7

Euklidischer Algorithmus für Polynome

Algebraisch betrachtet bildet $(\mathbb{Z}, +, \cdot)$ einen *euklidischen Ring*. Allgemein heißt ein Integritätsring $(R, +, \cdot)$ *euklidisch*, wenn es eine multiplikative Abbildung $N : R\backslash\{0\} \to \mathbb{N}$ gibt (die so genannte *Normfunktion*), so dass für alle Ringelemente $a, b \in R$, $b \neq 0$, weitere Ringelemente $s, r \in R$ existieren mit $a = sb + r$ wobei $r = 0$ oder $N(r) < N(b)$. Eine Abbildung $N : R\backslash\{0\} \to \mathbb{N}$ heißt genau dann *multiplikativ*, wenn $N(a \cdot b) = N(a) \cdot N(b)$ gilt für alle $a, b \in R$. Für den euklidischen Ring der ganzen Zahlen $\mathbb{Z}$ ist die Normfunktion entsprechend der Betrag $N(a) = |a|$. Einen weiteren euklidischen Ring, den wir nun betrachten werden, bildet der Polynomring $\mathbb{F}[x]$, wobei $\mathbb{F}$ ein Körper ist. Für Polynome $a \in \mathbb{F}[x]$ ist die Normfunktion durch den Grad $N(a) = \deg(a)$ des Polynoms definiert.

Im folgenden schreiben wir $a, b, c, \ldots$ als verkürzte Form für Polynome $a(x), b(x), c(x), \ldots$.

Sei im folgenden $\operatorname{msc}(a)$ der höchstwertige Koeffizient ungleich Null von $a \in \mathbb{F}[x]$ und $\operatorname{lsc}(a)$ der niederwertigste Koeffizient ungleich Null.

Folgendes Theorem haben wir bereits für den endlichen Körper $\mathbb{F} = \mathbb{Z}_p$ formuliert:

THEOREM 7.1. *Für Polynome $a, b \in \mathbb{F}[x], b \neq 0$, existieren eindeutige Polynome $s, r \in \mathbb{F}[x]$ mit $a = sb+r$, wobei $r = 0$ oder $\deg(r) < \deg(b)$ gilt.*

DEFINITION 7.2. Ein Polynom $a \in \mathbb{F}[x]$ *teilt* genau dann ein Polynom $b \in \mathbb{F}[x]$, wenn es ein $c \in \mathbb{F}[x]$ gibt mit $ac = b$. Das Polynom a heißt dann auch ein *Teiler* von b.

DEFINITION 7.3. Eine Zahl $t \in \mathbb{Z}$ heißt genau dann ein *größter gemeinsamer Teiler* von $a, b \in \mathbb{F}[x]$, wenn t ein Teiler von a und b ist und falls jeder Teiler $s \in \mathbb{F}[x]$ von a und b die Zahl t teilt. Die Menge der größten gemeinsamen Teiler von a und b wird mit $\gcd(a, b)$ abgekürzt.

Analog zum Ring der ganzen Zahlen ist der größte gemeinsame Teiler eindeutig bis auf die Menge der Einheiten:

$$\mathbb{F}[x]^* = \mathbb{F}^* = \mathbb{F} \setminus \{0\}$$

Es gilt $t \in \gcd(a,b)$ genau dann, wenn für die gesamte Menge der größten gemeinsamen Teiler $\gcd(a,b) = \{\lambda t \mid \lambda \in \mathbb{F}^*\}$ gilt. Einen *eindeutigen* Repräsentanten erhalten wir, indem ein beliebiges Polynom $t = \sum_{i=0}^{d} t_i x^i \in \gcd(a,b)$ mit $\mathrm{msc}(t) = t_d \neq 0$ normiert wird:

$$\widetilde{t} := \mathrm{msc}(t)^{-1} t = \sum_{i=0}^{d} t_d^{-1} t_i x^i.$$

Analog zu den Regeln für die Menge der größten gemeinsamen Teiler ganzer Zahlen erhalten wir die gleichen Ergebnisse für Polynome, aus denen man leicht den euklidischen Algorithmus in der rekursiven und iterativen Version ableiten kann.

Lemma 7.4. *Für die Menge der größten gemeinsamen Teiler von* $a, b, s \in \mathbb{F}[x]$ *gilt:*

(1) $\gcd(a,b) = \gcd(\pm a, \pm b)$
(2) $\gcd(a,a) = a\mathbb{F}^*$
(3) $\gcd(a,0) = a\mathbb{F}^*$
(4) $\gcd(a,1) = \mathbb{F}^*$
(5) $\gcd(as, bs) = s \gcd(a,b)$
(6) $\gcd(b, a - sb) = \gcd(a,b)$
(7) $\gcd(b, a \bmod b) = \gcd(a,b)$

Die entsprechende Variante des Lemmas von Bézout für Polynome lässt sich wie folgt formulieren.

Lemma 7.5 (Bézout für Polynome). *Für Polynome* $a, b \in \mathbb{F}[x]$ *existieren Polynome* $g, h \in \mathbb{F}[x]$ *mit* $ag + bh \in \gcd(a,b)$.

Mit der Gleichung

$$ag + bh = t \in \gcd(a,b)$$

erhält man eine Darstellung des normierten größten gemeinsamen Teilers $\widetilde{t} = \mathrm{msc}(t)^{-1} t$ durch

$$a\widetilde{g} + b\widetilde{h} = \widetilde{t} \in \gcd(a,b)$$

mit $\widetilde{g} := \mathrm{msc}(t)^{-1} g$ und $\widetilde{h} := \mathrm{msc}(t)^{-1} h$.

Da sich die Versionen des euklidischen und steinschen Algorithmus für Polynome formulieren lassen, geben wir hier ausschließlich den erweiterten steinschen Algorithmus an. Grundlage ist folgendes Lemma.

Lemma 7.6. *Für die Menge der größten gemeinsamen Teiler von* $a, b \in \mathbb{F}[x]$ *gilt:*

(1) $\gcd(a,b) = x \gcd(a/x, b/x)$, *falls* a *und* b *durch* x *teilbar sind.*
(2) $\gcd(a,b) = \gcd(a/x, b)$, *falls* a *durch* x *teilbar und* b *nicht durch* x *teilbar ist.*

Bei dem erweiterten steinschen Algorithmus gehen wir von den beiden invarianten Gleichungen

$$\begin{aligned} ag_1 + bh_1 &= v \\ ag_2 + bg_2 &= u \end{aligned}$$

mit $\deg(v) \geq \deg(u)$ aus, die zu Beginn des Algorithmus mit $v := a$, $u := b$ sowie $g_1 := 1$, $h_1 := 0$, $g_2 := 0$ und $h_2 := 1$ belegt werden.

Wir können davon ausgehen, dass nicht a und b beide durch x teilbar sind, ansonsten, kann man aus beiden Polynomen wiederholt x ausklammern, bis dieser Zustand erreicht wird. Wir nehmen ohne Einschränkung der Allgemeinheit an, dass v durch x teilbar ist und u nicht durch x geteilt werden kann.

Aufgrund von Lemma 7.6 gilt $\gcd(v, u) = \gcd(v/x, u)$, d.h. es muss die Gleichung $ag_1 + bh_1 = v$ derart angepasst werden, dass auf der rechten Seite v/x steht. Je nach Teilbarkeit von g_1 und h_1 durch x entstehen die folgenden vier Fälle:

(1) Falls g_1 und h_1 durch teilbar sind, so gilt

$$a(g_1/x) + b(h_1/x) = v/x.$$

(2) Falls g_1 durch x teilbar und h_1 nicht durch x teilbar ist, dann sind ag_1 und bh_1 durch x teilbar. Folglich ist b durch x teilbar und somit a nicht durch x teilbar. In diesem Fall schreiben wir

$$ag_1 + bh_1 + \operatorname{lsc}(a)^{-1}\operatorname{lsc}(h_1)ab - \operatorname{lsc}(a)^{-1}\operatorname{lsc}(h_1)ab = v$$

bzw.

$$a\frac{(g_1 + \operatorname{lsc}(a)^{-1}\operatorname{lsc}(h_1)b)}{x} + b\frac{(h_1 - \operatorname{lsc}(a)^{-1}\operatorname{lsc}(h_1)a}{x} = \frac{v}{x}.$$

Dabei bezeichnet $\operatorname{lsc}(t)$ den Wert des von Null verschiedenen Koeffizienten des Polynoms $t(x)$ mit dem niedrigsten Index.

(3) Falls g_1 nicht durch x teilbar und h_1 durch x teilbar ist, dann sind ag_1 und bh_1 durch x teilbar. Folglich ist a durch x teilbar und somit b nicht durch x teilbar. In diesem Fall schreiben wir

$$ag_1 + bh_1 + \operatorname{lsc}(b)^{-1}\operatorname{lsc}(g_1)ab - \operatorname{lsc}(b)^{-1}\operatorname{lsc}(g_1)ab = v$$

bzw.

$$a\frac{(g_1 - \operatorname{lsc}(b)^{-1}\operatorname{lsc}(g_1)b)}{x} + b\frac{(h_1 + \operatorname{lsc}(b)^{-1}\operatorname{lsc}(g_1)a}{x} = \frac{v}{x}.$$

(4) Falls g_1 und h_1 nicht durch x teilbar sind, dann sind ag_1 und bh_1 nicht durch x teilbar. Folglich ist a durch x teilbar und

somit b nicht durch x teilbar. In diesem Fall gilt auch
$$a\frac{(g_1 - \operatorname{lsc}(b)^{-1}\operatorname{lsc}(g_1)b)}{x} + b\frac{(h_1 + \operatorname{lsc}(b)^{-1}\operatorname{lsc}(g_1)a}{x} = \frac{v}{x}.$$
Insgesamt erhalten wir folgenden Algorithmus:

Algorithmus 7.7. Erweiterter steinscher Alg. (iterativ)
Input: $a, b \in \mathbb{F}[x]$ mit $\deg(a) \geq \deg(b)$
Output: (t, g, h) mit $ag + bh = t \in \gcd(a, b)$

$a' := a$, $b' := b$, $e := 1$
while a' and b' are divisible by x do
    $a' := a'/x$, $b' := b'/x$, $e := xe$
$g_1 := 1$, $h_1 := 0$, $v := a'$
$g_2 := 0$, $h_2 := 1$, $u := b'$
while $u \neq 0$ do
    while v is divisible by x do
        $v := v/x$
        if g_1 and h_1 are divisible by x then
            $g_1 := g_1/x$, $h_1 := h_1/x$
        else if g_1 is divisible by x and h_1 is not divisible by x then
            $\lambda := \operatorname{lsc}(a)^{-1}\operatorname{lsc}(h_1)$
            $g_1 := (g_1 + \lambda b')/x$, $h_1 := (h_1 - \lambda a')/x$
        else
            $\lambda := \operatorname{lsc}(b)^{-1}\operatorname{lsc}(g_1)$
            $g_1 := (g_1 - \lambda b')/x$, $h_1 := (h_1 + \lambda a')/x$
    while u is divisible by x do
        $u := u/x$
        if g_2 and h_2 are divisible by x then
            $g_2 := g_2/x$, $h_2 := h_2/x$
        else if g_2 is divisible by x and h_2 is not divisible by x then
            $\lambda := \operatorname{lsc}(a)^{-1}\operatorname{lsc}(h_2)$
            $g_2 := (g_2 + \lambda b')/x$, $h_2 := (h_2 - \lambda a')/x$
        else
            $\lambda := \operatorname{lsc}(b)^{-1}\operatorname{lsc}(g_2)$
            $g_2 := (g_2 - \lambda b')/x$, $h_2 := (h_2 + \lambda a')/x$
    if $\deg(v) \geq \deg(u)$ then
        $\lambda := \operatorname{lsc}(u)^{-1}\operatorname{lsc}(v)$
        $v := v - \lambda u$, $g_1 := g_1 - \lambda g_2$, $h_1 := h_1 - \lambda h_2$
    else
        $\lambda := \operatorname{lsc}(v)^{-1}\operatorname{lsc}(u)$
        $u := u - \lambda v$, $g_2 := g_2 - \lambda g_1$, $h_2 := h_2 - \lambda h_1$
return (ev, eg_1, eh_1)