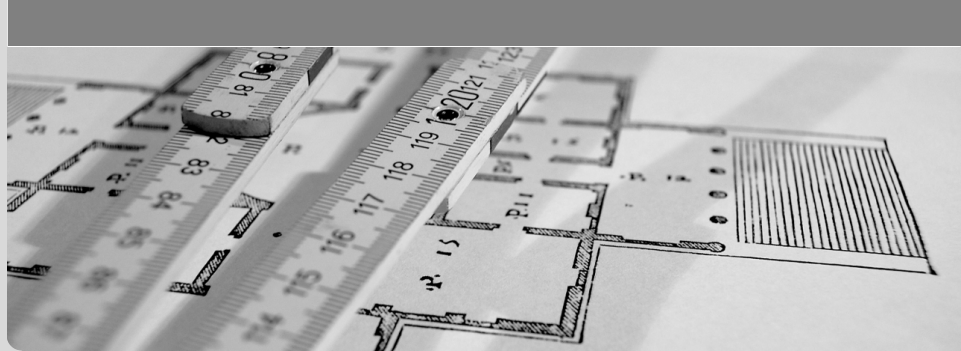


GBI Tutorium Nr.

Foliensatz 0333

Vincent Hahn – vincent.hahn@student.kit.edu | 6. November 2012



- 1 Division mit Rest
- 2 Algorithmen
- 3 Schleifeninvarianten

- 1 Division mit Rest
- 2 Algorithmen
- 3 Schleifeninvarianten

Definition

$$\forall x \in \mathbb{N}_0, \forall y \in \mathbb{N}_+ : \\ x = y \cdot (x \operatorname{div} y) + (x \bmod y)$$

Hierbei ist div die Ganzzahldivision ohne Rest.

Beispiel

Den Rest a der Ganzzahldivision erhält man also mit $a = x \bmod y$:

$$1 = 4 \bmod 3$$

Definition

$$\forall x \in \mathbb{N}_0, \forall y \in \mathbb{N}_+ : \\ x = y \cdot (x \operatorname{div} y) + (x \bmod y)$$

Hierbei ist div die Ganzzahldivision ohne Rest.

Beispiel

Den Rest a der Ganzzahldivision erhält man also mit $a = x \bmod y$:

$$1 = 4 \bmod 3$$

Folgerung

Aus der Definition kann direkt geschlossen werden:

$$\begin{aligned}x \operatorname{div} y &\in \mathbb{N}_0 \\x \operatorname{mod} y &\in \{0, \dots, y - 1\}\end{aligned}$$

mündlich

x	y	$x \text{ div } y$	$x \bmod y$
4	3		
2	1		
10	3		
8	3		
9	2		
4	3		

mündlich

x	y	$x \text{ div } y$	$x \bmod y$
4	3	1	1
2	1		
10	3		
8	3		
9	2		
4	3		

mündlich

x	y	$x \text{ div } y$	$x \bmod y$
4	3	1	1
2	1	2	0
10	3		
8	3		
9	2		
4	3		

mündlich

x	y	$x \text{ div } y$	$x \bmod y$
4	3	1	1
2	1	2	0
10	3	3	1
8	3		
9	2		
4	3		

mündlich

x	y	$x \text{ div } y$	$x \bmod y$
4	3	1	1
2	1	2	0
10	3	3	1
8	3	2	2
9	2		
4	3		

mündlich

x	y	$x \text{ div } y$	$x \bmod y$
4	3	1	1
2	1	2	0
10	3	3	1
8	3	2	2
9	2	4	1
4	3		

mündlich

x	y	$x \text{ div } y$	$x \bmod y$
4	3	1	1
2	1	2	0
10	3	3	1
8	3	2	2
9	2	4	1
4	3	1	1

Definition

Der größte gemeinsame Teiler zweier Zahlen ist die größtmögliche Zahl $m \in \mathbb{N}_0$, für die gilt:

$$a \operatorname{div} m = 0 \wedge b \operatorname{div} m = 0$$

Bestimmung

Der größte gemeinsame Teiler kann mit Primfaktorzerlegung bestimmt werden:

$$\begin{aligned} a &= 3528, b = 3780 \\ \Rightarrow a &= 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^2 \\ \Rightarrow b &= 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1 \end{aligned}$$



Definition

Der größte gemeinsame Teiler zweier Zahlen ist die größtmögliche Zahl $m \in \mathbb{N}_0$, für die gilt:

$$a \operatorname{div} m = 0 \wedge b \operatorname{div} m = 0$$

Bestimmung

Der größte gemeinsame Teiler kann mit Primfaktorzerlegung bestimmt werden:

$$a = 3528, b = 3780$$

$$\Rightarrow a = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^2$$

$$\Rightarrow b = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1$$

Programmierung

Die *ggt*-Funktion lässt sich so programmieren:

$$\text{ggt}(a, b) = \begin{cases} a & \text{falls } b = 0 \\ \text{ggt}(b, a \bmod b) & \end{cases}$$

- 1 Division mit Rest
- 2 Algorithmen**
- 3 Schleifeninvarianten

Eigenschaften

Ein Algorithmus. . .

- hat eine endliche Beschreibung,
- besteht aus elementaren Aussagen,
- ist deterministisch,
- gibt endliche Ausgabe auf endliche Eingabe aus,
- hat endlich viele Schritte,
- ist skalierbar
- und ist nachvollziehbar

Eigenschaften

Ein Algorithmus. . .

- hat eine endliche Beschreibung,
- besteht aus elementaren Aussagen,
- ist deterministisch,
- gibt endliche Ausgabe auf endliche Eingabe aus,
- hat endlich viele Schritte,
- ist skalierbar
- und ist nachvollziehbar

Eigenschaften

Ein Algorithmus. . .

- hat eine endliche Beschreibung,
- besteht aus elementaren Aussagen,
- ist deterministisch,
- gibt endliche Ausgabe auf endliche Eingabe aus,
- hat endlich viele Schritte,
- ist skalierbar
- und ist nachvollziehbar

Eigenschaften

Ein Algorithmus. . .

- hat eine endliche Beschreibung,
- besteht aus elementaren Aussagen,
- ist deterministisch,
- gibt endliche Ausgabe auf endliche Eingabe aus,
- hat endlich viele Schritte,
- ist skalierbar
- und ist nachvollziehbar

Eigenschaften

Ein Algorithmus. . .

- hat eine endliche Beschreibung,
- besteht aus elementaren Aussagen,
- ist deterministisch,
- gibt endliche Ausgabe auf endliche Eingabe aus,
- hat endlich viele Schritte,
- ist skalierbar
- und ist nachvollziehbar

Eigenschaften

Ein Algorithmus. . .

- hat eine endliche Beschreibung,
- besteht aus elementaren Aussagen,
- ist deterministisch,
- gibt endliche Ausgabe auf endliche Eingabe aus,
- hat endlich viele Schritte,
- ist skalierbar
- und ist nachvollziehbar

Eigenschaften

Ein Algorithmus. . .

- hat eine endliche Beschreibung,
- besteht aus elementaren Aussagen,
- ist deterministisch,
- gibt endliche Ausgabe auf endliche Eingabe aus,
- hat endlich viele Schritte,
- ist skalierbar
- und ist nachvollziehbar

Arten

while Wiederholen, wenn eine Bedingung erfüllt ist.

for n -Mal wiederholen.

do-while Wiederholen, danach nochmal, wenn eine Bedingung erfüllt ist.

Arten

while Wiederholen, wenn eine Bedingung erfüllt ist.

for n -Mal wiederholen.

do-while Wiederholen, danach nochmal, wenn eine Bedingung erfüllt ist.

Arten

while Wiederholen, wenn eine Bedingung erfüllt ist.

for n -Mal wiederholen.

do-while Wiederholen, danach nochmal, wenn eine Bedingung erfüllt ist.

Beispiel 1

Input: $x \in \mathbb{N}$

$i \leftarrow 0$

while $x > 1$ **do**

$x \leftarrow x \text{ div } 2$

$i \leftarrow i + 1$

od

Output: i

Beispiel 2

```
 $k \leftarrow 0$   
for  $i \leftarrow 0$  to 20 do  
     $k \leftarrow i$   
od  
Output:  $k$ 
```

Beispiel 3

Gegeben sei ein Wort w der Länge $|w| = n$. Das Array W hat an i -ter Stelle den i -ten Buchstabe von w . w ist ϵ -frei.

$c \leftarrow 0$

for $i \leftarrow 0$ **to** $n - 1$ **do**

$$c \leftarrow \begin{cases} c + 1 & \text{falls } W[i] = x \\ c & \text{sonst} \end{cases}$$

od

Output: c

Übung 1, Winter 2008/2009

Es sei A ein Alphabet.

Schreiben Sie einen Algorithmus auf, der folgendes leistet: Als Eingaben erhält er ein Wort w über A und zwei Symbole $x \in A$ und $y \in A$. Am Ende soll eine Variable r den Wert 0 oder 1 haben, und zwar soll gelten:

$$r = \begin{cases} 1 & \text{falls irgendwo in } w \text{ direkt hintereinander erst } x \text{ dann } y \text{ vorkommt} \\ 0 & \text{sonst} \end{cases}$$

Benutzen Sie zum Zugriff auf das i -te Symbol von w die Schreibweise $w(i)$. Formulieren Sie den Algorithmus mit Hilfe einer for-Schleife.

- 1 Division mit Rest
- 2 Algorithmen
- 3 Schleifeninvarianten**

Definition

Eine Schleifeninvariante ist eine Eigenschaft einer Schleife, die bei jedem Schleifenzeitpunkt gültig ist.

Hä?

Eine Schleifeninvariante ist zum Beispiel

- ein Wertebereich für eine Variable oder
- ein Verhältnis zweier Variablen.

Definition

Eine Schleifeninvariante ist eine Eigenschaft einer Schleife, die bei jedem Schleifenzeitpunkt gültig ist.

Hä?

Eine Schleifeninvariante ist zum Beispiel

- ein Wertebereich für eine Variable oder
- ein Verhältnis zweier Variablen.

Wofür?

Mit Schleifeninvarianten lassen sich Algorithmen überprüfen.

Wie?

Mit vollständiger Induktion :-)

Wofür?

Mit Schleifeninvarianten lassen sich Algorithmen überprüfen.

Wie?

Mit vollständiger Induktion :-)

Beispiel

Input: $a, b \in \mathbb{N}_0$

$S \leftarrow a$

$Y \leftarrow b$

for $i \leftarrow 0$ **to** $b - 1$ **do**

$S \leftarrow S - 1$

$Y \leftarrow Y - 1$

od

Output: S

Übung

Algorithmus mit $a = 3$ und $b = 4$ ausprobieren und Werte für S und Y bei jedem Schleifendurchlauf finden.

Beispiel

Input: $a, b \in \mathbb{N}_0$

$S \leftarrow a$

$Y \leftarrow b$

for $i \leftarrow 0$ **to** $b - 1$ **do**

$S \leftarrow S - 1$

$Y \leftarrow Y - 1$

od

Output: S

Übung

Algorithmus mit $a = 3$ und $b = 4$ ausprobieren und Werte für S und Y bei jedem Schleifendurchlauf finden.

Winter 2008/2009

Input: $a, b \in \mathbb{N}_0$

$X_0 \leftarrow a$

$Y_0 \leftarrow b$

$P_0 \leftarrow 1$

$Z_0 \leftarrow X_0 \bmod 2$

$n \leftarrow 1 + \lceil \log_2 a \rceil$

for $i \leftarrow 0$ **to** $n - 1$ **do**

$P_{i+1} \leftarrow P_i \cdot Y_i^{Z_i}$

$X_{i+1} \leftarrow X_i \operatorname{div}$

$Y_{i+1} \leftarrow Y_i^2$

$Z_{i+1} \leftarrow X_{i+1} \bmod 2$

od

Beweisen Sie durch
vollständige Induktion über i
die Schleifeninvariante:

$$\forall i \in \mathbb{N}_0 : P_i \cdot Y_i^{X_i} = b^a$$