Diskrete Mathematik 2

Jan Fässler

2. Semester (FS 2012)

If you use this documentation for a exam, you should offer a beer to the authors!

Inhaltsverzeichnis

1 Quantifizierung

1.1 Einleitung

Die bekannten mathematischen Quantifizierungen haben den Nachteil, dass sie nicht immer 100% genau sind. Deshalb definieren wir eine neue, genauere Schreibweise:

$$\sum_{i=1}^{n} i^2 = (+i : \mathbb{Z} | 1 \leq i \leq n : i^2)$$

1.2 Definition

$(\oplus v_1 : T_1, ..., v_n : T_n | R : P)$

- Anwendung von $\oplus$ auf die Werte von P für alle Kombinationen von Werten für $v_1, ..., v_n$ für die R wahr ist.
- Ist R für keine Kombination wahr, dann die Identität u von $\oplus$
- Datentyp der gesamten Quantifizierung: T

$\oplus$ - binärer Operator

- Typ: $T \times T \to T$
- Eigenschaften:
  - $a \oplus b = b \oplus a$ (kommutativ)
  - $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ (assoziativ)
  - $a \oplus u = a$

$T_1, ..., T_n$ - Datentypen

$v_1, ..., v_n$ - gebundene Variabeln

- Englisch: bound variables, dummies
- $n \geq 1$
- alle paarweise verschieden
- v_i hat den Typ T_i

R - boolescher Ausdruck

- ist der Bereich (Range)
- kann $v_1, ..., v_n$ enthalten

P - beliebiger Ausdruck von Typ T

- ist der Körper (Body)
- kann $v_1, ..., v_n$ enthalten
-

Quantor	Operator	Idendität	Typ
$\sum$	$+$	0	$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$\prod$	$*$	1	$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$\forall$	$\wedge$	$true$	$\mathbb{B} \times \mathbb{B} \to \mathbb{B}$
$\exists$	$\vee$	$false$	$\mathbb{B} \times \mathbb{B} \to \mathbb{B}$

1.3 Beispiele

- $(+i|0 \leq i < 4 : i * 8) = 0 * 8 + 1 * 8 + 2 * 8$
- $(*i|0 \leq i < 3 : i + (i + 1)) = (0 + 0 + 1) * (1 + 1 + 1) * (2 + 2 + 1)$
- $(\wedge i|0 \leq i < 2 : i * d \neq 6) = 0 * d \neq 6 \wedge 1 * d \neq 6 = d \neq 6$
- $(\vee i| \leq i < 21 : b[i] = 0) = b[0] = 0 \vee b[1] = 0 \vee ... \vee b[20] = 0$
- $(+k : \mathbb{N}|k^2 = 4 : k^2) = 2^2$
- $(+k : \mathbb{Z}|k^2 = 4 : k) = 2^2 + (-2)^2$

1.4 Variabeln

1.4.1 Definition

Def. Eine Variable v heisst frei in einem Ausdruck E, falls v in E frei auftritt.
FV(E) = Menge der freien Variablen in E

Bem. Werte der freien Variablen stehen nicht im Ausdruck selbst, diese Info muss aus anderer Quelle kommen. (Background Info)

Def. Ein Ausdruck E ohne freie Variable heisst geschlossen.

Bem. Die erste gebundene Variabel nennt man bindend und alle volgenden angewandt.

1.4.2 Beispiele

$$E_1 : (\sum \underbrace{i : \mathbb{Z}}_{gebunden})|0 \leq \underbrace{i}_{gebunden} < \overbrace{n}^{frei} : \underbrace{i^2}_{gebunden})$$

$$E_2 : \overbrace{(\sum \underbrace{i : \mathbb{Z}}_{gebunden}|0 \leq \underbrace{i}_{gebunden} < \overbrace{n}^{n\ muss\ gleich\ sein\ (frei)} : \underbrace{i^2 + i}_{gebunden}) + (\sum \underbrace{i : \mathbb{Z}}_{gebunden}|0 \leq \underbrace{i}_{gebunden} < \overbrace{n}^{n\ muss\ gleich\ sein\ (frei)} : \underbrace{i^3}_{gebunden})}$$

$$E_3 : (\pi \overbrace{\overbrace{u}^{gebunden}|\underbrace{k}_{frei} \leq \overbrace{u}^{gebunden} \leq \underbrace{b}_{frei} : (\sum \underbrace{\underbrace{i}_{gebunden}|0 \leq \underbrace{i}_{gebunden} \leq \overbrace{u}^{gebunden} : \underbrace{i^2 + i}_{gebunden}) * (\sum \underbrace{\underbrace{i}_{gebunden}|0 \leq \underbrace{i}_{gebunden} < \overbrace{u}^{gebunden} : \underbrace{i^3}_{gebunden}))}^{gebunden}$$

1.4.3 Umbenennung (dummy renaming)

Bed. $w \notin FV(R) \cup FV(P)$ (w darf nicht als FV im Ausdruck vorkommen)

Regel: $(\oplus v|R : P) = (\oplus w|R[v \leftarrow w] : P[v \leftarrow w])$

Def. $E[v \leftarrow F]$ bezeichnet den selben Ausdruck wie E, aber alle freien Aufteten von v ersetzt durch (F).

Bsp. $(i^2)[i \leftarrow (z + 3)] = (z + 3)^2$

Bsp. $(\sum i|0 \nleq i < n : i^2) = (\sum j|(0 \nleq i < n)[i \leftarrow j] : (i^2)[i \leftarrow j] = (\sum j|0 \nleq j \nleq n : j^2)$

1.5 Rechenregeln

Empty-Range

Bei einer leeren Range, ist das Resultat die Indendität:
$(\oplus v|false : P) = neutral\oplus$ (identität)

One-Point

Eine gebundene Variabel wird durch eine freie ersetzt:
$(\oplus v|v = E : P) = P[v \leftarrow E]$ wenn: $v \notin FV(E)$

Bsp $(\sum i|i = j + 3 : i^2) = (i^2)[i \leftarrow (i + 3)] = (j + 3)^2$

Split-Off Term

Die Range wird gekürzt. Weggenommenes Element anschliessend angefügt:
$(\oplus i|0 \leq i < n + 1 : P) = (\oplus i|0 \leq i < n : P) \oplus P[i \leftarrow n]$

Bsp: $\underbrace{(\sum i|0 \leq i < n + 1 : i^2)}_{0^2+1^2+...+(n-1)^2+n^2} = \underbrace{(\sum i|0 \leq i < n : i^2)}_{0^2+1^2+...+(n-1)^2} + \underbrace{(i^2)[i \leftarrow n]}_{n^2}$

Trading

Bei mehreren Bedingungen in der Range, kann eine in den Body genommen werden:
$(\oplus|\underbrace{R_1 \wedge R_2}_{Bool} : \underbrace{P}_{irgendeinDatentyp}) = (\oplus v|R_1 : \text{if } R_2 \text{ then P else } v_\oplus \text{ endif})$

Bsp: $\underbrace{(\sum i|0 \leq i < 10 \wedge odd(i) : i)}_{1+3+5+7+9} = \underbrace{(\sum i|0 \leq i < 10 : if\ odd(i)\ then\ i\ else\ 0\ endfi)}_{0+1+0+3+0+5+0+7+0+9}$

1.6 Prädikate

1.6.1 Definition

- $\oplus = \forall(\forall x|R : P) \Longrightarrow$ für alle x im Bereich R gilt P
- $\oplus = \exists(\exists x|R : P) \Longrightarrow$ es gibt ein x im Bereich R, das P erfüllt

1.6.2 Beispiele

- $\oplus = \forall(\forall x|R_1 \wedge R_2 : P) = (\forall u|R_1 : \text{if } R_2 \text{ then P else true endif }) = (\forall u|R_1 : R_2 \rightarrow P)$

R_2	P	if	$\rightarrow$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Sei $R_1 = true \Longleftrightarrow (\forall u|R_2 : P) = (\forall u|true : R_2 \rightarrow P) = (\forall u| : R_2 \rightarrow P)$

- $\oplus = \exists(\exists u|R_1 \wedge R_2 : P) = (\exists u|R_1 : \text{if } R_2 \text{ then P else false endif}) = (\exists u|R_1 : R_2 \wedge P)$

R_2	P	if	$\wedge$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

1.6.3 Übungen

b enthält eine -1: $(\exists i|0 \leq i < n : b[i] = -1)$

b enthält genau eine -1: $(\exists i|0 \leq i < n : b[i] = -1 \wedge (\forall j|0 \leq j < n \wedge j = i : b[j] \neq -1))$

b enthält keine -1: $(\forall i : \mathbb{Z}|0 \leq i < n : b[i] \neq -1)$

2 Induktion/Rekursion

2.1 Induktion

$$(P(0) \wedge (\forall n : \mathbb{N}| : P(n) \rightarrow P(n+1))) \rightarrow (\forall n : \mathbb{N}| : P(n))$$

Für alle $n : \mathbb{N}$ gilt : $n^3 + 5n$ ist Vielfaches von 6.

1.) Induktionsanfang zu zeigen: P(0), das heisst es gilt $r : \mathbb{Z}$ mit $0^3 + 5 * 0 = 6 * z$ klar, wähle z=0

2.) Induktionsschritt zu zeigen: $P(n) \rightarrow P(n+1)$ für alle $n \geq 0$. Sei n eine **beliebige** natürliche Zahl

Annahme: es gelte P(n), das heisst es gibt $r : \mathbb{Z}$ mit $n^3 + 5n = 6r$

zu Zeigen: es gibt ein $s : \mathbb{Z}$ mit $(n+1)^3 + 5(n+1) = 6s$

$(n+1)^3 + 5(n+1)$
$= < Arith >$ (arithmetische Veränderungen)
$(n^3 + 3n^2 + 3n + 1) + (5n + 5)$
$= < Arith >$
$(n^3 + 5n) + (3n^2 + 3n + 6)$
$= < Annahme >$
$6r + 3n(n+1) + 6$
$< n(n+1)$ immer durch 2 teilbar, d.h. $n(n+1) = 2t, t = \mathbb{Z} >$
$6r + 3 * 2t + 6$
$= < Arith >$
$6(r + t + 1)$
$= <$ wähle $s : \mathbb{Z} = r + t + 1 >$
$\underline{\underline{6s}}$

2.1.1 Schema

Induktionsanfang zu zeigen: P(0)

Induktionsschritt zu zeigen: $P(n) \rightarrow P(n+1)$ für alle $n : \mathbb{N}$
Sei n eine beliebige natürliche Zahl
Annahme: Es gelte P(n)
zu zeigen: Es gilt P(n+1)

2.1.2 Beispiel 1

Für alle $n : \mathbb{N}$ gilt: $(+i|1 \leq i < n : i) = \frac{n(n+1)}{2}$

1. Induktionsanfang:
zu zeigen: $< neutral+ > 0 = \frac{0(0+1)}{2} = 0$ ✓

2. Induktionsschritt:
zu zeigen: $P(n) \rightarrow P(n+1)$ für alle $n : \mathbb{N}$
Sei n eine beliebige Zahl
Annahme: es gelte $(i + |1 \leq i \leq n : i) = \frac{n(n+1)}{2}$
zu zeigen: es gilt $(i + |1 \leq i \leq n : i) = \frac{(n+1)(n+2)}{2}$

$(i + |1 \leq i \leq n+1 : i)$
$< splitof >$
$= (i + |1 \leq i \leq n : i) + n + 1$

$< Annahme >$
$= \frac{n(n+1)}{2} + n + 1$
$< Arith >$
$= \frac{n^2+n}{2} + \frac{2n+2}{2}$
$< Arith >$
$= \frac{(n+1)(n+2)}{2}$

2.1.3 Beispiel 2

Für alle $n : \mathbb{N}$ gilt: $(+i : \mathbb{N} | 1 \leq i \leq n : 2i - 1) = n^2$

1. Induktionsanfang:
zu zeigen: $\underbrace{(+i : \mathbb{N} | 1 \leq i \leq n : 2i - 1)}_{0(<neutral+>)} = \underbrace{n^2}_{=0}$

2. Induktionsschritt:
zu zeigen: $P(n) \to P(n+1)$ für alle $n : \mathbb{N}$
Sei n eine beliebige Zahl
Annahme: es gelte $(+i : \mathbb{N} | 1 \leq i \leq n : 2i - 1) = n^2$
zu zeigen: es gilt $(+i : \mathbb{N} | 1 \leq i \leq (n+1) : 2i - 1) = (n+1)^2$

$(+i : \mathbb{N} | 1 \leq i \leq (n+1) : 2i - 1)$
$< splitof >$
$= (+i : \mathbb{N} | 1 \leq i \leq n : 2i - 1 + 2(n + 1 - 1)$
$< Annahme >$
$= n^2 + 2(n+1) - 1$
$< Arith >$
$= n^2 + 2n + 1$
$< Arith >$
$= (n+1)^2)$

2.1.4 Induktion mit einem anderer Anfangswert

Sei $k : \mathbb{N}$
$\underbrace{P(k)}_{IA} \wedge \underbrace{(\forall n : \mathbb{N} | n \geq k : P(n) \Rightarrow P(n+1))}_{IS} \Rightarrow (\forall n : \mathbb{N} | n \geq k : P(n))$

Theorem
Für alle $n : \mathbb{N}$ mit $n \geq 3$ gilt: $2n + 1 < 2^n$

Beweis
IA: zu zeigen: P(3) $2 * 3 + 1 < 2^3$
IS: zu zeigen: $P(n) \Rightarrow P(n+1)$ für alle $n \geq 3$
Sei n eine beliebige nat. Zahl ≥ 3.
Annahme: Es gelte: $2n + 1 < 2^n$
zu zeigen: Es gilt: $2(n+1) + 1 < 2^{n+1}$
$2(n+1) + 1$
$= < Arith >$
$2n + 2 + 1$
$= < Arith >$
$(2n + 1) + 2$
$<< Anahme >$
$2^n + 2$
$<<$für $n + 1$ ist $2^n > 2 >$
$2^n + 2^n$
$= < Arith >$
2^{n+1}

2.2 Rekursion

$fact : \mathbb{N} \to \mathbb{N}$
$fact(0) = 1$
$\underbrace{fact(n) = n + fact(n-1)}_{Rekursion}$, für alle $n > 0$.

2.2.1 Factorial Beispiel

Für alle $n : \mathbb{N}$ gilt: fact$(n) = (*i : \mathbb{N} | 1 \leq i \leq n : i)$

1. Induktionsanfang:
fact$(0) = (*i : \mathbb{N} | 1 \leq i \leq 0 : i)$

2. Induktionsschritt:
Zeigen: $P(n) \to P(n+1)$, für alle $n \geq 0$
Sei n eine beliebige natürliche Zahl.
fact$(n) = (*i : \mathbb{N} | 1 \leq i \leq n : i)$
fact$(n) = (*i : \mathbb{N} | 1 \leq i \leq (n+1) : i)$

$(*i : \mathbb{N} | 1 \leq i \leq (n+1) : i)$
$< splitoff >$
$= (*i : \mathbb{N} | 1 \leq i \leq n : i) * (n+1)$
$< Annahme >$
=fact$(n) * (n+1)$
$< Rekursion >$
=fact$(n+1)$

2.2.2 Fibonaci Beispiel

Für alle $n : \mathbb{N}$ gilt: $(+i : \mathbb{N} | 1 \leq i \leq n : fib(i)) = fib(n+2) - 1$

1. Induktionsanfang:
$(+i : \mathbb{N} | 1 \leq i \leq 0 : fib(i)) = fib(0+2) - 1$

2. Induktionsschritt:
Zeigen: $P(n) \to P(n+1)$, für alle $n \geq 0$
Sei n eine beliebige natürliche Zahl.
$(+i : \mathbb{N} | 1 \leq i \leq n : fib(i)) = fib(n+2) - 1$
$(+i : \mathbb{N} | 1 \leq i \leq (n+1) : fib(i)) = fib(n+3) - 1$

$(+i : \mathbb{N} | 1 \leq i \leq (n+1) : fib(i))$
$< splitoff >$
$(+i : \mathbb{N} | 1 \leq i \leq n : fib(i)) + fib(n+1)$
$< Annahme >$
$fib(n+2) - 1 + fib(n+1)$
$< Rekursion >$
=fib$(n+3) - 1$

3 Zahlentheorie

3.1 Teilbarkeit

3.1.1 Definition

c\b

c teilt b
b ist teilbar durch c
c ist ein Teiler von b
b ist Vielfaches von c

Beispiel

$7 \setminus 13 \equiv false$
$(-7) \setminus 14 \equiv true$

oft $c|b$ statt $c \setminus b$

Formal $c|b \equiv (\exists k : \mathbb{Z} | b = k * c)$

Sätze

(1) $c \setminus c$ (reflexiv)
(2) $c \setminus 0$
(3) $1 \setminus b$
(4) $c \setminus 1 \Rightarrow c = 1 \vee c = -1$
(5) $d \setminus c \wedge c \setminus b \Rightarrow d \setminus b$ (transitiv)
(6) $b \setminus c \wedge c \setminus b \Rightarrow (b = c) \vee (b = -c)$ (antisymmetrie für Zahlen > 0)
(7) $b \setminus c \Rightarrow b \setminus (c * b)$
(8) $b \setminus c \Rightarrow (b * d) \setminus (c * d)$
(9) $1 < b \wedge b \setminus c \Rightarrow \neg(b \setminus (c + 1))$

Der Fall Null

- $0 \setminus 0 \equiv true$
- $0 \setminus 7 \equiv false$

3.1.2 Beweise

Beweis von Regel 5

$d \setminus c \wedge c|b \Rightarrow d \setminus b$
Annahmen: $d \setminus c, c \setminus b$
zu zeigen: $d \setminus b$
wegen $d \setminus c$ gibt es $k_1 : \mathbb{Z}$ mit $c = k_1 * d$
wegen $c \setminus b$ gibt es $k_2 : \mathbb{Z}$ mit $b = k_2 * d$
also $b = k_2 * c = k_2 * (k_1 * d) = (k_2 * k_1) * d = k_3 * d$
mit $k_3 = k_2 * k_1 : \mathbb{Z}$
also $d \setminus b$

Beweis von $a \setminus b \wedge a \setminus c \Rightarrow a \setminus (b + c)$

Annahmen: $a \setminus b, a \setminus c$
zu zeigen: $a \setminus (b + c)$
$a \setminus b$, also existiert ein $k_1 : \mathbb{Z}$ mit $b = k_1 * a$
$a \setminus c$, also existiert ein $k_2 : \mathbb{Z}$ mit $c = k_2 * a$
also $b + c = k_1 * a + k_2 * a = (k_1 + k_2) * a = k_3 * a$
mit $k_3 = k_2 + k_1$
also $a \setminus (b + c)$

3.2 Division

Theorem

$b, c : \mathbb{Z}, c \neq 0$. Dann gibt es eindeutig bestimmte $q, r : \mathbb{Z}$ mit $b = q * c + r \wedge 0 \leq r < c$.
Wir nennen q den **Quotienten** und r den **Rest** von c geteilt durch b.

Beispiel

$17 = 5 * 3 + 2 \wedge 0 \leq 2 < 3$
$b = q * c + r \wedge 0 \leq r < |c|$

Eindeutigkeit

Seien $b, c : \mathbb{Z}, c > 0$ Ausserdem $q, q', r, r' : \mathbb{Z}$ mit

$b = q * c + r$	$\wedge$	$0 \leq r < c$
$b = q' * c + r'$	$\wedge$	$0 \leq r' < c \mid * (-1)$
$b - b = (q - q') * c + (r - r')$		$-0 \geq -r' > -c \mid$ umdrehen
$0 \Rightarrow r - r' = (q' - q) * c$		$-c < -r' \leq -0$
		$0 \leq r < c$
$r = r' \equiv q = q'$		$-c < r - r' < c$
		$-c < (q' - q) * c < c$
		$-1 < q' - q < 1$

$\Rightarrow q' - q = 0$, also $q' = q$, also $r = r'$

Definition

Sei b, c, q, r : $\mathbb{Z}, c \neq 0$,
$b = q * c + r, 0 \leq r < |c|$

Nach Satz q, r existent und eindeutig.
Definieren die Funktionen **div** und **mod**.

div(b,c) = b div c = def q,
mod(b,c) = b mod c = def r div, mod: $\mathbb{Z}$ x $\mathbb{Z}^{\neq 0} \to \mathbb{Z}$

3.3 Greatest Common Divisor (GCD)

$x \uparrow y \Rightarrow$ if x $\geq y$ then x else y (max)
$x \downarrow y \Rightarrow$ if x $\leq y$ then x else y (min)

Sei $M \subseteq \mathbb{Z}, M \neq \varnothing$, M endlich
Dann max(M) = $(\uparrow b : \mathbb{Z} | b \in M : b)$

Definition

$D_m = \{d : \mathbb{Z} | d \backslash m\}$ (Menge aller Teiler von m)

Beispiele

$D_{12} = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$
$D_0 = \{\mathbb{Z}\}$
$1 \in D_m$, also $D_m \neq \varnothing$

Definition

$D_{m,n} = D_m \cap D_n$ (Menge der gemeinsamen Teiler von m und n)

Beispiele

$D_{4,6} = \{-4, -2, -1, 1, 2, 4\} \cap \{-6, -3, -2, -1, 1, 2, 3, 6\} = \{-2, -1, 1, 2\}$
$D_{2,0} = \{-3, -1, 1, 3\} \cap \mathbb{Z} = \{-3, -1, 1, 3\}$
$D_{0,0} = \mathbb{Z}$
$1 \in D_{m,n}$, also $D_{m,n} \neq \varnothing$

Sei b, c : $\mathbb{Z}$, $b \neq 0 \vee c \neq 0$.
Dann ist $D_{b,c} \neq \varnothing$ und $D_{b,c}$ hat ein grösstes Element.

gcd(b,c) = b gcd c = max($D_{b,c}$)
gcd(0,0) = 0 gcd 0 = 0

Satz

a) b gcd b = $|b|$

b) 0 gcd b = $|b|$

c) b gcd c = $|b|$ gcd $|c|$ (ged - Algo für N genug)

d) b gcd c = c gcd b

e) b = a * c + d $\Rightarrow$ b gcd c = c gcd d

Beweis

Annahme: Sei b = a*c + d
zu zeigen: Es gilt b gcd = c gcd d

1. Fall:
b = c = 0 Dann d= 0
Dann b gcd c = c gcd d

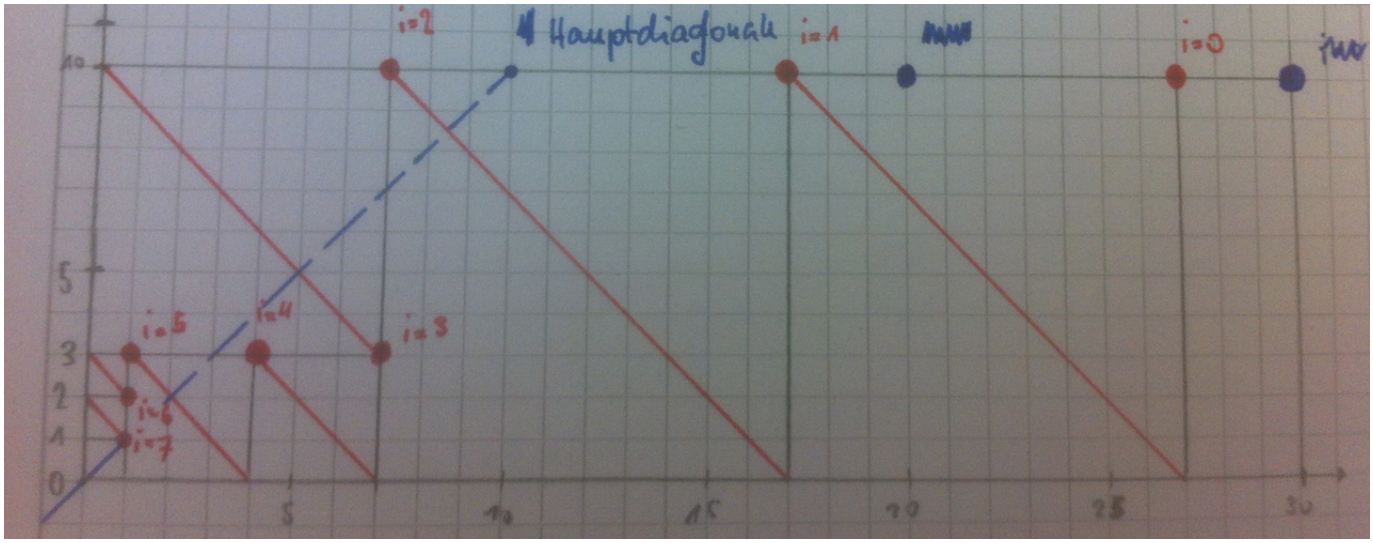
2. Fall:
$b \neq 0 \vee c \neq 0$
Wir zeigen $D_{b,c} = D_{c,d}$. Damit folgt b gcd = max($D_{b,c}$) = max($D_{c,d}$) = c gcd d.

zu zeigen: $D_{b,c} = D_{c,d}$ also $t \in D_{b,c} \Leftrightarrow t \in D_{c,d}$

Teil 1 ($t \in D_{b,c} \Rightarrow t \in D_{c,d}$)
$t \in D_{b,c}$
$\Rightarrow <$ $DefD_{m,n}$ $>$
$t \in D_b \cap D_c$
$\Rightarrow <$ $Def\cap$ $>$
$t \in D_b \wedge t \in D_c$
$\Rightarrow <$ $DefD_m$ $>$
$t \backslash b \wedge t \backslash c$
$\Rightarrow <$ Def $\backslash$ mit $k_1, k_2 : \mathbb{Z}$ $>$
$b = k_1 * t \wedge c = k_2 * t$
$\Rightarrow <$ $d = b - a * c$, nach Annahme$>$
$d = k_1 * t - a * (k_2 * t)$
$\Rightarrow <$ $Arith$ $>$
$d = t * (k_1 - a * k_2)$
$\Rightarrow <$ $Def\backslash$ mit $k_1 - a * k_2 : \mathbb{Z}$ $>$
$t \backslash d \wedge t \backslash c$
$\Rightarrow <$ $DefD_m$ $>$
$t \in D_d \wedge t \in D_c$
$\Rightarrow <$ $Def\cap$ $>$
$t \in D_d \cap D_c$
$\Rightarrow <$ $DefD_{d,c}$ $>$
$t \in D_{d,c}$

Teil 2 ($t \in D_{b,c} \Leftarrow t \in D_{c,d}$)
tbd

3.4 Euklid ged(27,10)



Regel e: b = a * c + d ⇒ b gcd c = c gcd d

b gcd c = c gcd (b - ac) Setze a = 1
x gcd y = y gcd (x - y)
gcd(x,y) = gcd(y, x-y)
gcd(x,y) = gcd (x-y, y) : Korollar zu Regel e

Algo:
Algo terminiert. Sei n Anzahl Iterationen. Dann gcd(bc) = x_n oder y_n (beides richtig)
$(x_0, y_0) = b, c$
$i := 0$
while $x_i \neq <_i$ **do**
if $x_i < y_i$ **then** $(x_i + 1, y_i - 1) = (x_i - y_i, y_i)$
else
$(x_i + 1, y_i - 1) = (x_i, y_i - x_i)$
endif
i := i+1
end

3.5 Erweiterter Euklid

Satz:

$r_{-2} \underbrace{=}_{A}$ a $r_{-1} \underbrace{=}_{B}$ b
$p_{-2} \underbrace{=}_{C} 0$ X $p_{-1} \underbrace{=}_{D} 1$
$q_{-2} \underbrace{=}_{E} 1$ $q_{-1} \underbrace{=}_{F} 0$

i := 0

while $r_{i-1} \underbrace{>}_{G} 0$ **do**
berechne c_i und r_i mit $r_{i-2} \underbrace{=}_{H} c_i * r_{i-1} + r_i \wedge 0 \underbrace{\leq}_{I} r_i \underbrace{<}_{J} r_{i-1}$
$p_i \underbrace{=}_{K} c_i * p_{i-1} + p_{i-2}$

$q_i \underbrace{=}_{L} c_i * q_{i-1} + 1_{i-2}$
$i := i + 1$
end

Seien a, b : $\mathbb{N}$.
Dann gibt es Zahlen $x, y : \mathbb{Z}$ mit $x * a + y * b = \gcd(a,b)$.
Wir konstruieren diese Zahlen durch erteiterten Euklidschen Algorithmus.

1) $r_{n-1} = gcd(a, b)$
2) $p_n\ gcd(a, b) = a$
3) $q_n\ gcd(a, b) = b$
4) $a * \frac{q_{n-1}}{(-1)^{n-1}} + b * \frac{p_{n-1}}{(-1)^n} = gcd(a, b)$

i	r_i	c_i	p_i	q_i	
-2	654		0	1	
-1	444		1	0	
0	210	1	1	1	=b
1	24	2	3	2	= 210
2	18	8	25	17	= 24
3	6	1	28	19	= 18
4	0	3	109	74	= 0

Beweis
Es gibt offensichtlich $n : \mathbb{N}$ mit $r_n = 0 \wedge (\forall i | 0 \leq i < n : r_i > 0)$
Invarianten für alle $i : 0 \leq i \leq n + 1$

I_1: ged(r_{i-2},r_{i-1}) = ged(a,b)

I_2: $p_{i-2} * r_{i-1} + p_{i-1} * r_{i-2} = a$

I_3: $q_{i-2} * r_{i-1} + q_{i-1} * r_{i-2} = b$

I_4: $q_{i-2} * p_{i-1} - q_{i-1} * p_{i-2} = (-1)^{i-1}$

Beispiel I_2:

Induktionsanfang

$i = 0, p_{-2} * r_{-1} + p_{-1} * r_{-2}$
$=< C, B, D, A >$
$0 * b + 1 + a$
$=< Arith >$
a

Induktionsschritt

zu zeigen: $I_2(i) \wedge r_{i-1} > 0 \Rightarrow I_2(i + 1)$ für alle i mit $0 \leq i \leq n$.
Sei n eine $\mathbb{N}$ mit $0 \leq i \leq n$

Annahme: es gibt $I_2(i) \wedge r_{i-1} > 0$
zu zeigen: es gibt $I_2(i + 1)$

$p_{(i+1)-2} * r_{(i+1)-1} + p_{(i+1)-1} * r_{(i+1)-2}$
$=< Arith >$
$p_{i-1} * r_i + p_i * r_{i-1}$
$=< H, <> >$
$p_{i-1} * (r_{i-2} - c_i * r_{i-1}) + (c_i * p_{i-1} + p_{i-2}) * r_{i-1}$
$=< Arith >$
$p_{i-1} * r_{i-2} + p_{i-2} * r_{i-1}$

$=< Annahme >$
a

Es gilt insbesondere: $p_n * r_{n-1} + p_{n-1} * \overbrace{r_n}^{0} = a$
$p_n * gcd(a,b) = a \rightarrow (2)$

3.6 Primzahlen

Def. Eine Zahl $n : \mathbb{N}$ heisst prim, wenn ihre einzigen positiven Teiler 1 und n sind, mit $1 \neq p$:

p ist prim $= p \geq 2 \wedge (\forall i : \mathbb{N} | 1 < i < p : i \neg\backslash\ p)$
$|D_p^+| = 2$

Sonst heissst, p zusammengesetzt.

Def. Zahlen $b, c : \mathbb{N}$ heisst relativ prim $(b \perp c)$ falls der $ged(b,c) = 1$

Satz Jede natürliche Zahl $n : \mathbb{N}, n \geq 1$ kann als Produkt von PRimzahlen geschrieben werden.
D.h. es existiert eine Zahl $m : \mathbb{N}$ und m Primzahlen $(p_0, p_1, ..., p_{m-1})$

$n := (*i | 0 \leq i < m : p^i)$

Satz Sei $n : \mathbb{N}, n \geq 1$. Die Zerlegung von n in Primzahlen ist eindeutig.

Bsp. $328 = 2 * 164 = 2 * 2 * 82 = 2 * 2 * 2 * 41$
$328 = 2^3 * 41^1$
$328 = p_0^{\alpha 0}, p_1^{\alpha 1}, ..., p_{m-1}^{\alpha m-1}$

Satz Es gibt unendlich viele Primzahlen.

3.7 Modulare Arithmetik

3.7.1 Kongruenz

Def $a, b : \mathbb{Z}, m : \mathbb{N}^{>0}$. a heisst kongruent b modulo n, wenn $n \setminus (a - b)$
$a \equiv_n b = n \setminus (a - b)$
$a \equiv b$ (mod n)

Bsp. $5 \equiv_3 7 = false$
$5 \equiv_3 8 = true$

Satz Sei $n : \mathbb{N}^{>0} \equiv_n$ eine Äquivalenzrellation.

Beweis

Symmetrisch $n \setminus (a - b) \rightarrow a - b = k * n \rightarrow b - a = (-k) * n \rightarrow n \setminus (b - a)$

Reflexiv $a \equiv_n a \rightarrow n \setminus (a - a) \rightarrow n \setminus 0$

Transitiv $a \equiv_n b \wedge b \equiv_n c \rightarrow a \equiv_n c$

1. Annahme
$a \equiv_n b$
$<$ def $\backslash k : \mathbb{Z} >$
$a - b = k_n * n$

2. Annahme
$b \equiv_n c$
$<$ def $\backslash k_2 : \mathbb{Z} >$
$(b - c) = k_2 * n$

zu zeigen

$a \equiv_n c$
$a - b = k_1 * n$
$b - c = k_2 * n$
$a - c = (k_1 + k_2) * n$
$<$ def $\setminus$ mit $(k_1 + k_2) : \mathbb{Z} >$
$n \setminus (a - c)$

3.7.2 Restklasse modulo n

Def. $[a]_n = \{n : \mathbb{Z} | : a + k * n\}$
Jedes $a' \in [a]_n$ ist ein Repräsentant von $[a]_n$

Satz Sei $a \equiv_n a'$ Dann $[a] = [a']$

Bsp. $[3]_7 = \{k : \mathbb{Z} | 3 + k * 7 :\} = \{..., -11, -4, 3, 10, 17, ...\}$
$[-4]_7 = \{k : \mathbb{Z} | -4 + k * 7 :\} = \{..., -11, -4, 3, 10, 17, ...\}$
$[2]_7 = \{k : \mathbb{Z} | 2 + k * 7 :\} = \{..., -12, -5, 2, 9, 16, ...\}$

3.7.3 Zerlegung, Partition

Def. $Z_n = \{a : \mathbb{N} | 0 \leq a < n : [a]_n\}$

Bsp. $Z_3 = \{[0]_3, [1]_3, [2]_3\}$

$Z_3 = \{\{..., \quad -3, \quad 0, \quad 3, \quad 6, \quad ...\},$
$\{..., \quad -2, \quad 1, \quad 4, \quad 7, \quad ...\},$
$\{..., \quad -1, \quad 2, \quad 5, \quad 8, \quad ...\}\}$

Satz $a, a', b, b' : \mathbb{Z}, n : \mathbb{N}^{>0}$
$a \equiv_n a'$ und $b \equiv_n b'$
$a + b \equiv_n a' + b'$
$a * b \equiv_n a' * b'$

Def $a, b : \mathbb{Z}$ $n : \mathbb{N}^{>0}$
$[a]_n +_n [b]_n = [a + b]_n$
$[a]_n *_n [b]_n = [a * b]_n$

Bsp. $[5]_n +_n [4]_n = [5 + 4]_n = [9]_7 = [2]_7$

3.7.4 Gruppe

Eine Gruppe $(S, \oplus)$ ist eine Menge S mit einer Operation $\oplus$ aus S mit: $\oplus : S \times S \to a'$

1. Abgeschlossenheit
$a \oplus b \in S'$
$\forall a, b \in S'$

2. Identität, neutrales Element
$\exists e \in S'$ mit $e \oplus a = a = a \oplus e$
$\forall a$

3. Assoziativität
$a \oplus (b \oplus c) = (a \oplus b) \oplus c$
$\forall a, b, c \in S$

4. Inverse
für jedes $a \in S$ gibt es ein $b \in S$ mit $a \oplus b = b \oplus a = e$

5. Symmetrie
$a \oplus b = b \oplus a$
$\forall a, b$

dan heisst $(S', \oplus)$ abelsche Gruppe.

3.7.5 endliche Gruppe

Ist S endlich, dann ist $(S, \oplus)$ eine endliche Gruppe.

Def. $(Z_n, +_n)$ heisst additive Gruppe modulo n.

Satz $(Z_n, +_n)$ ist endliche abelsche Gruppe.

Beispiel:

$+_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Beweis:

1. Abgeschlossen: klar aus Def
2. Identität $[0]_n$
3. Asso: aus Def
4. Inv: $[a]_n + [n-a]_n = [a + (n-a)]_n = [n]_n = [0]_n$
5. Sym: aus Def
6. $|Z_n| = n$ endlich

3.7.6 reduzierte Menge

Def. $Z_n^* = \{a : \mathbb{Z} | gcd(a, n) = 1 : [a]_n\}$
heisst reduzierte Menge Des Rest modulo n

Bsp. $Z_{10}^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$

$*_{10}$	$[1]_{10}$	$[3]_{10}$	$[7]_{10}$	$[9]_{10}$
$[1]_{10}$	$[1]_{10}$	$[3]_{10}$	$[7]_{10}$	$[9]_{10}$
$[3]_{10}$	$[3]_{10}$	$[9]_{10}$	$[1]_{10}$	$[7]_{10}$
$[7]_{10}$	$[7]_{10}$	$[1]_{10}$	$[9]_{10}$	$[3]_{10}$
$[9]_{10}$	$[9]_{10}$	$[7]_{10}$	$[3]_{10}$	$[1]_{10}$

Beweis:

1. Abgeschlossen:
   $\underbrace{gcd(a, n) = 1}_{a \in Z_n^*} \wedge \underbrace{gcd(b, n) = 1}_{b \in Z_n^*} \Rightarrow \underbrace{gcd(a * b, n) = 1}_{a*b \in Z_n^*}$
2. Identität:
   $[1]_n$ weil $[a]_n * [1]_n = [a * 1]_n = [a]_n$
3. Assozativität:
   $[a]_n *_n ([b]_n * [c]_n)$
   $=$ <Def $*_n$ >
   $[a]_n *_n [b * c]_n$
   $=$ <Def $*_n$ >
   $[a * (b * c)]_n$
   $=$ <Asso $*$ >
   $[(a * b) * c]_n$
   $=$ <Def $*_n$ >
   $[a * b]_n *_n [c]_n$
   $=$ <Def $*_n$ >
   $([a]_n *_n [b]_n) *_n [c]_n$

4. Inv: (erweiterter Euklid)
   $\exists x, y$
   $x * b + y * c = gcd(b, c)$
   $x * a + y * n = gcd(a, n) = 1$
   also $x * a \equiv_n 1$
   $[x]_n$ ist also multiplikativ Inverses
   $[x]_n * [a]_n = [x * a]_n = [1]_n$
   x ausrechenbar mit erweitertem Euklid

5. Sym: wie Asso

6. $|Z_n^*| < |Z_n|'$ endlich

Berechnung multiplikatives Inverses, am Beispiel 105mod31

1. Überprfen ob die beiden Werte koPrim sind.
   $105 *_x -31 *_y = 1$
   $105 = 3 * 31 + 12$
   $31 = 2 * 12 + 7$
   $12 = 1 * 7 + 5$
   $7 = 1 * 5 + 7$
   $5 = 2 * 2 + 1$
   $2 = 2 * 1 + 0$

   - Da diese Abfolge erstellen lässt ohne Rest, sind die beiden Zahlen koPrim

2. Rücksubstitution
   $1 = 5 - (2 * 2)$
   $1 = 5 - 2 * (7 - 5) = 3 * 5 - 2 * 7 - 1$
   $1 = 5 - 2 * (7 - 5) = 3 * 5 - 2 * 7 - 1$
   $1 = 3 * (12 - 7) - 5 * (31 - 2 * 12) = -5 * 31 + 13 * 12$
   $1 = 13 * 12 - 5 * 31$
   $1 = 13 * (105 - 3 * 31) - 5 * 31$
   $1 = 13 * 105 - 39 * 31 - 5 * 31$
   $1 = \underbrace{13}_{} * 105 - 44 * 31$
   gesuchter Wert für $105^{-}1 =_{31} 13$