Theorem A $(R, +, \cdot)$ ist Ring $\Rightarrow$ $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in R$ (0)

Insbesondere ist 0 nicht invertierbar (bzgl. $\cdot$), auch nicht im Körper!

Lemma B $(M, \circ)$ Monoid a, b invertierbar $\Rightarrow$ $(a \circ b)$ invertierbar, Inverses ist $b^{-1} \circ a^{-1}$.

Theorem 4.26 $(\mathbb{Z}_n, \oplus_n, \odot_n)$ ist Körper $\Leftrightarrow$ n ist Primzahl

"$\Rightarrow$" $\mathbb{Z}_n$, n keine Primzahl, $n \geq 4$

$\Rightarrow$ es ex. $a, b \geq 2$ $(a \neq 1, b \neq 1)$ mit $a \odot_n b = n$

Ann.: $(\mathbb{Z}_n, \oplus_n, \odot_n)$ ist Körper $\Rightarrow$ a, b invertierbar

$\Rightarrow$ $(a \odot_n b)$ invertierbar aber $\overline{a \odot_n b} = \overline{n} = \overline{0}$ ↯ Theorem A

↑ Lemma B

Lemma C: $(M, \circ)$ Monoid, $\circ$ kommutativ a, b nicht invertierbar $\Rightarrow$ $(a \circ b)$ nicht invertierbar

$(\mathbb{Z}_6, \odot_6)$

$\odot_6$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$
$\bar{5}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{0}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$

$(\{\bar{1}, \bar{5}\}, \odot_6)$

Gruppe (Einheiten -)

$(\{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}, \odot_6)$

Halbgruppe

Aber

$(\{\bar{0}, \bar{1}, \bar{5}\}, \oplus_6, \odot_6)$

kein Körper

$(\{\bar{0}, \bar{1}, \bar{5}\}, \oplus_6)$

↑

kein Vektorraum

$\bar{5} + \bar{5} = \bar{4}$

$\bar{1} + \bar{1} = \bar{2}$

nicht abgeschlossen!

4.33 Euklidischer Algorithmus

ggT - Berechnung zweier ganzer Zahlen

Kryptografie $\rightsquigarrow$ RSA

Definition 4.27

i) Seien $d, x \in \mathbb{Z}$

Wir sagen d teilt x (Notation: $d \mid x$)

$:\Leftrightarrow \exists z \in \mathbb{Z} \quad x = z \cdot d$

ii) Für $x, y \in \mathbb{Z}$ heißt $d \in \mathbb{N}$ der

größte gemeinsame Teiler (Notation: $d = ggT(x,y)$)

$:\Leftrightarrow$ ($d \mid x$ und $d \mid y$) und

($\forall d'$ mit ($d' \mid x$ und $d' \mid y$) $\Rightarrow$ $d' \mid d$) gilt

(BSP) $x = 50 \quad y = 20$

$5 \cdot 5 \cdot 2 \qquad 5 \cdot 2 \cdot 2 \qquad ggT(x,y) = ggT(50,20) = 10$

Definition 4.28 (teilfremd)

$x, y \in \mathbb{Z}$ teilfremd $:\Leftrightarrow ggT(x,y) = 1$

Euklidischer Algorithmus $\rightsquigarrow$ Lösungsplan für ggT.

(effizient)

Pseudo code Euklid ggT

Euklid $(x_0, x_1 \in \mathbb{Z})$

1. IF $(x_0 < x_1)$ vertausche die Zahlen (dann $x_0 > x_1$)
2. $i := 1$;
3. WHILE $(x_i \neq 0)$ {
4. $x_{i+1} := x_{i-1} \bmod x_i$; i
5. $i := i+1$;
6. }
7. Return x_{i-1};

$x_0 = 50 \quad x_1 = 20$

$i=1 \quad x_2 = 50 \bmod 20 = 10$

$i=2 \quad x_3 = 20 \bmod 10 = 0$

(x_1 x_2)

$i=3$ Stop $x_{i-1} = x_2 = 10$

$ggT(50,20) = 10$

↓

! Division mit Rest $x_{i+1} \in \{0, 1, 2, \ldots, |x_i|-1\}$!

Theorem 4.24 Euklid. Alg. berechnet den ggT.

$x_{j+1} \in \{0, 1, 2, \dots, |x_j| - 1\}$

Beweis: Tabellarisch!

2 ⇓

b) $d' \mid x_0$ $d' \mid x_1$	(a) $x_i = d$, $d \mid x_0$ und $d \mid x_1$		
$d' \mid x_2$	$x_i \mid x_0$	$x_0 = q_1 \cdot x_1 + x_2$	$x_2 := x_0 \bmod x_1$, $\lvert x_2 \rvert < \lvert x_1 \rvert$
$d' \mid x_3$	$x_i \mid x_1$	$x_1 = q_2 x_2 + x_3$	$x_3 := x_1 \bmod x_2$, $x_3 < x_2$
$d' \mid x_4$	$x_i \mid x_2$	$x_2 = q_3 \cdot x_3 + x_4$	$x_4 := x_2 \bmod x_3$, $x_4 < x_3$
	$x_i \mid x_3$		
⋮	⋮	⋮	⋮
$d' \mid x_{i-2}$	$x_i \mid x_{i-3}$	$x_{i-3} = q_{i-2} x_{i-2} + x_{i-1}$	
$d' \mid x_{i-1}$	$x_i \mid x_{i-2}$	$x_{i-2} = q_{i-1} x_{i-1} + x_i$ (= d)	$x_i := x_{i-2} \bmod x_{i-1}$, $x_i < x_{i-1}$
$\underline{d' \mid x_i}$	$d = x_i \mid x_{i-1}$ ⇑	$x_{i-1} = q_i x_i + 0$	$x_{i+1} = 0 := x_{i-1} \bmod \underline{x_i}$

$d = x_i$

1. Terminiert? $|x_1| > x_2 > x_3 > x_4 \dots > x_{i+1} = 0$

⇒ 2. Berechnet der ggT? Ist x_i das $ggT(x_0, x_1)$? ∎

BSP $x_0 = -50 \quad x_1 = 20$

$x_0 < x_1 \xrightarrow[\text{vertauscht}]{}$ $x_0' = 20 \quad x_1' = -50$

$20 = 0 \cdot -50 + 20$

$-50 = -3 \cdot 20 + \underset{x_2}{10}$

$20 = 2 \cdot 10 + 0$

$x_0' = q_1 x_1' + x_2'$

$x_1' = q_2 x_2' + x_3'$

$x_3' = q_3 \cdot x_3' + x_4'$

$x_4' = 0 \quad d = x_3' = 10$

$= ggT(-50, 20)$

Weiteres Ergebnis!

(P)

Lemma 4.24 $a, b \in \mathbb{Z}$ teilerfremd

$\Rightarrow$ es ex. $x, y \in \mathbb{Z}$ mit

$$a \cdot x + b \cdot y = 1 = gg^T(a,b)$$

Verallgemeinerung:

Lemma 4.30 Seien $a, b \in \mathbb{Z}$ und $d = gg^T(a,b)$

$\Rightarrow$ es ex. $x, y \in \mathbb{Z}$ mit $a \cdot x + b \cdot y = d$

Beweis: (konstruktiv) aus Eukl. Alg.

(8)

Statt a, b nehme x_0, x_1!

Darstellung des ggT's d als Linearkombination von

	$d = x_i = x_{i-2} - q_{i-1} x_{i-1}$	x_{i-2}, x_{i-1}
1. Schritt	$x_{i-1} = x_{i-3} - q_{i-2} x_{i-2}$	x_{i-2}, x_{i-3} (*)
2. Schritt	$x_{i-2} = x_{i-4} - q_{i-3} x_{i-3}$	x_{i-3}, x_{i-4}
	$\vdots$	$\vdots$
	$x_3 = x_1 - q_2 x_2$	x_1, x_2
Finaler Schritt	$x_2 = x_0 - q_1 x_1$	x_0, x_1

Genauer: 1. $d = \underbrace{-q_{i-1}}_{=: a_{i-3}} x_{i-3} + \underbrace{(1 + q_{i-1} q_{i-2})}_{=: b_{i-2}} x_{i-2}$ (*) So

2. $d = a_{i-4} x_{i-4} + b_{i-3} x_{i-3}$

$a_0 = x \quad b_1 = y$

Final $\quad d = a_0 x_0 + b_1 x_1$

$=$  Berechnet aus $q_1, q_2, \dots, q_{i-1}$ (Eukl. Alg.)

(BSP)

$x_0 = 1365 \quad x_1 = 510$

$x_2 = x_0 \bmod x_1 = 345$

$x_3 = x_1 \bmod x_2 = 165$

$x_4 = x_2 \bmod x_3 = 15 = x_i$

$x_5 = x_3 \bmod x_4 = 0 = x_{i+1}$

$x_5 = 0 \qquad x_4 = d = 15$

$x_0 = q_1 \cdot x_1 + x_2$

$1365 = 2 \cdot 510 + 345$

$510 = q_2 \cdot x_2 + x_3$

$= 1 \times 345 + 165$

$345 = 2 \cdot 165 + 15$

$x_2 = q_3 \cdot x_3 + x_4$

$165 = 11 \cdot 15 + 0$

$x_3 = q_4 \cdot x_4$

$$\underline{d=15} = 345 - 2 \cdot (165) \qquad \underline{165} = 510 - 1 \cdot 345$$
$$\qquad\qquad\qquad\quad x_3 \quad x_1 \quad x_2$$

$$= 345 - 2 \cdot (510 - 1 \cdot 345)$$

$$= -2 \cdot 510 + 3 \cdot (345) \qquad \underline{345} = \underline{1365} - 2 \cdot \underline{510}$$
$$\qquad\qquad\qquad\quad x_2 \quad x_0 \quad x_1$$

$$= -2 \cdot 510 + 3(1365 - 2 \cdot 510)$$

$$= 3 \cdot 1365 + (-8) \cdot 510 = 15$$

$$= x \cdot x_0 + y \cdot x_1 \quad \text{Darstellg}$$

OE. $x_0, x_1 \in \mathbb{N}$ $x_0 \geq x_1$ Analyse

Prinzip der Verlegung "schwer" Problem Laufzeit $\rightsquigarrow$ Algo

ggT Berechnung "leicht" # WHILE-Durchläufe

Theorem 4.31 Bei Eingabe $x_0, x_1 \in \mathbb{N}$ mit $x_0 \geq x_1$ beträgt die Anzahl der WHILE-Durchläufe im Euklid. Alg. max. $2 \cdot \log_2(x_0)$.

(Bsp)

$\mathbb{Z}_7$: $p = 7$ $\quad a = \overline{5}$

ggT$(5,7) = 1$

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = \underline{5} - 2(\underline{7} - 1 \cdot \underline{5})$

$1 = 3 \cdot 5 - 2 \cdot 7$

$\overline{5}^{-1} = \overline{3}$ $\quad \overline{3}$ Mult. Inverses zu $\overline{5}$.

m.d Erweit. Alg.

Existenz in $\mathbb{Z}_p$ beweisen!

$a \cdot x + p \cdot y = 1$

$x_2 \quad x_0 \quad x_1$

$2 = 7 - 1 \cdot 5$

$x_3 \quad x_1 \quad x_2$

$1 = 5 - 2 \cdot 2$

$x_4 \quad x_2 \quad x_3$

$0 = 2 - 2 \cdot 1$

Beweis Theorem 4.31:

Ann: $x_0 \geq x_1 \quad x_0, x_1 \in \mathbb{N}$

$\Rightarrow \quad x_0 \geq x_1 > x_2 > \cdots > x_i > x_{i+1} = 0$

x_j, q_j wie vorher $\quad j = 1, \ldots, i$

$x_{j-1} = q_j x_j + x_{j+1} \quad q_1, q_2, \ldots, q_i$

$\left(x_{j-1} \geq x_j > x_{j+1} \Rightarrow q_j \geq 1 \right)$

Also: $x_{j-1} \geq x_j + x_{j+1} > 2x_{j+1}$

$\Rightarrow x_{j+1} < \frac{x_{j-1}}{2}$ "alle 2 Durchläufe halbiert sich die Zahl" $j = 1, \ldots, i$

$\underline{s=1}$ $\quad$ $\underline{s=3}$ $\quad$ $\underline{s=5}$

Folg: $x_2 < \frac{x_0}{2}$, $x_4 < \frac{x_2}{2}$, $x_6 < \frac{x_4}{2} \rightsquigarrow x_6 < \frac{x_0}{2^3}$

allgemein $\underline{\underline{k \in \mathbb{N}}}$ $\quad x_{2k} < \frac{x_0}{2^k}$

oo. Argumente ... nach $2 \cdot \log_2(x_0)$ Schritte

muss $\forall_{2k} x_j < 1$ sein !

□