

Hypothetischer Syllogismus

$$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$$

Tautologie : $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$

Bsp.

Wir nehmen die Aussagen von unserem Einführungsbeispiel:

- p die Aussage „den Spinat auf fressen“.
- q die Aussage „essen wir ein Dessert“.
- r die Aussage „wir gehen in den Zoo“.
- $p \rightarrow q$ ist die Aussage „Wenn du den Spinat aufisst, essen wir ein Dessert“.
- $q \rightarrow r$ ist die Aussage „Wenn das Dessert gegessen ist, gehen wir in den Zoo“.

Folgerung: $p \rightarrow r$ ist die Aussage „Wenn du den Spinat aufisst, gehen wir in den Zoo“.

Disjunktiver Syllogismus

$$\begin{array}{c} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Tautologie : $[(p \vee q) \wedge \neg p] \rightarrow q$

Bsp.

- p die Aussage „ich belege das Modul ANLS“.
- q die Aussage „ich belege das Modul D-MATH“.
- $\neg p$ „ich belege das Modul ANLS nicht“.
- $(p \vee q) \wedge \neg p$ „ich belege ANLS oder D-MATH“ und „belege ANLS nicht“.

Folgerung: q ist die Aussage „Ich belege das Modul D-MATH“.

Addition

$$\begin{array}{c} p \\ \hline \therefore p \vee q \end{array}$$

Tautologie : $p \rightarrow (p \vee q)$

Bsp. Eines oder das Andere(Beides geht nicht)

- p die Aussage „ich besuche die Präsenz des Moduls D-MATH“.
- q die Aussage „ich gehe Gleitschirmfliegen“.

Folgerung: „Ich besuche die Präsenz des Moduls D-MATH oder ich gehe Gleitschirmfliegen“.

Simplifikation

$$\begin{array}{c} p \wedge q \\ \hline \therefore p \end{array}$$

Tautologie : $(p \wedge q) \rightarrow p$

auch
 $p \wedge q$
 $\therefore q$

Bsp.

- p die Aussage „ich belege das Modul ANLS“.
- q die Aussage „ich belege das Modul D-MATH“.
- $p \wedge q$ ist die Aussage „ich belege ANLS und D-MATH“

Folgerung: „Ich belege das Modul ANLS“.

Konjunktion

$$\begin{array}{c} p \\ q \\ \hline \therefore p \wedge q \end{array}$$

Tautologie : $[(p) \wedge (q)] \rightarrow (p \wedge q)$

Bsp.

- p die Aussage „ich belege das Modul ANLS“.
- q die Aussage „ich belege das Modul D-MATH“.
- $p \wedge q$ ist die Aussage „ich belege ANLS und D-MATH“.

Folgerung: „Ich belege die Module ANLS und D-MATH“.

Resolution

$$\begin{array}{c} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

Tautologie : $[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$

Bsp.

- p die Aussage „ich belege das Modul ANLS“.
- q die Aussage „ich belege das Modul D-MATH“.
- r die Aussage „ich belege das Modul KRYPT“.
- $p \vee q$ ist die Aussage „ich belege ANLS oder D-MATH“.
- $\neg p \vee r$ ist die Aussage „ich belege ANLS nicht oder ich belege KRYPT“.

Folgerung: „Ich belege die Module D-MATH oder KRYPT“.

Prüfungsaufgabe

Verifizieren Sie mittels Wertetabelle und logisch äquivalenten Umformungen, dass es sich bei dem hypothetischen Syllogismus um eine **Tautologie** handelt.

Wertetabelle:

$$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$$

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r)$	$(p \rightarrow r)$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

Achtung: Es kann gut sein, das in der Prüfung bei den **ersten Spalten** der Tabelle **nicht alle Zeilen ausgefüllt sind**.

Diese müssten entsprechend selbst ausgefüllt werden.

Logisch äquivalente Umformung:

$$\begin{aligned} [(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r) &\equiv [(\neg p \vee q) \wedge (\neg q \vee r)] \rightarrow (\neg p \vee r) \equiv \neg [(\neg p \vee q) \wedge (\neg q \vee r)] \vee (\neg p \vee r) \\ &\equiv p \wedge \neg q \vee q \wedge \neg r \vee \neg p \vee r \equiv p \vee \neg p \wedge \neg q \vee q \wedge \neg r \vee r \equiv T \wedge T \wedge T \equiv T \end{aligned}$$

Beispiel zu den Schlussregeln (Um welche Schlussregel handelt es sich?)

Geben Sie an, um welche Schlussregel es sich handelt.

- 1) Bettina ist sehr gut in Mathematik, also ist Bettina sehr gut in Mathematik oder in Englisch.

Addition

- 2) Conny ist sehr gut in Mathematik und sehr gut in Englisch, also ist Conny sehr gut in Mathematik.

Simplifikation

- 3) Wenn Semesterferien sind, dann werden keine Vorlesungen gehalten. Es sind Semesterferien. Also werden keine Vorlesungen gehalten.

Modus ponens

- 4) Wenn Semesterferien sind, dann werden keine Vorlesungen gehalten. Es werden Vorlesungen gehalten. Also sind keine Semesterferien.

Modus tollens

- 5) Wenn Vorlesungen gehalten werden, gehe ich sie besuchen. Wenn ich Vorlesungen besuche, bin ich in Rotkreuz. Also, wenn Vorlesungen gehalten werden, bin ich in Rotkreuz.

Hypothetischer Syllogismus

- 6) Ich gehe Velofahren oder mache eine Bergtour. Ich gehe nicht Velofahren. Also gehe ich auf eine Bergtour.

Disjunktiver Syllogismus**Anwendungen der Schlussregeln**

Siehe dazu **Beispiele in «4-Reason-Ind-Bew»**, S. 31 (Kapitel «Eine Anwendung»)

Schlussregeln – Denkfehler (Nicht alle Prämissen sind Tautologien)

Mit dem **Modus ponens** erhalten wir keine Informationen zum Wahrheitsgehalt der Prämissen, wenn q wahr ist. Konkret, wir haben keine Information, ob das Kind den Spinat aufgegessen hat, wenn es das Dessert kriegt.

Mehr dazu in in «**4-Reason-Ind-Bew**», S. 32 (Kapitel «Schlussregeln - Denkfehler»)

Schlussregeln für quantifizierte Aussagen

Es sei $P(x)$ eine Aussageform (Prädikat) mit der Variablen x. Damit wird sie für jede Belegung von x (z.B. $x = c$) eine Aussage, die entweder wahr oder falsch ist, d.h. $P(c)$ ist entweder wahr oder falsch. Aber der Ausdruck (eben der Aussageform oder Prädikat) $P(x)$ kann man nicht direkt entweder wahr oder falsch zuordnen, das kann man erst, wenn die Variable x mit einem konkreten (und erlaubten) belegt wird.

Mehr dazu in in «**4-Reason-Ind-Bew**», S. 33 (Kapitel «Schlussregeln für quantifizierte Aussagen»)

Kombinatorik – Counting (Permutation, Kombination, Variation)

Grundlegende Zählprinzipien

Anzahl Teilmengen ($|A|$)

Eine beliebige Menge mit n Elementen ($|A| = n$) hat 2^n Teilmengen.

Anzahl Teilmengen: 2^n ($n = \text{Anzahl Elemente der Menge}$)

Bsp. $A = \{a, b, c\}$

$n = 3$, also $2^3 = 8$ Teilmengen. ($\{a, b, c\}, \{\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a\}, \{b\}$ & $\{c\} \rightarrow$ also 8)

Produktregel (unabhängige Wahl, ohne wegnehmen)

Falls ein erstes Ereignis aus n_1 Möglichkeiten und danach ein zweites (unabhängig vom ersten Ereignis) aus n_2 Möglichkeiten ausgewählt werden kann, dann gibt es insgesamt $n = n_1 \cdot n_2$ Möglichkeiten, die beiden Ereignisse zu wählen.

Wird eine Aufgabe in k Schritten gelöst, die wiederum aus n_1, n_2, \dots, n_k Möglichkeiten bestehen, so existieren total

$$n_1 \cdot n_2 \cdot \dots \cdot n_k = \prod_{i=1}^k n_i$$

Möglichkeiten zur Lösung der Gesamtaufgabe, wenn wir je eine Möglichkeit pro Schritt auswählen können.

Bsp. #1

Wie viele Nummernschilder lassen sich herstellen, wenn jedes Schild aus einer Folge von drei Buchstaben und drei Ziffern besteht? **Reihenfolge wichtig**. Zuerst drei Buchstaben, dann drei Ziffern.

Lösung:

(Anzahl möglicher Buchstaben) $^3 \cdot$ (Anzahl möglicher Zahlen) 3

Also: $\rightarrow 26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 26^3 \cdot 10^3 = 17'576'000$

Bsp. #2

Sie besitzen 12 Hosen, 22 Hemden und fünf Pullis. Wie viele Möglichkeiten zum Ankleiden haben Sie, wenn Sie von jedem genau ein Stück anziehen möchten?

Lösung:

$12 \cdot 22 \cdot 5 = 1230$ Möglichkeiten

Produktregel & kartesisches Produkt von Mengen

Für die Menge der Elemente des kartesischen Produkts der Mengen A_1, A_2, \dots, A_n gilt die Produktregel:

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$$

D.h. Elemente multiplizieren (nicht Teilmengen, also nicht 2^n).

Bsp. $A = \{4, 5\}, B = \{x, y, z\}, C = \{\otimes, \square\}$

Lösung:

$|A| = 2; |B| = 3; |C| = 2 \quad \rightarrow |A \times B \times C| = 2 \cdot 3 \cdot 2 = 12$

Summenregel (entweder oder)

Kann ein erstes Ereignis auf n_1 Arten eintreten und ein zweites Ereignis auf n_2 Arten, wobei nicht beide Ereignisse gleichzeitig eintreten können, dann können die beiden Ereignisse auf $n_1 + n_2$ Arten eintreten

Wird eine Aufgabe in k Schritten gelöst, die wiederum aus n_1, n_2, \dots, n_k Möglichkeiten bestehen, so existieren total

$$n_1 + n_2 + \dots + n_k = \sum_{i=1}^k n_i$$

Möglichkeiten zur Lösung der Gesamtaufgabe, wenn die einzelnen Möglichkeiten aus n_1, n_2, \dots, n_k nicht gleichzeitig eintreten können. D.h. es kann nur eine von allen Möglichkeiten ausgewählt werden.

Bsp.

Sie besitzen 12 lange Hosen, 22 Jupes und fünf kurze Hosen. Wie viele Möglichkeiten zum Ankleiden haben Sie, wenn Sie genau ein Stück Anziehen möchten?

Lösung:

$$12 + 22 + 5 = 39 \text{ Möglichkeiten}$$

Summenregel & Vereinigung von Mengen

Für die **Menge** der Elemente einer Vereinigung paarweiser disjunkter Mengen (keine Schnittmenge, also Elemente von A_i sind nicht in A_j) gilt die **Summenregel**:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$$

D.h. **Anzahl Elemente addieren**.

Bsp. Gültige Passwörter

Ein gültiges Passwort bestehe aus sechs bis acht Zeichen (Großbuchstaben oder Ziffern) wobei mindestens eine Ziffer vorhanden sein muss. Wie viele mögliche Passwörter gibt es?

Lösung: Es macht Sinn die folgenden Variablen einzuführen:

P_6^u : Anzahl ungültige Passwörter der Länge 6.

P_6^g : Anzahl gültige Passwörter der Länge 6.

P_6 : Anzahl Passwörter der Länge 6.

Die ungültigen Passwörter bestehen nur aus Buchstaben. Nach der Produktregel ist deren Anzahl $P_6^u = 26^6$ (Buchstaben).

Die gesamte Anzahl Passwörter ergibt sich ebenfalls mit Hilfe der Produktregel: $P_6 = 36^6$ (Buchstaben oder Ziffern).

Somit erhalten wir für die Anzahl gültiger Passwörter der Länge 6:

$$P_6^g = P_6 - P_6^u = 36^6 - 26^6.$$

Analoge Ausdrücke findet man für P_7^g und P_8^g .

Wieder können wir die Summenregel verwenden und erhalten

$$P_6^g + P_7^g + P_8^g = (36^6 - 26^6) + (36^7 - 26^7) + (36^8 - 26^8) = \sum_{i=6}^8 (36^i - 26^i).$$

$$= 36^6 - 26^6 + 36^7 - 26^7 + 36^8 - 26^8 = 2'684'483'036'360 \approx 2,7 \cdot 10^{12}$$

Das Einschluss-/Ausschlussprinzip (Anzahl Lösungen)

Für zwei beliebige Mengen A und B gilt:

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

Bsp. #1

Sei $A = \{1, 2, 3, 4, 5\}$; $B = \{4, 5, 6, 7, 8, 9, 10, 11\}$, dann ist:

$A \cup B = \{1, 2, \dots, 11\}$ und $A \cap B = \{4, 5\}$

Und somit: $|A \cup B| = |A| + |B| - |A \cap B| = 5 + 8 - 2 = 11$

Bsp. #2

Wie viele Bitstrings der Länge 8 starten mit einer 1, oder enden mit den beiden Bits 00?

Lösung: Verwenden von folgenden Mengen:

$A = \text{«Bitstrings mit der Länge 8, die mit 1 beginnen»}$

$B = \text{«Bitstrings mit der Länge 8, die mit 00 enden»}$

Dank Produktregel wissen wir, dass es $2^7 = 128$ Bitstrings gibt, welche mit «1» beginnen. $\rightarrow |A| = 2^7 = 128$

Weiter gibt es $2^6 = 64$ Bitstrings, welche mit «00» aufhören. $\rightarrow |B| = 2^6 = 64$

Zudem wissen wir, dass es 2^5 Bitstrings gibt, welche mit «1» beginnen und mit «00» enden. $\rightarrow |A \cap B| = 2^5 = 32$

Also: $|A \cup B| = |A| + |B| - |A \cap B| = 128 + 64 - 32 = 160$ (Bitstrings, welche mit 1 beginnen und mit 00 enden.)

Es gibt auch Zählprobleme, welche sich mit einem Baumdiagramm lösen lassen. Mehr dazu in «[5-Counting](#)» S. 10.

Das Schubfachprinzip (Finden von (mindestens) einer Zahl, welche ...)

Definition

Falls man $k+1$ Objekte auf k Schubfächer verteilen muss, dann gibt es wenigstens ein Schubfach mit mehr als einem Objekt.

Bsp.

Hat man 6 Äpfel und 5 Körbe, so hat mindestens ein Korb mehr als 1 Apfel.

Zahlen finden, welche nur aus Einsen & Nullen besteht

Dafür gibt es eine bestimmte Formel, siehe «[5-Counting](#)» S. 12, erläutere ich hier aber nicht weiter.

Bsp. #1

Finden Sie eine Zahl $k \in \mathbb{N}$, so dass $13 \cdot k$ nur aus Einsen und Nullen besteht.

Lösung:

Wir bestimmen von den Zahlen 1, 11, 111, 1111, ..., $\underbrace{111\dots11}_{\max.14 \text{ Einsen}}$ den Modulus 13, bis wir entwe-

der den Rest Null oder zwei gleiche Reste haben. Danach bestimmen wir entweder $k = \frac{\text{Einserzahlen}}{n}$

oder $k = \frac{\text{Differenz der Einserzahlen mit gl.Rest}}{n}$

$$\begin{aligned} 1 \bmod 13 &\equiv 1 \\ 11 \bmod 13 &\equiv 11 \\ 111 \bmod 13 &\equiv 7 \\ 1111 \bmod 13 &\equiv 6 \\ 11111 \bmod 13 &\equiv 9 \\ 111111 \bmod 13 &\equiv 0 \end{aligned}$$

Somit ist $k = \frac{111111}{13} = 8547$

Bsp. #2

Finden Sie eine Zahl $k \in \mathbb{N}$, so dass $14 \cdot k$ nur aus Einsen und Nullen besteht

Lösung:

Wir bestimmen von den Zahlen $1, 11, 111, 1111, \dots, \underbrace{111\dots11}_{\text{max.15 Einsen}}$ den Modulus 14, bis wir entwe-

der den Rest Null oder zwei gleiche Reste haben. Danach bestimmen wir entweder $k = \frac{\text{Einserzahlen}}{n}$
oder $k = \frac{\text{Differenz der Einserzahlen mit gl.Rest}}{n}$

$$\begin{aligned} 1 \bmod 14 &\equiv 1 \\ 11 \bmod 14 &\equiv 11 \\ 111 \bmod 14 &\equiv 13 \\ 1111 \bmod 14 &\equiv 5 \\ 11111 \bmod 14 &\equiv 9 \\ 111111 \bmod 14 &\equiv 7 \\ 1111111 \bmod 14 &\equiv 1 \end{aligned}$$

$$\text{Somit ist } k = \frac{1'1110111-1}{14} = \frac{1'111'110}{14} = 79'365$$

Das verallgemeinerte Schubfachprinzip

Falls man N Objekte auf k Schubfächer verteilt, dann gibt es wenigstens ein Schubfach, welches mindestens $\lceil N/k \rceil$ Objekte enthält (Beweis: KR, p401).

Bsp.

In den beiden Kohorten des Modul D-MATH seien 100 Studierende eingeschrieben. Wie viele Studierende haben mindestens in einem Monat Geburtstag?

Lösung:

$$m = \left\lceil \frac{100}{12} \right\rceil = \lceil 8.33 \rceil = 9$$

Formel

N = Anzahl Objekte

k = Anzahl Schubfächer

m = Minimale Anzahl Objekte in mindestens einem Schubfach

$$\frac{N}{k} > m = \left\lceil \frac{N}{k} \right\rceil \quad \text{resp. } N > k \cdot (m - 1) \quad \text{resp. } N \geq k \cdot (m - 1) + 1 = k \cdot m + (k - 1)$$

Bsp.

Wie gross muss die Mindestzahl (N) von Studierenden in DMATH sein, damit mit absoluter Sicherheit **mindestens 5** Studierende dieselbe Note (A, B, C, D, E oder F) erhalten?

Lösung:

$$N = ? \quad k = 6 \quad m = 5$$

$$N \geq 6 * (5-1) + 1 \rightarrow N \geq 6 * 4 + 1 \rightarrow N \geq 25$$

Permutation und Kombination

Permutation ($P(n,n)$ / $P(n,r)$ = geordnete Auswahl)

Definition

Eine Permutation von n verschiedenen Elementen ist eine geordnete Anordnung dieser n Elemente. Eine r -Permutation von n verschiedenen Elementen ist eine geordnete Anordnung von r der n Elemente.

Bsp. Menge $S = \{1,2,3\}$

Permutation: $(3,1,2) \leftarrow$ eine geordnete Anordnung

2-Permutation: $(3,2) \leftarrow$ geordnete Anordnung einer Teilmenge

Es gibt $3 * 2 * 1 = 3! = 6$ 3-Permutationen und $3 * 2 = 6$ 2-Permutationen von S

Anzahl n -Permutationen einer Menge

Auf wie viele Arten kann ich **n Elemente** auf **n Plätze** anordnen?

$$P(n, n) = n!$$

Bsp.

Auf wie viele Arten können die 8 Buchstaben $\{a, b, c, d, e, f, g, h\}$ auf 8 Plätze (oder denken Sie an 8 Personen auf 8 unterscheidbare Stühle) angeordnet werden?

Lösung:

$$8! = 40320$$

Anzahl r -Permutationen(Variation) einer Menge

Auf wie viele Arten kann ich **$r < n$ Elemente** auf **n Plätze** auswählen, wenn es auf die **Reihenfolge ankommt**?

Die Anzahl von r -Permutationen einer Menge von n Elementen ist:

$$P(n, r) = n(n-1)(n-2) \cdots (n-r+1) = \frac{n!}{(n-r)!}, \quad 0 \leq r \leq n \in \mathbb{N}.$$

n = Anzahl Elemente einer Menge (A)

r = Teilmenge von der Menge A

MIT TR: Menu:5:2 (npr(n,r)) → Bsp. npr(100,3)

Bsp.

Auf wie viele Arten können die ersten drei Plätze bei einem Spiel mit 100 Teilnehmern ausgewählt werden?

Lösung:

$$\frac{1001 \cdot 1000 \cdot 999}{(100-3)!} = 100 \cdot 99 \cdot 98 = 970200$$

Kombination ($C(n,r)$ = ungeordnete Auswahl)

Definition

Eine r -Kombinationen von n verschiedenen Elementen ist eine ungeordnete Auswahl von r dieser n Elementen. Sie ist also nichts anderes als eine Teilmenge mit r Elementen.

- «ungeordnet» heisst, dass die **Reihenfolge der Ziehung** der Auswahl **nicht wichtig ist**.
- Bsp. Zahlenziehen beim Lotto. Reihenfolge ist unwichtig, nur die Zahlen sind wichtig.
- Also: **(1,2,3) ist das gleiche wie (3,2,1)**

N tief r (Binomialkoeffizient)

Wie in der unten ersichtlichen Formel gilt:

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}, n \geq 0 \text{ und } 0 \leq r \leq n \text{ und } n, r \in \mathbb{N}$$

$\binom{n}{r}$ wird «n tief r» ausgesprochen.

Mit TR: Menu:5:3 (ncr(n,r)) → Bsp. Für 8 tief 2 = ncr(8,2) = 28

Bsp.

$$\binom{10}{10-8} = \binom{10}{2} = \frac{10!}{2!(10-2)!} = \frac{10!}{2! \cdot 8!} = \frac{10 \cdot 9}{2 \cdot 1} = 45$$

Anzahl r-Kombinationen einer Menge n (Reihenfolge egal = Kombination)

$$C(n, r) = \frac{n!}{r! \cdot (n-r)!} = \binom{n}{r} = \binom{n}{n-r} = C(n, n-r), \text{ wobei } 0 \leq r \leq n \text{ gelten muss.}$$

Bsp. #1

Wie viele 3-er Teams können aus 5 Personen gebildet werden?

Lösung:

$$C(5, 3) = \frac{5!}{3! \cdot (5-3)!} = \frac{5!}{3! \cdot 2!} = \frac{5 \cdot 4}{2} = 10$$

Bsp. #2

Wie viele 2-er Teams können aus 6 Personen gebildet werden?

Lösung:

$$C(6, 2) = \frac{6!}{2! \cdot (6-2)!} = \frac{6!}{2! \cdot 4!} = \frac{6 \cdot 5}{2} = 15$$

Prüfungsaufgabe – Lotto

Wie viele Möglichkeiten gibt es im

a) Lotto (6 aus 40)? $\binom{40}{6} = \frac{40!}{6! \cdot 34!} = 3'838'380$

b) Lotto (6 aus 42)? $\binom{42}{6} = \frac{42!}{6! \cdot 36!} = 5'245'786$

c) Lotto (6 aus 45)? $\binom{45}{6} = \frac{45!}{6! \cdot 39!} = 8'145'060$

d) Lotto (6 aus 45) und dem Zusatzjoker (Auswahl von 1, 2 oder 3)? (*)

$$3 \cdot \binom{45}{6} = 3 \cdot \frac{45!}{6! \cdot 39!} = 3 \cdot 8'145'060 = 24'435'180$$

e) Lotto (6 aus 42) und dem Zusatzjoker (Auswahl von 1, 2, ..., 6)? (Seit 2013 in der Schweiz) (*)

$$6 \cdot \binom{42}{6} = 6 \cdot \frac{42!}{6! \cdot 36!} = 6 \cdot 5'245'786 = 31'474'716$$

f) Lotto (6 aus 49)? $\binom{49}{6} = \frac{49!}{6! \cdot 43!} = 13'983'816$

g) Euromillions (5 aus 50 [Zahlen] und 2 aus 12 [Sterne]) (*)

$$\binom{50}{5} \cdot \binom{12}{2} = \frac{50!}{5! \cdot 45!} \cdot \frac{12!}{2! \cdot 10!} = 2'118'760 \cdot 66 = 139'838'160$$

h) In den (*) Aufgaben kommt zusätzlich die Produktregel zur Anwendung.

Verallgemeinerte Permutationen und Kombinationen

r-Permutationen (Variation, geordnet) mit Wiederholung (mehrmals das gleiche Element/Wert)

Die Anzahl der r-Permutationen mit Wiederholung bei einer Menge mit n-Elementen ist gegeben durch:

$$n^r$$

n = Anzahl möglicher Elemente/Werte

r = Anzahl Wiederholungen/Stellen

Bsp. 1

Wie viele mögliche PIN's gibt es bei einer Kreditkarte, bei welcher man einen 4-, 5- oder 6-stelligem Pin wählen kann?

Lösung:

$$10^6 + 10^5 + 10^4 = 1'110'000 \text{ mögliche PIN's.}$$

r-Kombinationen(ungeordnet) mit Wiederholung (mehrmas das gleiche Element/Wert)

Die Anzahl r-Kombinationen bei einer Menge von n Objekten mit Wiederholung ist

$$C(n + r - 1, r) = \binom{n + r - 1}{r} \quad \text{Sorten/Arten/Objekte}$$

n = Anzahl mögliche Objekte/Arten/Sorten (Bsp. Äpfel)

r = Anzahl Stellen/Objekte, welche wir herausnehmen/betrachten (vier Früchte)

→ Ja, r kann auch grösser als n sein.

Bsp. #1

Auf wie viele Arten lassen sich aus einer Frücheschale mit Äpfel, Orangen und Birnen vier Früchte herausnehmen, wenn es auf die Reihenfolge nicht ankommt?

Lösung:

n = 3 (3 Objekte: Apfel, Orange, Birne) r = 4 (4 Früchte: Kombination von 4-Früchten ist gefragt)

$$\rightarrow C(3 + 4 - 1, 4) = C(6, 4) = \binom{6}{4} = \frac{6!}{4!(6-4)!} = \frac{6!}{4! \cdot 2!} = 15 \text{ Möglichkeiten}$$

Bsp. #2

Auf wie viele Arten lassen sich aus einer Kasse mit 1-, 2-, 5-, 10-, 20-, 50- und 100-Dollar Noten fünf Noten entnehmen, falls es nicht auf die Reihenfolge der Noten ankommt?

Lösung:

n = 7 (7 verschiedene Notengrössen) r = 5 (Kombination von fünf Noten ist gefragt)

$$\rightarrow C(7 + 5 - 1, 5) = C(11, 5) = ncr(11, 5) = 462 \text{ mögliche Arten}$$

Permutationen nicht unterscheidbarer Objekte

Dieser Fall wird in der Literatur **oft als „Permutationen mit Wiederholung“** bezeichnet.

Die Anzahl verschiedener Permutationen von n Objekten, von denen n_1 nicht unterscheidbare Objekte vom Typ 1, n_2 nicht unterscheidbare Objekte vom Typ 2, ... und schliesslich n_k nicht unterscheidbare Objekte vom Typ k sind, ist gegeben durch:

$$\frac{n!}{n_1!n_2!\dots n_k!}, \text{ wobei } n = \sum_{i=1}^k n_i$$

→ Gibt es **keine Wiederholungen**, so sind alle $n_i=1$ und damit die **Anzahl** der **Möglichkeiten** $n!$.

Bsp.

Wie viele unterschiedliche Wörter kann man erzeugen, wenn man die Zeichen im „Wort“

- a) SUCCESS umordnet?
- b) 1234567 umordnet?

Lösung a):

SUCCESS enthält 3 mal ein «S», 2 mal ein «CC». → $n_1=3$, $n_2=2$

$$\rightarrow \frac{7!}{3!2!} = 420 \text{ verschiedene Wörter}$$

Lösung b):

1234567 enthält keine Wiederholungen also gilt $n!$

$$\rightarrow 7! = 5040 \text{ verschiedene Wörter/Zahlen}$$

Binomialkoeffizienten (für α – reelle Zahlen (nicht \mathbb{N}))

Definition

$$\binom{\alpha}{k} = \alpha \cdot (\alpha - 1) \cdots (\alpha - k + 1), \text{ für } k > 0, \alpha \in \mathbb{R}, k \in \mathbb{N}_0$$

$$\binom{\alpha}{k} = 1, \text{ für } k = 0, \alpha \in \mathbb{R}, k \in \mathbb{N}_0$$

$$\binom{\alpha}{k} = \frac{\alpha}{1}, \text{ für } k = 1$$

Bsp.

$$\binom{\pi}{0} = 1, \text{ per Definition}; \binom{\pi}{1} = \frac{\pi}{1} \approx 3,1415; \binom{\pi}{2} = \frac{\pi \cdot (\pi - 1)}{2 \cdot 1} \approx 3,364;$$

$$\binom{\pi}{3} = \frac{\pi \cdot (\pi - 1) \cdot (\pi - 2)}{3 \cdot 2 \cdot 1} \approx 1,2801; \binom{\pi}{4} = \frac{\pi \cdot (\pi - 1) \cdot (\pi - 2) \cdot (\pi - 3)}{4 \cdot 3 \cdot 2 \cdot 1} \approx 0,0453$$

Pascal'sche Dreieck & Binomialkoeffiziente (Zahl vor x^7 herausfinden)

Für $x, y \in \mathbb{R}$ (ja sogar in \mathbb{C}) und $n \in \mathbb{N}_0$ gilt:

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k = \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \cdots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} x^0 y^n.$$

Bsp. Koeffizient x^5 gesucht in $(x+y)^7$

n-k = x-Potenz von gesuchtem Koeffizienten ($k = n - x$ -Potenz)

k = y-Potenz von gesuchtem Koeffizienten

x = von Aufgabenbeschreibung (Bsp. unten: **3x**)

y = von Aufgabenbeschreibung (Bsp. unten: **2y**)

Bsp. Wie lautet der Koeffizient von x^6 in $(3x+2y)^{15}$?

Lösung:

$$n = 15 \quad n-k = 6 \rightarrow k = 15 - 6 = 9$$

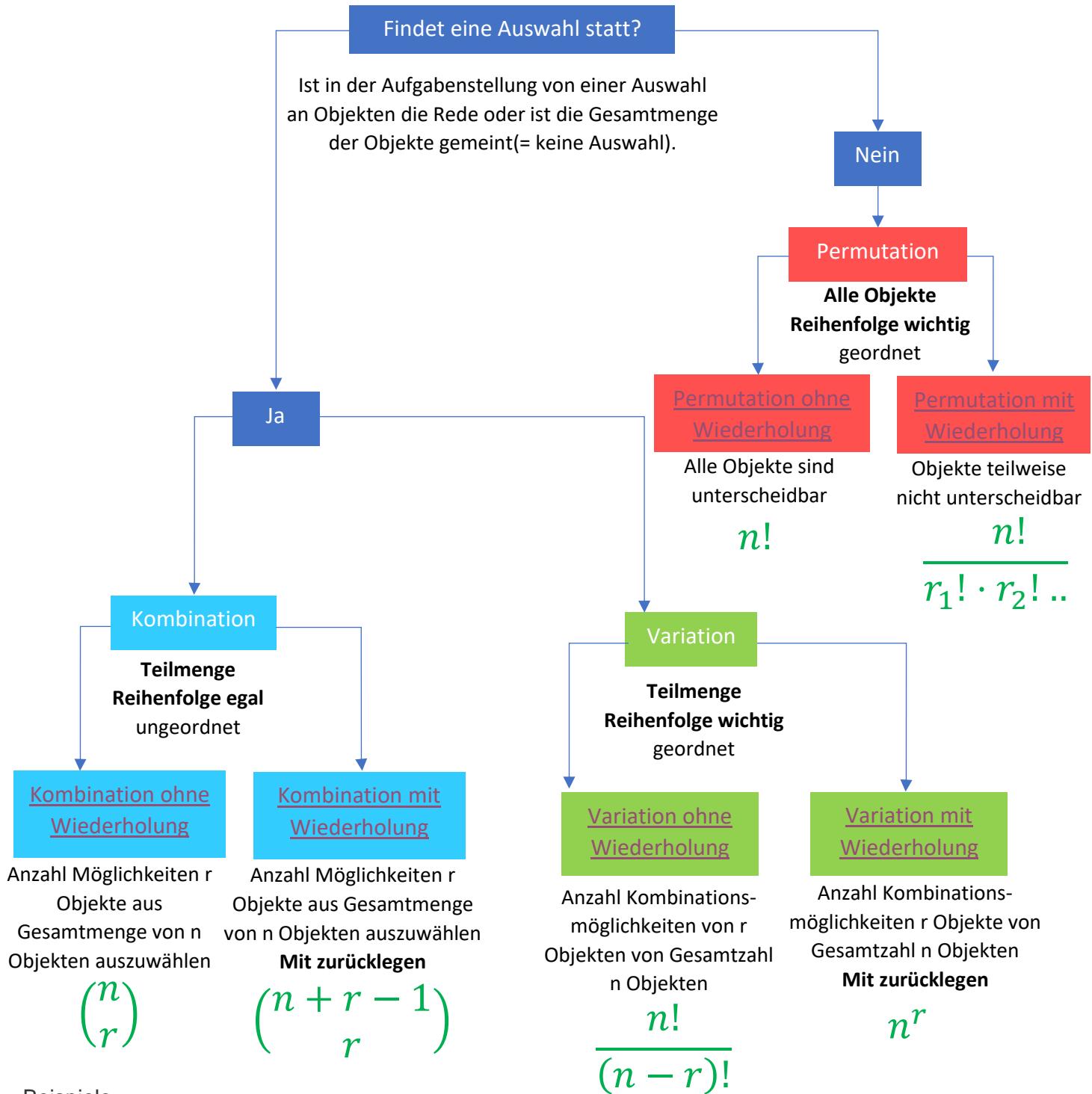
$$\binom{n}{k} \cdot x^{n-k} \cdot y^k = \binom{15}{9} \cdot (3x)^{15-9} \cdot (2y)^9 = \binom{15}{9} \cdot (3x)^6 \cdot (2y)^9$$

$$= \binom{15}{9} \cdot 3^6 \cdot x^6 \cdot 2^9 \cdot y^9 = \frac{15!}{9! \cdot (15-9)!} \cdot 3^6 \cdot x^6 \cdot 2^9 \cdot y^9 = \underbrace{1'868'106'240}_{\text{gesuchter Koeff.}} \cdot x^6 \cdot y^9$$

Mit TR: Menu:3:3 (Bsp. expand($(3x+2y)^{15}$) → dann scrollen bis stelle mit x^6 gefunden und Zahl(Koeffizient) ablesen)

Für Collary-Thema siehe [5-Counting-J-Schuler_V3-0.pdf](#) S. 32

Entscheidungsbaum Kombinatorik



Beispiele

P.o.W.: In einer Urne gibt es 6 versch. farbige Kugeln. Wie viele Mglkt gibt es, die Kugeln in einer Reihe anzuordnen?

P.m.W: In einer Urne gibt es 3 grüne und 2 gelbe Kugeln. Wie viele Mglkt gibt es, die Kugeln in einer Reihe zu ordnen?

V.o.W: In einer Kiste befinden sich sechs verschiedenfarbige Kugeln, von denen vier Kugeln gezogen werden. Wie viele Möglichkeiten gibt es, die Auswahl von vier Kugeln zu ordnen?

V.m.W: In einer Kiste befinden sich sechs verschiedenfarbige Kugeln, von denen vier Kugeln gezogen werden. Nach jedem Ziehen wird die gezogene Kugel zurück in die Urne gelegt. Wie viele mögliche Kombinationen an gezogenen Kugeln gibt es? Berechne die Kombinationen.

K.o.W: Beim Lotto werden sechs Zahlen aus insgesamt 49 gewählt. Wie viele Möglichkeiten gibt es?

K.m.W: In einem Gefäß befinden sich sechs verschiedenfarbige Kugeln. Es werden drei der Kugeln gezogen, wobei die gezogene Kugel nach jedem Zug wieder zurückgelegt wird (= mit Wiederholung).

Diskrete Wahrscheinlichkeit 1 & 2

Laplace'sche Wahrscheinlichkeit

Wenn **jede Möglichkeit**, die wir in der Kombinatorik eruiert haben, **gleichwahrscheinlich** ist, gilt die **Laplace'sche Wahrscheinlichkeitsformel**.

$$p = \frac{\text{Anzahl günstige Fälle}}{\text{Anzahl mögliche Fälle}} = \frac{|A|}{|\Omega|}$$

günstige Fälle: Wsk von einem oder mehreren möglichen Fällen / Resultate / Möglichkeiten (Aufgabenstellung)
mögliche Fälle: Anzahl Möglichkeiten / Resultate / Fälle (Kombinatorik)

Bsp.

Sie füllen einen Lottozettel (6 aus 49) mit 20 verschiedenen Kombinationen fürs Lotto aus. Wie gross ist die Chance den 6-er zu holen?

Lösung:

Anzahl Mögliche Fälle: → Kombination ohne Wiederholung → $\binom{49}{6} = 13'983'816$

Anzahl günstige Fälle: → Aus Aufgabenstellung → 20

$$\rightarrow p = \frac{20}{13'983'816} = \text{ca. } 1: 700'000$$

Grundlagen der Wahrscheinlichkeitstheorie

Grundbegriffe (Stichprobenraum, Ereignisse, etc.)

- **Zufallsexperiment:** Vorgang, der unter ganz bestimmten, reproduzierbaren Voraussetzungen durchgeführt und beliebig oft wiederholt werden kann. Dabei hängt das **Resultat alleine vom Zufall ab**.
- **Versuch:** Ist eine Durchführung des Zufallsexperiments
- **Ergebnis**(auch Elementarereignis): Resultat des Versuches
- **Stichprobenraum(S)**(auch Ergebnismenge): Menge aller möglichen Ergebnisse
 - o **Doppelte Einträge/Werte:** Hat bspw. Ein Würfel zweimal dieselbe Zahl, dann wird diese in S trotzdem nur einmal vorkommen, da das Resultat dasselbe ist. Bsp. doppelte 5 → S = {1,2,3,4,5}
- **Elementarereignis:** Ein Element des Stichprobenraums
- **Ereignis:** Teilmenge des Stichprobenraums/Ergebnissen (mit A,B,C,... abgekürzt)
 - o **Maximal mögliche Ereignisse:** Potenzmenge von 2^S, also 2^{|S|}, sprich 2 hoch |S|. Bsp. 6-er Würfel: |S| = 6 → 2⁶ = 64
- **Wahrscheinlichkeit:** Mit **Zahl p** gewichtete Chance, dass bei einem Zufallsexperiment ein bestimmtes Ereignis eintritt. (Wsk ist immer zwischen 0 und 1 (0%-100%))
 - o Wsk für sicheres Ereignis = 1
 - o Wsk für unmögliches Ereignis = 0

Bsp. Münzwurf

Stichprobenraum S = Kopf & Zahl = {K,Z}

Es gilt nun:

Ereignis K = „Kopf zu würfeln“ mit P(K) = $\frac{1}{2}$.

Ereignis Z = „Zahl zu würfeln“ mit P(Z) = $\frac{1}{2}$.

Ereignis S = „Kopf oder Zahl zu würfeln“ mit P(S) = 1 (also das sichere Ereignis).

Ereignis Ø = „Münze bleibt auf dem Rand stehen“ mit P(Ø) = 0 (also das unmöglichere Ereignis).

Mögliche Ereignisse: |S| = 2 (Da es zwei mögliche Resultate gibt) → |2^S| = 2² = 4 **mögliche Teilmengen**

Unendlicher Stichproberaum

Je nach Art des **Experiments** kann $S = \text{Stichproberaum}$ endlich oder unendlich sein.

Das **Resultat** muss aber eines der **Elemente von S sein** und heisst deshalb **Elementarereignis**.

Bsp.

Wählerbefragung	$S = \{\text{FDP; CVP; SVP; SP; Grüne; sonstige links; „Neue Mitte“; sonstige rechts}\}$	$ S = 8$
Beispiel 3.4: Glühdauer von Glühbirnen in Stunden.	$S = \mathbb{R}^+ = \text{positive, reelle Zahl}$	$ S < \infty$
Beispiel 3.5: Anzahl Würfe bis eine 6 gewürfelt wird.	$S = \mathbb{N} = \text{natürliche Zahl}$	$ S < \infty$
Beispiel 3.6: Anzahl Zerfälle.	$S = \mathbb{N} = \text{natürliche Zahl}$	$ S < \infty$

2 Unterscheidbare Würfel

Mit 2 unterscheidbaren Würfeln (z.B. ein blauer und ein roter) einmal würfeln ist dasselbe wie mit einem Würfel zweimal hintereinander würfeln. Wobei die **Reihenfolge** der gewürfelten Resultate **relevant** ist. Die **Ergebnismenge S** lautet:

$$S = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (3, 1), (3, 2), (3, 3), (3, 4), (3, 5), (3, 6), (4, 1), (4, 2), (4, 3), (4, 4), (4, 5), (4, 6), (5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6), (6, 1), (6, 2), (6, 3), (6, 4), (6, 5), (6, 6)\}$$



- Reihenfolge relevant $\rightarrow (3,6)$ & $(6,3)$ sind **nicht identisch**
- **Jedes Elementarereignis** hat die **gleiche Wahrscheinlichkeit** = $1/36$.
- Es gibt $6^2 = 36$ verschiedene Anordnungen, d.h. $|S| = 36$

2 nicht unterscheidbare Würfel

Mit 2 nicht unterscheidbaren Würfeln einmal würfeln (resp. mit einem Würfel zweimal würfeln, wobei die **Reihenfolge nicht betrachtet** wird) ergeben eine **andere Wahrscheinlichkeitsverteilung**. Die **Ergebnismenge S** lautet:

$$S = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (3, 1), (3, 2), (3, 3), (3, 4), (3, 5), (3, 6), (4, 1), (4, 2), (4, 3), (4, 4), (4, 5), (4, 6), (5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6), (6, 1), (6, 2), (6, 3), (6, 4), (6, 5), (6, 6)\}$$

- **Reihenfolge ist nicht relevant.** Ergebnis $(1,6)$ und $(6,1)$ **ist identisch**.
- Elementarereignisse der Form (ii) haben die Wsk $1/36$, die der Form (ij) mit $i \neq j$ und $i < j$ haben die Wsk $1/18$.
- Mit Zählen der Elemente $(6 + 5 + 4 + 3 + 2 + 1)$ in S erhalten wir auch $|S| = 21$

Bsp. #1

	1 Würfel:	2 unterscheidbare Würfel:	2 nicht unterscheidbare Würfel:
Ergebnismenge $\Omega =$	{1; 2; ...; 6}	{11, 12, ..., 16, 21, 22, ..., 26, 31, ..., 61, 62, ..., 66}	{11, 12, ..., 16, 22, 23, ..., 26, 33, 34, ..., 36, ..., 55, 56, 66}
$ S =$	6	$6^2 = 36$	21
$P(\text{Elementarereignisse})$	$= \frac{1}{6}$	$= \frac{1}{36}$	$P(ij) = \frac{1}{36}, P(ij) = \frac{1}{18} \text{ mit } i \neq j.$
$\# \text{ Ereignisse} = 2^n$	$2^n = 2^6$	$2^n = 2^{36}$	$2^n = 2^{21}$
Sicheres Ereignis = Ereignis mit Wsk. = $P(S) = 1$	„Augenzahl kleiner als 10 zu würfeln.“	„Eine zweistellige Augenzahl zu würfeln.“	„Eine zweistellige Augenzahl zu würfeln.“
Unmögliches Ereignis = Ereignis mit Wsk. = $P(\{\}) = 0$	„Augenzahl grösser als 10 zu würfeln.“	„Eine dreistellige Augenzahl zu würfeln.“	„Eine dreistellige Augenzahl zu würfeln.“
A = Ereignis „Augensumme ≤ 4 zu würfeln“	$A = \{1, 2, 3, 4\} = \frac{4}{36} = \frac{1}{9}$	$A = \{11, 12, 13, 21, 22, 31\} = \frac{6}{36} = \frac{1}{6}$	$A = \{11, 12, 13, 22\} = \frac{4}{36} + \frac{1}{18} + \frac{1}{18} + \frac{1}{36} = \frac{1}{6}$
B = Ereignis „Primzahl würfeln (*)“	$B = \{2, 3, 5\} = \frac{3}{36} = \frac{1}{12}$	$B = \{11, 13, 23, 31, 41, 43, 53, 61\} = \frac{8}{36} = \frac{2}{9}$	$B = \{11, 13, 23\} = \frac{3}{36} + 2 * \frac{1}{18} = \frac{5}{36}$

(*) 1 ist weder eine Primzahl noch eine zusammengesetzte Zahl!

Bsp. #2

- Berechnen Sie $P(AZ = 7)$ beim Würfeln von zwei nicht unterscheidbaren Würfeln.
- Berechnen Sie $P(AZ = 8)$ beim Würfeln von zwei unterscheidbaren Würfeln.
- Berechnen Sie $P(AZ = 8)$ beim Würfeln von zwei nicht unterscheidbaren Würfeln.

Lösung:

- $P(AZ = 7) = P((1, 6) + (2, 5) + (3, 4)) = 3 \cdot \frac{1}{18} = \frac{1}{6}$
- $P(AZ = 8) = P((2, 6) + (3, 5) + \dots + (6, 2)) = 5 \cdot \frac{1}{36} = \frac{5}{36}$
- $P(AZ = 8) = P((2, 6) + (3, 5) + (4, 4)) = 2 \cdot \frac{1}{18} + 1 \cdot \frac{1}{36} = \frac{5}{36}$

Mengenlehre vs. Wahrscheinlichkeit

Zusammenstellung der Gemeinsamkeiten (\subset =Teilmenge, \cap =und(Schnittmenge), \cup =oder, usw.)

Zeichen	Mengenlehre	Wahrscheinlichkeit
$\emptyset; \{\}$	Leere Menge	Unmögliches Ereignis
S	Grundmenge S	Sicheres Ereignis S
$A \subset S$	A ist Teilmenge von S	A ist ein Ereignis
$A \cap B$	A Durchschnitt B	Ereignis A und B treffen ein (*)
$A \cup B$	A Vereinigung B	Ereignis A oder B trifft ein (**)
\bar{A}	Komplementärmenge	Gegenereignis von A resp. A trifft nicht ein.
$A \cap B = \emptyset$	A und B sind disjunkt	A und B schliessen sich aus, resp. sie sind „unvereinbar“. Wenn A eintritt, dann kann B nicht eintreten, und umgekehrt.

(*) Logisches „Und“, d.h. „sowohl als auch“ trifft ein.

(**) Logisches „Oder“, d.h. „das Eine, das Andere oder beides“ trifft ein.

Wahrscheinlichkeit; Axiome von Kolmogorov

Definition

- **A, B:** Ereignisse $\rightarrow P(A) = 0 \leq P(A) \leq 1 \rightarrow P(B) = 0 \leq P(B) \leq 1$
- **\bar{A} :** Gegenereignis
- **S:** sichere Ereignis $\rightarrow P(S) = 1$
- **\emptyset :** unmögliche Ereignis

Annahmen/Regeln/Formeln

- Seien **A und B unvereinbare (= disjunkte)** Ereignisse (d.h. $A \cap B = \emptyset$), so gilt:

$$P(A \cup B) = P(A) + P(B)$$

- Daraus folgt:

$$P(\emptyset) = P(\{\}) = 0$$

$$P(\bar{A}) = 1 - P(A)$$

- Seien A_1, A_2, \dots, A_n **n paarweise unvereinbare** Ereignisse, so gilt:

$$P(A_1 \cup A_2 \cup \dots \cup A_n) = P(A_1) + P(A_2) + \dots + P(A_n) = \sum_{i=1}^n P(A_i)$$

- Seien **A und B beliebige** Ereignisse, so gilt:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Gleichverteilung

Besteht der Stichprobenraum S aus den n Elementarereignissen x_1, x_2, \dots, x_n , die alle mit der selben Wahrscheinlichkeit eintreten, dann hat man (nach Laplace) die **Gleichverteilung**:

$$p(x_i) = \frac{1}{|S|}, \quad i = 1, 2, \dots, n.$$

Die Wahrscheinlichkeit eines Ereignisses A des endlichen Stichprobenraumes S von lauter gleich wahrscheinlichen Ereignissen ist gegeben durch:

$$p(A) = \frac{|A|}{|S|} = \frac{\text{Anzahl günstige Fälle}}{\text{Anzahl mögliche Fälle}}$$

Bsp. Würfeln mit fairem Würfel

$$S = \{1, 2, 3, 4, 5, 6\}$$

Wie gross ist die Wsk einer «eins» zu würfeln?

$$P(AZ = 1) = P(x_1) = \frac{1}{|S|} = \frac{1}{6}$$

Wie gross ist die Wsk einer «gerade Zahl» zu würfeln?

$$A = \{2, 4, 6\}$$

$$P(A) = \frac{|A|}{|S|} = \frac{3}{6} = \frac{1}{2}$$

Bsp. #2

In einer Reinigungsfirma arbeiten **7 fix zusammengestellte Teams à 3 Mitarbeiter**. Für einen besonders heiklen Reinigungsauftrag muss der Chef von den **21 Mitarbeiter** 3 per Los bestimmen. Wie gross ist die Wahrscheinlichkeit, dass die Zusammensetzung der 3 Leute gerade einem der **7 Teams** entspricht?

Lösung

$$\text{Anzahl Möglichkeiten 3 aus 21: } \binom{21}{3} = \frac{21!}{18! \cdot 3!} = \frac{21 \cdot 20 \cdot 19}{1 \cdot 2 \cdot 3} = 7 \cdot 10 \cdot 19$$

$$\text{Wahrscheinlichkeit} = \frac{\# \text{ günstige Fälle}}{\# \text{ mögliche Fälle}} = \frac{7}{7 \cdot 10 \cdot 19} = \frac{1}{10 \cdot 19} = \frac{1}{190} = 0,00526$$

Wichtige Regeln im Detail

Ergebnisse sind **unabhängig**, wenn folgendes gilt: $P(A \cap B) = P(A) \cdot P(B)$

Wahrscheinlichkeit des Gegenereignisses(höchstens/mindestens eine ...)

Wird häufig verwendet, wenn in die Frage nach «**mindestens eine ...**» oder «**höchstens eine**» gestellt wird.

Falls A ein Ereignis des Stichprobenraumes S ist, dann gilt für deren Komplement:

$$p(\bar{A}) = 1 - p(A). \quad \text{resp. } P(A) = 1 - P(\bar{A})$$

Achtung: **Gegenteil von «mind. einmal ...» ist «nie eine ...»**

Bsp.

Sie würfeln 4-mal mit einem Würfel. Wie gross ist die Wahrscheinlichkeit, dass Sie mindestens einmal ein Sechs gewürfelt haben?

Lösung:

$$P(\text{mindestens eine Sechs}) = 1 - P(\text{nie eine Sechs}) = 1 - \frac{5}{6} \cdot \frac{5}{6} \cdot \frac{5}{6} \cdot \frac{5}{6} = 1 - \left(\frac{5}{6}\right)^4 = 1 - \frac{625}{1296} = \frac{671}{1296} = \text{ca. 51.8 \%}$$

(Wsk nie eine Sechs = Anzahl Würfe * Wsk keine sechs zu Würfeln in einem Wurf ($\frac{5}{6}$))

Additionssatz

Falls A_1 und A_2 zwei Ereignisse des Stichprobenraumes S sind, dann gilt die Additionsregel:

$$p(A_1 \cup A_2) = p(A_1) + p(A_2) - p(A_1 \cap A_2).$$

Wichtig: - $p(A_1 \cap A_2)$ nicht vergessen.

Für mehrere oders, bsp 3-oder-Ereignisse:

$$P(A_1 \cup A_2 \cup A_3) = P(A_1) + P(A_2) + P(A_3) - P(A_1 \cap A_2) - P(A_2 \cap A_3) - P(A_1 \cap A_3) + P(A_1 \cap A_2 \cap A_3)$$

Bsp. #1 - Zwölfer Würfel

Sie würfeln mit einem fairen „Zwölfer-Würfel“ (siehe Bild) einmal. Wie gross ist die **Wahrscheinlichkeit, dass Sie eine gerade Zahl oder Primzahl würfeln**.

Lösung direkt:

$$P(\{2,3,4,5,6,7,8,10,11,12\}) = 10/12 = 5/6$$

Lösung mit Additionssatz:

$$A = \text{„gerade Zahlen“} = \{2, 4, 6, 8, 10, 12\} \rightarrow P(A) = 6/12$$

$$B = \text{„Primzahl“} = \{2, 3, 5, 7, 11\} \rightarrow P(B) = 5/12$$

$$(A \cap B) = \{2\} \rightarrow P(A \cap B) = 1/12$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = \frac{6}{12} - \frac{5}{12} - \frac{1}{12} = \frac{11}{12} - \frac{1}{12} = \frac{10}{12} = \frac{5}{6}$$

Bsp. #2

Aus den Zahlen 1, 2, 3, ..., 100 wird zufällig eine Zahl gezogen. Mit welcher **Wahrscheinlichkeit** ist diese **Zahl durch 2 oder 5 teilbar**?

Lösung:

$$A_1 = \text{„Menge der Zahlen von 1-100, die durch 2 teilbar sind“} = \{2, 4, 6, \dots\}$$

$$A_2 = \text{„Menge der Zahlen von 1-100, die durch 5 teilbar sind“} = \{5, 10, 15, \dots\}$$

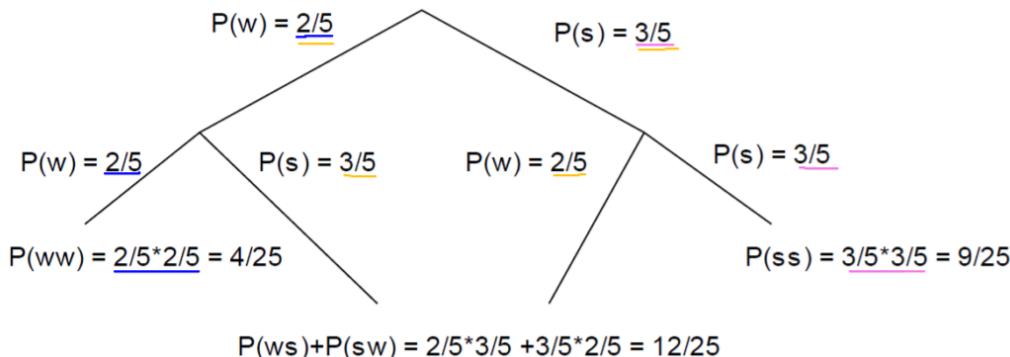
$$\begin{aligned} p(A_1 \cup A_2) &= p(A_1) + p(A_2) - p(A_1 \cap A_2) = \frac{|A_1|}{|S|} + \frac{|A_2|}{|S|} - \frac{|A_1 \cap A_2|}{|S|} \\ &= \frac{50}{100} + \frac{20}{100} - \frac{10}{100} = \frac{50 + 20 - 10}{100} = \frac{60}{100} = 0.6 \end{aligned}$$

$$A_1 \cap A_2 = \{10, 20, \dots, 90, 100\} \rightarrow |A_1 \cap A_2| = 10$$

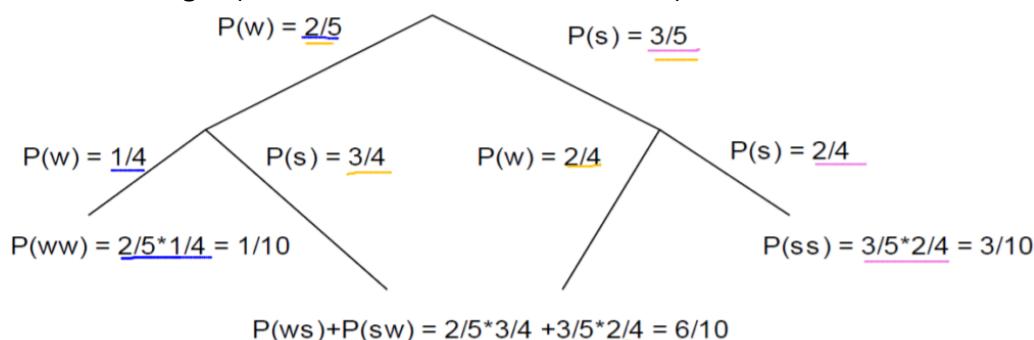
Mehrstufige Experimente – Baumdiagramm – Entscheidungsbäume

Gegeben sei eine Urne mit 2 weissen und 3 schwarzen Kugeln. Es wird **zweimal hintereinander** gezogen. Zeichnen Sie die Entscheidungsbäume für Ziehen ohne Zurücklegen und Ziehen mit Zurücklegen. Wie gross sind jeweils die Wahrscheinlichkeiten von zweimal schwarz, zweimal weiss, einmal schwarz und einmal weiss?

Mit zurücklegen (Wsk bleibt gleich nach erstem Ziehen)::



Ohne zurücklegen (Wsk ändert sich nach erstem Ziehen):

Bsp. Elfmeter

Ein weltbekannter Fussball-Profi hat bei Elfmeterschüssen eine **Trefferquote von 90%**.

1) Ergänzen Sie die fehlenden Wahrscheinlichkeiten (der Baum ist hier von links nach rechts nicht von oben nach unten gezeichnet).

2) Wie gross ist die Wahrscheinlichkeit, dass er bei zwei hintereinander ausgeführten Schüssen mindestens einen Treffer erzielt?

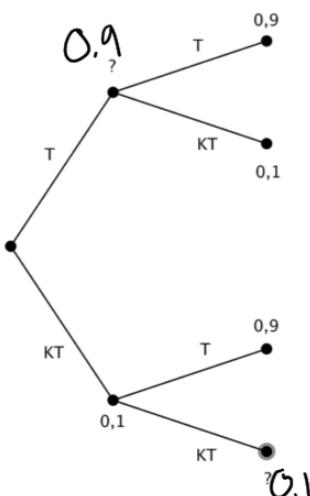
3) Wie gross ist die Wahrscheinlichkeit, dass er bei zwei hintereinander ausgeführten Schüssen beide trifft?

Lösung:

1) siehe rechts in der Grafik

2) $P(\text{min. 1 Treffer}) = 1 - P(\text{keinem Treffer}) = 1 - P(\text{KT} \cdot \text{KT}) = 1 - 0.1 = 0.99$

3) $P(\text{TT}) = P(\text{T}) \cdot P(\text{T}) = 0.9 \cdot 0.9 = 0.81$



Wahrscheinlichkeit einer Vereinigung mehrerer Mengen

Bsp.

Die Schule bietet Kurse in Fotografie, Informatik und Digitaltechnik an, die die Schüler auf freiwilliger Basis besuchen können. Von einer Klasse mit xy Schülern wählen:

- Neun Schüler den Fotokurs F = Anzahl Elemente in der Menge A
- Zwölf Schüler den Informatikkurs I = Anzahl Elemente in der Menge B
- Elf Schüler den Digitalkurs D = Anzahl Elemente in der Menge C
- Drei Schüler belegen F und I = Anzahl Elemente in der Menge A ∩ B
- Fünf Schüler belegen F und D = Anzahl Elemente in der Menge A ∩ C
- Sechs Schüler belegen I und D = Anzahl Elemente in der Menge B ∩ C
- Zwei Schüler belegen alle drei Kurse = Anzahl Elemente in der Menge A ∩ B ∩ C

Wie viele Schüler hat die Klasse?

Lösung:

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

Anzahl Schüler der Klasse: $|A \cup B \cup C| = 9 + 12 + 11 - 3 - 6 - 5 + 2 = 32 - 14 + 2 = 20$

Achtung: Addition vom letzten Teil ist wichtig, da dieser vorher zweimal korrekt und einmal zuviel **wegsubstriert** wird.

Wie viele Schüler belegen nur einen Kurs?

Lösung:

$\rightarrow 20 - (\text{Anzahl der Schüler, die zwei Kurse besuchen}) + 2 \text{ Mal} (\text{Anzahl der Schüler, die alle 3 Kurse besuchen}) =$
 Anzahl der Schüler, die nur einen Kurs besuchen, also: $20 - 3 - 6 - 5 + 2 * 2 = 10$.

Achtung: 2 mal, da dieser Teil dreimal subtrahiert wird, wir in aber eigentlich nur einmal subtrahieren möchten.

Mehr Beispiele dazu in [6-u-7-Disc-Prob-J-Schuler_V3-0.pdf](#) S. 30 ff.

Vertiefung der Wahrscheinlichkeitstheorie

Wahrscheinlichkeit von Ereignissen

Ergebnis (Elementarereignis) = Resultat aus Zufallsexperiment

Stichprobenraum (Ergebnismenge) = Menge der möglichen Ergebnisse

Ereignis = Teilmenge von S(Stichprobenraum)

Definition

Die Wahrscheinlichkeit des Ereignisses A ist gleich der Summe der Wahrscheinlichkeiten der Ergebnisse s in A:

$$p(A) = \sum_{s \in A} p(s).$$

Bsp.

Ein gezinkter Würfel hat die Eigenschaft, dass die **Zahl 3 doppelt so häufig wie jede andere Zahl** fällt. Mit welcher Wsk würfelt man mit diesem Würfel eine ungerade Zahl?

Lösung:

Da **3 doppelt** so häufig vorkommt hat 3 die Wsk. **2p** und alle anderen Zahlen **1p**.

$$\rightarrow 1 = 5 * 1p + 2p = 7p \rightarrow p = \frac{1}{7}$$

d.h. **1,2,4,5,6** haben die Wsk. **1p** $= \frac{1}{7}$, 3 hat die Wsk **2p** $= \frac{2}{7}$

$$\rightarrow p(\text{«ungerade Zahl»}) = p(1) + p(3) + p(5) = \frac{1}{7} + \frac{2}{7} + \frac{1}{7} = \frac{4}{7} = 0.57$$

Unabhängige Ereignisse und bedingte Wahrscheinlichkeit

Unabhängige Ereignisse

Zwei Ereignisse A und B heißen unabhängig:

$$P(A \cap B) = P(A) * P(B)$$

sonst heißen sie abhängig.

Bsp.

	1 Würfel:	2 unterscheidbare Würfel:	2 nicht unterscheidbare Würfel:
A = Ereignis „Summe ≤ 4 zu würfeln“	$A = \{1, 2, 3, 4\} = \frac{4}{6}$	$A = \{11, 12, 13, 21, 22, 31\} = \frac{6}{36} = \frac{1}{6}$	$A = \{11, 12, 13, 22\} = \frac{1}{36} + \frac{1}{18} + \frac{1}{18} + \frac{1}{36} = \frac{1}{6}$
B = Ereignis „Primzahl würfeln (*)“	$B = \{2, 3, 5\} = \frac{3}{6}$	$B = \{11, 13, 23, 31, 41, 43, 53, 61\} = \frac{8}{36} = \frac{2}{9}$	$B = \{11, 13, 23\} = \frac{1}{36} + 2 * \frac{1}{18} = \frac{5}{36}$
A und B würfeln	$A \cap B = \{2, 3\} = \frac{1}{3}$	$A \cap B = \{11, 13, 31\} = \frac{1}{12}$	$A \cap B = \{11, 13\} = \frac{1}{12}$
$P(A) * P(B)$	$\frac{4}{6} * \frac{3}{6} = \frac{1}{3}$	$\frac{1}{6} * \frac{2}{9} = \frac{1}{27}$	$\frac{1}{6} * \frac{5}{36} = \frac{5}{216}$
Abhängig oder unabhängig?	Unabhängig, da $P(A \cap B) = P(A) * P(B)$	Abhängig, da $P(A \cap B) \neq P(A) * P(B)$	Abhängig, da $P(A \cap B) \neq P(A) * P(B)$

- Unabhängig = keine gegenseitige Beeinflussung, Modell oft «Ziehen mit Zurücklegen»
- Abhängig = gegenseitige Beeinflussung, Modell oft „Ziehen ohne Zurücklegen“.

Bsp.

Ein Bitstring der Länge 4 wird zufällig erzeugt. Wir betrachten die beiden Ereignisse

- A = „String enthält mindestens zwei aufeinanderfolgende 0-en..“
- B = „erstes Bit ist 0,“ und

Bestimmen Sie durch überprüfen mit der Bedingung $P(A \cap B) = P(A) * P(B)$, ob die Ereignisse A und B unabhängig voneinander sind oder nicht.

Lösung:

$$S = 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111 \rightarrow |S| = 16$$

$$A = \{0000, 0001, 0010, 0011, 0100, 1000, 1001, 1100\} \rightarrow P(A) = 8/16 = 1/2$$

$$B = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111\} \rightarrow P(B) = 8/16 = 1/2$$

$$A \cap B = \{0000, 0001, 0010, 0011, 0100\} \rightarrow P(A \cap B) = 5/16$$

$$P(A) * P(B) = \frac{1}{2} * \frac{1}{2} = 1/4 \rightarrow \text{nicht gleich } 5/16 \rightarrow \text{also sind die Ereignisse A und B voneinander abhängig.}$$

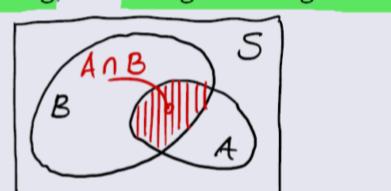
Bedingt Wahrscheinlichkeit (mit Voraussetzung)

Eine typische Frage lautet: „Beim dreimaligen Werfen einer fairen Münze wissen wir, dass beim ersten Mal „Kopf“ geworfen wurde. Wie gross ist dann die Wahrscheinlichkeit, dass eine ungerade Anzahl „Kopf“ geworfen wurden?“

Sind A und B zwei Ereignisse mit $p(B) > 0$, dann bezeichnet man die Wahrscheinlichkeit von A unter der Voraussetzung B mit $p(A|B)$.

Die Wahrscheinlichkeit für das Ereignis A unter der Voraussetzung, dass Ereignis B eingetreten ist, ist gegeben durch

$$p(A|B) = \frac{p(A \cap B)}{p(B)}$$



W'keit von A unter der Voraussetzung B, Oder der Bedingung B.

Interpretation der bedingten Wahrscheinlichkeit mit Flächen:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

entspricht dem **Verhältnis** der **schräffierten Fläche** ($A \cap B$) zur **Fläche B**. → Klar da die Formel $P(A \cap B)/B$ lautet.

Entsprechend:

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{P(A \cap B)}{P(A)}$$

entspricht dem **Verhältnis** der **schräffierten Fläche** ($B \cap A$) = ($A \cap B$) zur **Fläche A**.

Achtung: $P(A|B) \neq P(B|A)$

Bei unabhängigen Ereignissen gilt:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A) \cdot P(B)}{P(B)} = P(A)$$

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{P(B) \cdot P(A)}{P(A)} = P(B)$$

Bsp.

	1 Würfel:	2 unterscheidbare Würfel.	2 nicht unterscheidbare Würfel:
$A = \text{Ereignis „Summe} \leq 4 \text{ zu würfeln“}$	$A = \{1, 2, 3, 4\} = P(A) = \frac{2}{3}$	$A = \{11, 12, 13, 21, 22, 31\} P(A) = \frac{6}{36} = \frac{1}{6}$	$A = \{11, 12, 13, 22\} P(A) = \frac{1}{36} + \frac{1}{18} + \frac{1}{18} + \frac{1}{36} = \frac{1}{6}$
$B = \text{Ereignis „Primzahl würfeln“}$	$B = \{2, 3, 5\} P(B) = \frac{1}{2}$	$B = \{11, 13, 23, 31, 41, 43, 53, 61\} P(B) = \frac{8}{36} = \frac{2}{9}$	$B = \{11, 13, 23\} P(B) = \frac{1}{36} + 2 * \frac{1}{18} = \frac{5}{36}$
$A \text{ und } B \text{ würfeln}$	$A \cap B = \{2, 3\} P(A \cap B) = \frac{1}{3}$	$A \cap B = \{11, 13, 31\} P(A \cap B) = \frac{1}{12}$	$A \cap B = \{11, 13\} P(A \cap B) = \frac{1}{12}$
$P(A B) = \frac{P(A \cap B)}{P(B)}$ (*)	$\frac{P(A \cap B)}{P(B)} = \frac{\frac{1}{3}}{\frac{1}{2}} = \frac{2}{3}$ $P(A B) = 2/3$	$\frac{P(A \cap B)}{P(B)} = \frac{1/12}{2/9} = \frac{3}{8}$ $P(A B) = 3/8$	$\frac{P(A \cap B)}{P(B)} = \frac{1/12}{5/36} = \frac{3}{5}$ $P(A B) = 3/5$ (*)
Abhängig oder unabhängig? (**)	Da A und B unabhängig, $P(A B) = P(A) = \frac{2}{3}$	Abhängig	Abhängig
$P(B A) = \frac{P(B \cap A)}{P(A)}$	$\frac{P(B \cap A)}{P(A)} = \frac{1/3}{2/3} = \frac{1}{2}$ $P(B A) = \frac{1}{2}$	$\frac{P(B \cap A)}{P(A)} = \frac{1/12}{1/6} = \frac{1}{2}$ $P(B A) = 3/6 = \frac{1}{2}$	$\frac{P(B \cap A)}{P(A)} = \frac{1/12}{1/6} = \frac{1}{2}$ $P(B A) = \frac{1}{2}$
Abhängig oder unabhängig? (***)	Da A und B unabhängig, gilt: $\frac{P(B \cap A)}{P(A)} = P(B) = \frac{1}{2}$	Abhängig, da $P(A \cap B) \neq P(A) * P(B)$	Abhängig, da $P(A \cap B) \neq P(A) * P(B)$

(*) Wie gross ist die Wsk. dass $A = \{11, 12, 13, 22\}$, wenn ich weiss, dass $B = \{11, 13, 23\}$ gewürfelt wurde. 34

Diese Wsk. reduziert sich auf die Fragen wie gross ist die Wsk. dass 11 oder 13 gewürfelt wurde wenn ich weiss, dass 11, 13 oder 23 gewürfelt wurde. Diese Wsk. ist nicht etwa 2/3, da die Elementarereignisse nicht gleichwahrscheinlich sind.

(**) Bei Unabhängigkeit von den Ereignissen A und B gilt:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A) \cdot P(B)}{P(B)} = P(A)$$

(***) Bei Unabhängigkeit von den Ereignissen A und B gilt:

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{P(B) \cdot P(A)}{P(A)} = P(B)$$

Bsp. #2 – Lotto

In einem bestimmten Lottospiel muss man 6 Zahlen zwischen 1 und 30 raten. Nun werden in der Ziehung die Zahlen 1, 14, 15, 20, 23 & 27 gezogen. Sie erfahren aber lediglich, dass die Zahl 15 gezogen wurde. Um wieviel wird Ihre Gewinnchance durch diese Information vergrößert?

Lösung:

A = «Die Zahlen 1, 14, 15, 20, 23, 27 wurden gezogen»

B = «Die Zahl 15 wurde gezogen»

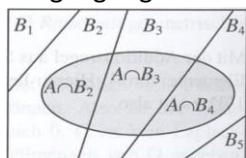
$$\rightarrow p(A|B) = \frac{p(A \cap B)}{p(B)} = \frac{p(A)}{p(B)} = \frac{\frac{1}{\binom{29}{5}}}{\frac{1}{\binom{29}{6}}} = \frac{1}{\binom{29}{5}} = \frac{1}{593775}$$

$\rightarrow p(A) = \frac{1}{\binom{30}{6}}$, d.h. $p(A) / p(A|B) = 5 \rightarrow$ Gewinnchancen sind um den Faktor 5 gestiegen.

Satz von Bayes*Satz der totalen Wahrscheinlichkeit*

$$P(A) = \sum_{i=1}^k P(A|B_i) \cdot P(B_i)$$

Ausgangslage:

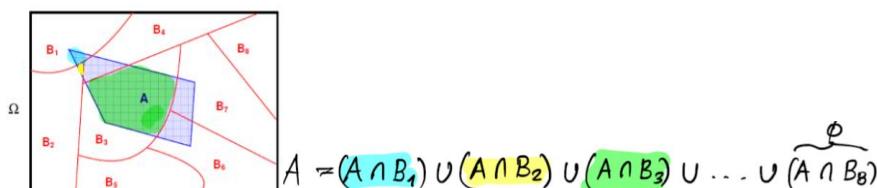
Voraussetzungen für den Satz von Bayes:

B_1, B_2, \dots, B_k bilden ein vollständiges System im Wahrscheinlichkeitsraum Ω wenn:

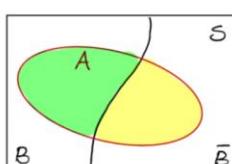
- **B_1, B_2, \dots, B_k paarweise disjunkt** sind (keine Überschneidungen)
- Die **Vereinigung** der B_k Ω ergibt, d.h.

$$\Omega = \bigcup_{i=1}^k B_i$$

Man nennt eine solche Zerlegung auch disjunkte Zerlegung von Ω .

Bsp.

Spezialfall für A und \bar{A} :



Spezialfall:

- $B, \bar{B} \subset S$ (vollständige Zerlegung)
- $p(B), p(\bar{B}) > 0$
- Ereignis A

Dann gilt:

$$p(A) = p(A|B) \cdot p(B) + p(A|\bar{B}) \cdot p(\bar{B})$$

$$p(A|B) = \frac{p(A \cap B)}{p(B)}$$

$$p(A|\bar{B}) = \frac{p(A \cap \bar{B})}{p(\bar{B})}$$

$$A = (A \cap B) \cup (A \cap \bar{B}) \rightarrow p(A) = p(A \cap B) + p(A \cap \bar{B})$$

disjunkt, d.h. wenn man sie schneidet kriegt man \emptyset "leere Menge"

Prüfungsbeispiel – Satz der Totalen Wahrscheinlichkeit

In 3 Säcken befinden sich **blaue und schwarze Kugeln**, und zwar in **B₁ (5 b & 3 s)**, in **B₂ (6 b & 2 s)** und in **B₃ (13 b & 3 s)**. Es wird zufällig in eine der 3 Säcke gegriffen und **eine Kugel gezogen**. Die Säcke sind verschieden gross. Die zweite ist nur **halb so gross wie die erste**. Die dritte ist **doppelt so gross wie die erste**. Die **Wahrscheinlichkeit** aus einer bestimmten Urne zu ziehen ist **proportional zu ihrer Grösse**.

Wie gross ist die Wahrscheinlichkeit, dass die Kugel **schwarz** (= Ereignis A) ist?

Lösung:

A = «schwarze Kugel gezogen»

B_k = «Aus Sack B_k wurde gezogen»

Schritt 1: Bestimmen der P(B_i) → Wsk. Das aus einem der Säcke gezogen wird.

$$p = \text{Grösse von } B_1 \rightarrow 1 = P(B_1) + P(B_2) + P(B_3) = p + \frac{1}{2}p + 2p \rightarrow 2 = 2p + p + 4p = 7p \rightarrow p = \frac{2}{7}$$

$$\text{Also: } P(B_1) = \frac{2}{7}; P(B_2) = \frac{1}{7}; P(B_3) = \frac{4}{7};$$

Schritt 2: Bestimmen von P(A).

$$P(A) = \sum_{i=1}^3 P(A|B_i) \cdot P(B_i) = \underline{P(A|B_1)} \cdot P(B_1) + \underline{P(A|B_2)} \cdot P(B_2) + \underline{P(A|B_3)} \cdot P(B_3)$$

$$P(A) = \sum_{i=1}^3 P(A|B_i) \cdot P(B_i) = \frac{3}{8} \cdot \frac{2}{7} + \frac{2}{8} \cdot \frac{1}{7} + \frac{3}{16} \cdot \frac{4}{7} = \frac{6}{56} + \frac{2}{56} + \frac{12}{56} = \frac{19}{56} = \frac{1}{4}$$

→ Mit einer Wsk. von $\frac{1}{4} = 25\%$ wird eine schwarze Kugel gezogen.

Satz von Bayes (mit P(B|A) zu P(A|B))

Die gesuchte **bedingte Wahrscheinlichkeit P(A|B)** kann nicht direkt berechnet werden. Sie muss durch die **bedingte – und gemäss Aufgabenstellung bekannte - Wahrscheinlichkeit P(B|A)** ausgedrückt werden.

→ **P(A|B) gesucht**, aber **P(B|A) gegeben**.

Wir wissen:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \Rightarrow P(A \cap B) = P(A|B) \cdot P(B)$$

und

$$P(B|A) = \frac{P(A \cap B)}{P(A)} \Rightarrow P(A \cap B) = P(B|A) \cdot P(A)$$

Daraus folgt:

$$P(A|B) \cdot P(B) = P(B|A) \cdot P(A)$$

Und damit:

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}, \text{ mit der Voraussetzung } P(B) \neq 0$$

resp.

$$P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}, \text{ mit der Voraussetzung } P(A) \neq 0$$

Bsp. Fortführung von oben

Es wurde eine schwarze Kugel gezogen, wie gross ist die Wahrscheinlichkeit, dass sie aus dem Sack B₁, B₂ resp. B₃ gezogen wurde?

Lösung: Gesucht ist

$$\begin{aligned} P(B_i|A) &= \frac{P(A|B_i) \cdot P(B_i)}{P(A)} \\ P(B_1|A) &= \frac{P(A|B_1) \cdot P(B_1)}{P(A)} = \frac{\frac{3}{8} \cdot \frac{2}{7}}{\frac{1}{4}*} = \frac{3}{7} \quad \left. \right\} = 1 \checkmark \\ P(B_2|A) &= \frac{P(A|B_2) \cdot P(B_2)}{P(A)} = \frac{\frac{2}{8} \cdot \frac{1}{7}}{\frac{1}{4}} = \frac{1}{7} \\ P(B_3|A) &= \frac{P(A|B_3) \cdot P(B_3)}{P(A)} = \frac{\frac{3}{16} \cdot \frac{4}{7}}{\frac{1}{4}} = \frac{3}{7} \end{aligned}$$

→ B₁ = 3/7
→ B₂ = 1/7
→ B₃ = 3/7

Weitere Beispiele dazu in [6-u-7-Disc-Prob-J-Schuler_V3-0.pdf](#) S. 40 ff.

Multiplikationssatz für beliebige zwei Ergebnisse ($P(A \cap B)$ berechnen für Additionssatz)

Der **Additionssatz** lautet: $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

→ $P(A \cap B)$ ist manchmal schwer zu berechnen.

Multiplikationssatz

$$P(A \cap B) = P(A|B) \cdot P(B) = P(B|A) \cdot P(A)$$

$P(B)$ & $P(A)$ dürfen **nicht 0** sein.

→ Also gilt nun für $P(A \cap B)$:

$$\begin{aligned} P(A \cup B) &= P(A) + P(B) - P(A \cap B) \\ &= P(A) + P(B) - P(A|B) \cdot P(B) \\ &= P(A) + P(B) - P(B|A) \cdot P(A) \end{aligned}$$

Zusammenfassung Berechnung von $P(A \cap B)$

Formel	$P(A \cap B) =$	Bedingung	Wie berechnen?
I)	0	$\Leftrightarrow A$ und B unvereinbar	Klar
II)	$P(A) \cdot P(B)$	$\Leftrightarrow A$ und B unabhängig	klar
III)	$P(A) \cdot P(B A)$	Gilt immer cf. Multiplikationssatz	<ul style="list-style-type: none"> ➢ Mit Satz von Bayes, dazu muss aber $P(A B)$ bekannt sein. ➢ Ev. kann $P(B A)$ mit Laplace gerechnet werden.
IV)	$P(B) \cdot P(A B)$	Gilt immer cf. Multiplikationssatz	<ul style="list-style-type: none"> ➢ Mit Satz von Bayes, dazu muss aber $P(B A)$ bekannt sein. ➢ Ev. kann $P(A B)$ mit Laplace gerechnet werden.
V)	$P(A \cap B)$	-----	<ul style="list-style-type: none"> ➢ Mit der Summe der Wsk. der Elementarereignisse ➢ Mit Entscheidungsbaum ➢ Ev. mit Laplace ➢ Mit dem Multiplikationssatz

Bsp. Verfügbarkeit eines Systems (Seite 47)

Ein System enthält 3 Komponententypen. Für einen erfolgreichen Betrieb **muss** die **Komponente K1** und **mindestens eine** der **Komponente K2 und K3** laufen.

a) **Beschreiben Sie das Ereignis G = „System funktioniert“, mit den Ereignissen A = „K1 läuft“, B = „K2 läuft“ und C = „K3 läuft“ in der Mengenschreibweise.**

b) Wie gross ist die Verfügbarkeit des Systems, wenn die Verfügbarkeit von **K1 95%**, von **K2 90%** und von **K3 80%** beträgt und man davon ausgehen kann, dass alle 3 Komponenten **unabhängig voneinander arbeiten**?

Lösung für a:

Das Gesamtsystem läuft, wenn A und (B oder C) laufen, also: $G = A \cap (B \cup C)$

Lösung für b:

Wegen der Unabhängigkeit der 3 Komponenten gilt:

$$\begin{aligned} P[G] &= P[A \cap (B \cup C)] = P[A] * P[B \cup C] = P[A] * \{P[B] + P[C] - P[B \cap C]\} \\ &= P[A] * \{P[B] + P[C] - P[B] * P[C]\} = \\ &= 0,95 * \{0,90 + 0,80 - 0,90 * 0,80\} = 0,9310 \end{aligned}$$

Resultat: Das System hat eine Verfügbarkeit von 93,10 %.

Wahrscheinlichkeitsverteilungen, Verteilungsfunktion

Wahrscheinlichkeitsverteilung

Allen Ergebnissen r des Stichprobenraums ordne ich eine Wahrscheinlichkeit zu. Somit besteht eine **diskrete Wahrscheinlichkeitsverteilung aus einer endlichen Anzahl Paare der Form:**

(Ergebnis r ; Wahrscheinlichkeit, dass r eintritt)

Was wir dann in mathematischer Form wie folgt schreiben:

$$\{(r, P(X = r)) \mid \forall r \in X(S)\}$$

Bsp. (weisse Kugel, P(0.3))

Berechnung des Erwartungswertes $E[X]$ der Zufallsvariablen X

Der **Erwartungswert $E[X]$** einer Zufallsvariablen X ist das **Pendant zum Durchschnittswert** (arithmetisches Mittel) in der beschreibenden Statistik. Wir **multiplizieren jeden Wert der Zufallsvariablen** (also die Werte -50; -20; 60; 100) **mit ihren Wahrscheinlichkeiten** (also den Werten 4/10; 3/10; 2/10 1/10).

→ Erwartungswert $E[X]$ ist also das **Durchschnittsresultat**, welches erwartet wird, mit Berücksichtigung der Wsk.

$$E[X] = \sum_{i=1}^4 x_i \cdot p_i$$

x_i = Spezifischer Wert (= r von X , X ist Teilmenge von S , S sind alle reellen Zahlen)

p_i = Wahrscheinlichkeit des Wertes x_i

Bsp. Mit Kugeln von oben und deren Wsk.

$$E[X] = (-50)*4/10 + (-20)*3/10 + 60*2/10 + 100*1/10 = -20 -6 +12 + 10 = -4$$

→ Das heisst, die Spielcasinoleitung gewinnt bei einer langen Spielserie 4.- pro Spiel.

Berechnung der Varianz $Var[X]$ der Zufallsvariablen X (Volatilität)

Die **Varianz $Var[X]$** einer Zufallsvariablen X ist der **mittlere quadratische Abstand vom Erwartungswert**. Die **Varianz** (siehe auch „Varianz“ in der beschreibenden Statistik) ist ein **Mass der Variabilität**.

Oft nimmt man die **Wurzel aus der Varianz**, dieser Wert heisst **Streuung** $\sigma(X) = \sqrt{Var[X]}$

$$\text{Also: } \sigma^2(X) = Var[X] \Rightarrow \sigma(X) = \sqrt{Var[X]}$$

Berechnungsmethode 1

$$Var[X] = \sum_{i=1}^4 (x_i - E[X])^2 \cdot p_i$$

x_i = Spezifischer Wert

$E[X]$ = Erwartungswert (Meist zuerst ausrechnen mit Formel von oben)

p_i = Wahrscheinlichkeit des Wertes x_i

Bsp. $E[X] = 2$, $x_1 = -50$, $x_2 = 20$, $p_1 = 0.4$, $p_2 = 0.6$

$$Var[X] = (-50 - 2)^2 * 0.4 + (20 - 2)^2 * 0.6 = 1276$$

Berechnungsmethode 2

$$Var[X] = E[X^2] - (E[X])^2 = \sum_{i=1}^4 (x_i)^2 \cdot p_i - (\cancel{E[X]})^2 = \left(\sum_{i=1}^4 (x_i)^2 \cdot p_i \right) - (\cancel{E[X]})^2$$

Bsp. $E[X] = 2$, $x_1 = -50$, $x_2 = 20$, $p_1 = 0.4$, $p_2 = 0.6$

$$Var[X] = (-50)^2 * 0.4 + 20^2 * 0.6 - (2)^2 = 1240 - 4 = 1236$$

Einführung und Definitionen (Begriffe)

- **Diskrete Wahrscheinlichkeit:** „Eine diskrete Wahrscheinlichkeitsverteilung“ ist eine **endliche Anzahl Stäbe deren Länge zusammengezählt Eins ergibt**. Die Wahrscheinlichkeitsfunktion besteht also aus endlichen Werten. Diese Werte sind separat angegeben oder lassen sich mit einer Formel (z.B. Binomialverteilung) berechnen.

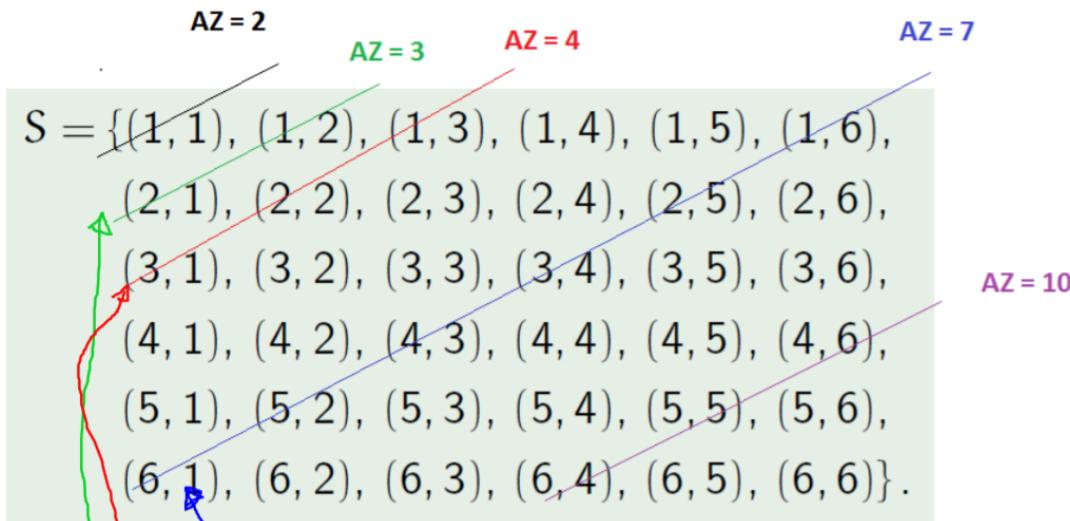
Einige Verteilmodelle

- **Gleichverteilung:** (z.B. Augenzahl bei einem fairen Würfel), allgemein: Laplace'sche Wsk.
- **Binomialverteilung:** (z.B. Anzahl „Nullen“ beim zufälligen Erzeugen eines Bitstrings der Länge n). Allgemein: Ein **Ziehen mit Zurücklegen** bei zwei verschiedenen Möglichkeiten.
- **Hypergeometrische Verteilung:** (z.B. erzielen von Anzahl defekter Teile). Allgemein: Ein **Ziehen ohne Zurücklegen** bei zwei verschiedenen Möglichkeiten.
- **Poisson Verteilung:** als **Approximation von Binomialverteilungen** und als **eigenständiges Modell** von „Anzahl Ereignisse in einem Kontinuum“, (z.B. Anzahl Autos, die in einer bestimmten Zeit über eine Brücke fahren).

Verteilungen ohne Modelle

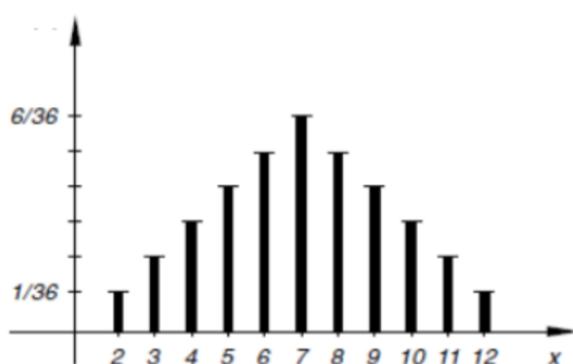
Es gibt auch Verteilungen, welche keinem Standardmodell entsprechen.

Bsp. Augensummen bei zwei fairen Würfeln



Durch einfaches Zählen können wir die Tabelle (= Wahrscheinlichkeitsfunktion, Wahrscheinlichkeitsverteilung) erstellen und damit deren Graphen zeichnen.

AZ	2	3	4	5	6	7	8	9	10	11	12
P(AZ)	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36



Die diskrete Gleichverteilung (Alle Wsk. sind gleich)

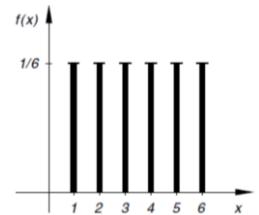
Alle Lösungen haben dieselbe Wahrscheinlichkeit.

Wahrscheinlichkeitsverteilung:

$$P(X = x_i) = \frac{1}{k} \quad (k = \text{Anzahl Ausprägungen})$$

Bsp. Augenzahl bei fairen Würfel

Wahrscheinlichkeitsverteilung: $P(X = x_i) = \frac{1}{6}$ $i = 1, \dots, 6$

Die Bernoulli-Verteilung (Einmal ziehen, mit zwei Mögliche Ausgänge mit unter. Wsk.)

Wir betrachten ein Zufallsexperiment mit zwei möglichen **Ausgängen E** (oder 1) und \bar{E} (oder 0), welche mit den **Wahrscheinlichkeiten p** und $q = 1 - p$ eintreten können.

Bernoulli = Einfache Ausführung, Binomialverteilung = x-fache Ausführun

Wahrscheinlichkeitsverteilung:

$$P(E) = p \text{ und } P(\bar{E}) = q = 1 - p$$

Bsp.

Beim Erzeugen eines zufälligen Bits (Zufallsbits) – z.B. mittels einem Zufallszahlengenerator – erhält man mit derselben Wahrscheinlichkeit eine Null oder eine Eins, d.h. $p = q = \frac{1}{2}$.

Würden wir dieses Experiment **n-mal ausführen**, so kommen wir automatisch zur **n-fachen Bernoulli-Verteilung was der Binomialverteilung entspricht**.

Die Binomialverteilung (Ziehen mit zurücklegen)

Z.B. **n-facher Münzwurf** (resp. n = Anzahl **durchgeführte Experimente**) mit gezinkter Münze ($p \neq \frac{1}{2}$ für Kopf) oder. mit fairer Münze ($p = \frac{1}{2}$). **Fragestellungen** der Art „trifft ein“ (codiert mit 1 oder mit Erfolg E) oder „trifft nicht ein“ (codiert mit 0 oder mit Misserfolg \bar{E}), resp. „ist wahr“ (codiert mit 1) oder „ist falsch“ (codiert mit 0), resp. „ist defekt“ (codiert mit 1) oder „ist nicht defekt“ (codiert mit 0).

Gesucht: Wahrscheinlichkeit, dass genau k Erfolge E eintreten. Für ($0 \leq k \leq n$ und $k \in \mathbb{N}$)

Wahrscheinlichkeitsverteilung:

$$B(k|n, p) = B_{n,p}(k) = C(n, k) \cdot p^k \cdot (1-p)^{n-k} = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}$$

k = genau k mal (wieviel gesuchtes eintrifft)

n = Anzahl Experimente/Durchführungen

p = mit Wahrscheinlichkeit

Mit TR: Menu:5:5:D + Menu:2:2 (Für Bruchdarstellung) Bsp. ($n \rightarrow n$, $p \rightarrow p$, $k \rightarrow x$, binomPdf(3,0.5,2))

Bsp. Erzeugen von Zufallsbits

$n = 3$, $p = \frac{1}{2} =$ Wsk. dass der Erfolg E = „Eine 1 wird erzeugt“ eintritt, resp. $q = (1 - p) = \frac{1}{2} =$ Wsk. dass E nicht eintritt („eine 0 wird erzeugt“) und $k = 2$:

$$\text{Für } k = 2 : \binom{3}{2} \cdot \left(\frac{1}{2}\right)^2 \cdot \left(1 - \frac{1}{2}\right)^{3-2} = \binom{3}{2} \cdot \frac{1}{8} = 3 \cdot \frac{1}{8} = \frac{3}{8}$$

Weitere Beispiele dazu in [6-u-7-Disc-Prob-J-Schuler_V3-0.pdf](#) S. 68 ff.

Die hypergeometrische Verteilung (Ziehen ohne zurücklegen - wegnehmen)

Wir wollen **von** einer **Menge(N)**, mit zwei verschiedenen Arten von Teilen, **n Teile herausnehmen und herausfinden mit welcher Wahrscheinlichkeit**, dass von diesen n Teilen genau k Teile eine bestimmte Eigenschaft haben (Bsp. weiss, falsch oder kaputt sind).

$$P(k) = \frac{\binom{M}{k} \cdot \binom{N-M}{n-k}}{\binom{N}{n}} = \frac{\# \text{günstige Fälle}}{\# \text{mögliche Fälle}}$$

M = Teile mit einer bestimmten Eigenschaft (Bsp. rote Kugeln/defekte Teile)

N = Alle Anzahl Teile (**M** ist eine Teilmenge von **N**) (Bsp. rote & blaue Kugeln / ganze und defekte Teile)

n = Anzahl Teile welche entnommen werden (Bsp. 5 Kugeln)

k = Anzahl gesuchter Teile mit Eigenschaft **M**, oder eben nicht **M** (Bsp. 3 rote Kugeln / 2 defekte Teile)

→ Output: Wahrscheinlichkeit, dass von diesen n-Teile genau k-Teile diese Eigenschaft haben. (Bsp. 3 rote Kugeln)

Zudem gilt folgendes:

1. n Teile können aus N Teilen auf $\binom{N}{n}$ Arten ausgewählt werden.
2. k defekte Teile können aus M defekten Teilen auf $\binom{M}{k}$ Arten ausgewählt werden.
3. n - k nicht defekte Teile können aus N - M nicht defekten Teilen auf $\binom{N-M}{n-k}$ Arten ausgewählt werden.

Es gilt für die Anzahl **günstige** Fälle: $\binom{M}{k} \cdot \binom{N-M}{n-k}$ und für die Anzahl **mögliche** Fälle: $\binom{N}{n}$

Bsp. Urne mit Kugeln

In einer Urne seien **N = 6 Kugeln**, davon **M = 3 weisse** und somit **N - M = 3 schwarze**. Wir ziehen **n = 2-Mal** ohne Zurücklegen. Wir bestimmen **p(k)** für **k ∈ {0, 1, 2}**. D.h. wie gross ist die Wahrscheinlichkeit, dass keine, genau eine resp. genau zwei weisse Kugeln gezogen werden.

Lösung:

$$P(k=0) = \frac{\binom{M}{k} \cdot \binom{N-M}{n-k}}{\binom{N}{n}} = \frac{\binom{3}{0} \cdot \binom{6-3}{2-0}}{\binom{6}{2}} = \frac{\binom{3}{0} \cdot \binom{3}{2}}{\binom{6}{2}} = \frac{1 \cdot 3}{\frac{6 \cdot 5}{2 \cdot 1}} = \frac{3}{15}$$

$$P(k=1) = \frac{\binom{3}{1} \cdot \binom{6-3}{2-1}}{\binom{6}{2}} = \frac{\binom{3}{1} \cdot \binom{3}{1}}{15} = \frac{3 \cdot 3}{15} = \frac{9}{15}$$

$$P(k=2) = \frac{\binom{3}{2} \cdot \binom{6-3}{2-2}}{\binom{6}{2}} = \frac{\binom{3}{2} \cdot \binom{3}{0}}{15} = \frac{3 \cdot 1}{15} = \frac{3}{15}$$

Die Poisson-Verteilung (μ , mittlere/erwartete Anzahl, Durchschnittl. /min, /m² – Anzahl E in Zeitraum)

Anwendung 1

Approximation der Binomialverteilung und damit auch der **Hypergeometrischen Verteilung**. Dabei wird **$\mu = n \cdot p$** gesetzt. Dann gilt für **k = 0, 1, 2, ...**

$$P(k) = \frac{\mu^k}{k!} \cdot e^{-\mu}$$

Anstatt der Binomialverteilung.

Bsp. #1 - mit $\mu = n \cdot p = 4 \cdot 0,05 = 0,2$

$$P(k) = \frac{0,2^k}{k!} \cdot e^{-0,2}$$

Für $k = 1 \rightarrow 0.1637$

Bsp. #2 – Grippeimpfung (für 3 Personen > als 2 Personen)

Die Wahrscheinlichkeit bei der Grippeimpfung an Nebenwirkungen zu erkranken ist $p = 0.001$. Nun werden $n = 2000$ Personen geimpft. Wie gross ist die Wahrscheinlichkeit, dass

- (i) genau 3 Personen
- (ii) mehr als 2 Personen

an diesen Nebenwirkungen erkranken? Verwenden Sie die Poissonverteilung!

Lösung: Der einzige Parameter in der Poissonverteilung ist der Mittelwert $\mu = np = 2000 \cdot 0.001 = 2$. Damit erhält man

- (i) genau 3 Personen: $p(k=3) = \frac{2^3}{3!} e^{-2} = \frac{4}{3} e^{-2} = 0.18$
- (ii) mehr als 2 Personen:

$$p(k>2) = [1 - (p(0) + p(1) + p(2))] = 1 - \left(\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!}\right) e^{-2} = 1 - (1 + 2 + 2) e^{-2} = 0.323$$

Anwendung 2:

Ausgehend von zufälligen Ereignissen, die innerhalb eines Kontinuums (z.B. Zeitraum, oder Messintervall) auftreten, definieren wir die Zufallsgrösse X: „Anzahl Ereignisse innerhalb eines Kontinuums“. Dabei handelt es sich um „gedächtnislose“ Ereignisse.

Anwendungsbeispiele:

1. Zahl von Staubteilchen auf einer Fläche
2. Anzahl radioaktive Zerfälle (Geigerzähler).
3. Zahl der Unwetter in einem Gebiet
4. Zahl der Unfälle in einem Zeitraum und oder Region
5. Anzahl rote Autos, die pro Tag vorbeifahren
6. Anzahl Telefonanrufe pro Stunde
7. Anzahl Tippfehler pro Seite
8. Anzahl Ausschussstücke in einer Produktion

Die **Wahrscheinlichkeit für das Eintreten eines Ereignisses hängt nur von der Länge des Intervalls**, nicht jedoch von der Lage auf dem Intervall ab. (! So ist das Modell definiert. Sollte bei einer konkreten Anwendung das nicht so sein, dann ist die Poissonverteilung nicht das geeignete Modell.) Die **Wahrscheinlichkeit für das k-malige Eintreten eines Ereignisses [P(k)] in diesem Kontinuum wird jetzt noch von der Intensitätsrate μ beeinflusst**.

$$P(k) = \frac{\mu^k}{k!} \cdot e^{-\mu}$$

Bsp. μ ist gegeben

Gegeben: $\mu = 1,5$

Gesucht: $P(k=3)$ und $p(k \leq 3)$

Lösung: $P(k=3) = \frac{1,5^3}{3!} \cdot e^{-1,5} = 0,12551$

Resp.

$$P(k \leq 3) = \sum_{k=0}^3 \frac{1,5^k}{k!} \cdot e^{-1,5} = \left(\frac{1,5^0}{0!} + \frac{1,5^1}{1!} + \frac{1,5^2}{2!} + \frac{1,5^3}{3!} \right) \cdot e^{-1,5} = 0,9344$$

Bsp. μ ist nicht gegeben

Das μ ist **nicht explizit gegeben** und **muss aus der Aufgabenstellung herausgelesen werden**. Aus der Aufgabenstellung wird das μ **umschrieben mit den Worten** wie z.B. „die mittlere Anzahl...“, „die erwartete Anzahl...“, „Durchschnittlich“, „im Schnitt“, „pro min“, „pro m²“ oder Ähnliches.

Gesucht: $P(X=k)$ oder $P(X \leq k)$

Weiter auf nächster Seite ...

Bsp.:

Beim Lackieren der Grundfarbe (Grundierung) von einem Kotflügel werden im Schnitt 10 Staubpartikel pro dm² einlackiert. Mit diesem Wissen, resp. der Angabe „im Schnitt werden 10“ können wir μ bestimmen (schätzen). In diesem Fall ist $\mu = 10$. Also:

$$P(k) = \frac{10^k}{k!} \cdot e^{-10}$$

$$\rightarrow \text{Für } P(2) = \frac{10^2}{2!} \cdot e^{-10} = 0.0023$$

Weitere Beispiele dazu in [6-u-7-Disc-Prob-J-Schuler_V3-0.pdf](#) S. 76 ff.

Strategie bei Verteilmodell-Aufgaben (Wsk von Teilmenge mit best. Eigenschaft)

Schritt 1: Wahl des richtigen Modells (wenn es für diese Aufgabe ein Modell gibt!)

Schritt 2: Mit den Angaben der Aufgabe (Text) sind die **Parameter des gewählten Models zu bestimmen**.

Schritt 3: Was für eine Wahrscheinlichkeit ist gesucht?

Schritt 4: Die gesuchte Wahrscheinlichkeit mit den Formeln rechnen.

Schritt 5: Resultatformulierung, vorzugsweise als Resultatsatz.

Wichtig: Bei **Aufgaben** nach der Wahrscheinlichkeit von einer **grösser als / kleiner als** einen bestimmten Wert ist es **manchmal einfacher** nicht die gewünschte Wahrscheinlichkeit direkt sondern **zuerst die Wahrscheinlichkeit der anderen Werte zu berechnen**. Und **danach 1 – Resultat** rechen = gewünschte Wsk.

Bsp. Gefragt ist: Wsk. mehr als 4 Fahrzeuge pro Minute eine Brücke überqueren.

Man rechne nun Wsk. von 0 – 4 Fahrzeuge pro Minute die die Brücke überqueren und danach 1 – das Resultat und man bekommt die gewünschte Wsk.

Zusammenfassung der diskreten Verteilungen

Die **Wahrscheinlichkeitsfunktion** $f(x)$ der Hypergeometrischen Verteilung kann im Grenzfall grosser N und M und kleinem n durch die Binomialverteilung mit $p = M/N$ approximiert werden. Diese kann für kleine p und grosse n durch die Poissonverteilung mit $\mu = np$ approximiert werden.

Verteilung	Parameter	$f(k)$	Bedingung für Approximation
Hypergeometrisch	N, M, n	$\frac{\binom{M}{k} \binom{N-M}{n-k}}{\binom{N}{n}}$	
Binomial	n, $p = M/N$	$\binom{n}{k} p^k (1-p)^{n-k}$	wobei $p = M/N$ $n \leq M/10, n \leq (N-M)/10$
Poisson	$\mu = np$	$\frac{\mu^k}{k!} e^{-\mu}$	wobei $\mu = np$ $p \leq 0.1, n \geq 100$

Zufallsvariablen (X – Wert einem Ergebnis zuordnen)

Definition

Eine Zufallsvariable X ist eine Abbildung vom Stichprobenraum S in die Menge der reellen Zahlen \mathbb{R} , wobei jedem Ergebnis $r \in S$ eine reelle Zahl $X(r)$ zugeordnet wird.

Bsp.

Die Schadenverteilung X einer Diebstahlversicherung. X sei die Schadenshöhe.

- $X(\text{kein Schaden}) = 0$
- $X(\text{kleiner Schaden}) = 100.-$
- $X(\text{grosser Schaden}) = 300.-$

Man beachte, dass nicht die zugeordnete Zahl zufällig ist, sondern die Auswahl des Ereignisses. Die zugeordnete Zahl ist „einfach“ eine **Folge des Ereignisses**. Mit der Auswahl des Ereignisses und der Definition der Zufallsvariablen ist die zugeordnete Zahl eindeutig und nicht zufällig.

Wahrscheinlichkeitsverteilung einer Zufallsvariable ($p(X = r)$)

Die Wahrscheinlichkeitsverteilung (oder kurz Verteilung) einer Zufallsvariablen X auf einem Stichprobenraum S ist die Menge

$$\{(r, p(X = r)) \mid \forall r \in X(S)\},$$

wobei $p(X = r)$ die Wahrscheinlichkeit dafür ist, dass die Zufallsvariable X den Wert r annimmt. Die Wahrscheinlichkeitsverteilung wird üblicherweise dadurch spezifiziert, dass man $p(X = r), \forall r \in X(S)$ spezifiziert.

Bsp. # 1

Die Schadenverteilung X einer Diebstahlversicherung. X sei die Schadenshöhe.

- $P(X = 0.-) = 0,7$
- $P(X = 100.-) = 0,2$
- $P(X = 300.-) = 0,1$
- Also r nimmt die Werte 0, 100 & 300 an.

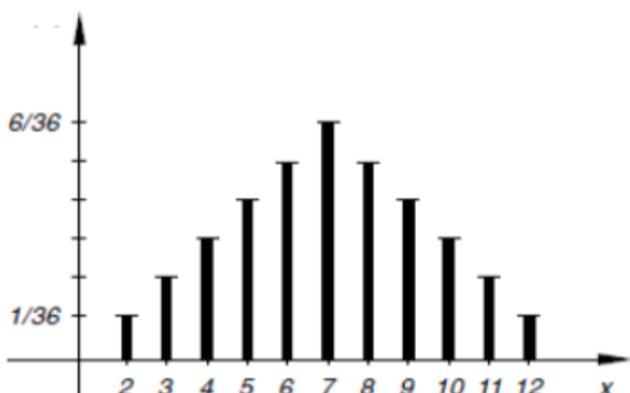
Bsp. #2 Wahrscheinlichkeitsverteilung Augensumme

Bestimmen Sie die Wahrscheinlichkeitsverteilung der Zufallsvariable $X = \text{"Augensumme beim Wurf zweier fairer Würfel"}$.

Durch einfaches Zählen können wir die Tabelle (= Wahrscheinlichkeitsfunktion, Wahrscheinlichkeitsverteilung) erstellen und damit deren Graphen zeichnen.

Wir bezeichnen nun eben $X = \text{"Augensumme beim Wurf zweier fairer Würfel"}$.

r	2	3	4	5	6	7	8	9	10	11	12
$p(X = r)$	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36



Erwartungswert von Zufallsvariablen ($E[X]$, «erwartete Gewinn», «Durchschnitt»,...)

Definition

Der **Erwartungswert** einer Zufallsvariablen $X(s)$ über dem Stichprobenraum S ist gegeben durch:

$$E(X) = \sum_{s \in S} X(s) \cdot p(s) = \sum_{r \in X(S)} r \cdot p(X = r).$$

Bsp. # 1 Bestimmen sie den Erwartungswert $E[X]$.

Die Schadenverteilung X einer Diebstahlversicherung. X sei die Schadenshöhe.

- $P(X = 0,-) = 0,7$
- $P(X = 100,-) = 0,2$
- $P(X = 300,-) = 0,1$
- Also r nimmt die Werte 0, 100 & 300 an.

Lösung:

$$E[X] = \sum_{i=1}^3 x_i \cdot p_i = 0 \cdot 0,7 + 100 \cdot 0,2 + 300 \cdot 0,1 = 50$$

→ Die Erwartete Durchschnittshöhe der Schadensumme ist 50.

Bsp. #2 Erwartungswert Augensumme zweier fairer Würfel

Zahlen von vorherigem Beispiel:

$$E[X] = \sum_{i=2}^{12} x_i \cdot p_i = 2 \cdot \frac{1}{36} + 3 \cdot \frac{2}{36} + 4 \cdot \frac{3}{36} + \dots + 12 \cdot \frac{1}{36} = \frac{252}{36} = 7$$

→ Die Erwartete Augensumme ist 7.

Weitere Anwendungen

Weitere Beispiele dazu in [6-u-7-Disc-Prob-J-Schuler_V3-0.pdf](#) S. 84 ff.

Beispielsweise:

- Roulette (Wie gross ist der erwartete Gewinn?)
- Komplexität von Algorithmen (Was ist die Durchschnittliche Komplexität?)

Rechnen mit dem Erwartungswert

Siehe weiter oben in der Theorie.

Unabhängige Zufallsvariablen

Man nennt die beiden Zufallsvariablen X_1 und X_2 auf dem Stichprobenraum S unabhängig, falls

$$\forall r_1 \in \mathbb{R} \forall r_2 \in \mathbb{R} \left[p(X_1(s) = r_1 \wedge X_2(s) = r_2) = p(X_1(s) = r_1) \cdot p(X_2(s) = r_2) \right].$$

In Worten: Die Wahrscheinlichkeit, dass $X_1(s) = r_1$ und $X_2(s) = r_2$ ist gleich dem Produkt der Wahrscheinlichkeiten, dass $X_1(s) = r_1$ und $X_2(s) = r_2$ und zwar für alle möglichen Werte r_1 und r_2 der Zufallsvariablen X_1 und X_2 .

Bsp.

Zeige, dass die oben verwendeten Zufallsvariablen X_1 und X_2 unabhängig sind (X_k : Augenzahl des k . Würfels)

		Mögliche Werte von X_2						$p(X_1 = r_1)$
		1	2	3	4	5	6	
Mögliche Werte von X_1	1	1/36	1/36	1/36	1/36	1/36	1/36	1/6
	2	1/36	1/36	1/36	1/36	1/36	1/36	1/6
	3	1/36	1/36	1/36	1/36	1/36	1/36	1/6
	4	1/36	1/36	1/36	1/36	1/36	1/36	1/6
	5	1/36	1/36	1/36	1/36	1/36	1/36	1/6
	6	1/36	1/36	1/36	1/36	1/36	1/36	1/6
	$p(X_2 = r_2)$	1/6	1/6	1/6	1/6	1/6	1/6	

Offensichtlich gilt:

$$\forall i \wedge \forall j \underbrace{(P(X_1 = i \wedge X_2 = j))}_{=\frac{1}{36}} = \underbrace{P(X_1 = i)}_{=\frac{1}{6}} \cdot \underbrace{P(X_2 = j)}_{=\frac{1}{6}} = \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}$$

Varianz von Zufallsvariablen

Siehe weiter oben.

Formelzusammenstellung von $E[X]$ und $\text{Var}[X]$ von unseren Modellen

Modelle	$E[X]$	$\text{Var}[X]$
Diskrete Gleichverteilung mit k Ausprägungen	$E[X] = \frac{k+1}{2}$	$\text{Var}[X] = \frac{k^2 - 1}{12}$
Bernoulli-Verteilung mit p	$E[X] = p$	$\text{Var}[X] = p(1-p)$
Binomial-Verteilung $B(n; p)$	$E[X] = np$	$\text{Var}[X] = np(1-p)$
Hypergeometrische Verteilung mit M, N, n	$E[X] = n \cdot \frac{M}{N}$	$\text{Var}[X] = n \cdot \frac{M}{N} \cdot \left(1 - \frac{M}{N}\right) \cdot \left(\frac{N-n}{N-1}\right)$
Poissonverteilung mit μ	$E[X] = \mu$	$\text{Var}[X] = \mu$

Bsp.

Modelle	$E[X]$	$\text{Var}[X]$
Diskrete Gleichverteilung mit $k = 6$ Ausprägungen = Augenzahl des Würfels	$E[X] = \frac{6+1}{2} = 3,5$	$\text{Var}[X] = \frac{6^2 - 1}{12} = \frac{35}{12}$
Bernoulli-Verteilung mit $p = \frac{1}{2}$	$E[X] = \frac{1}{2}$	$\text{Var}[X] = \frac{1}{2} \left(p - \frac{1}{2}\right) = \frac{1}{4}$
Binomial-Verteilung $B(n = 3; p = \frac{1}{2})$	$E[X] = \frac{3}{2}$	$\text{Var}[X] = 3 \cdot \frac{1}{2} \left(p - \frac{1}{2}\right) = \frac{3}{4}$
Hypergeometrische Verteilung mit $M = 3, N = 6, n = 2$	$E[X] = 2 \cdot \frac{3}{6} = 1$	$\text{Var}[X] = 2 \cdot \frac{3}{6} \cdot \left(1 - \frac{3}{6}\right) \cdot \left(\frac{6-2}{6-1}\right) = 0,4$
Poissonverteilung mit μ	$E[X] = \mu$	$\text{Var}[X] = \mu$

Fortgeschrittene Zähltechnik

Abkürzungen

- RB = Rekursionsbeziehung
- LHS = Left Hand Side
- RHS = Right Hand Side

Einführung von Rekursionsbeziehungen

Rekursive Gleichung

Form:

$$a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + c_3 \cdot a_{n-3}$$

Vorteil: Bei einem geg. Problem ist die Form „einfach“ herzuleiten.

Nachteil: Die Berechnung für z.B. a_{1000} bedingt, dass alle 999 vorgängigen Werte bekannt sind.

Explizite/Funktionale Gleichung

Form:

$$a_n = f(a_1, a_2, a_3)$$

Vorteil: Die Berechnung für z.B. a_{1000} kann direkt berechnet werden, ohne alle 999 vorgängigen Werte.

Nachteil: Bei einem geg. Problem ist die Form vermutlich nicht „einfach“ herzuleiten.

Beispiel Fibonacci-Folge

Die Formel lautet: $f_n = f_{n-1} + f_{n-2}$ mit der Anfangsbedingung $f_0 = 0$ und $f_1 = 1$.

Entsprechend können wir einfach das nächste Glied, f_3 , berechnen: $f_3 = f_1 + f_0 = 1 + 0 = 1$.

Zielformulierung

1. Bei einem Problem die Rekursionsgleichung oder Rekursionsbeziehung (RB) aufstellen.
2. Die Rekursionsbeziehung (RB) lösen, so dass wir eine funktionale Darstellung erhalten.

Definition der Rekursionsbeziehung

Eine Rekursionsbeziehung der Folge $\{a_n\}$ ist eine Beziehung der Form

$$a_n = f(a_{n-1}, a_{n-2}, \dots, a_2, a_1), \quad \forall n \geq n_0, n_0 \in \mathbb{N}^+.$$

Eine Lösung dieser Rekursionsbeziehung ist eine Folge, die diese Relation erfüllt.

Bsp.

Gegeben sei die Rekursionsbeziehung $a_n = 2a_{n-1} - a_{n-2}$ für alle $n = 2, 3, 4, \dots$ Sind die Zahlenfolgen Lösungen dieser Rekursion?

a) $a_n = 3n$ und somit ist $a_{n-1} = 3(n-1)$ und $a_{n-2} = 3(n-2)$

b) $a_n = 2^n$ und somit ist $a_{n-1} = 2^{n-1}$ und $a_{n-2} = 2^{n-2}$

c) $a_n = 5$ und somit ist $a_{n-1} = 5$ und $a_{n-2} = 5$

a) Einerseits gilt: $a_n = 3n$

Andererseits muss die Rekursionsbeziehung gelten:

$$2a_{n-1} - a_{n-2} = 2(3 \cdot (n-1)) - (3 \cdot (n-2)) = 6n - 6 - 3n + 6 = 3n$$

Somit erfüllt $a_n = 3n$ und damit auch die Zahlenfolge 6; 9; 12; 15; ... die Rekursionsbeziehung.

b) Einerseits gilt: $a_n = 2^n$

Andererseits muss die Rekursionsbeziehung gelten:

$$2a_{n-1} - a_{n-2} = 2 \cdot 2^{n-1} - 2^{n-2} = 2^n - 2^{n-2} \neq 2^n$$

Somit erfüllt $a_n = 2^n$ und damit auch die Zahlenfolge 4; 8; 16; 32; ... die Rekursionsbeziehung nicht.

c) Einerseits gilt: $a_n = 5$

Andererseits muss die Rekursionsbeziehung gelten:

$$2a_{n-1} - a_{n-2} = 2[5] - 5 = 5$$

Somit erfüllt $a_n = 5$ und damit auch die Zahlenfolge 5; 5; 5; ... die Rekursionsbeziehung.

Lösen von Rekursionsbeziehungen RB

Begriffe

Lineare Rekursionsbeziehung

Die lineare Rekursionsbeziehung entsteht durch Umformen der Rekursionsbeziehung:

Eine lineare, homogene Rekursionsbeziehung vom Grade k mit konstanten Koeffizienten ist eine Beziehung der Form

$$a_n - c_1 a_{n-1} - c_2 a_{n-2} - \dots - c_k a_{n-k} = 0,$$

wobei für die Koeffizienten gilt: $c_1, c_2, \dots, c_k \in \mathbb{R}$ und $c_k \neq 0$.

c = Koeffizienten

k = Grad

homogen = RB ist homogen, wenn die Formel wie oben auf = 0 umgeformt werden kann.

Bsp. Bitstrings

Die Rekursionsbeziehung für die Anzahl Bitstrings, die nicht 00 enthalten, lautet: $a_n = a_{n-1} + a_{n-2}$, resp. wie oben umgeformt: $a_n - a_{n-1} - a_{n-2} = 0$

Somit ist es eine **lineare, homogene Rekursionsbeziehung vom Grad k = 2, mit $c_1 = c_2 = -1$** .

Bsp. #2

Die Rekursionsbeziehung $a_n = 2a_{n-1} - a_{n-2}$, resp. wie oben umgeformt: $a_n - 2a_{n-1} + a_{n-2} = 0$, ist eine lineare, homogene Rekursionsbeziehung vom Grad k = 2, mit $c_1 = -2$; $c_2 = +1$.

Lösen von linearen Rekursionsbeziehungen (Allgemeines Vorgehen)

Allgemeines Vorgehen:

- Bestimme die allgemeine Lösung $\{a_n^{(h)}\}$ der zugehörigen homogenen Rekursionsbeziehung (RHS Null setzen)

$$a_n - c_1 a_{n-1} - c_2 a_{n-2} - \dots - c_k a_{n-k} = 0.$$

- Bestimme eine (einige) partikuläre Lösung $\{a_n^{(p)}\}$ der inhomogenen Rekursionsbeziehungen

$$a_n - c_1 a_{n-1} - c_2 a_{n-2} - \dots - c_k a_{n-k} = r(n).$$

- Dann ist die allgemeine Lösung der inhomogenen Rekursionsbeziehungen die Summe dieser beiden Lösungen

$$\{a_n\} = \left\{ a_n^{(h)} \right\} + \left\{ a_n^{(p)} \right\}.$$

1. Lösen der homogenen Rekursionsbeziehung

Die homogene Rekursionsbeziehung

$$\underline{a_n - c_1 a_{n-1} - c_2 a_{n-2} - \dots - c_k a_{n-k} = 0} \quad (1)$$

wird durch den folgenden **Ansatz** gelöst

$$\underline{a_k = r^k}, \quad k = n - k, n - k + 1, \dots, n. \quad (2)$$

Falls der Ansatz (2) die Gleichung (1) erfüllen soll, muss r die folgende **charakteristische Gleichung** erfüllen:

$$\underline{r^k - c_1 r^{k-1} - c_2 r^{k-2} - \dots - c_{k-1} r - c_k = 0}$$

Man erhält sie aus (1), indem man $\underline{a_k}$ durch $\underline{r^k}$ ersetzt, und den Ausdruck durch $\underline{r^{n-k}}$ dividiert.

Lösen der homogenen Rekursionsbeziehung wenn $k = 1$

Nachdem ich Schritt 1. (Lösen der homogenen Rekursionsbeziehung) gemacht habe und $k = 1$ ist, dann:

Zu dem Fall $k = 1$: $a_n = c \cdot a_{n-1}$ resp. $a_n - c \cdot a_{n-1} = 0$ mit der Anfangsbedingung $a_0 = \alpha$ (*)

Die charakteristische Gleichung ist für $k = 1$ eine lineare Gleichung, sie hat nach dem Ansatz $a_k = r^k$ die Form:

$$r^n - c \cdot r^{n-1} = 0$$

Und somit erhalten wir nach der Division mit r^{n-1} die charakteristische Gleichung:

$$r - c = 0$$

Sie hat trivialerweise die Lösung $r = c$

Und damit lautet die allgemeine Lösung: $a_n^{(h)} = \alpha \cdot r^n = \alpha \cdot c^n$ (**)

(*) Folge konkret aufgeschrieben: $\alpha, \alpha \cdot c, \alpha \cdot c^2, \alpha \cdot c^3, \dots$

(**) Folge konkret aufgeschrieben: $\alpha, \alpha \cdot c, \alpha \cdot c^2, \alpha \cdot c^3, \dots$

Variablen ersetzen in
 $a_n^{(h)} = \alpha \cdot c^n$
 $a_n^{(h)} = a_0$ ←
 $c = r$
 $n = 0$
 → auf α auflösen
 → α & c in Formel $a_n^{(h)}$ einsetzen

Beispiel-Output: $a_n = 5 * 2^n$ (Hier kann man nun n (1,2,3,...) einsetzen und die Folge testen)

→ Wenn die RB von der Aufgabenstellung eine homogene lineare RB ist, dann ist dies bereits die Lösung. Ist sie jedoch inhomogen. Also wäre da noch etwas wie $+3n$ oder $-2n$, also von n direkt abhängig (nicht $n-1$ oder $n-2$), am Schluss müssen wir mit dem Schritt 2., mit der partikulären Lösung weiterfahren.

→ Zum Weiterfahren müsste die Formel aber die Form $a_n^{(h)} = \alpha * r^n$ haben, also α nicht eingesetzt, α wird beim nächsten Schritt dann neue berechnet. «r» müsste aber eingesetzt werden.

Beispiel-Output zum weiterfahren: $a_n^{(h)} = \alpha * 2^n$

Lösen der homogenen Rekursionsbeziehung wenn $k = 2$

Nach dem ich Schritt 1. (Lösen der homogenen Rekursionsbeziehung) gemacht habe und $k = 2$ ist, dann:

Zu dem Fall $k = 2$: $a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2}$ resp. $a_n - c_1 \cdot a_{n-1} - c_2 \cdot a_{n-2} = 0$ mit der Anfangsbedingung $a_0 = \underline{a_1}, a_1 = \underline{a_2}$

Die charakteristische Gleichung ist für $k = 2$ eine quadratische Gleichung, sie hat nach dem Ansatz $a_k = r^k$ die Form:

$$\underbrace{r^n - c_1 \cdot r^{n-1} - c_2 \cdot r^{n-2}}_{} = 0$$

Und somit erhalten wir nach der Division mit r^{n-2} die charakteristische Gleichung:

$$\underbrace{r^2 - c_1 \cdot r - c_2}_{} = 0 \quad (3)$$

Sie wird typischerweise mit Lösungsformel für quadratische Gleichungen (die sog. „Mitternachtsformel“) gelöst. Die Lösungen lauten dann:

$$\rightarrow \text{Mitternachtsformel hat die Form: } \underline{ax^2 + bx + c = 0} \quad \rightarrow \quad x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Also ist in diesem Fall $a = 1, b = -c_1, c = -c_2$ und somit lautet die Lösung dann:

$$r_{1,2} = \frac{-(-c_1) \pm \sqrt{(-c_1)^2 - 4(-c_2)}}{2} = \frac{c_1 \pm \sqrt{(c_1)^2 + 4c_2}}{2} = \frac{c_1}{2} \pm \sqrt{\left(\frac{c_1}{2}\right)^2 + c_2}$$

Es gibt drei Fälle, abhängig von der Diskriminanten D der Gleichung (3)

$$D = \left(\frac{c_1}{2}\right)^2 + c_2$$

$D > 0$ Dann hat die charakteristische Gleichung zwei unterschiedliche Lösungen $r_1 \neq r_2$.
Die allgemeine Lösung der homogenen Gleichung ist dann

$$\underline{a_n^{(h)} = \alpha_1 r_1^n + \alpha_2 r_2^n}.$$

$D = 0$ Dann hat die charakteristische Gleichung eine Doppelösungen $r = r_1 = r_2$. Die allgemeine Lösung der homogenen Gleichung ist dann

$$\underline{a_n^{(h)} = (\alpha_1 + \alpha_2 n) r^n}.$$

$D < 0$ Dann hat die charakteristische Gleichung (für reelle c_1 und c_2) eine Paar konjugiert komplexer Lösungen. Dieser Fall ist für uns nicht interessant! \rightarrow keine Lösung

Beispiel-Output: $a_n = 5 * 2^n - 3^n$ (Hier kann man nun $n (1,2,3,\dots)$ einsetzen und die Folge testen)

\rightarrow Wenn die RB von der Aufgabenstellung eine homogene lineare RB ist, dann ist dies bereits die Lösung. Ist sie jedoch inhomogen. Also wäre da noch sowas wie $+3n$ oder $-2n$, also von n direkt abhängig (nicht $n-1$ oder $n-2$), am Schluss müssen wir mit dem Schritt 2., mit der partikulären Lösung weiterfahren.

\rightarrow Zum Weiterfahren müsste die Formel aber die Form, je nach Diskriminante, $a_n^{(h)} = \alpha_1 * r_1^n + \alpha_2 * r_2^n$ haben, also α nicht eingesetzt, α wird beim nächsten Schritt dann neue berechnet. « r » müsste aber eingesetzt werden.

Beispiel-Output zum weiterfahren: $a_n^{(h)} = \alpha_1 * 2^n + \alpha_2 * 3^n$

2. Bestimmen einer partikulären Lösung der inhomogenen Rekursionsbeziehung

Um man eine spezielle Lösung der inhomogenen Rekursionsbeziehungen zu berechnen, müssen die

Konstanten in $\{a_n^{(h)}\}$ bestimmt werden:

- Dazu wird der Ansatz (ist oft in der Aufgabenstellung angegeben) von $a_n^{(p)}$ in die inhomogene Rekursionsgleichung eingesetzt.
- Dann werden die Konstanten so gewählt, dass die Anfangsbedingungen erfüllt sind.
- Dies führt typischer Weise auf ein Gleichungssystem.

Vorgehen

Ist die **RB inhomogen** also hat es am Schluss noch einen Term welche von «n» abhängt (+3n, -2n), also nicht von «n-1» oder «n-2», dann muss $a_n^{(p)}$ bestimmt werden.

1. Inhomogene RB aufschreiben, hat die Form:

$$a_n - c_1 a_{n-1} - c_2 a_{n-2} - \dots - c_k a_{n-k} = r(n).$$

Bsp.: $a_n - 2a_{n-1} = 3n$ (#)

2. Danach mit dem Schema gemäss Aufgabenstellung weiterfahren:

Bsp. Ansatz $a_n^{(p)} = a \cdot n + b$

3. Dieser Ansatz in die inhomogene RB-Gleichung (#) einsetzen:

Bsp.:

$a_n^{(p)} = a \cdot n + b$ in die Gleichung (#) eingesetzt:

$$\begin{aligned} (a \cdot n + b) - 2 \cdot (a \cdot (n-1) + b) &= 3n \\ an + b - 2(a \cdot n - a + b) &= 3n \\ an + b - 2an + 2a - 2b &= 3n \\ -an + 2a - b &= 3n \\ 0 &= an - 2a + b + 3n \\ 0 &= n(a + 3) + (b - 2a), \text{ diese Gleichung muss nun für alle } n \text{ gelten!!} \end{aligned}$$

4. Da die erhaltene Gleichung in der Form $a + b = 0$ ist, muss der Term $a = 0$ und $b = 0$ sein. Wir erhalten entsprechend ein Gleichungssystem mit zwei Gleichungen und können auf a und b auflösen. (n kann vernachlässigt werden):

Bsp.:

$$a + 3 = 0 \quad \rightarrow a = -3$$

$$b - 2a = 0 \quad \rightarrow a \text{ einsetzen} \rightarrow b - 2 \cdot (-3) = 0 \rightarrow b + 6 = 0 \rightarrow b = -6$$

5. Somit können wir a und b in unser Schema einfügen.

$$a_n^{(p)} = -3 \cdot n - 6$$

6. Nun haben wir $a_n^{(h)}$ (von vorhergehender Berechnung Bsp. $\alpha \cdot 2^n$) und $a_n^{(p)}$ von jetzt und können somit a_n ausrechnen

Bsp.:

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha \cdot 2^n + -3 \cdot n - 6 = \alpha \cdot 2^n - 3n - 6$$

7. Durch Einsetzen der Anfangsbedingung a_0 (bsp. $a_0 = 5$) können wir α ausrechnen.

$$a_0 = 5 = \alpha \cdot 2^0 + -3 \cdot 0 - 6 \rightarrow 5 = \alpha - 6 \rightarrow \alpha = 5 + 6 = 11$$

8. a_n abhängig von «n» aufschreiben:

$$a_n = a_n^{(h)} + a_n^{(p)} = 11 \cdot 2^n - 3n - 6$$

9. Zur Kontrolle einfach $n = 0, 1, 2, 3, 4, \dots$ einsetzen.

- $a_0 = 11 \cdot 2^0 - 3 \cdot 0 - 6 = 11 - 6 = 5$
- $a_1 = 11 \cdot 2^1 - 3 \cdot 1 - 6 = 22 - 9 = 13$
- $a_2 = 11 \cdot 2^2 - 3 \cdot 2 - 6 = 44 - 12 = 32$
- $a_3 = 11 \cdot 2^3 - 3 \cdot 3 - 6 = 88 - 15 = 73$

3. Summe von Schritt 1 und 2 berechnen

Resultate der ersten beiden Schritte addieren:

$$\{a_n\} = \{a_n^{(h)}\} + \{a_n^{(p)}\}$$

VorgehenSiehe Schritte 6 – 9 vom Kapitel [Bestimmen einer partikulären Lösung der inhomogenen Rekursionsbeziehung](#)

Beispiele zum Lösen von linearen Rekursionsbeziehungen

Homogene, lineare RB vom Grad $k = 1$

rekursive Formel
 $a_n = 2 \cdot a_{n-1}$ mit der Anfangsbedingung $a_0 = 5$

Eine erste Betrachtung: Es wird offensichtlich die Folge 5, 10, 20, 40, ... beschrieben.

Das wollen wir nun mit unserem Schema lösen:

Schreiben der homogenen RB:

$$a_n - 2a_{n-1} = 0 \quad \text{homogen } \lambda = 0$$

Ansatz:

$$a_k = r^k \Rightarrow a_n = r^n$$

In RB eingesetzt:

$$r^n - 2r^{n-1} = 0 \Rightarrow r^{n-1}(r-2) = 0 \Rightarrow r^{n-1} = 0 \quad \text{oder} \quad r-2 = 0 \Rightarrow r=2$$

Division mit r^{n-1} :

$$\text{Und damit die allgemeine Lösung der homogenen RB: } a_n^{(h)} = \alpha \cdot r^n = \alpha \cdot 2^n$$

Durch Einsetzen der Anfangsbedingung $a_0 = 5$ in die allg. Lösung $a_n^{(h)} = \alpha \cdot 2^n$ erhalten wir α

$$\text{Also: } a_0 = \alpha \cdot 2^0 = 5 \Rightarrow \alpha = 5$$

Durch Einsetzen für $n = 0, 1, 2, \dots$ in $a_n^{(h)} = 5 \cdot 2^n$ bekommen wir die Folge 5, 10, 20, 40, ...

Inhomogene, lineare RB vom Grad $k = 1$

$$a_n = 2 \cdot a_{n-1} \quad \text{mit der Anfangsbedingung } a_0 = 5$$

Eine erste Betrachtung: Es wird offensichtlich die Folge 5, 10, 20, 40, ... beschrieben.

Das wollen wir nun mit unserem Schema lösen:

Schreiben der homogenen RB:

$$a_n - 2a_{n-1} = 0 \quad \leftarrow \text{homogener } \lambda_n = 0$$

Ansatz:

$$a_n = r^n \quad \Rightarrow a_n = r^n$$

In RB eingesetzt:

$$r^n - 2r^{n-1} = 0 \Rightarrow r^{n-1}(r-2) = 0 \Rightarrow r^{n-1} = r^{n-1}$$

Division mit r^{n-1} :

$$r-2 = 0 \Rightarrow r=2$$

Und damit die allgemeine Lösung der homogenen RB: $a_n^{(h)} = \alpha \cdot r^n = \alpha \cdot 2^n$

Durch Einsetzen der Anfangsbedingung $a_0 = 5$ in die allg. Lösung $a_n^{(h)} = \alpha \cdot 2^n$ erhalten wir α

$$\text{Also: } a_0 = \alpha \cdot r^0 = 5 \Rightarrow \alpha = 5$$

Durch Einsetzen für $n = 0, 1, 2, \dots$ in $a_n^{(h)} = 5 \cdot 2^n$ bekommen wir die Folge 5, 10, 20, 40, ...

$$a_n = 2 \cdot a_{n-1} + 3n \quad \text{mit der Anfangsbedingung } a_0 = 5 \quad a_2 = 2 \cdot 13 + 3 \cdot 2$$

Eine erste Betrachtung: Es wird offensichtlich die Folge 5, 13, 32, 73, 154, ... beschrieben.

Das wollen wir nun mit unserem Schema lösen:

Schreiben der inhomogenen RB: $a_n - 2a_{n-1} = 3n$ (#)

Bis zur allgemeinen Lösung der homogenen RB haben wir es schon gemacht: $a_n^{(h)} = \alpha \cdot c^n = \alpha \cdot 2^n$

Nun muss eine (einige) partikuläre Lösung der inhomogenen RB gefunden werden. Da die Störung $3n$

lautet, also linear ist, wählen wir als (linearen) Ansatz: $a_n^{(p)} = a \cdot n + b$

(Der Ansatz ist in einer MEP oft angegeben)

$a_n^{(p)} = a \cdot n + b$ in die Gleichung (#) eingesetzt:

$$(a \cdot n + b) - 2 \cdot (a \cdot (n-1) + b) = 3n$$

$$an + b - 2(a \cdot n - a + b) = 3n$$

$$an + b - 2an + 2a - 2b = 3n$$

$$-an + 2a - b = 3n$$

$$0 = an - 2a + b + 3n$$

$$0 = n(a+3) + (b-2a), \text{ diese Gleichung muss nun für alle } n \text{ gelten!!}$$

Weiter auf der nächsten Seite ...

Also: $0 = \frac{n \cdot (a+3) + (b-2a)}{=0 =0}$

Und wir erhalten zwei Gleichungen:

$$\begin{aligned} \text{i)} \quad & a+3=0 \Rightarrow a=-3 \\ \text{ii)} \quad & b-2a=0 \Rightarrow b-2 \cdot (-3)=0 \Rightarrow b+6=0 \Rightarrow b=-6 \end{aligned}$$

Mit den Lösungen: $a = -3$ und $b = -6$ in Schema $a \cdot n + b$ von oben einsetzen

$$\text{Und somit ist } a_n^{(p)} = \frac{(-3) \cdot n - 6}{= -3n - 6} \quad \text{Und damit: } a_n = a_n^{(h)} + a_n^{(p)} = \frac{\alpha \cdot 2^n - 3n - 6}{= \alpha \cdot 2^n - 3n - 6} \Rightarrow a_0 = \alpha \cdot 2^0 - 3 \cdot 0 - 6 = 5.$$

Nun müssen wir noch die Anfangsbedingung mit einbeziehen: $a_0 = 5$

$$5 = a_0 = \cancel{\alpha - 6} = 5 \Rightarrow \alpha = 5 + 6 = \underline{\underline{11}}$$

$$\text{Also: } a_n = a_n^{(h)} + a_n^{(p)} = \cancel{\underline{\underline{11}} \cdot 2^n - 3n - 6}$$

Kontrolle: Wir zeigen, dass die gleiche Folge 5, 13, 32, 73, 158, ... beschrieben wird.

- $a_0 = 11 \cdot 2^0 - 3 \cdot 0 - 6 = 11 - 6 = 5$
- $a_1 = 11 \cdot 2^1 - 3 \cdot 1 - 6 = 22 - 9 = 13$
- $a_2 = 11 \cdot 2^2 - 3 \cdot 2 - 6 = 44 - 12 = 32$

Homogene, lineare RB vom Grad $k=2$ und $D > 0$

$$a_n = 5 \cdot a_{n-1} - 6 \cdot a_{n-2} \text{ mit der Anfangsbedingung } a_0 = 2 \text{ & } a_1 = 3$$

Eine erste Betrachtung: Es wird offensichtlich die Folge 2, 3, 3, -3, -33, -147 ... beschrieben.

Das wollen wir nun mit unserem Schema lösen:

Schreiben der homogenen RB:

$$a_n - 5 \cdot a_{n-1} + 6 \cdot a_{n-2}$$

Ansatz:

$$a_k = r^k \Rightarrow a_n = r^n \quad a_{n-1} = r^{n-1}$$

In RB eingesetzt:

$$r^n - 5r^{n-1} + 6r^{n-2} = 0 \quad a_{n-2} = r^{n-2}$$

Division mit r^{n-2} :

$$r^2 - 5r + 6 = 0 \quad r_1 = 2; r_2 = 3 \quad \text{Faktor D70}$$

Und damit die allgemeine Lösung der homogenen RB: $a_n^{(h)} = \alpha_1 \cdot r_1^n + \alpha_2 \cdot r_2^n$

$$= \alpha_1 \cdot 2^n + \alpha_2 \cdot 3^n$$

Durch Einsetzen der Anfangsbedingung $a_0 = 2$ & $a_1 = 3$ in die allg. Lösung $a_n^{(h)}$ erhalten wir α_1 & α_2

$$\begin{aligned} \text{Also: } a_0 = 2 \Rightarrow 2 &= \alpha_1 \cdot 2^0 + \alpha_2 \cdot 3^0 \Rightarrow 2 = \alpha_1 + \alpha_2 \quad (*) \\ a_1 = 3 \Rightarrow 3 &= \alpha_1 \cdot 2^1 + \alpha_2 \cdot 3^1 \Rightarrow 3 = 2\alpha_1 + 3\alpha_2 \quad (***) \end{aligned}$$

(*) & (**) bilden ein lin. Gleichungssystem mit den Lösungen:

$$\alpha_1 = 3 \quad \& \quad \alpha_2 = -1$$

Und somit haben wir die Lösungen der RB mit den genannten Anfangsbedingungen:

$$a_n = 3 \cdot 2^n - 3^n$$

Kontrolle: Wir zeigen, dass die gleiche Folge 2, 3, 3, -3, -33, -147, ... beschrieben wird.

- $a_0 = 3 \cdot 2^0 - 3^0 = 3 - 1 = 2$
- $a_1 = 3 \cdot 2^1 - 3^1 = 6 - 3 = 3$
- $a_2 = 3 \cdot 2^2 - 3^2 = 12 - 9 = 3$

Inhomogene, lineare RB vom Grad $k = 2$ und $D > 0$

Erster Teil von oben Homogene, lineare RB vom Grad $k = 2$ und $D > 0$

Inhomogene, lineare Rekursionsbeziehung vom Grad $k = 2$ und Determinante $D > 0$.

$$a_n = 5 \cdot a_{n-1} - 6 \cdot a_{n-2} + 2n \quad (\#) \text{ mit der Anfangsbedingung } a_0 = 2 \text{ & } a_1 = 3$$

Eine erste Betrachtung: Es wird offensichtlich die Folge 2, 3, 7, 23, 81, 277 ... beschrieben.

Das wollen wir nun mit unserem Schema lösen:

Bis zur allgemeinen Lösung der homogenen RB bleibt es sich gleich.

$$\text{Und damit die allg. Lösung der homogenen RB: } \underline{\underline{a_n^{(h)}}} = \alpha_1 \cdot r_1^n + \alpha_2 \cdot r_2^n = \underline{\underline{\alpha_1 \cdot 2^n + \alpha_2 \cdot 3^n}}$$

Nun muss eine (einige) partikuläre Lösung der inhomogenen RB gefunden werden. Da die Störung $\underline{\underline{2n}}$

$$\text{lautet, also linear ist, wählen wir als (linearen) Ansatz: } a_n^{(p)} = \underline{\underline{a \cdot n + b}}$$

$$a_n^{(p)} = \underline{\underline{a \cdot n + b}} \text{ in die Gleichung } (\#) \text{ eingesetzt:}$$

$$\begin{aligned} a_{n-1} &= a \cdot (n-1) + b \\ a_{n-2} &= a \cdot (n-2) + b \end{aligned}$$

$$\begin{aligned} a \cdot n + b &= 5 \cdot (a \cdot (n-1) + b) - 6 \cdot (a \cdot (n-2) + b) + 2n \\ a \cdot n + b &= 5 \cdot (an - a + b) - 6 \cdot (an - 2a + b) + 2n \end{aligned}$$

$$a \cdot n + b = 5an - 5a + 5b - 6an + 12a - 6b + 2n$$

$$a \cdot n + b = -an + 7a - b + 2n$$

$$2an - 2n - 7a + 2b = 0$$

$$\begin{aligned} n \underbrace{(2a - 2)}_{=0} + \underbrace{(-7a + 2b)}_{=0} &= 0 \cdot n + 0 \end{aligned}$$

für a keine n gelten

$$\text{Also: } 2a - 2 = 0 \Rightarrow \underline{\underline{a = 1}}$$

$$\text{Und: } -7a + 2b = 0 \Rightarrow -7 + 2b = 0 \Rightarrow b = 3,5$$

$$\text{Und damit } a_n^{(p)} = \underline{\underline{a \cdot n + b}} = \underline{\underline{n + 3,5}}$$

$$\text{Und damit } a_n = \underline{\underline{a_n^{(h)}}} + \underline{\underline{a_n^{(p)}}} = \underline{\underline{\alpha_1 \cdot 2^n + \alpha_2 \cdot 3^n + n + 3,5}}$$

neues α , da nicht homogen

Durch Einsetzen der Anfangsbedingung $a_0 = 2$ & $a_1 = 3$ in die allg. Lösung a_n erhalten wir α_1 & α_2

$$\text{Also: } a_0 = 2 \Rightarrow 2 = \alpha_1 \cdot 2^0 + \alpha_2 \cdot 3^0 + 0 + 3,5 \Rightarrow -1,5 = \alpha_1 + \alpha_2 (*)$$

$$a_1 = 3 \Rightarrow 3 = \alpha_1 \cdot 2^1 + \alpha_2 \cdot 3^1 + 1 + 3,5 \Rightarrow -1,5 = 2\alpha_1 + 3\alpha_2 (**)$$

(*) & (**) bilden ein lin. Gleichungssystem mit den Lösungen:

$$\alpha_1 = -3 \text{ & } \alpha_2 = 1,5$$

Und somit haben wir die Lösungen der RB mit den genannten Anfangsbedingungen:

$$\underline{\underline{a_n = (-3) \cdot 2^n + 1,5 \cdot 3^n + n + 3,5}}$$

Kontrolle: Wir zeigen, dass die gleiche Folge 2, 3, 7, 23, 88, 277, ... beschrieben wird.

- $a_0 = (-3) \cdot 2^0 + 1,5 \cdot 3^0 + 0 + 3,5 = -3 + 1,5 + 3,5 = 2$
- $a_1 = (-3) \cdot 2^1 + 1,5 \cdot 3^1 + 1 + 3,5 = -6 + 4,5 + 4,5 = 3$
- $a_2 = (-3) \cdot 2^2 + 1,5 \cdot 3^2 + 2 + 3,5 = -12 + 13,5 + 5,5 = 7$
- $a_3 = (-3) \cdot 2^3 + 1,5 \cdot 3^3 + 3 + 3,5 = -24 + 40,5 + 6,5 = 23$
- $a_4 = (-3) \cdot 2^4 + 1,5 \cdot 3^4 + 4 + 3,5 = -48 + 121,5 + 7,5 = 81$
- $a_5 = (-3) \cdot 2^5 + 1,5 \cdot 3^5 + 5 + 3,5 = -96 + 364,5 + 8,5 = 277$

Homogene, lineare RB vom Grad $k = 2$ und $D = 0$

$$a_n = 4 \cdot a_{n-1} - 4a_{n-2} \text{ mit der Anfangsbedingung } a_0 = 1 \& a_1 = 3 \quad r_1 = r_2$$

Eine erste Betrachtung: Es wird offensichtlich die Folge 1, 3, 8, 20, 48, 112 ... beschrieben.

Das wollen wir nun mit unserem Schema lösen:

Schreiben der homogenen RB:

$$a_n - 4 \cdot a_{n-1} + 4a_{n-2}$$

Formel gemäß
Vorgabe für
 $D=0$

Ansatz:

$$a_k = \frac{r^n}{r^n - 4r^{n-1} + 4r^{n-2}} = 0$$

In RB eingesetzt:

$$r^2 - 4r + 4 = (r-2)^2 = 0 \Rightarrow r=2$$

Division mit r^{n-2} :

$$\text{Und damit die allg. Lösung der homogenen RB: } a_n^{(h)} = (\alpha_1 + \alpha_2 \cdot n) \cdot r^n = (\alpha_1 + \alpha_2 \cdot n) \cdot 2^n$$

Durch Einsetzen der Anfangsbedingung $a_0 = 1$ & $a_1 = 3$ in die allg. Lösung $a_n^{(h)}$ erhalten wir

α_1 & α_2

Also: $a_0 = 1 \Rightarrow 1 = (\alpha_1 + \alpha_2 \cdot 0) \cdot 2^0 \Rightarrow \alpha_1 = 1$

$$a_1 = 3 \Rightarrow 3 = (\alpha_1 + \alpha_2 \cdot 1) \cdot 2^1 \Rightarrow 3 = (1 + \alpha_2 \cdot 1) \cdot 2^1 \Rightarrow \alpha_2 = 0,5$$

Und somit haben wir die Lösungen der RB mit den genannten Anfangsbedingungen:

$$\underline{\underline{a_n = (1 + 0,5n) \cdot 2^n}}$$

Kontrolle: Wir zeigen, dass die gleiche Folge 1, 3, 8, 20, 48, 112, ... beschrieben wird.

- $a_0 = (1 + 0,5 \cdot 0) \cdot 2^0 = 1$
- $a_1 = (1 + 0,5 \cdot 1) \cdot 2^1 = 3$
- $a_2 = (1 + 0,5 \cdot 2) \cdot 2^2 = 2 \cdot 2^2 = 8$
- $a_3 = (1 + 0,5 \cdot 3) \cdot 2^3 = 2,5 \cdot 2^3 = 20$

Inhomogene, lineare RB vom Grad $k = 2$ und $D = 0$

Erster Teil von oben Homogene, lineare RB vom Grad $k = 2$ und $D = 0$.

Inhomogene, lineare Rekursionsbeziehung vom Grad $k = 2$ und Determinante $\mathbf{D} = 0$.

$$a_n = 4 \cdot a_{n-1} - 4 \cdot a_{n-2} - 2n \quad (\#) \text{ mit der Anfangsbedingung } a_0 = 1 \text{ & } a_1 = 3$$

Eine erste Betrachtung: Es wird offensichtlich die Folge 1, 3, 4, -2, -32, -130 ... beschrieben.

Das wollen wir nun mit unserem Schema lösen:

Bis zur allgemeinen Lösung der homogenen RB bleibt es sich gleich.

Und damit die allg. Lösung der homogenen RB $\underline{\underline{a_n^{(h)}}} = (\alpha_1 + \alpha_2 \cdot n) \cdot r^n = \underline{\underline{(\alpha_1 + \alpha_2 \cdot n) \cdot 2^n}}$

Nun muss eine (einige) partikuläre Lösung der inhomogenen RB gefunden werden. Da die Störung $-2n$

lautet, also linear ist, wählen wir als (linearen) Ansatz: $\underline{\underline{a_n^{(p)}}} = \underline{\underline{a \cdot n + b}}$

$\underline{\underline{a_n^{(p)}}} = \underline{\underline{a \cdot n + b}}$ in die Gleichung (#) eingesetzt:
 Ziel: $a \cdot n + b = 4 \cdot (a \cdot (n-1) + b) - 4 \cdot (a \cdot (n-2) + b) - 2n$
 einzelne Lsg erhalten.
 $a \cdot n + b = 4 \cdot (an - a + b) - 4 \cdot (an - 2a + b) - 2n$
 $a \cdot n + b = 4an - 4a + 4b - 4an + 8a - 4b - 2n$
 $a \cdot n + b = 4a - 2n$
 $an + 2n - 4a + b = 0$
 → wenn $a \neq b$
 bestimmt sind. $n \underbrace{(a+2)}_{=0} + \underbrace{(-4a+b)}_{=0} = 0 \cdot n + 0$
 Also: $a + 2 = 0 \Rightarrow a = -2$

Und: $-4a + b = 0 \Rightarrow 8 + b = 0 \Rightarrow b = -8$

Und damit $\underline{\underline{a_n^{(p)}}} = \underline{\underline{a \cdot n + b}} = \underline{\underline{-2n - 8}}$

Und damit $\underline{\underline{a_n}} = \underline{\underline{a_n^{(h)}}} + \underline{\underline{a_n^{(p)}}} = \underline{\underline{(\alpha_1 + \alpha_2 \cdot n) \cdot 2^n - 2n - 8}}$

Durch Einsetzen der Anfangsbed. $a_0 = 1$ & $a_1 = 3$ in die allg. Lösung a_n erhalten wir α_1 & α_2

Also: $a_0 = 1 \Rightarrow 1 = (\alpha_1 + \alpha_2 \cdot 0) \cdot 2^0 - 2 \cdot 0 - 8 \Rightarrow 9 = \alpha_1$

$a_1 = 3 \Rightarrow 3 = (9 + \alpha_2 \cdot 1) \cdot 2^1 - 2 \cdot 1 - 8 \Rightarrow -2,5 = \alpha_2$

Und somit haben wir die Lösungen der RB mit den genannten Anfangsbedingungen:

$$\underline{\underline{a_n = (9 - 2,5n) \cdot 2^n - 2n - 8}}$$

Kontrolle: Wir zeigen, dass die gleiche Folge 1, 3, 4, -2, -32, -130, ... beschrieben wird.

- $a_0 = (9 - 0) \cdot 2^0 - 0 - 8 = 9 - 8 = 1$
- $a_1 = (9 - 2,5 \cdot 1) \cdot 2^1 - 2 \cdot 1 - 8 = 6,5 \cdot 2^1 - 10 = 3$
- $a_2 = (9 - 2,5 \cdot 2) \cdot 2^2 - 2 \cdot 2 - 8 = 4 \cdot 2^2 - 12 = 4$
- $a_3 = (9 - 2,5 \cdot 3) \cdot 2^3 - 2 \cdot 3 - 8 = 1,5 \cdot 2^3 - 14 = -2$
- $a_4 = (9 - 2,5 \cdot 4) \cdot 2^4 - 2 \cdot 4 - 8 = (-1) \cdot 2^4 - 16 = -32$
- $a_5 = (9 - 2,5 \cdot 5) \cdot 2^5 - 2 \cdot 5 - 8 = (-3,5) \cdot 2^5 - 18 = -130$

Homogene/Inhomogene, lineare RB vom Grad $k = 2$ und $D < 0$

Gegeben sei die Rekursionsbeziehung $a_n = 2a_{n-1} - 3a_{n-2}$. Wir wollen (versuchen) die allg. Lösung zu bestimmen.

1) Aufstellen der homogenen Rekursionsbeziehung: $a_n - 2a_{n-1} + 3a_{n-2} = 0$

2) Die charakteristischen Gleichung lautet: $r^2 - 2r + 3 = 0$

3) Lösen der charakteristischen Gleichung:

$$r^2 - 2r + 3 = 0 \Rightarrow r_{1,2} = \frac{2 \pm \sqrt{(-2)^2 - 4 \cdot 3}}{2} = \frac{2 \pm \sqrt{-8}}{2} \rightarrow D < 0$$

Die charakteristische Gleichung hat keine Lösung, also können wir keine allgemeine Lösung der RB bestimmen.

Weitere Beispiele in [8-Advanced Counting-J-Schuler_V3-0.pdf](#) S. 23 ff.

Erzeugende FunktionenRepetition Polynom n-ten Grades

- i) Funktionen der Form $y = f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, mit $a_n \neq 0$ und $n \in \mathbb{N}$, heißen Polynome n-ten Grades.
- ii) Kurzschreibweise: $y = f(x) = \sum_{k=0}^n a_k \cdot x^k$
- iii) Die höchste Potenz heißt „Grad“ des Polynoms.
- iv) Die Koeffizienten $a_k \in \mathbb{R}$ sind beliebige, aber feste reelle Zahlen.

Definition

Die erzeugende Funktion der Folge $a_0, a_1, \dots, a_k, \dots$ von reellen Zahlen ist die unendliche Reihe

$$G(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + a_3 x^3 + \dots = \sum_{k=0}^{\infty} a_k x^k.$$

Bsp. #1

- $[3, 3, 3, \dots] \rightsquigarrow G(x) = 3x^0 + 3x^1 + 3x^2 + 3x^3 + \dots = \sum_{k=0}^{\infty} 3 x^k$
- $[1, 2, 3, \dots] \rightsquigarrow G(x) = 1x^0 + 2x^1 + 3x^2 + 4x^3 + \dots = \sum_{k=0}^{\infty} (k+1) x^k$
- $[1, 1, 1, 1, 1] \rightsquigarrow G(x) = 1x^0 + 1x^1 + 1x^2 + 1x^3 + 1x^4 = \sum_{k=0}^4 1 x^k$

Für die ersten zwei Beispiele (unendlich viele Summanden) könnte man auch wie folgt fragen: Gegeben ist die Folge $\{a_k\}$ mit $a_k = 3$ resp. $a_k = k + 1$, wie heißt die erzeugende Funktion.

Bsp. #2

Bestimmen Sie die erzeugenden Funktionen der folgenden Zahlenfolgen. Geben Sie die gefundenen Funktionen in möglichst einfacher Form (geschlossen) an.

- ① $\binom{m}{0}, \binom{m}{1}, \dots, \binom{m}{m}$, ② $1, 1, 1, 1, \dots$, ③ $1, a, a^2, a^3, \dots$

→ Lösung auf Folgeseite

zu 1: $G(x) = \binom{m}{0} \cdot x^0 + \binom{m}{1} \cdot x^1 + \binom{m}{2} \cdot x^2 + \dots + \binom{m}{m} \cdot x^m = \underbrace{\sum_{k=0}^m \binom{m}{k} \cdot x^k \cdot 1^{m-k}}_{=(1+x)^k}$

zu 2: $G(x) = \underbrace{1 \cdot x^0 + 1 \cdot x^1 + 1 \cdot x^2 + 1 \cdot x^3 + \dots}_{\text{geometrische Reihe mit } q=x} = \frac{1}{1-x} \text{ für } |x| < 1$

zu 3: $G(x) = \underbrace{1 + ax + (ax)^2 + (ax)^3 + \dots}_{\text{geometrische Reihe mit } q=ax} = \frac{1}{1-ax} \text{ für } |ax| < 1, \text{ also } |x| < \frac{1}{|a|}$

Tipps:

1. Zu 1: Repetieren Sie aus den Unterlagen zur Semesterwoche 5 die Theorie des Binomialkoeffizienten und Pascal'schen Dreieck, resp. die Berechnung von $(1+x)^m$. Bringen Sie das nun hier ein, um die erzeugende Funktion zu vereinfachen.

2. Repetieren Sie für 2 & 3 die Theorie zu den (unendlichen) geometrischen Reihen (siehe Unterlagen Semesterwoche 3). Bringen Sie das nun hier ein, um die erzeugende Funktion zu vereinfachen.

Anwendung: Anzahl Lösungen in den natürlichen Zahlen von Ungleichungen

Wieviele Lösungen hat die Gleichung $x_1 + x_2 + x_3 = 17$, falls $x_1, x_2, x_3 \in \mathbb{N}$ und

- $2 \leq x_1 \leq 5$
- $3 \leq x_2 \leq 6$
- $4 \leq x_3 \leq 7$

gelten soll?

Lösung:

Die Ungleichung $2 \leq x_1 \leq 5$ wird in der folgenden Form geschrieben:

$$\sum_{x_1=2}^5 x^{x_1} = x^2 + x^3 + x^4 + x^5$$

Die Ungleichung $3 \leq x_2 \leq 6$ wird in der folgenden Form geschrieben:

$$\sum_{x_2=3}^6 x^{x_2} = x^3 + x^4 + x^5 + x^6$$

Die Ungleichung $4 \leq x_3 \leq 7$ wird in der folgenden Form geschrieben:

$$\sum_{x_3=4}^7 x^{x_3} = x^4 + x^5 + x^6 + x^7$$

Nun bilden wir das Produkt:

$$\left(\sum_{x_1=2}^5 x^{x_1} \right) \cdot \left(\sum_{x_2=3}^6 x^{x_2} \right) \cdot \left(\sum_{x_3=4}^7 x^{x_3} \right) =$$

$$= (x^2 + x^3 + x^4 + x^5) \cdot (x^3 + x^4 + x^5 + x^6) \cdot (x^4 + x^5 + x^6 + x^7) =$$

$$= x^{2+3+4} + \dots + x^{4+6+7} + \dots + \underbrace{x^{x_1+x_2+x_3}}_{\text{allgemein}} + \dots + x^{5+6+7} = x^9 + \dots + x^{17} + \dots + x^{18} =$$

Vorfaktor

Frage: Wie oft kann man x^{17} darstellen?

Antwort:

Das erfährt man, wenn man das ausrechnet. Das kann man von Hand (natürlich mühsam) oder mit einem Tool (Wolfram Alpha, Maple) machen. Mit Maple Tool ausgerechnet gibt es:

$$\text{expand}(\sum(x^k, k=2..5) \cdot \sum(x^k, k=3..6) \cdot \sum(x^k, k=4..7))$$

$$x^{18} + 3x^{17} + 6x^{16} + 10x^{15} + 12x^{14} + 12x^{13} + 10x^{12} + 6x^{11} + 3x^{10} + x^9$$

Also: $\hookrightarrow \text{TR: direkt mit } \Sigma\text{-Zeichen ausfüllen}$

$$= x^{18} + 3x^{17} + \dots + x^9. \text{ Der Koeffizient von } x^{17}, \text{ also die } 3 \text{ ist die gesuchte Anzahl der Lösungen.}$$

Bemerkung: Die TI-Rechner haben den „expand“-Befehl auch!

\hookrightarrow nein, 3: Algebra, 3: Entwickle

Weiteres Beispiel (Wieviele Arten verteilen, wenn mindestens & maximal)

Sie haben 3 Kinder und 8 identisch aussehende SUGUS (z.B. grüne). Auf wie viele Arten können Sie nun die SUGUS verteilen, wenn jedes Kind mindestens zwei und kein Kind mehr als vier SUGUS erhalten soll? Für jedes Kind $i = 1, 2, 3$ gilt:

- $2 \leq x_i \leq 4$ und damit gilt für jedes Kind:

$$\sum_{x_i=2}^4 x^{x_i} = x^2 + x^3 + x^4 \text{ und somit } (x^2 + x^3 + x^4)^3$$

- $(x^2 + x^3 + x^4)^3 = x^{12} + 3x^{11} + 6x^{10} + 7x^9 + 6x^8 + 3x^7 + x^6$
- Also auf 6 Arten, was man sehr gut auch ohne erzeugende Funktionen überprüfen kann, denn es gibt nur die Möglichkeiten $(2, 2, 4); (2, 4, 2); (4, 2, 2); (2, 3, 3); (3, 2, 3); (3, 3, 2)$.

Erweitertes Ein-/Ausschlussprinzip

Mengenvereinigung

Für beliebige Mengen A und B gilt

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

Bsp.

Wie viele positive natürliche Zahlen nicht grösser als 1000 sind durch 7 oder 11 teilbar?

Lösung:

$\underbrace{(7)}_{\text{xheist } 7 \text{ teilt die Zahl } x} \times \text{heist } 7 \text{ teilt die Zahl } x$

$$A = \{x \mid x \in \mathbb{N} \wedge x \leq 1000 \wedge 7|x\} = \{7; 14, \dots; 994\}$$

$$= \underline{\underline{|A| = 142}}$$

$$B = \{y \mid y \in \mathbb{N} \wedge y \leq 1000 \wedge 11|y\} = \{11; 22, \dots; 990\}$$

$$= \underline{\underline{|B| = 90}} \quad \text{77} = 7 \cdot 11$$

$$A \cap B = \{z \mid z \in \mathbb{N} \wedge z \leq 1000 \wedge 7|z \wedge 11|z\} = \{1 \cdot 77; 2 \cdot 77; \dots; 12 \cdot 77\}$$

$$\Rightarrow \underline{\underline{|A \cap B| = 12}}$$

$$|A \cup B| = |A| + |B| - |A \cap B| = \underline{\underline{102 + 90 - 12 = 220}}$$

Definition Ein-/Ausschlussprinzip

Falls A_1, A_2, \dots, A_n beliebige, endliche Mengen sind, dann gilt:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$$

$$+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots$$

$$\dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|$$

→ Also immer $+, -, +, -, +, -, +, -, \dots$

Bsp. $n = 3$

$$\text{Für } n = 3: |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Bsp $n = 4$

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1| + |A_2| + |A_3| + |A_4|$$

$$- |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_3 \cap A_4|$$

$$+ |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4|$$

$$- |A_1 \cap A_2 \cap A_3 \cap A_4|$$

Derangement

Ein **Derangement** ist eine Permutation, die kein Objekt am selben Platz lässt.

Die Anzahl Derangements bei einer Menge von n Elementen ist:

$$D_n = n! \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} \right]$$

i unver = 0 → weglassen

Summenformel (selbst herausgefunden):

$$D_n = n! \cdot \left(\sum_{x=0}^n \left(\frac{1}{x!} \cdot (-1)^x \right) \right)$$

Mit TR: Einfach Summenformel eingeben. Und «crl» + «enter» Drücken um Dezimalzahl zu bekommen.

$$\rightarrow D_{10} = 10! \cdot \left(\sum_{x=0}^{10} \left(\frac{1}{x!} \cdot (-1)^x \right) \right) = 1334961$$

Bsp. DerangementPräsenzbeispiel 5.3:

Für $n = 2$

Geg. 12 → Derangements 21, also $D_2 = 1$ oder berechnet: $D_2 = 2! \left[1 - \frac{1}{1!} + \frac{1}{2!} \right] = 2 \cdot \frac{1}{2} = 1$

Für $n = 3$

Geg. 123 → Derangements 231; 312, also $D_3 = 2$ oder berechnet:

$$D_3 = 3! \left[\frac{1}{2!} - \frac{1}{3!} \right] = 6 \cdot \frac{1}{2} - \frac{1}{6} = 6 \cdot \frac{1}{3} = 2$$

Für $n = 4$

Geg. 1234 → Derangements 2341; 2413, 2143

3142; 3412; 3421

4123; 4312; 4321 $D_4 = 9$ oder berechnet:

$$D_4 = 4! \cdot \left[\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} \right] = 24 \cdot \left[\frac{1}{2} - \frac{1}{6} + \frac{1}{24} \right] = 24 \cdot \frac{12 - 4 + 1}{24} = 9$$

Anwendung (Anzahl Mögl. Etwas aufzuteilen ohne zweimal etwas an denselben Ort zu tun)

Wir haben n Briefe und stecken diese zufällig in n Couverts. Mit welcher Wahrscheinlichkeit befindet sich kein Brief im richtigen Couvert?

Allgemeine Lösung: $p(\text{kein B. steckt im richtigen C.}) = \frac{\# \text{günstige Fälle}}{\# \text{mögliche Fälle}} = \frac{D_n}{n!}$

Das gibt dann für $n = 2, \dots, 5$ die folgenden Resultate:

Für $n = 2$: $p(\text{kein B. steckt im richtigen C.}) = \frac{\# \text{günstige Fälle}}{\# \text{mögliche Fälle}} = \frac{D_2}{2!} = \frac{1}{2}$

Für $n = 3$: $p(\text{kein B. steckt im richtigen C.}) = \frac{\# \text{günstige Fälle}}{\# \text{mögliche Fälle}} = \frac{D_3}{3!} = \frac{2}{6} = \frac{1}{3}$

Für $n = 4$: $p(\text{kein B. steckt im richtigen C.}) = \frac{\# \text{günstige Fälle}}{\# \text{mögliche Fälle}} = \frac{D_4}{4!} = \frac{9}{24} = \frac{3}{8}$

Für $n = 5$: $p(\text{kein B. steckt im richtigen C.}) = \frac{\# \text{günstige Fälle}}{\# \text{mögliche Fälle}} = \frac{D_5}{5!} = \frac{44}{120} = \frac{11}{30}$

Bsp. #1

Es werden 100 Briefe zufällig in die adressierten Umschläge gesteckt. Mit welcher Wahrscheinlichkeit befindet sich kein Brief im richtigen Umschlag?

$$p = \frac{\# \text{günstige Fälle}}{\# \text{mögliche Fälle}} = \frac{D_{100}}{100!} = \frac{100! \cdot \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{1}{100!} \right]}{100!} = \underbrace{\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{1}{100!} \right]}_{\approx e^{-1}} \approx e^{-1} \approx 0,368 \cong \text{ca. } 37\%$$

Zahlentheorie

Mod n Operation und Euklidischer Algorithmus

Division mit Rest (Dividend, Divisor, Quotient, $R_n(a)$)

Für beliebige $a, n \in \mathbb{Z}$ mit $n \neq 0$ existieren eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ (genannt Quotient) und $r \in \mathbb{Z}$ (genannt Rest) mit

$$a = q \cdot n + r \quad \text{und} \quad 0 \leq r < |n|$$

Man nennt a den **Dividend** und n den **Divisor**. Oft schreibt man auch $r = R_n(a) = a \bmod n$ (Rest von a bei Division durch n).

Mit TR: Menu:2:6 (Bsp. 13 mod 5 → remain(13,5))

Achtung: Bei **negativen Werten** ist die Angabe vom TR nicht korrekt. Typischerweise muss **nochmals der Divisor hinzugerechnet** werden, um eine **positive Zahl zu bekommen**.

Bsp.

Wir geben nun im Detail an: $R_n(a); R_5(13); R_5(-13); R_{-5}(13); R_{-5}(-13)$

- a) $a = q \cdot n + r$ resp. $r = R_n(a) = a \bmod n$
- b) $13 = 2 \cdot 5 + 3$ resp. $r = R_5(13) = 13 \bmod 5 = 3$
- c) $-13 = (-3) \cdot 5 + 2$ resp. $r = R_5(-13) = -13 \bmod 5 = 2$

d) $13 = (-2) \cdot (-5) + 3$ resp. $r = R_{-5}(13) = 13 \bmod (-5) = 3$

Der TI-89 rechnet (siehe unten): $13 = (-3) \cdot (-5) - 2$, also $r = R_{-5}(13) = 13 \bmod (-5) = -2$

e) $-13 = 3 \cdot (-5) + 2$ resp. $r = R_{-5}(-13) = -13 \bmod (-5) = 2$

Der TI-89 rechnet (siehe unten): $-13 = 2 \cdot (-5) - 3$, also $r = R_{-5}(-13) = -13 \bmod (-5) = -3$

Bsp. #2

Beweisen Sie mit der Annahme, dass $a \geq 0$ gilt. Diese Annahme kann man ohne Beschränkung machen, da der Beweis für $a < 0$ analog laufen würde.

- a) $R_n(a) + R_n(-a) = n$
- b) $R_n(a) = R_{-n}(a)$

Lösung:

Beweis zu a) Es gilt für $a = q \cdot n + r$ gemäß Satz: $R_n(a) = r$

Somit gilt für $-a$:

$$\begin{aligned} -a &= (-q) \cdot n - r \Rightarrow -a + (q+1) \cdot n = (-q) \cdot n - r + (q+1) \cdot n = n - r = R_n(-a) \\ &\Rightarrow R_n(a) + R_n(-a) = r + (n - r) = n \end{aligned}$$

Beweis zu b)

$$r = R_{-n}(a) \Rightarrow a + (-q) \cdot (-n) + r = a + q \cdot n + r \Rightarrow r = R_n(a) \text{ und somit ist die Gleichheit gezeigt.}$$

Kongruenz mod n (Beide Zahlen haben denselben Rest bei Division durch n, (\equiv))

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{Z}^+$. Dann ist a kongruent zu b modulo n , falls n ein Teiler von $a - b$ ist, kurz: $n|(a - b)$. Wir schreiben dann kurz:

$$a \equiv b \pmod{n}$$

D.h. **a und b mod n haben denselben Rest**. Bzw. dasselbe Resultat.

Bsp. 18 und 13 mod 5

$$18 \equiv 13 \pmod{5} = 3 \quad \rightarrow 18 \bmod 5 = 3 \text{ und } 13 \bmod 5 = 3$$

Der Euklidische Algorithmus (ggT)

Seien $a, b \in \mathbb{Z}$ (nicht beide gleich 0). Der **größte gemeinsame Teiler ggT(a, b)** ist die **größte ganze Zahl**, die sowohl a als auch b teilt.

Vorgehen/Algorithmus

1. Man dividiere die größere Zahl durch die kleinere und erhalte den Rest.
2. Die kleinere Zahl wird zur größeren, der Rest zur kleineren Zahl
3. Und man beginnt wieder von vorne bis der Rest = 0, dann ist die letzte kleinere Zahl der ggT.

Bsp. ggT(18;48)

$$48 = 2 \cdot 18 + 12$$

$$18 = 1 \cdot 12 + 6$$

$$12 = 2 \cdot 6 + 0$$

Somit ist $ggT(18; 48) = 6$

Eigenschaften des ggT(a,b)

- $ggT(a, 0) = |a|$
- $\forall a, b \in \mathbb{Z} (ggT(a, b) = ggT(\pm a, \pm b))$
- $ggT(a, b) = ggT(a + k \cdot b, b)$
- $ggT(a, b) = ggT(b, R_b(a))$ (**Euklid'sche ggT-Relation**)

Bsp. #2 – Euklid'sche ggT-Relation

$$ggT(18; 48) = ggT(48; 18) = ggT(18; 48 \bmod 18) = ggT(18; 12) = ggT(12; 18 \bmod 12) = ggT(12; 6) = ggT(6; 12 \bmod 6) = ggT(6; 0) = |6| = 6$$

Diophantische Gleichungen

Lösen von linearen Diophantischen Gleichungen

Gleichungen mit zwei oder mehr Unbekannten und gesucht sind **ganzzahligen Lösungen** heissen **Diophantische Gleichungen**.

Satz von Bezout

Für $n, n_1, n_2 \in \mathbb{Z}$ hat die lineare Diophantische Gleichung

$$\boxed{n_1 \cdot x + n_2 \cdot y = n}$$

$n=1 \Rightarrow$ ganzzahlige Lösungen

genau dann ganzzahlige Lösungen $x, y \in \mathbb{Z}$, falls $ggT(n_1, n_2) | n$, d.h. falls $ggT(n_1, n_2)$ ein Teiler von n ist.

$$\rightarrow n_1 \cdot x + n_2 \cdot y = 1$$

Bemerkung:

Der **Grund** liegt darin, dass, wenn wir solche **lin. Dioph. Gl. der Form $n_1 \cdot x + n_2 \cdot y = 1$ lösen** können, dann können wir auch das sogenannte **multiplikative Inverse mod N** (also der Kehrwert einer Zahl mod N) **berechnen**. Diesen Kehrwert wiederum brauchen wir, damit wir die Division mod N definieren können.

Nach dem Satz von Bezout existieren solche Lösungen genau dann, wenn $ggT(n_1, n_2) | 1$, was nichts anderes heisst, als $ggT(n_1, n_2) = 1$, was wiederum nichts anderes heisst, als dass **n_1 und n_2 teilerfremd** sind.

Die Lösungen x und y der diophantischen Gleichung $n_1 \cdot x + n_2 \cdot y = 1$ sind **nicht eindeutig**, denn für jede ganze Zahl k gilt:

$$n_1 \cdot (x + k \cdot n_2) + n_2 \cdot (y - k \cdot n_1) = 1 \quad (*)$$

d.h. $(x + k \cdot n_2)$ und $(y - k \cdot n_1)$ sind für beliebige ganzzahlige k auch Lösungen dieser Gleichung.

Das Inverse mod N (Kehrwert)

Das additive Inverse mod N ((a + b) mod N)

$$(a + b) \text{ mod } N = (a \text{ mod } N + b \text{ mod } N) \text{ mod } N$$

$$(a - b) \text{ mod } N = (a \text{ mod } N - b \text{ mod } N) \text{ mod } N$$

Die Additionstabelle in \mathbb{Z}_5 , also die Addition mod 5:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Bsp.

$$(13 + 49) \text{ mod } 5 \equiv (13 \text{ mod } 5 + 49 \text{ mod } 5) \text{ mod } 5 \equiv (3 + 4) \text{ mod } 5 \equiv 7 \text{ mod } 5 = 2$$

Bei negativen Zahlen:

$$(-13) \text{ mod } 5 \equiv (-13 + 3 \cdot 5) \text{ mod } 5 \equiv 2 \text{ mod } 5 = 2$$

$$(13 - 49) \text{ mod } 5 \equiv -36 \text{ mod } 5 \equiv (-36 + 8 \cdot 5) \equiv 4 \text{ mod } 5 = 4$$

*Multiplikative Inverse mod N ((a * b) mod N)*

$$(a * b) \text{ mod } N = (a \text{ mod } N * b \text{ mod } N) \text{ mod } N$$

Die Multiplikationstabelle in \mathbb{Z}_5 , also die Multiplikation mod 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

Bsp.

$$(13 * 49) \text{ mod } 5 \equiv 637 \text{ mod } 5 = 2$$

$$(13 * 49) \text{ mod } 5 \equiv (13 \text{ mod } 5 * 49 \text{ mod } 5) \text{ mod } 5 \equiv (3 * 4) \text{ mod } 5 \equiv 12 \text{ mod } 5 = 2$$

Das "gezielte Durchprobieren" um multiplikatives Inverses welches 1 ergibt zu bekommen.

Gesucht ist die **Zahl y**, die das **multiplikative Inverse der Zahl x mod N** ist, also:

$$y \equiv x^{-1} \text{ mod } N$$

oder anders ausgedrückt, diejenige Zahl y, so dass:

$$y \cdot x \equiv 1 \text{ mod } N$$

→ **x * y mod N muss den Rest 1 ergeben.** Inverse ist also die Zahl, welche mit x multipliziert werden muss damit das Produkt mod N 1 ergibt.

→ **Online-Rechner** für multiplikatives inverse: <https://planetcalc.com/3311/>

Bsp. Alle inversen Zahlen zu mod 5

x	0	1	2	3	4
y	-	1	3	2	4

Die Kontrolle, ob $y \cdot x \equiv 1 \text{ mod } N$ gilt ist wahrlich einfach.

D.h. es gilt:

- $1 \equiv 1^{-1} \text{ mod } 5$, denn $1 \cdot 1 \equiv 1 \text{ mod } 5$
- $2 \equiv 3^{-1} \text{ mod } 5$, denn $2 \cdot 3 \equiv 6 \equiv 1 \text{ mod } 5$
- $3 \equiv 2^{-1} \text{ mod } 5$, denn $3 \cdot 2 \equiv 6 \equiv 1 \text{ mod } 5$
- $4 \equiv 4^{-1} \text{ mod } 5$, denn $4 \cdot 4 \equiv 16 \equiv 1 \text{ mod } 5$

Bsp. # 2

Gesucht ist $y \equiv 15^{-1} \pmod{26}$

Eine Methode ist das sukzessive berechnen von $y \cdot 15 \equiv z \pmod{N}$ für $y = 1, 2, \dots$ bis $z = 1$ ist.

Also einfach **y durch 0,1,2,...,26 in der Formel «y * 15 mod 26» ersetzen bis Resultat = 1 ist.**

y	0	1	2	3	4	5	6	7
y · 15 mod 26	0	15	4	19	8	23	12	1

Wann existiert das multiplikative inverse der Zahl $x \pmod{N}$?

- $y \equiv x^{-1} \pmod{N}$ existiert nur, wenn der $\text{ggT}(x; N) = 1$,
- d.h. **x und N müssen teilerfremd d.h. relativ prim sein**

Bsp.

$\text{ggT}(15; 26) = 1$, darum existiert $15^{-1} \pmod{26}$ (der Wert ist ja 7)

$\text{ggT}(7; 26) = 1$, darum existiert $7^{-1} \pmod{26}$ (der Wert ist ja 15).

Bsp. #2

Wir betrachten \mathbb{Z}_9 , d.h. alle Zahlen mod 9, $\mathbb{Z}_9 = \{0, 1, \dots, 8\}$ und wir geben, dort wo es möglich ist, die Inversen mod 9 an.

x	0	1	2	3	4	5	6	7	8
y = x⁻¹ mod 9	-	1	5	-	7	2	-	4	8

Sei p eine **Primzahl**, dann ist $\mathbb{Z}_p = \{0, 1, \dots, (p-1)\}$. Dann haben – mit **Ausnahme der Null** – alle Werte ein **multiplikatives Inverses mod p**.

Es gilt ja allgemein, dass $\frac{x}{y} = x \cdot y^{-1}$ ist. Grundsätzlich **schreiben wir $x \cdot y^{-1} \pmod{N}$** und **nicht $\frac{x}{y} \pmod{N}$** .

→ Nie kürzen!!

Das Inverse mod N & der erweiterte Euklidische Algorithmus

Wir betrachten die lineare diophantische Gleichung $n_1 \cdot x + n_2 \cdot y = 1$, die wir umformen, um das multiplikative Inverse zu bestimmen.

Gegeben ist folgendes und wir wollen das multiplikative inverse von x herausfinden:

$\text{ggT}(n_1, n_2) = \text{ggT}(963, 218) = 1$ und es existieren Zahlen $x = (-103)$; $y = 455$ sodass $963 \cdot (-103) + 218 \cdot 455 = 1$

Umformungsschritte	Operation	Beispiel
		$218 \cdot y \pmod{218} = 0$
$n_1 \cdot x + n_2 \cdot y = 1$		$963 \cdot (-103) + 218 \cdot 455 = 1$
$n_1 \cdot x = 1 - n_2 \cdot y$	<u>mod n₂</u> resp. mod 218	$963 \cdot (-103) \equiv 1 - 218 \cdot 455 \pmod{218}$
$n_1 \cdot x \equiv 1 \pmod{n_2}$		$(963 \cdot (-103)) \pmod{218} \equiv 1 \pmod{218}$
	Mit mod 218 weiterrechnen	* $91 \cdot 115 \equiv 1 \pmod{218}$
d.h. x ist das multiplikative Inverse von $n_1 \pmod{n_2}$	* $963 \pmod{218} = 91$ -103: Da negativ + k.N $\Rightarrow -103 + 1 \cdot 218 = 115$ $\Rightarrow 115 \pmod{218} = 115$	d.h. 115 ist das multiplikative Inverse von 91 mod 218 Also: <u>$115 \equiv 91^{-1} \pmod{218}$</u> Und <u>$91 \equiv 115^{-1} \pmod{218}$</u>

Für das multiplikative inverse von y kann das analog Berechnet werden. Siehe Lösung auf der nächsten Seite

Umformungsschritte	Operation	Beispiel
$n_1 \cdot x + n_2 \cdot y = 1$		$963 \cdot (-103) + 218 \cdot 455 = 1$
$n_2 \cdot y = 1 - n_1 \cdot x$	mod n_1 resp. mod 963	$218 \cdot 455 = 1 - 963 \cdot (-103)$
$n_2 \cdot y \equiv 1 \text{ mod } n_1$		$\underline{218 \cdot 455} \equiv 1 \text{ mod } 963$
	Mit mod 963 weiterrechnen	Nicht mehr nötig
d.h. y ist das multiplikative Inverse von $n_2 \text{ mod } n_1$		d.h. 455 ist das multiplikative Inverse von 218 mod 963 Also: $\underline{218 \equiv 455^{-1} \text{ mod } 963}$ Und $\underline{455 \equiv 218^{-1} \text{ mod } 963}$

Der erweiterte Euklidische Algorithmus (x & y finden, sodass $n_1 * x + n_2 * y = 1$)

Wir wollen $x, y \in \mathbb{Z}$ so finden, dass gilt: $211 \cdot x + 13 \cdot y = 1$

- Wir führen den (normalen) Euklidischen Algorithmus mit den beiden Zahlen n_1, n_2 durch:

$$\begin{aligned} 211 &= 16 \cdot 13 + 3 \quad (***) \\ 13 &= 4 \cdot 3 + 1 \quad (*) \\ (3 &= 3 \cdot 1 + 0) \\ \text{Also: ggT}(211, 13) &= 1 \end{aligned}$$

- Nun nutzen wir diese Gleichungen in umgekehrter Reihenfolge, um jeweils störende Terme zu eliminieren.

	Umformungsschritte	Beschreibung
$ggT(211; 13) = 1$	$= 13 - 4 \cdot 3$	Gleichung (*) auf 1 aufgelöst
	$= 13 - 4 \cdot (211 - 16 \cdot 13)$	Gleichung (**) auf 3 aufgelöst und für 3 eingesetzt
	$= 1 \cdot 13 - 4 \cdot 211 + 64 \cdot 13$	Nur noch ausrechnen
	$= (-4) \cdot 211 + 65 \cdot 13$	$* 1 \cdot 13 + 64 \cdot 13 \Rightarrow 65 \cdot 13$

Das Multiplikative Inverse ist demnach, siehe Theorie dazu im vorherigen Abschnitt:

- 65 ist das multiplikative Inverse von 13 mod 211, d.h. $65 \equiv 13^{-1} \text{ mod } 211$, die Kontrolle dazu ist einfach, denn $65 \cdot 13 \text{ mod } 211 \equiv 845 \text{ mod } 211 = 1$.
- 13 ist das multiplikative Inverse von 65 mod 211, d.h. $13 \equiv 65^{-1} \text{ mod } 211$, die Kontrolle dazu ist einfach, denn $13 \cdot 65 \text{ mod } 211 \equiv 845 \text{ mod } 211 = 1$.

Bevor wir die Interpretation mod 13 machen können, müssen wir noch umrechnen:

$$(-4) \text{ mod } 13 = 9 \text{ und } 211 \text{ mod } 13 = 3$$

- 211, resp. eben 3 ist das multiplikative Inverse von (-4), resp. 9 mod 13, d.h. $3 = 9^{-1} \text{ mod } 13$, die Kontrolle dazu ist einfach, denn $3 \cdot 9 \text{ mod } 13 \equiv 27 \text{ mod } 13 = 1$.
- Und umgekehrt.

Die Fragestellung könnte auch anders sein, zum Beispiel:

Wir suchen die Berechnung von $237^{-1} \text{ mod } 280$.

→ wenn 237 und 280 teilerfremd, also $\text{ggT} = 1$, dann wäre die Formel $280 \cdot x + 237 \cdot y = 1$. Diese dann gemäß Schema von oben ausrechnen.

Beispiel Prüfungsaufgabe (Finden Sie $x, y \in \mathbb{Z}$ mit $963 \cdot x + 218 \cdot y = 1$)

- Finden Sie $x, y \in \mathbb{Z}$ mit $963 \cdot x + 218 \cdot y = 1$
- Finden Sie ein modulares Inverses von 963 modulo 218.
- Finden Sie ein modulares Inverses von 218 modulo 963.
- Lösen Sie die Relation $963 \cdot x \equiv 1 \pmod{218}$.

Von oben nach unten der Euklid Alg.

$$\begin{aligned} 963 &= 4 \cdot 218 + 91 \\ 218 &= 2 \cdot 91 + 36 \\ 91 &= 2 \cdot 36 + 19 \\ 36 &= 1 \cdot 19 + 17 \\ 19 &= 1 \cdot 17 + 2 \\ 17 &= 8 \cdot 2 + 1 \end{aligned}$$

Von unten nach oben der ext. Euklid Alg.

$$\begin{aligned} &= 43 \cdot 218 - 103(963 - 4 \cdot 218) = (-103)963 + 455 \cdot 218 \\ &\stackrel{\uparrow}{=} -17 \cdot 91 + 43(218 - 2 \cdot 91) = 43 \cdot 218 - 103 \cdot 91 \\ &\stackrel{\uparrow}{=} 9 \cdot 36 - 17(91 - 2 \cdot 36) = -17 \cdot 91 + 43 \cdot 36 \\ &\stackrel{\uparrow}{=} -8 \cdot 19 + 9(36 - 1 \cdot 19) = 9 \cdot 36 - 17 \cdot 19 \\ &\stackrel{\uparrow}{=} 1 \cdot 17 - 8(19 - 1 \cdot 17) = -8 \cdot 19 + 9 \cdot 17 \\ &\stackrel{\uparrow}{=} 1 = 17 - 8 \cdot 2 \end{aligned}$$

Also

$$1 = \underbrace{(-103)}_{x} \underbrace{963}_{n_1} + \underbrace{455}_{y} \underbrace{218}_{n_2}$$

Damit

$$\begin{array}{lll} 455 \cdot 218 = 1 \pmod{963} & \text{d.h.} & 455 = 218^{-1} \pmod{963} \\ \underbrace{(-103)963 = 1 \pmod{218}}_{115 \cdot 91} & \text{d.h.} & 115 = 91^{-1} \pmod{218} \text{ oder} \\ & & 91 = 115^{-1} \pmod{218} \end{array}$$

$\pmod{218}$

Der Chinesische Restsatz

Definition

Seien $m_1, m_2, \dots, m_k \in \mathbb{N}^+$ paarweise teilerfremde Zahlen und $m := m_1 \cdot m_2 \cdots m_k$. Dann besitzt das System von k simultanen Kongruenzen

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &\vdots \\ x &\equiv r_k \pmod{m_k} \end{aligned} \quad \begin{array}{l} m_1 \dots m_k \\ \text{ggT}(m_i, m_j) = 1 \\ \text{für } i \neq j \end{array}$$

eine eindeutige Lösung $x \pmod{m}$.

Wichtig:

Der **Chinesische Restsatz** ist nur gültig (bringt eine Lösung), wenn:

1. m_1, m_2, \dots, m_k alle untereinander **teilerfremd** sind. ($\text{ggT} = 1$)
2. Ist die Bedingung nicht erfüllt kann es trotzdem eine Lösung geben, wir können diese aber mit dem Chinesischen Restsatz nicht ausrechnen.

Vorgehensweise anhand von einem Beispiel

Welche Zahl(en) x ergeben bei der Division durch 4 den Rest 3, bei der Division durch 3 den Rest 1 und bei der Division durch 5 den Rest 3?

Schritt 1: Variablen-deklaration (x = die gesuchte Zahl) und Aufstellen der Bedingungen.

$$\begin{array}{ll} \text{I. } x \equiv 3 \pmod{4} & \Rightarrow r_1 = 3 \\ \text{II. } x \equiv 1 \pmod{3} & \Rightarrow r_2 = 1 \\ \text{III. } x \equiv 3 \pmod{5} & \Rightarrow r_3 = 3 \end{array}$$

Teiler

3 mod 4 heisst:
bei Division durch 4 bleibt ein Rest von 3

Schritt 2:

Check, ob die Bedingungen des Chinesischen Restsatzes erfüllt sind. Wenn ja, dann berechnen von m und allen M_i .

Bedingungen OK, da 4, 3 & 5 paarweise teilerfremd, also $\text{ggT}(4, 3) = \text{ggT}(3, 5) = \text{ggT}(4, 5) = 1$.

$$m = 4 \cdot 3 \cdot 5 = 60; M_1 = \frac{m}{m_1} = \frac{60}{4} = 15$$

$$M_2 = \frac{m}{m_2} = \frac{60}{3} = 20$$

$$M_3 = \frac{m}{m_3} = \frac{60}{5} = 12$$

Mit Online-Tool berechnen:
<https://planetcalc.com/3311/>

Schritt 3: Berechnen von y_i , so dass $M_i \cdot y_i \equiv 1 \pmod{m_i}$

In diesen Fällen kann man das mit Durchprobieren machen, ansonsten mit dem erweiterten Euklid oder mit einem Tool. Achtung: Zumindest der TI-89 und weitere TI-Rechner können es nicht!!

$$M_1 \cdot y_1 \equiv 1 \pmod{m_1} \Rightarrow 15 \cdot y_1 \equiv 1 \pmod{4}; 15 \cdot 3 \equiv 45 \equiv 1 \pmod{4} \Rightarrow y_1 = 3 \equiv 15^{-1} \pmod{4}$$

$$M_2 \cdot y_2 \equiv 1 \pmod{m_2} \Rightarrow 20 \cdot y_2 \equiv 1 \pmod{3}; 20 \cdot 2 \equiv 40 \equiv 1 \pmod{3} \Rightarrow y_2 = 2 \equiv 20^{-1} \pmod{3}$$

$$M_3 \cdot y_3 \equiv 1 \pmod{m_3} \Rightarrow 12 \cdot y_3 \equiv 1 \pmod{5}; 12 \cdot 3 \equiv 36 \equiv 1 \pmod{5} \Rightarrow y_3 = 3 \equiv 12^{-1} \pmod{5}$$

Bemerkungen:

1) Man darf immer mit mod n reduzieren:

$$15 \cdot y_1 \equiv 3 \cdot y_1 \equiv 1 \pmod{4}; 3 \cdot 3 \equiv 9 \equiv 1 \pmod{4} \Rightarrow y_1 = 3 \equiv 3^{-1} \equiv 15^{-1} \pmod{4}$$

$$20 \cdot y_2 \equiv 2 \cdot y_2 \equiv 1 \pmod{3}; 2 \cdot 2 \equiv 4 \equiv 1 \pmod{3} \Rightarrow y_2 = 2 \equiv 2^{-1} \equiv 20^{-1} \pmod{3}$$

$$12 \cdot y_3 \equiv 2 \cdot y_3 \equiv 1 \pmod{5}; 2 \cdot 3 \equiv 6 \equiv 1 \pmod{5} \Rightarrow y_3 = 3 \equiv 2^{-1} \equiv 12^{-1} \pmod{5}$$

2) Die y_i können auch mit dem erweiterten Euklid gerechnet werden.

Schritt 4: Berechnen der Lösung:

Reste mod $i \rightarrow$ von Ausgangslage

$$x = \sum_{i=1}^3 r_i \cdot M_i \cdot y_i \equiv r_1 \cdot M_1 \cdot y_1 + r_2 \cdot M_2 \cdot y_2 + r_3 \cdot M_3 \cdot y_3 \pmod{m}$$

$$x = 3 \cdot 15 \cdot 3 + 1 \cdot 20 \cdot 2 + 3 \cdot 12 \cdot 3 \equiv 283 \pmod{60} \equiv 43 \pmod{60}$$

Schritt 5: Kontrolle durch Einsetzen der Lösung $x = 43$ in die Ausgangsbedingungen.

Resultatformulierung: Die gesuchten Zahlen sind von der Form $43 + k \cdot 60$.

Resultat immer in der Form $x + k \cdot m$

Eulerische ϕ -Funktion («Phi» - Teilerfremde natürliche Zahlen kleiner n)

Definition

Die Eulersche ϕ -Funktion ordnet jeder natürlichen Zahl n die Anzahl der zu ihr teilerfremden natürlichen Zahlen zu, die kleiner als n sind.

Die Eulersche ϕ -Funktion ist gegeben durch:

$$\phi : \mathbb{N} \rightarrow \mathbb{N}, n \mapsto |\mathbb{Z}_n^*| =: \phi(n)$$

- $\mathbb{Z}_n = \{0, 1, \dots, (n-1)\}$
- $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x > 0 \text{ und } \text{ggT}(x, n) = 1\}$
- $|\mathbb{Z}_n^*| = \underline{\text{Anzahl Elemente in } \mathbb{Z}_n^*}$

Bsp. Resultat = Anzahl Teilerfremde natürliche Zahlen

- a) $\mathbb{Z}_2 = \{0, 1\} \Rightarrow \mathbb{Z}_2^* = \{1\} \Rightarrow |\mathbb{Z}_2^*| = \phi(2) = 1$
- b) $\mathbb{Z}_3 = \{0, 1, 2\} \Rightarrow \mathbb{Z}_3^* = \{1, 2\} \Rightarrow |\mathbb{Z}_3^*| = \phi(3) = 2$
- c) $\mathbb{Z}_4 = \{0, 1, 2, 3\} \Rightarrow \mathbb{Z}_4^* = \{1, 3\} \Rightarrow |\mathbb{Z}_4^*| = \phi(4) = 2$
- d) $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \Rightarrow \mathbb{Z}_5^* = \{1, 2, 3, 4\} \Rightarrow |\mathbb{Z}_5^*| = \phi(5) = 4$
- e) $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow \mathbb{Z}_6^* = \{1, 5\} \Rightarrow |\mathbb{Z}_6^*| = \phi(6) = 2$
- f) $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, \dots, 6\} \Rightarrow \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} \Rightarrow |\mathbb{Z}_7^*| = \phi(7) = 6$
- g) $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, \dots, 7\} \Rightarrow \mathbb{Z}_8^* = \{1, 3, 5, 7\} \Rightarrow |\mathbb{Z}_8^*| = \phi(8) = 4$
- h) $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, \dots, 8\} \Rightarrow \mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} \Rightarrow |\mathbb{Z}_9^*| = \phi(9) = 6$
- i) $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, \dots, 11\} \Rightarrow \mathbb{Z}_{12}^* = \{1, 5, 7, 11\} \Rightarrow |\mathbb{Z}_{12}^*| = \phi(12) = 4$
- j) $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, \dots, 14\} \Rightarrow \mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\} \Rightarrow |\mathbb{Z}_{15}^*| = \phi(15) = 8$
- k) $\mathbb{Z}_{16} = \{0, 1, 2, 3, 4, \dots, 15\} \Rightarrow \mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\} \Rightarrow |\mathbb{Z}_{16}^*| = \phi(16) = 8$
- l) $\mathbb{Z}_{36} = \{0, 1, 2, 3, \dots, 35\} \Rightarrow \mathbb{Z}_{36}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} \Rightarrow |\mathbb{Z}_{36}^*| = \phi(36) = 12$

Seien p und q zwei verschiedene Primzahlen, $m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$ die Primfaktorzerlegung von $m \in \mathbb{N}$ und weiter $n \in \mathbb{N}$ teilerfremd zu m ($\text{ggT}(m, n) = 1$). Dann gilt

$\phi(p) = p - 1$

$\phi(p \cdot q) = (p - 1) \cdot (q - 1)$

$\phi(m) = (p_1 - 1) \cdot p_1^{r_1-1} \cdot (p_2 - 1) \cdot p_2^{r_2-1} \cdots (p_n - 1) \cdot p_n^{r_n-1}$

$\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

im TR factor(m) eintippen, um Primfaktorzerlegung zu erlangen.
Bsp. für $m = 8 \rightarrow 2^3$

→ Output = Anzahl teilerfremde nat. Zahlen $< n$

Anwendungsregeln / Ausrechnen von teilerfremden Zahlen

- a) Per Definition ist $\phi(1) = 1$
- b) Offensichtlich ist klar, dass für p prim gilt: $\phi(p) = p - 1$:
 - a. siehe oben für $p = 2, 3, 5, 7$ (Wichtig: 1 ist keine Primzahl!!)
- c) Wenn p und q prim sind gilt $\phi(p \cdot q) = (p - 1) \cdot (q - 1)$
 - a. $\phi(6) = \phi(2 \cdot 3) = (2 - 1) \cdot (3 - 1) = 1 \cdot 2 = 2$
 - b. $\phi(15) = \phi(3 \cdot 5) = (3 - 1) \cdot (5 - 1) = 2 \cdot 4 = 8$
- d) Wenn p prim, dann gilt $\phi(p^r) = (p - 1) \cdot (p^{r-1})$
 - a. $\phi(8) = \phi(2^3) = (2 - 1) \cdot (2^2) = 1 \cdot 4 = 4$
 - b. $\phi(9) = \phi(3^2) = (3 - 1) \cdot (3^1) = 2 \cdot 3 = 6$
 - c. $\phi(36) = \phi(6^2) \neq (6 - 1) \cdot (6^1), \text{ da } 6 \text{ keine Primzahl ist!!}$
- e) Wenn p und q prim, dann gilt $\phi(p^r \cdot q^s) = (p - 1) \cdot (p^{r-1}) \cdot (q - 1) \cdot (q^{s-1})$
 - a. $\phi(36) = \phi(4 \cdot 9) = \phi(2^2 \cdot 3^2) = (2 - 1) \cdot (2^{2-1}) \cdot (3 - 1) \cdot (3^{2-1}) = 2 \cdot 2 \cdot 3 = 12$
- f) Wenn m und n teilerfremd, dann gilt $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$
 - a. $\phi(36) = \phi(4 \cdot 9) = \phi(4) \cdot \phi(9) = 2 \cdot 6 = 12$
 - b. $\phi(12) = \phi(3 \cdot 4) = \phi(3) \cdot \phi(4) = 2 \cdot 2 = 4$
- g) Es gilt folgender Satz (ohne Beweis): Für $n \geq 3$ gilt $\phi(n)$ ist gerade,

Bsp.

Ein Beispiel zum letzten Teil des Satzes. Bekanntlich sind $m = 150 = 2 \cdot 3 \cdot 5^2$ und $n = 77 = 7 \cdot 11$ teilerfremd, d.h. $\text{ggT}(150, 77) = 1$. Dann gilt

$$\begin{aligned}\phi(11550) &= \phi(150 \cdot 77) = \phi(150) \cdot \phi(77) \\ &= (2-1) \cdot 2^0 \cdot (3-1)3^0 \cdot (5-1) \cdot 5^1 \cdot (7-1) \cdot (11-1) = 1 \cdot 2 \cdot 4 \cdot 5 \cdot 6 \cdot 10 = 2400.\end{aligned}$$

Oder ausführlicher:

Ein Beispiel zum letzten Teil des Satzes. Bekanntlich sind $m = 150 = 2^1 \cdot 3^1 \cdot 5^2$ und $n = 77 = 7^1 \cdot 11^1$ teilerfremd, d.h. $\text{ggT}(150, 77) = 1$. Dann gilt

$$\begin{aligned}\phi(11550) &= \phi(150 \cdot 77) = \phi(150) \cdot \phi(77) \\ &= (2-1) \cdot 2^0 \cdot (3-1)3^0 \cdot (5-1) \cdot 5^1 \cdot \underbrace{(7-1)}_{(1-1)} \cdot \underbrace{(11-1)}_{(1-1)} = 1 \cdot 2 \cdot 4 \cdot 5 \cdot 6 \cdot 10 = 2400.\end{aligned}$$

Primzahlen

Definition und Eigenschaften

Eine natürliche Zahl $p > 1$ heißt **Primzahl**, wenn sie nur durch 1 und sich selber teilbar ist.

Jede positive natürliche Zahl $n > 1$ kann (bis auf die Reihenfolge) eindeutig als Produkt von Primzahlen p_1, p_2, \dots, p_r geschrieben werden:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$$

Beispiel 6.1:

$$4536 = 2^3 \cdot 3^4 \cdot 5^0 \cdot 7^1 = 2^3 \cdot 3^4 \cdot 7$$

Der kleine Satz von Fermat ($m^p \bmod p$ – Potenz in Moduloberechnung)

Sei p eine Primzahl und m eine nichtnegative ganze Zahl. Dann gilt

$$m^p \bmod p = m \bmod p$$

Daraus folgt falls $m < p$ gilt: $m^{p-1} \bmod p = 1$ Weiter: $m^{p-2} = m^{-1} \bmod p$

- a) $p = 2: 4^{2-1} \bmod 2 \equiv 4^1 \bmod 2 \equiv 0 \rightarrow$ Bedingung $m < p$ nicht erfüllt.
- b) $p = 3: 4^{3-1} \bmod 3 \equiv 4^2 \bmod 3 \equiv 16 \bmod 3 \equiv 1 \rightarrow$ erfüllt, obwohl Bedingung nicht erfüllt ist. Das wird ja nicht ausgeschlossen mit dem obigen Satz!! Aber wenn $m < p$ nicht erfüllt ist, kann man mit dem kleinen Satz von Fermat **nichts** aussagen!!
- c) $p = 5: 4^{5-1} \bmod 5 \equiv 4^4 \bmod 5 \equiv 256 \bmod 5 \equiv 1 \rightarrow$ erfüllt gemäß kl. Satz von Fermat.
- d) $p = 6: 4^{6-1} \bmod 6 \equiv 4^5 \bmod 6 \equiv 1024 \bmod 6 \equiv 4 \rightarrow$ nicht erfüllt, $p = 6$ ist keine Primzahl.
- e) $p = 7: 4^{7-1} \bmod 7 \equiv 4^6 \bmod 7 \equiv 4096 \bmod 7 \equiv 1 \rightarrow$ erfüllt gemäß kl. Satz von Fermat.

Im Weiteren folgt daraus, dass gilt für $m < p: m^{p-2} = m^{-1} \bmod p$

Bsp.

Berechnen Sie das Inverse von $64 \bmod p$, $p = 311$ eine Primzahl, wenn Sie wissen, $64^{p-3} \equiv 223 \bmod p$.

Aufgabe 6.1:

$$64^{-1} \equiv 64^{p-2} \equiv a \cdot a^{p-3} \equiv 64 \cdot 223 \bmod 311 = 277 \quad * 64 \cdot 64^{311-3} \equiv 6^4 \cdot 64^{308} \equiv$$

Der kleine Satz von Fermat & der Chinesische Restsatz (Grosse Potenzen modulo schnell rechnen)

Mit kleinem Satz von Fermat schnell grosse Potenzen rechnen, denn es gilt:

$$a^{n(p-1)} \pmod{p} \equiv a^{(p-1)n} \pmod{p} \equiv (a^{p-1} \pmod{p})^n \pmod{p} \equiv 1^n \pmod{p} \equiv 1$$

Mit dem Chinesischen Restsatz können wir nun weitere Potenzen $\pmod{p \cdot q}$ mit p und q Primzahlen rechnen.

Es sei nun $t = n \cdot (p-1) = m \cdot (q-1)$ und $r = p \cdot q$, dann gilt: $a^{t \pmod{r}} \equiv 1 \pmod{r}$

$$a^t \pmod{r} \equiv 1$$

Den allgemeinen Beweis führen wir an dieser Stelle nicht, sondern zeigen das an einem Beispiel. Der allgemeine Beweis ginge exakt gleich wie das nachfolgende Zahlenbeispiel, man müsste nur die entsprechenden Parameter anstatt die konkreten Zahlen nehmen.

(Präsenz-)Beispiel 6.3:

$$4^{7-1} \pmod{7} \equiv 4^6 \pmod{7} \equiv 1 \rightarrow 4^{180} \pmod{7} = 4^{6 \cdot 30} \equiv (4^6)^{30} \equiv 1^{30} \equiv 1 \pmod{7}$$

Analog gilt: $4^{11-1} \pmod{11} \equiv 4^{10} \pmod{11} \Rightarrow 4^{480} \pmod{11} \equiv 4^{10 \cdot 48} \pmod{11} \equiv 1$

Nun zeigen wir mit dem Chinesischen Restsatz, dass gilt:

$$x = 4^{480} \pmod{77} \equiv 1$$

Prüfungsbeispiel – Satz von Fermat und Chinesischer Restsatz

- a) Zeigen Sie mit dem kleinen Satz von Fermat, dass gilt: $5^{1200} \pmod{7} \equiv 1$ und $5^{1200} \pmod{13} \equiv 1$
 b) Zeigen Sie nun mit dem Chinesischen Restsatz, dass gilt: $5^{1200} \pmod{91} \equiv 1$.

Lösung:

$$\begin{aligned} a) \quad 5^{1200} \pmod{7} &\equiv 5^{6 \cdot 200} \pmod{7} \equiv (5^6)^{200} \pmod{7} \equiv \left(\underbrace{5^6 \pmod{7}}_{\equiv 1}\right)^{200} \pmod{7} \equiv 1^{200} \pmod{7} \equiv 1 \\ 5^{1200} \pmod{13} &\equiv 5^{12 \cdot 100} \pmod{13} \equiv (5^{12})^{100} \pmod{13} \equiv \left(\underbrace{5^{12} \pmod{13}}_{\equiv 1}\right)^{100} \pmod{13} \\ &\equiv 1^{100} \pmod{13} \equiv 1 \end{aligned}$$

b) Schritt 1:

Wegen $5^{1200} \pmod{91} \equiv 1$ und dem kleinen Satz von Fermat haben wir das folgende System von linearen Kongruenzen:

- I. $x \equiv 1 \pmod{7}$, also $r_1 = 1$
- II. $x \equiv 1 \pmod{13}$, also $r_2 = 1$

Schritt 2:

Check, ob die Bedingungen des Chinesischen Restsatzes erfüllt sind. Wenn ja, dann berechnen von m und allen M_i .

Bedingungen OK, da 7, 13 je unterschiedliche Primzahlen und teilerfremd sind, d.h. $\text{ggT}(7, 13) = 1$.

$$m = 7 \cdot 13 = 91; M_1 = \frac{m}{m_1} = \frac{91}{7} = 13; M_2 = \frac{m}{m_2} = \frac{91}{13} = 7$$

Schritt 3: Berechnen von y_i , so dass $M_i \cdot y_i \equiv 1 \pmod{m_i}$

$$M_1 \cdot y_1 \equiv 1 \pmod{m_1} \Rightarrow 13 \cdot y_1 \equiv 1 \pmod{7}; 13 \cdot 6 \equiv 78 \equiv 1 \pmod{7} \Rightarrow y_1 = 6 \equiv 13^{-1} \pmod{7}$$

$$M_2 \cdot y_2 \equiv 1 \pmod{m_2} \Rightarrow 7 \cdot y_2 \equiv 1 \pmod{13}; 7 \cdot 2 \equiv 14 \equiv 1 \pmod{13} \Rightarrow y_2 = 2 \equiv 7^{-1} \pmod{13}$$

Schritt 4: Berechnen der Lösung und zeigen der Richtigkeit von $x = 5^{1200} \pmod{91} \equiv 1$:

$$x = \sum_{i=1}^2 r_i \cdot M_i \cdot y_i \equiv r_1 \cdot M_1 \cdot y_1 + r_2 \cdot M_2 \cdot y_2 \pmod{m} \equiv 1 \cdot 13 \cdot 6 + 1 \cdot 7 \cdot 2 = 92 \equiv 1 \pmod{91}$$

Verteilung der Primzahlen

Die Abschätzformel für die Anzahl Primzahl von 1 bis x lautet:

$$\pi(x) \approx \frac{x}{\ln(x)}$$

Primzahlsatz von C.F. Gauss (*):

Dieser grundlegende Satz der Zahlentheorie sagt, dass die Primzahlen relativ dicht zwischen den natürlichen Zahlen liegen, es gilt:

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\ln(n)} = \lim_{n \rightarrow \infty} \frac{\pi(n)}{\frac{n}{\ln(n)}} = 1$$

Der Satz sagt aus, dass die Anzahl der Primzahlen ungefähr so schnell wächst wie die Funktion $n/\ln(n)$. Wir sagen auch, dass die beiden Funktionen $\pi(n)$ und $n/\ln(n)$ **asymptotisch äquivalent** sind und bezeichnen das durch

Mehr dazu in [9-11-Einf-Zahlenth-J-Schuler_V3-0.pdf](#) S. 37

Mersenne-Primzahlen

Definition

Für $n \in \mathbb{N}$ heisst $M_n := 2^n - 1$ die n -te **Mersenne-Zahl**. Ist M_n eine Primzahl, so heisst sie **Mersenne-Primzahl**.

Satz

Die Mersenne-Zahlen sind genau die Zahlen, die in Binärschreibweise ausschliesslich aus 1' en bestehen:

$$M_n = 2^n - 1 = 1 \cdot 2^{n-1} + 1 \cdot 2^{n-2} + \dots + 1 \cdot 2^1 + 1 \cdot 2^0 = (11\dots11)_2$$

Mehr dazu in [9-11-Einf-Zahlenth-J-Schuler_V3-0.pdf](#) S. 39

Rechnen in Restesystemen

Relationen und Äquivalenzrelationen (Reflexiv, Symmetrisch, Transitiv)

Eine Relation R auf einer Menge A ist eine Teilmenge von $A \times A$, d.h. $R \subseteq A \times A$.

R ist eine Äquivalenzrelation auf der Menge A, wenn sie eine Relation mit folgenden Eigenschaften ist:

- (1) **Reflexiv:** d.h. $\forall x \in A$ gilt $(x, x) \in R$.
- (2) **Symmetrisch:** d.h. $\forall x, y \in A$ gilt, wenn $(x, y) \in R$ dann auch $(y, x) \in R$.
- (3) **Transitiv:** d.h. $\forall x, y, z \in A$ gilt, wenn $(x, y) \in R$ und $(y, z) \in R$, dann auch $(x, z) \in R$.

Bsp.

a) „... lebt im gleichen Haushalt...“ ist auf der Menge aller Personen (einer Stadt) eine Äquivalenzrelation.

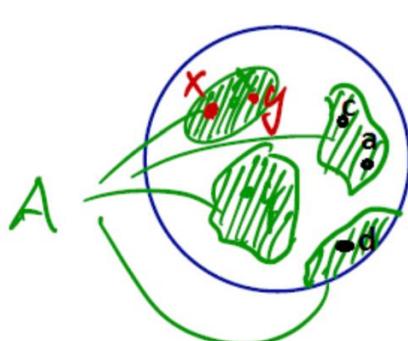
(1) **Reflexiv:** d.h. $\forall x \in A$ gilt $(x, x) \in R$, d.h. **--> x lebt im gleichen Haushalt wie x, also ist es reflexiv**

(2) **Symmetrisch:** d.h. $\forall x, y \in A$ gilt, wenn $(x, y) \in R$ dann auch $(y, x) \in R$, d.h. **--> wenn x im gleichen Haushalt wie y lebt, dann lebt y auch im gleichen Haushalt wie x, also ist es reflexiv**

(3) **Transitiv:** d.h. $\forall x, y, z \in A$ gilt, wenn $(x, y) \in R$ und $(y, z) \in R$, dann auch $(x, z) \in R$, d.h. **--> x lebt im gleichen Haushalt wie y und y lebt im gleichen Haushalt wie z, dann lebt x im gleichen Haushalt wie z, also ist es transitiv**

Bsp.

Wir wollen verifizieren, dass es sich bei R um eine Äquivalenzrelation handelt.



Die Menge A ist die Menge aller Landpunkte eines virtuellen Planeten.
Auf der Produktmenge $A \times A = \{(x, y) | x \in A, y \in A\}$ definieren wir die Relation R wie folgt:
 $R = \{(x, y) \in A \times A | y \text{ ist trock. Fuss. v. } x \text{ zu erreich.}\}$
Also: „y ist trockenen Fusses von x zu erreichen“
Oder: „von x aus ist y trockenen Fusses zu erreichen“
Oder: ... siehe unten

Also bezogen auf die Punkte der Skizze gilt:

- $(x, y) \in R$
- $(a, b) \in R$
- $(x, a) \notin R, (x, b) \notin R, (y, a) \notin R, (y, b) \notin R, (x, d) \notin R, (y, d) \notin R$ usw.

Restklassen (mod n)

Alle Zahlen in einer Restklasse haben denselben Rest bei mod n (n = Restklasse, bsp. 0 oder 1)

Die Äquivalenzklassen sind die folgenden Mengen, sie heißen Restklassen mod 5;

$[0] = \bar{0} = \{\dots, -10, -5, 0, 5, 10, 15, \dots\}$, also alle ganzzahligen Zahlen mit mod 5 = 0

$[1] = \bar{1} = \{\dots, -9, -4, 1, 6, 11, 16, \dots\}$, also alle ganzzahligen Zahlen mit mod 5 = 1

$[2] = \bar{2} = \{\dots, -8, -3, 2, 7, 12, 17, \dots\}$, also alle ganzzahligen Zahlen mit mod 5 = 2

$[3] = \bar{3} = \{\dots, -7, -2, 3, 8, 13, 18, \dots\}$, also alle ganzzahligen Zahlen mit mod 5 = 3

$[4] = \bar{4} = \{\dots, -6, -1, 4, 9, 14, 19, \dots\}$, also alle ganzzahligen Zahlen mit mod 5 = 4

Und offensichtlich gilt:



- $[i] \cap [j] = \emptyset$ für $i \neq j$, d.h. keine ganze Zahl kann in zwei Klassen sein, d.h. die Klassen sind paarweise disjunkt.

- $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$, d.h. es gibt keine ganze Zahl, die nicht in einer der Klassen drin ist.

- $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \{0, 1, 2, 3, 4\}$. D.h. zur Vereinfachung schreiben wir in Zukunft für die Klasse einfach den Hauptvertreter dieser Klasse, also anstatt $[0]$ oder $\bar{0}$ nur 0. Das ist eine Vereinfachung der Schreibweise. Wir dürfen aber nicht vergessen, dass wir in diesem Zusammenhang eigentlich nicht nur die 0 (also den Hauptvertreter) sondern die ganze Äquivalenzklasse $\{\dots, -10, -5, 0, 5, 10, 15, \dots\}$ meinen.

Verallgemeinerung auf n:

Satz: A. Die Kongruenz mod n ist für $n \geq 2$ eine Äquivalenzrelation auf der Menge \mathbb{Z} .

B. Die Äquivalenzklassen (hier Restklassen mod n) sind:

$$[r] = \{x \in \mathbb{Z} \mid x \equiv r \pmod{n}\}$$

C. In jeder Restklasse gibt es genau einen der Reste $\mathbb{Z}_n = \{0, 1, \dots, (n-1)\}$, die bei der Division durch n auftreten können.

Modulare Rechenoperationen

Addition und Multiplikation mod n (\oplus_n , \odot_n)

Sei $n \geq 2$. Wir führen auf der Menge $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ eine Addition \oplus_n und eine Multiplikation \odot_n ein. Für $a, b \in \mathbb{Z}_n$ sei:

$$a \oplus_n b = a + b \pmod{n} = R_n(a + b)$$

$$a \odot_n b = a \cdot b \pmod{n} = R_n(a \cdot b)$$

- \oplus_n ist die Addition mod n
- \odot_n ist die Multiplikation mod n
- Egal welche Berechnungen mod n wir auch ausführen, das Resultat ist immer ein Element von $\mathbb{Z}_n = \{0, 1, \dots, (n-1)\}$

Example (\mathbb{Z}_3)

\oplus_3	0	1	2		\odot_3	0	1	2	
0	0	1	2		0	0	0	0	
1	1	2	0		1	0	1	2	
2	2	0	1		2	0	2	1	

Example (\mathbb{Z}_4)

\oplus_4	0	1	2	3		\odot_4	0	1	2	3	
0	0	1	2	3		0	0	0	0	0	
1	1	2	3	0		1	0	1	2	3	
2	2	3	0	1		2	0	2	0	2	
3	3	0	1	2		3	0	3	2	1	

Beispiel 9.5:

Es sei $n = 6$ und $\mathbb{Z}_6 = \{0, 1, \dots, 5\}$

i. $3 \oplus_6 4 = R_6(3 + 4) = R_6(7) = 1$

ii. $3 \ominus_6 4 = 3 \oplus_6 (-4) = R_6(3 - 4) = R_6(-1) = 5$ Betrachtung der Subtraktion mod 6

iii. $3 \odot_6 4 = R_6(3 \cdot 4) = R_6(12) = 0$

Ist für uns noch ungewöhnlich, dass ein Produkt Null sein kann, ohne dass ein Faktor Null ist.

Bsp.

$$(1) ((5 \oplus_8 7) \odot_6 (2 \oplus_7 10)) = 4 \odot_6 5 = 2$$

5 + 7 \text{ mod } 8 *2 + 10 \text{ mod } 7*

alternativ *$2 \odot_7 3 = 5$*

$$(2) (7 \oplus_6 2) \odot_5 (12 \oplus_9 8) = 3 \odot_5 2 = 1$$

$10 \text{ mod } 7 = 3$

Man darf zu immer mit mod N vereinfachen, also, z.B.

$$(7 \oplus_6 2) \odot_5 (12 \oplus_9 8) = (1 \oplus_6 2) \odot_5 (3 \oplus_9 8) = 3 \odot_5 2 = 1$$

Aufgabe 9.2: Berechnen Sie indem Sie jeweils zuerst die Klammer(n) ausrechnen.

- i. $\underbrace{3 \odot_5 (2 \oplus_5 4)}_{= 3 \odot_5 1} = 3 \odot_5 1 = 3$
- ii. $\underbrace{(3 \odot_5 2) \oplus_5 (3 \odot_5 4)}_{= 1 \oplus_5 2} = 1 \oplus_5 2 = 3$
- iii. $\underbrace{3 \odot_7 (2 \oplus_7 4)}_{= 3 \odot_7 (6 \text{ mod } 7)} = 3 \odot_7 6 = 18 \text{ mod } 7 = 4$
- iv. $\underbrace{(3 \odot_7 2) \oplus_7 (3 \odot_7 4)}_{= 6 \oplus_7 5} = 6 \oplus_7 5 = 4$
- v. $(3 \oplus_5 2) \odot_5 (3 \oplus_5 4) = 0 \odot_5 2 = 0 \quad 0 \odot_5 (2) = 0 \cdot 2 \text{ mod } 3 = 0$
- vi. $(3 \oplus_7 2) \odot_7 (3 \oplus_7 4) = 5 \odot_7 0 = 0 \quad (5) \odot_7 (0) = 5 \cdot 0 \text{ mod } 7 = 0$

Die linken Seiten von i. & ii. resp. iii. & iv. sind jeweils identisch, sie sind nur mit einem DG umgeformt.

Square and Multiply (SAM-Algorithmus)

Ziel: Die Berechnung von $5^m \bmod 11$ mittels dem SAM-Algorithmus.

Schritte:

- Exponent m binär darstellen. Da Binär
- Erstes 1 „weglassen“, d.h. mit dem ersten 1 der binären Darstellung muss man nichts machen.
- Danach wird bei
 - „0“ quadriert.
 - „1“ wird zuerst quadriert dann mit dem Ausgangswert multipliziert.

Wir wollen nun konkret $5^{22} \bmod 11$ berechnen.

$$(22)_{10} = 16 + 4 + 2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 \\ = (10110)_2 = \text{D.h. Q, QM, QM, Q}$$

Step	Bit	Diese Spalte dient zur Verdeutlichung, sie kann auch weglassen werden!	Reduktion mod 11
0	1	$(5^1)_2 = 5_2 = 5$ Binär	5
1	0	$(5^2)_2 = 5^4 = 5$ (100)	$\equiv 25 \bmod 11 = 3$
2a)	1	$(5^2)_2 = 5^4 = 5$ (101)	$\equiv 3^2 \bmod 11 = 9$
2b)		$5^4 \cdot 5 = 5^6 = 5$ (1010)	$\equiv 9 \cdot 5 \bmod 11 = 1$
3a)	1	$(5^5)_2 = 5^{10} = 5$ (10101)	$\equiv 1^2 \bmod 11 = 1$
3b)		$5^{10} \cdot 5 = 5^4 = 5$ (101011)	$\equiv 1 \cdot 5 \bmod 11 = 5$
4)	0	$(5^{11})_2 = 5^{22} = 5$ (10110)	$\equiv 5^2 \bmod 11 = 3$

Bit	-
1	5
0	$Q \rightarrow 5^2 = 3 \bmod 11$
1	$Q \rightarrow 3^2 = 9 \bmod 11 \xrightarrow{M} 9 \cdot 3 = 1 \bmod 11$
1	$Q \rightarrow 1^2 = 1 \bmod 11 \xrightarrow{M} 1 \cdot 5 = 5 \bmod 11$
0	$\rightarrow 5^3 = 3 \bmod 11$

Bsp. #2

Ziel: Die Berechnung von $6^{27} \bmod 13$ mittels dem SAM-Algorithmus.

Schritte:

- Exponent m binär darstellen.
- Erstes 1 „weglassen“, d.h. mit dem ersten 1 der binären Darstellung muss man nichts machen.
- Danach wird bei
 - „0“ quadriert.
 - „1“ wird zuerst quadriert dann mit dem Ausgangswert multipliziert.

$$(27)_{10} = 16 + 8 + 2 + 1 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = (11011)_2$$

D.h. ~~QM~~ QM QM QM QM

nicht so wichtig Wichtig!

Step	Bit	Diese Spalte dient zur Verdeutlichung, sie kann auch weglassen werden!	Reduktion mod 13
0	1	$6 = 6^1$	6
1a)	1	$(6^1)^2 = 6^2 = 6^{(10)_2}$	$\equiv 36 \bmod 13 = 10$
1b)		$6^2 \cdot 6 = 6^3 = 6^{(11)_2}$	$\equiv 10 \cdot 6 \bmod 13 = 8$
2	0	$(6^3)^2 = 6^6 = 6^{(110)_2}$	$\equiv 8^2 \bmod 13 = 12$
3a)	1	$(6^6)^2 = 6^{12} = 6^{(1100)_2}$	$\equiv 12^2 \bmod 13 = 1$
3b)		$6^{12} \cdot 6 = 6^{13} = 6^{(1101)_2}$	$\equiv 1 \cdot 6 \bmod 13 = 6$
4a)	1	$(6^{13})^2 = 6^{26} = 6^{(11010)_2}$	$\equiv 6^2 \bmod 13 = 10$
4b)		$6^{26} \cdot 6 = 6^{27} = 6^{(11011)_2}$	$\equiv 10 \cdot 6 \bmod 13 = 8$

Nullteiler

Im Rechnen in den reellen Zahlen \mathbb{R} wissen wir, dass die folgende Regel gilt:

$$a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$$

Das Erfüllen dieser Eigenschaft heisst „**Nullteilerfreiheit**“. Also die reellen Zahlen sind nullteilerfrei.

Wenn die Eigenschaft **nullteilerfrei** nicht erfüllt ist, nennt man die Zahlen nicht nullteilerfrei. D.h.

$$\exists a, b \text{ mit } a \neq 0, b \neq 0 \text{ und } a \cdot b = 0$$

In diesem Falle heissen die Zahlen a, b Nullteiler

Bsp. Nicht nullteilerfrei

Nun betrachten wir die Zahlen $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ und deren Multiplikationstabelle (siehe Kap. 9.4.1). Wir sehen, dass diese Zahlen **nicht** nullteilerfrei sind. Denn es gibt Zahlen a, b deren Produkt gleich Null ist, obwohl beide Zahlen ungleich Null sind: $2 \odot_4 2 = 0$

Also: die Zahl 2 ist ein Nullteiler in \mathbb{Z}_4 .

Aufgabe 9.4:

Betrachten Sie nun \mathbb{Z}_5 und \mathbb{Z}_6 . Bestimmen Sie, ob diese Zahlen nullteilerfrei sind oder nicht. Wenn sie nicht nullteilerfrei sind, geben Sie die Nullteiler an.

Anbei die zwei Multiplikationstabellen.

\odot_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

\odot_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

Definition Nullteiler

Existiert zu einem $a \in \mathbb{Z}_n$ mit $a \neq 0$ ein $b \in \mathbb{Z}_n$ mit $b \neq 0$ so dass $a \odot_n b = 0$ gilt, so heisst a ein Nullteiler von \mathbb{Z}_n .

Konsequenz:

Wenn eine Zahlenmenge \mathbb{Z}_n nicht nullteilerfrei ist, also Nullteiler hat, dann folgt, dass nicht jede Gleichung $a \odot_n x = b$ eine Lösung für x hat.

Bsp.

Welche Zahlen in \mathbb{Z}_5 und \mathbb{Z}_6 haben kein multiplikatives Inverses?

Lösung:

\mathbb{Z}_5 ist nullteilerfrei.

\mathbb{Z}_6 ist nicht nullteilerfrei. Die Zahlen 2, 3 und 4 sind Nullteiler, denn

$$2 \odot_6 3 = 0.$$

$$3 \odot_6 4 = 0.$$

$$\text{Aber } 2 \odot_6 4 = 2.$$

In \mathbb{Z}_5 haben alle Zahlen ausser die Null ein multiplikatives Inverses.

In \mathbb{Z}_6 haben neben der Null die drei Nullteiler, 2, 3 und 4 kein multiplikatives Inverses.

Inverse Elemente

Sei n eine natürliche Zahl und $a \in \mathbb{Z}_n$. a hat genau dann ein Inverses bezüglich der Multiplikation \odot_n in \mathbb{Z}_n , wenn $\text{ggT}(a, n) = 1$ gilt.

Die Menge aller invertierbaren Elementen in \mathbb{Z}_n sei mit \mathbb{Z}_n^* bezeichnet. Es gilt also:

$$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1 \}.$$

Somit liefert Euler'sche ϕ -Funktion von n wegen $\phi(n) = |\mathbb{Z}_n^*|$ gerade die Anzahl invertierbarer Elemente kleiner als n .

Online-Rechner: <https://www.wolframalpha.com/widgets/view.jsp?id=1694d213f1a463560a0a1b142de02296>

Bsp. – Inverse Elemente → alle Multiplikationstabellen Werte = 1

Betrachten wir die Multiplikationstabellen von \mathbb{Z}_5 und \mathbb{Z}_6 , dann können wir sehr schnell die Inversen Elemente bestimmen.

In \mathbb{Z}_5 gilt: $1^{-1} = 1; 2^{-1} = 3; 3^{-1} = 2; 4^{-1} = 4$

In \mathbb{Z}_6 wissen wir nun, dass nur die Elemente in $\mathbb{Z}_6^* = \{1; 5\}$ ein multiplikatives Inverses haben:
 $1^{-1} = 1; 5^{-1} = 5$

Bsp. #2

Bestimmen Sie in \mathbb{Z}_9 die multiplikativen Inversen. Bestimmen Sie zudem $|\mathbb{Z}_9^*|$ mit der Eulerschen ϕ -Funktion.

$$\mathbb{Z}_9^* = \{1; 2; 4; 5; 7; 8\}, 1^{-1} = 1; 2^{-1} = 5; 4^{-1} = 7; 5^{-1} = 2; 7^{-1} = 4; 8^{-1} = 8$$

Allgemein:

$$\phi(p^r) = (p - 1) \cdot (p^{r-1})$$

$$|\mathbb{Z}_9^*| = \phi(9) = \phi(3^2) = (3 - 1) \cdot (3^{2-1}) = 2 \cdot 3 = 6$$

Aufgabe 9.6:

$$3^{-1} \equiv 3^{13-2} \equiv 3^{11} \equiv 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^2 \equiv 1 \cdot 1 \cdot 1 \cdot 3^2 = 9 \text{ mod } 13$$

Inverse berechnen mit dem kleinen Fermat (Nur wenn n = Primzahl!)

Sei p eine Primzahl! In diesem Fall kann der **kleine Satz von Fermat** genutzt werden, um die Inversen systematisch zu bestimmen. Sei $a \in \mathbb{Z}_p^*$. Dann gilt

$$a^{p-1} = a \cdot a^{p-2} = 1 \text{ mod } p$$

und somit

$$a \odot_p R_p(a^{p-2}) = 1$$

d.h. $a^{-1} = R_p(a^{p-2}) = a^{p-2} \text{ mod } p$ ist das Inverse zu a .

$$\begin{aligned} &\downarrow a^p \equiv a \text{ mod } p \\ \Rightarrow &a^{p-1} \equiv a^0 \equiv 1 \text{ mod } p \\ \Rightarrow &a^{p-2} \equiv a^{-1} \text{ mod } p \\ \star &a \cdot a^{-1} = a^0 \end{aligned}$$

Beispiel 9.11:

Wir berechnen die multikativen Inversen in $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ mit dem kleinen Satz von Fermat:

- $1^1 \equiv 1^{5-2} \equiv 1^3 \equiv 1 \text{ mod } 5$
- $2^{-1} \equiv 2^{5-2} \equiv 2^3 \equiv 8 \equiv 3 \text{ mod } 5$
- $3^{-1} \equiv 3^{5-2} \equiv 3^3 \equiv 27 \equiv 2 \text{ mod } 5$
- $4^{-1} \equiv 4^{5-2} \equiv 4^3 \equiv 64 \equiv 4 \text{ mod } 5$

Bemerkung:

Die multikativen Inversen in $\mathbb{Z}_6^* = \{1, 5\}$ können wir **nicht** mit dem kleinen Satz von Fermat berechnen, denn $n = 6$ ist keine Primzahl.

Wichtig:

Die Berechnung von Inversen Elementen mit dem kleinen Satz von Fermat kann nur für $\mathbb{Z}_p^* = \{1, 2, \dots, (p - 1)\}$ gemacht werden!

Primitive Elemente

Sei p eine Primzahl. Ein Element $z \in \mathbb{Z}_p^*$ heisst **primitives Element**, von \mathbb{Z}_p^* , falls jedes Element $a \in \mathbb{Z}_p^*$ eine Potenz von z ist.

- 1) Anstatt „primitives Element“ wird auch der Begriff „erzeugendes Element“ verwendet.
- 2) In \mathbb{Z}_p^* gibt es $\phi(\phi(p))$ primitive Elemente (ohne Beweis).

Beispiel 9.13:

Wir suchen in $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ die primitiven Elemente. Gemäss Bemerkung 2) oben gibt es

$$\phi\left(\underbrace{\phi(5)}_{=4}\right) = \phi(4) = \phi(2^2) = (2 - 1) \cdot 2^{2-1} = 1 \cdot 2^1 = 2 \text{ primitive Elemente.}$$

$z = 1$: $z = 1$ kann nie primitiv sein, dann $1^i \equiv 1 \pmod{n}$

$z = 2$: $2^1 \equiv 2 \pmod{5}$; $2^2 \equiv 4 \pmod{5}$; $2^3 \equiv 3 \pmod{5}$; $2^4 \equiv 1 \pmod{5}$ und somit ist $z = 2$ primitiv.

$z = 3$: $3^1 \equiv 3 \pmod{5}$; $3^2 \equiv 4 \pmod{5}$; $3^3 \equiv 2 \pmod{5}$; $3^4 \equiv 1 \pmod{5}$ und somit ist $z = 3$ primitiv.

$z = 4$: $4^1 \equiv 4 \pmod{5}$; $4^2 \equiv 1 \pmod{5}$; $4^3 \equiv 4 \pmod{5}$; $4^4 \equiv 1 \pmod{5}$ und somit ist $z = 4$ nicht primitiv,
denn 2 und 3 können nicht in der Form $4^i \pmod{5}$ dargestellt werden.

alle 4 Zahlen können als 2er Potenzen geschrieben werden

Zahl 2x3 kann ich nur als 4er Pot schreiben.

Die erwartete Anzahl von 2 primitiven Elementen haben wir also erhalten.

Beispiel 9.14:

Wir bestimmen die primitiven Elemente in \mathbb{Z}_{11}^* anhand der vorberechneten Tabelle

Tabelle der Potenzen aller Elemente in \mathbb{Z}_{11}^*

Elemente	1	2	3	4	5	6	7	8	9	10	Potenzen
11											
1	1	1	1	1	1	1	1	1	1	1	← Ordnung 1
2	2	4	8	5	10	9	7	3	6	1	○ 2x5 → Primitive Elern = Ordnung 10
3	3	9	5	4	1	3	9	5	4	1	○ 3x3 → Ord 9
4	4	5	9	3	1	4	5	9	3	1	○ 4x2 → Ord 8
5	5	3	4	9	1	5	3	4	9	1	○ 5x5 → Ord 5
6	6	3	7	9	10	5	8	4	2	1	○ 6x1 → Ord 1
7	7	5	2	3	10	4	6	9	8	1	○ 7x7 → Ord 7
8	8	9	6	4	10	3	2	5	7	1	○ 8x4 → Ord 4
9	9	4	3	5	1	9	4	3	5	1	○ 9x3 → Ord 3
10	10	1	10	1	10	1	10	1	10	1	○ 10x2 → Ord 2

Aufgrund der Tabelle ist nun ersichtlich, dass {2; 6; 7; 8} primitive Elemente sind.

Wir erwarten $\phi(\phi(11)) = \phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(5) = 1 \cdot 4 = 4$ primitive Elemente, die wir auch erhalten haben.

(10 Elemente)

Primitive Elemente = wenn in der Reihe keine 1 ausser in der letzten Spalte vorkommt.

Einwegfunktionen

Definition

Eine **Einwegfunktion** ist eine Abbildung f einer Menge X in eine Menge Y , so dass $f(x)$ für jedes Element in X leicht berechnet werden kann, während es für jedes y aus Y extrem schwer ist, ein Urbild x zu finden. Ist eine Einwegfunktion bijektiv, nennen wir sie

Einwegpermutation. Eine Einwegfunktion heisst **kollisionsfrei**, falls es praktisch unmöglich ist, zwei verschiedenen $x, x' \in X$ mit $f(x) = f(x')$ zu finden.

Einige Einwegfunktionen (nach heutigem Wissenstand). Die Zahlen p und q seien dabei stets verschiedene Primzahlen.

- Quadrieren modulo $n = pq$:** $x \mapsto y \equiv x^2 \pmod{n}$. Die Umkehrung $x \equiv \sqrt{y} \equiv \sqrt{x^2} \pmod{n}$ ist sehr schwierig für grosse Zahlen (d.h. n ca. eine 400-stellige Zahl, resp. p & q je eine 200-stellige Zahl). Damit man noch „lange“ sicher ist, nimmt man heute für n eine mind. 700-stellige Zahl, genauer, $n = 2048$ Bit (*).
- Potenziieren modulo $n = pq$:** $x \mapsto y \equiv x^e \pmod{n}$. Die Umkehrung $x \equiv \sqrt[e]{y} \equiv \sqrt[e]{x^e} \pmod{n}$ ist sehr schwierig für grosse Zahlen (d.h. n ca. eine 400-stellige Zahl, resp. p & q je eine 200-stellige Zahl). Dies obwohl die Werte $y \equiv x^e \pmod{n}$ sowie e und n bekannt sind. Damit man noch „lange“ sicher ist, nimmt man z.Z. für n eine mind. 700-stellige Zahl, also 2048 Bit (*).
- Diskrete Exponentialfunktion mod p :** $x \mapsto y \equiv g^x \pmod{p}$. Die Umkehrung $x = \log_g y \pmod{p}$ ist sehr schwierig für grosse Zahlen (d.h. p ca. eine 400-stellige Zahl). Dies obwohl, die Werte $y = g^x \pmod{p}$ sowie g und p bekannt sind. Damit man noch „lange“ sicher ist, nimmt man heute für p eine mindestens 700-stellige Zahl, also p 2048 Bit (*).

Modulare Quadratwurzel

Modulare Quadratwurzeln a. (und modulare Logarithmen c. – auch diskreter Logarithmus genannt) sind im oben definierten Sinne der Einwegfunktionen von besonderem Interesse in der Kryptographie. Das modulare Potenzieren b. ist von einem ganz anderen Typus von Einwegfunktionen, mit einem bestimmten Wissen (= geheimer Schlüssel) kann man die Funktion umkehren. Die Funktion ist als Funktion ebenfalls eine Einwegfunktion, aber es gibt – wegen dem geheimen Wissen – einen anderen Weg um die Umkehrung zu berechnen. Aus diesen Gründen werden im Folgenden „nur“ die modulare Quadratwurzel und der diskrete Logarithmus besprochen.

Definition *alle Elemente, die Teiler fremd zu n sind*

Sei $a \in \mathbb{Z}_n^*, n \geq 2$. Eine Lösung $x \in \mathbb{Z}_n^*$ (falls sie existiert) der Gleichung

$$x^2 \equiv a \pmod{n} \text{ bzw. } x \odot_n x = a$$

heisst **modulare Quadratwurzel von a modulo n** oder **quadratischer Rest (QR) modulo n** . Andernfalls heisst a **quadratischer Nichtrest (NR)**.

Bezeichnung: $x = \sqrt{a} \pmod{n}$

quadratischer Rest (QR), quadratischer Nichtrest (NR)

Bsp. QR und NR bestimmen

$n = 7$ und $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

(modulare) Wurzel - (ziehen.)

x	1	2	3	4	5	6
$x^2 = x \odot_7 x$	1	4	2	2	4	1

$1^2 \pmod{7} = 1$
 $2^2 \pmod{7} = 4$
 $3^2 \pmod{7} = 2$
 $4^2 \pmod{7} = 2$
 $5^2 \pmod{7} = 4$
 $6^2 \pmod{7} = 1$

a

1	2	3	4	5	6
$\sqrt{a} \pmod{7}$	1, 6	3, 4	-	2, 5	-

$x^2 \pmod{7} = a$

Es gibt in \mathbb{Z}_7^* Elemente

- ohne (3, 5 und 6) und
- mit genau zwei (1, 2 und 4)

Quadratwurzeln. Ungewöhnlich!?

Es gibt keine Zahl in \mathbb{Z}_7^* die quadriert 3 ergibt.

D.h. Die Elemente {1, 2, 4} sind quadratische Reste (QR) mod 7, die Elemente {3, 5, 6} sind quadratische Nicht-Reste (NR) mod 7.

Bsp. #2a) Geben Sie die Elemente von \mathbb{Z}_{14}^* an und füllen Sie die untenstehenden Tabellen aus.

b) Welche Elemente sind Quadratische Reste mod 14, welche sind Quadratische Nicht-Reste mod 14?

c) Geben Sie $|\mathbb{Z}_{14}^*|$ durch Zählen der Elemente und Berechnen mit der Eulerschen φ -Funktion an.Lösung:

$\mathbb{Z}_{14} = 2 \cdot 7 \Rightarrow$ Alle Zahlen die Teilerfremd von 2 und 7 sind

$x \in \mathbb{Z}_{14}^*$	1	3	5	9	11	13	...
$x^2 = x \odot_{14} x$	1	9	11	11	9	1	...

* Was im Quadrat mod 14 gibt $\rightarrow 3, 11 \Rightarrow 3, 11$

$a \in \mathbb{Z}_{14}^*$	1	3	5	9	11	13	...
$\sqrt{a} \text{ mod } 14$	1, 13	-	-	3, 11	5, 9	-	...

Anwendung: $\text{für } -1 + 14 = 13 \quad 5 \cdot 3 + 14 = 1$

Da 14 keine Primzahl nicht 1-3
* weil $S^2 = 11 \text{ mod } 14$
sodass $2^5 \text{ mod } 14 = 11$

Euler Kriterium

Euler-Kriterium: Sei p eine Primzahl, dann ist $a \in \mathbb{Z}_p^*$ genau dann einA. Quadratischer Rest (QR) mod p , wenn $a^{\frac{p-1}{2}} \equiv 1 \text{ mod } p$ B. Quadratischer Nichtrest (NR) mod p , wenn $a^{\frac{p-1}{2}} \equiv -1 \text{ mod } p = (p-1) \text{ mod } p$ **Beispiel 10.2, Fortsetzung:**Aus $p = 7$ folgt $(p-1)/2 = 3$. Also ist für $a = 1; 2; 4 \quad a^3 \equiv 1 \text{ mod } 7$ & für $a = 3; 5; 6 \quad a^3 \equiv -1 \equiv 6 \text{ mod } 7$ zu testen.Für $a = 1: 1^3 \equiv 1 \text{ mod } 7$; Für $a = 2: 2^3 \equiv 8 \equiv 1 \text{ mod } 7$; Für $a = 4: 4^3 \equiv 64 \equiv 1 \text{ mod } 7$ Für $a = 3: 3^3 \equiv 27 \equiv 6 \text{ mod } 7$;Für $a = 5: 5^3 \equiv 5^2 \cdot 5 \equiv 4 \cdot 5 \equiv 6 \text{ mod } 7$; Für $a = 6: 6^3 \equiv 6^2 \cdot 6 \equiv 1 \cdot 6 \equiv 6 \text{ mod } 7$

Schulbuchversion der Diffie-Hellman Schlüsselverteilung

Übersicht und Definitionen

Symmetrische Verschlüsselung

Asymmetrische Verschlüsselung

Auf dem Rechner bei Menü Punkt 5 (Wsk) und Verteilungen, Zufallszahlen schauen welche Formel bereits integriert sind.