Aufgabe 38. (a) Sind $a, b \in \mathbb{N}$ mit $a \geq b$ und gilt $a = bq + r$ mit $q, r \in \mathbb{N}_0$ und $r < b$, so ist

$$br \leq \frac{ab}{2}.$$

(b) Seien $a, b \in \mathbb{N}$ mit $a > b$. Zeigen Sie, dass der euklidische Algorithmus zur Berechnung von $\mathrm{ggT}(a, b)$ höchstens $\log_2(a) + \log_2(b)$ Schritte (=Divisionen mit Rest) benötigt.

Lösung (a) Ist $q = 0$, so ist $a = r < b$, im Widerspruch zu $a \geq b$. Also gilt $q = 1$. Dann ist aber $a = bq + r \geq b + r > r + r = 2r$. Multiplikation mit b ergibt $ab > 2rb$.

(b) Sei $r_{-1} := a$ und $r_0 := b$. Im i-ten Schritt ($i \geq 1$) des euklidischen Algorithmus berechnen wir r_i mittels Division mit Rest wie folgt: q_i und r_i sind die eindeutig bestimmten ganzen Zahlen für die gilt $0 \leq r_i < r_{i-1}$ und $r_{i-2} = r_{i-1}q_i + r_i$. Der Algorithmus terminiert, sobald $r_i = 0$ ist.

Sei k die Anzahl der Schritte des Algorithmus, also $r_k = 0$ und $r_i \geq 1$ für $-1 \leq i \leq k-1$. Aus (a) folgt

$$r_i r_{i-1} \leq \frac{r_{i-1} r_{i-2}}{2}$$

für alle $1 \leq i \leq k$. Mit einer trivialen Induktion folgt

$$r_i r_{i-1} \leq \frac{r_0 r_{-1}}{2^i} = \frac{ab}{2^i}.$$

Insbesondere folgt

$$r_{k-1} r_{k-2} \leq \frac{ab}{2^{k-1}}.$$

Wegen $r_{k-2} > r_{k-1} \geq 1$ (die strikte Ungleichung $r_{k-2} > r_{k-1}$ gilt aufgrund der Wahl von r_{k-1}, falls $k > 1$, und aufgrund der Voraussetzung $a > b$ falls $k = 1$), gilt $r_{k-2} \geq 2$ und damit $r_{k-1} r_{k-2} \geq 2$. Damit ist $2^k = 2 \cdot 2^{k-1} \leq ab$, und somit $k \leq \log_2(a) + \log_2(b)$.

Bemerkung. Was passiert bei $a = b$? Dann ist $k = 1$, $r_0 = r_{-1} = a = b$ und $r_1 = 0$. An Stelle von $r_{k-2} > r_{k-1}$ gilt bloß $r_{k-2} \geq r_{k-1}$. Ist $a \geq 2$, so gilt dennoch $r_{k-2} r_{k-1} = a^2 > 2$ und wir erhalten wie oben $k \leq \log_2(a) + \log_2(b)$. Aber im Fall $a = b = 1$ gilt die Ungleichung nicht, denn $k = 1$ (d.h. der Algorithmus benötigt einen Schritt), aber $\log_2(a) + \log_2(b) = 0$.