Serie 1

Aufgabe 1

Erstellen Sie eine Funktion, die den größten gemeinsamen Teiler der Zahlen a und b (ggT(a, b)) berechnet.

Hinweis: Beim euklidischen Algorithmus wird in aufeinanderfolgenden Schritten jeweils eine Division mit Rest durchgeführt, wobei der Rest im nächsten Schritt zum neuen Divisor wird. Der Divisor, bei dem sich Rest 0 ergibt, ist der größte gemeinsame Teiler der Ausgangszahlen.

Beispiel:
Wir wollen den ggT von 93 und 42 berechnen

$$\begin{aligned} 93 &= 2 \cdot 42 + 9 \\ 42 &= 4 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

ggT(93,42)=3 — Algorithmus endet wegen 0

Aufgabe 2

Implementieren Sie den erweiterten euklidischen Algorithmus.

Wir haben in der vorherigen Aufgabe den ggT zweier Zahlen berechnet, hier ggT(93,42)=3. Es gilt immer

$$\text{ggT}(a_0, a_1) = x \cdot a_0 + y \cdot a_1$$

In unserem Beispiel bedeutet das: $\text{ggT}(93, 42) = 3 = 5 \cdot 93 + (-11) \cdot 42$.
Mit Hilfe des erweiterten euklidischen Algorithmus können diese Zahlen x und y berechnet werden (diese werden später, z.B. beim RSA-Algorithmus benötigt). Wir wollen uns zunächst wieder ein Beispiel anschauen.

$$\begin{aligned} 93 &= 2 \cdot 42 + 9 \\ 42 &= 4 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

Wir starten mit der vorletzten Zeile und rechnen nun rückwärts:

$$
\begin{aligned}
3 &= 9 - 1 \cdot 6 \\
&= 9 - 1 \cdot (42 - 4 \cdot 9) \\
&= -42 + 5 \cdot 9 \\
&= -42 + 5 \cdot (93 - 2 \cdot 42) \\
&= 5 \cdot 93 + (-11) \cdot 42
\end{aligned}
$$

x y

Das obige Beispiel diente lediglich ihrem Verständnis, programmiertechnisch ist es nicht ratsam Formeln umzustellen.

Auf der folgenden Seite wird erklärt, wie Sie am besten die Werte berechnen: **Eingabe:** a_0 und a_1 als die zwei Eingabewerte

Ausgabe: a_{n-1}, x_{n-1} und y_{n-1}

Startbelegung: $x_0 = 1$, $x_1 = 0$, $y_0 = 0$ und $y_1 = 1$

Folgende Formeln müssen Sie implementieren:

$$
\begin{aligned}
q_i &= \lfloor a_{i-1}/a_i \rfloor \\
a_{i+1} &= a_{i-1} - q_i a_i \\
x_{i+1} &= x_{i-1} - q_i x_i \\
y_{i+1} &= y_{i-1} - q_i y_i
\end{aligned}
$$

Der Algorithmus endet, sobald $a_n = 0$

Beispiel

i	a_i	q_i	x_i	y_i
0	93	-	1	0
1	42	2	0	1
2	9	4	1	-2
3	6	1	-4	9
4	3	2	5	-11
5	0			

$x_{i+1} = x_{i-1} - q_i \cdot x_i$
$5 = 1 - 1 \cdot (-4)$