Diskrete Mathematik 2

FS 2013

Contents

1 Erste Woche

1.1 Semesterablauf

- Arithmetik in $\mathbb{Z}$

- Modulares Rechnen

- Gruppen

- RSA

- Quantifizierung

- Induktion
  - Rekurision
  - Invarianten

- Kein Laptop

- Zwischenpruefung: 30.04.2013 (1 Stunde)

- 5. Maerz 2013 Unterricht nur bis 18:20

- Buecher:

  - Gries/Schneider
    A logical approach to Discrete Math
    Springer, 1993

  - Jean Gallier
    Discrete Math
    Springer, 2010

  - Struckermann/Waetiger
    Mathematik fuer Informatiker
    Spektrum, 2007

1.2 Quantifizierung

$\mathbb{N} = \begin{cases} \{\underline{0}, 1, 2, ...\} \text{ (?)} \\ \{1, 2, ...\} \text{ (?)} \end{cases}$

$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + ... + n^2$

$$\sum_{i=1}^{-1} i^2 = \begin{cases} ungueltig\ (?) \\ 1^2\ (?) \\ 1^2 + 0^2 + (-1)^2\ (?) \\ 0\ (\rightarrow ja,\ Neutrales\ Element) \end{cases}$$

$\sum_{i=1}^{n} i^2 + 1 = 1^2 + 2^2 + ... + n^2 + 1$ (?)

$\sum_{i=1}^{n}(i^2 + 1) = (1^2 + 1) + (2^2 + 1) + ... + (n^2 + 1)$ (?)

$\sum_{\substack{i=1 \\ odd(i)}}^{n} i^2 = 1^2 + 3^2 + ... + n^2$, falls $odd(n)$, sonst $(n-1)^2$

$\prod_{i=1}^{n} i^2 = 1^2 * 2^2 * ... * n^2$

$\prod_{i=1}^{-1} i^2 = 1$ (neutrales Element)

(Java ==)

$\forall_{i=0}^{n-1}(b[i] == 0) = (b[0] == 0) \wedge (b[1] == 0) \wedge ... \wedge (b[n-1] == 0)$

$\exists_{i=0}^{n-1}(b[i] == 0) = (b[0] == 0) \vee (b[1] == 0) \vee ... \vee (b[n-1] == 0)$

$\sum_{i=1}^{n} i^2 = (\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n : i^2)$

$(\sum i : \mathbb{N}, j : \mathbb{N} \mid 1 \leqslant i \leqslant 2 \wedge 1 \leqslant j \leqslant 3 : i^j)$

$(\circ\, v_1 : T_1, ..., v_n : T_n \mid R : P)$

- $\circ : T \times T \rightarrow T$ (wobei T ein Typ ist)

Bsp: $+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
$+(3,4) = 7$

$$\text{ABELSCHES MONOID} \begin{cases} a \circ b = b \circ a \text{ fuer alle } a, b : T \text{ (Symmetrie)(Kommutativitaet)} \\ MONOID \begin{cases} (a \circ b) \circ c = a \circ (b \circ c) \text{ fuer alle } a, b, c : T \text{ (Assoziativitaet)} \\ u \circ a = a = a \circ u \\ \text{ es gibt ein } u : T, \text{ so dass fuer alle } a : T \text{ (neutrales Element)} \end{cases} \end{cases}$$

$\circ$	T	u
$+\sum$	$\mathbb{Z}$	0
$*\prod$	$\mathbb{Z}$	1
$\forall$	$\mathbb{B}$	$true$
$\exists$	$\mathbb{B}$	$false$

String mit Konkatenation: Nicht-abelsches Monoid
$("a" + "b") + "c"\ equals\ "a" + ("b" + "c")$
$"a" + ""\ equals\ "a"$
$"a" + "b"\ !equals\ "b" + "a"$ (nicht equals)

- $T_1, ..., T_n$ Datentypen

- $V_1, ..., V_n$ Variablen

alle paarweise verschieden

V_i vom Typ: T_i

- R : boolescher Ausdruck, kann $V_1 ... V_n$ enthalten, Bereich (Range)

- P : beliebiger Ausdruck vom Typ T, kann $V_1 ... V_n$ enthalten, Koerper (Body)

Typ der Quantifizierung : T

$(\forall i : \mathbb{N} \mid 0 \leqslant i \leqslant n : b[i] = 0)$ und das Ganze ist : $\mathbb{B}$
$(\circ\, V_1 : T_1 \mid R : P)$ wobei $T_1 : \mathbb{N}, P : \mathbb{B}$

$\wedge : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$

$P : T_1 \times T_2 \times ... \times T_n \rightarrow T$

1.3 Semantik

Bsp: $(+i : \mathbb{Z} \mid -1 \leqslant i \leqslant 2 : i^2)$

1. Fall (Topf $\neq \emptyset$)

Von $\mathbb{Z}$ alle Zahlen ausfiltern (-1,0,1,2) (Menge)

$\rightarrow^{1^2}$ $((-1)^2, 1^2, 0^2, 2^2)(1, 1, 0, 4)$ (Multimenge)

$\rightarrow 2^2 + 1^2 + (-1)^2 + 0^2$

2. Fall (Topf = 0)

$\rightarrow$ Topf leer $\rightarrow$ Resultat: Neutrales Element (von +) $\rightarrow$ 0

Beispiele:

1) $(+\, i : \mathbb{N} \mid 0 \leqslant i < 4 : i * 8) = (0 * 8) + (1 * 8) + ...$

2) $(*\, i : \mathbb{N} \mid 0 \leqslant i < 3 : i + 1) = (0 + 1) * (1 + 1) * ...$

3) $(\wedge\, i : \mathbb{N} \mid 0 \leqslant i < 2 : i * d \neq 6) = ((0 * d) \neq 6) \wedge ((1 * d) \neq 6) \wedge ...$

4) $(\vee\, i : \mathbb{N} \mid 0 \leqslant i < 21 : b[i] = 0) = (b[0] == 0) \vee (b[1] == 0) \vee ...$

5) $(\sum k : \mathbb{N} \mid k^2 = 4 : k^2) = 2^2 = 4$

6) $(\sum k : \mathbb{Z} \mid k^2 = 4 : k^2) = 2^2 + (-2)^2 = 8$

---

2 Zweite Woche

2.1 Freie/Gebundene Variablen

$(\circ\, v_1 : T_1, ..., v_n : T_n \mid R : P)$

E1: $(\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^2)$

- Wert haengt von n ab, nicht von i

$n = 3 :$ 0 1 2

$0^2 + 1^2 + 2^2 = 5$

$n = 0 :$ kein i

0 (neutral +)

E2: $(\sum j : \mathbb{Z} \mid 0 \leqslant j < n : j^2)$

$n = 3 \rightarrow 5$

$n = 0 \rightarrow 0$

E3: $(\sum i \text{①} : \mathbb{Z} \mid 0 \leqslant i \text{②} < n : i^2 \text{③}) + i \text{④}$

$(\leftarrow\rightarrow)$: Gueltigkeitsbereich von i (scope)

i tritt hier 4 mal auf (occurs)

Auftreten (occurances) ①,②,③ gebunden
Auftreten ④ frei
② und ③ gebunden an ①
② und ③ angewandte Auftreten (applied)
① bindende, deklarierende Auftreten (binding)

Eine Variable heisst frei in einem Ausdruck E (expression), falls sie in E frei vorkommt.

$FV(E)$ = Menge der freie Variablen von E

$FV(E_3) = \{'n', 'i'\}$ (Die Variablennamen und nicht die Werte der Variablen)

$x, y : \mathbb{Z}$
$x = 3, y = 5$
$\{x, y\} = \{3, 5\}$

$x = y = 3$
$\{x, y\} = \{3\}$

$x + y * 2$
$y, 2 : *$ Operator
dann das Resultat mit x und $+$ Operator

E4: $(\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^2) * (\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^3)$

$FV(E_4) = \{'n'\}$

E5: $(\prod n \mid k \leqslant n \leqslant l : (\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^2) * (\sum i : \mathbb{Z} \mid 0 \leqslant i < n : i^3))$

$FV(E_5) = \{'k', 'l'\}$

E6: $(\sum i : \mathbb{Z} \mid 0 \leqslant i \leqslant (\sum i : \mathbb{Z} \mid 2 \leqslant i < 3 : i^2) : i^2)$

$FV(E_6) = \emptyset$

Ein Ausdruck E ohne freie Variablen ($FV(E) = \emptyset$ oder $\{\}$) heisst geschlossen

$(\sum i : \mathbb{Z} \mid 1 \leqslant i < 2 : (\sum j : \mathbb{Z} \mid 1 \leqslant j < 3 : i + j))$

<u>i zuerst:</u>

$i :$ $\overset{1}{(\sum j : \mathbb{Z} \mid 1 \leqslant j < 3 : 1 + j)} + \overset{2}{(\sum j : \mathbb{Z} \mid 1 \leqslant j < 3 : 2 + j)}$

$j :$ $(\overset{1}{(1+1)} + \overset{2}{(1+2)} + \overset{3}{(1+3)}) + (\overset{1}{(2+1)} + \overset{2}{(2+2)} + \overset{3}{(2+3)})$

<u>j zuerst:</u>

$j :$ $(\sum i : \mathbb{Z} \mid 1 \leqslant i < 2 : (\overset{1}{(i+1)} + \overset{2}{(i+2)} + \overset{3}{(i+3)}))$

$i :$ $\overset{1}{((1+1) + (1+2) + (1+3))} + \overset{2}{((2+1) + (2+2) + (2+3))}$

---

3 Dritte Woche

3.1 Saetze zur Quantifizierung

<u>Satz</u> (Dummy renaming)

$(\circ\, v \mid R : P) = (\circ\, w \mid R[v \leftarrow w] : P[v \leftarrow w])$

<u>Voraussetzung:</u> $w \notin FV(R) \cup FV(P)$

<u>Dabei:</u> $E[v \leftarrow F]$ bezeichnet exakt denselben Ausdruck wie E, aber alle <u>freien</u> Auftreten von v ersetzt durch (F).

wobei E, F : Ausdruck, v : Variable

Bsp: $(i + 5)[i \leftarrow j + 3] = (j + 3) + 5$

wobei $(i + 5) : E$, $[i : v,\ j + 3 : F]$

$(i * 5)[i \leftarrow j + 3] = (j + 3) * 5$

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

$(\sum i \mid true : i^2) = (\sum j \mid true : j^2)$

$= (\sum j \mid true[i \leftarrow j] : i^2[i \leftarrow j])$

$= (\sum j \mid true : j^2)$

$42[i \leftarrow j+3] = 42$ "Man kann die Bedeutung des Universums nicht aendern."

Es ist ein Unterschied, ob die Ersetzung innerhalb oder ausserhalb einer Quantifizierung angegeben wird.

$(\sum i \mid true : i^2)[i \leftarrow j+3]$

Hier sollen alle freien Auftreten von Variable i in $(\sum i \mid true : i^2)$ durch $j+3$ ersetzt werden.
Aber alle Auftreten von i sind in diesem Ausdruck gebunden, also ist nichts zu ersetzen.

Dummy renaming sagt aus, dass wir die gebundenen Auftreten einer Variablen innerhalb einer Quantifizierung konsistent umbenennen duerfen, solange wir dabei keine freien Variablen einfangen.

$(\sum i \mid 1 \leqslant i \leqslant n : i^2)$
$= (\sum j \mid 1 \leqslant i \leqslant n[i \leftarrow j] : i^2[i \leftarrow j])$
$= (\sum j \mid 1 \leqslant j \leqslant n : j^2)$

Hier sind die Ersetzungen innerhalb der Quantifizierung.
Und beachten Sie: im Teilausdruck $1 \leqslant i \leqslant n$ ist die Variable i frei,
daher liefert $1 \leqslant i \leqslant n[i \leftarrow j]$ den Ausdruck $1 \leqslant j \leqslant n$

Im Gesamtausdruck $(\sum i \mid true : i^2)$ sind alle Auftreten von i hingegen gebunden.
Aber in diesem Ausdruck wollen wir auch nicht ersetzen, sondern eben in den beiden Teilausdruecken.

Ein Auftreten einer Variablen kann in einem Teilausdruck frei sein, aber im Gesamtausdruck gebunden.
Ob ein Auftreten frei oder gebunden ist, hängt immer vom betrachteten (Teil-)Ausdruck ab.

Bsp: $(\sum i \mid 1 \leqslant i \leqslant n : i^2)$

wobei $i : v$, $(1 \leqslant i \leqslant n) : R$, $i^2 : P$

$= (\sum j \mid (1 \leqslant i \leqslant n)[i \leftarrow j] : i^2[i \leftarrow j])$

wobei $j : w$

$= (\sum j \mid 1 \leqslant j \leqslant n : j^2)$

<u>Aber:</u> Vorsicht:

$(\sum i : \mid 1 \leqslant i \leqslant n : i^2)$
$n = 0, \qquad 0 (neutral +)$
$n = 1, \qquad 1$

haengt von n ab

$\neq$

$(\sum n : \mid 1 \leqslant n \leqslant n : n^2)$
∞ undefiniert

haengt <u>nicht</u> von n ab

---

4 Vierte Woche

4.1 Saetze zur Quantifizierung (Fortsetzung)

$(\sum i \mid 0 \leqslant i < n : i^2)[n \leftarrow n^2] = (\sum i \mid 0 \leqslant i < n^2 : i^2)$

$(\sum i \mid 0 \leqslant i < n : i^2)[n \leftarrow i+1] \neq (\sum i \mid 0 \leqslant i < i+1 : i^2)$ (geht nicht)
freies Auftreten von i wird gefangen $\rightarrow$ name clash

$(\sum i \mid 0 \leqslant i < n : i^2)[n \leftarrow i+1]$
$= (\sum j \mid 0 \leqslant j < n : j^2)[n \leftarrow i+1]$
$= (\sum j \mid 0 \leqslant j < i+1 : j^2)$

<u>Empty range</u>

$(\circ\, v \mid false : P) = u_\circ$ (Neutrales Element)

<u>One point</u>

Voraussetzung: $v \notin FV(E)$

$(\circ\, v \mid v = E : P) = P[v \leftarrow E]$

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

$(\sum i \mid i = j+i+3 : i^2) \neq i^2[i \leftarrow j+i+3] = (j+i+3)^2$ (geht nicht)

<u>Split-off term</u>

$(\circ\, i \mid 0 \leqslant i < n+1 : P) = (\circ\, i \mid 0 \leqslant i < n : P) \circ P[i \leftarrow n]$

Bsp. $(\sum i \mid 0 \leqslant i < n+1 : i^2) = (\sum i \mid 0 \leqslant i < n : i^2) + n^2$
$0^2 + 1^2 + ... + (n-1)^2 + n^2 = (0^2 + 1^2 + ... + (n-1)^2) + n^2$

$n = 0:$

$(\circ\, i \mid 0 \leqslant i < 1 : P) = (\circ\, i \mid 0 \leqslant i < 0 : P) \circ P[i \leftarrow 0]$

$i = 0:$

$P[i \leftarrow 0]$ (One point) $= u_\circ$(empty range) $\circ P[i \leftarrow 0]$

4.2 Anwendung

Praedikat

$i + 1 > j : \mathit{Bool}$ macht Aussage ueber Werte von freien Variablen

Feld $b[0...n-1]$ mit ganzen Zahlen; $n \geqslant 0$

"b enthaelt eine -1." $\rightarrow$ bedeutet mindestens

$(\exists i : \mathbb{N} \mid 0 \leqslant i < n : b[i] = -1)$

"b enthaelt genau eine -1."

$(\exists i : \mathbb{N} \mid 0 \leqslant i < n : (b[i] = -1) \wedge (\forall j : \mathbb{N} \mid (0 \leqslant j < n) \wedge (j \neq i) : b[j] \neq -1))$

$=$

$1 = (\sum i : \mathbb{N} \mid (0 \leqslant i < n) \underset{\&\&}{\wedge} (b[i] = -1 : 1)$

"b enthaelt keine -1."

$(\forall i : \mathbb{N} \mid 0 \leqslant i < n : b[i] \neq -1)$

$=$

$\neg(\exists i : \mathbb{N} \mid 0 \leqslant i < n : b[i] = -1) \rightarrow (\neg$ ("b enthaelt mindestens eine -1."))

$\neg(\exists v \mid R : P) = (\forall v \mid R : \neg P)$
$\neg(\forall v \mid R : P) = (\exists v \mid R : \neg P)$

de Morgan
$\neg(\exists v \mid R : P) = \neg(P_0 \vee P_1 \vee ... \vee P_{n-1} \vee P_n)$
$= ((\neg P_0) \wedge (\neg P_1) \wedge ...(\neg P_n))$
$= (\forall v \mid R : \neg P)$

---

5 Fuenfte Woche

5.1 Magisches Quadrat

<u>Uebungsblatt 2, Aufgabe 3</u>

$k, i : 1 \leqslant k \leqslant n, 1 \leqslant i \leqslant n$

1) $(\exists M : \mathbb{N} \mid true : (\forall i \mid 1 \leqslant i \leqslant n : (\sum k \mid 1 \leqslant k \leqslant n : Q[i,k]) = M$
$\wedge(\sum k \mid 1 \leqslant k \leqslant n : Q[k,i]) = M$
$\wedge(\sum k \mid 1 \leqslant k \leqslant n : Q[k,k]) = M$
$\wedge(\sum k \mid 1 \leqslant k \leqslant n : Q[k,(n+1)-k)]) = M$
$\wedge(\forall m : N \mid 1 \leqslant m \leqslant n^2 :$
$(\exists i,j \mid 1 \leqslant i < n \wedge 1 \leqslant j < n : m = Q[i,j])))$

2) $M = \frac{\sum_{i=1}^{n^2} i}{n}$

$n * M = (\sum i \mid 1 \leqslant i \leqslant n^2 : i)$

$M = \frac{(\sum i \mid 1 \leqslant i \leqslant n^2 : i)}{n} = \frac{n^2 * (n^2+1)}{2*n} = \frac{n*(n^2+1)}{2}$

5.2 Mathematische Induktion

$(\mathbb{B} : Boolean)$

Sei $P : \mathbb{N} \rightarrow \mathbb{B}$
zu zeigen:
$(\forall n : \mathbb{N} \mid true : P(n))$

<u>Beispiel</u>

$P(n) : n^3 + 5 * n$ ist ein Vielfaches von 6

z ist Vielfaches von 6 heisst:
$(\exists i : \mathbb{Z} \mid true : i * 6 = z)$

$0^3 + 5 * 0 = 0(\text{Zeuge}) * 6$
$1^3 + 5 * 1 = 1 * 6$

$2^3 + 5 * 2 = 3 * 6$ (Muss bei allen *true* zurueck geben!!)

Idee: Induktionsprinzip

Man zeigt:

1) $P(0)$
2) $P(n) \Rightarrow P(n+1)$ fuer alle $n : \mathbb{N}$

$P(0)$ gilt: Wegen 1)

$(P(0) \wedge (P(0) \Rightarrow P(1)) \Rightarrow P(1)$
wegen 2) mit $n = 0$

$(P(1) \wedge (P(1) \Rightarrow P(2)) \Rightarrow P(2)$
wegen 2) mit $n = 1$

Damit gilt $P(n)$ fuer alle $n : \mathbb{N}$

Unser Beispiel

1) Induktionsanfang (Base case)
zu zeigen: $P(0)$
$0^3 + 5 * 0 = 0(\text{Zeuge}) * 6$

2) Induktionsschritt (inductive step)
zu zeigen: $P(n) \Rightarrow P(n+1)$ fuer alle $n : \mathbb{N}$

Sei n eine beliebige natuerliche Zahl.

Annahme: Es gaelte $P(n) : n^3 + 5 * n$, dass heisst $n^3 + 5 * n = 6 * r$, mit $r : \mathbb{Z}$, ist vielfaches von 6.
zu zeigen: (unter dieser Annahme) $P(n+1) : (n+1)^3 + 5 * (n+1)$ ist vielfaches von 6.
das heisst: $(n+1)^3 + 5 * (n+1) = 6 * s$, mit $s : \mathbb{Z}$

$(n+1)^3 + 5 * (n+1)$

<Arith>

$= (n^3 + 3 * n^2 + 3 * n + 1) + (5 * n + 5)$

<Arith + Kaninchen>

$= (n^3 + 5 * n) + (3 * n^2 + 3 * n + 6)$

<Annahme>

$= 6 * r + 3 * n^2 + 3 * n + 6$

<Arith + Kaninchen>

$= 6 * r + 3 * n * (n+1) + 6$

<n*(n+1) ist gerade>

$= 6 * r + 3 * (2 * t) + 6$

<Arith>

$= 6 * (r + t + 1)$ (Zeuge) ✓

Modus ponens

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

$(p \Rightarrow r) \wedge (\neg p \Rightarrow s)$

$\equiv (p \wedge r) \vee (\neg p \wedge s)$

Sei p. Dann

$$
\begin{array}{ll}
 & (p \Rightarrow r) \wedge (\neg p \Rightarrow s) \\
= & r \quad \wedge \quad true \\
= & r
\end{array}
$$

$$
\begin{array}{ll}
 & (p \wedge r) \vee (\neg p \wedge s) \\
= & r \quad \vee \quad false \\
= & r
\end{array}
$$

Sei $\neg p$ Analog

---

6 Sechste Woche

6.1 Vollstaendige Induktion

Arbeitsblatt 1 - Aufgabe 1

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

wobei $P(0)$: Base Case
$(\forall n : \mathbb{N} \mid : P(n) \Rightarrow P(n+1))$: Iductive Case
$(\forall n : \mathbb{N} \mid : P(n))$: Ziel der Induktion

Complete Induction

$P(0)$
$(P(0) \wedge (P(0) \Rightarrow P(1))) \Rightarrow P(1)$
$(P(0) \wedge P(1) \wedge (P(0) \wedge P(1) \Rightarrow P(2))) \Rightarrow P(2)$
$(P(0) \wedge P(1) \wedge P(2) \wedge (P(0) \wedge P(1) \wedge P(2) \Rightarrow P(3))) \Rightarrow P(3)$

$(P(0) \wedge (\forall n : \mathbb{N} \mid : (\forall k : \mathbb{N} \mid k \leqslant n : P(k)) \Rightarrow P(n+1)) \Rightarrow (\forall n : \mathbb{N} \mid : P(n))$

Aufgabe 2

Sei $k : \mathbb{N}$, $k \geqslant 0$

$(P(k) \wedge (\forall n : \mathbb{N} \mid n \geqslant k : P(n) \Rightarrow P(n+1)) \Rightarrow (\forall n : \mathbb{N} \mid n \geqslant k : P(n))$

Fibonacci

$fib : \mathbb{N} \rightarrow \mathbb{N}$

A $fib(0) = 0$
B $fib(1) = 1$
C $fib(n) = fib(n-1) + fib(n-2)$, $n \geqslant 2$

Satz Fuer alle $n : \mathbb{N}$ gilt:

$P(n) : (\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n : fib(i)) = f(n+2) - 1$

Beweis

1) Induktionsanfang: zu zeigen: $P(0)$, also

$(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant 0 : fib(i)) = f(0+2) - 1$

$(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant 0 : fib(i))$

$<$ empty range, neutral $+$ $>$

$= 0$

$fib(0+2) - 1$

$<$ arith $>$

$= fib(2) - 1$

$<$ C mit $n = 2$ $>$

$= fib(0) + fib(1) - 1$

$<$ A, B $>$

$= 0 + 1 - 1$

$<$ arith $>$

$= 0$

2) Induktionsschritt:

Sei n eine beliebige natuerliche Zahl

Annahme: $(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n : fib(i)) = fib(n+2) - 1$

zu zeigen: $(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n+1 : fib(i)) = fib(n+3) - 1$

$(\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n+1 : fib(i))$

$<$ range split (split-off term) $>$

$= (\sum i : \mathbb{N} \mid 1 \leqslant i \leqslant n : fib(i)) + fib(n+1)$

$<$ Annahme $>$

$= fib(n+2) - 1 + fib(n+1)$

$<$ arith $>$

$= (fib(n+2) + fib(n+1)) - 1$

$<$ C, mit $n+3 \geqslant 2$ $>$

$= fib(n+3) - 1$

$\square$

Satz:

Fuer alle $n : \mathbb{N}$ mit $n \geqslant 3$ gilt:

$2n + 1 < 2^n$

Beweis

1) IA

$2 * 3 + 1 < 2^3 \equiv 7 < 8$ ✓

2) IS

Sei n eine beliebige natuerliche Zahl mit $n \geqslant 3$
Annahme Es gelte: $2n + 1 < 2^n$
zu zeigen: Es gilt: $2(n+1) + 1 < 2^{(n+1)}$

Beweis

$2(n+1)+1$

$\quad < \text{arith} >$

$= (2n+1)+2$

$\quad < \text{Annahme} >$

$\Rightarrow (2n+1)+2 < 2^n+2$

$\leqslant$

2^n+2^n

$\quad < \text{arith} >$

$= 2^n+1$ ✓

$2*2*...*2 = 2^n$
(n mal)

$pow1(n) = (\prod i : \mathbb{N} \mid 1 \leqslant i \leqslant n : 2)$

$pow2(n) \begin{cases} 2^0 = 1 \\ 2^n = 2*2^{n-1}, \text{ fuer } n > 0 \end{cases}$

```
int pow1(int n){
        int p=1;
        for(int i=1; i<=n; i++){
                p*=2;
        }
        return p;
}

int pow2(int n){
        return (n==0)? 1: 2*pow2(n-1);
}
```

Satz: Fuer alle $n : \mathbb{N}$ gilt: $pow1(n) = pow2(n)$

Beweis Aufgabe!

$x < y \Rightarrow x \leqslant y$

$x \leqslant y \Rightarrow x < y \vee x = y$

$p \Rightarrow p \vee q$

$x \leqslant y \not\Rightarrow x < y$

$15 \leqslant 15 \not\Rightarrow 15 < 15$

7 Siebte Woche

7.1 Zahlentheorie

Teilbarkeit

$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$, $c, b : \mathbb{Z}$

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

$c \backslash b$: "c teilt b"
"b ist teilbar durch c"
"c ist Teiler von b"
"b ist Vielfaches von c"

Beispiel:

$7 \backslash 13 = false$
$(-7) \backslash 14 = true$
nicht einheitlich in Literatur $\begin{cases} 0 \backslash 14 = false \text{ (es existiert kein } k) \\ 0 \backslash 0 = true \end{cases}$

Satz $b, c, d : \mathbb{Z}$

(1) $c \backslash c$ (Reflektivitaet)
(2) $c \backslash 0$
(3) $1 \backslash b$
(4) $c \backslash 1 \Rightarrow c = 1 \vee c = -1$
(5) $d \backslash c \wedge c \backslash b \Rightarrow d \backslash b$ (Transitivitaet)
(6) $b \backslash c \wedge c \backslash b \Rightarrow b = c \vee b = -c$
auf $\mathbb{Z}$ also nicht antisymmetrisiert, auf $\mathbb{N}$ aber schon
(7) $b \backslash c \Rightarrow b \backslash (c * d)$
(8) $b \backslash c \Rightarrow (b * d) \backslash (c * d)$
(9) $1 < b \wedge b \backslash c \Rightarrow \neg(b \backslash (c + 1))$

(1) und (5) und (6) heisst: \-Relation ist eine partielle Ordnung auf $\mathbb{N}$ (aber nicht auf $\mathbb{Z}$)

Beweis:

(1) zu zeigen: es gibt $k : \mathbb{Z}$ mit $c = k * c$
Waehle $k = 1 : \mathbb{Z}$
(2) $0 = k * c$, $k = 0 : \mathbb{Z}$
(3) $b = k * 1$, $k = b : \mathbb{Z}$
(4) $1 = k * c = 1 * 1 = (-1) * (-1) \Rightarrow c = 1 \vee c = -1$
(5)
$d \backslash c$, also gibt es $k_1 : \mathbb{Z}$ mit $c = k_1 * d$
$c \backslash b$, also gibt es $k_2 : \mathbb{Z}$ mit $b = k_2 * c$
aber $b = k_2 * c = k_2 * (k_1 * d) = (k_2 * k_1) * d$

also gibt es $k = k_1 * k_2 : \mathbb{Z}$ mit $b = k * d$, also $d \backslash b$
(6)
$b \backslash c$, also gibt es $k_1 : \mathbb{Z}$ mit $c = k1 * b$
$c \backslash b$, also gibt es $k_2 : \mathbb{Z}$ mit $b = k2 * c$
also $b = k_2 * c = k_2 * (k_1 * b) = (k_2 * k_1) * b$
also $b - (k_2 * k_1) * b = 0$
also $b * (1 - k_2 * k_1) = 0$
also $b = 0 \vee 1 - k_2 * k_1 = 0$
also $b = 0 \vee k_2 * k_1 = 1$
also $b = 0 \vee k_2 = k_1 = 1 \vee k_2 = k_1 = -1$
also $b = 0 \vee c = b \vee c = -b$
mit $b = 0$ ist $c = b$

Satz Seien $a, b, c : \mathbb{Z}$

Dann $\quad a \backslash b \wedge a \backslash c \Rightarrow a \backslash (b + c)$

$a \backslash b \Rightarrow b = k_1 * a$

$a \backslash c \Rightarrow c = k_2 * a$

$a \backslash (b + c) \Rightarrow a \backslash (k_1 * a + k_2 * a) \Rightarrow a \backslash a * (k_1 + k_2)$ ✓(Satz (7))

Beweis

Annahme 1: $a \backslash b$, also nach Definition existiert $k_1 : \mathbb{Z}$ mit $b = k_1 * a$

Annahme 2: $a \backslash c$, also nach Definition existiert $k_2 : \mathbb{Z}$ mit $c = k_2 * a$

zu zeigen: Es existiert $k_3 : \mathbb{Z}$ mit $b + c = k_3 * a$

$b + c$

$\quad$ $<$ Annahme 1 und 2 $>$

$= k_1 * a + k_2 * a$

$\quad$ $<$ arith $>$

$= (k_1 + k_2) * a$

$\quad$ $<$ mit $k_3 = k_1 + k_2 : \mathbb{Z}$ $>$

$= k_3 * a$

$\square$

---

8 Achte Woche

8.1 Euklidische Division

Satz (Euklidische Division auf $\mathbb{N}$)

Seien $a, b : \mathbb{N}$, $b \neq 0$.

Dann gibt es eindeutige $q, r : \mathbb{N}$ mit

$a = b * q + r \wedge 0 \leqslant r < b$

$\square$

Satz (Euklidische Division auf $\mathbb{Z}$)

Seien $a, b : \mathbb{Z}$, $b \neq 0$.

Dann gibt es eindeutige $q : \mathbb{Z}$, $r : \mathbb{N}$ mit

$a = b * q + r \wedge 0 \leqslant r < |b|$

$\square$

$a, b : \mathbb{N}$, $b \neq 0$

$a = 17$, $b = 5$

$17 = 5 * 0 + 17 \wedge 0 \leqslant 17$

$17 = 5 * 1 + 12 \wedge 0 \leqslant 12$

$17 = 5 * 2 + 7 \wedge 0 \leqslant 7$

$17 = 5 * 3 + 2 \wedge 0 \leqslant 2$

$a = b * q + r \wedge 0 \leqslant r$ (Invariante)

Stop bei $r < b$

q, r seien Variablen einer imperativer Programmiersprache (keine Mathematische Variablen)

$\{a \geqslant 0 \wedge b > 0\}$

VC3 $\Rightarrow$

$\{a = b * 0 + a \wedge 0 \leqslant a\}$

$q, r := 0, a;$

$\{a = b * q + r \wedge 0 \leqslant r\}$

<u>while</u> $r \geqslant b$ <u>do</u>

$\{a = b * q + r \wedge 0 \leqslant r \wedge r \geqslant b\}$

VC1 $\Rightarrow$

$\{a = b * (q + 1) + (r - b) \wedge 0 \leqslant r - b\}$ (Precondition)

$q, r := q + 1, r - b$

$\{a = b * q + r \wedge 0 \leqslant r\}$

<u>endwhile</u>

$\{a = b * q + r \wedge 0 \leqslant r \wedge \neg r \geqslant b\}$

VC2 $\Rightarrow$

$\{a = b * q + r \wedge 0 \leqslant r < b\}$

VC: Verification Condition

VC3: $a = b * 0 + a$ $(true)$

$a \geqslant 0 \wedge b > 0 \Rightarrow true \wedge 0 \leqslant a$

VC2: $\neg r \geqslant b \equiv r < b$

VC1: $a = b(q + 1) + (r - b)$
$\Leftarrow$
$a = b * q + b + r - b$
$\Leftarrow$
$a = b * q + r$

(von unten nach oben)

Warum gilt $0 \leqslant r - b$?

Weil $r \geqslant b$!

$r \geqslant b \Rightarrow r - b \geqslant 0 \Rightarrow 0 \leqslant r - b$

$\{x + 1 > 5\}$ (Vorbedingung)
$x := x + 1$
$\{x > 5\}$ (Nachbedingung)

8.2 Fundamentaler Schleifen-Satz

Satz (Fundamentaler Schleifen-Satz)

Seien B und I boolesche Ausdruecke und C ein Kommando.

Es gelte $\{I \wedge B\}\ C\ \{I\}$, d.h. I ist eine Invariante der Schleife while B do C end.

Die Ausfuehrung der Schleife beginne im Zustand der I erfuellt. Dann gilt I nach jedem Schleifendurchlauf.

□

Beweis

Durch Induktion. Wir zeigen, dass "Invariante ist nach n Schleifendurchlaeufe erfuellt" fuer alle $n \in M$.
Dabei ist $M = N$, falls ∞-Schleife, und $M = \{0...N\}$ mit $N : \mathbb{N}$ Anzahl der Schleifendurchlaeufe (SDL).

IA I ist nach 0 SDL erfuellt, nach Voraussetzung

Sei $M = N$ (Fall 2: Sei $M = \{0...N\}$)

IS Sei n eine beliebige natuerliche Zahl. (Fall 2: $n \leqslant N - 1$)

Annahme: Es gelte: I ist nach n SDL erfuellt.
zu zeigen: Es gilt: I ist nach $n + 1$ SDL erfuellt.

Beweis

I ist nach n SDL erfuellt. Weiterer SDL bedeutet, dass Schleifenbedingung B gilt.
$I \wedge B$ gilt also, also nach Ausfuehrung von C wieder I, wegen $\{I \wedge B\}\ C\ \{I\}$, also
I nach $n + 1$ SDL erfuellt.

□

Satz Falls Ausfuehrung terminiert, gilt am Ende $I \wedge \neg B$

Beweis

Nach obigem Satz, gilt I am Ende. Die Schleife terminiert, gilt auch $\neg B$.

$\{I \wedge B\}\ C\ \{I\}$

$\{I\}$ while $\{B\}$ do C end $\{I \wedge \neg B\}$

---

9 Neunte Woche

9.1 Euklid auf $\mathbb{Z}$, $\mathbb{N}$

Satz (Euklid auf $\mathbb{Z}$)

$a, b : \mathbb{Z}$, $b \neq 0$. Dann gibt es eindeutige $q : \mathbb{Z}$, $r : \mathbb{N}$ mit

$a = b * q + r \wedge 0 \leqslant r < |b|$

$\square$

Truncated Division

$a = b * q + r \wedge \begin{cases} 0 \leqslant r < |b|, & \text{if } a \geqslant 0 \\ -|b| < r \leqslant 0, & \text{if } a \leqslant 0 \end{cases}$

$r : \mathbb{Z}$

Satz (Euklid auf $\mathbb{N}$)

$a, b : \mathbb{N}$, $b \neq 0$. Dann gibt es eindeutige $q : \mathbb{N}$, $r : \mathbb{N}$ mit

$a = b * q + r \wedge 0 \leqslant r < b$

$\square$

Beweis fuer Euklid auf $\mathbb{Z}$

4 Faelle

1. Fall $a \geqslant 0$, $b > 0$

Trivial

2. Fall $a \geqslant 0$, $b < 0$

Euklid $\mathbb{N}$ anwenden auf $(a, -b)$. Liefert

$a = (-b) * q + r \wedge 0 \leqslant r < -b$

Waehle $(q', r') = (-q, r) \qquad -b = |b|$

$a = b * (-q) + r \wedge 0 \leqslant r < |b|$

$a = b * q' + r' \wedge 0 \leqslant r' < |b|$

<u>3. Fall</u> $a < 0 \wedge b > 0$

Euklid $\mathbb{N}$ anwenden auf $(-a, b)$ Liefert q, r mit

$-a = b * q + r \wedge 0 \leqslant r < b$

<u>Sei $r = 0$</u> Waehle $(q', r') = (-q, 0)$ $\qquad b = |b|$

$a = b * (-q) - r \wedge 0 \leqslant r < |b|$

$a = b * q' + r \wedge 0 \leqslant r < |b|$

<u>Sei $1 \leqslant r \leqslant b - 1$</u> Waehle $(q', r') = (-(q + 1), b - r)$

$-a = b * q + r$

$a = b * (-q) - r$

$= b * (-q) - b + b - r$

$= b * (-q - 1) + (b - r)$

$= b * (-(q + 1)) + (b - r)$

$= b * q' + r'$

$$1 \leqslant \underbrace{b - r}_{r'} \leqslant b - 1 \begin{cases} 1 \leqslant r \to -r \leqslant -1 \to b - r \leqslant b - 1 \\ r \leqslant b - 1 \to 1 \leqslant b - r \end{cases}$$

<u>4. Fall</u> $a < 0$, $b < 0$ (??)

Aehnlich

---

10 Zehnte Woche

10.1 Eindeutigkeit

<u>Satz</u>

Seien $a, b : \mathbb{Z}$, $b \neq 0$. Dann gibt es eindeutige $q, r : \mathbb{Z}$ mit

$a = b * q + r \wedge 0 \leqslant r < |b|$

Eindeutigkeit Seien $a, b, q, r, q', r' : \mathbb{Z}$ mit $b \neq 0$

Es gelte:

$a = b * q + r \wedge 0 \leqslant r < |b|$
$a = b * q' + r' \wedge 0 \leqslant r' < |b|$

Dann gilt $q = q'$ unr $r = r'$.

Beweis:

$a = b * q + r$
$a = b * q' + r' \qquad -$

$0 = b(q - q') + (r - r')$
$\rightarrow |b||q - q'| = |r - r'|$

$0 \leqslant r' < |b|$
$0 \geqslant -r' < -|b|$

$-|b| < -r' \leqslant 0$
$0 \leqslant r < |b| \qquad +$

$-|b| < r - r' < |b|$ $\qquad \rightarrow$ echt kleiner $<$!

$\rightarrow |r - r'| < |b|$
$|b||q - q'| < |b|$

$\rightarrow |q - q'| < 1$

$\rightarrow q - q' = 0$

$\rightarrow q = q'$

also auch $r = r'$

Definition Seien $a, b, q, r : \mathbb{Z}$ mit $b \neq 0$
Es gelte:

$a = b * q + r \wedge 0 \leqslant r < |b|$

Nach Satz q, r eindeutig

Definiere Funktion:

$div_E, mod_E : \mathbb{Z} \times \mathbb{Z}^{\neq 0} \rightarrow \mathbb{Z}$

$a \, div_E \, b = div(a, b) = q$

$a \, mod_E \, b = mod(a, b) = r$ $\qquad$ ($E \rightarrow$ Euklid)

$div = div_E$
hier im Kurs!
$mod = mod_E$

10.2 GCD (Greatest Common Divisor)

Def Seien $a, b : \mathbb{Z}$

$D_{a,b} = \{d : \mathbb{Z} \mid d \backslash a \wedge d \backslash b\}$

Beispiele
$D_{5,14} = \{-5, -1, 1, 5\} \wedge \{-14, -7, -2, -1, 1, 2, 7, 14\}$

$= \{-1, 1\}$

$D_{3,0} = \{-3, -1, 1, 3\} \wedge \mathbb{Z} = \{-3, -1, 1, 3\}$

$= D_{-3,0}$

$D_{0,0} = \mathbb{Z} \cap \mathbb{Z} = \mathbb{Z}$ (0\0 bei uns!)

Satz Seien $a, b : \mathbb{Z}$

(1) $1 \in D_{a,b}$, also $D_{a,b} \neq \emptyset$

(2) $a \neq 0 \wedge d \in D_{a,b} \Rightarrow |d| \leqslant |a|$
$b \neq 0 \wedge d \in D_{a,b} \Rightarrow |d| \leqslant |b|$
$a \neq 0 \wedge b \neq 0 \wedge d \in D_{a,b} \Rightarrow |d| \leqslant min(|a|, |b|)$

Korollar (Folgesatz)

Seien $a, b : \mathbb{Z}$ mit $a \neq 0 \vee b \neq 0$

Dann hat $D_{a,b}$ groesstes Element (wegen (1) hat es ueberhaupt ein Element, wegen (2) ist jedes Element durch $|a|$ bzw. $|b|$ begrenzt)

□

Def (GCD) Seien $a, b : \mathbb{Z}$ mit $a \neq 0 \vee b \neq 0$

$gcd(a, b) = a\, gcd\, b = max(D_{a,b}) =$

$(max\, d : \mathbb{Z} \mid d \backslash a \wedge d \backslash b\ : d)$

$gcd(0, 0) = 0 \leftarrow$ (selber so definiert - nicht einheitlich)

$a \leqslant b$
$c \leqslant d \qquad +$

$a + c \leqslant b + d$

$a \leqslant b$
$c < d \qquad +$

$a + c < b + d \qquad (< !)$

< ist in diesem Fall wertvoller fuer den Beweis und deshalb behalten wir das so.

GCD $a, b : \mathbb{Z}$

Satz

$gcd(a, 0) = |a|$
$gcd(0, b) = |b|$ 0 ist neutrales Element von gcd
$gcd(a, a) = |a|$
$a\, gcd\, b = b\, gcd\, a$ Symmetrie
$gcd(a, 1) = 1$ 1 ist Null von gcd (Destruktor) $(a * 0 = 0)$ $(a\, gcd\, 1 = 1)$
$gcd(a, b) = gcd(a\, mod\, b, b)$
$a \backslash b \Rightarrow gcd(a, b) = a$
$gcd(0, 0) = 0$
$gcd(a, b) = gcd(|a|, |b|),\ k : \mathbb{Z}$

$gcd(a, b) = gcd(a + k * b, b) \qquad k : \mathbb{Z}$
$gcd(a, b) = gcd(a, b + k * a)$
$gcd(a, b) = gcd(a - k * b, b)$

Beweis

1. Fall: $a = b = 0 \qquad a - k * b = 0$ Trivial!

2. Fall: $a \neq 0 \vee b \neq 0$

Wir zeigen: $D_{a,b} = D_{a-k*b,b}$ damit auch GCDs gleich

$d \in D_{a,b}$

$<$ Def. $D_{a,b}$ $>$

$\Rightarrow d \backslash a \wedge d \backslash b$

$<$ Def. $\backslash$ mit $k_1, k_2 : \mathbb{Z}$ $>$

$\Rightarrow a = k_1 * d \wedge b = k_2 * d$

$<$ Einsetzen fuer $a - k * b$ $>$

$\Rightarrow a - k * b = k_1 * d - k * k_2 * d \wedge b = k_2 * d$

$<$ Arith. $>$

$\Rightarrow a - k * b = d(k_1 - k_2 * k) \wedge b = k_2 * d$

$<$ Def. $\backslash$ mit $k_1 - k * k_2 : \mathbb{Z}$ $>$

$\Rightarrow d \backslash (a - k * b) \wedge d \backslash b$

$<$ Def. $D_{a-k*b,b}$ $>$

$\Rightarrow d \in D_{a-k*b,b}$

1/2 $\square$

Bisher gezeigt: $D_{a,b} \subseteq D_{a-k*b,b}$

Aufgabe: Zeigen Sie $D_{a-k*b,b} \subseteq D_{a,b}$

$\square$

Satz $b \backslash a \Rightarrow r = 0$

Beweis $b \backslash a$, also $\exists k : \mathbb{Z}$ mit $a = k * b$

ausserdem $a = b * q + r \wedge 0 \leqslant r < |b|$ (*)
mit eindeutige $q, r : \mathbb{Z}$

Setze $q = k$ und $r = 0$. Diese erfuellt Bedingung (*)

Da q, r eindeutig, folgt $r = 0$.

Beweis 2

$b \backslash a$, also $\exists k : \mathbb{Z}$ mit $a = k * b$

ausserdem ist $a = b * q + r \wedge 0 \leqslant r < |b|$
also
$$k * b = b * q + r$$
also
$$r = b(k - q) < |b|$$

$r = b(k - q) \geqslant 0$
also
$$b(k - q) = |b(k - q)| = |b||k - q|$$

$r = b(k - q) = |b||k - q| < |b|$

also mit $b \neq 0$ und $|b| > 0$ gilt

$$|k - q| < 1$$
also
$$k - q = 0$$
also
$$k = q$$

also

$r = 0$

□

$a \backslash b$, also $\exists k_1 : \mathbb{Z}$ mit $b = k_1 * a$

---

11 Elfte Woche

11.1 Euklidischer Algorithmus

$\{a > 0 \wedge b > 0\}$

$(x, y) := (a, b);$

while $x \neq y$ do

invariante $gcd(x, y) = gcd(a, b) \wedge x > 0 \wedge y > 0$

if $x > y$ then

$x := x - y$

else // $x < y$ (assert $x < y$)

$y := y - x$

endif

endwhile

postcondition: $\{x = y = gcd(a, b)\}$

Beweis

$\{(gcd(x, y) = gcd(a, b))^{Ⓐ} \wedge (x > 0)^{Ⓑ} \wedge (y > 0)^{Ⓒ} \wedge (x \neq y)^{Ⓓ} \wedge (x > y)^{Ⓔ}\}$

$\Rightarrow$

$\{(gcd(x - y, y) = gcd(a, b))^{①} \wedge (x - y > 0)^{②} \wedge (y > 0)^{③}\}$

$x := x - y$

$\{(gcd(x, y) = gcd(a, b)) \wedge (x > 0) \wedge (y > 0)\}$

① $gcd(x, y) = gcd(a, b)$ Ⓐ

$\quad < gcd(a, b) = gcd(a - k * b, b) >$

$\Rightarrow gcd(x - 1 * y, y) = gcd(a, b)$

② $x > y$ Ⓔ

$\Rightarrow x - y > 0$

③ $=$ Ⓒ

<u>Inv</u> $\{a > 0 \wedge b > 0\}$

$\{gcd(a, b) = gcd(a, b) \wedge a > 0 \wedge b > 0$

$(x, y) := (a, b)$

$\{gcd(x, y) = gcd(a, b) \wedge x > 0 \wedge y > 0$

$\{gcd(x, y) = gcd(a, b) \wedge x > 0 \wedge y > 0 \wedge x = y$

$\Rightarrow x = y = gcd(a, b)$

$gcd(x, y) = gcd(x, x) = x = gcd(a, b)$ ✓

---

12 Zwoelfte Woche

12.1 GCD langsam-schnell

$x\, mod\, y = 0 \rightarrow$ Stop bei schnellem Algorithmus. $gcd(a, b) = gcd(0, y) = y, \qquad x, y \geqslant 0$

$x = y \rightarrow$ Stop bei langsamen Algorithmus. $gcd(a, b) = gcd(x, x) = x, \qquad x, y > 0$

$gcd(a, b) \overset{*}{=} gcd(b, a\, mod\, b)$

$a, b, k : \mathbb{Z}$

$gcd(a, b) \overset{1}{=} gcd(a - k * b, b)$

Sei $b \neq 0$

$a = b * q + r \wedge 0 \leqslant r < |b|, \qquad q = a\,div\,b, \qquad r = a\,mod\,b$

$a = b * (a\,div\,b) + (a\,mod\,b)$

$a\,mod\,b \overset{②}{=} a - b * (a\,div\,b)$

$gcd(a, b)$

$< ① >$

$= gcd(a - k * b, b)$

$<$ setze $k = a\,div\,b >$

$= gcd(a - (a\,div\,b) * b, b)$

$< ② >$

$= gcd(a\,mod\,b, b) =^{<symm.>} gcd(b, a\,mod\,b)$

12.2 Euklid schnell

$\{a \geqslant 0 \wedge b \geqslant 0\}$

$(x, y) := (a, b);$

while $y \neq 0$ do

invariante $gcd(a, b) = gcd(x, y) \wedge x \geqslant 0 \wedge y \geqslant 0$

$(x, y) = (y, x\,mod\,y)$

endwhile

$\{x = gcd(a, b)\}$

$\rightarrow$ rueckwerts einsetzen

Invar. Schleifenbedingung

$\{(gcd(a, b) = gcd(x, y))^{①} \wedge (x \geqslant 0)^{②} \wedge (y \geqslant 0)^{③} \wedge (y \neq 0)^{④}\}$

VC
$\Rightarrow$

$\{(gcd(a, b) = gcd(y, x\,mod\,y))^{Ⓐ} \wedge (y \geqslant 0)^{Ⓑ} \wedge (x\,mod\,y)^{Ⓒ}\}$ (PRE)

$(x, y) = (y, x\,mod\,y)$

$\{(gcd(a,b) = gcd(x,y)) \wedge (x \geqslant 0) \wedge (y \geqslant 0)\}$ (POST=inv)

Wir wissen: ① $\wedge$ ② $\wedge$ ③ $\wedge$ ④
Zu zeigen: Ⓐ, Ⓑ, Ⓒ

Ⓐ: $gcd(a,b) =^{①} gcd(x,y) =^{(*)} gcd(y, x \, mod \, y)$ ✓

Ⓑ: ③ $\Rightarrow$ Ⓑ ✓

Ⓒ: 'mod' immer $\geqslant 0$, und $y \neq 0$ wegen ④

12.3 Erweiterter Euklid

Satz Seien $a, b : \mathbb{Z}$ Dann gibt es Zahlen

$u, v : \mathbb{Z}$ mit

$u * a + v * b = gcd(a,b)$ (Bezout-Identitaet)

$\rightarrow$ nicht eindeutig $\rightarrow$ unendlich

□

Wir konstruieren u und v fuer $a, b : \mathbb{N}$ durch Erweiterter Euklid

$u * a + v * b = gcd(a,b)$

$u' * a + v' * b = 0$

$(u + u') * a + (v + v') * b = gcd(a,b)$

Waehle z.B. $u' = b$ und $v' = -a$

$\{a \geqslant 0 \wedge b \geqslant 0\}$

$(x, y) = (a, b)$

$(u, u') = (1, 0)$

(v, v')

$sign = +1$

while $y \neq 0$

I_1 $\quad$ invariante $gcd(x, y) = gcd(a, b) \wedge x \geqslant 0 \wedge y \geqslant 0$
I_2 $\quad u * x + u' * y = a$
I_3 $\quad v * x + v' * y = b$
I_4 $\quad u * v' - u' * v = sign$

$(I_1, I_2, I_3, I_4$ unverknuepft)

do

$(q, r) = (x\ div\ y, x\ mod\ y)$

$(x, y) = (y, r)$

$(u, u') = (q * u + u', u)$

$(v, v') = (q * v + v', v)$

$sign = -sign$

endwhile

Post: $\{x = gcd(a, b) \wedge$
$u * x = a \wedge$
$v * x = b \wedge$
$(sign * v') * a + (-sign * u') * b = gcd(a, b)\}$

---

13 Dreizehnte Woche

13.1 GCD (Fortsetzung)

$a, b : \mathbb{Z}$ Dann gibt es $u, v : \mathbb{Z}$ mit

$u * a + v * b = gcd(a, b)$

Zeigen Sie

$c \backslash a$ 1 $\quad \wedge\, c \backslash b$ 2 $\quad \equiv c \backslash gcd(a, b)$

1) "$\Leftarrow$"

Sei $d = gcd(a, b)$

$c \backslash d$

d ist gcd von a und b. Also ist d cd (common divisor) von a und b. Also $d \backslash a \wedge d \backslash b$

$c \backslash d \wedge d \backslash a$, also $c \backslash a$
$c \backslash d \wedge d \backslash b$, also $c \backslash b$

Transitivitaet $\backslash$

2) "$\Rightarrow$"

$c \backslash a \wedge c \backslash b$, also

$\exists k_1 : \mathbb{Z}$ mit $a = k_1 * c$
$\exists k_2 : \mathbb{Z}$ mit $b = k_2 * c$

Es gibt $u, v : \mathbb{Z}$ mit

$$u * a + v * b = gcd(a, b)$$

also

$$u * (k_1 * c) + v * (k_2 * c) = gcd(a, b)$$

also

$$\underbrace{(u * k_1 + v * k_2)}_{\mathbb{Z}} * c = gcd(a, b)$$

also

$$c \backslash gcd(a, b)$$

13.2 Restklassen

Def (Menge der Reste modulo n)

$\mathbb{Z}_n = \{a : \mathbb{Z} \mid 0 \leqslant a < n\}$

Beispiel

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

Arithmetik

$+_n, *_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

$a +_n b = (a + b) mod\, n$
$a *_n b = (a * b) mod\, n$

Def Sei M eine Menge und $\circ$ eine Operation mit $\circ : M \times M \to M$. Das Paar $(M, \circ)$ heisst Gruppe, wenn:

1. Es gibt ein $e : M$ mit
   $a \circ e = a = e \circ a$ fuer alle $a : M$ (Identitaete, neutr. Element)

2. Es gilt

$(a \circ b) \circ c = a \circ (b \circ c)$ (Assoziativitaet)

3. Zu jedem $a : M$ gibt es ein $b : M$ mit
$a \circ b = e = b \circ a$ (inverses Element) (e: neutr. Elem. aus 1.)

Beispiel $(\mathbb{Z}_n, +_n)$

1. $0 +_n a = a = a +_n 0$

Beweis

$0 +_n a$

$= (0 + a)\, mod\, a$

$= a\, mod\, n$

$= a$ ✓ (weil $0 \leqslant a < n$)

2. $(a +_n b) +_n c = a +_n (b +_n c)$

Bew.

$(a +_n b) +_n c$

$= ((a + b)\, mod\, n + c)\, mod\, n$
$[a + b = n * q + (a + b)\, mod\, n] \in: \mathbb{Z}$

$= ((a + b) - n * q + c)\, mod\, n$

$= ((a + b) + c)\, mod\, n$

$= (a + (b + c))\, mod\, n$

$=$ das gleiche rueckwerts

3. $a +_n ((-a)\, mod\, n)$ $\leftarrow$ inverses Element zu a

$= (a + (-a)\, mod\, n)\, mod\, n$

$= (a + (-a))\, mod\, n$

$= 0\, mod\, n$

$= 0$ ✓

Beispiel $(\mathbb{Z}_n, *_n)$

1) $1 *_n a = a = a *_n 1$

2) $(a *_n b) *_n c = a *_n (b *_n c)$

3) im allgemeinen nicht erfuellt

Def. (reduzierte Menge der Reste modulo n)

$$\mathbb{Z}_n^* = \{a : \mathbb{Z} \mid 0 \leqslant a < n \wedge gcd(a, n) = 1\}$$

Beispiel $\quad \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
$gcd(0, 6) \quad$ 1 2 3 2 1

$$\mathbb{Z}_6^+ = \{1, 5\}$$

$gcd(a, 1) = 1$

Es gibt $u, v : \mathbb{Z}$ mit

$$u * a + v * n = 1$$

also

$$(u * a + v * n) \; mod \, n = 1 \; mod \, n$$

also

$$(u * a) \; mod \, n = 1$$

also

$$u *_n a = 1$$

Wir brauchen dazu noch ein Algorithmus (erweit. Euklid) ohne v um Werte zu berechnen.

Beispiel:

$1 *_6 1 = 1$

$5 *_6 5 = 1$

Also: $(\mathbb{Z}_n^{*\,!}, *_n)$ ist eine Gruppe

Aufgabe: Tabelle fuer $(\mathbb{Z}_{15}^*, *_{15})$
