Seminar Computeralgebra

Sebastian Wenzel

Effiziente Faktorisierung in $Z_p[x]$

1. Einführung
2. Faktorisierung
   - Berlekamp teil 1
   - Berlekamp teil 2
   - Quadratfrei
3. Fazit

Warum Faktorisierung in $Z_p[x]$

Ziel = faktorisieren von Polynomen aus Q[x]

$\frac{1}{2}x^4+\frac{3}{5}x^3+x^2+4x+20$ => Umwandeln in Z[x]?

Durch multiplizieren mit dem KGV aller Nenner wird Q[x] verlassen

$10 \cdot \frac{1}{2}x^4+\frac{3}{5}x^3+x^2+4x+20$ **ó** $5x^4+6x^3+10x^2+40x+200$

Somit haben wir jetzt ein Polynom aus Z[x]

Genauso sollte es möglich sein Polynome aus Z[x] zu vereinfachen!

$\frac{1}{2}\cdot 10x^4+12x^3+20x^2+80x+400$ **ó** $5x^4+6x^3+10x^2+40x+200$

Warum Faktorisierung in $Z_p[x]$

Somit können wir viele Polynome vereinfachen

a(x) = s b(x)

Hierbei soll gelten: a(x) $\in$ Q[x] und b(x) $\in$ Z[x] = „primitiv“ und s$\in$ Q

Welches wir auch definieren mit:

Der GGT aller Koeffizienten = 1

oder

Alle Koeffizienten sind teilerfremd

Was fehlt um faktorisieren zu können?

$$a(x) = a_1(x) \cdot a_2(x) \cdot \ldots \cdot a_n(x)$$

Wie sieht es also mit der Polynom Multiplikation aus?

Das Produkt von 2 primitiven Polynomen ist wieder primitiv

Warum Faktorisierung in $Z_p[x]$

Es gelte a(x) und b(x) primitiv und c(x)=a(x) b(x) dann sei c(x) primitiv mit: Dann ist:

$$a(x) = \sum_{j=0}^{n} a_j x^j \quad b(x) = \sum_{k=0}^{m} b_k x^k \qquad c(x) = \sum_{l=0}^{m+n} c_l x^l \quad c_l = \sum_{j+k=l} a_j b_k$$

Nun suchen wir uns ein p aus den Primzahlen heraus und schauen ob dieses p alle Koeffizienten von c(x) teilt

Wie teilt p die Koeffizienten von a(x) und b(x)?

-Bei beiden Polynomen gibt es mindestens einen Koeffizienten der von p nicht geteilt wird

Warum Faktorisierung in $Z_p[x]$

Nun wählen wir ein j_0 und ein k_0 so aus das gilt :
p teilt a_j für alle j < j_0
p teilt b_k für alle k < k_0
und
p teilt a_{j_0} nicht
p teilt b_{k_0} nicht

Nun mit $l_0 = j_0 + k_0$ betrachten wir $c_{l_0} = \sum_{j+k=l_0} a_j b_k$

Dies kann man allerdings auch anders darstellen :

$$c_{l_0} = \sum_{j+k=l_0}^{k>k_0,\, j<j_0} a_j b_k + \sum_{j+k=l_0}^{j>j_0,\, k<k_0} a_j b_k + a_{j_0} b_{k_0}$$

Damit teilt p c_{l_0} nicht und damit ist c(x) primitiv

Teil 1 Berlekamp

Sei a(x) das zu faktorisierende Polynom

Dann gebe es ein Polynom b(x) so das gilt:
- b(x) ist vom grad her kleiner als a(x)
- b(x) ist nicht das Nullpolynom
- a(x) teilt $b(x)^p - b(x)$
- bzw.
- a(x) teilt $\prod_{k=0}^{p-1} (b(x) - k)$

Teil 1 Berlekamp

b(x) ist vom grad her kleiner als a(x)
b(x) ist nicht das Nullpolynom
a(x) teilt $b(x)^p - b(x)$
bzw.
a(x) teilt $\prod_{k=0}^{p-1}(b(x)-k)$

Wenn diese Bedingungen gelten können wir eine Faktorisierung von a(x) bilden, denn:

a(x) teilt $ggT(a(x), \prod_{k=0}^{p-1}(b(x)-k))$

da im ggT gilt : Sind a und b teilerfremd, dann ist $ggT(ab, m) = ggT(a, m) \cdot ggT(b, m)$
und da für alle Werte k= 0,...,p-1 die Polynome b(x) – k paarweise teilerfremd sind gilt auch:

a(x) teilt $\prod_{k=0}^{p-1}(ggT(a(x), b(x)-k))$

Hierdurch gilt auch alle Werte k= 0,...,p-1 $ggT(a(x), b(x)-k)$ teilt a(x)

Da wieder alle Polynome b(x) – k teilerfremd sind gilt ebenfalls

$\prod_{k=0}^{p-1}(ggT(a(x), b(x)-k))$ teilt a(x)

Teil 1 Berlekamp

Damit gilt a(x) = $\prod_{k=0}^{p-1}(ggT(a(x), b(x)-k))$ und damit ist dies eine Faktorisierung von a(x)

Damit haben wir das Problem soweit vereinfacht,
so dass wir nun nur das Polynom b(x) finden müssen

Sei a(x) vom Grad n dann hat b(x) die Struktur $b_{n-1}x^{n-1} + ... + b_1x + b_0$
wobei $b_{n-1} = 0$ gelten kann. Dann ist:

$$\begin{aligned} b(x)^p &= (b_{n-1}x^{n-1} + ... + b_1x + b_0)^p \\ &= b_{n-1}^p x^{(n-1)p} + ... + b_1^p x^p + b_0^p \\ &= b_{n-1}x^{(n-1)p} + ... + b_1x^p + b_0 \end{aligned}$$

Teil 1 Berlekamp

$b(x)^p = b_{n-1}x^{(n-1)p} + \ldots + b_1 x^p + b_0$

Nun nehmen wir uns diesen Term und Dividieren die x mit a(x)
und merken uns den Rest und die Quotienten

$x^{jp} = a(x)q_j(x) + r_j(x)$ mit j= 0,...,n-1

Da wir definiert haben a(x) teilt $b(x)^p - b(x)$ gilt dies genau dann wenn a(x)
$b_{n-1}r_{n-1}(x) + \ldots + b_1 r_1(x) + b_0 - b(x)$ teilt

Allerdings ist dieses Polynom vom Grad her kleiner als a(x).
Damit kann a(x) nur diese Polynom teilen wenn es dass Nullpolynom ist.
$b_{n-1}r_{n-1}(x) + \ldots + b_1 r_1(x) + b_0 - b(x) = 0$ **ó** $b_{n-1}r_{n-1}(x) + \ldots + b_1 r_1(x) + b_0 = b(x)$

Diese Gleichungssystem kann mit Koeffizienten vergleich gelöst werden.

Teil 1 Berlekamp

Beispielrechnung mit a(x) = (x + 2)(x² + 1) = x³ + 2x² + x + 2 in Z_p p=3

1. Bestimmen der Reste

$\frac{x^{0\cdot 3}}{a(x)} rest = 1$ $\frac{x^{1\cdot 3}}{a(x)} rest = 1 + 2x + x^2$ $\frac{x^{2\cdot 3}}{a(x)} rest = x^2$

2. Bestimmen der Koeffizienten von b(x)

$b_2x^2 + b_1(1 + 2x + x^2) + b_0 = b_2x^2 + b_1x + b_0$
$b_2x^2 + b_1x^2 + 2b_1x + b_1 + b_0 = b_2x^2 + b_1x + b_0$
$b_1x^2 + b_1x + b_1 = 0$

Das zeigt und das $b_1 = 0$ sein muss und b_2 und b_0 frei wählbar sind allerding so das b(x)
nicht das Nullpolynom ist. Zur einfachen Weiterarbeit sei b(x) = x² + 2

1.Bestimmen der Reste
2.Bestimmen der Koeffizienten von b(x)
3.Berechnen der GGT zur Bestimmung der Faktorisierung

Teil 1 Berlekamp

$a(x) = (x + 2)(x^2 + 1) = x^3 + 2x^2 + x + 2$

3. Berechnen der ggTs zur Bestimmung der Faktorisierung

$ggT(a(x),b(x)\text{-}0) = ggT(x^3 + 2x^2 + x + 2 , x^2 + 2) = x+2$
$ggT(a(x),b(x)\text{-}1) = ggT(x^3 + 2x^2 + x + 2 , x^2 + 1) = x^2 + 1$
$ggT(a(x),b(x)\text{-}2) = ggT(x^3 + 2x^2 + x + 2 , x^2) = 1$

Damit haben wir die Faktorisierung gefunden

$x^3 + 2x^2 + x + 2 = 1 \quad (x + 2) \quad (x^2 + 1)$

Dabei sei zu Beachten, das hier die Selbe Faktorisierung wie in Z[x] herausgekommen ist, hat mit der Wahl von p zu tun.

Denn bei p = 5 währe z.B. herausgekommen $x^3 + 2x^2 + x + 2 = 1 \quad (4+4x+x^2) \quad (3+x) = x^3 + 7x^2 + 16x + 12$

Teil 2 Berlekamp

Neben dem Ergebnis der Faktorisierung kann durch den Berlekamp als Nebeneffekt die genaue Anzahl der verschiedenen irreduziblen Faktoren bestimmt werden

Hierzu schauen wir uns den eben gebildeten Algorithmus mal anders an.

$$R = \begin{pmatrix} r_{0,0} & r_{0,1} & \mathbf{L} & r_{0,n-1} \\ r_{1,0} & r_{1,1} & \mathbf{L} & r_{1,n-1} \\ \mathbb{M} & \mathbb{M} & \mathbf{O} & \mathbb{M} \\ r_{n-1,0} & r_{n-1,1} & \mathbf{L} & r_{n-1,n-1} \end{pmatrix}$$

sei eine n x n Matrix, welche aus den Koeffizienten der Restpolynome gebildet wird dabei sind $r_{a,b}$ gebildet aus a kommt von $r_a(x)$ und b kommt von x^b

$b_{n-1}r_{n-1}(x) + ... + b_1r_1(x) + b_0 - b(x) = 0$ kann man dadurch umformen in

$$(R - E) \cdot \begin{pmatrix} b_0 \\ b_1 \\ \mathbb{M} \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \mathbb{M} \\ 0 \end{pmatrix}$$

wobei E die n x n Einheitsmatrix ist und b(x) repräsentiert

Teil 2 Berlekamp

$$(R-E)\cdot\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Anhand der Matrix (R – E) können wir nun ablesen wie viele Faktoren a(x) besitzt.

Dafür müssen wir nur die Dimension der Matrix bestimmen und dann ist
J = N – D mit:
N = Anzahl der Restegleichungen
D = Rang der Matrix

Gezeigt am vorherigen Beispiel a(x) = (x + 2)(x² + 1) = x³ + 2x² + x + 2 in Z_p p=3
Wir haben wieder die Reste:

$$\frac{x^{0\cdot 3}}{a(x)} rest = 1 \qquad \frac{x^{1\cdot 3}}{a(x)} rest = 1 + 2x + x^2 \qquad \frac{x^{2\cdot 3}}{a(x)} rest = x^2$$

Teil 2 Berlekamp

$$(R-E)\cdot\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\frac{x^{0\cdot 3}}{a(x)} rest = 1 \qquad \frac{x^{1\cdot 3}}{a(x)} rest = 1 + 2x + x^2 \qquad \frac{x^{2\cdot 3}}{a(x)} rest = x^2$$

Damit ist $R = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ und $R - E = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ Damit ist der Rang von R – E = 1
Und die Anzahl der Faktoren = 3 – 1 = 2 so wie es gewollt war

Nach Anwendung dieser Algorithmen stellen wir fest das wir eine Faktorisierung in Verschiedene Faktoren finden, welche allerdings noch Quadrate enthalten.

Daher sollte stets, vor Anwendung des Berlekamp Algorithmus, eine quadratfreie Faktorisierung vorgenommen werden.

Quadratfrei in $Z_p[x]$

Nun wird ein Algorithmus beschrieben für $a(x) \in$ GF(q)[x] wenn gilt:
$a'(x) = 0$ ist
$q = p^n$ mit p als Primzahl
$b(x)^p$ sei das Ergebnis der Faktorisierung

Da $a'(x) = 0$ müssen alle Potenzen in a(x) durch p teilbar sein.

$$a(x) = a_0 + a_p x^p + \mathbf{K} + a_{kp} x^{kp}$$

Dann wählen wir

$$b(x) = b_0 + b_1 x + \mathbf{K} + b_k x^k \text{ mit } b_j = a_{jp}^{p^{n-1}}$$

Mit dieser Wahl ergibt sich:

$$\begin{aligned} b(x)^p &= (b_0 + b_1 x + \mathbf{K} + b_k x^k)^p \\ &= b_0^p + b_1^p x^p + \mathbf{K} + b_k^p x^{kp} \\ &= a_0 + a_p x^p + \mathbf{K} + a_{kp} x^{kp} = a(x) \end{aligned}$$

Gilt allerdings $a'(x) = 0$ nicht so muss und kann auf andere Algorithmen zugegriffen werden

Quadratfrei in $Z_p[x]$

Beispiel für $a(x) = 1 + 2x^{17} + 3x^{34} = (1 + 2x + 3x^2)^{17}$ in $Z_q[x]$ mit $q = p^n = 17^1$:

$$a'(x) = 17 \cdot 2x^{16} + 17 \cdot 6x^{33} = 0$$

Dann bestimmen wir das neue Polynom b(x) mit :

$b_j = a_{jp}^{p^{n-1}}$ für j = {0,1,2}

$b_0 = 1^{17^0} = 1 \qquad b_1 = 2^{17^0} = 2 \qquad b_2 = 3^{17^0} = 3$

Damit ist $b(x) = 1 + 2x + 3x^2$ und unsere Faktorisierung mit $a(x) = b(x)^p$ korrekt

Fazit

Wir haben gelernt, dass es genügt, um Polynome in Q[x] zu faktorisieren sich auf den Raum Z[x] zu beschränken.

Ebenfalls ist es einfach, bei intelligent Gewählten p, im Raum $Z_p[x]$ an viele Informationen zu kommen ohne den kompletten Raum Z[x] zu betrachten

Der Berlekamp Algorithmus hat die Vorteile durch die Arbeit in $Z_p[x]$, allerdings kann bei zu groß gewählten p langen Laufzeiten kommen.

Bessere und schnellere Algorithmen währen im nächsten Vortrag vorgestellt worden wem durch diesen Vortrag Interesse geweckt wurde kann sich im Koepf ab Kapitel 8.4 mehr Informationen hohlen.

ENDE

Fragen ???