Der **Rechenaufwand** für den euklidischen Algorithmus hängt ab von

- dem Aufwand für einen Divisionsschritt
- der Anzahl der Divisionsschritte

Mit dem zweiten Punkt wollen wir uns etwas genauer beschäftigen.

(9.13) DEF: Seien $a, b \in \mathbb{N}$. Dann bezeichne $\mathrm{D}_{\mathbf{EA}}(a,b)$ die Anzahl der Divisionsschritte, die für die Berechnung von $\mathrm{ggT}(a,b)$ mit Hilfe des **EA** erforderlich sind.

Beispiele :

$a = 34\ ,\ b = 20$

$$\begin{aligned} 34 &= 1 \cdot 20 + 14 \\ 20 &= 1 \cdot 14 + 6 \\ 14 &= 2 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 \end{aligned}$$

$\mathrm{D}_{\mathbf{EA}}(34,20) = 4$

$a = 34\ ,\ b = 21$

$$\begin{aligned} 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

$\mathrm{D}_{\mathbf{EA}}(34,21) = 7$

Sind die Quotienten klein, so werden die Reste nur langsam kleiner, und es sind mehr Divisionsschritte auszuführen. Im zweiten Beispiel sind a und b gerade **Fibonacci–Zahlen**. Es ist nämlich $34 = F_9$ und $21 = F_8$, und für $\mathrm{ggT}(F_9, F_8)$ werden genau 7 Divisionen benötigt, d.h. $\mathrm{D}_{\mathbf{EA}}(F_9, F_8) = 7$. Allgemein gilt

(9.14) LEMMA: Für $n \geq 1$ gilt $\mathrm{ggT}(F_{n+2}, F_{n+1}) = 1$ und $\mathrm{D}_{\mathbf{EA}}(F_{n+2}, F_{n+1}) = n$

Bew: Bei Division von F_{k+2} durch F_{k+1} ist 1 der Quotient und F_k , was wegen $0 \leq F_k < F_{k+1}$ für $k \geq 2$ sofort aus der Rekursionsgleichung $F_{k+2} = F_{k+1} + F_k$ folgt.

$$\begin{aligned} F_{n+2} &= 1 \cdot F_{n+1} + F_n && (0 < F_n < F_{n+1}) \\ F_{n+1} &= 1 \cdot F_n + F_{n-1} && (0 < F_{n-1} < F_n) \\ F_n &= 1 \cdot F_{n-1} + F_{n-2} && (0 < F_{n-2} < F_{n-1}) \\ &\vdots \\ F_4 &= 1 \cdot F_3 + \underbrace{F_2}_{=1} && (0 < F_2 < F_3) \\ F_3 &= 2 \cdot F_2 \end{aligned}$$

Damit gilt $\mathrm{ggT}(F_{n+2}, F_{n+1}) = 1$ für $n \geq 1$ und $\mathrm{D}_{\mathbf{EA}}(F_{n+2}, F_{n+1}) = n$. •

(9.15) HILFSSATZ: Für $a, b \in \mathbb{N}$ mit $a > b$ gilt:

$$\mathrm{D}_{\mathbf{EA}}(a,b) = n \quad \Longrightarrow \quad a \geq F_{n+2} \ \text{ und } \ b \geq F_{n+1}$$

Bew: Wir führen Induktion nach n.

$\underline{n=1}$ Es gilt dann $r_2 = 0$ und $a = q_1 b$. Wegen $a > b$ folgt dann $b \geq 1 = F_2$ und $a \geq 2 = F_3$.

(IV) Die Behauptung sei richtig für ein beliebiges $n \in \mathbb{N}$ und beliebige $a, b \in \mathbb{N}$.

Gelte $\mathrm{D}_{\mathbf{EA}}(a,b) = n+1$. Der erste Schritt des euklidischen Algorithmus lautet $r_0 = q_1 r_1 + r_2$ mit $0 < r_2 < r_1$.

Für die Berechnung von $\mathrm{ggT}(r_1, r_2)$ werden dann genau n Divsionsschritte benötigt, d.h. $\mathrm{D}_{\mathbf{EA}}(r_1, r_2) = n$. Nach (IV) folgt dann aber $\underline{b = r_1 \geq F_{n+2}}$ und $r_2 \geq F_{n+1}$. Also

$$a = r_0 = q_1 r_1 + r_2 \geq r_1 + r_2 \geq F_{n+2} + F_{n+1} = F_{n+3}$$

. •

(9.16) SATZ: (Lamé , 1844) Für $a, b \in \mathbb{N}$ mit $a > b \geq 2$ gilt:

a) $\mathrm{D}_{\mathbf{EA}}(a,b) < 5 \cdot \log_{10}(b) + 1$

b) Bezeichnet d die Anzahl der Dezimalstellen von b , so ist $\mathrm{D}_{\mathbf{EA}}(a,b) \leq 5 \cdot d$.

Bew: : Setze $m := \mathrm{D}_{\mathbf{EA}}(a,b)$.

a) Für $\underline{m=1}$ gilt $m < 5\log_{10}(b) + 1$, da $\log_{10}(b) > 0$. Sei nun $\underline{m \geq 2}$. Dann gilt $b \geq F_{m+1} > \alpha^{m-1}$ mit $\alpha = \frac{1}{2}(1+\sqrt{5})$. Da die Funktion $\log_{10}$ streng monoton wachsend ist, ergibt sich $\log_{10}(b) > \log_{10}(\alpha^{m-1}) = (m-1)\log_{10}(\alpha) > (m-1) \cdot \frac{1}{5}$, da $\log_{10}(\alpha) \approx 0.20898 > 0.2$

Also $m - 1 < 5 \cdot \log_{10}(b)$

b) Nach Voraussetzung ist $b < 10^d$, woraus $\log_{10}(b) < \log_{10}(10^d) = d$ folgt. Nach a) ist daher $m - 1 < 5 \cdot d \in \mathbb{N}$, also $m \leq 5 \cdot d$. •

BEM: Die Schranke in (9.16b) kann auch angenommen werden: $\mathrm{D}_{\mathbf{EA}}(F_7, F_6) = 5, F_6 = 8$, $\mathrm{D}_{\mathbf{EA}}(F_{12}, F_{11}) = 10, F_{11} = 89$, $\mathrm{D}_{\mathbf{EA}}(F_{17}, F_{16}) = 15, F_{16} = 987$.

Wir wollen jetzt noch kurz den Fall betrachten, daß der ggT zweier Zahlen a und b gleich 1 ist. Dann gibt es $x, y \in \mathbb{Z}$ mit $1 = xa + yb$.

(9.17) DEF: Zwei ganze Zahlen a und b heißen **teilerfremd** , wenn $\mathrm{ggT}(a,b) = 1$ gilt.

(9.18) DEF: Die Funktion $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ sei für $n \in \mathbb{N}$ definiert durch

$$\varphi(n) := |\{k \mid k \in \mathbb{N}, 1 \leq k \leq n, \mathrm{ggT}(k,n) = 1\}|$$

φ heißt **Eulersche φ–Funktion**.

Beispiele: $\varphi(n)$ zählt also, wieviel Zahlen aus der Menge $\{1, 2, 3, \ldots, n\}$ zu n teilerfremd sind.

$n = 1:$ $\quad \varphi(1) = 1$

$n = 6:$ $\quad 1 \quad \not 2 \quad \not 3 \quad \not 4 \quad 5 \quad \not 6 \qquad \varphi(6) = 2$

$n = 7:$ $\quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad \not 7 \qquad \varphi(7) = 6$

$n = 12:$ $\quad 1 \quad \not 2 \quad \not 3 \quad \not 4 \quad 5 \quad \not 6 \quad 7 \quad \not 8 \quad \not 9 \quad \not 10 \quad 11 \quad \not 12 \qquad \varphi(12) = 4$

Analog zum Begriff des ggT's definieren wir nun das kleinste gemeinsame Vielfache von zwei Zahlen.

(9.19) DEF: Seien $a, b \in \mathbb{Z}$. Eine Zahl $k \in \mathbb{Z}$ heißt **kleinstes gemeinsames Vielfaches (kgV)** von a und b, wenn folgendes gilt:

i) $k \geq 0$

ii) $a \mid k$ und $b \mid k$

iii) $\forall\, v \in \mathbb{Z} : \; a \mid v$ und $b \mid v \implies k \mid v$

Bezeichnung: $k = \mathrm{kgV}(a, b)$ **Beispiel:** $\mathrm{kgV}(35, 49) = 245$, $\mathrm{kgV}(-6, 18) = 18$

BEM: Existiert ein kgV zweier Zahlen, so ist es eindeutig bestimmt (vgl. (9.9a,b)). Auch hier wird die Eindeutigkeit durch Bedingung i) erzwungen. ii) bedeutet, daß k ein gemeinsames Vielfaches von a und b ist. iii) besagt, daß jedes gemeinsame Vielfache von a und b von k geteilt wird. Gibt es also ein gemeinsames Vielfaches $v \neq 0$, so folgt aus $k \mid v$, daß $k = |k| \leq |v|$ gilt, d.h. von allen gemeinsamen Vielfachen hat k den kleinsten Betrag.

(9.20) SATZ: Zu je zwei ganzen Zahlen a und b existiert genau ein kgV, und es gilt

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) \;=\; |a \cdot b|$$

Beispiel: $\mathrm{kgV}(35, -49) = 245$, $\mathrm{ggT}(35, -49) = 7$, $\mathrm{kgV}(35, -49) \cdot \mathrm{ggT}(35, -49) = 245 \cdot 7 = 1715 = |35 \cdot (-49)|$

(9.21) BEM: Für $a \neq 0$ oder $b \neq 0$ gilt $\mathrm{ggT}(a, b) \neq 0$, und es folgt

$$\mathrm{kgV}(a, b) \;=\; \frac{|\, a \cdot b \,|}{\mathrm{ggT}(a, b)}$$

Damit haben ein Berechnungsverfahren für das kgV, wenn man den ggT mit Hilfe des **EA** bestimmt.

Beispiel: $a = 1001414587, b = 42779171, \mathrm{ggT}(a, b) = 1237 \implies \mathrm{kgV}(a, b) = \dfrac{a \cdot b}{1237} = 34631920662221$

Einen mit dem **EA** vergleichbaren Algorithmus für die Berechnung des kgV's gibt es nicht. Auch eine Darstellung des kgV's, die der Darstellung des ggT's als Vielfachsumme der beiden Zahlen entspricht, gibt es nicht.

Eine andere Berechnungsmethode für ggT und kgV basiert auf der Primfaktorzerlegung.

Der euklidische Algorithmus beruhte auf der Möglichkeit der Division mit Rest. Eine andere Anwendung der Division mit Rest ist die Darstellung einer Dezimalzahl bzgl. einer anderen Basiszahl $b \geq 2$, etwa als Binärzahl ($b = 2$) oder als Oktalzahl ($b = 8$).

Beispiel:

$$\begin{aligned} 196 &= 65 \cdot 3 + 1 \\ 65 &= 21 \cdot 3 + 2 \\ 21 &= 7 \cdot 3 + 0 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 0 \cdot 3 + 2 \end{aligned}$$

Hierbei werden 196 und die entstehenden Quotienten durch 3 mit Rest geteilt. Man bricht ab, sobald ein Quotient 0 geworden ist. Ergebnis:

$$196 = (21021)_3$$

Ausführlich geschrieben:

$$b = 2 \cdot 3^4 + 1 \cdot 3^3 + 0 \cdot 3^2 + 2 \cdot 3^1 + 1 \cdot 3^0$$

(9.22) SATZ: Sei $b \geq 2$ eine feste natürliche Zahl. Dann läßt sich jede Zahl $a \in \mathbb{N}$ darstellen in der Form

$$a = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0$$

mit $n \in \mathbb{N}_0$ und eindeutig bestimmten Zahlen $a_k \in \{0, 1, \ldots, b-1\}$ für alle $k \in \{0, 1, \ldots, n\}$ und $a_n \neq 0$. Man schreibt:

$$a = (a_n a_{n-1} \ldots a_1 a_0)_b$$

und nennt dies die **Darstellung von a bzgl. der Basiszahl b.**