

Kostenanalyse von EAA für $F[x]$: Kosten für s und t

Die Kosten für die r_i und q_i sind $\sum_{1 \leq i \leq l} (2n_i + 1)(n_{i-1} - n_i + 1)$
 Operationen in F . Normaler Fall: $n_i = n_{i-1} - 1 = \dots = m - i + 1$
 $2 \leq i \leq l = m + 1 \leq 2mn + 2m$.

2.11 Lemma Sei s_i Wert von c_1 in Durchgang i und t_i Wert von c_2 in Durchgang i . Dann gilt

1. $\text{grad } s_i = \sum_{2 \leq j < i} \text{grad } q_j = n_1 - n_{i-1} \quad 2 \leq i \leq l + 1$
2. $\text{grad } t_i = \sum_{1 \leq j < i} \text{grad } q_j = n_0 - n_{i-1} \quad 1 \leq i \leq l + 1$

Beweis: Wir zeigen nur 1) und $\text{grad } s_{i-1} < \text{grad } s_i \quad (2 \leq i \leq l)$ durch Induktion nach i .

$i = 2$: $s_2 = (s_0 - q_1 s_1) = 1 - q_1 \cdot 0$, $\text{grad } s_1 = -\infty < 0 = \text{grad } s_2$.

Sei $i \geq 2$ Behauptung richtig für $2 \leq j \leq i$, dann

$$\text{grad } s_{i-1} < \text{grad } s_i < n_{i-1} - n_i + \text{grad } s_i = \text{grad } (q_i s_i)$$



Kostenanalyse von EAA für $F[x]$: Kosten für s und t

Also $\text{grad } s_{i+1} = \text{grad } (s_{i-1} - q_i s_i) = \text{grad } q_i + \text{grad } s_i > \text{grad } s_i$
 und

$$\text{grad } s_{i+1} = \text{grad } q_i + \text{grad } s_i = \sum_{2 \leq j < i} \text{grad } q_j + \text{grad } q_i = \sum_{2 \leq j < i+1} \text{grad } q_j$$

Die Berechnung $t_{i+1} = (t_{i-1} - q_i t_i)$ bzw. $s_{i+1} = (s_{i-1} - q_i s_i)$.

Multiplikation von Pol $\text{grad } n, m : \leq 2(n+1)(m+1)$ Operationen.

$2(\text{grad } t_i + 1)(\text{grad } q_i + 1) + (\text{grad } t_{i+1} + 1)$, d. h.

$$\sum_{2 \leq i \leq l} 2(n_0 - n_{i-1} + 1)(n_{i-1} - n_i + 1) + (n_0 - n_i + 1)$$

Normalfall

$$\sum_{2 \leq i \leq m+1} 2(n - m + i - 1)2 + n - (m - i + 1) + 1 =$$

$$\sum_{2 \leq i \leq m+1} 5n - 5m + 5i - 4 = 5nm - 5mm + \frac{5}{2}m(m+1) + O(m)$$



Kostenanalyse für \mathbb{Z} : Langzahlarithmetik

Darstellung von Zahlen: Wort 64 Bits. **2^{64} -Standard Darstellung:** Zahl als Feld von Wörtern. Erstes Wort für Vorzeichen und Länge des Feldes, d. h. $a \in \mathbb{Z}$

$$a = (-1)^s \sum_{0 \leq i \leq n} a_i 2^{64i}$$

$s \in \{0, 1\}, 0 \leq n + 1 < 2^{63}, a_i \in \{0, \dots, 2^{64} - 1\}$.

Als Feld: $s2^{63} + n + 1, a_0, \dots, a_n$ von 64 Bit-Wörtern, z. B.

$-1 : 2^{63} + 1, 1$ und $1 : 1, 1$.

Bereich: $-2^{64} \cdot 2^{63} + 1$ bis $2^{64} \cdot 2^{63} - 1$.

Länge von a : $\lambda(a) = \lfloor \log_{2^{64}} |a| \rfloor + 1 = \lfloor \frac{\log_2 |a|}{64} \rfloor + 1$.

Allgemein: Darstellung zur Basis b mit $2 \leq b < \frac{|w|}{2}$, wobei $|w|$ Wortlänge ist (Multiplikation der Koeffizienten in Wort).

$a = (u_1 \dots u_n)_b, 0 \leq u_i < b$, d. h. $a = \sum_{i=1}^n u_i b^{n-i}$

$= u_n + u_{n-1}b + \dots + u_1 b^{n-1}$ a ist n -stellig zur Basis b .

$$a < b^n \rightsquigarrow a \text{ hat Länge } \leq n.$$



Langzahlarithmetik: Klassische Algorithmen

Klassische Algorithmen für: $+, -, \cdot, \text{quo}$, Exponentiation

Maß in Grundoperationen (go):

- ▶ Addition, Subtraktion von 1-stelligen Zahlen
- ▶ Multiplikation von 1-stelligen Zahlen
- ▶ Division von 1-stelligen Zahlen



Algorithmen: Addition

A: Addition nicht negativer ganzer Zahlen zur Basis b .

Eingabe: $(u_1 \cdots u_n)_b$ $(v_1 \cdots v_n)_b$

Ausgabe: $(w_0 \cdots w_n)_b$ w_0 Übertrag mit
 $(u_0 \cdots u_n)_b + (v_1 \cdots v_n)_b = (w_0 \cdots w_n)_b$

```

begin
  j := n; k := 0                                {k = Übertrag}
  while j > 0 do
    begin
      w_j := (u_j + v_j + k) mod b;                {k ∈ {0, 1}}
      k := ⌊(u_j + v_j + k)/b⌋;
      j := j - 1;
    end
  end
  w_0 := k;
end.

```

Korrektheit! Aufwand $\approx 2n$ go.



Algorithmen: Substraktion

S: Substraktion nicht negativer ganzer Zahlen.

Eingabe: $(u_1 \cdots u_n)_b \geq (v_1 \cdots v_n)_b$

Ausgabe: Nichtnegative Differenz: $u - v = (w_1 \cdots w_n)_b$

```

begin
  j := n; k := 0
  while j > 0 do
    begin
      w_j := (u_j - v_j + k) mod b;
      k := ⌊(u_j - v_j + k)/b⌋                {k ∈ {0, -1}}
      j := j - 1;
    end
  end
end.

```

Korrektheit! Aufwand $\approx 2n$ go.



Algorithmen: Multiplikation

M: Multiplikation nicht negativer ganzer Zahlen Basis b .

Eingabe: $(u_1 \cdots u_n)_b \geq (v_1 \cdots v_m)_b$, d. h. $n \geq m$

Ausgabe: Produkt $u \cdot v = (w_1 \cdots w_{m+n})_b$

```

for i from 1 to n do
  w_{m+i} := 0;                                {Initialisierung m + i - te Stelle}
  j := m;
  while j > 0 do
    begin
      if v_j = 0 then
        w_j := 0
      else
        begin
          i := n; k := 0;
          while i > 0 do
            t := u_i v_j + w_{i+j} + k; w_{i+j} := t mod b; k := ⌊t/b⌋; i := i - 1;
            w_j := k;
          end
        end
      j := j - 1;
    end
  end
end

```

{Korrektheit! Aufwand $\approx 3nm$ go}



Algorithmen: Motivation für Multiplikationsalg.

$$(u_1 \cdots u_n)(v_1 \cdots v_m)$$

$$\left. \begin{matrix} (u_1 v_m) \cdots (u_{n-1} v_m)(u_n v_m) \\ (u_1 v_{m-1}) \cdots (u_n v_{m-1}) \end{matrix} \right\} m$$

$$(u_1 v_1) \cdots (u_n v_1)$$

$$w_1 \cdots w_m w_{m+1} \cdots w_{n+m}$$



Aufwand für EEA über \mathbb{Z}

Sei $n = \lambda(a), m = \lambda(b) \rightsquigarrow O(nm)$ für EA
(Kosten der Div mit Rest $a = qb + r \quad O((\lambda(a) - \lambda(b)) \cdot \lambda(b))$ go)
Für die Bezout Koeffizienten gilt analog
 $|s_i| \leq \frac{b}{r_{i-1}}$ und $|t_i| \leq \frac{a}{r_{i-1}} \quad 1 \leq i \leq l + 1$

2.14 Satz Der EEA für Zahlen $a, b \in \mathbb{N} \quad \lambda(a) = n \geq \lambda(b) = m$, kann mit $O(nm)$ go durchgeführt werden.

Weitere Ergebnisse und Bemerkungen siehe von zu Gathen, Gerhard bzw. Mignotte. Siehe auch Knuth Kap. 4.5.3, Bach/Shallit 4.2, 4.3.
Viele Varianten zur Berechnung vom GGT (z. B. ohne Division).
KGV Kleinste gemeinsamer Vielfache (LCM)

$$\text{KGV}(a, b) = \frac{|ab|}{\text{GGT}(a, b)}$$

Reduktion auf GGT-Berechnung.

Ringkonstruktionen: $R[x]$ Polynomring

R ZPE, so $R[x]$ ZPE-Ring. R euklidisch $\not\Rightarrow R[x]$ euklidisch
z. B. $\mathbb{Z}[x]$ nicht euklidisch, da kein Hauptidealring (z. B. $\langle 2, x \rangle$ wird nicht von $a(x) \in \mathbb{Z}[x]$ erzeugt oder $\mathbb{Q}[x, y]$ nicht euklidisch, da kein Hauptidealring (z. B. $\langle x, y \rangle$).

Vorteile E-Ringe: Euklidischer Algorithmus für GGT Berechnung.

Anwendungen: Lösung diophantischer Gleichungen in $F[x] : a(x), b(x), c(y)$ gesucht $\sigma(x)$ und $\tau(x)$ mit

$$\sigma(x)a(x) + \tau(x)b(x) = c(x)$$

Lösbar für $g(x) = \text{GGT}(a(x), b(x)) | c(x)$. Eindeutigkeit und Schranken für die Grade von $\sigma(x), \tau(x)$ (Übung).

Zerlegung rationaler Funktionen:

$$\frac{c(x)}{a(x)b(x)} = \frac{\tau(x)}{a(x)} + \frac{\sigma(x)}{b(x)} \rightsquigarrow \text{Integration}$$

Problem: wie berechnet man GGT in $\mathbb{Z}[x]$ oder $\mathbb{Q}[x, y]$.
 \rightsquigarrow Pseudodivision primitiver EA.

Quotienten-Körper von Integritätsbereichen

Übergang von $\mathbb{Z} \rightsquigarrow \mathbb{Q}$. D : Integritätsbereich \rightsquigarrow Körper.

Setze: $S = \{a/b : a \in D, b \in D - \{0\}\}$ formale Quotienten.

\sim auf S : $a/b \sim c/d$ gdw $ad = bc$ ist Äquivalenzrelation auf $S \quad [a/b]$

$S/\sim = \{[a/b] : a \in D, b \in D - \{0\}\}$, $a/b \in [a/b]$ Repräsentant.

Addition + Multiplikation auf S/\sim :

$$(a/b) + (c/d) = (ad + bc)/bd$$

$$(a/b) \cdot (c/d) = ac/bd$$

wohldefiniert auf Äquivalenzklassen.

S/\sim ist Körper: $Q(D) \quad (F_D)$: Quotientenkörper von D .

Kleinster Körper, der D enthält, $D \cong \{[a/1] : a \in D\}$

$0/1 \quad 1/1 \quad a/1$ mit a identifiziert.

Praxis: eindeutige Repräsentanten für $[a/b]$, Entscheidung für \sim .

Falls GGT in D existiert:

$a/b \in [a/b] \in S$ ist Repräsentant, falls $\text{GGT}(a, b) = 1$, b ist einheitsnormal, a, b in „Normalform“.

z. B. \mathbb{Z} Quotientenkörper $Q(\mathbb{Z}) = \mathbb{Q} \quad a/b$ „kanonisch“, ($b > 0$).

$-2/4, 2/-4, 100/-200, -600/1200$ Kan. repräsentant: $-1/2$.

Quotienten-Körper rationaler Funktionen

$D[x]$ mit D ZPE-Ring, $Q(D[x])$ Körper der rationalen Funktionen (Ausdrücke) in x : Schreibe $D(x)$.

Beachte: Operationen $+, \cdot$ sind „teuer“.

Addition: 3-Multiplikationen + Addition + GGT Berechnung

Multiplikation: 2 Multiplikationen und GGT Berechnung.

Wähle geeignete Darstellungen

Fall $\mathbb{Z}[x] \quad \mathbb{Q}[x]$ bzw. $\mathbb{Z}(x) \quad \mathbb{Q}(x)$

$$\text{in } \mathbb{Q}(x) : a(x)/b(x) = \left(\frac{17}{100}x^2 - \frac{3}{113}x + \frac{1}{2}\right) / \left(\frac{5}{9}x^2 + \frac{4}{5}\right)$$

Die Äquivalenzklasse enthält Repräsentanten mit ganzzahligen Koeffizienten: z. B.

$$a(x)/b(x) = (4284x^2 - 675x + 12600)/(14000x^2 + 20160) \in \mathbb{Z}(x).$$

D mit Quotienten-Körper F_D dann $D(x) \cong F_D(x)$.

Beachte: unterschiedliche kanonische Repräsentanten möglich.

Siehe Beispiel oben.

Einfache Simplifikationsregeln in CA-Systemen

- ▶ Unterdrücken von Klammern: Präfix-Postfix Notationen: Formebene
- ▶ Identitäten Vereinfachung: z. B. $0 \cdot u \rightarrow 0$, $1 \cdot u \rightarrow u$, $u/1 \rightarrow u$, $v^0 \rightarrow 1$ ($v \neq 0$), $0^w \rightarrow 0$ ($w > 0$)
- ▶ Vorzeichenregeln: z. B. $(-u)(-v^3) = uv^3$, $-(u+v) \rightarrow -u-v$?
- ▶ Numerische Vereinfachungen: $\frac{5}{8} - \frac{1}{8} \rightarrow \frac{1}{2}$, $9! \rightarrow 362880$
Vorsicht! oft nicht einfach: $(33282)\frac{1}{2} \sin\left(\frac{13\pi}{6}\right) \rightarrow \frac{122}{\sqrt{2}}$, e^e , e , π , ...
- ▶ Assoziativ-kommutative Gesetze
 $(uv)w + (p+q) \rightarrow uvw + p+q$ $q+p \rightarrow p+q$
- ▶ Anordnung: z. B. Polynomdarstellung

Einfache Simplifikationsregeln in CA-Systemen

- ▶ Zusammenfassung gemeinsamer Faktoren
 $u + \left(\frac{2}{3}\right)u \rightarrow \frac{5}{3}u$, $2^{x+2} \rightarrow 4 \cdot 2^x$, $e^{5+\log u} \rightarrow e^5 e^{\log u}$
- ▶ Operationen mit Exponenten: $(u^w)^v \rightarrow u^{wv}$, $(uv)^w \rightarrow u^w v^w$
- ▶ Distributiv Gesetze: $(u+v)w \rightarrow uw + vw$
- ▶ Potenzen erweitern: $(a+b)^2 \rightarrow a^2 + 2ab + b^2$, $(1+x)^{100} \rightarrow ?$
- ▶ GGT-Vereinfachungen: $\frac{4u^2+12u^3+12u^2+4u}{2u^4-2u^3-2u^2+2u} \rightarrow \frac{2u+2}{u-1}$

Wortproblem - Simplifikation

(M, \sim) WP:: Gegeben $u, v \in M$, Frage: $u \sim v$?

Wie ist M gegeben: oft endlich erzeugt, z. B. Termalgebra.

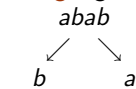
Wie ist \sim gegeben: oft Axiome (Gleichungen)

3.2 Beispiel Monoide, Gruppen: Erzeugende, Definierende Relationen

$M = (\{a, b\}; aba = \lambda, bab = \lambda)$

$G = (a, b, \bar{a}, \bar{b}; a\bar{a} = \bar{a}a = b\bar{b} = \bar{b}b = \lambda)$ freie Gruppe.

Frage: gilt $a =_M b$ $\bar{a}\bar{b}\bar{b}\bar{a} =_G \lambda$?



Wortersetzungssysteme: $M \cong (a; a^3 = \lambda)$,
 allg: Termersetzungssysteme

Simplifikation: Terme in „einfachste“ Form zu bringen.

Methode: Maß: wohlfundierte (Partial)-Ordnung \succ auf M .

$rep(u) = \min_{v \sim u} v$ sollte eindeutig sein.

Frage: Ist rep effektiv berechenbar? i. Allg. nicht, da WP damit lösbar.

Wortproblem - Simplifikation

Termersetzungssysteme: Methoden zur Behandlung von WP:

Regeln, Konfluenz, Terminierung, Vervollständigung (KB).

Oft genügt es ein **spezielles Wortproblem** zu betrachten:

Rolle der Konstanten z. B. 0, 1.

Gruppen: $u = v$ gdw $uv^{-1} = 1$

Ringe: $u = v$ gdw $u - v = 0$

\rightsquigarrow Eigenschaften einer speziellen Äquivalenzklasse.

Abstraktionsebenen für algebraische Strukturen

▶ \mathbb{Z}_m $f(n) = n \bmod m$ positive Reste
 Repr. $0, 1, \dots, m-1$, Definition von $+, \cdot$ auf \mathbb{Z}_m .

I) **Objektebene:** Menge Operationen = Elemente der Mengen

II) Form-Ebene

Objekte werden explizit dargestellt „Bezeichner“
 mehrere Gleichheiten \equiv syntaktische $=$ semantische
 gleiche Bezeichner gleiche Objekte

Typische Bezeichner: Terme $12x^2y - 4xy + 9x - 3$ $(3x - 1)(4xy + 3)$
 $(12y)x^2 + (-4y + 9)x - 3$

Syntaktisch verschieden, aber semantisch gleich.

Abstraktionsebenen für algebraische Strukturen

III) Datenstrukturebene

Darstellung der Objekte aus Ebenen I), II) im Rechner:
 Speicherorganisation
 Listen, Felder, Verbunde usw.
 Simplifikation definiert auf Ebene II).
 Realisiert in Ebene III).

Wichtige Entscheidungen: Welche Darstellungen erlaubt man in Ebene II), wie werden diese in III) dargestellt.

Oft Unterscheidung nötig: Eingabe, Intern, Ausgabe.

Beispiele

a) $E = \mathbb{Z}[x]$

Formebene

- ▶ Jedes Polynom $\sum_{i=0}^n a_i x^i \in \mathcal{F}$
- ▶ $p_1, p_2 \in \mathcal{F}$, so auch $(p_1 * p_2) \in \mathcal{F}$
- ▶ $p_1, p_2 \in \mathcal{F}$, so auch $(p_1 + p_2) \in \mathcal{F}$

Normalisierungsfunktionen:

f_1 $\left\{ \begin{array}{l} \text{Multipliziere Produkte aus (Distributivgesetz) } \Sigma \text{ Monom.} \\ \text{Fasse Monome mit gleichem Grad zusammen.} \\ \text{Ordne Monome nach aufsteigendem Grad} \end{array} \right.$
 (absteigendem)

Beispiele (2)

f_1 ist Normalisierungsfunktion, f_2 ist kanonische Funktion.

Normalform bzgl. f_1 :

$$a_1 x^{e_1} + a_2 x^{e_2} + \dots + a_m x^{e_m} \quad e_i \neq e_j \text{ für } i \neq j$$

Kanonische Form bzgl. f_2 :

$$a_1 x^{e_1} + a_2 x^{e_2} + \dots + a_m x^{e_m} \quad e_i < e_j \text{ für } i < j$$

Oft gilt $s \sim t$ gdw $M(s, t) \sim 0$, \exists Normalisierungsfunktion \rightsquigarrow kanonische Funktion.

Beispiele (3)

- b) Abelsche Halbgruppen Varietät
 Erzeugende Relationen
 $\Sigma :: a, b, c, f, s$ $E :: as = c^2s, bs = cs, s = f$
 + Kommutativität

Faktorhalbgruppe des freien komm. Monoids in a, b, c, f, s

Formebene: $\{a^{n_1} b^{n_2} c^{n_3} f^{n_4} s^{n_5} \mid n_i \in \mathbb{N}\}$

$\circ : M \times M \rightarrow M$ Addition der Exponenten.

Kongruenz, die von E erzeugt wird: **Ersetzungsregeln**

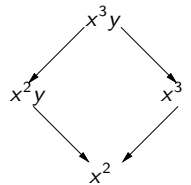
$s \rightarrow f$ $cf \rightarrow bf$ $b^2f \rightarrow af$ „Modulo Kommutativität“

Definiere kanonische Funktion $\xrightarrow{*}$ mit kanonischen Formen
 $\subseteq a^{n_1} b^{n_2} c^{n_3} f^{n_4}$

Beispiele (4)

- c) $E = \mathbb{Q}[x, y] : x^3 - x^2, x^2y - x^2$
 $i = \langle x^3 - x^2, x^2y - x^2 \rangle \quad E/i$

Regeln: $x^3 \rightarrow x^2$ $x^2y \rightarrow x^2$ Reduktionsfunktion



$$x^3 - x^2y \xrightarrow{*} 0$$

\rightarrow definiert Simplifikationsfunktion $p \xrightarrow{*} NF(p)$, sie ist kanonisch (\rightsquigarrow Gröbner Basen).

Normalformen für Polynomringe und Quotientenkörper, d. h.

Normalformen für Polynome und rationale Ausdrücke.

Beispiele (5)

Ringe: Axiome kommutative Ringe mit 1.

Signatur: $0, 1, -, +, *$

Axiome: $+$ Komm., Ass., 0 neutr. El., Gruppe inv. -

$*$ Komm., Ass., Einh. $+$ Distributivgesetz

Gleichheitsaxiome \rightsquigarrow Varietät.

Univariate Polynome: Formebene.

$R[x] : a_n x^n + \dots + a_1 x + a_0, n \geq 0, a_i \in R, a_n \neq 0 \cup \{0\}$

System kanonischer Formen für $R[x]$ (**dicht**) oder **dünn** alle Koeffizienten $\neq 0$.

Multivariate Polynome: Formebene.

Rekursive Darstellung: $R[x_1 \dots x_n] = R[x_1 \dots x_{n-1}][x_n]$

$\text{grad}(a(\bar{x}))$

$$a(x_1, \dots, x_n) = \sum_{i=0}^n a_i(x_1 \dots x_{n-1}) x_n^i$$

dicht/dünn

Beispiele (6)

3.14 Beispiel

$$a(x, y, z) = (3y^2 + (-2z^3)y + 5z^2)x^2 + 4x + ((-6z + 1)y^3 + 3y^2 + (z^4 + 1))$$

Distributive Darstellung $a(\bar{x}) \in D[x]$

$$a(\bar{x}) = \sum_{e \in \mathbb{N}^n} a_e x^e \text{ mit } a_e \in D$$

dicht /dünn $a_e \neq 0$

$x^e \quad e \in \mathbb{N}^n$ werden oft Terme genannt.

$$a(x, y, z) = 3x^2y^2 - 2x^2yz^3 + 5x^2z^2 + 4x - 6y^3z + y^3 + 3y^2 + z^4 + 1$$

Reihenfolge der Terme? Ordnungen auf Termmengen, die kompatibel mit Termmultiplikation sind, z. B.

Lex $x > y > z \quad x^2y^2 > x^2yz^3 > x^2z^2 > x > y^3z \dots$

oder

Grad-Lex $x^2yz^2 > x^2y^2 > x^2z^2 > y^3z > z^4 > y^3 > y^2 > x$

Beispiel

4.2 Beispiel

$$a(x) = 3x^3 + x^2 + x + 5$$

$$b(x) = 5x^2 - 3x + 1 \text{ in } \mathbb{Q}[x]$$

$\rightsquigarrow a(x) = b(x) \cdot q(x) + r(x)$ mit

$$q(x) = \frac{3}{5}x + \frac{14}{25} \quad r(x) = \frac{52}{25}x + \frac{111}{25}$$

Hauptkoeffizient von $b(x)$ ist 5. Nenner sind Potenzen von 5.

In $\mathbb{Z}[x]$ ist obige Division nicht möglich: $3 = 5q_1, q_1 \in \mathbb{Z} \nmid$

Wählt man $\bar{a}(x) = 5^2 \cdot a(x)$, so gilt

$$5^2 \cdot (3x^3 + x^2 + x + 5) = (5x^2 - 3x + 1) \cdot (15x + 14) + (52x + 111) \text{ in } \mathbb{Z}[x], \text{ wobei } \text{grad}(52x + 111) < \text{grad}(5x^2 - 3x + 1)$$

\rightsquigarrow Pseudo-Divisions-Eigenschaft

Pseudo-Division mit Rest-Primitiver EA

PD-Eigenschaft: D ZPE Ring, $a(x), b(x) \in D[x]$ mit $b(x) \neq 0$, $\text{grad}(a(x)) \geq \text{grad}(b(x))$. Dann gibt es Polynome $q(x), r(x) \in D[x]$ mit $\beta^l a(x) = b(x) \cdot q(x) + r(x) \quad \text{grad}(r(x)) < \text{grad}(b(x))$ wobei

- ▶ $\beta = \text{Haupt_Koeff}(b(x))$,
- ▶ $l = \text{grad}(a(x)) - \text{grad}(b(x)) + 1$
- ▶ $q(x)$:: Pseudo_Quotient und
- ▶ $r(x)$:: Pseudo_Rest.

Beachte: $q(x)$ und $r(x)$ sind eindeutig und können durch die „übliche“ Division bestimmt werden.

Pseudo-Division mit Rest

4.3 Definition

D ZPE Ring $0 \neq a(x) \in D[x]$ heißt **primitiv**, falls a EN und die Koeffizienten teilerfremd sind (d. h. $\text{GGT}(a_0, \dots, a_n) = 1$ für $\text{grad}(a) = n$).

z. B. $a_n x^n$ ist primitiv in $\mathbb{Z}[x]$ gdw $a_n = 1$.

Der **Inhalt (Content)** von $a(x)$ (Bez. $\text{cont}(a(x))$) ist der eindeutige EN GGT der Koeffizienten von $a(x)$, d. h. jedes Polynom hat eine eindeutige Darstellung

$$a(x) = u(a(x)) \cdot \text{cont}(a(x)) \cdot PP(a(x))$$

wobei $PP(a(x))$ primitiv ist: **Primitiver Anteil von $a(x)$** .

Für 0 setze $\text{cont}(0) = 0$ und $PP(0) = 0$.

Pseudo-Division mit Rest-Primitiver EA (Forts.)

Gauss Lemma: Produkt von primitiven Polynomen ist primitiv.

Man erhält:

$$\text{GGT}(a(x), b(x)) = \underbrace{\text{GGT}(\text{cont}(a(x)), \text{cont}(b(x)))}_{\text{Berechnung im Koeff. Bereich}} \text{GGT}(PP(a(x)), PP(b(x)))$$

Berechnung im Koeff. Bereich

Annahme: Berechnung vom GGT im Koeff. Bereich bekannt!

4.4 Satz Sei D ZPE Ring. Sind $a(x), b(x) \in D[x]$ primitiv mit $b(x) \neq 0$ und $\text{grad}(a(x)) \geq \text{grad}(b(x))$.

Seien $q(x), r(x)$ Pseudo_Quotient und Pseudo_rest mit $\beta^l a(x) = b(x) \cdot q(x) + r(x), b(x), r(x) \in D[x], \text{grad}(r(x)) < \text{grad}(b(x))$.

Dann gilt

$$\text{GGT}(a(x), b(x)) = \text{GGT}(b(x), PP(r(x)))$$

Pseudo-Division mit Rest-Primitiver EA (Forts.)

Beweis: $\text{GGT}(\beta^l a(x), b(x)) = \text{GGT}(b(x), r(x))$
 und
 $\text{GGT}(\beta^l a(x), b(x)) = \text{GGT}(\beta^l, 1) \text{GGT}(a(x), b(x)) = \text{GGT}(a(x), b(x))$
 da a, b primitiv. Somit

$$\begin{aligned} \text{GGT}(b(x), r(x)) &= \text{GGT}(1, \text{cont}(r(x))) \text{GGT}(b(x), \text{PP}(r(x))) \\ &= \text{GGT}(b(x), \text{PP}(r(x))) \end{aligned}$$

- ↪ Pseudo polynomiale Restefolge zur Berechnung des GGT
- ↪ Primitiver EA

Lässt sich verallgemeinern: **PP Restefolge** für F_1, F_2 :
 $F_1, F_2, \dots, F_{k-1}, F_k$ mit $F_i(x) = \alpha_i F_{i-2}(x) - q_i(x) F_{i-1}(x)$ mit
 $\text{grad}(F_i) < \text{grad}(F_{i-1}) (i > 2)$ $\alpha_i \in D, F_i \in D[x]$.
 (Eine Wahl für α_o ist $f_{i-1}^{n_i - n_{i-1} + 1}$ f_i HK von $F_{i-1}, n_i = \text{grad}(F_i)$)

Pseudo-Division mit rest-primitiver EA (Forts.)

Primitiver EA $D[x]$ D mit GGT-Berechnung

```

procedure PEA (a(x), b(x))
begin
    c(x) := PP(a(x)); D(x) := PP(b(x));
    while D(x) ≠ 0 do
        begin
            r(x) := Prem(c(x), D(x));
            c(x) := D(x);
            D(x) := PP(r(x));
        end
    γ := GGT(cont(a(x)), cont(b(x)));
    g(x) := γ · c(x); return (g(x));
end.
    
```

Beispiel

4.5 Beispiel in $\mathbb{Z}[x]$
 $a(x) = 48x^3 - 84x^2 + 42x - 36$
 $b(x) = -4x^3 - 10x^2 + 44x - 30$

Iter.	$r(x)$	$c(x)$	$d(x)$
0	–	$8x^3 - 14x^2 + 7x - 6$	$2x^3 + 5x^2 - 22x + 15$
1	$-68x^2 + 190x = 132$	$2x^3 + 5x^2 - 22x + 15$	$34x^2 - 95x + 66$
2	$4280x - 6420$	$34x^2 - 95x + 66$	$2x - 3$
3	0	$2x - 3$	0

$$\gamma = \text{GGT}(6, 2) = 2 \quad g(x) = 2 \cdot (2x - 3) = 4x - 6.$$

Vorteil: Anwendbar auf $D[\bar{x}]$ für D ZPE mit GGT.

Problem: Wachstum der Koeffizienten bei PD mit Rest!

Beispiel

4.6 Beispiel
 $a(x) = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$
 $b(x) = 3x^6 + 5x^4 - 4x^2 - 9x + 21$

Koeffizienten der Polynome in der PP-Restefolge

a	1	0	1	0	-3	-3	8	2	-5
b			3	0	5	0	-4	-9	21
r					-15	0	3	0	-9
F_4							15795	30375	-59535
F_5							1254542875143750	-1654608338437500	
F_6							12593338795500743100931141992187500		

d. h. teilerfremd GGT 1

Vergleich mit EEA (oder EA) für $F[x]$!

Beispiel (Forts.)

- b) $R = F[x]$, $m_i = x - a_i$, $0 \leq i \leq n$, $a_0, \dots, a_n \in F$ ($p \nmid v$).
 $f \equiv f(a_i) \pmod{(x - a_i)}$, $0 \leq i \leq n$, $f \rightarrow (f(a_0), \dots, f(a_n))$
- d. h. **Auswertungshom.** in a_0, \dots, a_n , F^{n+1} koordinatenweise Operationen.
 $l_i \equiv 1 \pmod{(x - a_i)}$ $l_i \equiv 0 \pmod{(x - a_j)}$, $j \neq i$
 $\text{grad}(l_i) \leq n$ sind die **Lagrange Interpolanden**

$$l_i = \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{x - a_j}{a_i - a_j}$$

Für $b_0, \dots, b_r \in F$, so $f = \sum_{0 \leq i \leq n} b_i l_i$ Lagrange Interpolationspolynom mit
 $f(a_i) = b_i$ für $0 \leq i \leq n$.
 d. h. Chinesische Reste Algorithmus für $n + 1$ Lin Polynome ist
 Interpolation in $n + 1$ Werte. Polynom ist eindeutig: $\text{Grad} \leq n$.

Die schnelle Fourier Transformation (FFT) Anwendung auf Polynommultiplikation

Koeffizientendarstellung $\xleftrightarrow[\text{Interpolation}]{\text{Auswertung}}$ Wertedarstellung.

Cooley, Tukey: An algorithm for machine calculation of complex fourier series, Math. Comp. 19 (1965) 297-301.

Idee: Fourier Transformierte: Reduktion auf einfachere Operationen

$$\text{trans}(f * g) = \text{trans}(f) \oplus \text{trans}(g)$$

$$\log(a \cdot b) = \log(a) + \log(b)$$

Um $a \cdot b$ zu berechnen: $\log(a), \log(b) \rightsquigarrow \log(a) + \log(b)$
 $\rightsquigarrow \text{trans}^{-1}(\) = a \cdot b$.

Die allgemeine Fourier Transformation

Die Variablen t und f stehen für Zeit und Frequenz

$$\mathcal{F}(a) :: A(f) = \int_{-\infty}^{\infty} a(t) e^{2\pi i f t} dt$$

$$\mathcal{F}^{-1}(A) :: a(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} A(f) e^{-2\pi i f t} df$$

Diskrete Fourier Transformation

a_0, \dots, a_{n-1} reelle Zahlen, i komplexe Zahl mit $i^2 = -1$, seien

$$A_j := \sum_{k=0}^{n-1} a_k e^{2\pi i j k / n} \quad 0 \leq j < n$$

$$a_k = \frac{1}{n} \sum_{j=0}^{n-1} A_j e^{-2\pi i j k / n} \quad 0 \leq k < n$$

Interpretation: Auswertung eines Polynoms $a(x)$ an n -Stellen.

D. h.:: $a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$

$A_j = a(\omega^j)$, wobei $\omega = e^{2\pi i / n}$, $\omega^n = 1$ n -te Einheitswurzel

d. h.

$$\omega^j = e^{2\pi i j / n}, (\omega^j)^k = e^{2\pi i j k / n}$$

Diskrete Fourier Transformation

Koeffizienten Darstellung zur modularen Darstellung (d. h. Wertedarstellung an speziellen Stellen)

$$x_0, \dots, x_{n-1} \quad (\text{hier } x_j = \omega^j \text{ } n\text{-te-Einheitswurzel.})$$

$T_{(x_0, \dots, x_{n-1})}(a_0, \dots, a_{n-1}) = (\hat{a}_0, \dots, \hat{a}_{n-1})$, wobei

$$\hat{a}_j = a_0 + a_1 x_j + \dots + a_{n-1} x_j^{n-1}.$$

Setzt man $a(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

\rightsquigarrow Auswertung von Polynomem vom Grad höchstens $n - 1$ an den Stellen $\{x_0, \dots, x_{n-1}\}$.

Auswertung eines Polynoms vom Grad $n - 1$ (Horner's Regel) an einer Stelle kostet $O(n)$ Operationen (in R). Übliche Kosten an n Stellen $\rightsquigarrow O(n^2)$.

Ziel: Reduktion dieser Kosten auf $O(n \log n)$ durch geeignete Wahl der Auswertungsstellen x_j : prim. E.W.

Diskrete Fourier Transformation: Die Auswertung

Angenommen n gerade, dann $a(x) = b(x^2) + x \cdot c(x^2)$, wobei

$$b(y) = a_0 + a_2 y + \dots + a_{n-2} y^{n/2-1}, \quad c(y) = a_1 + a_3 y + \dots + a_{n-1} y^{n/2-1}.$$

Hierbei haben $b(y)$ und $d(y)$ $\text{grad} \leq \text{grad}(a(x))/2$.

4.12 Lemma Sei $\{x_0, \dots, x_{n-1}\}$ Punktmenge in R , die die Symmetriebedingung

(*) $x_{(n/2)+i} = -x_i, i \in \{0, 1, \dots, n/2 - 1\}$ erfüllt.

Es gibt ein Auswertungsverfahren, so das für die Kosten $T(n)$ für die Auswertung eines Polynoms vom Grad $n - 1$ an dieser Punktmenge, gilt

$$T(1) = 0 \text{ und } T(n) = 2 \cdot T\left(\frac{n}{2}\right) + c \cdot \frac{n}{2}$$

für geeignete Konstante c .

Diskrete Fourier Transformation: Die Auswertung

Beweis: Wegen (*) gilt

$$x_0^2 = x_{n/2}^2, x_1^2 = x_{n/2+1}^2 \dots x_{n/2-1}^2 = x_{n-1}^2,$$

d. h. es gibt nur $n/2$ verschiedene Quadrate, d. h.

- ▶ a vom Grad höchstens $n - 1$ kann an den Stellen $\{x_0, \dots, x_{n-1}\}$ ausgewertet werden, durch Auswertung der Polynome b und c an den Stellen $\{x_0^2, \dots, x_{n/2-1}^2\}$, diese sind vom Grad höchstens $\frac{n}{2} - 1$.
- ▶ Hinzukommen $n/2$ Multiplikationen (Berechnung von x_j^2) und $\frac{n}{2}$ Multiplikationen, Additionen und Subtraktionen, um die Werte zu kombinieren. \rightsquigarrow Behauptung.

Die schnelle Fourier Transformation verwendet dieses Lemma rekursiv, d. h. Symmetrie-Eigenschaft muss für die $n/2$ Punkte gelten usw.

Symmetriebedingung: Primitive Einheitswurzeln

4.13 Definition Primitive Einheitswurzeln

Sei R kommutativer Ring, $\omega \in R$ ist prim. n -te EW gdw

1. $\omega^n = 1$
2. $\omega^i \neq 1$ für $0 < i < n$ (insb. $\omega \neq 1$)
3. $\sum_{j=0}^{n-1} \omega^{jp} = 0$ für $1 \leq p < n$

Die Menge $\{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ ist die Menge der Fourier Punkte zur n -ten EW ω .

Diskrete Fourier Transformation bzgl. Primitiven Einheitswurzeln

Voraussetzung:

n besitze eine multiplikative Inverse in R (z. B. wenn R Körper)

Seien

$A = (A_{ij})_{n \times n}$ mit $A_{ij} = \omega^{ij}$, $0 \leq i, j \leq n-1$, $\alpha = [a_0, \dots, a_{n-1}]^T$, dann

$$F(\alpha) := A\alpha, \text{ wobei } F(\alpha)_i = \sum_{k=0}^{n-1} a_k \omega^{ik}$$

heißt **diskrete Fourier Transformierte von α** (bzgl. ω).

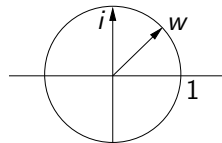
Beispiel

4.14 Beispiel

a) Sei $R = \mathbb{C}$ komplexe Zahlen, $n = 8$

$\omega = e^{2\pi i/8} = e^{\pi i/4} = \frac{(1+i)}{\sqrt{2}}$ ist primitive 8-EW.

$\omega^2 = e^{\pi i/2} = i$ erfüllt auch $(\omega^2)^8 = 1$, aber $(\omega^2)^4 = 1$, d. h. ω^2 ist 8-Wurzel von 1, aber nicht primitiv.



$$\sum_{j=0}^{8-1} e^{\pi i j/4} = 1 + e^{\pi i/4} + e^{\pi i/2} + e^{3\pi i/4} + \dots + e^{7\pi i/4} = 0$$

(heben sich paarweise auf!)

Beispiel (Forts.)

b) $R = \mathbb{Z}_{17}$, $n = 4$. 4 ist eine 4 EW, da $4^4 = 256 \equiv 1 \pmod{17}$.

Sie ist auch primitiv, da $4^2 = 16$ und $4^3 = 13$ und $\sum_{j=0}^3 4^j = 0 \pmod{17}$.

Fourier Punkte: $\{1, 4, 4^2, 4^3\} = \{1, 4, 16, 13\}$

Diskrete Fourier Transformation:

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 16 & 13 \\ 1 & 16 & 1 & 16 \\ 1 & 13 & 16 & 4 \end{bmatrix} : (\mathbb{Z}_{17})^4 \rightarrow (\mathbb{Z}_{17})^4$$

Symmetriebedingung für PEW

4.15 Lemma

Ist ω eine primitive n -te EW, so erfüllen die n Fourier Punkte die Symmetriebedingung *

Beweis:

Da ω primitive n -te EW ist, gilt

$$(\omega^{n/2+j})^2 = \omega^n (\omega^j)^2 = (\omega^j)^2, \text{ d. h.}$$

$$(\omega^{n/2+j} - \omega^j)(\omega^{n/2+j} + \omega^j) = ((\omega^{n/2+j})^2 - (\omega^j)^2) = 0$$

Ist $\omega^{n/2+j} - \omega^j = 0$ so $\omega^{n/2} = 1 \not\equiv 1$.

Also $\omega^{n/2+j} + \omega^j = 0$, d. h. $\omega^{n/2+j} = -\omega^j$.

(R muss wohl Integerbereich sein?).

Symmetriebedingung: Rekursiv

4.16 Lemma

Sei ω primitive n -te EW, n gerade. Dann

- a) ω^2 ist primitive $n/2$ -EW.
- b) Die $n/2$ Quadrate $\{1, \omega^2, \omega^4, \dots, \omega^n\}$ erfüllen die Symmetriebedingung *.

Beweis:

Wegen $(\omega^2)^{n/2} = \omega^n = 1$ ist ω^2 $n/2$ -EW.

Sie ist auch primitiv, da für $k < n/2$ mit $(\omega^2)^k = 1$ folgt $\omega^{2k} = 1$ mit $2k < n$.

Die zweite Behauptung folgt aus vorherigem Lemma.

Grundlage für die rekursive Auswertung der Fouriertransformation ist für primitive 2^m -EW gegeben.

Beispiel: PEW

4.17 Beispiel \mathbb{Z}_{41} , $n = 8$ symmetrische Darstellung von \mathbb{Z}_{41}

14 primitive 8-EW mit Fourier Punkte $\{1, 14, -9, -3, -1, -14, 9, 3\}$

$14^2 = -9$ ist primitive 4-EW mit Fourier Punkte $\{1, -9, -1, 9\}$.

$(-9)^2 = -1$ ist primitive 2-EW mit Fourier Punkte $\{1, -1\}$.

Sei $a(x) = 5x^6 + x^5 + 3x^3 + x^2 - 4x + 1 \in \mathbb{Z}_{41}[x]$.

$a(x) = b(y) + xc(y)$ für $y = x^2$ und $b(y) = 5y^3 + y + 1$,

$c(y) = y^2 + 3y - 4$.

Auswertung von $a(x)$ an den 8 Punkten $\{1, 14, -9, -3, -1, -14, 9, 3\}$:

Werte $b(y)$ und $c(y)$ an $\{1, -9, -1, 9\}$

$b(y) = d(z) + ye(z)$, wobei $z = y^2$, $d(z) = 1$, $e(z) = 5z + 1$.

Werte $d(z)$ und $e(z)$ an $\{1, -1\}$.

$d(1) = 1, e(1) = 6 \rightsquigarrow b(1) = 7, b(-1) = -5$.

$d(-1) = 1, e(-1) = -4 \rightsquigarrow b(-9) = -4, b(9) = 6$.

Analog $c(1) = 0, c(-1) = -2, c(-9) = 9, c(9) = -19$ und

$a(3) = b(9) + 3c(9) = -10$ und $a(-3) = b(9) - 3c(9) = -19$.

Ergebnis: $A \leftarrow \text{FFT}(8, 14, a(x)) = (7, -1, 8, -19, 7, -7, -18, -10)$

Schnelle Fourier Transformation (FFT)

```

procedure FFT( $N, \omega, a(x)$ )
begin
    { $N$  Potenz von 2,  $\omega$  primitive  $n$ -te EW,  $a(x)$  Polynom}
    {mit Grad ( $a(x)$ )  $\leq N - 1$ . Ausgabe  $N$  Komponenten der FFT}
if  $N=1$  then
     $A_0 := a_0$ 
else
    begin
     $b(x) := \sum_{i=0}^{N/2-1} a_{2i} \cdot x^i; c(x) := \sum_{i=0}^{N/2-1} a_{2i+1} \cdot x^i;$ 
     $B := \text{FFT}(N/2, \omega^2, b(x)); C := \text{FFT}(N/2, \omega^2, c(x));$ 
    for  $i$  from 0 to  $N/2 - 1$  do
        begin
         $A_i := B_i + \omega^i C_i; A_{N/2+i} := B_i - \omega^i C_i;$ 
        end
    end
    return  $((A_0, A_1, \dots, A_{N-1}))$ ;
end.
    
```

Schnelle Fourier Transformation (FFT): Analyse

Aufwand: $O(n \log n)$ Operationen: Sei $n = 2^m$ dann

$$T(1) = 0, T(2^k) = 2T(2^{k-1}) + c2^{k-1} \quad k \geq 1$$

$$\begin{aligned}
 T(n) &= T(2^m) = 2T(2^{m-1}) + c2^{m-1} = 2^2 T(2^{m-2}) + c2^{m-1} \cdot 2 \\
 &= 2^3 T(2^{m-3}) + c2^{m-1} \cdot 3 \dots = 2^m T(1) + c2^{m-1} m \\
 &= c2^{m-1} m = c \frac{n}{2} \log n
 \end{aligned}$$

Beachte: Eignet sich gut für Parallelisierung: Rekurrenzgleichung:

$$T^P(2^k) = T^P(2^{k-1}) + c2^{k-1}$$

(FFT):: Ergebniss

Modulare Darstellung eines Polynoms vom Grad $N - 1$ an N -Fourierpunkte kann mit $O(N \log N)$ Grundoperationen in $R (K)$ berechnet werden.

$$R[x]_{\text{grad} \leq N-1} \rightarrow R[x]/(x - \omega^0) \times \cdots \times R[x]/(x - \omega^{N-1})$$

Wie sieht es mit der Umkehrung aus

$$T_{(x_0, \dots, x_{N-1})} \leftrightarrow V(x_0, \dots, x_{N-1}) = \begin{vmatrix} 1 & x_0 & \cdots & (x_0)^{N-1} \\ 1 & x_1 & \cdots & (x_1)^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{N-1} & \cdots & (x_{N-1})^{N-1} \end{vmatrix}$$

Vandermonde Matrix

Inverse für Vandermonde Matrix

Finde Inverse der Vandermonde Matrix: Gauss Elimination $O(N^3)$

Polynominterpolation:

Gegeben N Punkte $(q_0, \dots, q_{N-1}) \in R$, finde Polynom vom Grad höchstens $N - 1$ mit

$$\hat{a}_i = a(x_i) = q_i \text{ für } i = 0, 1, \dots, N - 1$$

Lagrange Interpolation oder Newton Interpolation

Kosten $O(N^2)$ Operationen.

Inverse Fourier Transformation

4.18 Definition

Die Inverse diskrete Fourier Transformation (IDFT) für eine Menge Fourier Punkte ist definiert durch

$$S_{(1, \omega, \dots, \omega^{N-1})}(q_0, \dots, q_{N-1}) = (\bar{q}_0, \dots, \bar{q}_{N-1})$$

wobei

$$\bar{q}_j = N^{-1} \sum_{k=0}^{N-1} q_k (\omega^{-j})^k$$

Hierbei ist ω primitive n -te EW.

4.19 Satz DFT und IDFT sind inverse Transformationen, d. h.

$$T_{(1, \omega, \dots, \omega^{N-1})} S_{(1, \omega, \dots, \omega^{N-1})} = ID, S_{(1, \omega, \dots, \omega^{N-1})} T_{(1, \omega, \dots, \omega^{N-1})} = ID$$

Inverse Fourier Transformation

Beweis: Sei $0 < p < N$. Dann

$(\omega^p)^N = (\omega^N)^p = 1$ und $(\omega^p) \neq 1$. Da ω PEW

$(x^N - 1) = (x - 1)(x^{N-1} + x^{N-2} + \cdots + x + 1)$, d. h. ω^p ist Nullstelle von $x^{N-1} + \dots + x + 1 \rightsquigarrow 0 = (\omega^p)^{N-1} + (\omega^p)^{N-2} + \cdots + (\omega^p) + 1$.

Für $0 < p < N$ und $-N < p < 0$ (Mult. $\omega^{-p(N-1)}$).

Für $p = 0$ ist der Ausdruck N .

Sei $T_{(1, \omega, \dots, \omega^{N-1})}(a_0, \dots, a_{N-1}) = (\hat{a}_0, \dots, \hat{a}_{N-1})$ mit

$$\hat{a}_i = \sum_{j=0}^{N-1} a_j (\omega^i)^j, \quad i = 0, \dots, N - 1$$

$$N^{-1} \sum_{i=0}^{N-1} \hat{a}_i \omega^{-ki} = N^{-1} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} a_j \omega^{ij} \omega^{-ki}$$

$$= N^{-1} \sum_{j=0}^{N-1} a_j \sum_{i=0}^{N-1} \omega^{ij} \omega^{-ki} = N^{-1} \sum_{j=0}^{N-1} a_j \left(\sum_{i=0}^{N-1} \omega^{(j-k)i} \right) = a_k$$

Inverse Fourier Transformation

$$\begin{aligned}
 V(1, \omega, \dots, \omega^{N-1})^{-1} &= N^{-1} \begin{vmatrix} 1 & & & 1 \dots 1 \\ 1 & \omega^{-1} & & \dots \omega^{-(N-1)} \\ \vdots & & & \\ 1 & \omega^{-(N-1)} & \dots & \omega^{-(N-1)^2} \end{vmatrix} \\
 &= N^{-1} V(1, \omega^{-1}, \dots, \omega^{-(N-1)})
 \end{aligned}$$

Beispiel

4.20 Beispiel In \mathbb{Z}_{17} , $\omega = 4$ primitive 4-te EW.
 Inverse $S_{(1,4,16,13)} : (\mathbb{Z}_{17})^4 \rightarrow (\mathbb{Z}_{17})^4$

$$(4^{-1}) \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 13 & 16 & 4 \\ 1 & 16 & 1 & 16 \\ 1 & 4 & 16 & 4 \end{vmatrix} = \begin{vmatrix} 13 & 13 & 13 & 13 \\ 13 & 16 & 4 & 1 \\ 13 & 4 & 13 & 4 \\ 13 & 1 & 4 & 16 \end{vmatrix}$$

Sowohl T als auch S sind Fourier Transformationen.

- ▶ $T_{(1, \omega, \dots, \omega^{N-1})} \vec{p} = \vec{q}$
- ▶ $N^{-1} T_{(1, \omega^{-1}, \dots, \omega^{-(N-1)})} \vec{q} = \vec{p}$. Da ω^{-1} primitive n -te EW.

Die inverse Fourier Transformation kann mit $O(N \log N)$ Operationen berechnet werden.

Schnelle Polynommultiplikation

$$\begin{array}{lll}
 a(x) \text{ grad } m & a(x) \cdot b(x) & \text{grad } m+n \\
 b(x) \text{ grad } n & &
 \end{array}$$

- ▶ Sei $N = 2^k > m+n$ ω prim. n -te EW
- ▶ $T_{(1, \omega, \dots, \omega^{N-1})}(a_0, \dots, a_m, 0, \dots, 0) = (\hat{a}_0, \dots, \hat{a}_m, \dots, \hat{a}_{N-1})$
- ▶ $T_{(1, \omega, \dots, \omega^{N-1})}(b_0, \dots, b_n, 0, \dots, 0) = (\hat{b}_0, \dots, \hat{b}_n, \dots, \hat{b}_{N-1})$
- ▶ $a(x) \cdot b(x) = (c_0, c_1, \dots, c_{m+n})$
- ▶ $T_{(1, \omega, \dots, \omega^{N-1})}(c_0, \dots, c_{m+n}, 0, \dots, 0) = (\hat{a}_0 \hat{b}_0, \dots, \hat{a}_{N-1} \hat{b}_{N-1})$

Schnelle Fourier Polynommultiplikation

procedure FFT_Multiplikation($a(x), b(x), m, n$)
begin {Eingabe: Polynome a, b vom Grad m, n }
 {Berechne $c(x) = a(x) \cdot b(x)$ mit FFT's}

$N :=$ erste Zweierpotenz größer als $m+n$; $\omega :=$ primitive n -te EW;
 $A := FFT(N, \omega, a(x)); B := FFT(N, \omega, b(x));$

for i from 0 to $N-1$ **do**

begin
 $C_i := A_i B_i;$
end

$C := N^{-1} FFT(N, \omega^{-1}, C(x)); c(x) := \sum_{i=0}^{N-1} C_i x^i;$

return ($c(x)$)
end.

Aufwand (ohne Berechnungskosten für ω) ($O((m+n) \log(m+n))$)
 Grundoperationen in R .
 Kommt zum Tragen erst für $m+n \geq 600$ (Moenck)

Beispiel

4.21 Beispiel

$$a(x) = 3x^3 + x^2 - 4x + 1$$

$$b(x) = x^3 + 2x^2 + 5x - 3 \pmod{41}$$

14 primitive 8-te EW (wie eben).

$$A = FFT(8, 14, a(x)) = (1, 9, -19, -18, 3, 16, 19, -3)$$

$$B = FFT(8, 14, b(x)) = (5, 5, 0, 14, -7, -6, -10, 16)$$

$$C = (5, 4, 0, -6, 20, -14, 15, -7)$$

$$= FFT(8, 14, a(x)b(x))$$

$$c = 8^{-1} FFT(8, 3, -7x^7 + 15x^6 - 14x^5 + 20x^4 - 6x^3 + 4x + 5)$$

$$= (-3, 17, 20, -11, 13, 7, 3, 0)$$

$$c(x) = 3x^6 + 7x^5 + 13x^4 - 11x^3 + 20x^2 + 17x - 3$$

Berechnung primitiver n-ter EW

- ▶ $F = \mathbb{C}$ einfach $\omega = e^{2\pi i/n}$
 z. B. $e^{\pi i/6} = (\sqrt{3} + i)/2$ ist primitive 12-te EW in \mathbb{C}
- ▶ $\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p$

4.22 Satz \mathbb{Z}_p hat primitive n-te EW gdw $n \mid p - 1$.

Beweis: Ist w primitive n-te EW in \mathbb{Z}_p , so bildet die Menge der Fourier Punkte $\{1, \omega, \dots, \omega^{n-1}\}$ eine zyklische Untergruppe der multiplikativen Gruppe von \mathbb{Z}_p . Diese hat $p - 1$ Elemente $\rightsquigarrow n \mid p - 1$ (Lagrange).

Die multiplikative Gruppe endlicher Körper ist zyklisch. Sei α erzeugendes Element der multiplikativen Gruppe von $\mathbb{Z}_p : \mathbb{Z}_p^\times = \{1, \alpha, \alpha^2, \dots, \alpha^{p-2}\}$ mit $\alpha^{p-1} = 1$

Sei $n \mid p - 1$. Setzt man $\omega = \alpha^{(p-1)/n}$, so gilt $\omega^n = \alpha^{p-1} = 1$, d. h. ω ist n-te EW. Für $0 < k < n$, gilt $(p - 1) \cdot k/n < (p - 1)$, $\omega^k = \alpha^{(p-1)k/n} \neq 1$, also ist ω primitive n-te EW.

Berechnung primitiver n-ter EW

4.23 Beispiel In \mathbb{Z}_{41} gilt $8 \mid (41 - 1)$, d. h. es gibt primitive 8-te EW in \mathbb{Z}_{41} , z. B. 14 ist primitive 8-te EW in \mathbb{Z}_{41} .

Wie bestimmt man eine primitive n-te EW, wenn $n \mid p - 1$ testen ! oder finde erzeugende für \mathbb{Z}_p^\times .

Anwendung $n = 2^r$ für Fourier-Transformation $2^r \mid p - 1$ oder $p = 2^r k + 1$ für ein k ungerade.

Solche Primzahlen heißen **Fourier Primzahlen** zu 2^r .

Vorteil: Es gibt viele primitive Elemente.

Hilfsatz: Seien $a, b \in \mathbb{Z}$ mit $\text{GGT}(a, b) = 1$. Die Anzahl der Primzahlen $\leq x$ der Form $ak + b$, $k = 1, 2, \dots$ ist in etwa

$$\frac{x}{\log x \cdot \Phi(a)} \quad (\Phi \text{ Euler Funktion}).$$

Da alle ungeraden Zahlen $< 2^r$ teilerfremd zu 2^r sind und dies die Hälfte der ganzen Zahlen ist, gilt $\Phi(2^r) = 2^{r-1}$, d. h. es gibt etwa $\frac{x}{\log x \cdot 2^{r-1}}$

Fourier Primzahlen $\leq x$.

Berechnung primitiver n-ter EW

4.24 Beispiel Sei $x = 2^{31}$ SP-Zahlen 32 Bit Wörter. Für $r = 20$

$$\rightsquigarrow \frac{2^{31}}{\log(2^{31}) \cdot \Phi(2^{19})} \approx 130 \text{ Primzahlen der Form } 2^e \cdot k + 1, e \geq 20 \text{ im Intervall } 2^{20} << 2^{31}.$$

Jede solche Fourier Primzahl kann zur Berechnung von FFT's der Größe 2^{20} verwendet werden.

4.25 Satz a ist erzeugendes Element für \mathbb{Z}_p^\times gdw $a^{(p-1)/q} \neq 1 \pmod{p}$ für jeden Primfaktor von $p - 1$.

Beweis folgt aus Lagrange ($H \leq G \rightsquigarrow |H| \mid |G|$)

\rightsquigarrow Probabilistischer Algorithmus um erzeugendes Element für \mathbb{Z}_p^\times :

Faktoriere $p - 1$ (möglich für $p \approx 2^{31}, 2^{63}$?) vorprozess. Wähle zufällig $a \in \{2, \dots, p - 1\}$, berechne $a^{(p-1)/q}$ für alle Teiler q von $p - 1$.

Beispiel

4.26 Beispiel

Wegen $41 - 1 = 40 = 2^3 \cdot 5$, Primfaktoren 2, 5,
 d. h. ein Element a erzeugt \mathbb{Z}_{41}^* , falls $a^8 \neq 1 \neq a^{20}$, z. B.

$$15 : \quad 15^8 = 18 \pmod{41} \quad 15^{20} \equiv -1 \pmod{41} \\ \neq 1 \quad \quad \quad \neq 1$$

Also ist 15 ein erzeugendes Element für \mathbb{Z}_{41}^* , ist insbesondere eine primitive 40 EW in \mathbb{Z}_{41} , da $15^{40} = 1 \pmod{41}$ und $\alpha^p \neq 1 \pmod{41}$ für $0 < p < 40$.

Die Anzahl der Erzeugenden für \mathbb{Z}_p^* ist $\Phi(p-1)$, d. h. Anteil $\Phi(p-1)/(p-1) \approx 3/\pi^2$, 0.3 Wahrscheinlichkeit.

Beispiel (Forts.)

\mathbb{Z}_m N gegeben, bestimme m und ω , $N = 2^k$

- ▶ N invertierbar in $\mathbb{Z}_m \rightsquigarrow \text{GGT}(N, m) = 1$.

$$a \in R, N = 2^k \rightsquigarrow \sum_{i=0}^{N-1} a^i = \prod_{i=0}^{k-1} (1 + a^{2^i}) \text{ Ind. nach } k \\ = (1 + a) \sum_{i=0}^{N/2-1} (a^2)^i$$

- ▶ Sei $m = \omega^{N/2} + 1$ mit $\omega \in R$, $\omega \neq 0$. Dann

$$\sum_{i=0}^{N-1} \omega^{ip} \equiv 0 \pmod{m} \text{ für } 1 \leq p < N$$

Beispiel (Forts.)

Beweis: Zeige $1 + \omega^{2^j p} \equiv 0 \pmod{m}$ für ein j $0 \leq j < k$. Sei $p = 2^s p'$ mit p' ungerade, dann $0 \leq s < k$. Wähle j mit $j + s = k - 1 \rightsquigarrow 1 + \omega^{2^j p} = 1 + \omega^{2^{k-1} p'} = 1 + (m-1)^{p'}$ wegen $(m-1) \equiv -1 \pmod{m}$, p' ungerade $\rightsquigarrow (m-1)^{p'} \equiv -1 \pmod{m}$, \rightsquigarrow Behauptung.

4.27 Satz

Seien n, ω positive Potenzen von 2 und $m = \omega^{n/2} + 1$, dann besitzt n Inverse in \mathbb{Z}_m und ω ist in \mathbb{Z}_m primitive n -te EW.

Beweis: $\omega \neq 1$ $\omega^n = \omega^{n/2} \cdot \omega^{n/2} \equiv (-1)(-1) \pmod{(\omega^{n/2} + 1)}$.

Problem: primitive EW $R[x]/\langle x^n + 1 \rangle$

$$x^n \equiv -1 \pmod{x^n + 1} \quad x^{2n} = (x^n)^2 \equiv 1 \pmod{x^n + 1}$$

$\omega = (x \pmod{x^n + 1})$ ist $2n$ -te EW.

Anwendung FFT auf Langzahlmultiplikation

Multiplikation nach Schönhage-Strassen: div & conq + FFTA

Idee: Partitionierung der Zahlen in b -Blöcke der Länge l , d. h. $n = b \cdot l$, falls n Länge der Eingabezahlen.



Die b -Blöcke werden als Koeffizienten eines Polynoms (vom Grad $b-1$) mit Koeffizienten $< 2^l$ aufgefasst.

Wertet man diese Polynome an geeigneten Stellen aus, multipliziert diese Werte und interpoliert, so lässt sich das Produkt bestimmen.

FFT + Faltungssätze.

Aufwand: $O(n \log n \log \log n)$ für die Multiplikation von Langzahlen der Länge n . Siehe von zur Gathen/Gerhard pp.225.

Modulare Algorithmen: Allgemeine Methoden

Anwendungsfälle

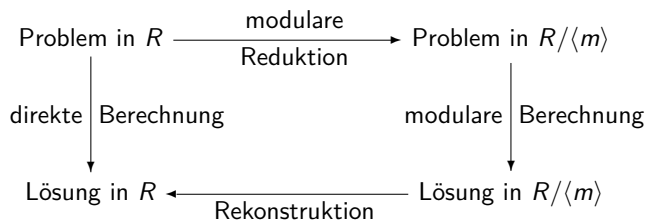
- ▶ FFT-Anwendung zur Multiplikation von Polynomen.
- ▶ GGT-Berechnung in $\mathbb{Z}_m \cong \mathbb{Z}_{m_0} \times \dots \times \mathbb{Z}_{m_k}$ um Koeffizientenwachstum zu vermeiden.
- ▶ $\mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$
nicht euklid euklidisch
- ▶ Faktorisierung, Wurzelberechnung,...

3 Varianten:

Big-Prime, Small-Primes, Prime-Power

Modulare Methoden: Big-Prime

Big-Prime: R euklidisch $m = p$

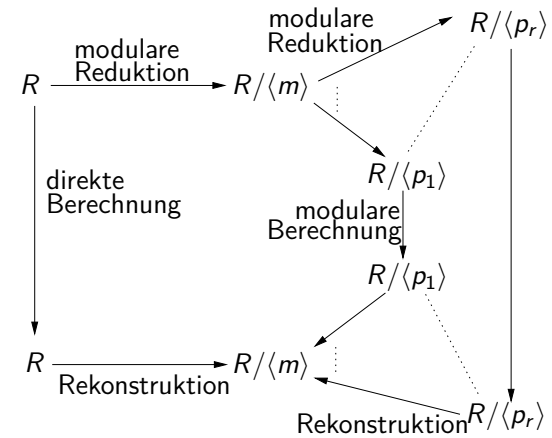


Benötigt werden:

- ▶ Schranke für die Lösung in R .
- ▶ Finde geeignete Moduli.

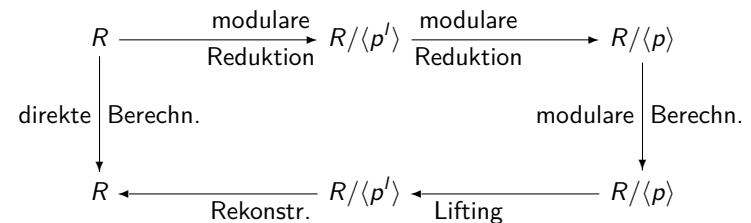
Modulare Methoden: Small-Primes

▶ **Small Primes:** $m = p_1 \dots p_r$ $p_i \neq p_j (i \neq j)$



Modulare Methoden: Prime Power

▶ **Prime-Power:** $m = p^l$ p Primzahl



- ▶ Wahl der p_i steht frei, z. B. Fourier Primzahlen (schnelle Polynomarithmetik)
- ▶ Verteilung (Parallelisierung)

Chinesische Reste Algorithmen

Die Algorithmen von Garner und Newton:

Umkehrung modularer- und Auswertungshomomorphismen.

4.28 Beispiel Wachstum der Zwischenergebnisse.

Systeme linearer Gleichungen. Gauss Methode::

$$\begin{array}{l}
 22x + 44y + 74z = 1 \quad \text{Gauss} \quad 22x + 44y + 74z = 1 \\
 15x + 14y - 10z = -2 \quad \rightsquigarrow \quad -352y - 1330z = -59 \\
 -25x - 28y + 20z = 34 \quad \text{Elimin.} \quad 484y + 2290z = 773 \\
 \begin{array}{l}
 * \\
 \rightsquigarrow \quad 1257315840x = 7543895040 \\
 \quad \quad -57150720y = 314328960 \\
 \quad \quad \quad 162360z = 243540 \\
 \rightsquigarrow \quad x = 6 \quad y = -11/2 \quad z = 3/2
 \end{array}
 \end{array}$$

n -Gleichungen, n unb, Koeffizientenlänge w .

\rightsquigarrow Reduziertes System mit Koeffizienten $\approx 2^{n-1}w$ Länge

Beispiel (Fort.)

Cramers Regel::

$$x = \frac{\text{Det}[\dots]}{\text{Det}[\dots]} \quad y = \dots \quad z = \dots$$

wobei Länge $\text{Det}[\dots] \approx n \cdot w$, d. h. Ergebnis (Länge) ist nicht Ursache der Komplexität.

Beachte Methode ist anwendbar auf lineare Gleichungssysteme mit Koeffizienten in Polynomringen. Dann tritt exponentielles Wachstum der Grade der Polynome (als Koeffizienten) auf.

Normierung durch Rechnung im Quotientenkörper. Kosten!

Ringmorphisimen

$\Phi : R \rightarrow R'$ Homomorphismus, falls

- i) $\Phi(a + b) = \Phi(a) + \Phi(b) \quad (a, b \in R)$
- ii) $\Phi(ab) = \Phi(a)\Phi(b) \quad (a, b \in R)$
- iii) $\Phi(1) = 1$
- iv) $(\Phi(0) = 0 \quad \Phi(-a) = -\Phi(a))$

Ringmorphisimen: Beispiele

4.29 Beispiel

- a) **Modulare Homomorphismen:** $m \in \mathbb{Z}$

$$\Phi_m \mathbb{Z}[x_1, \dots, x_n] \rightarrow \mathbb{Z}_m[x_1, \dots, x_n]$$

mit $\Phi_m(x_i) = x_i \quad \Phi_m(a) = (a \text{ mod } m) \quad a \in \mathbb{Z}$.

- b) **Auswertungshomomorphismen:** $\alpha \in D$

$$\Phi_{x_i - \alpha} : D[x_1, \dots, x_n] \rightarrow D[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$$

$$\Phi_{x_i - \alpha}(a(x_1, \dots, x_n)) = a(x_1, \dots, x_{i-1}, \alpha, x_{i+1}, \dots, x_n)$$

- c) **Komposition Homomorphismen:**

$$\mathbb{Z}[x_1, \dots, x_n] \xrightarrow{\Phi_p} \mathbb{Z}_p[x_1, \dots, x_n] \xrightarrow{x_n - \alpha_n \in \mathbb{Z}_p} \dots \xrightarrow{x_2 - \alpha_2 \in \mathbb{Z}_p} \mathbb{Z}_p[x_1]$$

Interpolationsproblem: Anwendungsfälle

2 Anwendungsfälle:

Rekonstruktion von a aus $\Phi_{m_i}(a), i = 0, \dots, n$

- ▶ \mathbb{Z} : Finde $a \in \mathbb{Z}$ mit $u \leq a < u + m$, $a \equiv a_i \pmod{m_i}$ für festes u (z. B. $u = 0$ oder $u = -m/2$).

- ▶ $\mathbb{Z}[x_1, \dots, x_\nu] : \Phi_p : \mathbb{Z}[x_1, \dots, x_\nu] \rightarrow \mathbb{Z}_p[x_1, \dots, x_\nu]$
 $\Phi_I : \mathbb{Z}_p[x_1, \dots, x_\nu] \rightarrow \mathbb{Z}_p[x_1]$ (oder \mathbb{Z}_p).

I Komposition von Auswertungshomomorphismen $x_i - \alpha_i, \alpha_i \in \mathbb{Z}_p$.

$\Phi_{x-\alpha_i} : D[x] \rightarrow D$ D Polynomring über $\mathbb{Z}_p, \alpha_i \in \mathbb{Z}_p, i = 0, \dots, n$.

Es gibt ein eindeutiges Polynom $a(x) \in F_D[x]$ mit

$$\text{grad}_x(a(x)) \leq n \quad a(x_i) = a_i \in D \quad 0 \leq i \leq n.$$

Garner & Newton Interpolationsalgorithmen

Mixed Radix Darstellung: $a \in R/\langle m \rangle$ lässt sich darstellen als

$$(*) \quad a = \nu_0 + \nu_1(m_0) + \nu_2(m_0 m_1) + \dots + \nu_n \left(\prod_{i=0}^{n-1} m_i \right)$$

wobei $\nu_k \in R/\langle m_k \rangle \quad k = 0, 1, \dots, n$.

Beachte: Ausdruck (*) muss richtig interpretiert werden.

- ▶ Summe und Produkte sind in $R/\langle m \rangle$ zu rechnen.
- ▶ Die $\nu_k \in R/\langle m_k \rangle \hookrightarrow R/\langle m \rangle$. Diese Einbettung ist möglich, da $\langle m \rangle \subseteq \langle m_k \rangle$ für $k = 0, 1, \dots, n$, d. h. die Repräsentanten mod m_k können als Repräsentanten mod m gewählt werden.
- ▶ Existenz und Eindeutigkeit als Verallgemeinerung der Standarddarstellung einer Zahl zur basis β : $a = \sum_{i=0}^n \nu_i \beta^i \quad 0 \leq a < \beta^{n+1}, 0 \leq \nu_i < \beta$

Garner & Newton Interpolationsalgorithmen

- ▶ Fall \mathbb{Z} : $\mathbb{Z}_{m_k}, \mathbb{Z}_m$ in positiver Darstellung oder $\mathbb{Z}_{m_k}, \mathbb{Z}_m$ in symmetrischer Darstellung. Nicht gemischt!.
- ▶ Fall $D[x]$ D Polynomring über $\mathbb{Z}_p, \alpha_i \in \mathbb{Z}_p \quad (D), \nu_k \in F_D, 0 \leq k \leq n$.

$$a(x) = \nu_0 + \nu_1(x - \alpha_0) + \nu_2(x - \alpha_0)(x - \alpha_1) + \dots + \nu_n \prod_{i=0}^{n-1} (x - \alpha_i)$$

Darstellung ist eindeutig unter diesen Bedingungen Existenz!

Jede Menge von Polynomen $m_k(x) \in F_D[x], k = 0, \dots, n$ mit $\text{grad}(m_k(x)) = k$ ist Basis für Polynome mit $\text{grad} \leq n$ über F_D .

Newton Koeffizienten

Berechnung der $\nu_i, i = 0, \dots, n, \nu_i \in R/\langle m_k \rangle$

$$a = \nu_0 + \nu_1(m_0) + \nu_2(m_0 m_1) + \dots + \nu_n \left(\prod_{i=0}^{n-1} m_i \right)$$

$$\Phi_i(a) = a_i \quad i = 0, \dots, n \quad a_i \in R/\langle m_i \rangle$$

- ▶ $a \equiv \nu_0 \pmod{m_0}$ (oder $a(\alpha_0) = \nu_0 = a_0$), d. h. $\nu_0 = a_0$.
- ▶ Sind die Koeffizienten ν_0, \dots, ν_{k-1} bestimmt, so folgt

$$a \equiv \nu_0 + \nu_1(m_0) + \dots + \nu_k \left(\prod_{i=0}^{k-1} m_i \right) \pmod{m_k}$$

Newton Koeffizienten (Fort.)

Wähle ν_k , so dass

$$\nu_0 + \nu_1(m_0) + \dots + \nu_k \left(\prod_{i=0}^{k-1} m_i \right) \equiv a_k \pmod{m_k}$$

Da $\text{GGT} \left(\prod_{i=0}^{k-1} m_i, m_k \right) = 1$, ist $\prod_{i=0}^{k-1} m_i$ invertierbar mod m_k
 (Beachte im Polynomfall

$$a(\alpha_k) = \nu_0 + \nu_1(\alpha_k - \alpha_0) + \dots + \nu_k \prod_{i=0}^{k-1} (\alpha_k - \alpha_i) = a_k \in D$$

Da die $\alpha_i \in \mathbb{Z}_p, \alpha_i \neq \alpha_j, i \neq j$, folgt $\prod_{i=0}^{k-1} (\alpha_k - \alpha_i) \in \mathbb{Z}_p$ invertierbar).



Newton Koeffizienten (Forts.)

Also gilt

$$\nu_k \equiv \left[a_k - \left[\nu_0 + \nu_1(m_0) + \dots + \nu_{k-1} \left(\prod_{i=0}^{k-2} m_i \right) \right] \right] \cdot \left(\prod_{i=0}^{k-1} m_i \right)^{-1} \pmod{m_k}$$

oder

$$\nu_k = \left[a_k - \left[\nu_0 + \nu_1(\alpha_k - \alpha_0) + \dots + \nu_{k-1} \left(\prod_{i=0}^{k-2} (\alpha_k - \alpha_i) \right) \right] \right] \cdot \left(\prod_{i=0}^{k-1} (\alpha_k - \alpha_i) \right)^{-1}$$

d. h. $\nu_k \in \mathbb{Z}/\langle m_i \rangle = \mathbb{Z}_{m_i}$ bzw. $\nu_k \in D$.



Garner's Algorithmus/Newton Interpol. Algorithmus Gemischte Basisdarstellung

```

procedure INTEGERCRA  $((m_0, \dots, m_n), (a_0, \dots, a_n))$ 
     $\{m_i \in \mathbb{Z}, \text{GGT}(m_i, m_j) = 1 (i \neq j), a_i \in \mathbb{Z}_{m_i}\}$ 
    {Ausgabe  $a \in \mathbb{Z}_m$  mit  $m = \prod m_i \quad a \equiv a_i \pmod{m_i}, i = 1, \dots, n$ }
    { Schritt 1: Berechne die benötigten Inversen }
    {Inverse( $a, q$ ) =  $a^{-1} \pmod{q}$ }
    for  $k$  from 1 to  $n$  do
        begin
            product :=  $\Phi_{m_k}(m_0)$ ;
            for  $i$  from 1 to  $k-1$  do
                product :=  $\Phi_{m_k}(\text{product} \cdot m_i)$ ;
             $\gamma_k := \text{inverse}(\text{product}, m_k)$ ;
        end
    
```



Garner's Algorithmus (Forts.)

```

    { Schritt 2: Berechne die  $\{\nu_k\}$  }
     $\nu_0 := a_0$ ;
    for  $k$  from 1 to  $n$  do
        begin
            temp :=  $\nu_{k-1}$ ;
            for  $j$  from  $k-2$  to 0 do
                temp :=  $\Phi_{m_k}(\text{temp} \cdot m_j + \nu_j)$ ;
             $\nu_k := \Phi_{m_k}((a_k - \text{temp})\gamma_k)$ ;
        end
    { Schritt 3: Transformiere gemischte Radixdarstellung in Standard Darstellung }
     $a := \nu_n$ ;
    for  $k$  from  $n-1$  to 0 do
         $a := am_k + \nu_k$ ;
    return ( $a$ )
    
```



Bemerkungen zu Garner's Algorithmus

Üblicherweise m_i SP-Zahlen oder $\alpha_i \in \mathbb{Z}_p$ mit p SP-Zahl.

Die Reste a_i sind im Fall \mathbb{Z} auch SPZ. a ist dann Langzahl (die Liste (a_0, \dots, a_n) kann als Langzahldarstellung interpretiert werden). Bis auf Schritt 3 nur Operationen mit SPZ.

Beachte Schreibweise:

Φ_{m_k} (Ausdruck) \equiv Werte-Ausdruck in $\mathbb{Z}_{m_k}(R/\langle m_k \rangle)$.

Alle Operationen werden mit SP-Zahlen bzw. \mathbb{Z}_p Zahlen gemacht.

Inverse mit EEA (in \mathbb{Z}).

GGT(a, q) = 1 \leftrightarrow $sa + tq = 1$, $\Phi_q(s) = (s \bmod q) = \text{inverse}(a, q)$.

Schritt 3: Operationen in \mathbb{Z} . Warum kommt Element aus \mathbb{Z}_m als Ergebnis heraus?

Bemerkungen zu Garner's Algorithmus

Symmetrische Darstellung: $|\nu_k| \leq (m_k - 1)/2$
 $k = 0, \dots, n$

$$|a| \leq \frac{m_0 - 1}{2} + \frac{m_1 - 1}{2} m_0 + \dots + \frac{m_{n-1} - 1}{2} \left(\prod_{i=0}^{n-1} m_i \right) \leq \frac{1}{2} \left[\left(\prod_{i=0}^n m_i \right) - 1 \right]$$

Auch für $0 \leq \nu_k \leq m_k - 1$ $k = 0, \dots, n$

$$a \leq \left(\prod_{i=0}^{n-1} m_i \right) - 1$$

Berechnet wird

$$a = \nu_0 + m_0(\nu_1 + m_1(\nu_2 + \dots + m_{n-2}(\nu_{n-1} + m_{n-1}(\nu_n))))$$

Newton Interpolationsalgorithmus

- ▶ Im Fall $D[x]$ sind die Homomorphismen Auswertungshomomorphismen an Stellen α_i d.h. $\Phi_{x-\alpha_i} : D[x] \rightarrow D$ D Polynomring über \mathbb{Z}_p , $\alpha_i \in \mathbb{Z}_p$, $i = 0, \dots, n$. Zu bestimmen ist eind. Polynom $a(x) \in F_D[x]$ mit $\text{grad}(a(x)) \leq n$ mit $a(\alpha_i) = a_i \in D$ ($0 \leq i \leq n$).
- ▶ Man beachte, dass in den Anwendungen die a_i und somit die berechneten ν_i polynome mit Koeffizienten in \mathbb{Z}_p sind und bei der Bestimmung von ν_i nur Koeffizientenoperationen durchzuführen sind.
- ▶ Beide Algorithmen sehen identisch aus. Im NIA steht an Stelle der m_i stets $(\alpha_k - \alpha_i)$ und für Φ_{m_k} steht stets Φ_p und die Inverse ist in \mathbb{Z}_p zu berechnen.
- ▶ In beiden Algorithmen haben die Objekte stets drei Darstellungen.

Beispiel Garner's Algorithmus

4.30 Beispiel

Angenommen SP-Zahlen beschränkt $-100 < a < 100$ (2 Bit). Modulii: $m_0 = 99, m_1 = 97, m_2 = 95, m = m_0 m_1 m_2 = 919985$. Symmetrische konsistente Darstellung: $-456142 \leq a \leq 456142$

- ▶ Bestimme $a \in \mathbb{Z}_m$ mit $a \equiv 49 \pmod{99} \equiv -21 \pmod{97} \equiv -30 \pmod{95}$
 $a_0 = 49, a_1 = -21, a_2 = -30$.

Garner:

- ▶ Schritt 1:
 $\gamma_1 = m_0^{-1} \pmod{m_1} = 99^{-1} \pmod{97} = 2^{-1} \pmod{97} = -48$
 $\gamma_2 = (m_0 m_1)^{-1} \pmod{m_2} = 8^{-1} \pmod{95} = 12$
- ▶ Schritt 2: Gemischte Basiskoeffizienten für a
 $\nu_0 = 49, \nu_1 = -35, \nu_2 = -28$
- ▶ $a = 49 - 35(99) - 28(99)(97) = -272300$

Beispiel (Forts.)

4.31 Beispiel Eingangsproblem : System linearer Gleichungen.
 Schwierigkeit: Muss keine Lösung in \mathbb{Z} haben!

$$x_1 = \det \begin{vmatrix} 1 & 44 & 74 \\ -2 & 14 & -10 \\ 34 & -28 & 20 \end{vmatrix} \quad y_1 = \det \begin{vmatrix} 22 & 1 & 74 \\ 15 & -2 & 10 \\ -25 & 34 & 20 \end{vmatrix}$$

$$z_1 = \det \begin{vmatrix} 22 & 44 & 1 \\ 15 & 14 & -2 \\ -25 & -28 & 34 \end{vmatrix} \quad d = \det \begin{vmatrix} 22 & 44 & 74 \\ 15 & 14 & -10 \\ -25 & -28 & 20 \end{vmatrix}$$

$x = x_1/d \quad y = y_1/d \quad z = z_1/d \in \mathbb{Q}$

- In \mathbb{Z}_p berechne $x \bmod p, y \bmod p, z \bmod p, d \bmod p$ via Gauss \rightsquigarrow aus $x_1 \equiv xd \bmod p, y_1 \equiv yd \bmod p, z_1 \equiv zd \bmod p \rightsquigarrow x_1, y_1, z_1, d$ aus $\mathbb{Z} \rightsquigarrow \mathbb{Q}$ Lösung.

Beispiel (Forts.)

In \mathbb{Z}_7 :

$$\begin{array}{ll} x + 2y - 3z = 1 & \text{Gauss} \quad x \equiv -1 \pmod{7} \\ x - 3z = -2 & \rightsquigarrow y \equiv -2 \pmod{7} \\ 3x - z = -1 & z \equiv -2 \pmod{7} \\ & d \equiv -2 \pmod{7} \end{array}$$

In $\mathbb{Z}_{11}, \mathbb{Z}_{13}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$ liefert

$$\begin{array}{llll} x_1 \equiv -5 \pmod{11} & y_1 \equiv 0 \pmod{11} & z_1 \equiv -4 \pmod{11} & d \equiv 1 \pmod{11} \\ -2 & 4 & 6 & 4 \pmod{13} \\ 5 & -6 & -3 & -2 \pmod{17} \\ 9 & 6 & 7 & -8 \pmod{19} \end{array}$$

Beispiel (Forts.)

Modulare Darstellungen für x_1 und d

$$x_1 = (2, -5, -2, 5, 9), \quad d = (-2, 1, 4, -2, -8)$$

$$m_0 = 7, \quad m_1 = 11, \quad m_2 = 13, \quad m_3 = 17, \quad m_4 = 19$$

Garner $\rightsquigarrow x_1 = -44280, \dots, d = -7380$

Vergleiche diese mit den Zahlen die über Gauss Elimination in \mathbb{Z} auftreten!

$$\rightsquigarrow x = \frac{-44280}{-7380} = 6 \quad y = \frac{40590}{-7380} = -\frac{11}{2} \quad z = \frac{-11070}{-7380} = \frac{3}{2}$$

Problem hier: Lösung ist nicht ganzzahlig, sondern in \mathbb{Q} .
 Rekonstruktion rationaler Lösungen bei Koeffizienten in \mathbb{Z} .

Newton Interpolationsalgorithmus

4.32 Beispiel Polynombeispiel

Bestimme Polynom $a(x, y) \in \mathbb{Z}_{97}[x, y]$ vom Max. Grad 2 in x und Max.

Grad 1 in y mit

$$\begin{array}{ll} a(0, 0) = -21 & a(0, 1) = -30 \\ a(1, 0) = 20 & a(1, 1) = 17 \\ a(2, 0) = -36 & a(2, 1) = -31 \end{array}$$

- Rekonstruktion von $a(x, y)$ in $\mathbb{Z}_{97}[x, y]/\langle x - 0 \rangle$

$$D = \mathbb{Z}_{97}, \quad \alpha_0 = 0, \quad \alpha_1 = 1, \quad a_0 = -21, \quad a_1 = -30$$

Berechne Polynom $a(0, y) \in \mathbb{Z}_{97}[y]$:

Schritt 1:

$$\gamma_1 = (\alpha_1 - \alpha_0)^{-1} \pmod{97} = 1^{-1} \pmod{97} = 1.$$

Schritt 2:

$$\text{Newton Koeff: } \nu_0 = -21, \nu_1 = -9$$

Polynombeispiel (Forts.)

Schritt 3:

$$a(0, y) = -21 - 9(y - 0) = -9y - 21$$

- ▶ **Analog:** $\mathbb{Z}_{97}[x, y]/\langle x - 1 \rangle$ und $\mathbb{Z}_{97}[x, y]/\langle x - 2 \rangle$ liefert

$$a(1, y) = -3y + 20$$

$$a(2, y) = 5y - 36$$

- ▶ **Multivariater Schritt:** Garner mit $D = \mathbb{Z}_{97}[y]$
 $\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = 2, a_0 = a(0, y), a_1 = a(1, y), a_2 = a(2, y)$
- ▶ **Gesucht** $a(x, y) \in D[x] = \mathbb{Z}_{97}[y][x]$.

Polynombeispiel: Berechnung von $a(x, y)$

▶ **Schritt 1:**

$$\gamma_1 = 1, \gamma_2 = [(\alpha_2 - \alpha_0)(\alpha_2 - \alpha_1)]^{-1} \bmod 97 = -48$$

▶ **Schritt 2:**

$$\nu_0 = -9y - 21, \nu_1 = 6y + 41, \nu_2 = y$$

▶ **Schritt 3:**

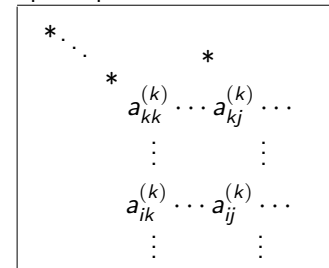
$$a(x, y) = (-9y - 21) + (6y + 41)(x - 0) + y(x - 0)(x - 1)$$

Beispiel: Modulare Determinantenberechnung

4.33 Beispiel Modulare Determinantenberechnung (vzGG S101)

Sei $A = (a_{ij})_{1 \leq i, j \leq n} \in \mathbb{Z}^{n \times n}$. Berechne $\det A$

Gauss Elimination über \mathbb{Q} , $2n^3$ Operationen in \mathbb{Q} . Ist dies "pol Zeit"?
 Die Anzahl der Wortoperationen hängt von den Zähler und Nenner der Zwischenergebnissen ab. Wie ist ihr Wachstum? Betrachte Stufe k bei der Elimination. A nichtsingulär und keine Zeilen oder Spaltenpermutationen notwendig.



$$a_{kk}^{(k)} \neq 0 \text{ für } k < i \leq n, k \leq j \leq n$$

$$a_{ij}^{(k+1)} = a_{ij}^{(k)} - \frac{a_{ik}^{(k)}}{a_{kk}^{(k)}} a_{kj}^{(k)}$$

Sei b_k obere Schranke für Zähler und Nenner der $a_{ij}^{(k)}$ ($1 \leq i, j \leq n$).

$k - 1$ Pivoting-Schritte

Beispiel: Modulare Determinantenberechnung (Forts.)

Insbesondere: $|a_{ij}| \leq b_0$ für $1 \leq i, j \leq n$. Es folgt

$$b_k \leq 2b_{k-1}^4 \leq 4b_{k-2}^{4^2} \leq \dots \leq 2^k b_0^{4^k},$$

d. h. exponentiell in der Länge der Eingabe $n^2 \lambda(b_0) \approx n^2 \log b_0$

Ist Gauss Elimination überhaupt polynomial in Eingabelänge?

Ja, aber nichttrivialer Beweis.

2 Alternativen: **Big-Prime**, **Small-Primes**

Modulare Determinantenberechnung (Forts.)

Sei $d = \det A$. Wähle Primzahl $p > 2|d|$. Wende Gauss Elimination auf $A \bmod p \in \mathbb{Z}_p^{n \times n}$ an. Sei r Ergebnis in symmetrischer Darstellung von \mathbb{Z}_p , d. h. $r \equiv d \bmod p - \frac{p}{2} < r < \frac{p}{2}$.
 Da $p \mid d - r$ und $|d - r| \leq |d| + |r| < \frac{p}{2} + \frac{p}{2} = p$ folgt $d = r$.
 Schranken für $\det A$: Hadamard Ungleichung

$$|\det A| \leq n^{n/2} B^n \text{ mit } B = \max_{1 \leq i, j \leq n} |a_{ij}|$$

Wortlänge $\lambda(C) = \lambda(n^{n/2} B^n)$ ist $\frac{1}{64} \log_2 C = \frac{1}{64} n (\frac{1}{2} \log_2 n) + \log_2 B$
 Polynomial in Eingabelänge $n^2 \lambda(B)$.

- ▶ Primzahl p zwischen $2C$ und $4C$. Finden (prob. Algorithmus). Arithmetik modulo p $O(\log^2 C)$ Wortoperationen.
- ▶ $O(n^3 n^2 (\log n + \log B)^2)$ Wortoperationen.

Modulare Determinantenberechnung (Forts.)

Small Primes:

$$C = n^{n/2} B^n, r = \lceil \log_2(2C + 1) \rceil.$$

- ▶ Wähle r verschiedene Primzahlen $m_0, \dots, m_{r-1} \in \mathbb{N}$.
- ▶ Für $0 \leq i < r$ berechne $d_i \equiv \det A \bmod m_i$ (Gauss) in \mathbb{Z}_{m_i} .
- ▶ Chinesischer R.A $d \equiv d_i \bmod m_i \quad 0 \leq i < r$.

Dann $\det A \equiv d \bmod m_i$ und somit $\det A \equiv d \bmod m$ für $m = m_0 \dots m_{r-1}$.

Wegen $m \geq 2^r > 2^{n/2} n B^n \geq 2|d|$ gilt $d = \det A$.

Modulare Determinantenberechnung (Forts.)

Kosten: Berechnung der r Primzahlen (ersten r PZ),

- ▶ $O(r \log^2 r \log \log r)$ Wort-Operationen, $\log m_i \in O(\log r)$.
 $\log m = \sum_{0 \leq i < r} \log m_i \in O(r \log r)$.
- ▶ Operationen $\bmod m_i \leftrightarrow O(\log^2 m_i)$, d. h. $O(\log^2 r)$ Operationen.
 $O(n^3 r \log^2 r)$ Wortoperationen, $A \bmod m_i \rightarrow O(n^2 r \log^2 r)$.
- ▶ r Werte $O(n^2 r^2 \log^2 r)$.

$$O(n^4 \log^2(nB)(\log^2 n + (\log \log B)^2))$$

Praxis: Vorberechnung von Primzahlen mit Wortlänge.

Inhalt Kapitel 5

Newton's Iteration und Hensel's Konstruktion

Motivation

- P-adische und ideal-adische Darstellungen
- Ideal-adische Darstellung und Approximation
- Iteration nach Newton für $F(u) = 0$
- Ideal-adische Newton Iteration
- Hensel's Lemma
- Hensel Lifting
- Multifaktor Hensel Lifting. Algorithmus nach Zassenhaus
- Multivariate Verallgemeinerung von Hensel's Lemma
- Lösung diophantischer Polynomgleichungen in $\mathbb{Z}_p[x_1]$

Iteration nach Newton für $F(u) = 0$

Lineare p-adische Iteration

- ▶ Inversion von $\Phi_p : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$. Nur eine Primzahl p , als bekannt $u_0(x) \in \mathbb{Z}_p[x]$: Bild der gesuchten Lösung $u(x) \in \mathbb{Z}[x]$, d.h. $u_0(x)$ ist p-adische Approximation erster Ordnung.

Gesucht: Methode zur Berechnung der Approximation der Ordnung k , d. h.

$$u_0(x) + u_1(x)p + \dots + u_{k-1}(x)p^{k-1} \in \mathbb{Z}_p^k[x] \quad k = 1, \dots, n + 1$$

Lifting von Bild $u_0(x) \in \mathbb{Z}_p[x]$.

- ▶ Offenbar benötigt man **zusätzliche Information**, um $u(x)$ festzulegen. Üblicherweise ist diese Information in Form von **Gleichungen** gegeben, die $u(x)$ **erfüllen muss**
z. B. $F(u) = 0$ wobei $F(u) \in \mathbb{Z}[x][u]$. Z.B. $u^2 - a(x) = 0$.

Klassisches Newton-Verfahren zur Lösung einer nichtlinearen Gleichung $F(u) = 0$

- ▶ Entwicklung von F als Taylor-Reihe um Punkt $u^{(k)}$:

$$F(u) = F(u^{(k)}) + F'(u^{(k)})(u - u^{(k)}) + \frac{1}{2}F''(u^{(k)})(u - u^{(k)})^2 + \dots$$

- ▶ Setzt man $u = \tilde{u}$ und betrachtet man nur lineare Terme, so $0 = F(u^{(k)}) + F'(u^{(k)})(\tilde{u} - u^{(k)})$, d.h.

$$u^{(k+1)} = u^{(k)} - \frac{F(u^{(k)})}{F'(u^{(k)})} \quad (F'(u^{(k)}) \neq 0)$$

- ▶ Startpunkt $u^{(1)} \rightsquigarrow$ **Quadratische Konvergenz**.

Newton-Verfahren zur Lösung einer nichtlinearen Gleichung $F(u) = 0$

Annahme: Es gibt eine Lösung $\tilde{u} = u(x) \in \mathbb{Z}[x]$.
Gegeben: Approximation erster Ordnung $u_0(x) \in \mathbb{Z}_p[x]$ von \tilde{u}

- ▶ Schreibt man die Lösung in ihrer p-adischen Pol-Darstellung

$$\tilde{u} = u_0(x) + u_1(x)p + \dots + u_n(x)p^n$$

- ▶ **Aufgabe:** Bestimme die $u_i(x) \in \mathbb{Z}_p[x] \quad i = 1, 2, \dots, n$ wobei $u^{(k)} = u_0(x) + u_1(x)p + \dots + u_{k-1}(x)p^{k-1} \quad 1 \leq k \leq n + 1$ die p-adische Approximation k-ter Ordnung von \tilde{u} ist.
- ▶ **Gesucht Iterationsformel**, die im Schritt k aus $u^{(k)}$ den p-adischen Polynomkoeffizienten $u_k(x) \in \mathbb{Z}_p[x]$ berechnet und somit zu $u^{(k+1)} = u^{(k)} + u_k(x)p^k \quad 1 \leq k \leq n$ führt.

Newton-Verfahren:: Gleichung $F(u) = 0$ (Forts.)

5.5 Lemma Sei $a(x) \in D[x]$. Dann gilt in $D[x][y]$

$$a(x + y) = a(x) + a'(x)y + b(x, y)y^2$$

für ein geeignetes Polynom $b(x, y) \in D[x, y]$.

5.6 Lemma Sei $a(x, y) \in D[x, y]$ bivariates Polynom. Dann gilt im Polynomring $D[x, y][\xi, \eta]$.

$$\begin{aligned} a(x + \xi, y + \eta) &= a(x, y) + a_x(x, y)\xi + a_y(x, y)\eta \\ &\quad + b_1(x, y, \xi, \eta)\xi^2 + b_2(x, y, \xi, \eta)\xi\eta \\ &\quad + b_3(x, y, \xi, \eta)\eta^2 \end{aligned}$$

Für geeignete Polynome $b_i(x, y, \xi, \eta) \in D[x, y, \xi, \eta]$.

Newton-Verfahren:: Gleichung $F(u) = 0$ (Forts.)

- Das Polynom $F(u) \in \mathbb{Z}[x][u]$ hat dann folgende Darstellung

$$F(u^{(k)} + u_k(x)p^k) = F(u^{(k)}) + F'(u^{(k)})u_k(x)p^k + g(u^{(k)}, u_k(x)p^k)[u_k(x)]^2 p^{2k}$$

für ein $g(u, w) \in D[u, w]$.

- Wegen $u^{(k)} \equiv \tilde{u} \pmod{p^k}$ und $F(\tilde{u}) = 0$ folgt $F(u^{(k)}) \equiv 0 \pmod{p^k}$.
- Analog gilt $F(u^{(k)} + u_k(x)p^k) \equiv 0 \pmod{p^{k+1}}$ falls $u^{(k+1)} = u^{(k)} + u_k(x)p^k$.

Newton-Verfahren:: Gleichung $F(u) = 0$ (Forts.)

- D. h.

$$\frac{F(u^{(k)} + u_k(x)p^k)}{p^k} = \frac{F(u^{(k)})}{p^k} + F'(u^{(k)})u_k(x) + g(u^{(k)}, u_k(x)p^k)[u_k(x)]^2 p^k$$

- Wende Φ_p an, so erfüllt $u_k(x) \in \mathbb{Z}_p[x]$ die Gleichung

$$0 = \Phi_p\left(\frac{F(u^{(k)})}{p^k}\right) + \Phi_p(F'(u^{(k)}))u_k(x) \in \mathbb{Z}_p[x]$$

Wegen $u^{(k)} \equiv u^{(1)} \pmod{p}$ für $k \geq 1$ gilt

$$F'(u^{(k)}) \equiv F'(u^{(1)}) \pmod{p}$$

Newton-Verfahren:: Gleichung $F(u) = 0$ (Forts.)

Genügt die gegebene Approximation erster Ordnung $u^{(1)}$ der Bedingung

$$F'(u^{(1)}) \not\equiv 0 \pmod{p}$$

so ist der gesuchte p-adische Polynomkoeffizient

$$(\#) \quad u_k(x) = -\frac{\Phi_p\left(\frac{F(u^{(k)})}{p^k}\right)}{\Phi_p(F'(u^{(1)}))} \in \mathbb{Z}_p[x]$$

Diese Division ist exakt im Polynomring $\mathbb{Z}_p[x]$, falls eine Polynomlösung existiert.

Die Gleichung (#) ist die **lineare Aktualisierungsformel** zusammen mit $u^{(k+1)} = u^{(k)} + u_k(x)p^k \rightsquigarrow$ lineare p-adische Newtonverfahren.

Beachte: $F(u^{(k)})$ wird in $\mathbb{Z}[x]$ durchgeführt, sowie auch Division durch p^k erst dann Φ_p anwenden!

Beispiel: Iteration nach Newton für Quadratwurzel

5.7 Beispiel Bestimme Polynom $u(x) \in \mathbb{Z}[x]$, das die Quadratwurzel des Polynoms

$$a(x) = 36x^4 - 180x^3 + 93x^2 + 330x + 121 \in \mathbb{Z}[x]$$

(unter der Annahme, dass $a(x)$ quadratisch ist).

$u(x)$ als Lösung von $F(u) = a(x) - u^2 = 0$.

Wähle $p = 5$ $\Phi_5(a(x)) = x^4 - 2x^2 + 1 \in \mathbb{Z}_5[x]$.

Approximation 1 Ordnung muss Quadratwurzel von $\Phi_5(a(x))$ sein, d. h.

$$u^{(1)} = u_0(x) = x^2 - 1 \in \mathbb{Z}_5[x].$$

$$F'(u) = -2u \text{ und } \Phi_5(F'(u^{(1)})) = \Phi_5(-2u^{(1)}) = -2x^2 + 2$$

Beispiel: Quadratwurzel

Dann

$$u_1(x) = -\frac{\Phi_5\left(\frac{F(u^{(1)})}{5}\right)}{(-2x^2 + 2)} = -\frac{\Phi_5\left(\frac{35x^4 - 180x^3 + 95x^2 + 330x + 120}{5}\right)}{(-2x^2 + 2)}$$

$$= -\frac{(2x^4 - x^3 - x^2 + x - 1)}{(-2x^2 + 2)} = x^2 + 2x - 2 \in \mathbb{Z}_5[x]$$

und $u^{(2)} = (x^2 - 1) + (x^2 + 2x - 2)5 \in \mathbb{Z}_{25}[x]$

Analog

$$u_2(x) = -\frac{(-2x^3 + 2x)}{(-2x^2 + 2)} = -x \in \mathbb{Z}_5[x]$$

d. h. $u^{(3)} = (x^2 - 1) + (x^2 + 2x - 2)5 + (-x)5^2 \in \mathbb{Z}_{125}[x]$

$F(u^{(3)}) = 0 \rightsquigarrow$ Terminierung, d. h.

Quadratwurzel ist $u(x) = u^{(3)} = 6x^2 - 15x - 11 \in \mathbb{Z}[x]$.

Beispiel: Division mit Rest

5.8 Beispiel Division mit Rest über Newton Iteration

$\mathbb{Z}, F[x]$ sind Euklidische Bereiche \rightsquigarrow Division mit Rest.

Komplexität $O(n^2)$ (Wort- oder Körperoperationen)

- Kann verbessert werden auf $O(M(n))$ wobei M die Multiplikationsschranke ist.
- **Polynomfall:** Sei D Ring $a, b \in D[x]$ Grade n, m mit $m \leq n, b$ monisch. Finde $q, r \in D[x]$ mit $a = qb + r$ $\text{Grad}(r) < \text{Grad}(b)$. [Da b monisch ist, ist die Existenz sicher].
- Es gilt:

$$(*) \quad x^n a\left(\frac{1}{x}\right) = \left(x^{n-m} q\left(\frac{1}{x}\right)\right) \cdot \left(x^m b\left(\frac{1}{x}\right)\right) + x^{n-m+1} \left(x^{m-1} r\left(\frac{1}{x}\right)\right)$$

Beispiel: Division mit Rest

Setze $rev_k(a) := x^k a(1/x)$. Für $k = n$ erhält man

$$a = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$rev_n(a) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

$$(*)' \quad rev_n(a) = rev_{n-m}(q) \cdot rev_m(b) + x^{n-m+1} \cdot rev_{m-1}(r)$$

d. h.

$$rev_n(a) \equiv rev_{n-m}(q) \cdot rev_m(b) \pmod{x^{n-m+1}}$$

- Da $rev_m(b)$ 1 als Konstanten Koeffizienten hat, ist es invertierbar mod x^{n-m+1} also

$$rev_{n-m}(q) \equiv rev_n(a) rev_m(b)^{-1} \pmod{x^{n-m+1}}$$

hieraus lassen sich q und r berechnen:

$$q = rev_{n-m}(rev_{n-m}(q)) \text{ und } r = a - qb$$

Beispiele (Forts.)

z.B. $a = 5x^5 + 4x^4 + 3x^3 + 2x^2 + x$ $b = x^2 + 2x + 3$ $\mathbb{F}_7[x]$

$$rev_5(a) = x^4 + 2x^3 + 3x^2 + 4x + 5$$

$$rev_2(b) = 3x^2 + 2x + 1$$

Wie berechnet man $rev_2(b)^{-1} \pmod{x^4}$?

$$rev_2(b)^{-1} \equiv 4x^3 + x^2 + 5x + 1 \pmod{x^4} \text{ in } \mathbb{F}_7[x]$$

$$\rightsquigarrow rev_3(q) \equiv 6x^3 + x + 5 \pmod{x^4}$$

$$\rightsquigarrow q = 5x^3 + x^2 + 6 \text{ und } r = a - qb = 3x + 3$$

Inversion modulo x^l in $D[x]$

Problem:

Gegeben $f \in \mathbb{D}[x]$, $l \in \mathbb{N}$ mit $f(0) = 1$

Finde $g \in \mathbb{D}[x]$ mit $fg \equiv 1 \pmod{x^l}$

- ↪ Newton Iteration Lösungen von $\Phi(g) = 0$ aus Anfangsnäherung g_0 :

$$g_{i+1} = g_i - \frac{\Phi(g_i)}{\Phi'(g_i)}$$

- ▶ $\Phi(g) = \frac{1}{g} - f = 0$

$$\rightsquigarrow g_{i+1} = g_i - \frac{1/g_i - f}{-1/g_i^2} = 2g_i - fg_i^2$$

Inversion modulo x^l in $D[x]$

Seien $f(0) = 1$, $g_0 = 1$, $g_{i+1} \equiv 2g_i - fg_i^2 \pmod{x^{2^{i+1}}}$.

Dann $fg_i \equiv 1 \pmod{x^{2^i}}$ für $i \geq 0$

Beweis: Ind. $i = 0$ $f \cdot g_0 \equiv f(0)g_0 \equiv 1 \cdot 1 \equiv 1 \pmod{x^{2^0}}$

Ind. Schritt:

$$\begin{aligned} 1 - fg_{i+1} &\equiv 1 - f(2g_i - fg_i^2) \\ &\equiv 1 - 2fg_i + f^2g_i^2 \\ &\equiv (1 - fg_i)^2 \\ &\equiv 0 \pmod{x^{2^{i+1}}} \end{aligned}$$

- ▶ Beachte: Ist $f(0)$ Einheit ungleich 1, so verwende für g_0 $f(0)^{-1}$.
Ist $f(0)$ keine Einheit, so gibt es keine Inverse von $f \pmod{x^l}$ da aus $fg \equiv 1 \pmod{x^l} \rightsquigarrow f(0)g(0) = 1$

Inversion modulo x^l in $D[x]$: Beispiel

5.9 Beispiel $f = 3x^2 + 2x + 1$ in $\mathbb{F}_7[x]$, $l = 4$

Alg. berechnet mit $g_0 = 1$ $r = 2 = \lceil \log(l) \rceil$

$$g_1 \equiv 2g_0 - fg_0^2 = 2 - (3x^2 + 2x + 1) \equiv 5x + 1 \pmod{x^2}$$

$$g = g_2 \equiv 2g_1 - fg_1^2 = 2x^4 + 4x^3 + x^2 + 5x + 1 \equiv 4x^3 + x^2 + 5x + 1 \pmod{x^4}$$

- ▶ Aufwand: $l = 2^r$ $3M(l) + l \in O(M(l))$ Arithm. Operationen (siehe auch von zur Gathen/Gerhard s.246)

- ▶ Division mit Rest nach diesem Verfahren kostet

$$4M(n) + M(n) + O(n)$$

Ringoperationen

$$M(n) \in O(n \log n \log \log n)$$

p-adische Inversion mit Newton Iteration

5.10 Beispiel Sei R beliebiger Ring $0 \neq p \in R$. p-adische Darstellung ist auch hier sinnvoll.

Problem: Berechnung eines Inversen von $a \pmod{p^l}$ $l > 1$, aus Inverse von $a \pmod{p}$.

Gegeben: b_0 mit $ab_0 \equiv 1 \pmod{p}$

Gesucht: b mit $ab \equiv 1 \pmod{p^l}$::Liften von Inversen.

```

procedure InvLift ( $a, b_0, l$ ) { $ab_0 \equiv 1 \pmod{p}$   $l \in \mathbb{N}$ }
 $r := \lceil \log l \rceil$ 
for  $i = 1$  to  $r$  do
    berechne  $b_i := (2b_{i-1} - ab_{i-1}^2) \pmod{p^{2^i}}$ 
return  $b_r$ 
    
```

Behauptung: $ab_i \equiv 1 \pmod{p^{2^i}}$ Induktion: $i = 0$

$$1 - ab_{i+1} \equiv 1 - a(2b_i - ab_i^2) \equiv 1 - 2ab_i + a^2b_i^2 \equiv (1 - ab_i)^2 \equiv 0 \pmod{p^{2^{i+1}}}$$

Bsp:: $R = \mathbb{Z}$, $p > 1$ oder $R = D[x]$ p monisch, $\text{grad } b < l$ $\text{grad } p$ etwa $p = x$.

P-adische Inversion mit Newton Iteration (Forts.)

5.11 Folgerung Sei R Ring, $p \in R$, $l \in \mathbb{N}^+$:

a ist invertierbar mod p^l gdw a invertierbar mod p .

Aufwand: $O(M(l \log p))$ Wortoperationen, M multipl. Kosten bzw. $O(M(l \text{ grad } p))$ Operationen in D .

Newton Iteration mit quadratischer Konvergenz

5.12 Lemma Sei $F \in R[u]$, $a, b \in R$ mit $F(a) \equiv 0 \pmod{p^k}$ für ein $k \in \mathbb{N}^+$, $F'(a)$ invertierbar modulo p . Weiterhin gelte

$$(*) \quad b \equiv a - F(a)F'(a)^{-1} \pmod{p^{2k}}$$

Dann gilt $F(b) \equiv 0 \pmod{p^{2k}}$, $b \equiv a \pmod{p^k}$ und $F'(b)$ ist invertierbar mod p .

„Ist a eine gute Approximation einer Nullstelle von F , so ist b eine bessere Approximation, mindestens doppelt so gut“.

Quadratische Konvergenz der Newton Iteration

Beweis: $F'(a)$ ist invertierbar mod p^k , d. h. rechte Seite von $(*)$ ist wohldefiniert. $F'(a)^{-1} \pmod{p^{2k}}$ lässt sich aus $F'(a)^{-1} \pmod{p}$ berechnen.

Da $p^k \mid p^{2k}$ gilt $(*)$ auch mod $p^k \rightsquigarrow b \equiv a - F(a)F'(a)^{-1} \equiv a \pmod{p^k}$.

$$\begin{aligned} F(b) &\equiv F(a) + F'(a)(b - a) + \rightsquigarrow (b - a)^2 \\ &\equiv F(a) + F'(a)(b - a) \equiv F(a) + F'(a)(-F(a)F'(a)^{-1}) \\ &\equiv 0 \pmod{p^{2k}} \end{aligned}$$

Da $p^{2k} \mid (a - b)^2$ und $F(a) \equiv 0 \pmod{p^k}$.

Wegen $a \equiv b \pmod{p^k}$ gilt $a \equiv b \pmod{p}$. $F(a) \equiv F(b) \pmod{p}$ für alle $F \in R[u]$. Insbesondere für F' .

Für p Primelement im euklidischem Bereich ist die Bedingung $F'(a)$ invertierbar mod p gdw $F'(a) \not\equiv 0 \pmod{p}$.

Algorithmus p-adische Newton Iteration

begin

{Eingabe : $F \in R[u]$, R Ring, $p \in R$, $l \in \mathbb{N}^+$, $a_0 \in R$,
 {Startlösung mit $F(a_0) \equiv 0 \pmod{p}$, $F'(a_0)$ invertierbar mod p ,
 $\{s_0$ modulare Inverse für $F'(a_0) \pmod{p}$
 {Ausgabe : $a \in R$ mit $F(a) \equiv 0 \pmod{p^l}$ und $a \equiv a_0 \pmod{p}$

$r := \lceil \log l \rceil$

for $i := 1$ **to** $r - 1$ **do**

begin

berechne $a_i, s_i \in R$ mit

$$a_i \equiv a_{i-1} - F(a_{i-1})s_{i-1} \pmod{p^{2^i}}$$

$$s_i \equiv 2s_{i-1} - F'(a_i)s_{i-1}^2 \pmod{p^{2^i}}$$

end

Berechne $a \in R$ mit $a \equiv a_{r-1} - F(a_{r-1})s_{r-1} \pmod{p^l}$

return a

end

Algorithmus p-adische Newton Iteration

Korrektheit: Sei $a_r \equiv a_{r-1} - F(a_{r-1})s_{r-1} \pmod{p^{2^r}}$.

► Dann $a \equiv a_r \pmod{p^l}$ und es genügt die Invarianten.

$$a_i \equiv a_0 \pmod{p}, \quad F(a_i) \equiv 0 \pmod{p^{2^i}}, \quad s_i \equiv F'(a_i)^{-1} \pmod{p^{2^i}}$$

Für $0 \leq i \leq r$. Per Induktion zu zeigen.

(Anwendung Lemma+Inversionsalg.).

Ist $R = \mathbb{Z}$ oder $R = F[x]$, F Körper, und $p \in R$ prim oder irreduzibel, so ist der Startwert als Lösung für Polynom in $K = R/\langle p \rangle$.

Aufwand:

$R = D[x]$, $F \in R[u]$, $p = x$, $l = 2^k$, $\text{grad}_u F = n$,
 $\text{grad}_x F < l \rightsquigarrow O(nM(l)) + O(nl)$ Operationen in D .

$R = \mathbb{Z}$, $0 \leq a_0 < p$, F grad n , mit Koeffizienten $< p^l$

$\rightsquigarrow O(nM(l \log p))$ Wortoperationen.

Beispiel

5.13 Beispiel

- i) $R = \mathbb{Z}$, $p = 5$ bestimme nicht-triviale Lösung von $u^4 \equiv 1 \pmod{625}$, d. h. $F(u) = u^4 - 1$.

Startlösung $a_0 = 2$, da $F(2) \equiv 0 \pmod{5}$.

$F'(2) = 4 \cdot 2^3 \equiv 2 \not\equiv 0 \pmod{5}$, d. h. $s_0 \equiv 2^{-1} \equiv 3 \pmod{5}$.

$$\begin{aligned} a_1 &\equiv a_0 - F(a_0)s_0 = 2 - 15 \cdot 3 \equiv 7 \pmod{25} \\ s_1 &\equiv 2s_0 - F'(a_1)s_0^2 = 2 \cdot 3 - 1372 \cdot 3^2 \equiv 8 \pmod{25} \\ a &\equiv a_1 - F(a_1)s_1 = 7 - 2400 \cdot 8 \equiv 182 \pmod{625} \end{aligned}$$

In der Tat gilt $182^4 = 1 + 1755519 \cdot 625$.

Beispiel

- ii) $R = \mathbb{F}_3[x]$, $p = x$. Bestimme Quadratwurzel a von $f = x + 1$ modulo x^4 mit $a(0) = -1$. $F = u^2 - f \in \mathbb{F}_3[x][u]$, $a_0 = -1$ als Startlösung, da $a_0(0) = -1$, $F(a_0) = -x \equiv 0 \pmod{x}$ sowie $F'(a_0) = 2a_0 \equiv 1 \not\equiv 0 \pmod{x}$, d. h. $s_0 = 1$.

$$\begin{aligned} a_1 &\equiv a_0 - F(a_0)s_0 = -1 - (-x)1 = x - 1 \pmod{x^2} \\ s_1 &\equiv 2s_0 - F'(a_1)s_0^2 = 2 \cdot 1 - 2(x-1) \cdot 1^2 \\ &= x + 1 \pmod{x^2} \\ a &\equiv a_1 - F(a_1)s_1 = x - 1 - x^2(x+1) \\ &= -x^3 - x^2 + x - 1 \pmod{x^4} \end{aligned}$$

Offenbar

$$(-x^3 - x^2 + x - 1)^2 = (x + 1) + x^4(x^2 - x - 1)$$

Ideal-adische Newton Iteration

- Inversion eines multivariaten Auswertungshomomorphismus

$$\Phi_I : \mathbb{Z}_p[x_1, \dots, x_\nu] \rightarrow \mathbb{Z}_p[x_1]$$

mit Kern $I = \langle x_2 - \alpha_2, \dots, x_\nu - \alpha_\nu \rangle$, $\alpha_i \in \mathbb{Z}_p$, $2 \leq i \leq \nu$.

- Startpunkt: Approximation erster Ordnung zur gesuchten Lösung $\tilde{u} \in \mathbb{Z}_p[\vec{x}]$.

$$u^{(1)} = \Phi_I(\tilde{u}) \in \mathbb{Z}_p[x_1] = \mathbb{Z}_p[\vec{x}]/I$$

- Zusatzinformation: \tilde{u} Lösung der Polynomgleichung $F(u) = 0$, wobei $F(u) \in \mathbb{Z}_p[\vec{x}][u]$.

- Ziel: Definition einer Iterationsformel $u^{(k+1)} = u^{(k)} + \Delta u^{(k)}$, wobei $u^{(i)}$ ideal-adische Approximation i -ter Ordnung und $\Delta u^{(k)} \in I^k$.

Ideal-adische Newton Iteration (Forts.)

Durch Anwendung von Hilfssatz erhält man als Taylorentwicklung $F(u^{(k)} + \Delta u^{(k)}) = F(u^{(k)}) + F'(u^{(k)})\Delta u^{(k)} + G(u^{(k)}, \Delta u^{(k)})[\Delta u^{(k)}]^2$

Ideal-adische Approximation der Ordnung $k + 1$, d. h. $u^{(k+1)}$ so $F(u^{(k)} + \Delta u^{(k)}) \in I^{k+1}$ und wegen $\Delta u^{(k)} \in I^k$ folgt $[\Delta u^{(k)}]^2 \in I^{2k}$, d. h. wendet man $\Phi_{I^{k+1}}$ an, so gilt

$$(*) \quad 0 = \Phi_{I^{k+1}}(F(u^{(k)})) + \Phi_{I^{k+1}}(F'(u^{(k)}))\Delta u^{(k)} \in \mathbb{Z}_p[\vec{x}]/I^{k+1}$$

und $\Delta u^{(k)}$ muss diese Gleichung erfüllen für $k = 1$ so $\Delta u^{(1)} \in I$ und

$$\Delta u^{(1)} = \sum_{i=2}^{\nu} u_i(x_1)(x_i - \alpha_i) \text{ mit } u_i(x_1) \in \mathbb{Z}_p[x_1]$$

Quadratisches Hensel Lifting (Forts.)

$$e = a - uw = x^4 - 1 - x^4 - 2x^3 + x^2 + 2x + 2x^3 + 4x^2 - 2x - 4 = 5x^2 - 5$$

$$\hat{u} = u + te = 10x^4 - 9x^3 - 13x^2 + 9x + 3$$

$$\hat{w} = w + se = -10x^2 + x + 8$$

Und somit

$$a - \hat{u}\hat{w} = 25(4x^6 - 4x^5 - 8x^4 + 7x^3 + 5x^2 - 3x - 1) \equiv 0 \pmod{25}, \text{ d. h.}$$

$$a \equiv \hat{u}\hat{w} \pmod{25}.$$

Problem: Grade von \hat{u}, \hat{w} sind größer als die von u bzw. w insbesondere ist ihre Summe $> \text{grad } a$.

- Dies geschieht z. B. wenn Vielfache von m Nullteiler $\pmod{m^2}$ sind und somit ist Produkt der Hauptkoeffizienten $\equiv 0 \pmod{m}$.

Quadratisches Hensel Lifting (Forts.)

- Dies kann vermieden werden durch Verwendung der Division mit Rest in $\mathbb{R}[x]$. Sie ist möglich wenn der Divisor monisch ist:

► Altlemma:

i) $a, b \in R[x], b \neq 0$ monisch, dann gibt es eindeutige Polynome $q, r \in R[x]$ mit $a = qb + r$ und $\text{grad } r < \text{grad } b$.

ii) Sind a, b, q, r wie in i) und gilt $a \equiv 0 \pmod{m}$ für ein $m \in R$, so $q \equiv r \equiv 0 \pmod{m}$.

(**Beweis ii**): Sei $\text{grad } b = n \geq 0 \rightsquigarrow$ aus $a \equiv 0 \pmod{m}$ b monisch, $qx^n \equiv 0 \pmod{m}$, d. h. $q \equiv 0 \pmod{m}$ und somit auch $r \equiv 0 \pmod{m}$.

- Überlegung führt zu: **Algorithmus Hensel Schritt**

//Eingabe: $m \in R \quad a, u, w, s, t \in R[x]$ mit
 $a \equiv uw \pmod{m}, su + tw \equiv 1 \pmod{m}$, wobei w monisch,
 $\text{grad } a = n = \text{grad } u + \text{grad } w, \text{grad } s < \text{grad } w$ und $\text{grad } t < \text{grad } u$.

Ausgabe: Polynome $u^*, w^*, s^*, t^* \in R[x]$ mit

$$a \equiv u^*w^* \pmod{m^2} \text{ und } s^*u^* + t^*w^* \equiv 1 \pmod{m^2}$$

wobei w^* monisch, $u^* \equiv u \pmod{m}, w^* \equiv w \pmod{m}$,
 $s^* \equiv s \pmod{m}, t^* \equiv t \pmod{m}, \text{grad } u^* = \text{grad } u$,
 $\text{grad } w^* = \text{grad } w, \text{grad } s^* < \text{grad } w^*, \text{grad } t^* < \text{grad } u^*.$ //

1. Berechne $e, q, r, u^*, w^* \in R[x]$ mit $\text{grad } r < \text{grad } w$ und $e \equiv a - uw \pmod{m^2}, se \equiv qw + r \pmod{m^2}$
 $u^* \equiv u + te + qu \pmod{m^2}, w^* \equiv w + r \pmod{m^2}$
2. Berechne $b, c, d, s^*, t^* \in R[x]$ mit $\text{grad } d < \text{grad } w^*$ und $b \equiv su^* + tw^* - 1 \pmod{m^2}, sb \equiv cw^* + d \pmod{m^2}$
 $s^* \equiv s - d \pmod{m^2}, t^* \equiv t - tb - cu^* \pmod{m^2}$
3. Return u^*, w^*, s^*, t^* .

Algorithmus Hensel-Schritt: Korrektheit

5.18 Satz Der Algorithmus ist korrekt. Aufwand für:

- $R = \mathbb{Z} : 0(M(n)M(\log m))$ Wortoperationen, falls Eingaben in max-Norm $< m^2$.
- $R = F[y] : 0(M(n)M(\text{grad}_y m))$ Operationen in F Falls grad in y der Eingaben $< 2\text{grad}_y m$.

Beweis: Nachrechnen. \mathbb{Z} : Grad der Polynome $\leq n$. Koeffizienten $\leq m^4$ Länge $0(\log m)$. Division mit Rest $0(M(n))$.

Beispiel: Hensel Lifting

5.22 Beispiel Sei $m = 3$ $a = x^4 - 2x^3 - 11x^2 + 4x + 3 \in \mathbb{Z}[x]$.
 Dann gilt

- ▶ $a \equiv x(x+1)(x^2+1) \pmod{3}$. $u_0 = x^2 + xw_0 = x^2 + 1$ teilerfremd mod 3.
- ▶ $s_0 = x + 1$ $t_0 = -x + 1$ $s_0 u_0 + t_0 w_0 \equiv 1 \pmod{3}$

Zwei Hensel Schritte liefern:

- ▶ $e_1 \equiv a - u_0 w_0 \equiv -3x^3 - 3x^2 + 3x + 3 \pmod{9}$
 $q_1 \equiv -3x^2 + 3x + 3 \pmod{9}$ $r_1 \equiv 3x \pmod{9}$
- ▶ $u_1 \equiv x^2 + 4x + 3 \pmod{9}$
- ▶ $w_1 \equiv x^2 + 3x + 1$, $b_1 \equiv 3x^2 + 3$, $c_1 \equiv 3x + 3$, $d_1 \equiv 0 \pmod{9}$
- ▶ $s_1 \equiv x + 1 \pmod{9}$
- ▶ $t_1 \equiv -x - 2 \pmod{9}$ $e_2 \equiv a - u_1 w_1 \equiv -9x^3 - 27x^2 - 9x \pmod{81}$
 $q_2 \equiv -9x^2 - 9x \pmod{81}$ $r_2 \equiv 0 \pmod{81}$

Beispiel (Forts.)

- ▶ $u_2 \equiv x^2 - 5x + 3 \pmod{81}$
- ▶ $w_2 \equiv x^2 + 3x + 1 \pmod{81}$ $b_2 \equiv -9x^2 - 9x \pmod{81}$
 $c_2 \equiv -9x + 9 \pmod{81}$ $d_2 \equiv -27x - 9 \pmod{81}$
- ▶ $s_2 \equiv 28x + 10 \pmod{81}$
- ▶ $t_2 \equiv -28x - 29 \pmod{81}$

$$\begin{aligned}
 e_3 &= a - u_2 w_2 = x^4 - 2x^3 - 11x^2 + 4x + 3 \\
 &\quad - \underbrace{(x^2 - 5x + 3)(x^2 + 3x + 1)} \\
 &= -(x^4 + 3x^3 + x^2 - 5x^3 - 15x^2 - 5x + 3x^2 + 9x + 3) \\
 &\quad + x^4 - 2x^3 - 11x^2 + 4x + 3 \\
 &= 0
 \end{aligned}$$

d.h. Wir erhalten sogar die Faktorisierung in $\mathbb{Z}[x]$, da u_2, w_2 irreduzibel in $\mathbb{Z}[x]$.

Eindeutigkeit des Hensel-Liftings

5.23 Satz

Sei R Ring, $m \in R$ nicht Nullteiler, $l \in \mathbb{N}^+$.

$u, w, u^*, w^*, s, t \in R[x]$ nicht Null mit $su + tw \equiv 1 \pmod{m}$.

Die Hauptkoeffizienten von u und w seien keine Nullteiler mod m , u und u^* (bzw. w und w^*) haben gleiche Hauptkoeffizienten, gleichen Grad und $u \equiv u^* \pmod{m}$ bzw. $w \equiv w^* \pmod{m}$.

Gilt $uw \equiv u^* w^* \pmod{m^l}$, so $u \equiv u^* \pmod{m^l}$ und $w \equiv w^* \pmod{m^l}$.

Beweis: Angenommen $u \not\equiv u^* \pmod{m^l}$ oder $w \not\equiv w^* \pmod{m^l}$. Wähle

$1 \leq i < l$ maximal, so dass $m^i \mid u^* - u$ und $m^i \mid w^* - w$. D. h.

$$u^* - u = gm^i, \quad w^* - w = hm^i$$

$g, h \in R[x]$ und $m \nmid g$ oder $m \nmid h$. **O.b.d.A.** $m \nmid g$

$$\begin{aligned}
 0 &\equiv u^* w^* - uw = u^*(w^* - w) + w(u^* - u) \\
 &= (u^* h + wg)m^i \pmod{m^l}
 \end{aligned}$$

Eindeutigkeit des Hensel-Liftings (Forts.)

- ▶ Da m kein Nullteiler ist, gilt $m \mid m^{l-i} \mid (u^* h + wg)$.

- ▶ Bezeichne mit $\bar{}$ Reduktion mod m : Dann

$$\bar{s}u + \bar{t}w = 1, \quad \bar{u}^* = \bar{u}, \quad \bar{u}^* \bar{h} + \bar{w} \bar{g} = 0 \text{ also}$$

$$0 = \bar{t}(\bar{u}^* \bar{h} + \bar{w} \bar{g}) = \bar{t} \bar{u} \bar{h} + (1 - \bar{s}u) \bar{g}$$

$$= (\bar{t} \bar{h} - \bar{s} \bar{g}) \bar{u} + \bar{g}, \text{ d. h. } \bar{u} \mid \bar{g}$$

- ▶ Wegen $HK(u) = HK(u^*)$ und $\text{grad } u = \text{grad } u^*$ gilt $\text{grad } \bar{g} < \text{grad } \bar{u}$.
 Da $HK(\bar{u}) = HK(u)$ kein Nullteiler ist auch \bar{u} kein Nullteiler und \bar{g} muss 0 Polynom sein. Widerspruch zu $m \nmid g$.

Beispiele (Forts.)

Ende Iter. Nr.	$\sigma(x)$	$\tau(x)$	$u(x)$	$w(x)$	$e(x)$	
5	0	-	-	$x^2 + 2$	$x^2 - 2$	5
5^2	1	-1	1	$x^2 + 7$	$x^2 - 7$	50
5^3	2	-2	2	$x^2 + 57$	$x^2 - 57$	3250
5^4	3	-1	1	$x^2 + 182$	$x^2 - 182$	33125
5^5	4	2	-2	$x^2 - 1068$	$x^2 + 1068$	1140625

- ∞ -Folge Faktoren in $\mathbb{Z}_{5^k}[x]$ Ende von Iteration k gilt stets

$$u(x)w(x) \equiv x^4 + 1 \pmod{5^{k+1}}$$

- Dies gilt sogar für jede Primzahl p .

Schranke für die Anzahl der Iterationen

- Apriori Schranke für die Anzahl der Iterationen:

$$B \geq \max\{|b| : b \text{ Koeffizienten in Polynom } a \text{ oder in jeden möglichen Faktor von } a \text{ mit Grad} \leq \max\{\text{grad}(u^{(1)}), \text{grad}(w^{(1)})\}\}$$

$p^l > 2B$ Schranke für die Anzahl der Iterationen.

Beispiele (Forts.)

5.28 Beispiel 3 Das Leitkoeffizienten Problem

Nicht-monischer Fall:
$$c(x) = \frac{a(x) - u(x)w(x)}{p}$$

- $\sigma(x)u^{(1)}(x) + \tau(x)w^{(1)}(x) \equiv c(x) \pmod{p}$
Eindeutigkeit wird mit $\text{grad } \sigma(x) < \text{grad } (w^{(1)}(x))$ erreicht.

- Updates:
 $u(x) := u(x) + \tau(x)p$ $w(x) := w(x) + \sigma(x)p$
 \rightsquigarrow Hauptkoeffizienten von w wird niemals verändert.
 Im monischen Fall gilt auch $\text{grad } (\tau(x)) < \text{grad } (u^{(1)}(x))$.
 \rightsquigarrow Hauptkoeffizienten von u wird ebenfalls niemals verändert.

i.A. $\text{grad } (c(x)) \leq \text{grad } (a(x)) = \text{grad } (u^{(1)}(x)) + \text{grad } (w^{(1)}(x))$,

d. h. $\text{grad } (\tau(x)) \leq \text{grad } (u^{(1)}(x))$.

Beispiele (Forts.)

- Alle Veränderungen vom Hauptkoeffizienten müssen in u realisiert werden.

$$a(x) = 12x^3 + 10x^2 - 36x + 35 \in \mathbb{Z}[x]$$

$$= u(x)w(x) = (2x + 5)(6x^2 - 10x + 7) \in \mathbb{Z}[x]$$

- $p = 5$ $\Phi_5(a(x)) = 2x^3 - x \in \mathbb{Z}_5[x] = 2(x)(x^2 + 2)$
2 ist Einheit in $\mathbb{Z}_5[x]$.

Wahl der Anfangsfaktoren: 2 zum Faktor x oder
2 zum Faktor $x^2 + 2$

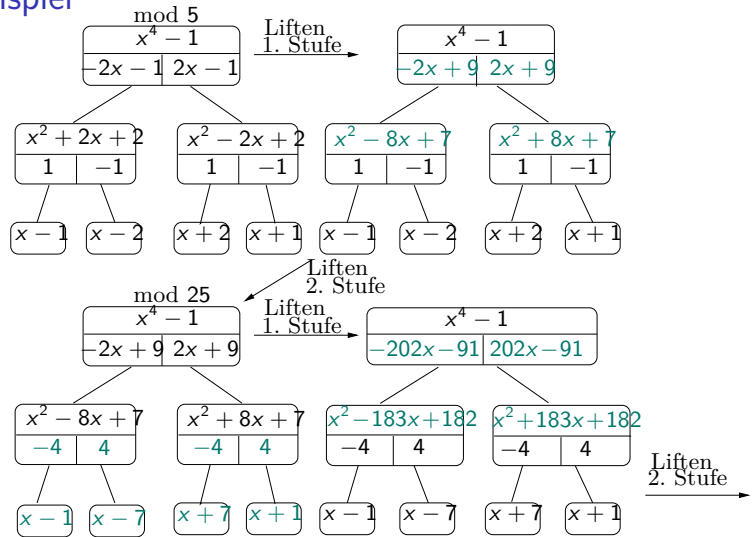
d.h. $\Phi_5(a(x)) = (2x)(x^2 + 2) = (x)(2x^2 - 1) \in \mathbb{Z}_5[x]$

- Die richtigen Faktoren sind
 $u^{(1)}(x) = 2x$ und $w^{(1)}(x) = x^2 + 2$

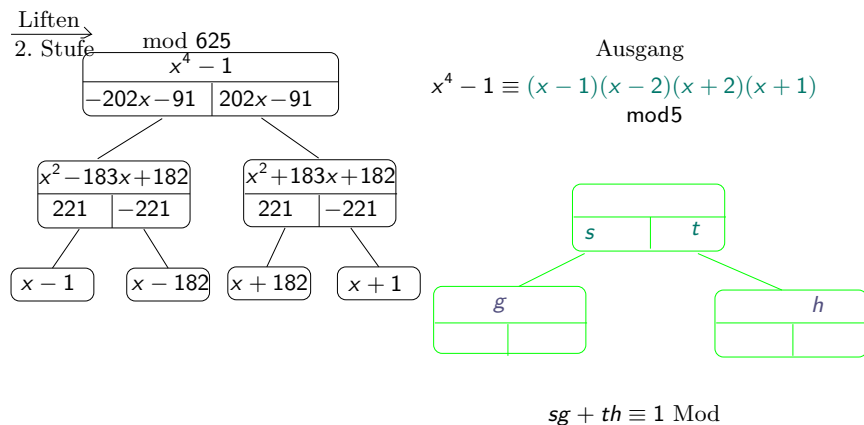
- Hensel's Konstruktion: $s(x) = x$ $t(x) = -2$

$$u(x) = 2x \quad w(x) = x^2 + 2 \quad e(x) = 10x^3 + 10x^2 - 40x + 35 \pmod{5}$$

Beispiel



Beispiel(Forts.)



Faktorisierung in $\mathbb{Z}[x]$ mit quadratischem Hensel Lifting. Der Algorithmus Faktorisierung in $\mathbb{Z}[x]$ nach Zassenhaus

//Eingabe: $f \in \mathbb{Z}[x]$ quadratfrei, primitiv, grad $n \geq 1$ mit $HKoeff(f) > 0$, $\max_norm f = A$.

Ausgabe: Irreduzible Faktoren $\{f_1, \dots, f_k\} \subseteq \mathbb{Z}[x]$ von f //

- 1 if $n = 1$ then return $\{f\}$
 $b := HKoeff(f)$; $B := (n + 1)^{1/2} 2^n A b$;
 $c := (n + 1)^{2n} A^{2n-1}$; $\gamma := \lceil 2 \log_2 c \rceil$;
- 2 repeat wähle Primzahl $p \leq 2\gamma \ln \gamma$, $\bar{f} := f \bmod p$
 until $p \nmid b$ and \bar{f} quadratfrei in $\mathbb{F}_p[x]$
 $l := \lceil \log_p(2B + 1) \rceil$
- 3 {Modulare Faktorisierung}
 Berechne $h_1, \dots, h_r \in \mathbb{Z}[x]$ mit \max_norm höchstens $p/2$ die nicht konstant, monisch und irreduzibel modulo p mit $f \equiv b h_1 \cdots h_r \bmod p$

Algorithmus (Forts.)

- 4 {Hensel Lifting}
 $a := b^{-1} \bmod p$
 Verwende EEA in $\mathbb{F}_p[x]$ um Faktorbaum für f modulo p mit Blätter $h_1 \cdots h_r$ zu bestimmen
 Call MFHL um Faktorisierung $f \equiv b g_1 \cdots g_r \bmod p^l$ mit monischen Polynome $g_1, \dots, g_r \in \mathbb{Z}[x]$ mit \max_norm höchstens $p^l/2$ so dass $g_i \equiv h_i \bmod p$ ($1 \leq i \leq r$) zu berechnen
- 5 {Initialisiere die Indexmenge T der modularen Faktoren, die noch behandelt werden müssen, die Menge G der gefundenen Faktoren, sowie Restpolynom das noch faktorisiert werden muss f^* }
 $T := \{1, \dots, r\}$; $s := 1$; $G := \emptyset$; $f^* := f$;

Algorithmus (Forts.)

```

6 {Faktoren-Kombination}
  while  $2s \leq \#T$  do
7   for all subsets  $S \subseteq T$  of cardinality  $\#S = s$  do
8     Compute  $g^*, h^* \in \mathbb{Z}[x]$  mit  $\max\_norm \leq p^l/2$  und
        $g^* \equiv b \prod_{i \in S} g_i \pmod{p^l}$   $h^* \equiv b \prod_{i \in T \setminus S} g_i \pmod{p^l}$ 
9     if  $\|g^*\|_1 \|h^*\|_1 \leq B$  then
        $T := T \setminus S$ ;  $G := G \cup \{pp(g^*)\}$ ;
        $f^* := pp(h^*)$ ;  $b := \text{HKoeff}(f^*)$ ;
       goto 6;
10     $s := s + 1$ ;
11  return  $G \cup \{f^*\}$ 
    
```

Algorithmus (Forts.)

- Hierbei ist $\|f\|_1 = \sum_{0 \leq i \leq \text{grad } f} |f_i|$, $\|f\|_\infty \leq \|f\|_1 \leq (n+1)\|f\|_\infty$
- $\|g^*\|_1 \|h^*\|_1 \leq B$ gdw. $g^* h^* = bf^*$
 „ \curvearrowright “ Mignotes Schranke (vzG. S. 156).
 „ \curvearrowright “ wegen $g^* h^* \equiv bf^* \pmod{p^l}$.
 $\|g^* h^*\|_\infty \leq \|g^* h^*\|_1 \leq \|g^*\|_1 \|h^*\|_1 \leq B < p^{l/2}$, d. h. | alle Koeff. | $< p^{l/2} \rightsquigarrow$ gleich.

5.33 Satz (Beweis später). Der Algorithmus ist korrekt, Kosten später.

Algorithmus Zassenhaus: Beispiel

5.34 Beispiel $f = 6x^4 + 5x^3 + 15x^2 + 5x + 4 \in \mathbb{Z}[x]$.

Wähle $p = 5, \bar{f} = x^4 - 1$ mit $f \equiv \bar{f} \pmod{5}$.

\bar{f} ist quadratfrei in $\mathbb{Z}_5[x]$. $B := \sqrt{5} \cdot 2^4 \cdot 15 \cdot 6 \approx 3220$,

► $l = \lceil \log_5(2B + 1) \rceil = 6$.

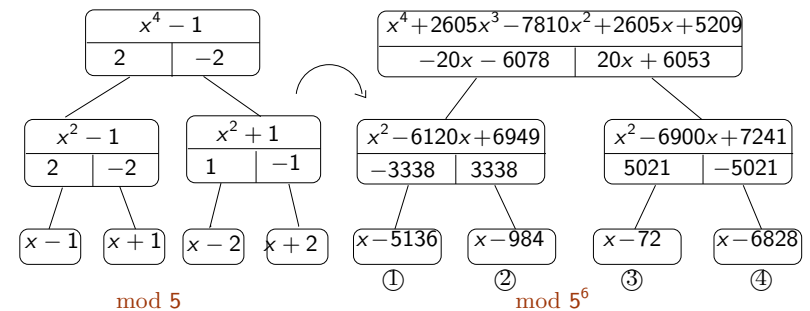
► Schritt 3: modulare Faktorisierung

$$f \equiv bh_1 h_2 h_3 h_4 = 1(x-1)(x+1)(x-2)(x+2) \pmod{5}$$

► Schritt 4: Liften eines Faktorbaumes für $f \pmod{5}$ zu Faktorbaum für f modulo 5^6 ($\pmod{5^6}$ aus Schranke l).

Algorithmus Zassenhaus: Beispiel (Forts.)

Schritt 4:



mod 5

mod 5^6

Algorithmus Zassenhaus: Beispiel (Forts.)

- Teilmengen von $S \subseteq \{1, 2, 3, 4\}$ mit $S = 1$: Keine Faktorisierung.

$$S = \{1, 3\} : g^* \equiv bg_1g_3 = 6(x - 5136)(x - 72)$$

$$\equiv 6x^2 + 2x + 2 \pmod{5^6}$$

$$h^* \equiv bg_2g_4 = 6(x - 984)(x - 6828) \equiv 6x^2 + 3x + 12 \pmod{5^6}$$

$$\|g^*\|_1 \|h\|_1 \leq B, \text{ d. h. } g^*h^* = bf^*$$

- $pp(g^*) = 3x^2 + x + 1$ und $pp(h^*) = 2x^2 + x + 4$ sind die irreduziblen Faktoren von f .

Multivariate Verallgemeinerung von Hensel's Lemma

Problemstellung: Finde $u, w \in \mathbb{Z}[x_1, \dots, x_\nu]$ mit

$$F(u, w) = a(x_1, \dots, x_\nu) - uw = 0$$

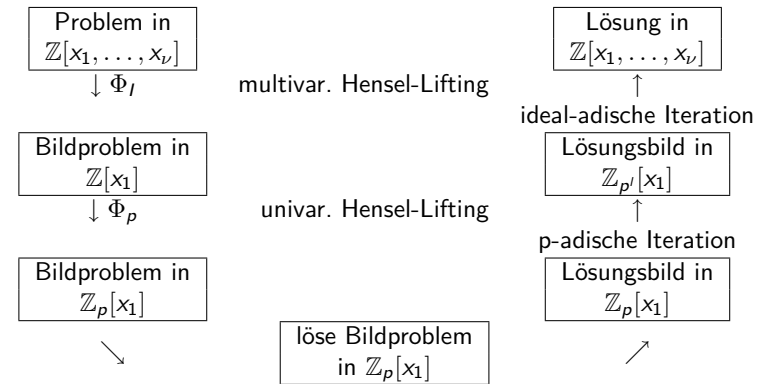
und

$$\begin{aligned} u(x_1, \dots, x_\nu) &\equiv u_0(x_1) \pmod{\langle I, p \rangle} \\ w(x_1, \dots, x_\nu) &\equiv w_0(x_1) \pmod{\langle I, p \rangle} \end{aligned}$$

Bei Geg. u_0, w_0 mit $a \equiv u_0w_0 \pmod{\langle I, p \rangle}$

$$I = \langle x_2 - \alpha_2, \dots, x_\nu - \alpha_\nu \rangle, p \text{ Primzahl.}$$

Homomorphismus Diagramm



Beachte den Unterschied zum Lifting von $F(u) = 0$ via Newton Iteration: Φ_I und Φ_p vertauscht. Bei p-adischer Iteration steht $\mathbb{Z}_{p^l}[x_1]$ und nicht $\mathbb{Z}[x_1]$: Hierbei muss l groß genug gewählt werden. Trennung vom multivariaten und univariaten Fall.

Multivariate Verallgemeinerung von Hensel's Lemma

Die Grundoperation bei der Hensel Iteration zur Lösung von $F(u, w) = a(x_1, \dots, x_\nu) - uw = 0$ ist die Bestimmung der Lösungen einer polynomialen diophantischen Gleichung der Form

$$(*) \quad A^{(k)} \Delta u^{(k)} + B^{(k)} \Delta w^{(k)} = C^{(k)}$$

Für Korrekturterme $\Delta u^{(k)}, \Delta w^{(k)}$ mit $A^{(k)}, B^{(k)}$ und $C^{(k)}$ gegebene Polynome.

- Bei Vertauschung von Φ_I, Φ_p müssten für das l-adische Lifting die Gleichungen in $\mathbb{Z}_p[x_1]$ gelöst werden und für das p-adische Lifting in $\mathbb{Z}_p[x_1, \dots, x_\nu]$.
- Die Lösung von (*) im euklidischen Bereich $\mathbb{Z}_p[x]$ ist einfach, aber in $\mathbb{Z}_p[x_1, \dots, x_\nu]$ schwierig (kein euklidischer Bereich).

Multivariate Hensel Konstruktion

Finde multivariate Polynome

$u(x_1, \dots, x_\nu), w(x_1, \dots, x_\nu) \in \mathbb{Z}_{p^l}[x_1, \dots, x_\nu]$ mit

$$a(x_1, \dots, x_\nu) - uw \equiv 0 \pmod{p^l},$$

so dass

$$\begin{aligned} u(x_1, \dots, x_n) &\equiv u^{(1)}(x_1) \pmod{\langle I, p^l \rangle} \\ w(x_1, \dots, x_n) &\equiv w^{(1)}(x_1) \pmod{\langle I, p^l \rangle} \end{aligned}$$

wobei $u^{(1)}(x_1), w^{(1)}(x_1) \in \mathbb{Z}_{p^l}[x_1]$ gegeben mit

$$a(x_1, \dots, x_\nu) - u^{(1)}(x_1)w^{(1)}(x_1) \equiv 0 \pmod{\langle I, p^l \rangle}$$

$$\begin{aligned} a(x_1, \dots, x_\nu) &\in \mathbb{Z}_{p^l}[x_1, \dots, x_\nu], I \in \mathbb{N}, \\ I &= \langle x_2 - \alpha_2, \dots, x_\nu - \alpha_\nu \rangle. \end{aligned}$$

Multivariate Hensel Konstruktion

Bezeichnet man die gesuchten Lösungen mit \bar{u}, \bar{w} und betrachtet man ihre I-adischen Entwicklungen, so

$$\begin{aligned} \bar{u} &= u^{(1)} + \Delta u^{(1)} + \Delta u^{(2)} + \dots + \Delta u^{(d)} \\ &\text{bzw.} \\ \bar{w} &= w^{(1)} + \Delta w^{(1)} + \Delta w^{(2)} + \dots + \Delta w^{(d)} \end{aligned}$$

wobei d maximaler totaler Grad von Termen in \bar{u} oder \bar{w} , $u^{(1)} = \Phi_I(\bar{u}), w^{(1)} = \Phi_I(\bar{w})$ und $\Delta u^{(k)}, \Delta w^{(k)} \in I^{(k)}$ ($k = 1, 2, \dots, d$).

Multivariate Taylor Darstellung

$$\Delta u^{(k)} = \sum_{i_1=2}^{\nu} \sum_{i_2=i_1}^{\nu} \dots \sum_{i_k=i_{k-1}}^{\nu} u_i(x_1) \prod_{j=1}^k (x_{i_j} - \alpha_{i_j})$$

$$i = (i_1, \dots, i_k) \quad u_i(x_1) \in \mathbb{Z}_{p^l}[x_1].$$

Analog mit $\Delta w^{(k)}$.

Multivariate Taylor Darstellung

Zu lösen ist

$$(*) \quad w^{(k)} \Delta u^{(k)} + u^{(k)} \Delta w^{(k)} \equiv a(x_1 \dots x_\nu) - u^{(k)} w^{(k)} \pmod{\langle I^{k+1}, p^l \rangle}$$

wobei $u^{(k)} w^{(k)}$ die ideal-adische Approximation der Ordnung k sind, d. h.

$$a(x_1, \dots, x_\nu) - u^{(k)} w^{(k)} \in I^k$$

Rechte Seite von (*) hat die Gestalt

$$\sum_{i_2=2}^{\nu} \sum_{i_2=i_1}^{\nu} \dots \sum_{i_k=i_{k-1}}^{\nu} c_i(x_1) \prod_{j=1}^k (x_{i_j} - \alpha_{i_j})$$

für geeignete $c_i(x_1) \in \mathbb{Z}_{p^l}[x_1]$. Ersetzen und Koeffizientenvergleich liefert

$$(**) \quad w^{(k)} u_i(x_1) + u^{(k)} w_i(x_1) \equiv c_i(x_1) \pmod{\langle I, p^l \rangle}$$

Hieraus lassen sich die I-adischen Koeffizienten $u_i(x_1), w_i(x_1) \in \mathbb{Z}_{p^l}[x_1]$ bestimmen.

Multivariate Hensel Konstruktion

Da dies eine Kongruenz mod I ist, kann man Φ_I auf die linke Seite anwenden, d. h. zu lösen ist.

$$w^{(1)}(x_1)u_i(x_1) + u^{(1)}(x_1)w_i(x_1) \equiv c_i(x_1) \pmod{p^l}$$

wobei $u^{(1)}(x_1), w^{(1)}(x_1) \in \mathbb{Z}_{p^l}[x_1]$ die Ausgangspolynome der Lösung sind. Unter den vorgegebenen Bedingungen gilt sogar Eindeutigkeit der Lösungen.

5.36 Satz Multivariate Hensel Konstruktion

Sei p -Primzahl, $I \in \mathbb{N}^+, a(x_1, \dots, x_\nu) \in \mathbb{Z}_{p^l}[x_1, \dots, x_\nu]$,

$I = \langle x_2 - \alpha_2, \dots, x_\nu - \alpha_\nu \rangle, \alpha_2, \dots, \alpha_\nu \in \mathbb{Z}_p,$

$p \nmid \text{HKoeff}(\Phi_I(a(x_1, \dots, x_\nu)))$ und seien $u^{(1)}(x_1), w^{(1)}(x_1) \in \mathbb{Z}_{p^l}[x_1]$ mit

- i) $a(x_1, \dots, x_\nu) \equiv u^{(1)}(x_1)w^{(1)}(x_1) \pmod{\langle I, p^l \rangle}$
- ii) $\Phi_p(u^{(1)}(x_1)), \Phi_p(w^{(1)}(x_1))$ teilerfremd in $\mathbb{Z}_{p^l}[x_1]$.

Satz: Multivariate Hensel Konstruktion

- ▶ Dann gibt es für $k \geq 1$ multivariate Polynome $u^{(k)}, w^{(k)} \in \mathbb{Z}_p[x_1, \dots, x_\nu]/I^k$, so dass

$$a(x_1, \dots, x_\nu) \equiv u^{(k)} w^{(k)} \pmod{\langle I^k, p^l \rangle}$$

und $u^{(k)} \equiv u^{(1)}(x_1) \pmod{\langle I, p^l \rangle}$ $w^{(k)} \equiv w^{(1)}(x_1) \pmod{\langle I, p^l \rangle}$

- ▶ Eindeutigkeit: Falls $a(x_1, \dots, x_\nu)$ monisch bzgl. x_1 , d. h. der Koeffizient in $a(x_1, \dots, x_\nu)$ von $x_1^{d_1}$ ist 1, wobei d_1 der Grad von a in x_1 ist. Werden $u^{(1)}(x_1)$ und $w^{(1)}(x_1)$ monisch gewählt, so sind die Lösungen der diophantischen Gleichungen (***) eindeutig.
- ▶ Probleme bei der Anwendung: Leading Coeff. Problem und Bad Zero Problem. \rightsquigarrow exponentielles Wachstum für Zwischenergebnisse.

Beispiel

5.37 Beispiel Sei $p = 5$ $l = 1$

$$a(x, y, z) = x^2 y^4 z - xy^9 z^2 + xyz^3 + 2x - y^6 z^4 - 2y^5 z$$

$$I = \langle y - 1, z - 1 \rangle \text{ max } x\text{-Grad } 2.$$

$$a(x, y, z) \equiv x^2 + 2x + 2 \pmod{\langle I, 5 \rangle}$$

Es gilt

$$a(x, y, z) \equiv (x - 2)(x - 1) \pmod{\langle I, 5 \rangle}.$$

Wählt man $u^{(1)}(x) = x - 2$, $w^{(1)}(x) = x - 1$, so sind die Bedingungen vom Satz erfüllt.

$a(x, y, z)$ ist nicht monisch aber $w(x, y, z)$ ist monisch und somit liefert Hensel Lifting die richtige Antwort.

Beispiel (Forts.)

Betrachte die l-adische Darstellung von $a(x, y, z)$:

$$a(x, y, z) \equiv (x^2 + 2x + 2) - (x^2 + 1)(y - 1) + (x^2 + x - 1)(z - 1)$$

$$\begin{aligned} &+ (x^2 - x)(y - 1)^2 - (x^2 - 1)(y - 1)(z - 1) + (2x - 1)(z - 1)^2 \\ &- (x^2 - x)(y - 1)^3 + (x^2 - 2x)(y - 1)^2(z - 1) - \\ &- (x + 1)(y - 1)(z - 1)^2 + (x - 1)(z - 1)^3 + (x^2 - x)(y - 1)^4 \\ &+ (-x^2 + 2x)(y - 1)^3(z - 1) - x(y - 1)^2(z - 1)^2 \\ &+ (x - 1)(y - 1)(z - 1)^3 - (z - 1)^2 - (x - 2)(y - 1)^5 \\ &+ (x^2 - 2x)(y - 1)^4(z - 1) + x(y - 1)^3(z - 1)^2 \\ &- (y - 1)(z - 1)^4 + (x - 1)(y - 1)^6 - (2x + 1)(y - 1)^5(z - 1) \\ &- x(y - 1)^4(z - 1)^2 - x(y - 1)^7 + (2x + 1)(y - 1)^6(z - 1) \\ &\dots \\ &\dots \\ &\dots \\ &- (y - 1)^6(z - 1)^4 - x(y - 1)^9(z - 1)^2 \pmod{5} \end{aligned}$$

Hensel Konstruktion für das Beispiel

l-adische Darstellung enthält 38 Terme im Vergleich zu 6 Terme in der l-adischen Darstellung bzgl. $I = \langle y, z \rangle$.

Problem: Anzahl der zu lösenden polynomialen diophantischen Gleichungen ist proportional zur Anzahl der Terme in der l-adischen Darstellung von $a(x, y, z)$.

Die Hensel Konstruktion für dieses Beispiel liefert

$$u^{(7)} = (x - 2) + (-x + 1)(y - 1) + (x - 2)(z - 1) + x(y - 1)^2$$

$$\begin{aligned} &+ (-x - 2)(y - 1)(z - 1) + (-2)(z - 1)^2 + (-x)(y - 1)^3 + \\ &+ x(y - 1)^2(z - 1) + (-2)(y - 1)(z - 1)^2 + (z - 1)^3 \\ &+ (x)(y - 1)^4 + (-x)(y - 1)^3(z - 1) + (1)(y - 1)(z - 1)^3 \\ &+ (x)(y - 1)^4(z - 1) \end{aligned}$$

$$w^{(7)} = (x - 1) + (-1)(z - 1) + (-1)(y - 1)^5 + (-1)(y - 1)^5(x - 1)$$

Hensel Konstruktion für das Beispiel

Ausmultiplizieren mod5 liefert

$$u^{(7)} \equiv xy^4z + yz^3 + 2 \pmod{5} \quad w^{(7)} \equiv x - y^5z \pmod{5}$$

Die Iteration hält hier, da

$$e^{(7)} = a(x, y, z) - u^{(7)}w^{(7)} = 0.$$

Problem: Auswertungspunkt $\neq 0$. Leider kann man nicht immer Auswertungspunkte = 0 wählen, da $p \nmid \text{HKoeff}(\Phi_I(a(x_1, \dots, x_\nu)))$.

Möglichkeit: Variablentransformation

$$x_j \leftarrow x_j + \alpha_j \quad 2 \leq j \leq \nu, \text{ falls } I = \langle x_2 - \alpha_2, \dots, x_\nu - \alpha_\nu \rangle$$

Problem der Zwischenergebnisse bleibt erhalten.

Möglichkeit (Forts.)

- ▶ Möglichkeiten zur einfacheren Berechnung siehe G.C.L 262 → dünn besetzte MV Polynome.

$$c_I(x_1) = \frac{1}{n_1! \dots n_m!} \Phi_I \left(\left(\frac{\partial}{\partial x_{j-1}} \right)^{n_1} \dots \left(\frac{\partial}{\partial x_{j_m}} \right)^{n_m} e^{(k)} \right)$$

- ▶ Wang EEZ-GCD Algorithmus: Variablenweise

$$\mathbb{Z}_p[x_1] \rightarrow \mathbb{Z}_p[x_1, x_2] \rightarrow \mathbb{Z}_p[x_1, x_2, x_3] \dots$$

Inhalt Kapitel 6

Anwendungen modularer und p-adischer Methoden

- GCD Berechnungen
- Faktorisierung
- Quadratfreie Faktorisierung
- Getrennte Grad Faktorisierung-Distinct Degree Factorization
- Equal-Degree Factorization (Gleiche-Grad-Faktorisierung)-Algorithmus von Cantor und Zassenhaus
- Anwendung: Nullstellen-Bestimmung
- Faktorisierungsalgorithmen, die auf linearer Algebra basieren
- Anwendung: Irreduzible Polynome: Test und Konstruktion
- Faktorisierung in $\mathbf{R}[x_1, \dots, x_n]$, \mathbf{R} ZPE Ring
- Faktorisierung in $K[x]$ für K algebraischer Zahlkörper

GCD Berechnung - Faktorisierung

GCD (GGT)-Berechnungen

- ▶ klassisch EEA (euklid. Ringe) Z.B. $F[x]$ $O(M(n) \log n)$ Körperoperationen.
- ▶ (Pseudo-) Polynomiale Restfolgen, reduzierte PRS (primitiver EA $\mathbb{Z}[x_1, \dots, x_\nu]$) (kleiner Grad ≤ 2) Problem Koeffizientenwachstum
- ▶ Sylvester Matrix und Subresultanten
- ▶ Modularer Algorithmus (Brown) **Big-Prime, Small-Primes**
- ▶ p-adisch EZGCD (Moses u. Yun)
- ▶ EEZ-GCD (Wang).
- ▶ GCD-Heuristic

Faktorisierung (Forts.)

Insbesondere für Faktorisierung in $\mathbb{Q}[x]$ bzw. $\mathbb{Z}[x]$:

Ist $a \in \mathbb{Z}[x]$ primitiv $\rightsquigarrow a = f_1 \dots f_k$ in irreduziblem $f_i \in \mathbb{Q}[x]$ liefert Faktorisierung $a = f_1^* \dots f_k^*$ mit $f_i^* \in \mathbb{Z}[x]$ irreduzibel.
(Durch Multiplikation mit Nennern und Entfernung von Inhalt).

$a \in \mathbb{Z}[x]$ beliebig. Faktorisierung von a ist Faktorisierung vom Inhalt von a (als Element von \mathbb{Z}) + Faktorisierung von $pp(a)$, d. h.

Faktorisierung in $\mathbb{Z}[x] \rightsquigarrow$ Faktorisierung in $\mathbb{Q}[x]$ plus Faktorisierung in \mathbb{Z} .

Quadratfreie Faktorisierung

Reduktion des Faktorisierungsproblems auf Faktorisierung von Polynomen ohne Mehrfachfaktoren.

6.1 Definition Sei R ZPE-Ring, $a(x) \in R[x]$ primitives Polynom. $a(x)$ heißt **quadratfrei**, falls $a(x)$ ohne Mehrfachfaktoren, d. h. es gibt kein $b(x)$, $\text{grad}(b) \geq 1$, $b(x)^2 | a(x)$.
Die **quadratfreie Faktorisierung** von $a(x)$ ist

$$a(x) = \prod_{i=1}^k a_i(x)^i \quad (\text{genauer: die Folge der } a_i(x))$$

wobei für jedes i $a_i(x)$ quadratfreies Polynom und

$$\text{GGT}(a_i(x), a_j(x)) = 1 \text{ für } i \neq j$$

Beachte: Einige der a_i in der QFF von a können 1 sein.

Quadratfreie Faktorisierung

6.2 Beispiel

Sei $a(x) = (x^2 + 1)(x^2 - 1)(x^3 + 3x)^5$. Hierbei sind $a_2(x) = a_3(x) = 1$.

Beachte ebenfalls, dass die a_i nicht faktorisiert sein müssen.

QFF($a(x)$) = $(x^2 + 1, 1, 1, x^2 - 1, x^3 + 3x)$.
(Folge der **Quadratfreienfaktoren** von $a(x)$).

Quadratfreiheit wird über die Ableitung bestimmt.

Sei $a = \sum_{i=0}^n a_i x^i$, dann ist die **Ableitung** von a :

$$a'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1}$$

hierbei ist $n = \underbrace{1 + 1 + \dots + 1}_{n\text{-mal}}$.

Es gelten die üblichen Ableitungsregeln!

Charakterisierung der Quadratfreiheit

6.3 Lemma Sei $a(x)$ primitiv in $R[x]$. R ZPE-Ring mit Charakteristik 0 (d. h. $\underbrace{1 + \dots + 1}_{n} \neq 0$ für alle $n \geq 1$).

Sei $c(x) = \text{GGT}(a(x), a'(x))$, dann hat a mehrfache Faktoren gdw $c(x) \neq 1$. Also $a(x)$ quadratfrei gdw $c(x) = 1$.

Beweis: \Leftarrow : Sei $a(x) = b(x)^2 w(x)$, $\text{grad } b \geq 1$
 $\rightsquigarrow a'(x) = 2b(x)b'(x)w(x) + b(x)^2 w'(x) = b(x)\hat{w}(x) \rightsquigarrow c(x) \neq 1$.

\Leftarrow : Angenommen $c(x) \neq 1$, aber $a(x)$ quadratfrei.

$a(x) = p_1(x)p_2(x) \dots p_k(x)$, $p_i(x)$ irreduzibel.

$\text{grad}(p_i(x)) \geq 1$, $\text{GGT}(p_i(x), p_j(x)) = 1$ für $i \neq j$. Dann

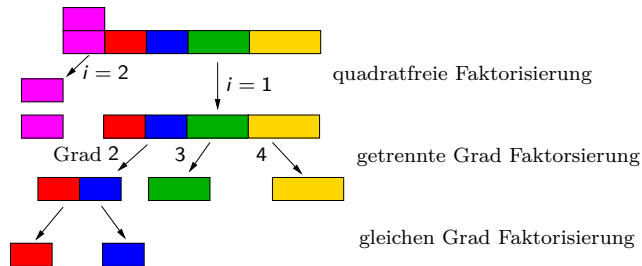
$$a'(x) = p_1'(x)p_2(x) \dots p_k(x) + \dots + p_1(x) \dots p_{k-1}(x)p_k'(x)$$

Angenommen $p_i(x) | c(x)$ (Es gibt mindestens ein solches i .)

O.B.d.A. $i = 1$ $p_1(x) | a'(x) \rightsquigarrow p_1(x) | p_1'(x)p_2(x) \dots p_k(x) \rightsquigarrow p_1(x) | p_1'(x)$
geht nur, wenn $p_1'(x) = 0$. Char 0 $\rightsquigarrow p_1(x)$ konstant. ζ

Distinct Degree Factorization

Spaltung der irreduziblen Faktoren nach Grad:
Getrennte Grad Faktorisierung



$a(x) \in \mathbb{F}_q[x]$, $q = p^m$, quadratfrei.
Gesucht Faktorisierung von $a(x)$ der Form $a(x) = \prod a_i(x)$ wobei a_i
Produkt der irreduziblen Faktoren von $a(x)$ mit Grad i , d. h.
 $\text{grad}(a_i) = k \cdot i :: k$ Faktoren mit Grad i .

Satz von Fermat: Folgerungen

Erinnerung: Kleiner Fermatscher Satz: $0 \neq a \in \mathbb{F}_q$, so $a^{q-1} = 1$ und
 $a^q = a$ alle $a \in \mathbb{F}_q$, d. h. $x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$ in $\mathbb{F}_q[x]$.

Allgemeiner

6.12 Lemma Für $d \geq 1$ ist $x^{q^d} - x \in \mathbb{F}_q[x]$ Produkt aller monischen
irreduziblen Polynome in $\mathbb{F}_q[x]$, deren Grad d teilt.

Kleiner Fermat angewendet auf \mathbb{F}_{q^d} zeigt $h = x^{q^d} - x$ ist Produkt aller
 $x - a$ mit $a \in \mathbb{F}_{q^d}$.

Falls $g^2 \mid h$ (in \mathbb{F}_q) mit $g \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$, so teilt ein $x - a$ auch g und
somit $(x - a)^2 \mid h$.

Dies geht nicht, d. h. $x^{q^d} - x$ ist quadratfrei
(einfacher GGT(h, h') = 1).

Satz von Fermat: Folgerungen

Es genügt zu zeigen: Für $f \in \mathbb{F}_q[x]$, monisch, irreduzibel mit
 $\text{Grad}(f) = n$:

$$f \mid x^{q^d} - x \quad \text{gdw} \quad n \mid d$$

Sei f irreduzibel, monisch, $n \mid d$, $d = n \cdot s$.

Betrachte $F = \mathbb{F}_q[x]/\langle f \rangle$ ist Körper mit q^n Elementen.

Kleiner Fermat liefert für $a \in F$

$$a^{q^n} = a \text{ und somit } a^{q^d} = \underbrace{((a^{q^n})^{q^n} \dots)^{q^n}}_{s\text{-mal}} = a$$

Betrachte $a = [x]$ Repräsentant von x in F .

$[h] = [x^{q^d} - x] = [x]^{q^d} - [x] = a^{q^d} - a = 0$ in F , d. h. $h \equiv 0 \pmod{f}$, und
somit $f \mid h$.

Satz von Fermat: Folgerungen

Umgekehrt sei f monisch, irreduzibel $\text{grad}(f) = n$, $f \mid x^{q^d} - x$.

Betrachte die Körpererweiterung $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$.

Da $f \mid x^{q^d} - x$ folgt aus kleinen Fermat angewendet mit \mathbb{F}_{q^d} , dass es
 $A \subseteq \mathbb{F}_{q^d}$ gibt mit $f = \prod_{a \in A} (x - a)$.

Wähle $a \in A$ und sei $\mathbb{F}_q[x]/\langle f \rangle \cong \mathbb{F}_q(a) \subseteq \mathbb{F}_{q^d}$, wobei $\mathbb{F}_q(a)$ kleinster
Teilkörper von \mathbb{F}_{q^d} , der a enthält.

Dieser Körper hat q^n Elemente und \mathbb{F}_{q^d} ist eine Erweiterung von $\mathbb{F}_q(a)$,
d. h. $q^d = (q^n)^s$ für ein s also $n \mid d$.

Getrennte Grad Faktorisierung (Forts.)

Anwendung: Sei $a(x) = \prod a_i(x)$. Um das Produkt aller linearen irreduziblen Faktoren von $a(x)$ zu bestimmen, genügt es

$$a_1(x) = \text{GGT}(a(x), x^q - x)$$

zu berechnen.

Setzt man $a(x) = a(x)/a_1(x)$, so hat a keine linearen irreduziblen Faktoren, d. h.

$$a_2(x) = \text{GGT}(a(x), x^{q^2} - x)$$

Usw. Hat $a(x)$ Grad n , so muss man nur Faktoren bis zum Grad $n/2$ bestimmen.

6.13 Beispiel 1 $a = x(x+1)(x^2+1)(x^2+x+2) \in \mathbb{F}_3[x]$ getrennte GF

$$(x^2+x, \quad x^4+x^3+x+2)$$

\uparrow \uparrow
 Grad1 Grad2

$$\text{GGT}(a, x^3 - x) = x^2 + x, \quad \text{GGT}(a/x^2 + x, x^9 - x) = x^4 + x^3 + x + 2$$

Beispiel (Forts.)

2) $a(x) = x^{63} + 1 \in \mathbb{F}_2[x]$, dann

$$a_1(x) = \text{GGT}(a(x), x^2 - x) = x + 1 \quad \text{1-Faktor Grad 1}$$

$$a(x) = a(x)/a_1(x) = \frac{x^{63}+1}{x+1} = x^{62} + x^{61} + \dots + x^2 + x + 1$$

$$a_2(x) = \text{GGT}(a(x), x^4 - x) = x^2 + x + 1 \quad \text{1-Faktor Grad 2}$$

$$a(x) = a(x)/a_2(x) = x^{60} + x^{57} + x^{54} + \dots + x^6 + x^3 + 1$$

$$a_3(x) = \text{GGT}(a(x), x^8 - x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

2-Faktoren Grad 3

$$a(x) = x^{54} + x^{53} + x^{51} + x^{50} + x^{48} + x^{46} + x^{45} + x^{42} + x^{33} + x^{30} + x^{29} + x^{27} + x^{25} + x^{24} + x^{22} + x^{21} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1$$

$$\text{GGT}(a(x), x^{16} - x) = 1, \quad \text{GGT}(a(x), x^{32} - 1) = 1,$$

$$\text{GGT}(a(x), x^{64} - x) = a(x) = a_6(x)$$

$$x^{63} + 1 = (x+1)(x^2+x+1)(x^6+x^5+x^4+x^3+x^2+x+1) a_6(x)$$

Grad 1 2 3 – 2Fakt 6 – 9Fakt

Algorithmus Getrennte Grad Faktorisierung

procedure PARTIALFACTOR-DD($a(x), q$)

{Eingabe: Quadratfreies mon. Polynom $a(x) \in \mathbb{F}_q[x]$, $n = \text{grad}(a) > 0$ }

{Ausgabe: Getrennte Grad Zerlegung $(a_1, \dots, a_s), s \leq n/2$ von $a(x)$ }

(1) $w := x; a_0 := 1; i := 0;$

(2) **repeat**

$i := i + 1$; call wied. quadrat. Algorithm. in $R = \mathbb{F}_q(x)/\langle a(x) \rangle$

(3) um $w = w^q \text{ mod } a(x)$ zu berechnen

(4) $a_i := \text{GGT}(w - x, a(x));$

if $a_i(x) \neq 1$ **then**

$a(x) := a(x)/a_i(x); w(x) := w(x) \text{ mod } a(x);$

until $a(x) = 1;$

return (a_1, \dots, a_i)

Die GGT-Berechnungen $\text{GGT}(a(x), x^{q^i} - x)$ werden durch Berechnung von $x^{q^i} - x$ modulo $a(x)$, d. h. Berechnung wird in $\mathbb{F}_q[x]/(a(x))$ durchgeführt (z. B. wiederholtes Quadrieren um $(x^{q^{i-1}})^q \text{ mod } (a(x))$ zu berechnen).

Algorithmus Getrennte Grad Faktorisierung (Forts.)

6.14 Satz Algorithmus Getrennte Grad Faktorisierung ist korrekt, d. h. es wird die getrennte Grad-Zerlegung von a berechnet.

Aufwand: $O(sM(n) \log(nq))$ Operationen in \mathbb{F}_q , wobei s der größte Grad eines irreduziblen Faktors von a ist.

z.Z. Für i -ten Durchgang gilt:

$$w_i \equiv x^{q^i} \text{ mod } f_i, \quad f_i = G_{i+1} \cdots G_t, \quad a_i = G_i \text{ für } i \geq 1,$$

wobei (G_1, \dots, G_t) die getrennte Grad-Zerlegung von a ist.

Induktion nach i : $i = 0$ klar, $i > 0$ wegen

$$w_i \equiv w_{i-1}^q \equiv (x^{q^{i-1}})^q = x^{q^i} \text{ mod } f_{i-1} \text{ d. h. } w_i - x \equiv x^{q^i} - x \text{ mod } f_i \text{ und}$$

$$a_i = \text{GGT}(w_i - x, f_{i-1}) = \text{GGT}(x^{q^i} - x, f_{i-1})$$

Also ist a_i Produkt aller monisch irreduziblen Polynome in $\mathbb{F}_q[x]$ deren Grad i teilt und $f_{i-1} = G_i \cdots G_t$ teilen, d. h. $a_i = G_i$ und somit $f_i = G_i \cdots G_t / G_i = G_{i+1} \cdots G_t$. $i = t$ beim Ausgang.

Algorithmus Getrennte Grad Faktorisierung (Forts.)

Kosten für die Berechnung von w_i in Schritt (2)
 $0(\log q)$ Multiplikationen mod a , d. h. $0(M(n) \log q)$ Operationen in \mathbb{F}_q .

Die Kosten in (3) und (4) sind ebenfalls $0(M(n) \log n)$ Operationen in $\mathbb{F}_q[x]$.

Berechnung kann gestoppt werden sobald $\text{grad } f_i = \text{grad } a(x) < 2(i + 1)$, da alle irreduziblen Faktoren von f_i grad mindestens $i + 1$ haben, d. h. $a(x)$ ist irreduzibel. Mit dieser Überprüfung: **early abort**

Somit $i = \max\{m_1/2, m_2\} \leq n/2$, wobei m_1 und m_2 die Grade des größten und zweitgrößten irreduziblen Faktors von $a(x)$ sind.

Beachte in Schritt 2 w_i wird nur mod f_{i-1} benötigt.

Beispiel

6.15 Beispiel Sei $q = 3$ Algorithmenverlauf für

$$a(x) = x^8 + x^7 - x^6 + x^5 - x^3 - x^2 - x \in \mathbb{F}_3[x]$$

$$a'(x) = -x^7 + x^6 - x^4 + x - 1 \quad \text{GGT}(a, a') = 1, \text{ d. h. QF}$$

$$w_1 = x^3 \text{ mod } a = x^3$$

$$a_1 = \text{GGT}(x^3 - x, a) = x \neq 1$$

$$f_1 = a/a_1 = x^7 + x^6 - x^5 + x^4 - x^2 - x - 1 \text{ (neues } a)$$

$$w_1 \text{ unverändert } x^3$$

$$w_2 = w_1^3 \text{ mod } a = x^9 \text{ mod } a = -x^7 + x^6 + x^5 + x^4 - x$$

$$a_2 = \text{GGT}(w_2 - x, f_1) = \text{GGT}(-x^7 + x^6 + x^5 + x^4 + x, f_1)$$

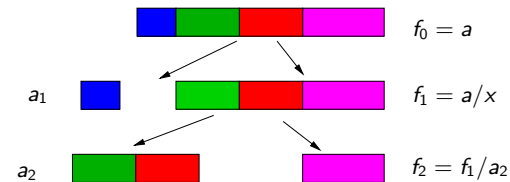
$$= x^4 + x^3 + x - 1$$

$$f_2 = f_1/a_2 = a/a_2 = \frac{x^7 + x^6 - x^5 + x^4 - x^2 - x - 1}{x^4 + x^3 + x - 1}$$

$$= x^3 - x + 1$$

Beispiel (Forts.)

Der Algorithmus würde noch eine Iteration durchführen aber $\text{grad}(f_2) < 2(2 + 1) = 6 \rightsquigarrow$ nicht notwendig, da f_2 irreduzibel. a hat einen Lin-Faktor x , zwei verschiedene irreduziblen quadratische Faktoren, da $\text{Grad } a_2 = 4$ und einen irreduziblen kubischen Faktor $x^3 - x + 1$.



Equal-Degree Factorization (Gleiche-Grad-Faktorisierung)

Der Algorithmus von Cantor und Zassenhaus

Faktorisiere die a_i , die aus der Getrennte-Grad-Faktorisierung berechnet werden.

Ungerade Primzahlpotenzen, Char 2 Fall getrennt.

6.16 Beispiel $a(x) = x^{15} - 1 \in \mathbb{F}_{11}[x]$. DDF liefert

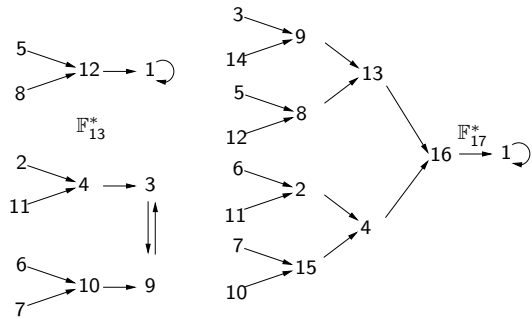
$$a(x) = a_1(x)a_2(x) = (x^5 - 1)(x^{10} + x^5 + 1)$$

a hat 5 lineare Faktoren, 5 irreduzible quadratische Faktoren.

Probabilistische Verfahren um Faktoren zu finden.

Gleiche-Grad-Faktorisierung (1)

Betrachte Quadrat-Abbildung $\sigma : \mathbb{F}_q^* \rightarrow \mathbb{F}_q^*$ mit $\sigma(a) = a^2$, z. B.



Jedes Element hat entweder zwei oder 0 eingehende Pfeile.

Zwei bedeutet ist Quadrat

gleiche Anzahl

0 bedeutet ist kein Quadrat

Gleiche-Grad-Faktorisierung (2)

6.17 Lemma Sei q Primzahlpotenz, $k \mid q - 1$.

$S = \{b^k : b \in \mathbb{F}_q^*\}$ die Menge der k -ten Potenzen in \mathbb{F}_q^* . Dann gilt

i) S ist eine Untergruppe der Ordnung $(q - 1)/k$

ii) $S = \{a \in \mathbb{F}_q^* : a^{(q-1)/k} = 1\}$

Beweis: S als Bild eines Homomorphismus ($\sigma_k : a \rightarrow a^k$) ist Untergruppe von \mathbb{F}_q^* .

Der Kern von σ_k ist $\ker \sigma_k = \{a \in \mathbb{F}_q^* : \sigma_k(a) = 1\} = \{a \in \mathbb{F}_q^* : a^k = 1\}$

d.h die Menge der k -ten EW. Da \mathbb{F}_q Körper ist hat $x^k - 1 \in \mathbb{F}_q[x]$

höchstens k Wurzeln in $\mathbb{F}_q[x]$, d. h. $|\ker \sigma_k| \leq k$.

Wegen $(b^k)^{(q-1)/k} = b^{q-1} = 1$ für $b \in \mathbb{F}_q^*$ (Fermat), gilt

$S \subseteq \ker \sigma_{(q-1)/k}$, d. h. $|S| \leq (q - 1)/k$.

Also

$q - 1 = |\mathbb{F}_q^*| = |\ker \sigma_k| \cdot |\text{Bild } \sigma_k| = |\ker \sigma_k| \cdot |S| \leq k(q - 1)/k = q - 1 \rightsquigarrow$

$|\ker \sigma_k| = k \quad |S| = (q - 1)/k$ und $S = \ker \sigma_{(q-1)/k}$

Gleiche-Grad-Faktorisierung (3)

Wendet man das Lemma 6.17 mit $k = 2$ und $k = (q - 1)/2$ an, so gilt

6.18 Lemma Sei q ungerade Primzahlpotenz und $S = \{a \in \mathbb{F}_q^* : \exists b \in \mathbb{F}_q^* \ a = b^2\}$ Menge der Quadrate. Dann

i) $S \subseteq \mathbb{F}_q^*$ ist multiplikative Ugr. der Ordnung $(q - 1)/2$

ii) $S = \{a \in \mathbb{F}_q^* \ a^{(q-1)/2} = 1\}$

iii) $a^{(q-1)/2} \in \{1, -1\}$ für alle $a \in \mathbb{F}_q^*$

Faktorisierungsaufgabe: Sei $a \in \mathbb{F}_q[x]$, $\text{grad } a = n$, monisch und $d \in \mathbb{N}^+$

mit $d \mid n$ und jeder irreduzible Faktor von a habe den Grad d .

Dann gibt es $r = n/d$ solcher Faktoren und $a = f_1 \cdots f_r$, f_i verschiedene

monische irreduziblen in $\mathbb{F}_q[x]$ o.B.d.A. $r \geq 2$. Bestimme die f_i .

Gleiche-Grad-Faktorisierung (4)

Da $\text{GGT}(f_i, f_j) = 1$ für $i \neq j$, gibt es nach chinesischem Restesatz Ring Homomorphismus

$\chi : R = \mathbb{F}_q[x]/\langle a \rangle \rightarrow \mathbb{F}_q[x]/\langle f_1 \rangle \times \cdots \times \mathbb{F}_q[x]/\langle f_r \rangle = R_1 \times \cdots \times R_r$

Die R_i sind Körper mit q^d Elemente und algebraische Erweiterungen vom Grad d von \mathbb{F}_q , d. h. alle isomorph.

$$\mathbb{F}_{q^d} \cong R_i = \mathbb{F}_q[x]/\langle f_i \rangle \supseteq \mathbb{F}_q$$

Für $f \in \mathbb{F}_q[x]$. Sei $f \text{ mod } a \in R$ und

$\chi(f \text{ mod } a) = (f \text{ mod } f_1, \dots, f \text{ mod } f_r) = (\chi_1(f), \dots, \chi_r(f))$, wobei

$\chi_i(f) = f \text{ mod } f_i \in R_i$ gilt.

Es gilt für $f \in \mathbb{F}_q[x]$, $i \leq r$, $f_i \mid f$ gdw $\chi_i(f) = 0$.

Hat man ein $f \in \mathbb{F}_q[x]$ mit einigen $\chi_i(f) = 0$ und anderen nicht null, so ist $\text{GGT}(f, a)$ ein nichttrivialer Teiler von a .

\rightsquigarrow Probabilistisches Verfahren um Spaltungspolynom f von a zu bestimmen.

Gleiche-Grad-Faktorisierung (5)

Sei q ungerade. Setze $e = (q^d - 1)/2$.

Für alle $\beta \in R_i^* = \mathbb{F}_{q^d}^*$ gilt $\beta^e \in \{1, -1\}$ und beide Möglichkeiten treten gleich oft vor (Lemma 6.18 mit q^d an Stelle von q).

Wählt man $f \in \mathbb{F}_q[x]$ mit $\text{Grad } f < n$ und $\text{GGT}(a, f) = 1$ zufällig, so sind $\chi_1(f), \dots, \chi_r(f)$ unabhängige uniform verteilte Elemente aus $\mathbb{F}_{q^d}^*$ und $\varepsilon_i = \chi_i(f^e) \in R_i$ ist 1 oder -1 . Jedes mit Wahrscheinlichkeit $1/2$.

Somit

$$\chi(f^e - 1) = (\varepsilon_1 - 1, \dots, \varepsilon_r - 1)$$

und $f^e - 1$ ist Spaltungspolynom, es sei denn $\varepsilon_1 = \dots = \varepsilon_r$.

Dieses kann mit Wahrscheinlichkeit $2(1/2)^r = 2^{-r+1} \leq 1/2$ vorkommen.

Beispiel

6.19 Beispiel Fortsetzung:: In $\mathbb{F}_{11}[x]$

$$a(x) = (x^5 - 1)(x^{10} + x^5 + 1) = a_1 a_2$$

5 lineare Faktoren, 5 quadratische Faktoren.

$$n = 5 \quad d = 1 \quad e = (11^1 - 1)/2 = 5 \quad a_1 = x^5 - 1$$

Zufallspolynom: $x + 4$

$$\text{GGT}(a_1, (x + 4)^5 - 1) = x^2 + 5x + 5$$

$$(x^5 - 1) = (x^2 + 5x + 5)(x^3 - 5x^2 - 2x + 2)$$

Zufallspolynom: $x + 8$

$$\text{GGT}(x^2 + 5x + 5, (x + 8)^5 - 1) = x - 1 \text{ mit}$$

$$x^2 + 5x + 5 = (x - 1)(x - 5) \text{ 2 lineare Faktoren.}$$

$$\text{GGT}(x^3 - 5x^2 - 2x + 2, (x + 8)^5 - 1) = x - 4, \text{ wobei}$$

$$x^3 - 5x^2 - 2x + 2 = (x - 4)(x^2 - x + 5).$$

Man erhält $a_1(x) = (x - 1)(x - 3)(x - 4)(x - 5)(x + 2)$.

Beispiel (Forts.)

Spaltung von $a_2(x)$ nach Zufallsmuster $e = (11^2 - 1)/2 = 60$

Zufallspolynom: $x + 2$

$$\text{GGT}(a_2(x), (x + 2)^{60} - 1) = x^6 + 3x^5 + 4x^4 - 2x^3 + 5x^2 + 4x - 2$$

$$a_2(x) = (x^6 + 3x^5 + 4x^4 - 2x^3 + 5x^2 + 4x - 2)(x^4 - 3x^3 + 5x^2 - x + 5)$$

Versuche mit $x + 7$

$$\text{GGT}(x^4 - 3x^3 + 5x^2 - x + 5, (x + 7)^{60} - 1) = x^2 + 3x - 2 \text{ und}$$

$$\text{GGT}(x^6 + 3x^5 + 4x^4 - 2x^3 + 5x^2 + 4x - 2, (x + 7)^{60} - 1) = x^4 + 2x^3 + x^2 - 5x - 2$$

3-Faktoren Grad 2, verwende $x^4 + 2x^3 + x^2 - 5x - 2$

$$(x^2 + 3x - 2)(x^2 + 5x + 3)(x^2 + 4x + 5)(x^2 - 2x + 4)(x^2 + x + 1) = a_2(x).$$

Algorithmus: Gleiche-Grad-Faktorisierung

procedure Equal_Degree_Splitting ($a(x), d, q = p^m$)

{**Eingabe:** QF monisches Polynom $a \in \mathbb{F}_q[x]$, $\text{grad } a = n$, $q = p^m$, p ungerade, $d < n$, $d \mid n$, alle irreduzibeln Faktoren von a mit Grad d }

{**Ausgabe:** Ein echter monischer Faktor $g \in \mathbb{F}_q[x]$ von a oder „Failure“}

begin

1 Wähle $f \in \mathbb{F}_q[x]$ mit $\text{grad } f < n$ zufällig

if $f \in \mathbb{F}_q$ **then return** „Failure“

2 $g_1 := \text{GGT}(a, f)$

if $g_1 \neq 1$ **then return** g_1

3 Call repeated squaring algorithm in $\mathbb{F}_q[x]/\langle a(x) \rangle$

 um $b = f^{(q^d - 1)/2} \text{ mod } a(x)$ zu berechnen

4 $g_2 := \text{GGT}(b - 1, a)$

if $g_2 \neq 1$ and $g_2 \neq a$ **then return** g_2

else return „Failure“

end.

Algorithmus (Forts.)

6.20 Satz Der Algorithmus ist korrekt bzgl. seiner Spezifikation.
 „Failure“ wird mit der Wahrscheinlichkeit $< 2^{1-r} \leq 1/2$ mit $r = n/d \geq 2$ ausgegeben.

Die Anzahl der erwarteten Operationen in \mathbb{F}_q ist $O((d \log q + \log n)M(n))$.

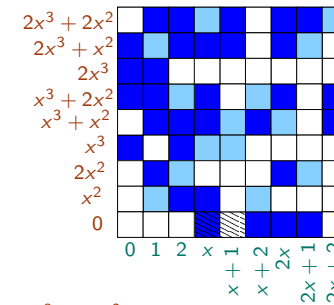
Beweis:

- Für $\text{GGT}(a, f) = 1$, so 2^{-r+1} als Fehlerwahrscheinlichkeit, wegen Schritt (2): $< 2^{-r+1}$.
- Kosten für die Schritte 2) und 4) $O(M(n) \log n)$.
- Schritt 3: $2 \log_2(q^d) \in O(d \log q)$ Multiplikationen mod a , d. h. $O(M(n)d \log q)$ Operationen in \mathbb{F}_q .
- Ruft man den Algorithmus k mal auf, so gilt **Failure Wahrscheinlichkeit** $< 2^{(1-r)k} \leq 2^{-k}$.

Algorithmus: Beispiel in $\mathbb{F}_3[x]$

- $a(x) = x^8 + x^7 - x^6 + x^5 - x^3 - x^2 - x$ hat einen linearen Faktor: x , zwei irreduzible Faktoren Grad 2: $x^4 + x^3 + x - 1$ $d = 2$, einen irreduziblen Faktor Grad 3: $x^3 - x + 1$
- $a(x) = x^4 + x^3 + x - 1$ faktorisiert sich in $r = 2$ irreduziblen Polynome mit Grad $d = 4/r = 2$.
- Angenommen $f = x + 1$ erste Wahl. Dann ist
 $g_1 = \text{GGT}(f, a) = \text{GGT}(x + 1, x^4 + x^3 + x - 1) = 1$
 $b = (x + 1)^4 \text{ mod } a = (x + 1)^4 \text{ mod } x^4 + x^3 + x - 1 = -1$
 $g_2 = \text{GGT}(b - 1, a) = \text{GGT}(1, a) = 1$ **Pech gehabt!**
- Zweite Wahl: $f = x$. Dann
 $g_1 = \text{GGT}(f, a) = \text{GGT}(x, x^4 + x^3 + x - 1) = 1$
 $b = x^4 \text{ mod } a = -x^3 - x + 1$
 $g_2 = \text{GGT}(b - 1, a) = \text{GGT}(-x^3 - x, x^4 + x^3 + x^2 - 1) = x^2 + 1 \rightsquigarrow$
- $x^2 + 1$ ist einer der irr. Faktoren und $a/g_2 = x^2 + x + 1$ der andere.

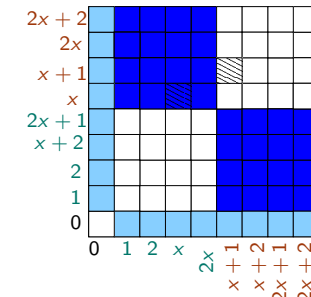
Algorithmus (Forts.)



$$a_3x^3 + a_2x^2 + a_1x + a_0$$

$$R = \mathbb{F}_3[x]/(a)$$

$$a_i \in \mathbb{F}_3$$



$$R \cong \mathbb{F}_3[x]/(x^2 + 1) \times \mathbb{F}_3[x]/x^2 + x - 1$$

$$\mathbb{F}_9 \times \mathbb{F}_9$$

Will man alle r -Faktoren bestimmen, so rekursive Anwendung auf die einzelnen Spaltungs-Faktoren.

Algorithmus Gleiche_Grad_Faktorisierung

procedure Equal_Degree_Fact ($a(x), d, q$)

{Eingabe: QF monisches Polynom $a \in \mathbb{F}_q[x]$, p ungerade,
 $\{q = p^m, \text{grad } a = n, d \mid n \text{ alle irreduziblen Faktoren grad } d\}$
 {Ausgabe: die monischen irreduziblen Faktoren von a in $\mathbb{F}_q[x]$ }

- begin**
- if** $n = d$ **then return** a
- call Equal_Degree_Splitting($a(x), d, q$) bis ein echter Faktor $g \in \mathbb{F}_q[x]$ von a gefunden.
 FAC \leftarrow Equal_Degree_Fact(g, d, q) \cup Equal_Degree_Fact($a/g, d, q$)
return (FAC)
end.

Algorithmus Gleiche_Grad_Faktorisierung (Forts.)

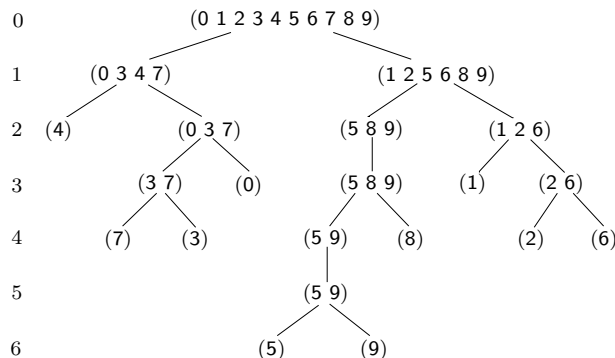
6.21 Satz Ein QF-Polynom vom Grad $n = r \cdot d$ mit r irreduziblen Faktoren vom Grad d kann vollständig durch diesen Algorithmus faktorisiert werden mit einer erwarteten Anzahl von Operationen in \mathbb{F}_q von $O((d \log q + \log n)M(n) \log r)$.

Die Arbeitsweise der Prozedur kann mit Hilfe eines markierten Baums beschrieben werden. Die Marken der Knoten sind Faktoren von a .

- ▶ a Marke der Wurzel.
- ▶ Die Blätter sind markiert mit den irreduziblen Faktoren von a .
- ▶ Falls in Schritt 2 Failure, so ist ein Sohn mit gleicher Marke, sonst sind 2 Söhne mit Marken g bzw. a/g .

Algorithmus Gleiche_Grad_Faktorisierung (Forts.)

6.22 Beispiel $a = f_0 \dots f_9 \in \mathbb{F}_q[x]$, f_i mon. irr. paarweise verschieden.



Algorithmus Gleiche_Grad_Faktorisierung (Forts.)

- ▶ Produkt der Marken in einer Stufe ist Teiler von a , d. h. Grad vom Produkt höchstens n .
- ▶ Kosten für Knoten vom Grad m ist $O((d \log q + \log m)M(n))$ Operationen in \mathbb{F}_q , Subadditivität vom $M \rightsquigarrow$ Kosten für jede Stufe: $O((d \log q + \log n)M(n))$ Operationen.
- ▶ Erwartete Tiefe ist $O(\log r)$ ($r \leq n \rightsquigarrow$ Behauptung).
- ▶ **Tiefenschranke: Beweis** Im Algorithmus Equal_Degree_Splitting ist die Wahrscheinlichkeit, dass $f \bmod f_i$ und $f \bmod f_j$ weder beide Quadrate, noch beide nicht Quadrate, mindestens $1/2$. (Chin-RS)
- ▶ Die Wahrscheinlichkeit, dass f_i und f_j in Stufe k durch einen Aufruf von EDS getrennt werden (falls sie noch nicht getrennt sind) ist somit mindestens $1/2$. Also ist die Wahrscheinlichkeit, dass f_i und f_j in Stufe k noch nicht getrennt sind höchstens $(1/2)^k$ und dies gilt für jedes Paar irreduzibler Faktoren von a .

Algorithmus Gleiche_Grad_Faktorisierung (Forts.)

- ▶ Es gibt $(r^2 - r)/2 < r^2$ solcher Paare.
- ▶ Die Wahrscheinlichkeit p_k , dass nicht alle irreduziblen Faktoren in Tiefe k getrennt sind, ist höchstens $r^2 2^{-k}$.
 Diese ist die Wahrscheinlichkeit, dass der Baum die Tiefe $> k$ hat und $p_{k-1} - p_k$ ist die Wahrscheinlichkeit der Baumtiefe genau k .

▶ Sei $s = \lceil 2 \log_2 r \rceil$, dann ist die erwartete Baumtiefe

$$\sum_{k \geq 1} k(p_{k-1} - p_k) = \sum_{k \geq 0} p_k = \sum_{0 \leq k < s} p_k + \sum_{s \leq k} p_k \leq \sum_{0 \leq k < s} 1 + \sum_{s \leq k} r^2 2^{-k} = s + r^2 2^{-s} \sum_{k \geq 0} 2^{-k} \leq s + 2 \in O(\log r).$$

- ▶ Beispiel: Tiefe $6 < \lceil 2 \log_2 10 \rceil + 2 = 9$.
- ▶ Für Varianten siehe vzG,G Übung 14.7.

Fall Charakteristik 2

Für Char= 2 Varianten der Algorithmen: Verwende **m-tes Spur-Polynom** über \mathbb{F}_2

$$T_m = x^{2^{m-1}} + x^{2^{m-2}} + \dots + x^4 + x^2 + x \in \mathbb{F}_2[x]$$

Angenommen $q = 2^k$ für ein $k \in \mathbb{N}^+$, $f \in \mathbb{F}_q[x]$ quadratfrei, grad $f = n$, mit $r \geq 2$ irreduziblen Faktoren $f_1, \dots, f_r \in \mathbb{F}_q[x]$
 $R = \mathbb{F}_q[x]/\langle f \rangle$ $R_i = \mathbb{F}_q[x]/\langle f_i \rangle$ $\chi_i : R \rightarrow R_i$ wie gehabt.

- i) $x^{2^m} + x = T_m(T_m + 1) \rightsquigarrow T_m(\alpha) \in \mathbb{F}_2$ für $\alpha \in \mathbb{F}_{2^m}$ (T_m ist \mathbb{F}_2 linear)
 $T_m(\alpha) = 0$ und $T_m(\alpha) = 1$ gleichwahrscheinlich $1/2$
- ii) Angenommen alle irreduziblen Faktoren von f haben den grad d , dann ist $\chi_i(T_{kd}(\alpha)) \in \mathbb{F}_2$ für $\alpha \in R$, somit für $\alpha \in R$ zufällig \rightsquigarrow
 $T_{kd}(\alpha) \in \mathbb{F}_2$ mit Wahrscheinlichkeit $2^{1-r} \leq 1/2$.
- iii) Berechne $b = T_{kd}(f)$ mod a im Algorithmus Equal_Degree_Splitting.

Eigenschaften

Die **wesentlichen Eigenschaften**, die verwendet wurden, sind folgende Faktorisierungen:

- ▶ Für q ungerade:

$$* \quad x^q - x = x(x^{(q-1)/2} - 1)(x^{(q-1)/2} + 1)$$

d. h. für $W = \{v(x) \in \mathbb{F}_q[x] : v(x)^q = v(x) \text{ mod } a(x)\}$ und $v(x) \in W$ ist $v(x)(v(x)^{(q-1)/2} - 1)(v(x)^{(q-1)/2} + 1) = v(x)^q - v(x) \equiv 0 \text{ mod } a(x)$ und die nichttrivialen gemeinsamen Faktoren von $v(x)^q - v(x)$ verteilen sich auf die drei Polynome.

- ▶ Für q gerade, d. h. $q = 2^k$, gilt * nicht, aber

$$** \quad x^{2^k} + x = T_k(x)(T_k(x) + 1)$$

\rightsquigarrow Wahrscheinlichkeit $\text{GGT}\left(\overset{T_{kd}(f)}{\rightsquigarrow}, a\right)$ nicht trivial $\geq 1/2$
 $(f^{(q-1)/2} - 1, a)$

Vollständiger Faktorisierungsalgorithmus für endliche Körper

Eingabe: Polynom $a(x) \in \mathbb{F}_q[x]$, $a \notin \mathbb{F}_q$, $q = p^m$, p Primzahl.

Ausgabe: Die monischen irreduziblen Faktoren von a mit ihren Vielfachheiten.

Monisch \rightsquigarrow QFF-Faktorisierung \rightsquigarrow DD-Faktorisierung \rightsquigarrow ED-Faktorisierung.

Aufwand für grad $a = n$: Erwartete Anzahl von OP in \mathbb{F}_q
 $O(nM(n) \log(qn))$, d. h. polynomial in n und $\log q$.

$n^2 + n \log q$ Operationen in \mathbb{F}_q (mit Frobenius Aut.) siehe vz G/G. Auch für Variante ohne QFF-Faktorisierung zu verwenden (S. 365). Frobenius Automorphismus: $\sigma : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$, $a \rightarrow a^q$, es gilt $\sigma^n = id$ und kann als Automorphismus von $R = \mathbb{F}_q[x]/\langle f \rangle$ für f quadratfrei betrachtet werden \rightsquigarrow Iterated Frobenius (Siehe S.374).

Anwendung: Nullstellen-Bestimmung

Problem: Bestimme Nullstellen von $a(x) \in \mathbb{F}_q[x]$.
 Es genügt die **linearen irreduziblen Faktoren** von $a(x)$ zu berechnen, d. h. $\text{GGT}(x^q - x, a(x)) = g$ und dann ED-Faktorisierung anzuwenden.

procedure Root_Finding ($a(x), q$)

{**Eingabe:** nichtkonstantes Polynom $a(x) \in \mathbb{F}_q[x]$, $q = p^m$.}

{**Ausgabe:** Die Nullstellen von $a(x)$ in \mathbb{F}_q .}

- 1 call Repeated Squaring Algorithmus in $R = \mathbb{F}_q[x]/\langle a(x) \rangle$ zur Berechnung von $x^q \text{ mod } a(x) =: h$
- 2 $g := \text{GGT}(h - x, a)$
if $g = 1$ **then** return \emptyset
else
- 3 call Equal_Degree Fact($g, 1, q$)
 // es werden die irreduziblen linearen Faktoren $x - u_1, \dots, x - u_r$ mit $r = \text{grad } g$ berechnet//
- 4 **return** u_1, \dots, u_r

Faktorisierungsalgorithmen, die auf linearer Algebra basieren

Die Algorithmen von Berlekamp 1967/1970.

Erste Faktorisierungsalgorithmen für Polynome über endliche Körper, die **pol. Laufzeiten** hatten.

Anstelle der Getrennte-Grad Faktorisierung werden Methoden der linearen Algebra verwendet um das Polynom zu spalten.

- ▶ Sei $a(x) \in \mathbb{F}_q[x]$ quadratfrei, monisch grad $n > 0$.
- ▶ $R = \mathbb{F}_q[x]/\langle a \rangle$ ist Vektorraum der Dimension n über \mathbb{F}_q (sogar eine \mathbb{F}_q -Algebra).
- ▶ Die Abbildung $\beta = \sigma - id : R \rightarrow R$ mit $\beta(f) = f^q - f$ ist \mathbb{F}_q -linear.
- ▶ Wie bestimmt man den Kern von β :

Grundlagen für Berlekamps Algorithmen

- ▶ Ist $a = f_1 \cdots f_r$ die Faktorisierung von a in verschiedenen monischen irreduziblen Polynome aus $\mathbb{F}_q[x]$, so gilt nach chinesischem Restsatz

$$R \cong \mathbb{F}_q[x]/\langle f_1 \rangle \times \cdots \times \mathbb{F}_q[x]/\langle f_r \rangle$$

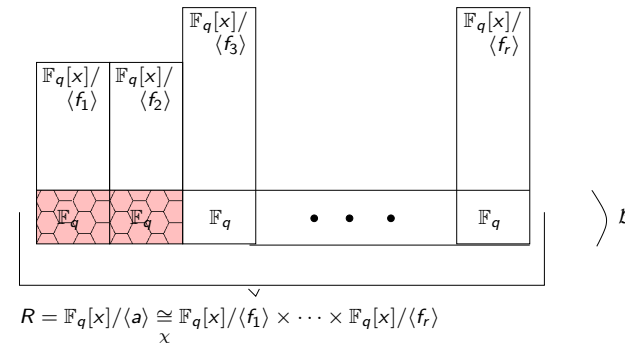
- ▶ Die $\mathbb{F}_q[x]/\langle f_i \rangle$ sind Körper mit $q^{\text{grad } f_i}$ Elementen und enthalten \mathbb{F}_q (Konstanten mod f_i).

- ▶ Für $f \in \mathbb{F}_q[x]$ gilt
 - $f \bmod a \in \ker \beta \iff f^q \equiv f \bmod a$
 - $\iff f^q \equiv f \bmod f_i \quad \text{für } 1 \leq i \leq r$
 - $\iff f \bmod f_i \in \mathbb{F}_q \quad \text{für } 1 \leq i \leq r$

Nach kleinem Fermat (alle Nullstellen von $x^q - x$ liegen in \mathbb{F}_q , da $x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$ in $\mathbb{F}_q[x]$).

Grundlagen für Berlekamps Algorithmen

Also ist $\mathcal{B} = \text{Kern } \beta$ der Unterraum, der $\mathbb{F}_q \times \cdots \times \mathbb{F}_q = \mathbb{F}_q^r$ entspricht.



Grundlagen für Berlekamps Algorithmen

- ▶ \mathcal{B} ist sogar eine \mathbb{F}_q -Unteralgebra von R : Die **Berlekamp-Unteralgebra**.

- ▶ d.h. $f \bmod a \in \mathcal{B} \iff \chi(f \bmod a) = (a_1 \bmod f_1, \dots, a_r \bmod f_r)$ für Konstanten $a_1, \dots, a_r \in \mathbb{F}_q$.

- ▶ Die Matrix $Q \in \mathbb{F}_q^{n \times n}$, die den **Frobenius-Hom.** $\sigma : f \rightarrow f^q$ bezüglich der **Basis** $x^{n-1} \bmod a, \dots, x \bmod a, 1 \bmod a$ von R darstellt, heißt **Petr-Berlekamp-Matrix von a**. $x^{qj} \equiv q_{j,0} + q_{j,1}x + \cdots + q_{j,n-1}x^{n-1}$

Der Berlekamp Faktorisierungsalgorithmus basiert nun auf folgenden Berechnungen:

- ▶ Bestimme zunächst eine Basis $b_1 \bmod a, \dots, b_r \bmod a$ von \mathcal{B} durch **Gauss-Elimination** angewendet auf $Q - I$.

- ▶ Beachte: a ist irreduzibel $\iff r = 1 \iff \text{Rang}(Q - I) = n - 1$. r gibt somit die **Anzahl der irreduziblen Faktoren** von $a(x)$ an.

Berlekamp Faktorisierungsalgorithmus

- ▶ Angenommen q sei **ungerade** und sei $b = c_1 b_1 + \dots + c_r b_r$ eine zufällige Linearkombination der Basiselemente mit $c_1, \dots, c_r \in \mathbb{F}_q$ unabhängig gewählt, d. h. $b \bmod a$ ist ein zufälliges Element aus \mathcal{B} .
- ▶ Wende $(q-1)/2$ Trick, wie bei ED-Faktorisierung, an: Die $b \bmod f_i$ sind gleichmäßig zufällig verteilte Elemente von \mathbb{F}_q für $1 \leq i \leq r$. Falls keines der f_i b teilt, so ist $b^{(q-1)/2} \equiv \pm 1 \pmod{f_i}$ und beide Möglichkeiten treten mit Wahrscheinlichkeit $1/2$ auf, unabhängig für alle i (Lemma 6.18).

▶ **Beachte:** Falls b nicht konstant ist, so gilt $a(x) = \prod_{s \in \mathbb{F}_q} \text{GGT}(b-s, a(x))$

$$\text{Da } x^q - x = \prod_{s \in \mathbb{F}_q} (x - s), \text{ d.h. } b^q - b = \prod_{s \in \mathbb{F}_q} (b - s)$$

$$\text{und } f_i \mid a \text{ für alle } i \rightsquigarrow f_i \mid b^q - b = \prod_{s \in \mathbb{F}_q} (b - s)$$

Berlekamp Faktorisierungsalgorithmus (Forts.)

- ▶ Für $s \neq t$ gilt aber $\text{GGT}(b-s, b-t) = 1$, d. h. für gegebenes i gilt $f_i \mid b - s_k$ für genau ein s_k , d. h.

$$a = \text{GGT}(b^q - b, a) = \text{GGT}\left(\prod_{s \in \mathbb{F}_q} (b - s), a\right) = \prod_{s \in \mathbb{F}_q} \text{GGT}(b - s, a)$$

- ▶ Berechnung von Q :

$$\begin{aligned} x^q \bmod a(x), \quad x^{2q} \bmod a(x), \dots, x^{(n-1)q} \bmod a(x) \\ a(x) &= a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + x^n \\ x^m &\equiv r_{m,0} + r_{m,1} x + \dots + r_{m,n-1} x^{n-1} \bmod a(x) \\ x^{m+1} &\equiv -r_{m,n-1} a_0 + (r_{m,0} - r_{m,n-1} a_1) x + \dots \\ &\quad + (r_{m,n-2} - r_{m,n-1} a_{n-1}) x^{n-1} \\ &\equiv r_{m+1,0} + r_{m+1,1} x + \dots + r_{m+1,n-1} x^{n-1} \end{aligned}$$

- ▶ $r_{m+1,0} = -r_{m,n-1} a_0$
 $r_{m+1,i} = r_{m,i-1} - r_{m,n-1} a_i \quad i = 1, \dots, n-1 \rightsquigarrow O(qn^2)$ Körperoperationen.

Berlekamp-Algorithmus: Ein echter Faktor

{Eingabe: Monisches QF-Polynom $a \in \mathbb{F}_q[x]$, $\text{grad}(a) = n$, q ungerade PZP}
 {Ausgabe: Entweder echter faktor g von a oder Failure, d.h. Las-Vegas Typ PA}

- 1 Call repeated squaring Algorithm in $\mathbb{F}_q[x]/\langle a \rangle$ zur Berechnung von $x^q \bmod a$;
- 2 **for** $0 \leq i < n$ berechne $x^{qi} \bmod a = \sum_{0 \leq j < n} q_{ij} x^j \quad Q := (q_{ij})_{0 \leq i, j < n}$;
 //siehe auch Bemerkung zur Berechnung von Q //
- 3 Wende Gausselimination auf $Q - I \in \mathbb{F}_q^{n \times n}$ an um die Dimension und eine Basis $b_1 \bmod a, \dots, b_r \bmod a$ der Berlekamp Algebra \mathcal{B} zu bestimmen, hierbei sind $b_1, \dots, b_r \in \mathbb{F}_q[x]$ mit Graden $< n$
if $r = 1$ **then return** a ;
- 4 Wähle unabhängige zufällige $c_1, \dots, c_r \in \mathbb{F}_q \quad b := c_1 b_1 + \dots + c_r b_r$;
- 5 $g_1 := \text{GGT}(b, a)$; **if** $g_1 \neq 1$ **then return** g_1 ;
- 6 Call repeated squaring algorithm in $R = \mathbb{F}_q[x]/a$ zur Berechnung von $f := b^{(q-1)/2} \bmod a$;
- 7 $g_2 := \text{GGT}(f-1, a)$; **if** $g_2 \neq 1$ **and** $g_2 \neq a$ **then return** g_2
else return „Failure“

Berlekamp-Algorithmus: Ein echter Faktor

6.25 Satz Der Algorithmus ist korrekt und Failure kommt mit Wahrscheinlichkeit $\leq 1/2$ vor. Er benötigt $O(n^3 + M(n) \log q)$ Operationen in \mathbb{F}_q .

Beweis: Korrektheit: Falls $g_1 \neq 1$, so echter Teiler. Falls $g_2 \neq 1$ und $g_2 \neq a$, so ebenfalls echter Teiler. Falls $g_1 = 1$ in Schritt 5, so ist g_2 trivial (d. h. 1 oder a). In Schritt 7 gdw $f^{(q-1)/2} \equiv 1 \pmod{f_i}$ für alle i . Diese Fälle kommen mit der Wahrscheinlichkeit 2^{-1} vor. Die Erfolgswahrscheinlichkeit ist mindestens $1 - 2 \cdot 2^{-r} \geq 1/2$. Da $r \geq 2$ ist. Die Kosten für Schritt 1 sind $O(M(n) \log q)$ Körper Operationen. Schritt 2 verwendet $n-2$ Multiplikationen mod a , d. h. $O(nM(n))$ Operationen in \mathbb{F}_q . Kosten für Schritt 3 $O(n^3)$ dominiert die Kosten von 2, die $O(nr)$ Körper für Schritt 4 und die $O(M(n) \log n)$ Operationen der GGT Berechnungen in den Schritten 5 und 7. 6 benötigt $O(M(n) \log q)$ Körperoperationen.

Faktorisierungsalgorithmus

Für eine vollständige Faktorisierung von $a(x)$ wird die Basis von B nur einmal berechnet, der Spaltungsprozess der Schritte 4-7 wird rekursiv auf g und a/g angewandt. Alle irreduziblen Faktoren mit erwarteten Operationenzahl von $O(n^3 + M(n) \log r \log q)$.

Viele Varianten + Verbesserungen des Berlekamp Algorithmus in der Literatur. Problem für q groß: Die Kosten für die Erzeugung von Q und die Berechnung der GGT's wird durch $O(qkn^2)$ dominiert. Somit nur brauchbar für kleine q 's. Etwa Polynom mit 4 Faktoren mit grad $n = 100$ über \mathbb{F}_{314} benötigt 191 Milliarden Körperoperationen. Generiere Matrix durch binäres Potenzieren. Variante von Zassenhaus (siehe Geddes et al S 360).

Kaltofen und Lobo: Minimalpolynom-Berechnung.

$O(M(n^2) \log n + M(n) \log q)$.

Dies ist wichtig, falls $\log q$ klein im Vergleich zu n ist.

Variante, Big Prime Berlekamp Algorithm siehe Geddes et.al

Beispiel

6.26 Beispiel

$$a(x) = x^6 - 3x^5 + x^4 - 3x^3 - x^2 - 3x + 1 \in \mathbb{Z}_{11}[x] = \mathbb{F}_{11}[x]$$

Q Matrix 6×6 , $x^{q^j} \equiv q_{j,0} + q_{j,1}x + \dots + q_{j,5}x^5 \pmod{a}$.

Zeile 0 von Q $(1, 0, 0, 0, 0, 0)$, $1 \equiv 1 \pmod{a(x)}$

$$\begin{aligned} x &\equiv x \pmod{a(x)} \\ x^2 &\equiv x^2 \pmod{a(x)} \\ x^3 &\equiv x^3 \pmod{a(x)} \\ x^4 &\equiv x^4 \pmod{a(x)} \\ x^5 &\equiv x^5 \pmod{a(x)} \\ x^6 &\equiv 3x^5 - x^4 + 3x^3 + x^2 + 3x - 1 \pmod{a(x)} \\ x^7 &\equiv 3x^6 - x^5 + 3x^4 + x^3 + 3x^2 - x \\ &\equiv -3x^5 - x^3 - 5x^2 - 3x - 3 \pmod{a(x)} \\ &\vdots \\ x^{11} &\equiv 5x^5 - 5x^4 - 3x^3 - 3x^2 + 5x + 3 \pmod{a(x)} \end{aligned}$$

Beispiel (Forts.)

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 5 & -3 & -3 & -5 & 5 \\ 3 & -5 & -5 & 1 & -1 & 0 \\ -2 & 4 & -1 & 3 & -4 & -2 \\ -4 & -3 & -1 & 0 & 0 & -3 \\ -3 & -1 & -4 & -3 & -1 & -3 \end{bmatrix}$$

Basis für $Q - I$, bringe in Δ -Form 0,1 in diagonalen, falls 1 einzige 1 in Zeile dreiecks-idempotenter Form.

$$Q - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 4 & -3 & -3 & -5 & 5 \\ 3 & -5 & 5 & 1 & -1 & 0 \\ -2 & 4 & -1 & 2 & -4 & -2 \\ -4 & -3 & -1 & 0 & -1 & -3 \\ -3 & -1 & -4 & -3 & -1 & -4 \end{bmatrix}$$

Beispiel (Forts.)

$$\rightsquigarrow L = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & -1 & 0 & 0 \\ 0 & 0 & 4 & 2 & 0 & 0 \end{bmatrix}$$

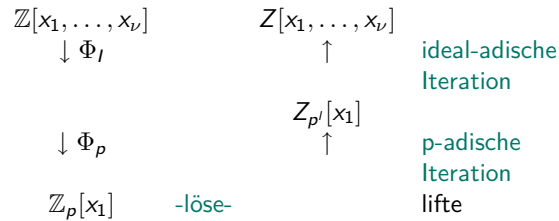
Δ idemp-Form, Rang 3

$$I - L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & -4 & -2 & 0 & 1 \end{bmatrix}$$

Basis für Nullraum ablesen, da $(I - L)L = 0$

Multivariate Polynomfaktorisierung in $\mathbb{Q}[x_1, \dots, x_\nu]$ bzw. $\mathbb{Z}[x_1, \dots, x_\nu]$

- Siehe Homomorphismus-Diagramm Fol. 303



- Problem Liste der korrekten multivariaten Leit-Koeffizienten.
 $a(x_1, \dots, x_\nu) \in \mathbb{Z}[x_1, \dots, x_\nu]$ x_1 als Hauptvariable.
 $a(x_1, \dots, x_\nu) \equiv u_1(x_1) \cdots u_n(x_1) \pmod{\Phi_I}$
- Leitkoeffizienten von $a(x_1, \dots, x_\nu)$ (als Polynome in x_1) ist multivariates Polynom in Variablen x_2, \dots, x_ν .

Multivariate Polynomfaktorisierung... (Forts.)

Leitkoeffizienten Problem tritt auch hier auf, die Leitkoeffizienten der Faktoren müssen korrekt gewählt werden.
 (Normierungstrick: korrekte Koeffizienten auf alle Faktoren verteilen).
 Wang's Lösung

$$a(x_1, \dots, x_\nu) = a_d(x_2, \dots, x_\nu)x_1^d + \dots$$

- Faktorisiere $a_d(x_2, \dots, x_\nu)$ (rekursiver Aufruf).
 Verteile die Faktoren von $a_d(x_2, \dots, x_\nu)$ auf die $u_1(x_1), \dots, u_n(x_1)$.
 Geeignete Wahl von Φ_I . Auswertungspunkte: $\alpha_2, \dots, \alpha_\nu \in \mathbb{Z}$ mit
 - $a_d(\alpha_2, \dots, \alpha_\nu) \neq 0$.
 - $a(x_1, \alpha_2, \dots, \alpha_\nu)$ quadratfrei.
 - Jeder Faktor von $a_d(x_2, \dots, x_\nu)$ wenn ausgewertet in $\alpha_2, \dots, \alpha_\nu$ hat Primzahlfaktor, der nicht in den anderen Auswertungen der restlichen Faktoren vorkommt.

Faktorisierung in $K[x]$ für K algebraischer Zahlkörper

Anwendung: Symbolische Integration

Trager (Kronecker).

Algebraische Zahlkörpern, algebraische Erweiterungen von F , d. h. $F(\alpha) = F[x]/\langle m(x) \rangle$, m irreduzibles Polynom in $F[x]$.
 α ist „Wurzel“ von $m(x)$ mit Grad n (z. B. $x^2 + 1$ in $\mathbb{Q}[x]$ oder $\mathbb{R}[x]$)

$$F(\alpha) = \{f_0 + f_1\alpha + \dots + f_{n-1}\alpha^{n-1} : f_i \in F\}$$

6.33 Beispiel $F = \mathbb{Q}$, $\alpha = \sqrt{2}$, $m(x) = x^2 - 2$, dann

$$\mathbb{Q}[x]/\langle x^2 - 2 \rangle \simeq \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \text{ mit}$$

$$\begin{aligned}
 (a + b\sqrt{2}) + (a' + b'\sqrt{2}) &= (a + a') + (b + b')\sqrt{2} \\
 (a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) &= (aa' + 2bb') + (ab' + ba')\sqrt{2}
 \end{aligned}$$

Grundlagen: Konjugation

- Sei $m(x)$ eindeutiges monisches Minimalpolynom von α über F .
 Die Konjugierten von α über F sind die restlichen verschiedenen Nullstellen von $m(x)$. Seien diese $\alpha_2, \dots, \alpha_n$
 z.B. $-\sqrt{2}$ ist konjugiert zu $\sqrt{2}$ über \mathbb{Q} .
- Sei $\beta \in F(\alpha)$ mit $\beta = f_0 + f_1\alpha + \dots + f_{n-1}\alpha^{n-1}$.
 Die Konjugierten von β sind β_2, \dots, β_n , wobei

$$\beta_i = f_0 + f_1\alpha_i + \dots + f_{n-1}\alpha_i^{n-1}$$

- Konjugation induziert Isomorphismen:

$$\sigma_i : F(\alpha) \rightarrow F(\alpha_i) \text{ mit } \sigma_i(\beta) = \beta_i$$

Grundlagen (Forts.)

- ▶ Beachte: $p(\alpha, z) \mid \text{Norm}(p)$ in $F(\alpha)[z]$.
- ▶ Die Norm-Funktion ist **multiplikativ**, d. h. $\text{Norm}(pq) = \text{Norm}(p)\text{Norm}(q)$ d.h. Jedes Polynom p welches in $F(\alpha)[z]$ in Faktoren zerfällt, liefert eine Faktorisierung von $\text{Norm}(p)$ in $F[z]$
- ▶ Trager's Algorithmus basiert auf einer Umkehrung dieser Eigenschaft. Prozedur:
Faktoriere $\text{Norm}(p)$ in $F[z]$ und lifte diese Faktoren von $F[z]$ zu Faktoren von $p(z)$ in $F(\alpha)[z]$.
- ▶ Benötigt wir noch **Irreduzibilitätstest** in $F(\alpha)[z]$.

Irreduzibilitätstest für $a(z) \in F(\alpha)[z]$

6.37 Satz Sei $a(z) \in F(\alpha)[z]$ **irreduzibel** über $F(\alpha)$.
 Dann ist $\text{Norm}(a)$ **Potenz eines irreduziblen Polynoms über F** .

Beweis: Angenommen $\text{Norm}(a) = b(z)c(z)$ mit teilerfremde Polynome $b, c \in F[z]$. Da $a(z) \mid \text{Norm}(a)$ in $F(\alpha)[z]$ und $a(z)$ irreduzibel ist, gilt

- ▶ $a(z) \mid b(z)$ oder $a(z) \mid c(z)$ in $F(\alpha)[z]$.
- ▶ o.b.d.A. $a(z) \mid b(z)$: d.h. $b(z) = a(z)d(z)$ mit $d(z) \in F(\alpha)[z]$ und teilerfremd zu $a(z)$ da irreduzibel.
- ▶ Konjugation liefert $b(z) = \sigma_i(a(z))\sigma_i(d(z))$,
 d. h. $\sigma_i(a(z))$ ist **Faktor von $b(z)$ für alle i** . Dann aber
- ▶ $\text{Norm}(a) = \prod_i \sigma_i(a) \mid b(z)$ also $c(z) = 1$. d.h. $\text{Norm}(a) = b(z)$ und $b(z)$ ist entweder irreduzibel oder Potenz eines irreduziblen Elements.

Folgerung

Satz 6.37 hat als Folgerung:
 Angenommen $a(z) \in F(\alpha)[z]$ habe die Eigenschaft, dass

- ▶ **$\text{Norm}(a)$ quadratfrei in $F[z]$** . Dann
 - ▶ $a(z)$ irreduzibel gdw $\text{Norm}(a)$ irreduzibel.
 - ▶ Falls $a(z)$ in $F(\alpha)[z]$ sich faktorisieren lässt als $a(z) = a_1(z) \cdots a_k(z)$ mit $a_i(z)$ irreduzibel, so ist $\text{Norm}(a) = \text{Norm}(a_1)\text{Norm}(a_2) \cdots \text{Norm}(a_k)$, wobei jedes $\text{Norm}(a_i)$ irreduzibel ist.
- ▶ Wenn $\text{Norm}(a)$ **quadratfrei** ist, muss $\text{Norm}(a_i) \neq \text{Norm}(a_j)$ für $i \neq j$ gelten. d.h.:
 Es gibt eine **eindeutige Korrespondenz** zwischen den Faktoren von $a(z)$ über $F(\alpha)$ und den Faktoren von $\text{Norm}(a)$ über F .

Umkehrung

6.38 Satz Sei $a(z) \in F(\alpha)[z]$, $\text{Norm}(a)$ quadratfrei. Ist $p_1(z), \dots, p_k(z)$ eine vollständige Faktorisierung von $\text{Norm}(a)$ über $F[z]$, so ist

$$a(z) = \prod_{i=1}^k \text{GGT}(a(z), p_i(z))$$

eine vollständige Faktorisierung von $a(z)$ über $F(\alpha)[z]$.

Beweis:

- ▶ Angenommen $a(z) = a_1(z) \cdots a_k(z)$ vollständige Faktorisierung von $a(z)$ in $F(\alpha)[z]$, dann ist $\text{Norm}(a) = \text{Norm}(a_1) \cdots \text{Norm}(a_k)$ eine Faktorisierung von $\text{Norm}(a)$ in $F[x]$. d.h.
 Für jedes i gilt $p_i(z) = \text{Norm}(a_j)$ für ein geeignetes j .
 Da $\text{Norm}(a)$ quadratfrei, folgt $\text{Norm}(a_j) \neq \text{Norm}(a_h)$ für $h \neq j$.

Umkehrung (Forts.)

- ▶ Behauptung: Gilt $p_i(z) = \text{Norm}(a_j)$, so

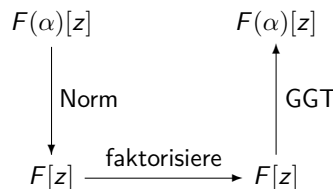
$$(*) \quad a_j(z) = \text{GGT}(a(z), p_i(z))$$

wobei der GGT in $F(\alpha)[z]$ genommen wird.

- ▶ Aus der Definition der Norm und den Eigenschaften folgt $a_j(z) \mid a(z)$ und $a_j(z) \mid p_i(z)$ in $F(\alpha)[z]$. Ein größerer Teiler würde bedeuten: es gibt $a_h(z) \mid a(z)$ und $p_i(z)$ in $F(\alpha)[z]$ für ein h , $h \neq j$.
- ▶ Da $a_h(z) \mid p_i(z)$, gilt $\text{Norm}(a_h) \mid \text{Norm}(p_i)$. Aber $p_i(z) \in F[z]$ so folgt $\text{Norm}(p_i) = p_i(z)^n$
- ▶ Aber $\text{Norm}(a_h)$ ist irreduzibel, d. h. $\text{Norm}(a_h) = p_i(z) \nmid$ falls $h \neq j$, d. h. $(*)$ gilt.

Faktorisierung in $F(\alpha)[z]$

- ▶ Wenn $\text{Norm}(a)$ quadratfrei, so kann $a(z)$ wie folgt faktorisiert werden:



- ▶ Ist $a(z) \in F(\alpha)[z]$ nicht quadratfrei, so kann man wie gehabt o.b.d.A. auf quadratfreien Fall reduzieren. Benötigt wird aber $\text{Norm}(a)$ quadratfrei.
- ▶ Finde $s \in F$, so dass $b(z) = a(z + s\alpha)$ quadratfrei. Dann faktorisiere $b(z) = b_1(z) \cdots b_k(z)$.
- ▶ Die Faktorisierung für $a(z) = a_1(z) \cdots a_k(z)$ mit $a_i(z) = b_i(z - s\alpha)$.

Faktorisierung in $F(\alpha)[z]$ (Forts.)

6.39 Satz Sei $a(z)$ quadratfreies Polynom in $F(\alpha)[z]$. Dann ist $\text{Norm}(a(z - s\alpha))$ quadratfrei bis auf endlich vielen $s \in F$.

Beweis:

- ▶ Sei $\text{Norm}(a) = \prod_{i=1}^r p_i(z)^i$ quadratfreie Faktorisierung von $\text{Norm}(a)$ in $F[z]$.
- ▶ Da $a(z)$ quadratfrei ist und $a(z) \mid \text{Norm}(a) \rightsquigarrow a(z) \mid p(z) = p_1(z) \cdots p_r(z)$. Beachte hierbei $p(z) \in F[z]$.
- ▶ Seien β_1, \dots, β_k die Wurzeln von $p(z)$, d. h. $p(z) = \prod (z - \beta_i)$.
- ▶ Da $p(z)$ quadratfrei ist, so sind alle β_i verschieden.

Beweis (Forts.)

- ▶ Sei $s \in F$, dann $c_s(z) := \text{Norm}(p(z - s\alpha)) = \prod_j \prod_i (z - (s\alpha_j + \beta_i)) \in F[z]$.
- ▶ Dieses Polynom kann mehrfach Wurzeln haben gdw $s \cdot \alpha_j + \beta_i = s \cdot \alpha_u + \beta_v$ für j, i, u, v geeignet gdw $s = \frac{\beta_v - \beta_i}{\alpha_j - \alpha_u}$
- ▶ d. h. für fast alle $s \in F$ gilt $\text{Norm}(a(z - s\alpha)) \mid p(z - s\alpha) \mid c_s(z)$ mit $c_s(z)$ Polynom ohne Mehrfachwurzeln.
- ▶ In diesen Fällen ist $a_s(z) = a(z - s\alpha)$ Polynom in $F(\alpha)[z]$ mit quadratfreier Norm.

Faktorisierung über alg. Zahlkörpern

```

procedure Alg_Factorization( $a(z), m(x), \alpha$ )
    {Eingabe: quadratfrei  $a(z) \in F(\alpha)[z]$ 
    { $\alpha$  Alg-Zahl mit minimal Polynom  $m(x)$ , grad  $n$ ,  $a$  als Polynom in  $\alpha, z$ }
    {Ausgabe: Faktorisierung von  $a$ }

    1 //Finde  $s : \text{Norm}(a_s(z))$  quadratfrei //
       $s := 0; a_s(\alpha, z) := a(\alpha, z);$ 
       $\text{Norm}(a_s) := \text{Res}_x(m(x), a_s(x, z))$ 
      while Grad (GGT ( $\text{Norm}(a_s), \text{Norm}(a_s)'$ ))  $\neq 0$  do
         $s := s + 1; a_s(\alpha, z) := a_s(\alpha, z - \alpha);$ 
         $\text{Norm}(a_s) := \text{Res}_x(m(x), a_s(x, z))$ 
    2 //Faktorisiere  $\text{Norm}(a_s)$  in  $F[z]$  und lifte Ergebnis //
       $b := \text{factors}(\text{Norm}(a_s));$ 
      if sizeof( $b$ ) = 1 then return  $a(z)$ 
      else
        for each  $a_i(z) \in b$  do
           $a_i(\alpha, z) := \text{GGT}(a_i(z), a_s(\alpha, z))$ 
           $a_i(\alpha, z) := a_i(\alpha, z + s\alpha)$ 
          substitute( $a_i(z) \leftarrow a_i(\alpha, z), b$ )
      return ( $b$ )
    
```

Beispiel

6.40 Beispiel Sei

$$a_\alpha(z) = z^4 + z^3 + (2 + \alpha - \alpha^2)z^2 + (1 + \alpha^2 - 2\alpha^3)z - 2 \in \mathbb{Q}(\alpha)[z]$$

Mit $\alpha = 3^{1/4}$ minimal Polynom für α , $m(x) = x^4 - 3$.

► $\text{Norm}(a_\alpha(z)) = \text{Res}_x(a_\alpha(z), m(x)) =$
 $= z^{16} + 4z^{15} + 14z^{14} + 32z^{13} + 47z^{12} + 92z^{11} + 66z^{10} + 120z^9$
 $- 50z^8 - 24z^7 - 132z^6 - 40z^5 - 52z^4 - 64z^3 - 64z^2 - 32z + 16$

Ist QF in $\mathbb{Q}[z]$

► Faktoriert man in $\mathbb{Q}[z]$ so $\text{Norm}(a_\alpha(z)) = g(z) \cdot h(z)$ mit

$$g(z) = z^8 + 4z^7 + 10z^6 + 16z^5 - 2z^4 - 8z^3 - 20z^2 - 8z + 4$$

$$h(z) = z^8 + 4z^6 + 9z^4 + 4z^2 + 4$$

Beispiel (Forts.)

► Berechne GGT in $\mathbb{Q}(\alpha)[z]$

$$\text{GGT}(a_\alpha(z), g(z)) = z^2 + (1 - \alpha)z + (1 - \alpha^2) \text{ und}$$

$$\text{GGT}(a_\alpha(z), h(z)) = z^2 + \alpha z + (1 + \alpha^2)$$

Faktorisierung von $a_\alpha(z)$ in $\mathbb{Q}(\alpha)[z]$ ist

$$a_\alpha(z) = (z^2 + (1 - \alpha)z + (1 - \alpha^2))(z^2 + \alpha z + (1 + \alpha^2))$$

- Problem:**
- Gradwachstum von $\text{Norm}(a)$.
 - Koeffizientenwachstum
- Forschungsgegenstand**
- Vermeidung von Wachstum
 - Berechnungen mit Körpererweiterungen
 - Galois Korrespondenz

Inhalt Kapitel 7

Primzahltesten und Faktorisierung in \mathbb{Z}

- Primzahltesten
- Primzahlen mit vorgegebenen Eigenschaften
- Faktorisierung in \mathbb{Z}
- Anwendung: Cryptosysteme

Andere Primzahltests (Fort.)

- Ist N Primzahl, so gilt für alle $a \in \mathbb{Z}$

$$(*) \left(\frac{a}{N}\right) \equiv a^{(N-1)/2} \pmod{N}$$

- Solovay-Strassen zeigen: Ist N zusammengesetzt und nicht Primzahlpotenz, so gilt (*) nicht für mindestens die Hälfte der Zahlen $a \in 1 \dots N - 1$. Ihr Algorithmus testet (*) für zufällig gewählte a 's und kostet $O(\log N \cdot M(\log N))$ Wortoperationen pro Test.
- Spezielle Primzahltests:
 - Pepin (1877) für Fermat Zahlen $F_n = 2^{2^n} + 1$
 F_n ist Primzahl gdw $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$
 - Lucas-Lehmer Test (1878,1935) für Mersenne-Zahlen $M_n = 2^n - 1$
 $2^n - 1$ ist Primzahl gdw $l_{n-1} \equiv 0 \pmod{M_n}$.
Hierbei l_i rek. definiert durch $l_1 = 4$ und $l_i = l_{i-1}^2 - 2 (i \geq 1)$

Primzahltesten ist in P

Siehe

<http://www.cse.iitk.ac.in/news/primality.html>

Finden von Primzahlen mit vorgebenen Eigenschaften

z. B. Primzahl mit n -Bits, Big-Prime Methoden, Hensel Lifting Methoden.

- Primzahlsatz:

- Seien $\Pi(x) = |\{p \in \mathbb{N} : p \leq x, p \text{ Primzahl}\}|$, $p_n = n$ te Primzahl
- Dann gilt: $\Pi(x) \approx \frac{x}{\ln x}$ und $p_n \approx n \ln n$

d.h. Eine zufällige Zahl nahe bei x ist eine Primzahl mit Wahrscheinlichkeit $1/\ln x$.

d. h. wählt man zufällige n -Bit Zahl und testet sie auf Primalität, so erwartet man eine Primzahl zu finden mit etwa $n \ln 2$ Versuchen.

- Wie findet man Primzahl p mit $B < p \leq 2B$ (B vorgegeben). Wähle zufälliges Element im Intervall, teste auf Primalität k mal und gebe erste Zahl aus, die diesen Test erfüllt.
- Ist p nicht Primzahl, so ist die Wahrscheinlichkeit Antwort „mögliche Primzahl“ $\leq 2^{-k}$. Dies bedeutet aber nicht, dass die Ausgabe Primzahl mit Wahrscheinlichkeit $1 - 2^{-k}$ ist.

Finden von Primzahlen mit vorgebenen Eigenschaften

7.3 Satz Gegeben B, k , die Ausgabe des Verfahrens ist eine Primzahl mit Wahrscheinlichkeit mindestens $1 - 2^{-k+1} \ln B$ und benötigt im Mittel $O(k(\log^2 B)M(\log B))$ Wortoperationen.

- Beachte $|P| = \Pi(2B) - \Pi(B) \geq B/2 \ln B (B \geq 6) \rightsquigarrow \frac{|P|}{B} \geq \frac{1}{2 \ln B}$
- Erwarteten Wahlen: $2 \ln B$ und jede kostet $O(k \log B \cdot M(\log B))$

7.4 Lemma Sei $P \subset \mathbb{N}$ Menge von Primzahlen, $a = \min P$. Sei $M \in \mathbb{Z}$ mit $0 \neq |M| \leq C$. Wählt man p zufällig aus P , so gilt

$$\text{Prob}\{M \equiv 0 \pmod{p} : p \in P\} \leq \frac{\log_a C}{|P|}$$

(es gibt höchstens $\log_a |M| \leq \log_a C$ Primzahlen in P , die M teilen).

Finden von Primzahlen mit vorgegebenen Eigenschaften

7.5 Satz

- ▶ Es gibt einen probabilistischen Algorithmus, der mit Wahrscheinlichkeit mindestens $3/4$ eine Primzahl p zwischen $B + 1$ und $2B$ berechnet für jede Zahl $B \in \mathbb{N}$ mit Wortlänge β .
- ▶ Ist $M \in \mathbb{Z}, M \neq 0$ mit $6 \ln |M| \leq B$, so gilt: p Primzahl und $p \nmid M$ mit Wahrscheinlichkeit mindestens $1/2$.
- ▶ Der Algorithmus benötigt $O(\beta^2 M(\beta) \log(\beta))$ Wortoperationen.
 - ▶ Wähle $k = 2 + \lceil \log_2 \ln B \rceil$ (dann Satz)
 - ▶ $p \mid M$ für p prim mit Wahrscheinlichkeit

$$\frac{\log_B C}{|P|} \leq \frac{\ln C \cdot 2 \ln B}{\ln B \cdot B} \leq \frac{1}{3} \quad (B \geq 6) \rightsquigarrow \frac{3}{4} \left(1 - \frac{1}{3}\right) = \frac{1}{2}$$

- ▶ Die ersten r Primzahlen können deterministisch in $O(r \log^2 r \log \log r)$ Wortoperationen berechnet werden.

Kosten und Voraussetzungen für Primzahlen in Algorithmen

				cost for
	modular algorithm	prime requirements	prime finding	algorithm
deter-	big	$p > 2n^{n/2} A^n$	$n^3 \log^3 A$	$n^4 \log A$
minant	small	$p_i < 2r \ln r$	$n \log^3 A$	$n^4 \log A$
gcd	big	$p > \sqrt{n+1} 2^{n+1} A^2$	$n^3 + \log^3 A$	$n^2 + n \log A$
	small	$p_i < 2r \ln r$	$n \log A$	$n^2 + n \log A$
EEA	small	$p_i < 2r \ln r$	$n \log A$	$n^3 \log A$
root finding	big power	$p > 2n(A^2 + A)$	$\log^3 A$	$n^2 \log A + n \log^2 A$
factor-	big power	$p > \sqrt{n+1} 2^{n+1} A^2$	$n^3 + \log^3 A$	$n^{10} + n^8 \log^2 A$
		$p < 2r \ln r$	$n \log A$	$n^{10} + n^8 \log^2 A$

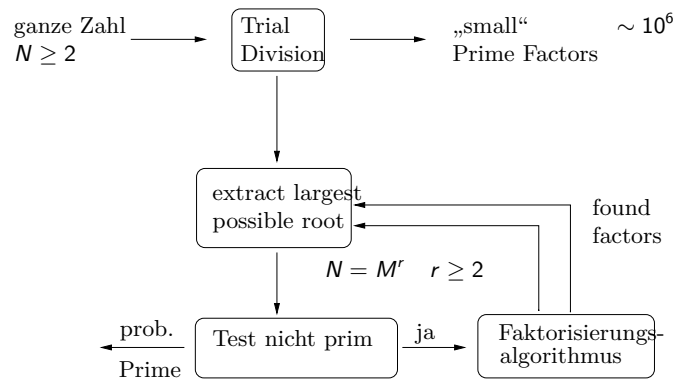
Faktorisierung in \mathbb{Z} (Übersicht)

Methode	Jahr	Zeit
Trialdivision	$-, \infty$	$O^{\sim}(2^{n/2})$
Pollard's $p - 1$ Methode	1974	$O^{\sim}(2^{n/4})$
Pollard's ρ -Methode	1975	$O^{\sim}(2^{n/4})$
Pollard-Strassen	1976	$O^{\sim}(2^{n/4})$
Morrison/Brillhart	1975	$\exp(O^{\sim}(n^{1/2}))$
Dixon's Random Squares	1981	$\exp(O^{\sim}(n^{1/2}))$
Lenstra's Elliptic Curves	1987	$\exp(O^{\sim}(n^{1/2}))$
Number Field Sieve	1990	$\exp(O^{\sim}(n^{1/3}))$

Faktorisierung in \mathbb{Z} (Übersicht) (Forts.)

- ▶ Faktorisierung von Polynome über \mathbb{F}_2 Grad 200000.
- ▶ Faktorisierung von Zahlen der Länge 150 noch als **extrem hart**. „Praktische Relevanz von P “ \rightsquigarrow wichtig für Cryptosysteme.
- ▶ Tabellen: Cunningham Projekt 1925. Faktorisierungen von $b^n \pm 1$.
- ▶ "Most Wanted" Factorizations.
 - ▶ RSA Cryptosystem: p_1, p_2 große Pzahl $p_1 p_2$. 130-Digits RSA Zahlen geknackt $\sim 2 \times 65 \times 96$
 - ▶ Faktorisierung Fermat'scher Zahlen $F_y = 2^{2^y} + 1$
 F_{10}, F_{11} ellipt. Kurven, „most wanted 98“ $2^{569} - 1 / (PF) 23$ Dig.
 $F_{12} = 114689 \cdot 26017793 \cdot 63766529 \cdot 190274191361 \cdot 1256132134125569 \cdot C$ (C mit 1187 Digits).
 - ▶ <http://www.cerias.purdue.edu/homes/ssw/cun/index.htm> (siehe Wagstaff).

Format der Faktorisierungsalgorithmen



siehe Kap. 19, vz. Gathen/Gerhard
 + Kap.20: Anwendung Public Key Cryptography.

Faktorisierungsalgorithmen in \mathbb{Z}

Annahme: N ist keine perfekte Potenz, d.h. $N \neq M^k$ für $M \in \mathbb{Z}, k \geq 2$

- ▶ Ganzzahlige Wurzeln berechnen: Gegeben $a, n \in \mathbb{N}$
 Entscheide ob a eine n -te Potenz einer Zahl ist und berechne diese gegebenenfalls.
- ▶ Gesucht Lösung von $y^n - a = 0$::
 Verwende hierfür Newtons Iteration (2-adisch) für a, n ungerade in $O(M(\log N))$.
- ▶ Bestimme b, d, e, r mit $N = 2^d 3^e b^r$ $\text{GGT}(b, 6) = 1$ r maximal in $O(\log N \cdot M(\log N))$ Wortoperationen.
 (Siehe Aufgaben 9.44 und 18.6 in vzG,G).

Trial Division Faktorisierungsalgorithmus

1. Trial_Division_Fakt_Algorithmus

{Eingabe: $N \in \mathbb{N}_{\geq 3}$, weder Prim noch perfekte Potenz, $b \in \mathbb{N}$ }
 {Ausgabe: kleinster Primfaktor von N falls kleiner b sonst „Failure“}

```
begin
1 for  $p = 2, 3, \dots, b$  do
2   if  $p \mid n$  then return  $p$ 
3 return „Failure“
end
```

- ▶ Um alle p -Faktoren zu finden, dividiere durch p so oft wie möglich dann weiter. Verwende: nächster Primteiler $> p$. Ist $S_1(N)$ bzw. $S_2(N)$ der grösste bzw. zweitgrösste P-Faktor von N . So $S_2(N) < \sqrt{N}$, d.h $S_2(n)(\log N)^{O(1)}$ Schritte. Für zufällige Zahlen N gilt

$$\text{Prob}(S_1(N) > N^{0.85}) \approx 0.20 \quad \text{Prob}(S_2(N) > N^{0.30}) \approx 0.20$$

- ▶ $O(N^{0.30})$ erwartete Schrittkomplexität für 1.

Pollard und Strassen Methode

Sei $a \mapsto \bar{a}$ die mod N Reduktion und $1 \leq c \leq \sqrt{N}$. Betrachte $F = (x+1)(x+2)\dots(x+c) \in \mathbb{Z}[x]$ $f = \bar{F} \in \mathbb{Z}_N[x]$

Dann gilt $\bar{c}! = \prod_{0 \leq i < c} f(\bar{i})$. Strategie: "baby step/giant step":

2. Pollard_Strassen_Faktorisierung

{Eingabe: $N \in \mathbb{N}_{\geq 3}$, weder Prim noch perfekte Potenz, $b \in \mathbb{N}$ }
 {Ausgabe: kleinster Primfaktor von N falls $< b$ sonst „Failure“}

```
begin
1  $c \leftarrow \lceil b^{1/2} \rceil$ ; Berechne Koeffizienten von  $f = \prod_{1 \leq j \leq c} (x + \bar{j}) \in \mathbb{Z}_N[x]$ ;
2 Berechne  $g_i \in \{0, \dots, N-1\}$  mit  $g_i \bmod N = f(\bar{i})$  für  $0 \leq i < c$ ;
3 Falls  $\text{GGT}(g_i, N) = 1$  für  $0 \leq i < c$  then return „Failure“
    $k \leftarrow \text{Min} \{0 \leq i < c : \text{GGT}(g_i, N) > 1\}$ 
4 return  $\text{Min} \{kc + 1 \leq d \leq kc + c : d \mid N\}$ 
end
```

Fakt. Alg. Pollard/Strassen (Forts.)

7.6 Satz

Algorithmus 2. ist korrekt und benötigt $O(M(b^{1/2})M(\log N)(\log b + \log \log N))$ Wortoperationen und Platz für $O(b^{1/2} \log N)$ Wörter.

Beweis: Für $0 \leq i < c$ gilt:

- ▶ Ein Primteiler p von N teilt $F(ic)$ und somit auch $\text{GGT}(g_i, N) = \text{GGT}(F(ic) \bmod N, N)$ gdw. p teilt Zahl im Intervall $\{ic + 1, \dots, ic + c\} \rightsquigarrow$ Korrektheit.
- ▶ Kosten für 1. und 2. $O(M(c) \log c)$ Add., Mult. in \mathbb{Z}_N
 Schritt 3 $O(cM(\log N) \log \log N)$ Wortoperationen
 Schritt 4 $O(cM(\log N))$ Wortoperationen
 Add., Mult. in \mathbb{Z}_N kostet $O(M(\log N))$.
- ▶ Platz für $O(b^{1/2})$ Zahlen der Größe $O(\log N)$
- ▶ Schleife mit $b = 2^i, (i = 1, 2, \dots, b > S_2(N))$ liefert vollständige Faktorisierung in $O(M(S_2(N)^{1/2})M(\log N) \log N)$.

Pollards ϱ -Methode (1975)

Idee

Wähle Funktion $f : \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ und Startwert $x_0 \in \mathbb{Z}_N$ Setze $x_i = f(x_{i-1})$ für $i > 0$. Betrachte die Folge (x_i) :

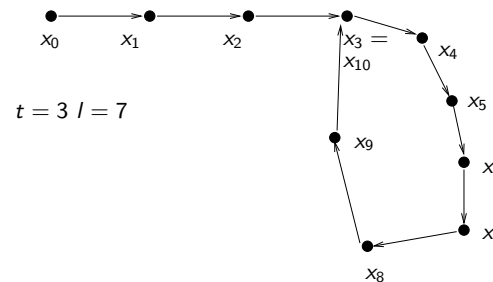
- ▶ Hoffe nun die Folge x_0, x_1, x_2, \dots verhält sich wie eine Folge unabhängiger Zufallselemente von \mathbb{Z}_N .
- ▶ Ist p ein unbekannter Primfaktor von N so findet eine **Kollision mod p** statt, falls es t, l gibt mit $l > 0$ und $x_t \equiv x_{t+l} \pmod p$
- ▶ Ist N keine Primzahlpotenz und q ein weiterer p -Teiler von N , so sind, für unabhängige Reste modulo N , $x_i \bmod p$ und $x_i \bmod q$ ebenfalls unabhängige Zufallsvariablen (Chin. Restsatz).
- ▶ D.h. mit großer Wahrscheinlichkeit $x_t \not\equiv x_{t+l} \pmod q$ und somit $\text{GGT}(x_{t+l} - x_t, N)$ ist nicht trivialer Faktor von N .

Pollards ϱ -Methode (Forts.)

- ▶ **Frage:** Wie groß sind t, l ?
 Offenbar $t + l \leq p$ und der erwartete Wert ist $O(\sqrt{p})$ für eine Zufallsfolge $(x_i)_{i \in \mathbb{N}}$.
- ▶ **Geburtstagsproblem:** Wieviel Personen benötigt man um eine Wahrscheinlichkeit (zwei Personen mit gleichem Geburtstag zu haben) $\geq 1/2$ zu erhalten (23 reichen 50,7%)
- ▶ Auswahl (mit Wiederholung) aus Urne mit p Marken. Die erwartete Anzahl von Wahlen bis zu einer Kollision ist $O(\sqrt{p})$
- ▶ **Wie bestimmt man Zykel : Floyd's Trick.**
 Sei $x_0 \in \{0, \dots, p-1\}$ $f : \{0, \dots, p-1\} \rightarrow \{0, \dots, p-1\}$
 Betrachte $(x_i)_{i \geq 0}$ mit $x_{i+1} = f(x_i)$.
- ▶ **Zykel** der Länge $l > 0$ mit $x_i = x_{i+l}$ für alle $i \geq t$ für $t \in \mathbb{N}$

Pollards ϱ -Methode (Forts.)

l, t seien minimal



Speichere Folge bis $x_t = x_j$
 $O(t+l)$ zuviel Platz

Floyd's 1-step/2-step cycle detection method::

Führe zweite sequenz mit $y_i = x_{2i}$ speichere nur x_i, y_i bis $x_i = y_i = x_{2i}$

FLOYD_Cycle_Det_ALG

```

y0 ← x0; i ← 0;
repeat i ← i + 1; x_i ← f(x_{i-1}); y_i ← f(f(y_{i-1})) until x_i = y_i;
return i
    
```

Floyd's 1-Step/2-Step cycle Detection Method

7.7 Lemma FLOYD_Cycle_Det_ALG hält nach höchstens $t + l$ Iterationen.

Beweis: Da $x_{2i} = y_i$ für alle i gilt:

- ▶ $x_i = y_i$ gdw. $i \geq t$ und $l \mid (2i - i) = i$, und der kleinste Index ist $i = t + (-t \text{ REM } l) < t + l$ falls $t > 0$ und $i = l$ falls $t = 0$.

★ **Pollard's ρ -Methode zur Faktorisierung von N :**
 Erzeuge Folge $x_0, x_1, \dots \in \{0, \dots, N - 1\}$ wie folgt:
 x_0 wird zufällig gewählt, $x_{i+1} = f(x_i) = x_i^2 + 1 \text{ REM } N$.

- ▶ Sei p kleinste Primzahl die N teilt $\rightsquigarrow x_{i+1} \equiv x_i^2 + 1 \pmod p$ für $i \geq 0$. Kollision mod p kann nach $O(\sqrt{p})$ Schritte erwartet werden. Verwende hierfür FLOYD'S-ALG.

Pollards ρ -Methode zur Faktorisierung

3. **Pollard_ ρ _Faktorisierung**
 {Eingabe: $N \in \mathbb{N}_{\geq 3}$, weder Prim noch perfekte Potenz}
 {Ausgabe: entweder echter Teiler oder „Failure“}

```

begin
1 Wähle  $x_0 \in \{0, \dots, N - 1\}$  zufällig;  $y_0 \leftarrow x_0$ ;  $i \leftarrow 0$ ;
2 repeat
3    $i \leftarrow i + 1$ ;  $x_i \leftarrow x_{i-1}^2 + 1 \pmod N$ ;  $y_i \leftarrow (y_{i-1}^2 + 1) \pmod N$ ;
4    $g \leftarrow \text{GGT}(x_i - y_i, N)$ ;
   if  $1 < g < N$  then return  $g$ 
   else if  $g = N$  then return „Failure“
end
    
```

7.8 Satz Ist p der kleinste P-Teiler von $N \rightsquigarrow$ erwartete Laufzeit ersten Teiler zu finden $O(\sqrt{p}M(\log N) \log \log N)$.
 Vollständige Faktorisierung $S_2(N)^{1/2} \sim (\log^2 N) \approx 0 (N^{1/4})$

Pollards S-Methode zur Faktorisierung (Forts.)

7.9 Beispiel $N = 82123$ $x_0 = 631$

i	$x_i \pmod N$	$x_i \pmod{41}$	$y_i \pmod N$	GGT $(x_i - y_i, N)$
0	631	16	631	N
1	69670	11	28986	1
2	28986	40	13166	1
3	69907	2	40816	1
4	13166	5	20459	1
5	64027	26	6685	1
6	40816	21	75835	1
7	80802	32	17539	41
8	20459	0		
9	71874	1		
10	6685	2		

$$N = 41 \cdot 2003$$

$$x_{38} \equiv 4430 \equiv x_{143} \pmod N$$

Dixon's Random Square Faktorisierungsmethode

- ▶ Erstes Verfahren mit Aufwand kleiner als $\exp(\varepsilon \cdot \log N)$ für jedes $\varepsilon > 0$
Idee: Die Gleichungen

$$N = s^2 - t^2 = (s + t)(s - t)$$

$$N = a \cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Beschreiben **Bijektion** zwischen Faktorisierungen von N und Darstellungen von N als Differenz zweier Quadrate.

- ▶ **Naiver Faktorisierungsalgorithmus:** Für $t = \lceil \sqrt{N} \rceil, \lceil \sqrt{N} \rceil + 1, \dots$
 Teste ob $t^2 - N$ perfektes Quadrat ist.
 Findet man solch ein Quadrat so Faktorisierung erfolgreich!
- ▶ Gut Falls $N = ab$ mit $|a - b|$ klein, da **Laufzeit** abhängig von $|a - b|$ ist.
 Fermat kannte dieses Argument: $N = 2027651281$ $\sqrt{N} \approx 45029$

$$N = 45041^2 - 1020^2 = 46061 \cdot 44021$$

Dixon's Random Square Methode (Forts.)

- ▶ Variante: Wähle $k \ll N$ $t = \lceil \sqrt{kN} \rceil, \lceil \sqrt{kN} \rceil + 1, \dots$ und teste ob $t^2 - kN$ perfektes Quadrat.
 Falls $t^2 - kN = s^2$ so GGT($s + t, N$) ist hoffentlich nichttrivialer Faktor von N , so dass $s \not\equiv \pm t \pmod N$
- ▶ Das finden von Relationen der Form $s^2 \equiv t^2 \pmod N$ auf dieser Weise ist für große N sehr unwahrscheinlich.

7.10 Beispiel

$N = 2183$ Angenommen wir haben folgende Kongruenzen
 $453^2 \equiv 7 \pmod N$ $1014^2 \equiv 3 \pmod N$ $209^2 \equiv 21 \pmod N$
 Dann $(453 \cdot 1014 \cdot 209)^2 \equiv 21^2 \pmod N$ oder
 $687^2 \equiv 21^2 \pmod N$ \rightsquigarrow
 $37 = \text{GGT}(687 - 21, N)$ $59 = \text{GGT}(687 + 21, N)$
 Dieses ist auch die Faktorisierung von N

Dixon's Random Square Methode (Forts.)

- ▶ Systematisches Vorgehen:
 Wähle b zufällig und hoffe, dass $b^2 \pmod N$ Produkt kleiner Primzahlen ist. Sind genügend solcher gefunden, so erhält man eine Kongruenz $s^2 \equiv t^2 \pmod N$. Dann GGT($s - t, N$) bzw. GGT($s + t, N$)
- ▶ Faktorisierungsbasis Primzahlen p_1, \dots, p_h bis zu einer Schranke $B \in \mathbb{R}^+$
 Eine Zahl b heißt **B-Zahl** falls $b^2 \pmod N$ (Rest der Division von b^2 durch N) Produkt der P -Zahlen p_1, \dots, p_h ist.
- ▶ Im Beispiel sind 453, 1014, 209 B-Zahlen für jedes $B \geq 7$ und $N = 2183$
- Für eine B-Zahl b sei $b^2 \equiv p_1^{\alpha_1} p_2^{\alpha_2} \dots p_h^{\alpha_h} \pmod N$ mit $\alpha_1 \dots \alpha_h \in \mathbb{N}$.
 Assoziiere dazu **Binären Exponenten Vektor**

$$\varepsilon = (\alpha_1 \pmod 2, \alpha_2 \pmod 2, \dots, \alpha_h \pmod 2) \in \mathbb{F}_2^h$$

- ▶ Für B-Zahl b_i , sei $b_i^2 \equiv \prod_{1 \leq j \leq h} p_j^{\alpha_{ij}} \pmod N$

Dixon's Random Square Methode (Forts.)

- ▶ Angenommen man hat b_1, \dots, b_l mit $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_l = 0$ in \mathbb{F}_2^h dann

$$\left(\prod_{1 \leq i \leq l} b_i \right)^2 = \prod_{1 \leq j \leq h} p_j^{\sum_{1 \leq i \leq l} \alpha_{ij}} = \prod_{1 \leq j \leq h} p_j^{2\gamma_j} = \left(\prod_{1 \leq j \leq h} p_j^{\gamma_j} \right)^2 \pmod N$$
 wobei $\gamma_j = \frac{1}{2} \sum_{1 \leq i \leq l} \alpha_{ij}$ (durch 2 teilbar nach Voraussetzung)
- ▶ Dann $s^2 \equiv t^2 \pmod N$ mit

$$s = \prod_{1 \leq i \leq l} b_i \quad t = \prod_{1 \leq j \leq h} p_j^{\gamma_j}$$

- ! Man benötigt nicht mehr als $h + 1$ B-Zahlen, d.h. $l \leq h + 1$, da jede Menge von $h + 1$ Vektoren in \mathbb{F}_2^h linear abhängig ist.

Dixon's Random Square Methode (Forts.)

- ! Die Hoffnung ist nun s, t gefunden zu haben mit $s \not\equiv \pm t \pmod N$
- ▶ Ist N keine Primzahlpotenz mit $r \geq 2$ verschiedene Primfaktoren, so folgt aus Chinesischer-Restsatz, dass jedes Quadrat in \mathbb{Z}_N^* genau 2^r Quadratwurzeln in \mathbb{Z}_N hat.
- ▶ Ist somit s eine zufällige Quadratwurzel von t^2 so gilt

$$\text{Prob} \{s \equiv \pm t \pmod N\} = \frac{2}{2^r} \leq \frac{1}{2}$$

- ▶ Im Beispiel mit $B = \{2, 3, 5, 7\}$ gilt
 $\varepsilon_1 = (0, 0, 0, 1)$ $\varepsilon_2 = (0, 1, 0, 0)$ $\varepsilon_3 = (0, 1, 0, 1)$
 $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 0$ in \mathbb{F}_2^4 und $\gamma_1 = \gamma_3 = 0$ $\gamma_2 = \gamma_4 = 1$
 $s = 453 \cdot 1014 \cdot 209$ $t = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1$

Lenstra's Elliptische-Kurven Methode (1987)

- ▶ Statt $G = \mathbb{Z}_N^*$, werden Gruppen von Elliptischen-Kurven und deren Ordnung als Testkandidat B -Zahl zu sein, verwendet.
Algebraische Geometrie

▶ Sei F Körper mit $\text{char} \neq 2, 3$ und $x^3 + ax + b \in F[x]$ quadratfrei. Dann ist

$$E = \{(u, v) \in F^2 : v^2 = u^3 + au + b\} \cup \{O\} \subseteq F^2 \cup \{O\}$$

eine **elliptische Kurve über F** . O Punkt im Unendlichen von E .

- ▶ $x^3 - x = x(x - 1)(x + 1)$, $x^3 - x + b$ definieren elliptische Kurven.
- ▶ **Gruppenstruktur:** E wird zu einer abelschen Gruppe mit $+$ wie folgt: Ist $P = (u, v) \in E$, so sei der **Spiegelpunkt** $-P = (u, -v)$ wobei $-O = O$. Sind $P, Q \in E$, so schneidet die Gerade durch P, Q E in Punkt S . Dann $R = P + Q = -S$. Spezialfälle $P = Q$ (Tangente), $P + O = -(-P) = P$ und $P + (-P) = -O = O$.



Lenstra's Elliptische-Kurven Methode (1987)

- ▶ Die Größe elliptischer Kurven über \mathbb{F}_q :
- ▶ Sei E elliptische Kurve über \mathbb{F}_q , $\text{char} > 3$, dann gilt $|E| \leq 2q + 1$.
- ▶ Hasse's Schranke: $||E| - (q + 1)| \leq 2\sqrt{q}$
- ▶ Sei $y^2 = x^3 + x$ mit $q = 7$. E enthält $(0, 0), (1, 0), (4, 2), (4, 5), (5, 1), (5, 6), (6, 0), O$. Die Gruppe wird von $(4, 2)$ mit Ordnung 4 und $(0, 0)$ mit Ordnung 2 erzeugt, d.h. isomorph zu $\mathbb{Z}_4 \times \mathbb{Z}_2$.
- ▶ $|E| \cdot P = O$. Die Ordnung eines Elements ist wie üblich definiert.
- ▶ Rationale Funktionen zur Berechnung der Summe $(x_1, y_1) + (x_2, y_2)$

$$x_1 \neq x_2 \rightsquigarrow x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, y_3 = -y_1 + \frac{y_2 - y_1}{x_2 - x_1} \cdot (x_1 - x_3)$$

$$(x_1, y_1) = (x_2, y_2) \rightsquigarrow x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, y_3 = -y_1 + \frac{3x_1^2 + a}{2y_1} \cdot (x_1 - x_3)$$



Lenstra's Elliptische-Kurven Faktorisierungsalgorithmus

5. Lenstra's_Elliptic_Curve_Faktorisierung

{Eingabe: Ungerade Zahl $N, 3 \nmid N$, keine perfekte Potenz, $B \in \mathbb{R}^+$, $\min_{p|N} \leq C$ }
{Ausgabe: entweder echter Teiler oder „Failure“}

- 1 Wähle zufällig $(a, u, v) \in \{0, \dots, N - 1\}^3$;
 $b \leftarrow v^2 - u^3 - au; g \leftarrow GGT(4a^3 + 27b^2, N)$;
if $1 < g < N$ **then return** g **else if** $g = N$ **return** „Failure“;
- 2 //Sei E die "elliptische Kurve" über \mathbb{Z}_N mit Koeffizienten a, b //
Berechne die Primzahlen $p_1 = 2 < \dots < p_h \leq B$;
 $P \leftarrow (u, v); Q \leftarrow P; t \leftarrow 1$;
- 3 **for** $1 \leq j \leq h$ **do**
 $e_j \leftarrow \lfloor \log_{p_j}(C * 2\sqrt{C} + 1) \rfloor$;
for $0 \leq j < e_j$ **do** //Invarianten: $t = p_j^j \prod_{1 \leq r \leq j} p_r^{e_r}$ und $Q = tP$ //
- 4 Versuche $p_i Q$ in E über \mathbb{Z}_N zu berechnen;
if ein Zähler w Nullteiler in \mathbb{Z}_N **then return** $GGT(w, N)$
else $Q \leftarrow p_i Q; t \leftarrow p_i t$;

5 **return** „Failure“



Analyse von Lenstra's Faktorisierungsalgorithmus

- ▶ Benötigt wird: $E \text{ mod } p$ ist elliptische Kurve für jeden Primteiler $p | N$. E ist i.A. keine Gruppe mit $+$ definiert durch die Gleichungen, d.h die rationalen Ausdrücke müssen nicht mod N wohldefiniert sein.
- ▶ Sei $p | N$ prim, dann $p \nmid 4a^3 + 27b^2$, da sonst Ausgang in 1. Sei E_p die Reduktion von $E \text{ mod } p$, d.h. die elliptische Kurve über \mathbb{Z}_p mit Koeffizienten $a, b \text{ mod } p$. Zu $P \in E$ sei P_p der korrespondierende Punkt $P \text{ mod } p$. O_p korrespondiert zu O und für alle $P \in E \setminus \{O\}$ gilt $P_p \neq O_p$.
- ▶ Bis der Teiler p in Schritt 4 gefunden wird ($p | GGT(w, N)$), implementieren die Berechnungen die Arithmetik von E_p in folgenden Sinn: Ein partielles Ergebnis $Q = tP$ in E liefert (mod p) das partielle Ergebnis $Q_p = tP_p$ in E_p , d.h. $tP_p = (tP)_p$.
- ▶ Eine Faktorisierung wird gefunden wenn für zwei Primteiler p, q von N ein Vielfaches der Ordnung von P_p in E_p erreicht wird, der nicht Vielfaches der Ordnung von P_q in E_q ist.



Analyse von Lenstra's Faktorisierungsalgorithmus

7.11 Lemma Angenommen (E, P) ist gewählt, $p, q \mid N$ verschieden, l sei der größte Primfaktor der Ordnung von P_p in E_p , $p \leq C$, $|E_p|$ sei B -glatt und $l \nmid |E_q|$. Dann wird N vom Algorithmus faktorisiert.

Beweis: Sei $k = \prod_{1 \leq r \leq h} p_r^{e_r}$, e_r wie in 3.

- Da $|E_p|$ B -glatt ist und $p \leq C$, folgt aus der Hasse Schranke: $|E_p| \mid k$.
- Sei d die Ordnung von P_p in E_p . Dann $d \parallel |E_p|$ und somit $l \leq B$ und $d \mid k$.
- Sei $p_i = l$ und e der Exponent von l in d , d.h. $1 \leq e \leq e_i$. Ist $j = e - 1$ so $t = l^{e-1} \prod_{1 \leq r < i} p_r^{e_r}$ und $Q = tP$ vor Schritt 4. $t \not\equiv 0 \pmod{d}$ und $lt \equiv 0 \pmod{d}$

Somit $Q_p = tP_p \neq O_p$ und $lQ_p = ltP_p = O_p$. Wir zeigen, der Algorithmus kommt **nicht** bis zu dieser Stelle. Angenommen $lQ = O$, dann auch $lQ_q = (lP)_q = O$. Da aber $l \nmid |E_q|$ muss bereits $Q_q = tP_q = O_q$ gelten und somit $Q = O$. Aber dann $Q_p = O_p \neq O_p$

Analyse von Lenstra's Faktorisierungsalgorithmus

7.12 Satz (Lenstra) Sei p Primzahl, $S \subseteq (p + 1 - \sqrt{p}, p + 1 + \sqrt{p}) \subset \mathbb{N}$ und seien $a, b \in \mathbb{F}_p$ zufällig gewählt.

Sei

$$E_p = \{(u, v) : v^2 = u^3 + au + b\} \cup \{O\}$$

eine elliptische Kurve über \mathbb{F}_p . Dann gibt es eine Konstante $c \in \mathbb{R}^+$ mit

$$\text{prob}\{|E_p| \in S\} \geq \frac{c |S|}{\sqrt{p} \log p}$$

7.13 Folgerung Sei $p \leq C$ ein Primteiler von N und $\sigma = |\{B\text{- glatte Zahlen in } (p + 1 - \sqrt{p}, p + 1 + \sqrt{p})\}|$. Dann erfüllt die Anzahl M der Tripel $(a, u, v) \in \{0, \dots, N - 1\}^3$ für die der Algorithmus N faktorisiert

$$\frac{M}{N^3} \geq \frac{c_1 \sigma}{\sqrt{p} \log p} \text{ für ein } c_1 \in \mathbb{R}^+$$

Laufzeitanalyse von Lenstra's Faktorisierungsalgorithmus

- Die Laufzeit hängt wesentlich ab von der Anzahl der Auswahlen die der Algorithmus benötigt um mit großer Wahrscheinlichkeit erfolgreich zu faktorisieren (Siehe Seite 540 vzG,G).
- **Vermutung:** Für $x, u \in \mathbb{R}^+$ und $d \in \mathbb{Z}$ zufällig gewählt aus Intervall $(x - \sqrt{x}, x + \sqrt{x})$ gilt

$$\text{prob}\{d \text{ ist } x^{\frac{1}{d}} \text{ glatt}\} = u^{-u(1+o(1))}$$

- Unter der Annahme der Vermutung, kann man eine erwartete Laufzeitschranke von

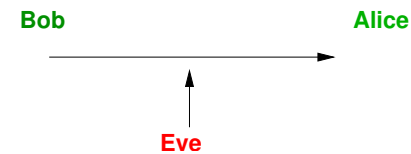
$$L(p)^{\sqrt{2}+o(1)} \text{ wobei } L(p) = e^{\sqrt{\ln p \ln \ln p}}$$

zeigen. **Praxis:** Wähle C "klein" und bestimme $B = e^{\sqrt{(\ln C \ln \ln C)/2}}$. Verdopple C falls nicht erfolgreich.

Moderne Anwendung: Public Key Cryptography

Cryptosysteme

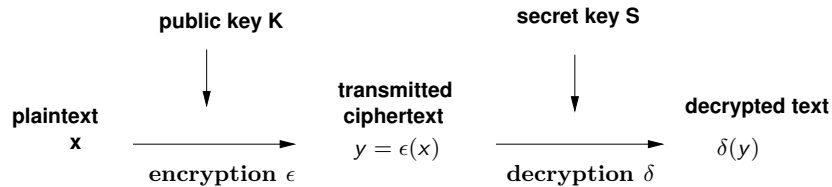
- **Szenario:** Bob will Nachricht an Alice senden, so dass ein Lauscher (Eve) die Nachricht nicht verstehen kann. Dies wird durch eine Chiffrierung der Nachricht erreicht, so dass nur Alice, mit den richtigen Schlüssel, die Nachricht leicht entschlüsseln kann aber Eve ohne den richtigen Schlüssel die Nachricht nicht verstehen kann.



- **Klassische Chiffrierungen:** **Caesar Chiffrierung:** Permutationen vom Alphabet mit 26 Buchstaben oder **One -Time Pad:** Um eine Nachricht der Länge n zu Verschlüsseln wird ein zufälliges Wort gleicher Länge buchstabenweise mod26 aufaddiert. **Symmetrisch.**

Public Key Cryptosysteme: Diffie & Hellman

- Idee: Zwei verschiedene Schlüssel K für die Verschlüsselung und S für die Entschlüsselung, beide "einfach" aber Entschlüsselung ohne S "hart".



K kann öffentlich bekannt sein. Da $x = \delta(y) = \delta(\epsilon(x))$ ist δ Inverse von ϵ . Funktionen die leicht zu berechnen sind aber eine harte Inverse besitzen heißen **trapdoor Funktionen**. K ist der öffentliche Schlüssel und S der geheime Schlüssel. Hier genügen n öffentliche-geheime Schlüsselpaare um sichere Kommunikation zwischen je zwei Partnern unter n zu realisieren.

Public Key Cryptosysteme: Anforderungen

- Ein Cryptosystem gilt als **geknackt**, wenn es ein Boolesches Prädikat $B(x)$ gibt - z.B. die Parität von x falls x eine Zahl ist - und ein pol. Zeit probabilistischer Algorithmus der $B(x)$ mit einer etwas besseren Wahrscheinlichkeit als Zufallsraten berechnet. Andernfalls gilt das System als **semantisch sicher**.
- Was bedeutet ein Cryptosystem ist "hart"? **Möglichkeiten:**
 - Der Erfinder (oder niemand) kennt keinen pol. Zeit Algorithmus.
 - Falls das System geknackt wird, so wird möglicherweise ein bekanntes "harte" Problem gelöst werden.
 - Falls das System geknackt wird, so ist ein bekanntes "harte" Problem gelöst.
 - Falls das System geknackt wird, so ist eine pol. Zeit Lösung für ein **NP**-vollständiges Problem gefunden.
 - Es gibt nachweisbar keinen (prob.) pol. Zeit Algorithmus wie oben.

Das RSA Cryptosystem

Rivest, Shamir & Adleman (1978) basiert auf die vermeintliche "Härte" der Faktorisierung in \mathbb{Z} . Das Prinzip ist einfach: Alice wählt zufällig zwei große Primzahlen (etwa 150 stellig) $p \neq q$ und setzt $N = pq$. Jeder der N faktorisieren kann, kann auch das System knacken.

Nachrichten werden als Folgen von Elementen aus $\mathbb{Z}_N = \{0, 1, \dots, N-1\}$ kodiert. Verwendet man als Alphabet $\Sigma = \{A, \dots, Z\}$ mit $|\Sigma| = 26$, so kann man Nachrichten mit bis zu $212 = \lfloor \log_{26} 10^{300} \rfloor$ Buchstaben mit einer Zahl darstellen, durch Verwendung der 26-adischen Darstellung. Etwa "CAESAR" wird dargestellt durch

$$2 \cdot 26^0 + 0 \cdot 26^1 + 4 \cdot 26^2 + 18 \cdot 26^3 + 0 \cdot 26^4 + 17 \cdot 26^5 = 200233302466 \in \mathbb{Z}_N$$

Will Alice Nachrichten von Bob erhalten, so wählt sie zufällig $e \in \{2, \dots, \varphi(N) - 2\}$ mit $\text{GGT}(e, \varphi(N)) = 1$, ($\varphi(N) = (p-1)(q-1)$). Dann berechnet sie $d \in \{2, \dots, \varphi(N) - 2\}$ mit $de \equiv 1 \pmod{\varphi(N)}$. $K = (N, e)$ ist ihr öffentlicher Schlüssel und $S = (N, d)$ ihr geheimer Schlüssel.

Das RSA Cryptosystem (Fort.)

- Die Ver- und Entschlüsselungsfunktion $\epsilon, \delta : \mathbb{Z}^\times \rightarrow \mathbb{Z}^\times$ werden durch $\epsilon(x) = x^e$ bzw. $\delta(y) = y^d$ definiert.
- Bob schickt eine Nachricht x an Alice in dem er $y = \epsilon(x)$ berechnet und versendet. Alice berechnet dann $\delta(y)$ mit ihren geheimen Schlüssel.
- Ist $u \in \mathbb{Z}$ mit $de - 1 = u\varphi(N)$, so gilt

$$(\delta \circ \epsilon)(x) = x^{de} = x^{1+u\varphi(N)} = x(x^{\varphi(N)})^u \equiv x \pmod{N}$$

(Man sollte darauf achten, dass $\text{GGT}(x, N) = 1$, da sonst eine Faktorisierung von N ermöglicht wird. Dies ist aber sehr unwahrscheinlich)

- RSA kann auch zur **Authentifizierung** verwendet werden, d.h der Sender muss nachweisen, dass es seine Nachricht ist. \rightsquigarrow **Digitale Signaturen**.

Das RSA Cryptosystem (Fort.)

- ▶ Bob versendet entweder $y = \delta_B(x)$ oder $y = \epsilon_A(\delta_B(x))$, da Alice ϵ_B kennt kann sie diese Nachrichten entschlüsseln.

7.14 Satz Folgende Probleme sind polynom-Zeit äquivalent:

- ▶ N zu faktorisieren
- ▶ $\varphi(N)$ zu berechnen
- ▶ Berechnung von $d \in \mathbb{N}$ mit $de \equiv 1 \pmod{\varphi(N)}$ aus $K = (N, e)$

Das Diffie-Hellman Schlüsselaustauschprotokoll (1976)

- ▶ **Zweck:** Protokoll zum Austausch von Schlüsseln zum Versenden von Nachrichten mit einem symmetrischen Cryptosystem.
- ▶ sei $q \in \mathbb{N}$ eine große Primzahlpotenz (etwa 1000 bits) und g ein Erzeuger (Generator) von \mathbb{F}_q^\times . Dann ist \mathbb{F}_q^\times isomorph zur additiven (zyklischen) Gruppe \mathbb{Z}_{q-1} via $g^i \longleftrightarrow i$.
- ▶ Das Protokoll arbeitet wie folgt:
 - ▶ Alice und Bob einigen sich auf q und g die öffentlich sein können.
 - ▶ Alice wählt für sich $a \in \mathbb{Z}_{q-1}$, berechnet und sendet $u = g^a \in \mathbb{F}_q^\times$ an Bob.
 - ▶ Bob wählt für sich $b \in \mathbb{Z}_{q-1}$, berechnet und sendet $v = g^b \in \mathbb{F}_q^\times$ an Alice.
 - ▶ Alice und Bob berechnen $v^a = g^{ab} = u^b$ und benutzen dies als gemeinsamen Schlüssel.

Das Diffie-Hellman Schlüsselaustauschprotokoll: Probleme

- ▶ Problem 1: Diffie-Hellman Problem:: DH

Gegeben $g^a, g^b \in \mathbb{F}_q^\times$, berechne g^{ab} .

- ▶ Problem 2: Diskreter Logarithmus Problem:: DL

Gegeben $g^a \in \mathbb{F}_q^\times$, berechne a .

- ▶ Es wird vermutet, dass DH ein hartes Problem ist. Die bisher schnellsten Algorithmen haben Laufzeiten wie die Faktorisierung in \mathbb{Z} . Scheint nicht NP-vollständig zu sein. Ein Lauscher der q, g, u, v kennt muss DH lösen um g^{ab} (den Schlüssel) zu berechnen. Dies ist pol-reduzibel auf DL (die Umkehrung ist nicht bekannt).
- ▶ Die beste Schranke für die Berechnung von DL in \mathbb{F}_q^\times ist $\exp(O((n \log^2 n)^{1/3}))$ Wortoperationen mit $n \approx \log_2 q$.

Das ElGamal Cryptosystem

- ▶ Wie gehabt \mathbb{F}_q^\times groß und g Generator.
- ▶ Um Nachrichten von Bob zu erhalten wählt Alice zufällig $S = b \in \mathbb{Z}_{q-1}$ als ihr geheimer Schlüssel und gibt $K = (q, g, g^b)$ als ihr öffentlicher Schlüssel bekannt.
- ▶ Will Bob eine Nachricht x an Alice senden, wählt er zufällig $k \in \mathbb{Z}_{q-1}$, berechnet g^k und xg^{kb} und sendet $y = (u, v) = (g^k, xg^{kb})$ an Alice.
- ▶ Alice berechnet $x = v/u^b$
- ▶ Die Berechnung von x aus y ohne Kenntnis von S ist pol Zeit äquivalent zu DH.

Rabin's Cryptosystem

- ▶ Basiert auf die Härte der Berechnung von Quadratwurzeln modulo $N = pq$, hierbei sind p, q Primzahlen wie bei RSA.
- ▶ Die Faktorisierung von N kann auf die Berechnung von Quadratwurzeln wie folgt reduziert werden: Wähle $x \in \mathbb{Z}_N$ und berechne $y = \sqrt{x^2}$. Dann $x^2 \equiv y^2 \pmod{N}$ oder $pq = N \mid (x + y)(x - y)$. Ist $x \not\equiv \pm y \pmod{N}$, so erhält man eine Faktorisierung von N (Siehe Dixon's random square A).
- ▶ Um eine Nachricht x an Alice zu senden, verwendet Bob ihr öffentlicher Schlüssel N und sendet $x^2 \pmod{N}$. Alice berechnet die zwei Quadratwurzeln von $y \pmod{p}$ und q mit EDF und kombiniert sie mit CRA. Es gibt Tricks um mit den 4 Möglichkeiten umzugehen.
- ▶ System ist anfällig für aktive Attacken: Falls Eve ein zufälliges x wählt und Alice dazu bringt eine Nachricht $y \equiv x^2 \pmod{N}$ zu signieren, in dem sie die Quadratwurzel z von $y \pmod{N}$ zurückgibt, so ist mit Wahrscheinlichkeit $1/2$, $GGT(x - z, N)$ ein echter Teiler von N .

Cryptosystem die auf elliptische Kurven basieren

- ▶ Die Idee ist analog zum ElGamal System, man verwendet an Stelle von \mathbb{F}_q^\times die additive Gruppe einer elliptischen Kurve E über \mathbb{F}_q .
- ▶ Die Kurve E und ein Punkt $P \in E$ sind öffentlich. Sei n die Ordnung von P in E .
- ▶ Alice wählt zufällig $a \in \{2, \dots, n - 2\}$ und gibt aP bekannt.
- ▶ Wenn Bob eine Nachricht $(m_1, m_2) \in \mathbb{F}_q^2$ an Alice senden, so wählt er ein zufälliges k , berechnet $kP = (r_1, r_2)$ und $k \cdot aP = (s_1, s_2)$ und sendet $(y_1, y_2, y_3, y_4) = (r_1, r_2, s_1 m_1, s_2 m_2) \in \mathbb{F}_q^4$ an Alice.
- ▶ Alice berechnet $a \cdot (r_1, r_2) = a \cdot kP = (s_1, s_2)$ und berechnet die Nachricht als $(m_1, m_2) = (s_1^{-1} y_3, s_2^{-1} y_4)$.
- ▶ Kommerzielle Implementierung auf Chip mit $\mathbb{F}_{2^{155}}$.

Inhalt Kapitel 8

Polynomideale und Gröbner-Basen

- Motivation: Buchberger's Algorithmus
- Reduktionstechniken zur Lösung des Wortproblems
- Termordnungen und multivariate Division mit Rest: Reduktion in $K[x_1, \dots, x_n]$
- Polynom-Reduktion
- Längen von Reduktionsketten
- Term-Ideale und Hilbert's Basissatz
- Gröbnerbasen und S-Polynome
- Buchberger's Algorithmus
- Anwendungen von Gröbner Basen
- Eliminationseigenschaften - Polynomgleichungen (Syzygien)
- Zur Komplexität der Berechnung von G-Basen

Motivation: Buchberger's Algorithmus

Polynomringe in mehreren Variablen. Werkzeug zur Modellierung vieler Probleme aus der (Alg)-Geometrie, Robotik (eukl. Geometrie), Invarianten, Singularitäten.

Polynomideale: $\{p_1, \dots, p_k\} \subseteq R[x_1, \dots, x_n] = \mathfrak{A}$, $\langle p_1, \dots, p_k \rangle_{\mathfrak{A}}$ Ideal.
 Wortproblem: $p \in \mathfrak{A}$ gilt $p \in \langle p_1, \dots, p_k \rangle$.
 Gegebenenfalls berechne Darstellung

$$p = \sum_{i=1}^k f_i p_i \text{ mit } f_i \in \mathfrak{A}$$

Division durch $\langle p_1, \dots, p_k \rangle$ mit Rest: $p = \sum_{i=1}^k f_i p_i + \text{Rest}$.

- ▶ Polynomideale als Kern von Homomorphismen
- ▶ Rechnen im Quotientenring

Buchberger's Algorithmus

- z. B. in $\mathbb{Q}[x, y, z]$
 - $p_1 = x^3yz - xz^2$
 - $p_2 = xy^2z - xyz$
 - $p_3 = x^2y^2 - z^2$

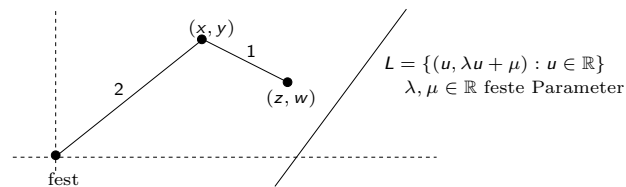
Frage: Liegt $q = x^2yz - z^3 \in \langle p_1, p_2, p_3 \rangle$.

Gegebenenfalls finde $f_1, f_2, f_3 \in \mathbb{Q}[x, y, z]$ mit $q = \sum_{i=1}^3 f_i p_i$.

- Spezialfall vom O -Äquivalenzproblem:
 - $q \approx 0 \pmod{\langle p_1, p_2, p_3 \rangle}$
 - \approx Kongruenz, die von $\mathfrak{i} = \langle p_1, p_2, p_3 \rangle$ induziert wird.
- $q_1 \approx_{\mathfrak{i}} q_2$ gdw $q_1 - q_2 \in \mathfrak{i}$

Beispiele

8.1 Beispiel Einfacher Roboter



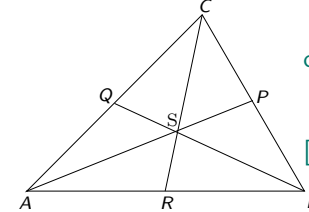
- Die möglichen Positionen $(x, y, z, w) \in \mathbb{R}^4$ des Roboters sind charakterisiert durch

$$(*) \quad x^2 + y^2 = 4 \qquad (z - x)^2 + (w - y)^2 = 1$$

- Frage: Kann der Roboter die Linie erreichen?
 - (*) muss erfüllt sein und $w = \lambda z + \mu$.

Beispiele

8.2 Beispiel Euklidische Geometrie: Die drei Medianen eines Δ schneiden sich in einem Punkt. Schnittpunkt drittelt jedes Median.



o.B.d.A.:

$$A = (0, 0) \quad B = (1, 0)$$

$$C = (x, y) \quad x, y \in \mathbb{R}$$

[da Satz invariant unter transl, rot., Skalierung]

- d.h. $P = ((x + 1)/2, y/2)$, $Q = (x/2, y/2)$, $R = (1/2, 0)$.
Sei $S = (u, v)$ Schnittpunkt AP und BQ .
- S liegt auf AP ist äquivalent zur Aussage \overline{AS} und \overline{AP} haben gleiche Steigung, d. h.
 $\frac{v}{u} = \frac{y/2}{(x+1)/2}$ $f_1 := uy - v(x + 1) = 0$
- S liegt auf \overline{BQ} analog $f_2 := (u - 1)y - v(x - 2) = 0$

Beispiele (Forts.)

- S liegt auch auf \overline{CR} :
 $g_1 := -2(u - x)y - (v - y)(1 - 2x)$
 $= -2uy - (v - y) + 2vx = 0$
- S drittelt die drei Medianen: d. h.
 - $(u, v) = \overline{AS} = 2\overline{SP} = (x + 1 - 2u, y - 2v)$
 - $(u - 1, v) = \overline{BS} = 2\overline{SQ} = (x - 2u, y - 2v)$
 - $(u - x, v - y) = \overline{CS} = 2\overline{SR} = (2u - 1, 2v)$
oder äquivalent dazu:
 - $g_2 := 3u - x - 1 = 0$
 - $g_3 := 3v - y = 0$
- Offenbar gilt $g_1 = -f_1 - f_2$, d. h. $g_1 = 0$ folgt aus $f_1 = f_2 = 0$, d. h. die drei Medianen schneiden sich in S .

Erinnerung: Grundlagen

- Sei F Körper $R = F[x_1, \dots, x_n]$ Polynomring in n -Variablen. $f_1, \dots, f_s \in R$. Die Polynome f_1, \dots, f_s erzeugen ideal I .

$$I = \langle f_1, \dots, f_s \rangle = \left\{ \sum_{1 \leq i \leq s} q_i f_i : q_i \in R \right\}$$

$$V(I) := \{u \in F^n : f(u) = 0 \text{ für alle } f \in I\} \quad \text{Die Varietät von } I \\ = \{u \in F^n : f_1(u) = \dots = f_s(u) = 0\}$$

- Schreibe $V(f_1, \dots, f_s)$ statt $V(\langle f_1, \dots, f_s \rangle)$.
- Fragen über Varietäten bzw. I :
 - Ist $V(I) \neq \emptyset$?
 - Ist $V(I)$ endlich?
 - Wortproblem: $f \in R$ gilt $f \in I$.
 - Trivialitätsproblem: Gilt $I = R$?

Beispiele (Forts.)

Fortsetzung Beispiel

$$g_1 = -f_1 - f_2 \in \langle f_1, f_2 \rangle \subseteq \mathbb{R}[u, v, x, y]$$

d.h. $V(f_1, f_2) \subseteq V(g_1)$

- S dreht Medianen: d.h. $AS = 2SP \quad BS = 2SQ \quad CS = 2SR$ oder

$$\begin{pmatrix} u - (x + 1 - 2u) \\ v - (y - 2v) \end{pmatrix} = \begin{pmatrix} u - 1 - (x - 2u) \\ v - (y - 2v) \end{pmatrix} =$$

$$\begin{pmatrix} u - x - (1 - 2u) \\ v - y + 2v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

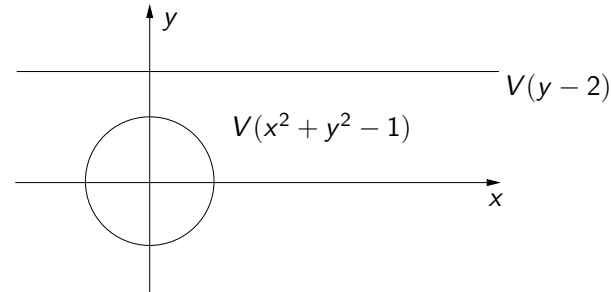
d.h. $g_2 = 3u - x - 1 = 0$ und $g_3 = 3v - y = 0$

- Zeige also $g_2, g_3 \in \langle f_1, f_2 \rangle$ oder $V(f_1, f_2) \subseteq V(g_2)$ und $V(g_3)$.

Beispiele (Forts.)

8.3 Beispiel

- Sei $f_1 = x^2 + y^2 - 1 \quad f_2 = y - 2 \in \mathbb{R}[x, y]$
 $I = \langle f_1, f_2 \rangle$. Dann
 $V(I) = \{(u, v) \in \mathbb{R}^2 : u^2 + v^2 - 1 = v - 2 = 0\}$
 $= \{(u, 2) \in \mathbb{R}^2 : u^2 = -3\} = \emptyset$



Beispiele (Forts.)

- Betrachtet man f_1, f_2 als Polynome in $\mathbb{C}[x, y]$ und $V(I)$ als Varietät über \mathbb{C}^2 , so

$$V(I) = \{(u, 2) \in \mathbb{C}^2 : u^2 = -3\} = \{(\sqrt{3}i, 2), (-\sqrt{3}i, 2)\}$$

- d.h. 2 Punkte (mit $i = \sqrt{-1} \in \mathbb{C}$).

- ii) Sei $f = (y^2 + 6)(x - 1) - y(x^2 + 1)$
 $g = (x^2 + 6)(y - 1) - x(y^2 + 1) \quad \text{in } \mathbb{C}[x, y]$
 $h = (x - 5/2)^2 + (y - 5/2)^2 - 1/2$

$$I = \langle f, g \rangle$$

Reduktionstechniken zur Lösung des Wortproblems (Forts.)

- ▶ Reduktionsrelation $\rightarrow \subseteq U \times U : a \rightarrow b$
 - Komposition $\rightarrow \circ \rightarrow' : a \rightarrow \rightarrow' b : a \rightarrow c \rightarrow' b$
 - Inverse Relation $\leftarrow : a \leftarrow b \text{ gdw } b \rightarrow a$
 - Symmetrischer Abschluß $\leftrightarrow : \rightarrow \cup \leftarrow$
 - Potenz $\rightarrow^i : \rightarrow^0 = id \rightarrow^{i+1} = \rightarrow^i \circ \rightarrow$
 - Transitive Hülle $\rightarrow^+ = \bigcup_{i=1}^{\infty} \rightarrow^i$
 - Reflex. trans. Hülle $\rightarrow^* = \bigcup_{i=0}^{\infty} \rightarrow^i$
 - Reflex. trans. symm. Hülle $\leftrightarrow^* \rightarrow$ **Äquivalenzrelation**
- i. Allg. \rightarrow rekursiv
- ▶ Spezialfälle: WP Monoide, WP Gruppen
 - $B = \langle a, b; ab = 1 \rangle$ monoid (byzykl. Monoid)
 - $G = \langle \{a, b\} \mid \{a^2, b^2, aba^{-1}b^{-1}\} \rangle$

Reduktionstechniken zur Lösung des Wortproblems (Forts.)

- ▶ R kommutativer Ring $I \subseteq R$ ideal
 - gdw $p, q \in I \rightsquigarrow p - q \in I \quad p \in I, r \in R \rightsquigarrow rp \in I$.
- ▶ $R[x_1, \dots, x_n]$, R Ring (i.A. kommutativ), $I = \langle p_1, \dots, p_m \rangle$ von p_1, \dots, p_m erzeugt Ideal in $R[x_1, \dots, x_n]$.
 - $f, g \in R[x_1, \dots, x_n]$, $f \equiv g \pmod{I}$
 - oder $f - g \in I$, d.h. f, g stellen gleiche Elemente im Quotientenring $R[x_1, \dots, x_n]/I$ dar.
- ▶ Idee: Finde Reduktionsrelation \rightarrow_I mit
 - $\leftrightarrow_I^* \equiv \equiv_I$

Reduktionstechniken zur Lösung des Wortproblems (Forts.)

- ▶ Standardbegriffe für \rightarrow Reduktionsrelation:
 - ▶ $x \rightarrow$ x ist reduzibel d. h. $\exists y : x \rightarrow y$
 - ▶ \underline{x} x ist irreduzibel oder in Normalform
 - ▶ $x \downarrow y$ ($x \uparrow y$) x, y haben gemeinsamen direkten Nachfolger / Vorgänger, d.h.
 - $\exists z : x \rightarrow z \leftarrow y / x \leftarrow z \rightarrow y$
 - ▶ x ist eine \rightarrow -Normalform von y gdw $y \rightarrow^* \underline{x}$
 - Wichtige Eigenschaften von \rightarrow :**
 - ▶ **Noethersch:**
 - Jede Reduktionsfolge terminiert
 - d. h. es gibt keine ∞ Folge $x_1 \rightarrow x_2 \rightarrow \dots$
 - ▶ **Church Rosser** $a \xrightarrow{*} b \rightsquigarrow a \downarrow_* b$
 - ▶ **konfluent** $a \uparrow^* b \rightsquigarrow a \downarrow^* b$
 - ▶ **lokal-konfluent** $a \uparrow b \rightsquigarrow a \downarrow^* b$

Reduktionstechniken zur Lösung des Wortproblems (Forts.)

8.4 Satz \rightarrow noethersch und Church Rosser, so WP für \leftrightarrow^* entscheidbar.
 d.h. Kanonische Simplifikationsfunktion
 $x \mapsto y$ mit $x \xrightarrow{*} \underline{y}$ NF für x (**Beachte \rightarrow effektiv**).

8.5 Beispiel

- 1) Kommutative Halbgruppe mit Erzeugenden a, b, c, f, s . Relationen

$$as = c^2s \quad bs = cs \quad s = f \quad :: E$$

Reduktionsrelation auf der freien kommutativen Halbgruppe in a, b, c, f, s

$$R : \quad s \rightarrow f \quad cf \rightarrow bf \quad b^2f \rightarrow af$$

auf Wörter in $a, b, c, f, s : u \rightarrow v$, so $ut \rightarrow vt$.

\rightarrow_R ist noethersch, Church-Rosser und äquivalent zu E .

$$a^3bcf^3 =_E a^2b^4fs^2$$

Reduktionstechniken: Beispiel (Forts.)

- 2) I ideal in $\mathbb{Q}[x, y]$ erzeugt von $x^3 - x^2 \quad x^2y - x^2$
 → Def. auf $\mathbb{Q}[x, y]$: Jedes "Vorkommen" von x^3 oder x^2y kann durch x^2 ersetzt werden.

Behauptung: → ist noethersch + Church Rosser.

8.6 Satz

- a) → Church Rosser gdw → konfluent.
 - b) Newman Lemma. Sei → noethersch:
 → konfluent gdw → lokal konfluent.
- Verbunden unterhalb.

Termordnungen

- **Partialordnung** $<$ auf S ist eine irreflexive transitive Relation $< \subseteq S \times S$.
 d.h. $\neg(\alpha < \alpha) \wedge \alpha < \beta < \gamma \Rightarrow \alpha < \gamma$ für alle $\alpha, \beta, \gamma \in S$
 d. h. $<$ ist asymmetrisch.
- Partialordnung ist **total**, falls $\alpha = \beta \vee \alpha < \beta \vee \beta < \alpha \quad (\alpha, \beta \in S)$.
- Ordnung ist eine **Wohlordnung**, falls jede nicht leere Menge ein kleinstes Element besitzt.
- Schreibe $\alpha \leq \beta$, falls $\alpha = \beta$ oder $\alpha < \beta$.
- $<$ auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind total, **nur** auf \mathbb{N} Wohlordnung.
- $X = \{x_1, \dots, x_n\}$: freie kommutative Halbgruppe (Monoid) über X **ist die Menge der Terme** über X .
 Darstellung der Terme:: Sei $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$.
Identifikation $\alpha \rightarrow x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in F[x_1, \dots, x_n]$,
 d. h. $\mathbb{N}^n \simeq$ Menge der Terme über $X := T(X)$. Operationen: $\cdot, |, KGV, ..$

Termordnungen

8.7 Definition Eine **Termordnung** auf $T(X)$ ist eine Relation \prec auf \mathbb{N}^n mit

- i) \prec ist totale Ordnung.
- ii) $\alpha \prec \beta \Rightarrow \alpha + \gamma \prec \beta + \gamma$ für alle $\alpha, \beta, \gamma \in \mathbb{N}^n$
 ($s \prec t \Rightarrow su < tu$ für alle $s, t, u \in T(X)$ kompatibel mit Multiplikation)
- iii) \prec ist Wohlordnung

!(insbesondere $1 = x_1^0 \cdots x_n^0 \prec t$ für alle $t \in T(X) \setminus \{1\}$.)!

- Falls i) gilt so ist iii) äquivalent zu, es gibt keine ∞ -fallende Ketten.
- $n = 1$ Standard Ordnung auf \mathbb{N} ist die übliche Grad Ordnung auf $T(X)$.

Beispiel: Termordnungen

8.8 Beispiel 3 Standard Termordnungen

- i) **Lexikographische Ordnung**
 - $\alpha \prec_{lex} \beta$ gdw erste nicht Null-Eintrag in $\alpha - \beta$ ist negativ (von links).
 (Entspricht **Präzedenz** $x_1 \succ x_2 \succ \cdots \succ x_n$).
 - $n = 3 \quad \alpha_1 = (0, 4, 0) \quad \alpha_2 = (1, 1, 2) \quad \alpha_3 = (1, 2, 1) \quad \alpha_4 = (3, 0, 0)$.
 Dann $\alpha_1 \prec_{lex} \alpha_2 \prec \alpha_3 \prec \alpha_4$.
- ii) **Graduierte lexikographische Ordnung:**
 $\alpha = (\alpha_1, \dots, \alpha_n) \quad \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$
 - $\alpha \prec_{grlex} \beta$ gdw $\sum_{1 \leq i \leq n} \alpha_i < \sum_{1 \leq i \leq n} \beta_i$ oder $(\sum \alpha_i = \sum \beta_i \wedge \alpha \prec_{lex} \beta)$
 (oft noch mit **Gewichtsfunktion** $W : \{1, \dots, n\} \rightarrow \mathbb{R}^+$).
 - Es gilt $\alpha_4 \prec_{grlex} \alpha_1 \prec_{grlex} \alpha_2 \prec_{grlex} \alpha_3$.

Beispiel: Termordnungen (Fort.)

iii) **Graduierte inverse lexikographische Ordnung:**

▶ $\alpha \prec_{grevlex} \beta$ gdw $\sum_{1 \leq i \leq n} \alpha_i < \sum_{1 \leq i \leq n} \beta_i$ oder
 $(\sum \alpha_i = \sum \beta_i \wedge$ am weitesten rechts stehende nicht Null-Eintrag in $\alpha - \beta$ ist positiv).

▶ Es gilt $\alpha_4 \prec_{grevlex} \alpha_2 \prec_{grevlex} \alpha_3 \prec_{grevlex} \alpha_1$.

↔ $n = 1 \quad \prec_{lex} = \prec_{grlex} = \prec_{grevlex}$.

↔ $f = 4xyz^2 + 4x^3 - 5y^4 + 7xy^2z \in \mathbb{Q}[x, y, z]$
 $lex : 4x^3 + 7xy^2z + 4xyz^2 - 5y^4$
 $grlex : 7xy^2z + 4xyz^2 - 5y^4 + 4x^3$.

Termordnungen: Zentrales Lemma

8.9 Lemma

a) $\prec_{lex}, \prec_{grlex}, \prec_{grevlex}$ sind Termordnungen.

b) $s, t \in T[X], s \mid t$ dann ist $s \preceq t$ für jede Termordnung \prec .

c) Die antilexikographische Ordnung \prec_{alex} auf \mathbb{N}^2 mit $\alpha \prec_{alex} \beta$ gdw $\beta \prec_{lex} \alpha$ ist Ordnung für die Bedingung iii) nicht gilt.

z. B. $S = \mathbb{N} \times \{0\}$ hat kein kleinstes Element, da $(0, 0) \succ_{alex} (1, 0) \succ_{alex} (2, 0) \succ \dots$

Wichtige Begriffe für Polynome und deren Reduktion

8.10 Definition Sei $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha \in R = K[x_1, \dots, x_n], f \neq 0$.
 $c_\alpha \in F$ (nur endlich viele $\neq 0$), \prec Termordnung.

- i) $c_\alpha x^\alpha$ ist **Monom** in f für $c_\alpha \neq 0$ **Coeff**(f, α) = c_α .
- ii) Der **Multigrad** von f ist $mdeg(f) = \max_{\prec} \{\alpha \in \mathbb{N}^n : c_\alpha \neq 0\}$
- iii) $LT(f) := x^{mdeg(f)} = \max_{\prec} \{t \in T[X] \mid \text{Coeff}(f, t) \neq 0\}$
Leitterm (Hauptterm) von f .
- iv) $LC(f) := c_{mdeg(f)} \in F \setminus \{0\}$ **Leitkoeffizient**.
- v) $LM(f) = LC(f) \cdot LT(f) \in R$ **Leitmonom**.
- vi) $Red(f) = f - LM(f)$ **Redukt von f** .

Beispiel

↔ \prec induziert noethersche Partialordnung \ll auf R : (**Beweis!**)

- ▶ $f \ll g$ gdw $f = 0$ und $g \neq 0$ oder
- ▶ $f \neq 0, g \neq 0 \wedge LT(f) \prec LT(g)$ oder
- ▶ $f \neq 0, g \neq 0 \wedge LT(f) = LT(g) \wedge Red(f) \ll Red(g)$

8.11 Beispiel Sei $f = 4xyz^2 + 4x^3 - 5y^4 + 7xy^2z \in \mathbb{Q}[x, y, z]$

$mdeg(f)$	\prec_{lex} (3, 0, 0)	\prec_{grlex} (1, 2, 1)	$\prec_{grevlex}$ (0, 4, 0)
$LC(f)$	4	7	-5
$LT(f)$	x^3	xy^2z	y^4
$LM(f)$	$4x^3$	$7xy^2z$	$-5y^4$

Lemma

8.12 Lemma Sei \prec Termordnung auf $T[X]$, $f, g \in R \setminus \{0\}$.

- i) $\text{mdeg}(fg) = \text{mdeg}(f) + \text{mdeg}(g)$
 $(LT(fg) = LT(f) \circ LT(g) \text{ in } T[X])$
- ii) $f + g \neq 0$ so $\text{mdeg}(f + g) \leq \max\{\text{mdeg}(f), \text{mdeg}(g)\}$
 d. h. $LT(f + g) \leq \max\{LT(f), LT(g)\}$
 Gleichheit, falls $\text{mdeg}(f) \neq \text{mdeg}(g)$.

- ▶ Verallgemeinerung der Division mit Rest: **Reduktion**
- ▶ $f, f_1, \dots, f_s \in R$ gesucht Darstellung von f mit $f = q_1 f_1 + \dots + q_s f_s + r$ mit $q_1, \dots, q_s, r \in R$.
- ? Wie bestimmt man q_i , welche Eigenschaften hat r ?

Beispiel

8.13 Beispiel

a) Sei $\prec = \prec_{lex}$ $f = xy^2 + 1$ $f_1 = xy + 1$ $f_2 = y + 1$

	$xy + 1$	$y + 1$
$xy^2 + 1$	y	
$-(xy^2 + y)$		
$-y + 1$		-1
$-(-y - 1)$		
2		

$$f = y f_1 - 1 \cdot f_2 + 2$$

- ▶ Kein Term in 2 bzw. $-x + 1$ ist durch ein $LT(f_i)$ teilbar.

b) Sei $\prec = \prec_{lex}$ $f = x^2 y + xy^2 + y^2$ $f_1 = xy - 1$ $f_2 = y^2 - 1$

	$xy - 1$	$y^2 - 1$	Rest
$x^2 y + xy^2 + y^2$	x		
$-(x^2 y - x)$			
$xy^2 + x + y^2$	y		
$-(xy^2 - y)$			
$x + y^2 + y$			x
$-x$			
$y^2 + y$		1	
$-(y^2 - 1)$			
$y + 1$			

$$f = (x + y) \cdot f_1 + 1 \cdot f_2 + (x + y + 1)$$

- ▶ Kein Term in $x + y + 1$ durch ein $LT(f_i)$ teilbar.

Polynom-Reduktion

procedure Algorithmus multivariate Division mit Rest

{Eingabe: Polynome $f, f_1, \dots, f_s \in R = F[x_1, \dots, x_n]$, F Körper}
 {Termordnung \prec auf $T[x]$.}

{Ausgabe: $q_1, \dots, q_s, r \in R$ mit $f = q_1 f_1 + \dots + q_s f_s + r$.}
 {Kein Monom in r ist durch ein $LT(f_1), \dots, LT(f_s)$ teilbar.}

begin

1 $r := 0; p := f;$

for $i = 1, \dots, s$ do $q_i := 0$

2 **while** $p \neq 0$ **do**

3 if $LM(f_i) \mid LM(p)$ für ein $i \in \{1, \dots, s\}$

then choose some such $i: q_i := q_i + \frac{LM(p)}{LM(f_i)}; p := p - \frac{LM(p)}{LM(f_i)} f_i;$

else $r := r + LM(p); p := p - LM(p)$

4 **return** q_1, \dots, q_s, r

end

Polynom-Reduktion (Forts.)

8.14 Satz Bei Schritt 3 gelten folgende Invarianten

i) $mdeg(p) \preceq mdeg(f) \quad f = p + q_1 f_1 + \dots + q_s f_s + r.$

ii) $q_i \neq 0 \Rightarrow mdeg(q_i f_i) \preceq mdeg(f) \quad 1 \leq i \leq s.$

iii) Kein Term in r ist teilbar durch ein $LM(f_i)$.

▶ Ist p_j der Wert von p in Durchgang j , so $p_{j+1} \prec p_j$.

▶ Der Algorithmus terminiert

Frage: Platz und Zeit Bedarf für den Algorithmus? Wovon hängen diese ab?.

Einschrittreduktion mit einer Menge $P = \{f_1, \dots, f_s\}$

▶ **Einschritt Reduktionsrelation:** $f, g, h \in K[X] \quad g \xrightarrow{f} h$

g reduziert sich nach h mit f gdw. es gibt $s, t \in T[X]$
 $\text{Coeff}(g, s) = c \neq 0 \quad s = \text{LT}(f)t$ (d.h. $\text{LT}(f) \mid s$) und

$$h = g - \frac{c}{\text{LC}(f)} \cdot t \cdot f \quad \text{Ein „Monom“ in } g \text{ wird ersetzt}$$

▶ $g \xrightarrow{P} h$ gdw $\exists f_i \in P \quad g \xrightarrow{f_i} h$

▶ \xrightarrow{P}^* , \xleftarrow{P}^* wie üblich.

▶ **Beachte:** Multivariate Division mit Rest liefert ein r mit $r \xrightarrow{P}$ irreduzibel und $g \xrightarrow{P}^* r$. **Strategie: Left-Most-Reduktion.**

▶ Es gilt $\xleftarrow{P}^* = \equiv_{\langle P \rangle}$ (Übung)

Beispiel

8.15 Beispiel $\prec = \prec_{lex}$, $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$
 f ist mit f_1 reduzibel in x^2y und xy^2
 f ist mit f_2 reduzibel in xy^2 und y^2

	$xy - 1$	$y^2 - 1$	Rest
$x^2y + xy^2 + y^2$	x	x	$x^2y + xy^2 + y^2$
$-(x^2y - x)$			$-(xy^2 - x)$
$xy^2 + x + y^2$	y	1	$x^2y + y^2 + x$
$-(xy^2 - y)$			$-(y^2 - 1)$
$x + y^2 + y$	x		$x^2y + x + 1$
$-x$			$-(x^2y - x)$
$y^2 + y$		1	
$-(y^2 - 1)$			
$x + y + 1$			$2x + 1$

d.h. Rest muss nicht eindeutig sein, d. h. i. Allg. keine Konfluenz.

Beispiel (Forts.)

Beachte i. Allg. **Wahl von i** mit $HT(f_i) \mid HT(P)$. Wähle kleinstes $i \rightsquigarrow$ die Quotienten q_1, \dots, q_s und der Rest r sind eindeutig festgelegt, schreibe $r = f \text{ rem}(f_1, \dots, f_s)$ für diese Wahl.

Gewünscht wird:

- ▶ $f \in \langle f_1, \dots, f_s \rangle$ gdw $r = f \text{ rem}(f_1, \dots, f_s) = 0$
 - ▶ Dies stimmt, falls $s = 1$ ist.
 - ▶ Für $s \geq 2$ für Gröbner Basen! Sonst i. Allg. nicht
- ▶ " \Leftarrow " stimmt aber \Rightarrow nicht.

8.16 Beispiel $f = xy^2 - x$, $f_1 = xy + 1$, $f_2 = y^2 - 1$
 $xy^2 - x \xrightarrow{f_1} -x - y = r$, d. h. $f = yf_1 + 0f_2 + (-x - y)$,
 aber $f = 0f_1 + xf_2 + 0$, d. h. $f \in \langle f_1, f_2 \rangle$.

Term-Ideale und Hilbert's Basissatz

8.17 Definition Ein **Termideal** $I \subseteq R = F[x_1, \dots, x_n]$ ist ein von Terme erzeugtes Ideal in R , d. h. es gibt eine Teilmenge $A \subseteq \mathbb{N}^n$ mit

$$I = \langle x^A \rangle = \langle \{x^\alpha : \alpha \in A\} \rangle$$

D.h. es wird von **Monomen** mit Koeffizienten 1 erzeugt.

8.18 Lemma Sei $I = \langle x^A \rangle \subseteq R$ Termideal, $\beta \in \mathbb{N}^n$, dann

$$x^\beta \in I \text{ gdw } \exists \alpha \in A : x^\alpha \mid x^\beta$$

Beweis: " \Leftarrow " klar, " \Rightarrow " sei $x^\beta \in I$, dann

$x^\beta = \sum_{i \in E} q_i x^{\alpha_i}$ für eine endliche Menge E mit $q_i \in R = F[x_1, \dots, x_n]$. Jeder Term, der in der rechten Summe vorkommt, ist teilbar durch ein $\alpha \in A$. x^β muss als Term in der rechten Seite vorkommen, also folgt die Behauptung.

Term-Ideale und Hilbert's Basissatz (Forts.)

8.19 Lemma Sei $I \subseteq R = F[x_1, \dots, x_n]$ **Termideal**, $f \in R$, dann sind äquivalent

- i) $f \in I$.
- ii) Jedes Monom von f liegt in I .
- iii) f ist eine F -Linearkombination von Terme in I .

Beweis:

i) \Rightarrow ii) nach Voraussetzung $f = \sum_{i \in E} q_i x^{\alpha_i} \quad \alpha_i \in A$.

Jeder Term in f ist teilbar durch ein x^γ mit $\gamma \in A$ also ist jedes Monom von f in I .

ii) \Rightarrow iii) \Rightarrow i) klar. (gilt sogar für beliebige Ideale).

Term-Ideale und Hilbert's Basissatz (Forts.)

8.20 Beispiel $I = \langle x^3, x^2y \rangle \subseteq \mathbb{Q}[x, y] \rightsquigarrow 3x^4 + 5x^2y^3 \in I$
 $2x^4y + 7x^2 \notin I$.

Die Implikation i) \Rightarrow ii) ist i. Allg. falsch. z. B.

$g = x^3 - 2xy, h = x^2y - 2y^2 + x, I = \langle g, h \rangle$
 $x^2 = -yg + xh$, dann $x^2 \in \langle LT(I) \rangle, x^2 \notin \langle LT(g), LT(h) \rangle$.

8.21 Folgerung Gleichheit von Termidealen::

Zwei Termideale sind gleich gdw sie enthalten die gleichen Terme.

8.22 Satz Dickson's Lemma

Termideale sind endlich erzeugt, d.h. für $A \subseteq \mathbb{N}^n$ gibt es eine endliche Teilmenge $B \subseteq A$ mit $\langle x^A \rangle = \langle x^B \rangle$.

Beweis: $A = \emptyset$ so klar. Sei $A \neq \emptyset$.

Dickson's Lemma (Forts.)

- ▶ Betrachte \leq auf \mathbb{N}^n mit $\alpha \leq \beta$ gdw $\alpha_i \leq \beta_i, 1 \leq i \leq n$ (d. h. $x^\alpha \mid x^\beta$).
 Schreibe $\alpha < \beta$, falls $\alpha \leq \beta$ und $\alpha \neq \beta$.
- ▶ $<$ ist Partialordnung auf \mathbb{N}^n die i. Allg. nicht total ist $n \neq 1$.
- ▶ Sei $B = \{\alpha \in A : \forall \beta \in A, \beta \not< \alpha\}$ die Menge der minimalen Elemente von A bzgl. $<$.

Behauptung: B ist endlich, $B \subseteq A$,

$$(*) \quad \forall \alpha \in A \quad \exists \beta \in B, \beta \leq \alpha$$

- ▶ Für $\alpha \in \mathbb{N}^n$ gibt es nur endlich viele $\beta \in \mathbb{N}^n$ mit $\beta \leq \alpha$.
 d.h. Es gibt keine ∞ fallende Kette

$$\alpha^{(1)} > \alpha^{(2)} > \alpha^{(3)} > \dots \text{ in } \mathbb{N}^n$$

- ▶ Insbesondere folgt (*).

Dickson's Lemma (Forts.)

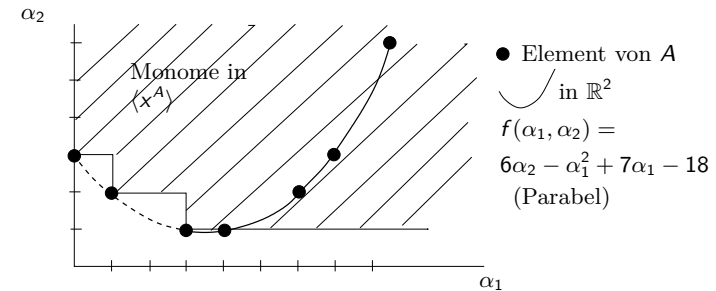
- ▶ z. Z. B ist endlich. Induktion nach n .
 - ▶ $n = 1$, dann ist \prec total $B = \{\text{kleinstes Element von } A\}$.
 - ▶ $n \geq 2$, sei $A^* = \{(\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{N}^{n-1} : \exists \alpha_n \in \mathbb{N} : (\alpha_1, \dots, \alpha_n) \in A\}$ nach Induktionvoraussetzung ist die Menge B^* der minimalen Elemente von A^* endlich.
- ▶ Für jedes $\beta = (\beta_1, \dots, \beta_{n-1}) \in B^*$ wähle $b_\beta \in \mathbb{N}$ mit $(\beta_1, \dots, \beta_{n-1}, b_\beta) \in A$ und sei $b = \max\{b_\beta : \beta \in B^*\}$.
- ▶ **Behauptung:** $(\alpha_1, \dots, \alpha_n) \in B$, so $\alpha_n \leq b$.
- ▶ Sei $\alpha = (\alpha_1, \dots, \alpha_n) \in A$, dann gibt es ein minimales Element $\beta = (\beta_1, \dots, \beta_{n-1}) \in B^*$ von A^* mit $\beta \leq (\alpha_1, \dots, \alpha_{n-1})$.

Dickson's Lemma (Forts.)

- ▶ Ist $\alpha_n > b$, so $(\beta_1, \dots, \beta_{n-1}, b_\beta) \leq (\beta_1, \dots, \beta_{n-1}, b) < \alpha$
 α ist nicht minimal, d. h. $\alpha_n \leq b$.
- ▶ Analog zeigt man, dass alle Komponenten beschränkt sind, es gibt nur endlich viele $(\alpha_1, \dots, \alpha_n) \in B$.
- ▶ $\alpha \leq \beta$ gdw $x^\alpha \mid x^\beta \rightsquigarrow x^\alpha \subseteq \langle x^\beta \rangle$ und somit $\langle x^\alpha \rangle \subseteq \langle x^\beta \rangle$.
 \supseteq folgt aus $B \subseteq A$.
- ▶ Beachte: Ideale können auch in Monoiden betrachtet werden. Ideale in e.e. kommutativen Monoiden sind endlich erzeugt (als Ideal).

Beispiel

8.23 Beispiel $n = 2$, $A = \{(\alpha_1, \alpha_2) \in \mathbb{N}^2 : 6\alpha_2 = \alpha_1^2 - 7\alpha_1 + 18\}$
 Die Menge der minimalen Elemente ist $B = \{(0, 3), (1, 2), (3, 1)\}$, d. h. $\langle x^A \rangle = \langle y^3, xy^2, x^3y \rangle$



Folgerung

- 8.24 Folgerung** Sei \prec eine totale Ordnung auf \mathbb{N}^n mit $\forall \alpha, \beta, \gamma \in \mathbb{N}^n, \alpha \prec \beta \Rightarrow \alpha + \gamma \prec \beta + \gamma$.
- ▶ \prec ist wohlfundiert gdw $\alpha \succeq 0$ für $\alpha \in \mathbb{N}^n$.
 - Beweis:** " \Leftarrow " $A \subseteq \mathbb{N}^n, A \neq \emptyset, I = \langle x^A \rangle \subseteq R$ ist endlich erzeugt nach Dickson's Lemma, d. h. $\exists \alpha_1, \dots, \alpha_s \in A$:
 $I = \langle x^{\alpha_1}, \dots, x^{\alpha_s} \rangle$ seien sie als $\alpha_1 \prec \alpha_2 \prec \dots \prec \alpha_s$ geordnet.
 Behauptung $\min_{\prec} A = \alpha_1$.
 ▶ Sei $\alpha \in A$ beliebig, da $x^\alpha \in I \exists i \leq s, \gamma \in \mathbb{N}^n : \alpha = \alpha_i + \gamma$, d. h. $\alpha = \alpha_i + \gamma \succeq \alpha_1 + \gamma \succeq \alpha_1 + 0 = \alpha_1 \rightsquigarrow \alpha_1 = \min_{\prec} A$.
 - ▶ D.h. die Bedingung iii) der Termordnungen kann durch (iii)* $\forall \alpha \in \mathbb{N}^n, \alpha \succeq 0$ ersetzt werden.

Notation-Beispiel

Schreibweise: $G \subseteq R = F[x_1, \dots, x_n]$

$$LM(G) = \{LM(g) : g \in G\}, \quad LT(G) = \{LT(g) : g \in G\}$$

- Ist $I \subseteq R$ ideal, dann gibt es eine endliche Teilmenge $G \subseteq I$ mit $\langle LT(G) \rangle = \langle LT(I) \rangle$ nach Dickson's Lemma.

- Es kann aber endliche Mengen G die I erzeugen geben mit

$$\langle LT(G) \rangle \subsetneq \langle LT(I) \rangle$$

- Beispiel: $g = x^3 - 2xy$ $h = x^2y - 2y^2 + x$ \prec_{grlex}
 $G = \{g, h\}$ $I = \langle G \rangle$ $x^2 = -yg + xh$, d. h.
 $x^2 \in \langle LT(I) \rangle$, aber $x^2 \notin \langle LT(G) \rangle = \langle x^3, x^2y \rangle$.

Hilbert's Basissatz

8.25 Lemma Sei I ideal in $R = F[x_1, \dots, x_n]$.

Ist $G \subseteq I$ endlich mit $\langle LT(G) \rangle = \langle LT(I) \rangle$, so gilt $\langle G \rangle = I$.

Beweis: Sei $G = \{g_1, \dots, g_s\}$ $f \in I$ beliebig.

Division mit Rest liefert

- $f = q_1g_1 + \dots + q_sg_s + r$ mit $q_1, \dots, q_s, r \in R$.
Wobei $r = 0$ oder kein Term in r ist durch $LT(f_i)$ für ein i teilbar.

- $r = f - q_1g_1 - \dots - q_sg_s \in I \rightsquigarrow LT(r) \in LT(I) \subseteq \langle LT(G) \rangle$.

- Wegen Lemma 8.18 folgt $r = 0$. Also $f \in \langle g_1, \dots, g_s \rangle = \langle G \rangle$.

8.26 Satz Hilbert's Basissatz

Jedes Ideal I in $R = F[x_1, \dots, x_n]$ ist endlich erzeugt. **Genauer**, es gibt endliche Teilmenge $G \subseteq I$ mit $\langle G \rangle = I$ und $\langle LT(G) \rangle = \langle LT(I) \rangle$.

- Dickson's Lemma angewendet auf $\langle LT(I) \rangle$.

Folgerungen

8.27 Folgerung Aufsteigende Kettenbedingung (E.Noether)

Sei $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ eine aufsteigende Kette von Idealen in R . Dann gibt es ein n mit

$$I_n = I_{n+1} = I_{n+2} = \dots \text{ für ein } n \in \mathbb{N}.$$

Beweis: $I = \bigcup_{j \geq 1} I_j$ ist ideal, endlich erzeugt d. h.

$$I = \langle g_1, \dots, g_s \rangle. \text{ Wähle } n = \min\{j \geq 1, g_1, \dots, g_s \in I_j\}.$$

- Ringe die diese Bedingung erfüllen heißen **noethersch**, d. h. $F[x_1, \dots, x_n]$ ist noethersch.

- Allgemeiner gilt: Ist R noethersch so auch $R[x]$.

Gröbnerbasen bezüglich Termordnungen

8.28 Definition Sei \prec eine Termordnung und $I \subseteq R$ ein Ideal. Eine endliche Teilmenge $G \subseteq I$ heißt **Gröbner Basis** für I bzgl. \prec , falls $\langle LT(G) \rangle = \langle LT(I) \rangle$.

Beachte: Jede Gröbner Basis für I ist eine Idealbasis von I nach Lemma 8.25, es gilt

$$f \in I \text{ gdw } r = f \text{ rem}(G) = 0 \\ \text{gdw } f \xrightarrow{*}_G 0$$

- d. h. $\xrightarrow{*}_G$ ist konfluent auf I .

8.29 Folgerung Jedes Ideal I in $R = F[x_1, \dots, x_n]$ hat eine Gröbner Basis (Satz 8.26 Hilbert's Basissatz).

8.30 Beispiel $g = x^3 - 2xy$, $h = x^2y - 2y^2 + x$ ist **keine** G -Basis von $\langle g, h \rangle$.

Konfluenz von \xrightarrow{G} für Gröbner Basen

8.31 Lemma Sei G G -Basis für $I \subseteq R$, $f \in R$.
 Dann gibt es ein **eindeutiges Polynom** $r \in R$ mit

- i) $f - r \in I$.
- ii) Kein Monom in r ist teilbar durch ein Element in $LT(G)$.

Beweis:

- **Existenz** folgt aus Algorithmus multivariate Division mit Rest.
- **Eindeutigkeit:** Angenommen $f = h_1 + r_1 = h_2 + r_2$ $h_1, h_2 \in I$.
 Kein Monom in r_1, r_2 ist teilbar durch ein Element in $LT(G)$.
 $r_1 - r_2 = h_2 - h_1 \in I \rightsquigarrow LM(r_1 - r_2)$ ist teilbar durch $LT(G)$ mit $g \in G$
 nach Lemma 8.18 $\rightsquigarrow r_1 - r_2 = 0$.

Konfluenz von \xrightarrow{G} für Gröbner Basen (Forts.)

► **Folgerung:** Wir können für Gröbnerbasen G schreiben
 $f \text{ rem } G = r \in R$
 r ist die **einzige Normalform** von f bzgl. \xrightarrow{G} .

► $\rightsquigarrow \xrightarrow{G}$ ist konvergent.

8.32 Satz Sei G Gröbner-Basis für $I \subseteq R$ bzgl. Termordnung \prec , $f \in R$.

- $f \in I$ gdw $f \text{ rem } G = 0$ gdw $f \xrightarrow{*}_G 0$.

Umgekehrt: Falls diese Eigenschaft für G gilt, so ist G eine Gröbner Basis (**Beweis!**).

Beachte: Beweis von Hilbert's Basissatz **nicht konstruktiv**, auch Dickson's Lemma liefert uns keine Konstruktion für die Menge der minimalen Elemente für $A = \{\alpha : x^\alpha \in \langle LT(I) \rangle\}$.

S-Polynome: Konfluenztest

8.33 Definition

Seien $g, h \in R$ nicht Null, $\alpha = (\alpha_1, \dots, \alpha_n) = \text{mdeg}(g)$,
 $\beta = (\beta_1, \dots, \beta_n) = \text{mdeg}(h)$ und $\gamma = (\max\{\alpha_1, \beta_1\}, \dots, \max\{\alpha_n, \beta_n\})$
 das **S-Polynom** von g und h ist

$$S(g, h) = \frac{x^\gamma}{LM(g)}g - \frac{x^\gamma}{LM(h)}h \in R$$

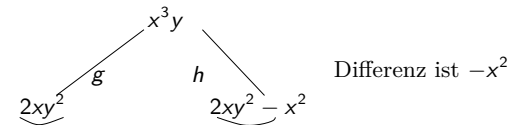
- Offenbar $S(g, h) = -S(h, g)$.
- Da $\frac{x^\gamma}{LM(g)}, \frac{x^\gamma}{LM(h)} \in R$ gilt, folgt $S(g, h) \in \langle g, h \rangle$.
- **Beachte:** $LT(S(g, h)) \prec x^\gamma$.
 (Wichtig für Noethersche Induktionsbeweise nach \prec).

S-Polynome: Konfluenztest (Forts.)

8.34 Beispiel $g = x^3 - 2xy$ $h = x^2y - 2y^2 + x \in \mathbb{Q}[x, y] \prec_{grlex}$

$\hookrightarrow \alpha = (3, 0), \beta = (2, 1), \gamma = (3, 1)$

$$\bullet S(g, h) = \frac{x^3y}{x^3}g - \frac{x^3y}{x^2y}h = y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2$$



- Um Konfluenz auf $\langle g, h \rangle$ zu erreichen müssen S-Polynome sich nach 0 reduzieren lassen. **Frage:** Folgt aus $u - v \xrightarrow{*}_{\langle g, h \rangle} 0$ auch $u \downarrow_{\langle g, h \rangle}^* v$
- Die Leitmonome bei Linearkombinationen können sich wegheben, dieses kann durch die S-Polynome charakterisiert werden.

S-Polynome: Hauptlemma

8.35 Lemma Sei $g_1, \dots, g_s \in R$, $\alpha_1, \dots, \alpha_s \in \mathbb{N}^n$, $c_1 \dots c_s \in F \setminus \{0\}$

► $f = \sum_{1 \leq i \leq s} c_i x^{\alpha_i} g_i \in R$ und

► $\delta \in \mathbb{N}^n$ mit $\alpha_i + \text{mdeg}(g_i) = \delta$ für $1 \leq i \leq s$ und $\text{mdeg}(f) < \delta$ (d. h. x^δ ist nicht Leitterm von f).

Dann gilt $x^{\gamma_{ij}}$ teilt x^δ für $1 \leq i < j \leq s$ wobei $x^{\gamma_{ij}} = \text{KGV}(LT(g_i), LT(g_j))$ und es gibt $c_{ij} \in F$ mit

$$(*) \quad f = \sum_{1 \leq i < j \leq s} c_{ij} x^{\delta - \gamma_{ij}} S(g_i, g_j)$$

und $\text{mdeg}(x^{\delta - \gamma_{ij}} S(g_i, g_j)) < \delta$ für alle $1 \leq i < j \leq s$.

S-Polynome: Hauptlemma-Beweis

Beweis: O.b.d.A. $LC(g_i) = 1$ (sonst verändere die c_i) und somit $LT(g_i) = LM(g_i) = x^{\text{mdeg}(g_i)}$ für alle i .

► Sei $1 \leq i < j \leq s$. Der Term $x^\delta = x^{\alpha_i} LT(g_i) = x^{\alpha_j} LT(g_j)$ ist gemeinsamer Vielfacher von $LT(g_i)$ und $LT(g_j)$

↔ d. h. $x^{\gamma_{ij}} \mid x^\delta$ und $\alpha_i + \text{mdeg}(g_i) = \alpha_j + \text{mdeg}(g_j) = \delta$
Wegen

$$S(g_i, g_j) = \frac{x^{\gamma_{ij}}}{LT(g_i)} g_i - \frac{x^{\gamma_{ij}}}{LT(g_j)} g_j$$

► Also $\text{mdeg}(S(g_i, g_j)) < \gamma_{ij}$, da die Leiterte in dieser Summe sich wegheben, es gilt somit

► $\text{mdeg}(x^{\delta - \gamma_{ij}} S(g_i, g_j)) = \delta - \gamma_{ij} + \text{mdeg}(S(g_i, g_j)) < \delta - \gamma_{ij} + \gamma_{ij} = \delta$

► (*) Wird nun durch Induktion nach s bewiesen.

- $s = 1$ nicht möglich, **Behauptung richtig.**

S-Polynome: Hauptlemma-Beweis

► Sei $s \geq 2$

$$\begin{aligned} g &= f - c_1 x^{\delta - \gamma_{12}} S(g_1, g_2) \\ &= c_1 x^{\alpha_1} g_1 + c_2 x^{\alpha_2} g_2 + \sum_{3 \leq i \leq s} c_i x^{\alpha_i} g_i - c_1 x^{\delta - \gamma_{12}} \left(\frac{x^{\gamma_{12}}}{LT(g_1)} g_1 - \frac{x^{\gamma_{12}}}{LT(g_2)} g_2 \right) \\ &= c_1 \underbrace{(x^{\alpha_1} - x^{\delta - \text{mdeg}(g_1)})}_{=0} g_1 + (c_2 x^{\alpha_2} + c_1 x^{\delta - \text{mdeg}(g_2)}) g_2 + \sum_{3 \leq i \leq s} c_i x^{\alpha_i} g_i \\ &= (c_1 + c_2) x^{\alpha_2} g_2 + \sum_{3 \leq i \leq s} c_i x^{\alpha_i} g_i \end{aligned}$$

► Hierbei verwende $\alpha_1 + \text{mdeg}(g_1) = \delta = \alpha_2 + \text{mdeg}(g_2)$.

S-Polynome: Hauptlemma-Beweis

► $\text{mdeg}(g) \leq \max\{\text{mdeg}(f), \text{mdeg}(x^{\delta - \gamma_{12}} S(g_1, g_2))\} < \delta$,
 g hat die ursprüngliche Gestalt mit $s - 1$ Summanden (falls $c_1 + c_2 \neq 0$)
sonst $s - 2$ Summanden.

↔ Nach Induktionsvor. $g = \sum_{2 \leq i < j \leq s} c_{ij} x^{\delta - \gamma_{ij}} S(g_i, g_j)$.

Für $c_{ij} \in F$ ($2 \leq i < j \leq s$). $g = 0$, falls $s = 2$.

Setzt man $c_{12} = c_1$ und $c_{1j} = 0$ für $3 \leq j \leq s$, so

↔

$$f = g + c_1 x^{\delta - \gamma_{12}} S(g_1, g_2) = \sum_{1 \leq i < j \leq s} c_{ij} x^{\delta - \gamma_{ij}} S(g_i, g_j)$$

Charakterisierungssatz mit S-Polynome

8.36 Satz Eine endliche Menge $G = \{g_1, \dots, g_s\} \subseteq R$ ist eine Gröbner Basis für $\langle G \rangle$ gdw

$$S(g_i, g_j) \text{ REM } (g_1, \dots, g_s) = 0 \text{ für } 1 \leq i < j \leq s$$

$$\text{gdw } S(g_i, g_j) \xrightarrow{*}_G 0 \text{ für } 1 \leq i < j \leq s.$$

Beweis: "⇒" klar, "⇐" sei $f \in I \setminus \{0\}$ zeige $LT(f) \in \langle LT(G) \rangle$

$$f = \sum_{1 \leq i \leq s} q_i g_i \quad \blacktriangleright \quad \delta = \max_{\prec} \{mdeg(q_i g_i), 1 \leq i \leq s\}$$

Angenommen $mdeg(f) \prec \delta$, d. h. δ Monome heben sich weg.

- ▶ $f^* = \sum_{1 \leq i \leq s, mdeg(q_i g_i) = \delta} LM(q_i) g_i$ hat die Gestalt, wie sie in Lemma 8.35 vorausgesetzt wird.

- ▶ f^* lässt sich als Linearkombination von Polynomen der Form $x^{\alpha_{ij}} S(g_i, g_j)$ mit $\alpha_{ij} \in \mathbb{N}^n$ darstellen, wobei $\alpha_{ij} + mdeg(S(g_i, g_j)) \prec \delta$ nach Lemma 8.35.

Charakterisierungssatz mit S-Polynome

- ▶ Nach Voraussetzung gilt $S(g_i, g_j) \text{ rem } (g_1, \dots, g_s) = 0$, d. h.

$$f^* = \sum_{1 \leq i \leq s} q_i^* g_i \text{ mit } \max_{\prec} \{mdeg(q_i^* g_i) : 1 \leq i \leq s\} \prec \delta$$

- ▶ $f - f^*$ und f^* haben Darstellungen der Form $\sum q_i, g_i$ mit $\max_{\prec} \{mdeg(q_i g_i) : 1 \leq i \leq s\} \prec \delta$ also auch f .

- ▶ Wiederholte Anwendung liefert Darstellung von f mit

$$f = \sum_{1 \leq i \leq s} q_i g_i \text{ und } mdeg = \delta = \max \{mdeg q_i g_i\}$$

d. h. $mdeg(f) = mdeg(q_i g_i)$ für mindestens ein i und somit $LT(f) \in \langle LT(G) \rangle$.

Beispiel

8.37 Beispiel Twisted Cubic

$C = V(G)$ mit $G = \{y - x^2, z - x^3\}$, d. h. $C = \{(a, a^2, a^3) : a \in F\}$.
In \mathbb{R}^3 Schnitt von $V(y - x^2)$ und $V(z - x^3)$.

G ist Gröbner Basis für $\langle G \rangle$ bzgl. lex. Ordnung $y \succ z \succ x$.

$$\begin{aligned} \bullet S(y - x^2, z - x^3) &= z(y - x^2) - y(z - x^3) = yx^3 - zx^2 \xrightarrow{*}_G 0 \\ &= x^3(y - x^2) + (-x^2)(z - x^3) + 0 \end{aligned}$$

Buchberger's Algorithmus

{Eingabe: $f_1, \dots, f_s \in R = F[x_1, \dots, x_n]$, \prec Termordnung.}
{Ausgabe: Gröbner Basis $G \subseteq R$ für $I = \langle f_1, \dots, f_s \rangle$ bzgl. \prec .}
{ mit $\{f_1, \dots, f_s\} \subseteq G$.}

begin

1 $G := \{f_1, \dots, f_s\}$

2 **repeat**

$S := \emptyset$

Ordne die Elemente von G als g_1, \dots, g_t

for $i \leq j \leq t$ **do**

$r := S(g_i, g_j) \text{ rem } (g_1, \dots, g_t)$

if $r \neq 0$ **then** $S := S \cup \{r\}$

if $S = \emptyset$ **then** **return** G **else** $G := G \cup S$

end

Buchberger's Algorithmus: Korrektheit

8.38 Satz Algorithmus ist korrekt und terminierend.

Beweis: Es gilt stets $\langle G \rangle = I$ (nur Elemente aus I hinzu), falls Terminierung, so korrekt.

- $G_i \subseteq G_{i+1}$, d. h. $\langle LT(G_i) \rangle \subseteq \langle LT(G_{i+1}) \rangle$ aufsteigende Kette, die stabil werden muss.
D.h., wenn $G_i = G_{i+1}$, so erfüllen alle S Polynome von G_i : $S(\cdot, \cdot) \text{ rem } (G_i) = 0$.

► **Frage:** Platz und Zeitbedarf, Implementierungen.

8.39 Folgerung Folgende Probleme sind mit G -Basen entscheidbar

- i) Wortproblem ($f \in \langle G \rangle$)
- ii) $\langle G \rangle \subseteq \langle H \rangle$
- iii) $\langle G \rangle = \langle H \rangle$



Beispiel

$$f_1 = x^3 - 2xy \quad f_2 = x^2y - 2y^2 + x \in \mathbb{Q}[x, y], y < x \prec_{\text{grlex}}$$

- $S(f_1, f_2) = -x^2 \quad LT(S(f_1, f_2)) = -x^2 \notin \langle x^3, x^2y \rangle$
 - $f_3 := S(f_1, f_2) \text{ rem } (f_1, f_2) = -x^2$.
 - Dann $S(f_1, f_2) \text{ rem } (f_1, f_2, f_3) = 0$
- $S(f_1, f_3) = 1f_1 - (-x)f_3 = -2xy$
 $S(f_1, f_3) \text{ rem } (f_1, f_2, f_3) = -2xy =: f_4$ •
 $S(f_1, f_3) \xrightarrow{*}_{f_1, f_2, f_3, f_4} 0$
- $S(f_1, f_4) = yf_1 - (-\frac{1}{2}x^2)f_4 = -2xy^2 = yf_4 \xrightarrow{*} 0$
- $S(f_2, f_3) = 1f_2 - (-y)f_3 = -2y^2 + x$ irred.
 - $f_5 = S(f_2, f_3) \text{ rem } (f_1, \dots, f_4) = -2y^2 + x$
 - $\rightsquigarrow S(f_i, f_j) \text{ rem } (f_1, \dots, f_5) = 0$ für $1 \leq i < j \leq 5$,
 - d. h. $\{f_1, \dots, f_5\}$ ist Gröbner Basis.



Buchberger's Algorithmus (Forts.)

► Varianten des Buchberger Algorithmus um:

1. Gewisse S -Polynome nicht zu reduzieren.
2. Basis so klein wie möglich zu halten.
3. Wiederholungen zu vermeiden.

► Ziel:: Implementierung zu optimieren

Beachte:

Ist G Gröbner Basis und $f \in \langle G \rangle$, so ist $G \cup \{f\}$ auch Gröbner Basis.

8.40 Lemma Ist G Gröbner Basis von $I \subset R$, $g \in G$.
 $LT(g) \in \langle LT(G \setminus \{g\}) \rangle$, dann ist $G \setminus \{g\}$ Gröbner Basis von I .

Beweis: z.z. $\langle LT(G) \rangle = \langle LT(G \setminus \{g\}) \rangle = \langle LT(I) \rangle$ wegen $LT(g) \in \langle LT(G \setminus \{g\}) \rangle$ folgt die Behauptung.



Minimale- und reduzierte- Gröbner Basen

8.41 Definition Eine Menge $G \subseteq R$ heißt **minimale** (bzw. **reduzierte**) Gröbner Basis für $I = \langle G \rangle$, falls G eine G -Basis ist und für alle $g \in G$

- i) $LC(g) = 1$
- ii) $LT(g) \notin \langle LT(G \setminus \{g\}) \rangle$ (**minimal**)
- iii) g ist irreduzibel bzgl. $G \setminus \{g\}$. (**reduzierte**)

8.42 Satz Eindeutigkeitsatz

Jedes Ideal hat eine eindeutige reduzierte Gröbner Basis bzgl. \prec .

Beweis: **Existenz:** Anwendung von Lemma 8.40 o.B.d.A.

$G = \{g_1, \dots, g_s\}$ minimal.

$$\text{Sei } h_i = g_i \text{ rem } \{h_1, \dots, h_{i-1}, g_{i+1}, \dots, g_s\} \quad i = 1, \dots, s \\ = \text{NF}(g_i, G \setminus \{g_i\})$$



Eindeutigkeit reduzierter Gröbner Basen

- ▶ Seien G, G^* reduzierte Gröbner Basen für I . Dann $LT(G) = LT(G^*)$: für $t \in LT(G) \subseteq \langle LT(G) \rangle = \langle LT(I) \rangle = \langle LT(G^*) \rangle$ gibt es $g^* \in G^*$ mit $LT(g^*) \mid t$ und es gibt $g \in G$ mit $LT(g) \mid LT(g^*) \mid t$.
 G ist reduziert $\rightsquigarrow LT(g) = LT(g^*) = t \rightsquigarrow LT(G) \subseteq LT(G^*)$.
 = aus Symmetrie
- ▶ Sei $g \in G$ und $g^* \in G^*$ mit $LT(g) = LT(g^*)$. Da beide reduziert sind, ist kein Monom in $g - g^* \in I$ reduzibel also $g = g^*$, d. h. $G \subseteq G^*$ und umgekehrt.

8.43 Lemma Translationslemma:

$$p - q \xrightarrow{F} h \rightsquigarrow \exists p', q' : p \xrightarrow{*} p', q \xrightarrow{*} q', h = p' - q'$$

$$p - q \xrightarrow{*} 0 \rightsquigarrow \exists g : p \xrightarrow{*} g, q \xrightarrow{*} g$$

$$p \rightarrow q \rightsquigarrow tp \rightarrow tq \wedge p + h \downarrow^* q + h$$

Frage: Wieviele Polynome müssen hinzugenommen werden, um eine Gröbner Basis zu bekommen?

Äquivalente Charakterisierungen für GB

8.44 Satz Charakterisierungssatz für Gröbner Basen bzgl. \prec

Sei $G \subseteq R$ endlich $I = \langle G \rangle$. Dann sind äquivalent

1. (Normalform) jedes $f \in R$ hat eindeutige \xrightarrow{G} Normalform
2. (Standard Basen) $\langle LT(G) \rangle = \langle LT(I) \rangle$
3. (Buchberger Krit.) für alle $f, g \in G$ gilt $S(f, g) \xrightarrow{*} 0$
4. (Church Rosser) \xrightarrow{G} ist Church-Rosser, d. h. $f \xleftarrow{*} g$, so $f \downarrow_G^* g$
5. (Extended Standard) Jedes $f \in I$ hat eine Darstellung

$$f = \sum_{1 \leq i \leq s} q_i g_i \quad \text{mit } mdeg(f) \succeq mdeg(q_i g_i) \quad i = 1, \dots, s$$
6. (Ideal Membership) für alle $f \in I$ gilt $f \xrightarrow{*} 0$ oder $f \text{ rem}(G) = 0$.

Beispiele von GB

8.45 Beispiel $\{f_1, \dots, f_5\}$, Beispiel ist Gröbner Basis

$$x^3 - 2xy, \quad x^2y - 2y^2 + x, \quad -x^2, \quad -2xy, \quad -2y^2 + x$$

$\hookrightarrow \{x^2, xy, y^2 - \frac{1}{2}x\}$ ist minimale reduzierte Gröbner Basis, sie ist eindeutig bzgl. \prec_{grlex} .

Beachte: Bzgl. einer anderen Ordnung kann die G -Basis mehr oder weniger Polynome enthalten.

z.B. $x \succ y : \{x - 2y^2, y^3\}$
 $y \succ x : \{y^2 - \frac{1}{2}x, yx, x^2\}$

Beachte: Termideale, Monomideale und homogene Ideale haben reduzierte Gröbner Basen, die **unabhängig** von der Ordnung sind.

Homogene Ideale

Ein Polynom $f = \sum \alpha_e x^e$ ist **homogen**, falls alle Terme x^e gleichen Grad haben, d. h. $\sum_{i=1}^n e_i = k :: f$ ist dann **homogen vom Grad k** .

- ▶ Jedes Polynom lässt sich eindeutig als Summe homogener Polynome (die **homogenen Komponenten**) darstellen.
- ▶ I ist homogen, falls $I = \langle G \rangle$, G enthält homogene Polynome gdw $\forall f \in I$ jede homogene Komponente von f liegt in I .

Anwendungen von Gröbner Basen

1. Berechnungen in Quotientenringen: $K[x_1, \dots, x_n]/I$

$$a \in R \mapsto \bar{a} = a + I \in S = R/I$$

\bar{a} Restklasse von a .

- Ist G eine reduzierte G -Basis von I , so kann man als Repräsentant von a die Normalform von a bzgl. G wählen, d. h. $rep_G(a) = a \text{ rem } (G)$.

Offenbar

$$\bar{a} = \bar{b} \text{ gdw } a - b \in I \text{ gdw } rep_G(a - b) = 0 \text{ gdw } rep_G(a) = rep_G(b)$$

- Arithmetik in S :

$$\bar{a} \pm \bar{b} \iff rep_G(a) \pm rep_G(b)$$

$$\bar{a} \cdot \bar{b} \iff rep_G(rep_G(a) \cdot rep_G(b))$$



Anwendungen von Gröbner Basen (Forts.)

8.46 Lemma Sei $I \subseteq R = K[x_1, \dots, x_n]$, G Gröbnerbasis von I .

- $V = R/I$ ist K -Vektorraum.
- $B = \{t \in T[X] : t = rep_G(t)\}$. Dann ist $\bar{B} = \{\bar{t} : t \in B\}$ eine K -Vektorraumbasis von V .
- V hat endliche K -Dimension gdw I nulldimensional.

- Eine Teilmenge $S \subseteq R$ ist nulldimensional, falls $Zero(S) \subseteq \bar{K}^n$, (\bar{K} alg. Abschluss von K) endlich ist
- hier $Var_{\bar{K}}(I)$ endlich. (S Ideal)



Anwendungen von Gröbner Basen (Forts.)

8.47 Satz $I \subseteq K[x_1, \dots, x_n]$.

I ist nulldimensional gdw für jedes $i = 1, \dots, n$ $I \cap K[x_i] \neq \{0\}$.

Beweis:

“ \Leftarrow ” Sei $0 \neq f_i \in I \cap K[x_i]$ $i = 1, \dots, n$.

Sei $\xi \in Var(I)$, ξ muss Nullstelle von f_i sein, d. h. ξ_i muss Nullstelle von f_i sein und davon gibt es nur endlich viele. $\rightsquigarrow Var(I)$ ist endlich.

“ \Rightarrow ” angenommen $Var_{\bar{K}}(I) = \{\xi^1, \dots, \xi^m\}$ mit $\xi^j = (\xi_1^j, \dots, \xi_n^j)$. Da $\xi_i^j \in \bar{K}$, gibt es Polynome $f_i \in K[x_i]$ mit $f_i(\xi_i^j) = 0$ für $j = 1, \dots, m$, d. h. f_i ist null auf $Var(I)$.

Nach Hilbert's Nullstellensatz gibt es $m_i \in \mathbb{N}^+$ mit $f_i^{m_i} \in I$, d. h. $I \cap K[x_i] \neq \{0\}$.



Anwendungen von Gröbner Basen (Forts.)

8.48 Folgerung Sei G eine Gröbner Basis für I .

I ist nulldimensional gdw für jedes $i = 1, \dots, n$ es ein $g_i \in G$ gibt mit $LT(g_i) \in T[x_i]$ gdw $V = R/I$ hat endliche K -Dimension.

Beweis: $\langle LT(G) \rangle = \langle LT(I) \rangle$, da Gröbner Basis. Für $i = 1, \dots, k$:

$$I \cap K[x_i] \neq \{0\} \text{ gdw } \langle LT(I) \rangle \cap K[x_i] \neq \{0\}$$

$$\text{gdw } LT(G) \cap K[x_i] \neq \emptyset$$

$$\text{gdw } B = \{t \in T[x] : t = rep_G(t)\} \text{ ist endlich.}$$

Bedingung: “ \Rightarrow ” klar, da x_i^k , $k > k_i$ reduzibel.

“ \Leftarrow ” Ist I nicht nulldimensional, so gibt es eine Variable x_i , so dass $x_i^l \in B$ für alle $l \geq 0$, d. h. B ist unendlich und V ist ∞ -dimensional als K -Vektorraum.



Beispiele

8.49 Beispiel $I = \langle x^3y - 2y^2 - 1, x^2y^2 + x + y \rangle$ in $\mathbb{Q}[x, y]$.

- $\prec = \prec_{grlex}$ mit $x \succ y$.

$$GB(I, \prec) = \left\{ \begin{array}{l} \underline{x^4 + x^2y - 2xy + 1}, \underline{x^3y - 2y^2 - 1}, \underline{x^2y^2 + x + y}, \\ x^2 + xy + \underline{2y^3 + y} \end{array} \right\}$$

- $\prec = \prec_{lex}$ mit $y \succ x$.

$$GB(I, \prec) = \left\{ \begin{array}{l} 34y + 8x^8 - x^7 - 2x^6 - 4x^5 + 7x^3 - 35x^2 + 30x - 8, \\ x^9 + x^5 + 3x^4 - 4x^3 + 4x^2 + 2 \end{array} \right\}$$

► Dimension als \mathbb{Q} -Vektorraum:

- 1) $\{x^3, x^2, x, x^2y, xy, y^2, y, xy^2, 1\}$ irr. Terme
- 2) $\{x^8, x^7, x^6, x^5, x^4, x^3, x^2, x, 1\}$ irr. Terme.

d.h. $DIM_{\mathbb{Q}}(\mathbb{Q}[x, y]/I) = 9$

Übung: Berechne Polynome in $I \cap \mathbb{Q}[x]$ und $I \cap \mathbb{Q}[y]$.

Beispiele

- Man kann auch eine Multiplikationstafel für B berechnen: für $p, q \in B$ berechne Normalform von pq (ist dann Polynom), z. B. oben $x \cdot x^3 = -x^2y + 2xy - 1$

Wortproblem für I bzw. \equiv_I Idealmembership.
Problem für e.e. Ideale $I \subseteq R = K[x_1, \dots, x_n]$.

Gegeben: $f, f_1, \dots, f_m \in R$.

Frage: $f \in \langle f_1, \dots, f_m \rangle$ ggf. Darstellung.

Lösung: Berechne G -Basis $G = \{g_1, \dots, g_s\}$ für I , wobei die Darstellungen von $g_i = \sum_{j=1}^m q_j^i f_j$ berechnet werden.

$f \in \langle f_1, \dots, f_m \rangle$ gdw $f \text{ res } (G) = 0 +$ Darstellung in $g_i \rightsquigarrow$ Darstellung in f_j berechnen.

Beispiele (Forts.)

8.50 Beispiel Folgende Polynomrelationen seien gegeben.

$$I :: \begin{array}{l} f_1 = 4z - 4xy^2 - 16x^2 - 1 = 0 \\ f_2 = 2y^2z + 4x + 1 = 0 \quad f_i \in \mathbb{R}[x, y, z] \\ f_3 = 2x^2z + 2y^2 + x = 0 \end{array}$$

► Folgt hieraus

$$g(x, y) = 4xy^2 + 16x^2y^2 + y^2 + 8x + 2 = 0$$

Für (x, y) mit $\exists z : (x, y, z) \in \text{Var}(I)$?

► Ist $g \in I = \langle f_1, f_2, f_3 \rangle$? g ist irreduzibel bzgl. $\{f_1, f_2, f_3\}$

Beispiele (Forts.)

► Berechne Gröbner Basis bzgl. lex. Ordnung $x < y < z$ liefert:

$$\begin{array}{l} g_1 = 32x^7 - 216x^6 + 34x^4 - 12x^3 - x^2 + 30x + 8 \\ g_2 = 2745y^2 - 112x^6 - 812x^5 + 10592x^4 - 61x^3 - 812x^2 + 988x + 2 \\ g_3 = 4z - 4xy^2 - 16x^2 - 1 \end{array}$$

• $\rightsquigarrow \text{Var}(I)$ ist endlich.

$$g \xrightarrow{*} 0 \quad , \text{ d. h. } \quad g(x, y) = 0 \quad \text{auf Var. } I.$$

► Lösung von Systemen von Polynomgleichungen

$$V = \{a \in K^n : f_1(a) = \dots = f_m(a) = 0\}$$

Fragen: $V \neq \emptyset$? Gegebenenfalls finde $a \in V$.
 $g \in K[x_1, \dots, x_n]$, ist $g(a) = 0$ für alle $a \in V$.

\hookrightarrow Hilbert's Nullstellensatz, Radikal, Eliminationsmethoden.

Eliminationseigenschaften - Polynomgleichungen

8.51 Definition Sei $I \subseteq K[x_1, \dots, x_n] = R$, $\text{radikal}(I)$ ist ideal in R mit:

$$f \in \text{radikal}(I) \text{ gdw } f^n \in I \text{ für ein } n \in \mathbb{N}^+$$

Schreibweise Lit: \sqrt{I} (Übung \sqrt{I} ist Ideal).

Motivation: Sei $\mathbb{Z} \subseteq R_0 \subseteq R_1 \subseteq \mathbb{C}$ (oder alg. abg. Körper).

- ▶ $R_1^d = \mathbb{A}^d(R_1)$ d -dimensionaler affiner Raum von R_1 .
- ▶ $U \subseteq \mathbb{A}^d(R_1)$, $f \in R_0[x_1, \dots, x_d]$, f verschwindet auf U , falls $f(a) = 0$ für alle $a \in U$.
- $\text{Ideal}(U) \subseteq R_0[x_1, \dots, x_d]$ sei definiert durch
 $\text{Ideal}(U) = \{f \in R_0[x_1, \dots, x_d] \mid f \text{ verschwindet auf } U\}$ ist Ideal!.
- ▶ $I = \langle f_1, \dots, f_n \rangle$, $f_i \in R_0[x_1, \dots, x_d]$
 $\text{Zero}_{R_1}(I) = \text{Var}_{R_1}(I) = \{a \in \mathbb{A}^d(R_1) : f_i(a) = 0, i = 1, \dots, n\}$

Eliminationseigenschaften - Polynomgleichungen (Forts.)

- $U \mapsto \text{Ideal}(U)$ für $U \subseteq \mathbb{A}^d(R_1)$
- $I \mapsto \text{Zero}_{R_1}(I)$ für $I = \langle f_1, \dots, f_n \rangle \subseteq R_0[x_1, \dots, x_d]$

Algebraische Teilmengen von $\mathbb{A}^d(R_1)$ (Zariski Topologie)

- ▶ Es gilt: für $I \subseteq R_0[x_1, \dots, x_d]$ und $U \subseteq \mathbb{A}^d(R_1)$.
 - ▶ $I \subseteq \text{Ideal}[\text{Zero}_{R_1}(I)]$
 - ▶ $U \subseteq \text{Zero}_{R_1}[\text{Ideal}(U)]$
 - ▶ $\text{Zero}[\text{Ideal}[\text{Zero}(I)]] = \text{Zero}(I)$ $I \subseteq R_0[x_1, \dots, x_d]$
 - ▶ $\text{Ideal}[\text{Zero}[\text{Ideal}(U)]] = \text{Ideal}(U)$ $U \subseteq \mathbb{A}^d(R_1)$
- ▶ Schränkt man die Abbildungen auf ideale und alg. Mengen, sind sie dann **invers zueinander**?
 Nur für ideale, die radikal sind, d. h. $f^n \in I$, $n \geq 1 \rightsquigarrow f \in I$.
 Da $\text{Ideal}(U)$ stets radikal ist.

Hilbert's Nullstellensatz

- ▶ Hilberts Nullstellensatz (schwache Form)

Sei D noetherscher ZPE-Ring, \bar{D} alg. Abschluss.

Ein Ideal $I \subseteq D[x_1, \dots, x_d]$ hat keine Nullstellen in $\mathbb{A}^d(\bar{D})$ gdw I enthält nichtriviales Element von D .

- ▶ Hilberts Nullstellensatz (starke Form)

Sei D wie oben. $I \subseteq D[x_1, \dots, x_d]$ Ideal und $f \in D[x_1, \dots, x_d]$.

f verschwindet auf $\text{Var}_{\bar{D}}(I)$ gdw es gibt $m \geq 0$, $0 \neq a \in D$ mit $a \cdot f^m \in I$.

\hookrightarrow d.h. $f \in \sqrt{I}$ (Körperfall).

$\hookrightarrow f_1(\bar{x}) = 0 \wedge \dots \wedge f_m(\bar{x}) = 0 \Rightarrow f(\bar{x}) = 0$

$\rightsquigarrow f \in \sqrt{\langle f_1, \dots, f_m \rangle}$

Hilbert's Nullstellensatz: Motivation

- ▶ Offenbar gilt:

- ▶ Starke Form \rightsquigarrow schwache Form.

- ▶ Schwache Form \rightsquigarrow starke Form:

Sei $f \in D[x_1, \dots, x_d]$, f verschwindet auf $\text{Var}_{\bar{D}}(I)$.

Sei $I = \langle f_1, \dots, f_m \rangle$ "Rabinowitz-Trick" neue Var. z : Setze $g := 1 - z \cdot f$, dann hat das Ideal $\langle f_1, \dots, f_m, g \rangle$ keine Nullstellen, da g nicht null an den Nullstellen von f_1, \dots, f_m \rightsquigarrow es gibt $0 \neq a \in D \cap \langle f_1, \dots, f_m, g \rangle$

$$a = \sum_{i=1}^m \alpha_i f_i + \beta(1 - zf) \quad \alpha_i, \beta \in D[x_1, \dots, x_d, z]$$

- ▶ Setze $z = 1/f \rightsquigarrow a = \sum_{i=1}^m \alpha'_i f_i$ mit $\alpha'_i \in D(x_1, \dots, x_d)$.

Rationale Funktionen mit Nenner Potenz von $f \rightsquigarrow$

- ▶ $a \cdot f^n = \sum (\alpha'_i f^{m_i}) f_i$ mit $\alpha'_i f^{m_i} \in D[x_1, \dots, x_d]$.

Anwendungen von Hilbert's Nullstellensatz

Anwendung: Radikal-Membership-Problem

▶ Seien $f_1, \dots, f_m \in K[x_1, \dots, x_d]$, $f \in K[x_1, \dots, x_d]$

Frage: Gilt $f \in \sqrt{\langle f_1, \dots, f_m \rangle}$?

$$f \in \sqrt{\langle f_1, \dots, f_m \rangle} \quad \text{gdw} \quad f \text{ verschwindet auf } \text{Var}_K(\langle f_1, \dots, f_m \rangle)$$

$$\text{gdw} \quad f_1(\bar{x}) = f_2(\bar{x}) = \dots = (1 - z \cdot f)(\bar{x}) = 0$$

hat keine Lösungen in \bar{K}^d

$$\text{gdw} \quad 1 \in \langle f_1, \dots, f_m, 1 - zf \rangle_{K[x_1, \dots, x_d, z]}$$

$$\text{gdw} \quad 1 \in \text{GB}(f_1, \dots, f_m, 1 - zf)$$

▶ **Frage:** Gilt $\text{Var}_{\bar{K}}(\langle f_1, \dots, f_m \rangle) = \emptyset$?

Lösung: Ja, falls $1 \in \text{GB}(f_1, \dots, f_m)$.

Anwendungen: Eliminationseigenschaften, Varietäten

▶ **Frage:** Gilt $\text{Var}_{\bar{K}}(\langle f_1, \dots, f_m \rangle)$ endlich, $I = \langle f_1, \dots, f_m \rangle$ ist nulldimensional.

Lösung: Berechne GB und K -Dimension von $K[x_1, \dots, x_d]/I$.

Angenommen $\text{Var}_{\bar{K}}(\langle f_1, \dots, f_m \rangle)$ sei endlich:

▶ **Frage:** Kann man die Lösungen explizit darstellen?

8.52 Satz Eliminationseigenschaft für Gröbner Basen.

Sei G Gröbner Basis von $I = \langle f_1, \dots, f_m \rangle$ bzgl. der Lex-Ordnung mit $x_1 < x_2 < \dots < x_n$. Dann gilt

$$J = I \cap K[x_1, \dots, x_j] = \langle G \cap K[x_1, \dots, x_j] \rangle_{K[x_1, \dots, x_j]}$$

Insbesondere ist $G \cap K[x_1, \dots, x_j]$ eine G -Basis für J .

Eliminationseigenschaften: Beweis

Beweis:

“ \supseteq ” klar.

“ \subseteq ” $LT(f) \in T[x_1, \dots, x_j]$ gdw $f \in K[x_1, \dots, x_j]$,
 $f \in I \cap K[x_1, \dots, x_j] \rightsquigarrow f \xrightarrow{G} 0$ und die Leitertme der Basispolynome bei der Reduktion liegen in $T[x_1, \dots, x_j]$, d. h. diese Basispolynome liegen in $G \cap K[x_1, \dots, x_j]$.

8.53 Folgerung Sei G G -Basis von I bzgl. der Lex Ordnung mit $x_1 < x_2 < \dots < x_n$.

I ist nulldimensional gdw für jedes $i = 1, \dots, n$ gibt es ein $g_i \in G$ mit $HT(g_i) \in K[x_1, \dots, x_i] \setminus K[x_1, \dots, x_{i-1}]$.

Eliminationseigenschaften: Beweis (Forts.)

Beweis:

“ \supseteq ” klar

“ \subseteq ” $\xi = (\xi_1, \dots, \xi_n) \in \text{Var}_{\bar{K}}(I)$. So $g_i(\xi_1, \dots, \xi_i) = 0 \quad i = 1, \dots, n$.

• $i = 1$ g_1 Polynom in einer Var. \rightsquigarrow endlich viele Nullstellen, d. h. nur endlich viele Möglichkeiten für ξ_1 .

• **Induktiv** $\rightsquigarrow g_i(\xi_1, \dots, \xi_{i-1}, \xi_i) = 0$ für ξ_1, \dots, ξ_{i-1} nur endlich viele Möglichkeiten \rightsquigarrow für ξ_i nur endlich viele Möglichkeiten.

Anwendung: Polynomgleichungen

8.54 Beispiel Pol. Gleichungssystem

$$\begin{aligned} f_1 &:: 4xz - 4xy^2 - 16x^2 - 1 = 0 \\ f_2 &:: 2y^2z + 4x + 1 = 0 \\ f_3 &:: 2x^2z + 2y^2 + x = 0 \end{aligned} \quad \mathbb{Q}[x, y, z] \quad x < y < z$$

► Gröbner Basis bzgl. lex. Ordnung:

$$\begin{aligned} g_1 &= 65z + 64x^4 - 423x^3 + 168x^2 - 354x + 104 \\ g_2 &= 26y^2 - 16x^4 + 108x^3 - 16x^2 + 17x \\ g_3 &= 32x^5 - 216x^4 + 64x^3 - 42x^2 + 32x + 5 \end{aligned}$$

Anwendung: Polynomgleichungen (Forts.)

↪ $\text{Var}_{\mathbb{C}}(\langle f_1, f_2, f_3 \rangle)$ ist endlich, $\text{DIM}_K(\mathbb{Q}[x, y, z]/I) = 10$,
 d. h. $|\text{Zero}(f_1, f_2, f_3)| = 10$ (Nullstellen mit Vielfachheit zählen).

► Lösungen von g_3 als Parameter: α (5-Nullstellen)

$$\left(\alpha, \pm \frac{1}{\sqrt{26}} \sqrt{\alpha \sqrt{16\alpha^3 - 108\alpha^2 + 16\alpha - 17}}, \frac{1}{65}(64\alpha^4 - 423\alpha^3 + \dots)\right)$$

↪ Darstellung von $\text{Var}_{\mathbb{C}}(\langle f_1, f_2, f_3 \rangle)$.

Beispiel: Polynomgleichungen

8.55 Beispiel Parametrisiertes Gleichungssystem.

$$\begin{aligned} f_1 &:= x_4 + b - d = 0 \\ f_2 &:= x_4 + x_3 + x_2 + x_1 - a - c - d = 0 \\ f_3 &:= x_3x_4 + x_1x_4 + x_1x_3 - ad - ac - cd = 0 \\ f_4 &:= x_1x_3x_4 - acd = 0 \end{aligned}$$

• Parameter: $a, b, c, d \in K, <:: x_1 < x_2 < x_3 < x_4$

G-Basis bzgl. lex Ordnung: $\mathbb{Q}(a, b, c, d)[x_1, x_2, x_3, x_4]$

$$\begin{aligned} g_1 &= x_4 + b - d \\ g_2 &= x_3 - \frac{b^2 - 2bd + d^2}{acd} x_1^2 - \frac{abc + abd - 2acd - ad^2 + bcd - cd^2}{acd} x_1 - a - c - d \\ g_3 &= x_2 + \dots \quad g_4 = x_1^3 + \dots \end{aligned}$$

Eine Wurzel von g_4 ist $\frac{-ad}{b-d}$ (?)

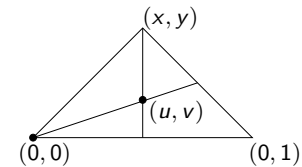
$$\rightsquigarrow \left(\frac{-ad}{bd}, \frac{ab + b^2 - bd}{b-d}, c, -b + d \right)$$

► Anwendungen: Schaltungsentwurf: Verstärker usw.

Automatisches Beweisen in der Geometrie

8.56 Beispiel Dreieck, Schnitt der Medianen, Formulierung:

$$f_1, f_2 \in \mathbb{R}[u, v, x, y]$$



► $f_1 = 0 \wedge f_2 = 0 \Rightarrow g_1 = 0 \wedge g_2 = 0 \wedge g_3 = 0$,
 • falls $g_1, g_2, g_3 \in \langle f_1, f_2 \rangle$, so ok. g_1 bereits gezeigt.

► $GB(\langle f_1, f_2 \rangle) \quad u \succ v \succ x \succ y$ lex Ordnung.
 $f_1 = uy - vx - v \quad f_2 = uy - vx + 2v - y$

↪ $S(f_1, f_2) = f_1 - f_2 = -3v + y = -g_3$
 $\{f_1, f_2, g_3\}$ ist Gröbner Basis.

Automatisches Beweisen in der Geometrie (Forts.)

- Die eindeutige reduzierte G -Basis ist

$$G = \left\{ uy - \frac{1}{3}xy - \frac{1}{3}y, v - \frac{1}{3}y \right\}$$

$$\begin{aligned} g_1 &= -2uy - (v - y) + 2vx && \xrightarrow{*}_G 0 \\ g_2 &= 3u - x - 1 && \text{irreduzibel d. h. } g_2 \notin \langle G \rangle \\ g_3 &= 3v - y && \xrightarrow{*}_G 0 \end{aligned}$$

- Beachte aber $yg_2 = 3uy - xy - y \xrightarrow{*}_G 0$, d. h. $yg_2 \in I$

\hookrightarrow d. h. $g_2(x, y) = 0$, falls $(x, y) \in V(I)$ und $y \neq 0$
 nicht Degeneriertheitsbedingung $y \neq 0$.

- Nimmt man $1 - yz$ zu G hinzu, z neue Variablen garantiert.
 $y \neq 0$: $g_2 = g_2 \cdot (1 - yz) + zyg_2 \in \langle f_1, f_2, 1 - yz \rangle$

Implizitierung (Implication)

- Seien $f_1, \dots, f_n \in K[t_1, \dots, t_m]$ und eine affine Alg. Varietät $V \subseteq K^n$ sei in parametrisierte Form gegeben, d. h.

$$\begin{aligned} x_1 &= f_1(t_1, \dots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \dots, t_m) \end{aligned}$$

$\hookrightarrow V = \{a \in K^n : \exists b \in K^m \ a = (f_1(b), \dots, f_n(b))\}$

- Finde Polynome $g_1, \dots, g_s \in K[x_1, \dots, x_n]$, so dass $V = \text{Var}(I)$ mit $I = \langle g_1, \dots, g_s \rangle$ "implizite Darstellung".

8.57 Beispiel

- Twisted Cubic: $x = t \quad y = t^2 \quad z = t^3$
 Implizitierung: $g_1 = y - x^2 \quad g_2 = z - x^3$
- $x = t^2, y = t^3, z = t^4$
 Implizitierung: $g_1 = z - x^2 \quad g_2 = y^2 - x^3$

Implizitierung : Lösungsansatz

Lösung mit G -Basen:

- Betrachte $J = \langle x_1 - f_1, \dots, x_n - f_n \rangle \subseteq K[t_1, \dots, t_m, x_1, \dots, x_n]$. Wähle Ordnung $t_1 \succ \dots \succ t_m \succ x_1 \succ \dots \succ x_n \prec_{lex}$.

\hookrightarrow Einige der g in $GB(J)$ hängen nur von x_1, \dots, x_n ab, dies sind Kandidaten für die Implizitierung.

8.58 Beispiel

- $t \succ z \succ y \succ x$
- $GB\{x - t, y - t^2, z - t^3\}$ ist $\{t - x, z - x^3, y - x^2\}$
- $GB\{x - t^2, y - t^3, z - t^4\}$ ist $\{t^2 - x, ty - x^2, tx - y, z - x^2, y^2 - x^3\}$
- Die Varietät, die von $G \cap K[x_1, \dots, x_n]$ definiert wird, ist die kleinste Varietät (Alg-Menge), die das Bild der Parametrisierung enthält.

Lösung linearer Gleichungen in $K[\bar{x}]$: Syzygien

Lösung linearer Gleichungen in $K[\bar{x}]$

Gegeben: $f_1, \dots, f_s, f \in K[\bar{x}] = R$.

Gesucht: Lösungen von $f_1z_1 + \dots + f_s z_s = f$
 bzw. $f_1z_1 + \dots + f_s z_s = 0$ (*)

mit $z_i \in K[\bar{x}]$.

- Jede Lösung von (*) heißt eine Syzygie von f_1, \dots, f_s .
- Beachte die Menge der Lösungen von (*) ist ein R -Modul, hat eine endliche Basis.
- Gesucht wird eine Modul-Basis für $\text{syz}(\{f_1, \dots, f_s\})$.

Basis für Syzygienmodul für Gröbner-Basen

8.59 Satz Basis für Syzygienmodul für Gröbner-Basen.

Sei $G = \{f_1, \dots, f_s\}$ Gröbner-Basis. Eine Basis S für $\text{syz}(G)$ erhält man wie folgt:

► Für $1 \leq i \leq s$ sei $e_i = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{R}^s$ i -te Einheitsvektor.

► Für $1 \leq i < j \leq s$ $t_{ij} = \text{KGV}(LT(f_i), LT(f_j))$

$$p_{ij} = \frac{t_{ij}}{LM(f_i)} \quad q_{ij} = \frac{t_{ij}}{LM(f_j)}$$

$$\begin{aligned} \text{► } S(f_i, f_j) &= p_{ij}f_i - q_{ij}f_j \xrightarrow{*} 0 \\ &= \sum_{l=1}^s k_{ij}^l f_l \text{ mit } k_{ij}^l \in R \end{aligned}$$

$$\text{► } S = \{p_{ij}e_i - q_{ij}e_j - (k_{ij}^1, \dots, k_{ij}^s) \mid 1 \leq i < j \leq s\}$$

Basis für Syzygienmodul für Gröbner-Basen (Forts.)

Beweis:

- Jedes Element in S ist eine Syzygie von G .
Sei $s_{ij} = p_{ij}e_i - q_{ij}e_j - (k_{ij}^1, \dots, k_{ij}^s)$ als Zeilenvektor.

$$\hookrightarrow s_{ij} \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix} = p_{ij}f_i - q_{ij}f_j - \sum_{l=1}^s k_{ij}^l f_l = 0$$

- Sei $z = (z_1, \dots, z_s) \in R^s$ nichttriviale Syzygie von G , d. h. $\sum z_i f_i = 0$, und p maximaler Term in dieser Summe. Lemma 8.35 liefert das Ergebnis: Durch Abziehen geeigneter Vielfacher von $s_{i,j}$ von z lässt sich Summe mit kleinerem p erreichen, d. h. z ist Linearkombination der s_{ij} und somit bildet S eine Basis für $\text{syz}(G)$.

Basis für Syzygienmodul für Gröbner-Basen (Forts.)

8.60 Satz Sei $F = (f_1, \dots, f_s)^T$ mit $f_i \in K[\bar{x}]$ und $G = (g_1, \dots, g_m)^T$ eine Gröbner-Basis für $\langle F \rangle$. (Betrachte F, G als Spaltenvektoren aus R^s bzw. R^m).

- Die Matrix $R_{r \times m}$ bestehe aus r Zeilen, die eine Basis für $\text{syz}(G)$ bilden (S von 8.59). Weiterhin seien die Matrizen A, B definiert durch $G = A_{m \times s} F$ bzw. $F = B_{s \times m} G$ (Darstellungen der g_i in den f_i und umgekehrt.)

$$\text{Sei } Q := \begin{pmatrix} I_s - B \cdot A \\ R \cdot A \end{pmatrix}_{s+r,s}$$

Dann bilden die Zeilen von Q eine Basis für $\text{syz}(F)$.

Beweis

$$\begin{aligned} \text{Beweis} \text{ Seien } b_1, \dots, b_{s+r} \text{ Polynome } b &= (b_1 \dots b_{s+r}). \\ (b \cdot Q)F &= ((b_1, \dots, b_s)(I_s - BA) + (b_{s+1} \dots b_{s+r})RA)F \\ &= (b_1 \dots b_s)(F - \underbrace{BAF}_{=F}) + (b_{s+1} \dots b_{s+r})R \underbrace{AF}_{=G} \\ &= 0 \end{aligned}$$

\hookrightarrow d.h. Jede Linearkombination der Zeilen von Q ist eine Syzygie von F .

- Sei $H = (h_1 \dots h_s)$ eine Syzygie von F . Dann ist $H \cdot B$ eine Syzygie von G . Für ein H' gilt dann $H \cdot B = H' \cdot R$ und somit $H \cdot B \cdot A = H' \cdot R \cdot A$, d. h. $H = H \cdot (I_s - BA) + H' \cdot R \cdot A = (H, H')Q$, also ist H Linearkombination der Zeilen von Q .

Lösung inhomogener Gleichungen

- $f_1 z_1 + \dots + f_s z_s = f$ Existenz gdw $f \in \langle F \rangle$ Gröbner Basis für F ,
 $G = A \cdot F$, $f \xrightarrow{*}_G f' \neq 0$ nicht lösbar, sonst $f \xrightarrow{*}_G 0$,
 $g_1 h'_1 + \dots + g_m h'_m = f \iff H = (h'_1 \dots h'_m)A$ ist **partikuläre Lösung**.

Effektive Operationen mit Idealen

Seien $I = \langle f_1, \dots, f_r \rangle$ und $J = \langle g_1, \dots, g_s \rangle$ Ideale in $K[X]$

- ▶ $I + J := \{f + g : f \in I, g \in J\} = \langle f_1, \dots, f_r, g_1, \dots, g_s \rangle$
- ▶ $I \cdot J := \{fg : f \in I, g \in J\} = \langle f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s \rangle$
- ▶ $I \cap J := \{f : f \in I \text{ und } f \in J\} = (\langle t \rangle I + \langle 1-t \rangle J) \cap K[X]$
- ▶ $I : J := \{f : fg \in I, \forall g \in J\} = \bigcap_{j=1, \dots, s} (I : \langle g_j \rangle)$
wobei $I : \langle g \rangle = \langle h_1/g, \dots, h_m/g \rangle$ mit $I \cap \langle g \rangle = \langle h_1, \dots, h_m \rangle$
- ▶ Transformation von G-Basen bzgl. verschiedener Termordnungen (Lazard)
- ▶ GGT-Berechnung mit G-Basen (Gianni, Trager)

Zur Komplexität der Berechnung von G-Basen

Probleme:

- ▶ Ordnungen, Längen von Ketten bei Reduktion.
- ▶ Wachstum der Größen bei der Berechnung: Eingabe weniger Polynome, kleine Grade, kleine Koeffizienten: Ausgabe Polynome mit großen Graden, große Koeffizienten.
D. h. Ergebnisse können groß werden.
- ▶ Klassen P , BPP , NP , $EXPSPACE$
- $EXPSPACE$ -vollständige Probleme benötigen $2^{2^{O(n)}}$ Zeit.
 IM (Wortproblem für Ideale über $\mathbb{Q}[x_1, \dots, x_s]$.)
- Mayr & Mayer 82: IM ist $EXPSPACE$ -hart für allg. Ideale.
- Mayr 89,92: IM ist in $EXPSPACE$, d.h. IM ist vollständig.

Zur Komplexität der Berechnung von G-Basen (Forts.)

- ▶ $f \in \langle f_1, \dots, f_m \rangle$ gdw $f \xrightarrow{GB(f_1, \dots, f_m)}^* 0$
- $f \xrightarrow{GB}^* 0$ kann in $EXPSPACE$ berechnet werden (für G-Basen).
- Entscheidungsproblem: Ist $\{f_1, \dots, f_m\}$ Gröbner Basis ist $EXPSPACE$ -hart.

8.61 Satz Kühnle, Mayr 96

Die Berechnung einer reduzierten G-Basis kann in $EXPSPACE$ erfolgen. (Beachte $EXPSPACE = DSPACE(2^{lin})$ wird nur Platz auf Arbeitsband gemessen).

- ▶ Gleiche Ergebnisse gelten für binomial-ideale, d. h. Ideale werden durch Binome $x^\alpha - x^\beta$ erzeugt.

Zur Komplexität der Berechnung von G-Basen (Forts.)

- ▶ Bürgisser (98) K ∞ -Körper. IM benötigt exponentielle parallele Zeit.
- ▶ Für homogene Ideale: Mayr 95: IM ist $PSPACE$ -vollständig. Berechnung der G-Basis bleibt $EXPSPACE$ -hart.

Gradschranken

- ▶ Hermann 1926: $f \in \langle f_1, \dots, f_s \rangle$, $f = \sum_{1 \leq i \leq s} q_i f_i$
Grade der q_i doppelte exponentiell. Siehe auch Mayr & Mayer 82.
- ▶ Die Grade der Polynome in einer reduzierten Gröbner Basis für $\langle f_1, \dots, f_s \rangle \subseteq F[x_1, \dots, x_n]$ sind höchstens

$$2 \left(\frac{d^2}{2} + d \right)^{2^{n-1}}$$

wobei $deg(f_i) \leq d$ für alle i .

Zur Komplexität der Berechnung von G -Basen (Forts.)

Beachte: die Schranke hängt nicht von der Anzahl der Polynome oder von den Koeffizienten ab. Sie ist polynomial im Grad und doppelt exponentiell in der Anzahl der Variablen.

- ▶ Es gibt Ideale, für die jede G -Basis mindestens $2^{2^{cn}}$ Elemente enthält mit Elementen vom Grad mindestens $2^{2^{c^*n}}$ ($c, c^* \in \mathbb{R}^+$).
- ▶ Varietäten: $V(f_1, \dots, f_s)$ ist leer gdw $1 \in \langle f_1, \dots, f_s \rangle$ in PSPACE.
- ▶ Für nulldimensionale Ideale einfache Exp-Schranken.
[Lakshman \(90\)](#), [Mayr \(97\)](#) Übersicht.
- ▶ Systeme: Macaulay, Singular. Projekte: Posso Frisco.