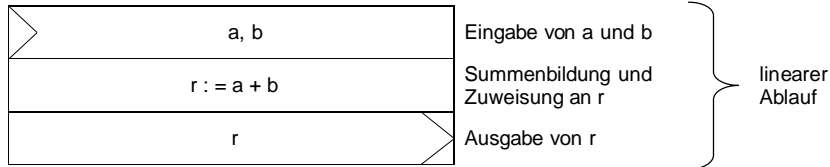


Struktogramme

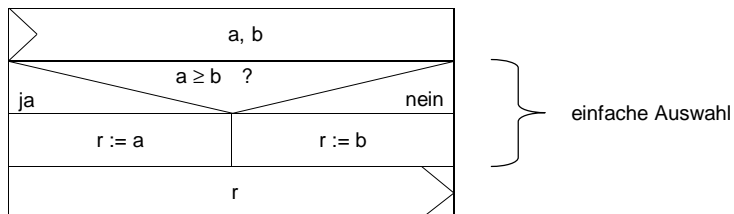
nach Nassi-Shneiderman

<http://de.wikipedia.org/wiki/Nassi-Shneiderman-Diagramm>

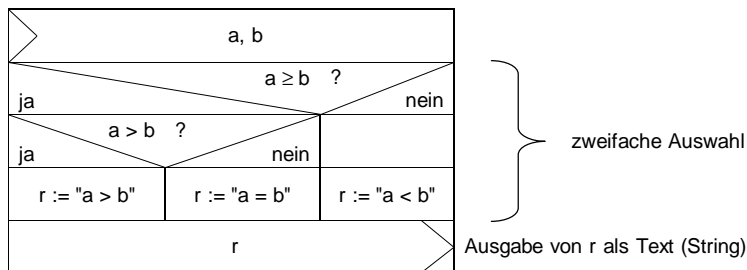
1. Addition von a und b



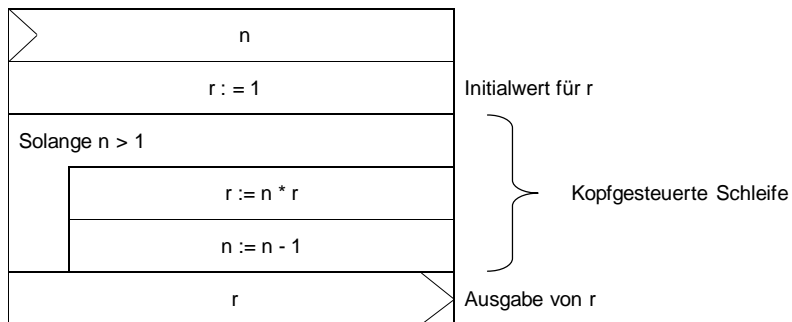
2. Bestimme das Maximum von a und b



3. Welche Zahl ist grösser: a oder b?

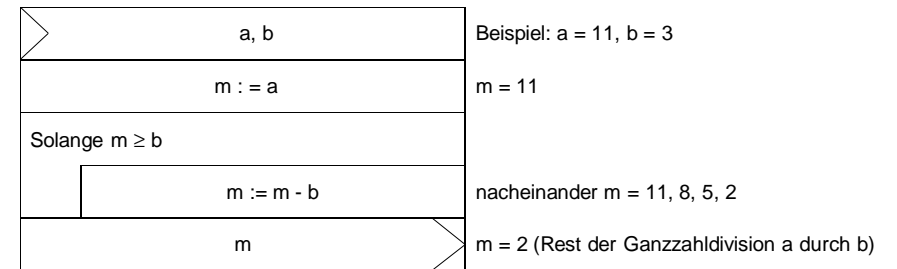


4. Fakultät n!

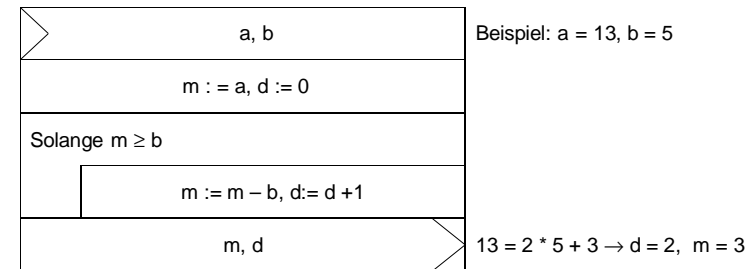


5. Bestimme a mod b mit a, b ∈ N

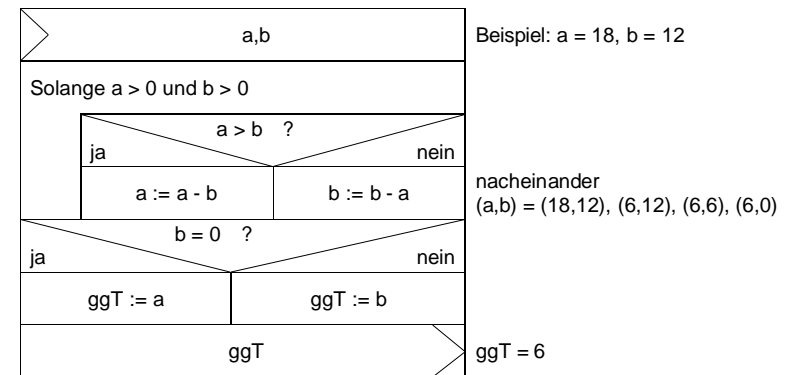
Annahme: Der Rechner kenne nur die Subtraktion, keine Division.



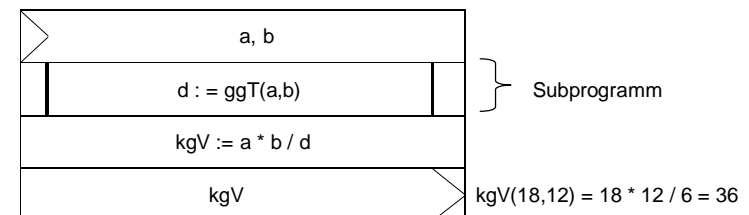
6. Erweitere um das Ergebnis d der Ganzzahldivision



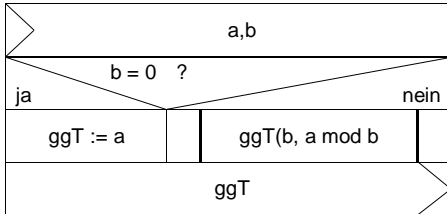
7. Grösster gemeinsamer Teiler ggT(a,b)



8. Kleinstes gemeinsames Vielfaches kgV(a,b)

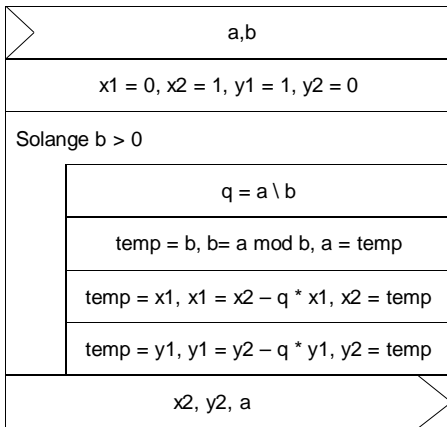


9. ggT(a,b) rekursiv



Programm ruft sich selber neu auf (rekursiv)

10. Erweiterter Euklidischer Algorithmus



Ziel: $x \cdot a + y \cdot b = \text{ggT}(a,b)$

Ganzzahldivision

temp ist Zwischenspeicher

Ausgabe von x, y, und ggT

Erweiterter Euklid am Beispiel ggT(38,14)

Anders als im Code wird hier zuerst einzig der ggT ermittelt.
Man durchläuft dann die einzelnen Schritte rückwärts und findet x und y.

$$38 = 2 \cdot 14 + 10 \rightarrow 10 = 38 - 2 \cdot 14 \rightarrow 2 = 3 \cdot (38 - 2 \cdot 14) - 2 \cdot 14 = 3 \cdot 38 - 8 \cdot 14 = 10$$

$$14 = 1 \cdot 10 + 4 \rightarrow 4 = 14 - 1 \cdot 10 \rightarrow 2 = 10 - 2 \cdot (14 - 10) = 3 \cdot 10 - 2 \cdot 14 = 4$$

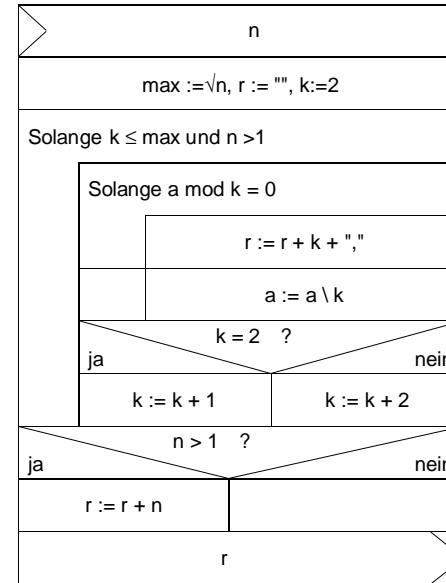
$$10 = 2 \cdot 4 + 2 \rightarrow 2 = 10 - 2 \cdot 4 = 2$$

$$4 = 2 \cdot 2 + 0 \rightarrow \text{ggT} = 2$$

Wir finden für $x \cdot 38 + y \cdot 14 = \text{ggT}$, d.h. $3 \cdot 38 - 8 \cdot 14 = 114 - 112 = 2$

Der erweiterte Euklid wird benötigt, um beim bekannten RSA-Verschlüsselungsverfahren (verwendet im Verkehr mit Banken) den Entschlüsselungscode zu konstruieren.

11. Zerlegung einer natürlichen Zahl n in ihre Primfaktoren



Beispiele n = 12 und n=15

Es gibt höchstens einen Primfaktor $> \max$.
r wird als vorerst leerer String definiert.

Ganzzahldivision; mehrere gleiche k möglich

Jeder neue Faktor wird an r angehängt

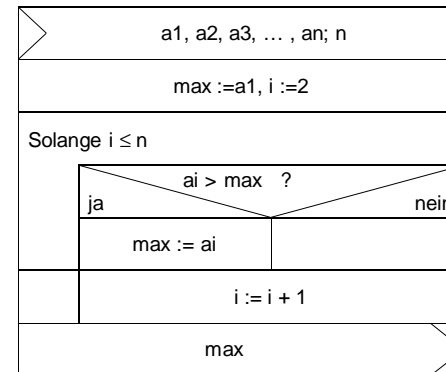
Ganzzahldivision

k wird erhöht
Ab k = 3 werden nur ungerade k abgefragt

Hier gilt "ja", falls ein Primfaktor $> \max$ ist.

r = "2, 2, 3," und r = "5, 5,"

12. Bestimme das Maximum der Zahlen a1, a2, a3, ..., an

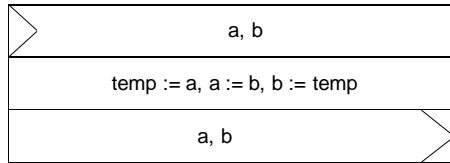


Beispiel: 5, 2, 7, 1; 4

max nimmt nacheinander die Werte 5, 5, 7, 7 an

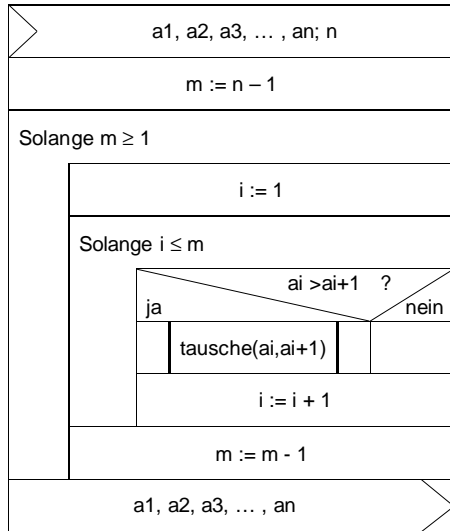
max = 7

13. Unterprogramm "tausche" die Werte von a und b



Eine der beiden Zahlen muss temporär zwischengespeichert werden.
Die Variablen a und b haben nun die Werte vertauscht.

14. Sortieren vom Kleinen zum Grossen (Algorithmus "Bubble-Sort")

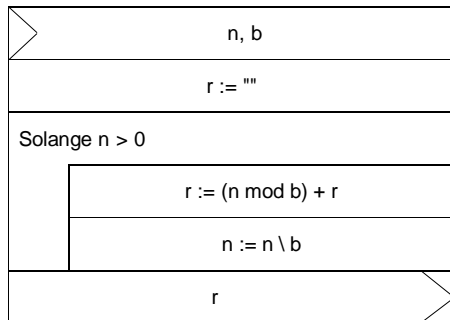


Beispiel: 5,2,7,1;4

nacheinander, nach jeweils einem Tausch
 m = 3, i = 1: (2,5,7,1)
 m = 3, i = 3: (2,5,1,7)
 m = 2, i = 2: (2,1,5,7)
 m = 1, i = 1: (1,2,5,7)

Resultat: 1,2,5,7

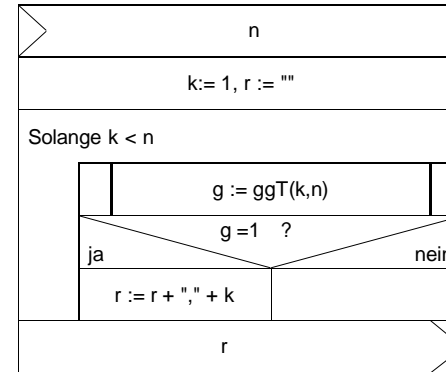
15. Basiswechsel: Gegeben Zahl n im Zehnersystem und eine neue Basis 2 ≤ b ≤ 9



Beispiel: 126, 4

nacheinander:
 (r,n) = ("2", 31), ("32", 7), ("332", 1), ("1332", 0)
 $r = "1332" = 1 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4^1 + 2 \cdot 4^0 = 64 + 48 + 12 + 2 = 126$

16. Welche Zahlen kleiner n sind zu n teilerfremd (können mit n nicht gekürzt werden)?



Beispiele: 3, 6

max nimmt nacheinander die Werte 5, 5, 7, 7 an
 3 → r = ",1, 2", 6 → r = ",1,5")

Die Anzahl der zu n teilerfremden Zahlen ist die berühmte Eulersche j -Funktion:

$j(3) = 2, j(6) = 2, j(7) = 6, j(11) = 10$

Falls n eine Primzahl p ist gilt $j(p) = p - 1$

Auch die Eulersche j -Funktion spielt beim RSA-Verschlüsselungsverfahren eine zentrale Rolle.

27.8.09, Gerold Brändli