DIENSTAG 9.3.2021 VORMITTAG

SINGULAR

2+2;

int a = 2;

Name : a
Typ : int, Element von $\mathbb{Z}$
der Wert : 2

Deklaration

a = 3;

Anweisung

n++;   n = n + 1;

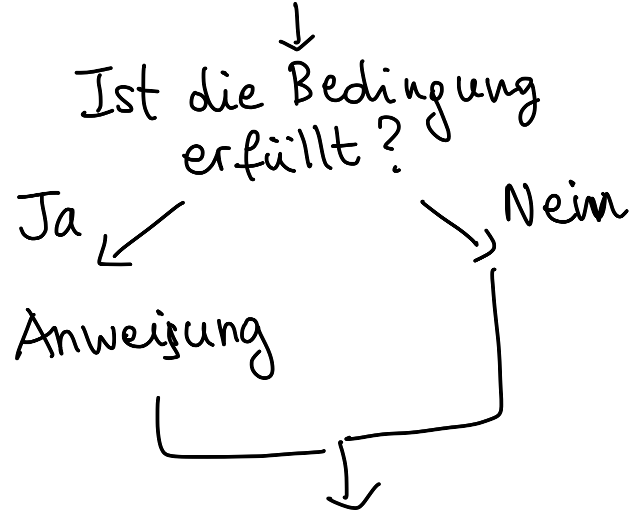
Boolesche Ausdrücke:

(3 > 2)   wahr   1

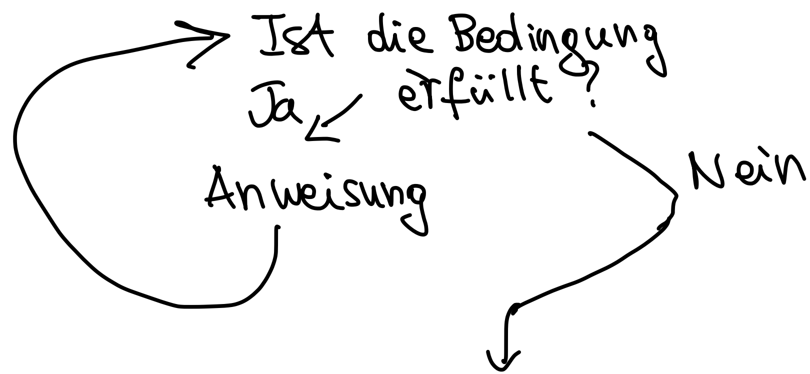
(3 < 2)   falsch   0

3 == 2   falsch   0

```
if (BEDINGUNG) {
    ANWEISUNG
}
```




```
while (BEDINGUNG) {
    ANWEISUNG
}
```



Beispiel 1.10

4!

ITERATION

```
int i = 1;
int s = 1;
while (i<=4) {
      s = s*i;
      i++;
}
s;
```

running index

partial result

s=1

s=2

s=6

s=24

Funktionen

$$f: A \to B$$
$$a \mapsto f(a)$$

```
proc NAME(INPUT) {
    ⋮
  RETURN (OUTPUT)
}
```

INPUT → typ Name der Variablen

Beispiel 1.12

```
proc Factorial (int n) {
    int i = 1;
    int s = 1;
    while (i<=n) {
        s = s*i;
        i++;
    }
    return(s);
}
```

REKURSION

Beispiel 1.14

```
proc Fact(int n) {
    if (n==1) {
        return(1);
    }
    return(n * Fact(n-1));
}
```

$$\begin{aligned} Fact(4) &= 4 \cdot Fact(3) = \\ &= 4 \cdot (3 \cdot Fact(2)) \\ &= 4 \cdot (3 \cdot (2 \cdot Fact(1))) \\ &= 4 \cdot 3 \cdot 2 \cdot 1 \end{aligned}$$

Integers $\mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$

$\mathbb{Z}$ ist ein Ring: es gibt zwei Operationen $+$ und $\cdot$

- $(\mathbb{Z}, +)$ abelsche Gruppe
- $\cdot$ associativ
- $a(b+c) = ab + ac$
- neutrales Element bezüglich $\cdot$: 1

```
int a = 1;
int b = 2;

a+b;
a*b;
```

Satz (Teilung / Division) $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $b \neq 0$.

$\Rightarrow \underbrace{\exists!}_{\text{es gibt und sie sind eindeutig bestimmt}}$ $q \in \mathbb{Z}$ und $r \in \mathbb{Z}$ mit $a = qb + r$ und

$$0 \leq r < |b|$$

q = Quotient

r = Rest

$b > 0$

a div b; Quotient in der Teilung von a durch b

a mod b; Rest

Def $a, b \in \mathbb{Z}$

$$b \mid a \iff \exists c \in \mathbb{Z} : a = bc$$

b ist ein Teiler von a
Divisor

b teilt a

a ist durch b teilbar

Def Eine PRIMZAHL ist $p \in \mathbb{Z}$

- $p \neq 0$, $p \neq \pm 1$
- die einzigen Divisoren von p sind $\pm 1, \pm p$

Fundamentalsatz Arithmetik (Primfaktorzerlegung in $\mathbb{Z}$)

$n \in \mathbb{Z}$, $n \neq 0$

$\Rightarrow \exists!\ c \in \{\pm 1\}$, $p_1, \dots, p_s$ Primzahlen

$\alpha_1, \dots, \alpha_s \in \mathbb{N}^+$

$$2 \leq p_1 < p_2 < \dots < p_s$$

$$n = c\, p_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

$$12 = 2^2 \cdot 3$$

$$12 = 3 \cdot 4$$

Größter gemeinsamer Teiler

Def $a, b \in \mathbb{Z}$. Der ggT von a und b ist das einzige ganze Zahl $d \in \mathbb{Z}$:

- $d \geq 0$
- $d \mid a$, $d \mid b$
- $\forall c \in \mathbb{Z}$, $c \mid a$, $c \mid b \Rightarrow c \mid d$

d existiert, ist eindeutig bestimmt, $d =: \gcd(a,b)$

$72 = 8 \cdot 9 = 2^3 \cdot 3^2$

$60 = 6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5 = 2^2 \cdot 3 \cdot 5$

$\gcd(72, 60) = 2^2 \cdot 3 = 12$

Hilfssatz $a, b, q, r \in \mathbb{Z}$ mit $a = qb + r$.

$\Rightarrow \gcd(a, b) = \gcd(b, r)$

Beispiel 2.11 (Euklidischer Algorithmus)

$\gcd(2002, 420) = \gcd(420, 322) = \gcd(322, 98) =$

$2002 = 4 \cdot 420 + 322$ $\quad$ $420 = 322 + 98$

$= \gcd(98, 28) = \gcd(28, 14) = \gcd(14, 0) = 14$

$322 = 3 \cdot 98 + 28$ $\quad$ $98 = 3 \cdot 28 + 14$ $\quad$ $28 = 2 \cdot 14 + 0$

$$\boxed{\begin{array}{l} \forall a \in \mathbb{Z} \\ \gcd(a, 0) = |a| \end{array}}$$

Aufgabe 1.5.1

1.5.2

1.6.1, 1.7.1

1.6.2, 1.7.2

1.6.3

2.1.1 istPrim

2.2.2 ggT (Euklidischer Algorithmus)