Proseminar: Primzahlen
1. Vortrag
Der erweiterte euklidische Algorithmus

Max Zoller

14. April 2008

1 Der klassische euklidische Algorithmus

Beispiel: $ggT(105, 56)$?

$$\begin{aligned} 105 &= 1 \cdot 56 + 49 \\ 56 &= 1 \cdot 49 + 7 \\ 49 &= 7 \cdot 7 + 0 \\ \Longrightarrow ggT(105, 56) &= 7 \end{aligned}$$

Algorithmus 1. *Gesucht ggT(x,y) mit* $x, y \neq 0$ *Setze*

$$\begin{aligned} r_0 &= x \\ r_1 &= y \\ r_{i+1} &= \begin{cases} \textit{Rest bei Division } r_{i-1} \textit{ durch } r_i \textit{ falls } r_i \neq 0 \\ 0 \textit{ sonst} \end{cases} \\ \Longrightarrow r_{i-1} &= q_i \cdot r_i + r_{i+1} \end{aligned}$$

Dann gibt es ein kleinstes $n \in \mathbb{N} : r_{n+1} = 0 \Longrightarrow ggT(x, y) = r_n$

Fragen:

- Wo (in welchen algebraischen Strukturen) funktioniert dieser Algorithmus?
- Wie definiert ganz allgemein in einer solchen Struktur ggT und kgV und sind diese eindeutig?
- Welche Eigenschaften haben diese Strukturen?

- Wie kann man den Algorithmus erweitern um mehr Informationen zu erhalten?

Im wesentlichen braucht man für den obigen Algorithmus die Division mit Rest und die Eigenschaft, dass er nach endlich vielen Schritten abbricht.

Definition 1. *Ein* ***Integritätsring*** *ist ein nullteilerfreier, kommutativer Ring mit einem von Null verschiedenen Einselement.*

Definition 2. *Ein Integritätsring mit einer Abbildung* $\delta : R\backslash\{0\} \to \mathbb{N}$ *heißt* ***Euklidischer Ring****, wenn gilt:*

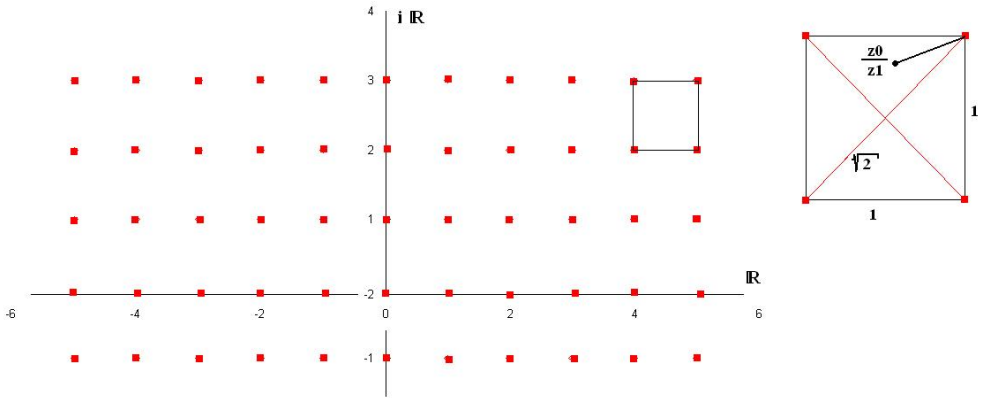
$$\forall f, g \in R,\ g \neq 0 \qquad \exists q, r \in R : \qquad f = q \cdot g + r \ \textit{und}\ \delta(r) < \delta(g)$$

.

Beispiele

- Im obigen Beispiel des Ringes $\mathbb{Z}$ kann man $\delta : \mathbb{Z}\backslash\{0\} \to \mathbb{N}$, $z \mapsto |z|$ wählen. $\Longrightarrow (\mathbb{Z}, \delta)$ ist ein eukl. Ring.
- Im Ring der Polynome über einen Körper $\mathbb{K}$ wählt man $\delta : \mathbb{K}[X]\backslash\{0\} \to \mathbb{N}$, $p \mapsto \text{grad } p$. $\Longrightarrow (\mathbb{K}[X], \delta)$ ist ein eukl. Ring.
- Jeder Körper (trivial, da Division sogar immer ohne Rest möglich)
- Der Ring der ganzen Gaußschen Zahlen $\mathbb{Z}[i] = \{z = a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ ist ein eukl. Ring mit $\delta : \mathbb{Z}[i]\backslash\{0\} \to \mathbb{N}$, $z = a + ib \mapsto a^2 + b^2 = |z|^2$.

Beweis: Sei $z_0, z_1 \in \mathbb{Z}[i]$.



Gesucht $q_1, r_2 \in \mathbb{Z}[i] : z_0 = q_1 \cdot z_1 + z_2$

sodass $\delta(z_2) < \delta(z_1) \iff |z_2| < |z_1|$ oder $z_2 = 0$
(Rechenoperationen definiert wie in $\mathbb{C}$)
1.Fall $\frac{z_0}{z_1} \in \mathbb{Z}[i] \Longrightarrow z_2 := 0, q_1 := \frac{z_0}{z_1}$ $\surd$

2.Fall $\frac{z_0}{z_1} \in \mathbb{C} \backslash \mathbb{Z}[i]$

$$\begin{aligned} \exists q_1 \in \mathbb{Z}[i]: \qquad & \left| \frac{z_0}{z_1} - q_1 \right| \leq \frac{\sqrt{2}}{2} < 1 \\ \Longrightarrow & |\underbrace{z_0 - q_1 \cdot z_1}_{=:z_2}| \leq \frac{1}{\sqrt{2}} |z_1| < |z_1| \\ \Longrightarrow & |z_2| < |z_1| \end{aligned}$$

$\diamond$

Anmerkung: r und q sind i.a. nicht eindeutig bestimmt. Im obigen Beispiel: $105 = 2 \cdot 56 - 7$ statt $105 = 1 \cdot 56 + 49$ möglich!

Erinnerung: In einem Ring R heißt x Teiler von y (Schreibweise x|y), wenn es ein $t \in R$ gibt mit $y = t \cdot x$

Definition 3. *In einem Ring R heißt c der* ***ggT*** *von a und b, wenn gilt:*

1. *c|a und c|b*
2. *$\forall d \in R$: (d|a und d|b $\Longrightarrow$ d|c)*

Weiter heißt $v \in R$ ***kgV*** *von $a, b \in R$, wenn gilt:*

1. *a|v und b|v*
2. *$\forall d \in R$: (a|d und b|d $\Longrightarrow$ v|d)*

Frage: Sind ggT, kgV eindeutig bestimmt?
Antwort: i.a. Nein! Aber es gibt eine einfache Äquivalenzrelation zwischen allen möglichen ggT/kgV, so dass man einen Repräsentanten der entsprechenden Klasse wählen kann.

Definition 4. *In einem Ring R (mit Einselement) heißt ein Element u* ***Einheit*** *(unit), wenn das multiplikative Inverse $u^{-1} \in R$ exisitert.*
Die Elemente $a, b \in R$ heißen ***assoziiert****, wenn es eine Einheit $u \in R$ gibt: $a = u \cdot b$*

Assoziiertheit ist eine Äquivalenzrelation. (Beweis leicht)

Beispiele

- In $\mathbb{Z}$ sind 1 und -1 die einzigen Einheiten. Damit sind genau z und -z assoziert $\forall z \in \mathbb{Z}$. Wähle als Repräsentanten der entsprechenden Äquvalenzklasse $z \geq 0$
- In einem Körper $\mathbb{K}$ sind alle Elemente außer 0 Einheiten und damit auch alle Elemente $a, b \in \mathbb{K}\backslash\{0\}$ assoziiert miteinander.
- Im Polynomring $\mathbb{K}[X]$ (über einen Körper) sind genau die Polynome vom Grad 0 Einheiten. Man kann also z.B. als Repräsentanten einer Klasse assoziierter Polynome z.B. dasjenige mit Leitkoeffizient 1 wählen. Man gewinnt so die Normalform des entsprechenden Polynoms.

Allgemein:

Definition 5. *Zeichne in einem euklidischen Ring einen Repräsentanten jeder Klasse assoziierter Elemente als* ***Normalform*** *aus (Bezeichnung normal(a) für a aus der Klasse). Dann heißt die Einheit $l \in R$ mit $a = l \cdot normal(a)$* ***Leitkoeffizient*** *(Schreibweise l=lc(a)) von a.*

Setze lc(0):=1 und normal(0):=0.

Proposition 1. *Der ggT zweier Elemente $a, b \in R$ (R eukl. Ring) ist bis auf Assoziiertheit eindeutig.*

Beweis: Sei R eukl. Ring und $a, b \in R$ (a,b nicht beide 0). Seien weiter $g_1, g_2 \in R$ ggT von a und b.
$g_i|a \wedge g_i|b \qquad (i = 1, 2)$
Nach Def. von ggT muss gelten (jeder andere Teiler von a,b teilt den ggT(a,b)):
$g_1|g_2 \wedge g_2|g_1$
$\Longrightarrow g_1 = \alpha g_2 \wedge g_2 = \beta g_1 \qquad \alpha, \beta \in R$
$\Longrightarrow g_1 = \alpha\beta g_1$
$\Longrightarrow g_1(1 - \alpha\beta) = 0$
Nun ist $g_1 \neq 0$ da ggT und R ist nullteilerfrei und kommutativ (Integritätsring).
$\Longrightarrow \alpha\beta = \beta\alpha = 1 \Longrightarrow \alpha = \beta^{-1} \qquad \alpha, \beta$ sind Einheiten und g_1, g_2 assoziiert.

$\diamond$

Beweis von Algorithmus 1:
1. Sei R eukl. Ring und $\delta : R\backslash\{0\} \Rightarrow \mathbb{N}$ zugeh. Gradabbildung. Wähle $x, y \in R\backslash\{0\}$ und betrachte die Folge $r_0, r_1, r_2, \ldots$ Wegen $\delta(r_{i+1}) < \delta(r_i)$ oder $z_{i+1} = 0$ ist für i>0 streng monoton fallend, solange $z_i \neq 0$. δ bildet nach $\mathbb{N}$ ab und $\mathbb{N}$ ist diskret und nach unten beschränkt. $\Longrightarrow \exists n \in \mathbb{N} : r_{n+1} = 0$
2. Betrachte das endliche LGS

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 && (1)\\ r_1 &= q_2 r_2 + r_3 && (2)\\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n && (n-1)\\ r_{n-1} &= q_n r_n && (n) \end{aligned}$$

Dann folgt von unten nach oben induktiv:
Aus (n): $r_n | r_{n-1}$ da $r_{n-1} = q_n r_n$
In (n-1): $r_{n-2} = (q_{n-1} q_n + 1) r_n$ also $r_n | r_{n-2}$ usw.
In (2) und (1): $r_n | r_1 = y$ und $r_n | r_0 = x$
Hat man einen weiteren Teiler t von x,y, so folgt induktiv von oben nach unten:
$t | r_0$ und $t | r_1$. Also $r_0 = \alpha_0 t$ und $r_1 = \alpha_1 t$ mit $\alpha_i \in R$
Damit folgt aus (1): $r_2 = (\alpha_0 - q_1 \alpha_1) t$ also $t | r_2$
In (2): $t | r_3$ usw. In (n-1): $t | r_n$

$\diamond$

Nun zu weiteren Eigenschaften euklidischer Ringe:

2 Idealtheoretisches

Definition 6. *Sei R Ring. Eine TM $I \subseteq R$ heißt **Ideal** in R, falls gilt:*

1. *I ist additive Untergruppe von R*
2. $\forall r \in R, i \in I : r \cdot i \in I$

In jedem Ring gibt es das Nullideal $\{0\}$ und das Einheitsideal R.

Weitere Beispiele

a) Die Mengen $m \cdot \mathbb{Z}$ wobei $m \in \mathbb{Z}$ sind Ideale in $\mathbb{Z}$

b) Die Menge der Polynome $span(x, x^2, x^3, \ldots)$ bilden ein Ideal in $\mathbb{K}[X]$

Verknüpfung von Idealen I und J $\subseteq R$:

- $I + J := \{i + j | i \in I, j \in J\}$
- $I \cdot J := \{\sum_{k=1}^{n} i_k j_k | i_k \in I, j_k \in J; n \in \mathbb{N}\}$
- $I \cap J$

sind wieder Ideale.

Definition 7. *Eine Menge von Elementen $(i_k)_k$ aus dem Ideal I heißt* ***Erzeugendensysteme von I****, falls $I = \sum_k R \cdot i_k$ wobei $R \cdot a := \{r \cdot a | r \in R\}$*

Umgekehrt lassen sich aus einer Menge von Elementen aus R so Ideale konstruieren.
Schreibweise: $(i_1, \ldots, i_n) = Ri_1 + \ldots + Ri_n$

Definition 8. *Wird ein Ideal I von einem einzigen Element i erzeugt, so heißt I=(i)* ***Hauptideal***

Die Ideale a) sind wie man leicht sieht Hauptideale $m\mathbb{Z} = (m)$, das in b) ebenfalls, da $span(x, x^2, x^3, \ldots) = (x)$

Definition 9. *Ein Integritätsring R, in dem jedes Ideal ein Hauptideal ist heißt* ***Hauptidealring***

Satz 2. *Jeder euklidische Ring R ist ein Hauptidealring*

Beweis: Sei $I \subseteq R$ Ideal, o.B.d.A. nicht das Nullideal (das von 0 erzeugt wird). Wähle von den Elementen aus I ein $i \neq 0$, sodass $\delta(i)$ minimal in $I \backslash \{0\}$ (das geht, da δ nach $\mathbb{N}$ abbildet), dann gilt: I=(i).
Ist nämlich $j \in I$ so gilt wegen der Euklidizität $j = q \cdot i + r$ mit $\delta(r) < \delta(i)$ oder r=0. Wegen der Minimalität von $\delta(i)$ folgt r=0.
Also $j = qi \in (i) \quad \Longrightarrow I \subseteq (i)$
$(i) \subseteq I$ ist nach Definition von Idealen trivial.

$\diamond$

Korollar 3. *Die Ringe $\mathbb{Z}$, $\mathbb{Z}[i]$ und $\mathbb{K}[X]$ sind Hauptidealringe*

Randbemerkungen:

- Damit sind in Bsp. a) bereits alle möglichen Ideale in $\mathbb{Z}$ abgedeckt.
- In Hauptidealringen gibt es eine bis auf Assoziiertheit und Reihenfolge eindeutige Zerlegegung der Elemente in Primelemente (das sind solche $p \in R$ für die gilt p|xy $\Longrightarrow$ p|x oder p|y wobei $x, y \in R$)
  Ohne Beweis.

3 Der erweiterte euklidische Algorithmus

Algorithmus 2. *Sei R eukl. Ring, auf dem eine Normalform definiert ist, und $x, y \in R$ (nicht beide 0, o.B.d.A. $y \neq 0$)*
1.

$$\begin{aligned} r_0 &= normal(x) & r_1 &= normal(y) \\ \rho_0 &= lc(x) & \rho_1 &= lc(y) \\ s_0 &= \rho_0^{-1} & s_1 &= 0 \\ t_0 &= 0 & t_1 &= \rho_1^{-1} \end{aligned}$$

2.

$$\tilde{r}_{i+1} = \begin{cases} \textit{Rest bei Division } r_{i-1} \textit{ durch } r_i \textit{ falls } r_i \neq 0 \\ 0 \textit{ sonst} \end{cases}$$

$$\begin{aligned} \Longrightarrow r_{i-1} &= q_i \cdot r_i + \tilde{r}_{i+1} \\ r_{i+1} &= normal(\tilde{r}_{i+1}) \\ \rho_{i+1} &= lc(\tilde{r}_{i+1}) \qquad \underline{\textit{Beachte:}}\ \textit{Die } \rho_i \textit{ sind Einheiten} \\ s_{i+1} &= (s_{i-1} - q_i s_i)\rho_{i+1}^{-1} \\ t_{i+1} &= (t_{i-1} - q_i t_i)\rho_{i+1}^{-1} \end{aligned}$$

Wie schon im klassischen eukl. Algorithmus gibt es ein kleinstes $l \in \mathbb{N}$: $r_{l+1} = 0 \Longrightarrow r_n$ ist der normierte ggT(x,y).
Man erhält als Informationen

- Die **Euklidische Länge** $l \in \mathbb{N}$ von (x,y)
- Die **Quotienten** $q_i \in R \qquad 1 \leq i \leq l$
- Die **Reste** $r_i \in \mathbb{R} \qquad 0 \leq i \leq l+1$
- Die Leitkoeffizienten $\rho_i \in R \qquad 0 \leq i \leq l+1$ der Reste
- Die Elemente $r_i, s_i, t_i \in R$ bilden die sogenannte **i-te Reihe** des erw. eukl. Alg. Es gilt:

  $$s_i \cdot x + t_i \cdot y = r_i \qquad \forall 0 \leq i \leq l+1$$

  Speziell für i=l

  $$s_l \cdot x + t_l \cdot y = r_l = ggT(x,y) \text{ (normiert)}$$

  wobei s_l, t_l die **Bézout Koeffizienten** von x,y heißen.

Beispiel: Sei $R = \mathbb{Q}[X]$ und $f, g \in \mathbb{Q}[X]$ mit
$f = 2x^3 + 7x^2 + 8x + 3$
$g = 2x^2 + 3x + 1$
Darstellung als Tabelle

i	q_i	ρ_i	r_i	s_i	t_i
0	-	2	$x^3 + \frac{7}{2} + 4x + \frac{3}{2}$	$\frac{1}{2}$	0
1	$x + 2$	2	$x^2 + \frac{3}{2}x + \frac{1}{2}$	0	$\frac{1}{2}$
2	$x + \frac{1}{2}$	$\frac{1}{2}$	$x + 1$	1	$-x - 2$
3	-	1 (nach Def.)	0	$-x - \frac{1}{2}$	$x^2 + \frac{5}{2}x + \frac{3}{2}$

Rechnung Polynomdivision liefert

$$\begin{aligned}
x^3 + \frac{7}{2} + 4x + \frac{3}{2} &= \left(x^2 + \frac{3}{2} + \frac{1}{2}\right)(x+2) + \left(\frac{1}{2}x + \frac{1}{2}\right) \\
\Longrightarrow q_1 &= x + 2 \\
\tilde{r}_2 &= \frac{1}{2}x + \frac{1}{2} \\
\Longrightarrow r_2 &= x + 1 \\
\rho_2 &= \frac{1}{2} \\
s_2 &= \left(\frac{1}{2} - (x+2)\,0\right) 2 = 1 \\
t_2 &= \left(0 - (x+2)\,\frac{1}{2}\right) 2 = -x - 2
\end{aligned}$$

$$\begin{aligned}
x^2 + \frac{3}{2}x + \frac{1}{2} = (x+1)\left(x + \frac{1}{2}\right) \Longrightarrow q_2 &= x + \frac{1}{2} \\
\tilde{r}_3 &= 0 \\
\Longrightarrow r_3 &= 0 \\
\rho_3 &= 1 \qquad \text{nach Definition} \\
s_3 &= \left(0 - \left(x + \frac{1}{2}\right) 1\right) 1 = -x - \frac{1}{2} \\
t_3 &= \left(\frac{1}{2} - \left(x + \frac{1}{2}\right) 1\right) 1 = x^2 + \frac{5}{2}x + \frac{3}{2}
\end{aligned}$$

Insbesondere ist damit

$$r_2 = ggT(f,g) = s_2 \cdot f + t_2 \cdot g = 1(2x^3+7x^2+8x+3) + (-x-2)(2x^2+3x+1) = x+1$$

Korollar 4. *Zwei beliebige Elemente $x, y \in R$, wobei R ein euklidischer Ring ist, haben einen ggT h, der sich als Linearkombination von x,y darstellen lässt:*

$$h = s \cdot x + t \cdot y \qquad \text{mit } s, t \in R$$

Übersichtlichere Darstellung des erw. eukl. Algorithmus:
Definiere für $1 \leq i \leq l$ folgende Matrizen in $R^{2\times 2}$

$$R_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} \qquad Q_i = \begin{pmatrix} 0 & 1 \\ \rho_{i+1}^{-1} & -q_i\rho_{i+1}^{-1} \end{pmatrix} \qquad \text{und} \qquad R_i = Q_i \cdots Q_1 R_0$$

Satz 5. *(beweist u.a. auch den Algorithmus mit 1.,3.,4. Die Tatsache, dass der Algorithmus nach endlich vielen Schritten abbricht wurde oben schon begründet) Für $0 \leq i \leq l$:*

1. $R_i \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$
2. $R_i = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix}$
3. $ggT(f, g) = ggT(r_i, r_{i+1}) = r_l$
4. $s_i f + t_i g = r_i$ *(auch für i=l+1)*
5. $s_i t_{i+1} - t_i s_{i+1} = (-1)^i(\rho_0 \cdots \rho_{i+1})^{-1}$
6. $ggT(r_i, t_i) = ggT(f, t_i)$
7. $\begin{array}{l} f = (-1)^i \rho_0 \cdots \rho_{i+1}(t_{i+1}r_i - t_i r_{i+1}) \\ g = (-1)^{i+1} \rho_0 \cdots \rho_{i+1}(s_{i+1}r_i - s_i r_{i+1}) \end{array}$

Beweis:

1. Vollst. Ind. nach i: $i = 0$ $\surd$ (1. Schritt des Algorithmus).
   IS für $i \geq 1$ (IV: Beh. wahr $\forall k < i$):

$$R_i \begin{pmatrix} f \\ g \end{pmatrix} =^{IV} Q_i \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ \rho_{i+1}^{-1} & -q_i\rho_{i+1}^{-1} \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}$$
$$= \begin{pmatrix} r_i \\ (r_{i-1} - q_i r_i)\rho_{i+1}^{-1} \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$$

2. analog zu 1. Im IS verwendet man

$$Q_i \begin{pmatrix} s_{i-1} & t_{i-1} \\ s_i & t_i \end{pmatrix} = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix}$$

3. Sei $i \in \{0, \ldots, l\}$, aus 1. folgt:

$$\begin{pmatrix} r_l \\ 0 \end{pmatrix} = Q_l \cdots Q_{i+1} R_i \begin{pmatrix} f \\ g \end{pmatrix} = Q_l \cdots Q_{i+1} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$$

Also ist r_l LK von $r_i, r_{i+1} \Longrightarrow$ jeder gemeinsame Teiler von r_i, r_{i+1} teilt auch r_l.
Da die Q_i invertierbar sind mit $Q_i^{-1} = \begin{pmatrix} q_i & \rho_{i+1} \\ 1 & 0 \end{pmatrix}$ folgt:

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = Q_{i+1}^{-1} \cdots Q_l^{-1} \begin{pmatrix} r_l \\ 0 \end{pmatrix}$$

Also sind r_i, r_{i+1} LK von r_l und damit durch r_l teilbar.
Für i=0 folgt speziell $ggT(f, g) = r_l$

4. folgt durch Einsetzen von 2. in 1.

5. $s_i t_{i+1} - t_i s_{i+1} = det(R_i) = det(Q_i) \cdots det(Q_1) det(R_0) = (-\rho_{i+1}^{-1}) \cdots (-\rho_2^{-1}) \underbrace{s_0 t_1}_{=\rho_0^{-1}\rho_1^{-1}} =$

   $(-1)^i (\rho_0 \cdots \rho_{i+1})^{-1}$ also eine Einheit!

6. Daraus folgt, dass $ggT(s_i, t_i)$=1 (Einheit wird auf 1 normiert), sonst könnte man oben eine Nichteinheit aus der Determinante ziehen (Lineatrität in Zeile). Man sagt, s_i und t_i sind koprim.
   Sei $p \in R$ Teiler von t_i. Dann gilt: $p|f \Longrightarrow p|s_i f + t_i g = r_i$
   $p|r_i \Longrightarrow p|s_i f = r_i - t_i g \Longrightarrow p|f$ da $ggT(s_i, t_i) = 1$ Also $p|f \Leftrightarrow p|r_i$

7. Mithilfe von 5. erhält man die Inverse von R_i:

   $R_i^{-1} = (-1)^i (\rho_0 \cdots \rho_i + 1) \begin{pmatrix} t_{i+1} & -t_i \\ -s_{i+1} & s_i \end{pmatrix}$ da $\begin{pmatrix} t_{i+1} & -t_i \\ -s_{i+1} & s_i \end{pmatrix} \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix}$

   $= \begin{pmatrix} s_i t_{i+1} - t_i s_{i+1} & 0 \\ 0 & s_i t_{i+1} - t_i s_{i+1} \end{pmatrix}$

   Multipliziere nun beide Seiten von 1. mit R_i^{-1}:

   $\begin{pmatrix} f \\ g \end{pmatrix} = R_i^{-1} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$ und schreibe das LGS aus.

$\diamond$

Zurück zur Idealtheorie:
Das zeigt, dass mit je zwei Elementen auch deren ggT in einem Ideal eines euklidischen Ringes ist.
Spannen also n Elemente $(i_1, \ldots, i_n)$ ein Ideal I auf, so gilt:
$I = (ggT(i_1, \ldots, i_n) = ggT(i_1, ggT(i_2, \ldots ggT(i_{n-1}, i_n) \ldots))$
Mit dem Wissen, dass eukl. Ringe Hauptidealringe sind (das könnte man damit sogar evtl. beweisen, Schwierigkeit: unendlich erzeugte Ideale) kann man sagen, dass ein Ideal I in einem eukl. Ring bereits vom ggT eines bel. Erzeugendensystems erzeugt wird.