$\Rightarrow$ Laut Definition vom GGT gilt
GGT(a , b) = GGT(a , b mod a)

$lg_2$ = Logarithmus dualis d.h. zur Basis 2

$lg_{10}$ = Logarithmus dezimalis d.h. zur Basis 10

$10^x = y \Rightarrow \log_{10} = y = x$

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Beweis zu Lemma A.95

$$\text{z.z.} \left(\frac{3}{2}\right)^k \leq a + b, \qquad a, b \in \mathbb{N}_+$$

Annahme: $0 < a < b$
$b = q \cdot a + r$ $\qquad q = 1$ (ungünstigster Fall)
$a + b = a + q \cdot a + r = 2a + r$

$$= \left(\frac{3}{2}\right) q + \left(\frac{1}{2}\right) a + r$$

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

$r < a, \quad a = a_1, b = b_1$

<u>1. Schritt</u> $\quad a_1 + b_1 > \frac{3}{2} a_1 + \frac{3}{2} r_1 = \frac{3}{2} + (a_1 + r_1)$

<u>2. Schritt</u> $\quad (a_1 + r_1) > \frac{3}{2} (a_2 + r_2)$

k-te Satz IA

$$a_k + b_k > \left(\frac{3}{2}\right)(a_{k-1} + r_{k-1})$$

$$a_1 + b_1 > \left(\frac{3}{2}\right)^k (a_{k-1} + r_{k-1})$$

Mit $\quad a_{k-1} + r_{k-1} \leq 1 \quad \Rightarrow \quad GGT(a_{k-1}, r_{k-1}) = 1,$

$$\Rightarrow \quad \underset{\underset{a+b}{\parallel}}{a_1 + b_1} < \left(\frac{3}{2}\right)^k \cdot 1$$

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Berechnung von k:

$$a + b > \left(\frac{3}{2}\right)^k \mid lg_2$$

$$lg_2(a + b) > k \, lg_2\left(\frac{3}{2}\right) \quad \Rightarrow \quad k < \frac{\lg_2(a+b)}{\lg_2\left(\frac{3}{2}\right)}$$

Beweis zu Lemma A96

Es gilt: $a^{-1} = s \bmod b$ falls a , b relativ prim sind, d.h. GGT(a , b) = a

Beweistechnik: $A \Leftrightarrow B$

Aussage A: GGT(a , b) = 1 mit $1 = s\,a + t\,b$
Aussage B: $a^{-1}$ existiert mit $a^{-1} = s \bmod b$

1. Teil $A \Rightarrow B$
A ist hinreichend für B

2. Teil $B \Rightarrow A$

$\Updownarrow$

$\neg A \Rightarrow \neg B$
A ist notwendig für B

zu Teil 1: $A \Rightarrow B$
Annahme: GGT(a , b) = 1 mit $1 = s\,a + t\,b$
$\Rightarrow s\,a = 1 - t\,b$
$\Rightarrow sa = 1 \bmod b$
mod b
$\Rightarrow s = a^{-1} \bmod b$
$a^{-1}$
Inverses existiert

Zu Teil 2: $\neg A \Rightarrow \neg B$
Annahme: GGT(a , b) = c > 1 ,
$a = a' \cdot c \wedge b = c \cdot b'$ , $a' < a$ , $b' < b$ ,

$\Rightarrow$ $(a \cdot b') \bmod b$ $\parallel$ $b \nmid b'$,

$\Rightarrow$ $(a' \cdot c \cdot b') \bmod b$

$\Rightarrow$ $(a' \cdot b) \bmod b$

0 mod b

Herleitung des erweiterten Euklidischen Algorithmus:

$s_a = s$ ; $s_b = r$

$$\left.\begin{aligned} a &= s_a \cdot a_0 + t_a \cdot b_0 \\ b &= s_b \cdot a_0 + t_b \cdot b_0 \\ r &= s_r \cdot a_0 + t_r \cdot b_0 \end{aligned}\right\} \Rightarrow s_r = s_b - q \cdot s_a$$

Euklidischer Algorithmus

$\Rightarrow$ $1 = s_a + t_b \bmod b$ $b = q \cdot a + r$

$a^{-1} = s \bmod b$ $r = q \cdot a - b$

2.) GGT(a , b) = a $a < b$ ;

$a \mid b \Rightarrow g = s\,a + t\,b$

$= sa + t \cdot q\,a$

$= (s + t \cdot q) \cdot a = a\,\mathbb{Z}$

d.h. kein Inverses möglich $\Rightarrow$ GGT(a , b) $\neq 1$

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

$\Rightarrow$ a ist Nullteiler, d.h. $a^k = 0 \bmod b$

Lemma A.29 (Inverses oder Nullteiler)

$\Rightarrow$ $a^{-1}$ ist nicht möglich

$(s + t \cdot q) \cdot a = 0 \bmod a$ $\Rightarrow$ kein Inverses möglich!

Beispiel GGT(6 , 22) = g

Schritt 0: $b_1 = q_1 \cdot a_1 + r_1$ $a < b$ ,

$22 = 3 \cdot 6 + 4 \quad \downarrow \qquad$ Reduktionsschritt (ii) von Lemma A.90

Schritt 1: $b_2 = q_2 \cdot a_2 + r_2$

$6 = 1 \cdot 4 + 2 \quad \downarrow$

Schritt 2: $b_3 = q_3 \cdot a_3 + r_3$

$4 = 2 \cdot 2 + 0 \quad \Rightarrow \qquad$ GGT(6 , 22) = 2 ; (i) von Lemma A.90

Beweis zu Lemma A.90

(i) $0 < a \quad \Rightarrow \quad \mathrm{GGT}(0, a) = a$

$\mathrm{GGT}(0, a) = 0 \cdot s + a \cdot t \in a^{\mathbb{Z}} = g^{\mathbb{Z}}$

$\Rightarrow a = g = \mathrm{GGT}(0, a)$

(ii) $0 < a < b$

z.z. GGT(a , b) = GGT (b mod a , a) ,

$\Rightarrow \quad b = q \cdot a + r$

$R = b \cdot q\,a$

Falls $c \mid a \wedge c \mid b \Rightarrow c \mid r$

$\|$

$c \mid a \cdot a + r$

$\Rightarrow c \mid a \wedge c \mid r \Rightarrow c \mid b = c \mid q \cdot a + r = c \mid b \bmod a$