Prof. K. Bongartz/
D. Skorodumov
BU Wuppertal
Fachbereich C - Mathematik

Linearen Algebra I WS 08/09

Beispiel 5:

Gesucht wird der größte gemeinsame Teiler der Polynome $P = X^4 - X^3 - 3X^2 - X + 4$ und $Q = X^3 + X^2 + X - 3$ in $\mathbb{Q}[X]$.

Lösung

Benutze den Euklidischen Algorithmus, setze $Q_0 = P$, $Q_1 = Q$ und rechne

$$\begin{array}{r} (X^4\ -X^3-3X^2\ -X+4) : (X^3+X^2+X-3) = X-2 \\ \underline{-(X^4\ +X^3\ +X^2-3X\ \ \ )} \\ -2X^3-4X^2+2X+4 \\ -(\underline{-2X^3-2X^2-2X+6)} \\ -2X^2+4X-2, \end{array}$$

also haben wir

$$\underbrace{X^4 - X^3 - 3X^2 - X + 4}_{=Q_0} = \underbrace{(X-2)}_{=S_1} \cdot \underbrace{(X^3 + X^2 + X - 3)}_{=Q_1} + \underbrace{(-2X^2 + 4X - 2)}_{=Q_2}.$$

Nächster Schritt:

$$\begin{array}{r} (X^3\ +X^2\ +X-3) : (-2X^2+4X-2) = -\frac{1}{2}X - \frac{3}{2} \\ \underline{-(X^3-2X^2\ +X\ \ \ )} \\ 3X^2\ \ \ -3 \\ -(\underline{\ 3X^2-6X+3)} \\ 6X-6, \end{array}$$

also

$$\underbrace{X^3 + X^2 + X - 3}_{=Q_1} = \underbrace{\left(-\frac{1}{2}X - \frac{3}{2}\right)}_{=S_2} \cdot \underbrace{(-2X^2 + 4X - 2)}_{=Q_2} + \underbrace{(6X - 6)}_{=Q_3}.$$

Letzter Schritt:

$$\begin{array}{r} (-2X^2+4X-2) : (6X-6) = -\frac{1}{3}X + \frac{1}{3} \\ \underline{-(-2X^2+2X\ \ \ )} \\ 2X-2 \\ -(\underline{\ 2X-2)} \\ 0, \end{array}$$

die Division geht auf $(Q_4 = 0)$, also ist Q_3 bis auf Normierung der ggT. Weiter erhalten wir durch Rückeinsetzen

$$Q_3 = Q_1 - S_2Q_2 = Q_1 - S_2(Q_0 - S_1Q_1) = (1 + S_1S_2)Q_1 - S_2Q_0$$

beziehungsweise nach Normieren

$$\mathrm{ggT}\,(P,Q) = (P,Q) = \frac{1}{6}Q_3 = X - 1 = \left(-\frac{1}{12}X^2 - \frac{1}{12}X + \frac{2}{3}\right)Q + \left(\frac{1}{12}X + \frac{1}{4}\right)P.$$

Zusatz

Mit dem gleichen Verfahren läßt sich schnell das Inverse in $\mathbb{Z}/p\mathbb{Z}$, p prim, berechnen. Sei etwa $p = 113$, $q = 30$. Gesucht ist $\overline{q}^{-1}$ in $\mathbb{Z}/113\mathbb{Z}$. Setze $q_0 = p$, $q_1 = q$ und rechne

$$\begin{array}{rcll} 113 & = & 3 \cdot 30 + 23 & (q_0 = s_1 q_1 + q_2) \\ 30 & = & 1 \cdot 23 + 7 & (q_1 = s_2 q_2 + q_3) \\ 23 & = & 3 \cdot 7 + 2 & (q_2 = s_3 q_3 + q_4) \\ 7 & = & 3 \cdot 2 + 1. & \end{array}$$

Durch Rückeinsetzen folgt

$$\begin{aligned} 1 = 7 - 3 \cdot 2 = 7 - 3(23 - 3 \cdot 7) = 10 \cdot 7 - 3 \cdot 23 = 10(30 - 23) - 3 \cdot 23 \\ = 10 \cdot 30 - 13 \cdot 23 = 10 \cdot 30 - 13(113 - 3 \cdot 30) = 49 \cdot 30 - 13 \cdot 113. \end{aligned}$$

Der Übergang $\mathbb{Z} \to \mathbb{Z}/113\mathbb{Z}$ liefert

$$\overline{1} = \overline{49} \cdot \overline{30} - \overline{13} \cdot \overline{113} = \overline{49} \cdot \overline{30}, \text{ also } \overline{30}^{-1} = \overline{49}.$$