WS 2005/06

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2005WS/ds/index.html.de

25. November 2005

Satz 122

Seien $a, b \in \mathbb{N}$. *Dann gibt es* $c, d \in \mathbb{Z}$, *so dass*

$$c \cdot a + d \cdot b = \mathrm{ggT}(a, b)\,.$$

Beweis:

Sei o.B.d.A. $a > b$. Der Euklidische Algorithmus (fortgesetzte ganzzahlige Division mit Rest) (Euklid von Alexandria, ca. 325–265 v. Chr.) liefert eine Folge

$$
\begin{aligned}
r_0 := a &= q_2 \cdot b + r_2 && \text{, mit } 0 < r_2 < b, q_2, r_2 \in \mathbb{N}_0 \\
r_1 := b &= q_3 \cdot r_2 + r_3 && \text{, mit } 0 < r_3 < r_2, q_3, r_3 \in \mathbb{N}_0 \\
r_2 &= q_4 \cdot r_3 + r_4 && \text{, mit } 0 < r_4 < r_3, q_4, r_4 \in \mathbb{N}_0 \\
&\vdots \\
r_{m-3} &= q_{m-1} \cdot r_{m-2} + r_{m-1} && \text{, mit } 0 < r_{m-1} < r_{m-2} \qquad (*) \\
r_{m-2} &= q_m \cdot r_{m-1} + r_m && \text{, mit } 0 = r_m < r_{m-1}
\end{aligned}
$$

Dann gilt $r_{m-1} | a$ und $r_{m-1} | b$ sowie $\mathrm{ggT}(a, b) | r_{m-1}$.
Also $r_{m-1} = \mathrm{ggT}(a, b)$.
Rückwärtiges iteratives Ersetzen von $r_{m-2}, r_{m-3}, \ldots$ in Gleichung (*) entsprechend den vorhergehenden Gleichungen liefert die gewünschte Darstellung. □

Satz 123

Bezeichnet man mit $+_n$ und $\cdot_n$ die Addition bzw. Multiplikation modulo n, so gilt:

$$\langle \mathbb{Z}_n, +_n, \cdot_n \rangle \text{ ist ein Körper} \quad \Longleftrightarrow \quad n \text{ ist Primzahl .}$$

Beweis:

Die Axiome K1 und K3 sind durch die Addition und Multiplikation modulo n offensichtlich erfüllt. Wir haben bereits gesehen, dass a modulo n genau dann ein multiplikatives Inverses hat, wenn a und n teilerfremd sind, also

$$\mathrm{ggT}(a, n) = 1 \; .$$

Falls n prim ist, gilt dies für alle a, $1 \leq a < n$.
Umgekehrt kann $\mathrm{ggT}(a, n) = 1$ für alle a, $1 \leq a < n$ nur gelten, falls n prim ist. □

2.2 Multiplikative Gruppe endlicher Körper

Satz 124

In jedem endlichen Körper K ist die multiplikative Gruppe $K^* = K \setminus \{0\}$ zyklisch, d.h. es gibt ein Element $g \in K^*$ mit $K^* = \{1, g, g^2, \ldots, g^{|K|-2}\}$.

Beweis:

Es gilt: $\mathrm{ord}(a) < \infty$ für alle $a \in K^*$. Sei a ein Element in K^* mit maximaler Ordnung:

$$\max\{\mathrm{ord}(b) \mid b \in K^*\} = \mathrm{ord}(a) \ .$$

Es ist zu zeigen, dass $\mathrm{ord}(a) = |K| - 1$. Dazu betrachten wir das Polynom $x^{\mathrm{ord}(a)} - 1$, das Grad $\mathrm{ord}(a)$ hat.
Für jedes $b \in K^*$ gilt, dass $\mathrm{ord}(b) \mid \mathrm{ord}(a)$ (da sonst ab größere Ordnung als a hätte). Also ist jedes Element von K^* eine Nullstelle des obigen Polynoms. Da ein Polynom vom Grad k höchstens k verschiedene Nullstellen haben kann (warum?), folgt daraus $\mathrm{ord}(a) \geq |K^*| = |K| - 1$. □

2.3 Primitive Elemente

Definition 125

Sei K ein endlicher Körper. Ein Element a, das die multiplikative Gruppe $K^* = K \setminus \{0\}$ erzeugt, nennt man primitives Element.

Beispiel 126

In $\mathbb{Z}_5^*$ sind sowohl 2 als auch 3 primitive Elemente:

$$\begin{aligned} 2^0 &= 1 \\ 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 3 \\ (2^4 &= 1 \end{aligned} \qquad \begin{aligned} 3^0 &= 1 \\ 3^1 &= 3 \\ 3^2 &= 4 \\ 3^3 &= 2 \\ 3^4 &= 1) \end{aligned}$$

Bemerkung: $\langle \mathbb{Z}_4, +_4, \cdot_4, 0, 1 \rangle$ ist kein Körper!

Beispiel 127

Setzt man $K = \{0, 1, a, b\}$ und definiert eine Addition und Multiplikation wie folgt:

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

so bildet $\langle K, \oplus, \odot, 0, 1 \rangle$ einen Körper (Übung!).

3. Polynome

3.1 Definition und Grundlagen

Definition 128
Sei R ein (kommutativer) Ring. Ein Polynom über R in der Variablen x ist eine Funktion p der Form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ ,$$

wobei $n \in \mathbb{N}_0$, $a_i \in R$ und $a_n \neq 0$.
n heißt der Grad des Polynoms, $a_0, \ldots, a_n$ seine Koeffizienten.
$R[x]$ bezeichnet die Menge der Polynome über dem Ring R in der Variablen x.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel 129

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

3.2 Rechnen mit Polynomen

Berechnung des Funktionswertes

Um den Wert eines Polynoms an einer bestimmten Stelle $x_0 \in R$ zu bestimmen, verwendet man besten das sogenannte Hornerschema:

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ &= ((\ldots(((a_n x + a_{n-1})x + a_{n-2})x + \ldots.)x + a_1)x + a_0. \end{aligned}$$

Hat man die Koeffizienten in einem Array $a[0..n]$ abgespeichert, kann man den Funktionswert $p(x_0)$ daher wie folgt berechnen:

```
begin
   p ← a[n]
   for i = n-1 downto 0 do
      p ← p · x_0 + a[i]
   end
   return(p)
end
```

Beobachtung:
Für die Auswertung eines Polynoms vom Grad n genügen damit $O(n)$ Multiplikationen und Additionen.

Addition

Die Summe zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_n x^n + \cdots + b_1 x + b_0$ ist definiert durch

$$(a+b)(x) = c_n x^n + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = a_i + b_i \ .$$

Bemerkungen:

- An sich fehlende Koeffizienten sind gleich 0 gesetzt.
- Für den Grad des Summenpolynoms gilt

$$\mathrm{grad}(a+b) \leq \max\{\mathrm{grad}(a), \mathrm{grad}(b)\} \ .$$

Beispiel 130

1. Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich $(a+b)(x) = x^2 + x + 7$.
   Hier gilt $\mathrm{grad}(a+b) = 2 = \mathrm{grad}(a)$.
2. Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 1$ ergibt sich hingegen $(a+b)(x) = 2$ und somit
   $\mathrm{grad}(a+b) = 0 < 3 = \max\{\mathrm{grad}(a), \mathrm{grad}(b)\}$.

Beobachtung:
Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad $\leq n$ lässt sich in $O(n)$ arithmetischen Schritten berechnen.

Multiplikation

Das Produkt zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ erhält man durch Ausmultiplizieren und anschliessendes Sortieren und Zusammenfassen der Koeffizienten. Also

$$(a \cdot b)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Für den Grad des Produktpolynoms gilt

$$\operatorname{grad}(a \cdot b) = \operatorname{grad}(a) + \operatorname{grad}(b) \ ,$$

falls R nullteilerfrei ist, ansonsten

$$\operatorname{grad}(a \cdot b) \leq \operatorname{grad}(a) + \operatorname{grad}(b) \ .$$

Beispiel 131

Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich

$$\begin{aligned}(a \cdot b)(x) &= (1 \cdot 4)x^3 + (1 \cdot 2 + (-3) \cdot 4)x^2 + \\ &\qquad ((-3) \cdot 2 + 5 \cdot 4)x + 5 \cdot 2 \\ &= 4x^3 - 10x^2 + 14x + 10\,.\end{aligned}$$

Man sagt auch, dass die Koeffizienten

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

des Produktpolynoms durch Faltung der Koeffizientenfolgen von $a(x)$ und $b(x)$ entstehen.

Beobachtung:
Das Produkt zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Es gibt dafür aber auch schnellere Algorithmen!