Projektarbeit

Polynomfaktorisierung

Lorenz Panny

Betreuer: Prof. Dr. Gregor Kemper

Technische Universität München

7. März 2015

Inhaltsverzeichnis

1 Einführung

Ein zentrales Problem der (algorithmischen) Zahlentheorie ist seit jeher die *Faktorisierung* natürlicher Zahlen, also die multiplikative Zerlegung in Primzahlpotenzen. Bis heute ist kein Verfahren bekannt, das diese Aufgabe in Polynomialzeit lösen kann.

Thema dieser Arbeit ist das Analogon des Faktorisierungsproblems für Polynome über endlichen Körpern $\mathbb{F}_q$ sowie dem Ring $\mathbb{Z}$ der ganzen Zahlen. Die präzise Aufgabenstellung lautet für $R \in \{\mathbb{F}_q, \mathbb{Z}\}$ wie folgt:

> *Gegeben ein Polynom $f \in R[X]$ vom Grad $\geqslant 1$, berechne eine Folge paarweise verschiedener irreduzibler Polynome $(g_1, \ldots, g_r) \subseteq R[X]$ mit zugehörigen positiven Vielfachheiten $(e_1, \ldots, e_r) \subseteq \mathbb{N}$, sodass*
>
> $$f = \prod_{i=1}^{r} g_i^{e_i}$$
>
> *erfüllt ist.*

Da $\mathbb{F}_q$ und $\mathbb{Z}$ — und somit auch die Polynomringe über diesen Ringen — faktoriell sind, ist diese Zerlegung (bis auf Umordnung der Faktoren und Multiplikation mit Einheiten) eindeutig.

Überraschenderweise scheint die Faktorisierung von Polynomen deutlich einfacher zu sein, als es für ganze Zahlen der Fall ist. Der 1967 veröffentlichte Berlekamp-Algorithmus [1] war das erste Verfahren, das es ermöglichte, Polynome über einem endlichen Körper effizient zu faktorisieren. Wenig später ging man dazu über, den monolithischen Algorithmus durch zwei kleinere Teilschritte zu ersetzen: *Distinct-* und *Equal-degree*-Faktorisierung. Erstere bezeichnet das Trennen des (quadratfreien Teils des) Eingabepolynoms in Produkte der irreduziblen Teiler gleichen Grades, zweitere das Aufspalten dieser Produkte. Durch einfache Probedivision lassen sich zum Schluss die Vielfachheiten der gefundenden irreduziblen Teiler bestimmen. Berlekamps *Distinct-degree*-Verfahren [2], das in Abschnitt 2.1 vorgestellt wird, benutzt ein Resultat von Legendre [cf. 6, 4.6.2]. Der Algorithmus zur *Equal-degree*-Aufspaltung, siehe Abschnitt 2.2, ist eine Variante des Verfahrens von Cantor und Zassenhaus [3].

Es stellt sich heraus, dass sich Polynome f in $\mathbb{Z}[X]$ unter Verwendung des Algorithmus für endliche Körper faktorisieren lassen. Wählt man beispielsweise eine Primzahl p hinreichend groß, so entsprechen die symmetrischen Repräsentanten der Koeffizienten eines modulo p reduzierten Teilers von f bereits den Koeffizienten über $\mathbb{Z}$; es ist also hinreichend, das Bild eines Teilers unter dem Reduktionshomomorphismus modulo p zu bestimmen. Eine effizientere Methode ist, modulo einer *kleinen* Primzahl p zu faktorisieren, um dann mithilfe des Hensel-Lemmas (Abschnitt 3.2) eine Faktorisierung modulo p^e für beliebig große e berechnen zu können.

Dabei tritt jedoch ein Problem auf: durch die Reduktion modulo p^e kann ein über $\mathbb{Z}$ irreduzibles Polynom in ein echtes Produkt über $\mathbb{Z}/p^e\mathbb{Z}$ zerfallen. Zum Beispiel ist das Polynom $X^2 + 1$ irreduzibel über $\mathbb{Z}$, aber sein Reduziertes modulo 2 ist gleich $(X + 1)^2 \in \mathbb{F}_2[X]$. Es ist also nötig, Produkte von Teilern modulo p^e zu finden, die sich zu echten Teilern über $\mathbb{Z}$ ergeben (Abschnitt 3.4). Die einfachste Methode ist Ausprobieren: Gegeben eine irreduzible Faktorisierung $g_1, \ldots, g_r \in (\mathbb{Z}/p^e\mathbb{Z})[X]$ von $f \bmod p^e$, prüfe für alle nichtleeren Teilmengen $\mathcal{S} \subseteq \{1, \ldots, r\}$, ob $g = \prod_{i \in \mathcal{S}} g_i$ über $\mathbb{Z}$ ein Teiler von f ist. Iteriert man über die Teilmengen in aufsteigender Kardinalität und entfernt bei einem Fund jeweils die zugehörigen g_i, so ist garantiert, dass g dann auch irreduzibel ist. Man beachte, dass $\mathcal{S}$ im schlimmsten Fall $2^r - 1$ Teilmengen durchlaufen muss. Daher hat dieses Verfahren prinzipiell exponentielle Laufzeit, obwohl es sich für praktische Zwecke als wertvoll erwiesen hat. Eine theoretische Verbesserung erzielten zunächst Lenstra, Lenstra und Lovász [7], wobei ihr Polynomialzeitalgorithmus keine vollständige *Equal-degree*-Faktorisierung durchführt, sondern mithilfe einer Gitterreduktion Faktoren über $\mathbb{Z}$ konstruiert werden, um das Kombinationsproblem gänzlich zu vermeiden. Eine praktische Verbesserung, die der hier vorgestellten Struktur folgt, ist das Verfahren nach van Hoeij [8, 4]. Es benutzt ebenfalls Gitterreduktion; allerdings nicht, um das Kombinationsproblem gänzlich zu umgehen, sondern um es effizient (in polynomieller Zeit) zu lösen.

Die Komponenten des in dieser Arbeit vorgestellten Faktorisierungsalgorithmus werden in Abbildung 1 veranschaulicht.

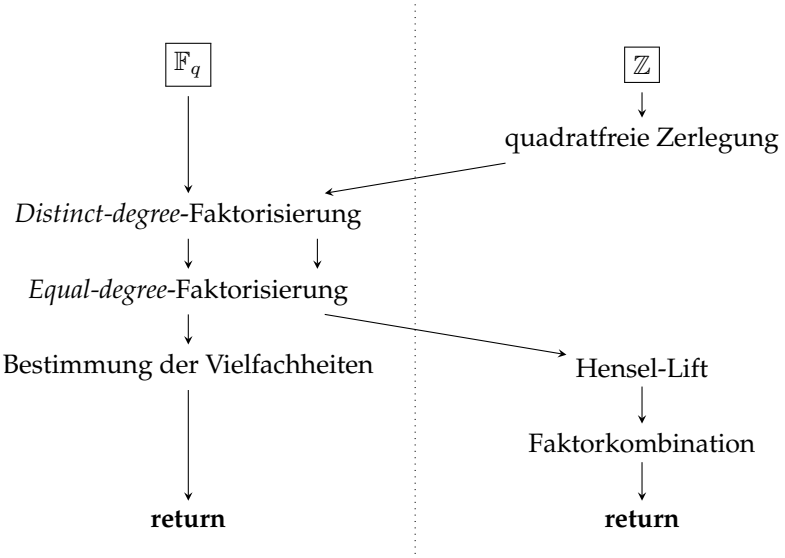

Abbildung 1: Struktur eines modernen Polynomfaktorisierungsalgorithmus

2 Faktorisierung über endlichen Körpern

Im Folgenden sei $q = p^e > 1$ stets eine Primzahlpotenz.

2.1 *Distinct-degree*-Faktorisierung

Definition 1. Sei $f \in \mathbb{F}_q[X]$ normiert vom Grad $n \geqslant 1$. Die *Distinct-degree*-Faktorisierung von f ist eine Folge von $s \leqslant n$ normierten Polynomen $(g_1, \ldots, g_s)$, sodass jedes g_d genau das Produkt der normierten, irreduziblen Teiler von f vom Grad d ist.

Um eine solche Folge berechnen zu können, benötigen wir zunächst zwei Hilfslemmata.

Lemma 2. $X^q - X = \prod_{a \in \mathbb{F}_q} (X - a)$.

Beweis. Nach dem kleinen Satz von Fermat ist jedes $a \in \mathbb{F}_q$ Nullstelle von $X^q - X \in \mathbb{F}_q[X]$. Daher folgt aus der Gleichheit der Grade und der Normiertheit die Behauptung. □

Lemma 3. Sei $d \in \mathbb{N}$. Sei $\mathcal{S}$ die Menge aller normierten, irreduziblen Polynome in $\mathbb{F}_q[X]$, deren Grad Teiler von d ist. Dann gilt

$$X^{q^d} - X = \prod_{f \in \mathcal{S}} f \ \in \mathbb{F}_q[X].$$

Beweis. Wir zeigen: Ist $f \in \mathbb{F}_q[X]$ vom Grad n normiert und irreduzibel, so gilt

$$f \mid X^{q^d} - X \quad \Longleftrightarrow \quad n \mid d.$$

Wegen $(X^{q^d} - X)' = q^d X^{q^d - 1} - 1 = -1 \in \mathbb{F}_q^\times$ ist $X^{q^d} - X$ separabel, womit dann die Aussage folgt.
Man betrachte dazu die Körpererweiterung $\mathbb{F}_{q^d}/\mathbb{F}_q$.

„⇒". Falls $f \mid X^{q^d} - X$ über $\mathbb{F}_{q^d}$ gilt, dann existiert wegen Lemma 2, angewandt auf $\mathbb{F}_{q^d}$, und der Eindeutigkeit der Zerlegung in irreduzible Elemente ein $a \in \mathbb{F}_{q^d}$ mit $X - a \mid f$ über $\mathbb{F}_{q^d}$, also $f(a) = 0$. Da f irreduzibel ist, ist es bereits das Minimalpolynom von a über $\mathbb{F}_q$. Daraus folgt

$$\mathbb{F}_q[X]/\langle f \rangle \cong \mathbb{F}_q(a), \quad \text{und daher} \quad |\mathbb{F}_q(a)| = |\mathbb{F}_q[X]/\langle f \rangle| = |\mathbb{F}_q|^{\deg f} = q^n.$$

Andererseits ist $\mathbb{F}_q(a)$ wegen $a \in \mathbb{F}_{q^d}$ Teilkörper von $\mathbb{F}_{q^d}$. Somit gibt es einen Exponenten $e \in \mathbb{N}$ mit $q^d = (q^n)^e = q^{ne}$, und es folgt die Behauptung $n \mid d$.

„⇐". Es sei umgekehrt n Teiler von d. Setze $F = \mathbb{F}_q[X]/\langle f\rangle \cong \mathbb{F}_{q^n}$ und $a = X + \langle f\rangle \in F$. Offensichtlich ist $f(a) = f(X + \langle f\rangle) = f + \langle f\rangle = 0$, also $X - a \mid f$ in $F[X]$. Da mit $e = \sum_{i=1}^{\lfloor d/n\rfloor} q^{d-i\cdot n}$

$$q^d - 1 = (q^n - 1)\cdot e,$$

ist

$$X^{q^d-1} - 1 = (X^{q^n-1} - 1)\cdot \sum_{i=1}^{e} X^{(q^n-1)(e-i)},$$

und Multiplikation mit X ergibt

$$X^{q^n} - X \mid X^{q^d} - X.$$

Es folgt nach Lemma 2, angewandt auf $F \cong \mathbb{F}_{q^n}$, dass

$$X - a \mid X^{q^n} - X \mid X^{q^d} - X$$

und somit

$$X - a \mid \gcd(f, X^{q^d} - X) \in F[X].$$

Da aber der größte gemeinsame Teiler beim Übergang in einen einen Erweiterungskörper unverändert bleibt, ist $\gcd(f, X^{q^d} - X) \in \mathbb{F}_q[X]$ nichtkonstant und wegen der Irreduzibilität von f gleich f. Dies zeigt die Behauptung $f \mid X^{q^d} - X$. □

Mithilfe der in Lemma 3 gezeigten Identität und dem euklidischen Algorithmus zur Berechnung des größten gemeinsamen Teilers kann ein Algorithmus zur *Distinct-degree*-Faktorisierung konstruiert werden:

Algorithmus 4 (*Distinct-degree*-Faktorisierung)**.**
Eingabe. q Primzahlpotenz, $f \in \mathbb{F}_q[X]$ normiert.
Ausgabe. Die *Distinct-degree*-Faktorisierung des quadratfreien Teils von f.

1. $d := 1$; $h := X^q \in \mathbb{F}_q[X]$.
2. $g_d := \gcd(h - X, f)$; $t := g_d$.
3. $f := f/t$; $t := \gcd(f, t)$. Falls $t \neq 1$, **goto** 3.
4. Falls $f = 1$, **return** $(g_1, \ldots, g_d)$.
5. $h := h^q \bmod f$; $d := d + 1$. **goto** 2.

Lemma 5. Algorithmus 4 arbeitet korrekt.

Beweis. Offensichtlich gilt in Schritt 2 stets $h \equiv X^{q^d} \pmod f$. Mit Lemma 3 ist damit g_d das Produkt der irreduziblen Teiler von f, deren Grad d teilt. Da Schritt 3 in jeder Iteration die neu gefundenen Teiler von f „herausdividiert" und f somit in Schritt 2 keine Teiler kleineren Grades als d hat, folgt die Behauptung. □

2.2 *Equal-degree*-Faktorisierung

Wie in Abschnitt 1 angekündigt, benötigen wir als nächstes ein Verfahren, um die soeben berechneten Produkte von irreduziblen Polynomen gleichen Grades weiter zu zerlegen.

Im folgenden Abschnitt sei stets $f \in \mathbb{F}_q[X]$ vom Grad $n \geqslant 2$ normiert und quadratfrei und $d < n$ mit $d \mid n$, sodass alle $r = n/d$ irreduziblen Teiler $f_1, \ldots, f_r \in \mathbb{F}_q[X]$ von f vom Grad d sind. (Insbesondere sind diese Bedingungen von einer *Distinct-degree*-Faktorisierung erfüllt.)

Definition 6. Die *Equal-degree*-Faktorisierung berechnet zu gegebenem f, d und q die irreduziblen Teiler $f_1, \ldots, f_r$ von f.

Sei zunächst q ungerade. Dann lässt sich das folgende Verfahren auf ein Polynom f anwenden, um mit großer Wahrscheinlichkeit ein echtes Teilerpolynom von f zu erhalten.

Algorithmus 7 (*Equal-degree*-Aufspaltung für *ungerade* q)**.**
Eingabe. q ungerade Primzahlpotenz, $f \in \mathbb{F}_q[X]$ vom Grad n quadratfrei und normiert das Produkt irreduzibler Polynome gleichen Grades $d < n$.
Ausgabe. Im Erfolgsfall ein echter Teiler von f, sonst nichts.

1. Wähle $a \in \mathbb{F}_q[X] \backslash \{0\}$ mit $\deg a < n$ zufällig und gleichverteilt.
2. $g_1 := \gcd(a, f)$. Falls $g_1 \neq 1$, **return** g_1.
3. $b := a^{(q^d-1)/2} - 1 \bmod f$.
4. $g_2 := \gcd(b, f)$. Falls $g_2 \notin \{1, f\}$, **return** g_2.
5. **fail**.

Lemma 8. Algorithmus 7 findet mit Wahrscheinlichkeit $\geqslant 1 - 2^{1-r} \geqslant \frac{1}{2}$ einen echten Teiler von f.

Beweis. Falls der Algorithmus ein Ergebnis g liefert, so gilt in Schritt 2 offenbar $\deg g \leqslant \deg a < n$, womit $g \neq f$ und damit bei jeder möglichen Rückgabe $g \notin \{1, f\}$ sichergestellt ist.

Um die Aussage über die Erfolgswahrscheinlichkeit zu zeigen, betrachten wir zunächst den Fall, dass der Algorithmus in Schritt 2 noch nicht terminiert. Wir halten lediglich fest, dass a beim Erreichen von Schritt 3 teilerfremd zu f ist, weswegen $\overline{a} := a + \langle f \rangle$ gleichverteilt auf $\mathcal{G} := (\mathbb{F}_q[X]/\langle f \rangle)^\times$ ist. Alle f_i sind irreduzibel und paarweise verschieden, und somit teilerfremd. Nach dem chinesischen Restsatz existiert daher der Isomorphismus

$$\begin{aligned} \chi \colon R := \mathbb{F}_q[X]/\langle f \rangle &\longrightarrow \mathbb{F}_q[X]/\langle f_1 \rangle \times \cdots \times \mathbb{F}_q[X]/\langle f_r \rangle =: R_1 \times \cdots \times R_r, \\ \alpha + \langle f \rangle &\longmapsto (\alpha + \langle f_1 \rangle, \ldots, \alpha + \langle f_r \rangle) =: (\chi_1(\alpha), \ldots, \chi_r(\alpha)). \end{aligned}$$

Für alle $i \in \{1, \ldots, r\}$ ist der Faktorring R_i isomorph zu $\mathbb{F}_{q^d}$. Schreibe $e := (q^d - 1)/2$. Da die Gruppe $(R_i^\times, \cdot) \cong (\mathbb{F}_{q^d}^\times, \cdot)$ zyklisch ist von Ordnung $q^d - 1 = 2e$, ist $\chi_i(\overline{a})^e \in \{-1, 1\}$. Beide Fälle treten mit Wahrscheinlichkeit $\frac{1}{2}$ auf, da $\chi_i(\overline{a})$ gleichverteilt auf $R_i^\times$ ist. Es folgt, dass

$$\chi_i(\overline{a})^e - 1 = \chi_i(b + \langle f \rangle) = \chi_i(\overline{b}) = 0$$

für genau die Hälfte der a gilt.

Aber es gilt $\chi_i(\overline{b}) = 0$ genau dann, wenn $f_i \mid b$, also ist für jede Partitionierung $\mathcal{S} \dot\cup \bar{\mathcal{S}} := \{1, \ldots, r\}$ die Wahrscheinlichkeit, dass genau diejenigen f_i mit $i \in \mathcal{S}$ Teiler von b sind, gleich $\left(\frac{1}{2}\right)^r$. Da $\prod_{i \in \mathcal{S}} f_i$ genau dann *kein* echter Teiler von f ist, wenn $\mathcal{S} = \varnothing$ oder $\mathcal{S} = \{1, \ldots, r\}$, ist die *Erfolgs*wahrscheinlichkeit gegeben durch $1 - 2^{-r} - 2^{-r} = 1 - 2^{1-r}$.

Ist p die Wahrscheinlichkeit, dass bereits in Schritt 2 ein echter Teiler gefunden wird, so folgt für die gesamte Erfolgswahrscheinlichkeit des Algorithmus nach dem Satz von der totalen Wahrscheinlichkeit

$$\Pr[\textbf{return}] = 1 \cdot p + (1 - 2^{1-r}) \cdot (1 - p) = 1 - 2^{1-r} + 2^{1-r} p \geqslant 1 - 2^{1-r} \geqslant \frac{1}{2}.$$

□

Bemerkung 9. Eine naheliegende Optimierung ist: Man wähle in Schritt 1 des Algorithmus 7 nur aus den nichtkonstanten Polynomen. Dies vergrößert die Erfolgswahrscheinlichkeit und führt zu einem früheren Erkennen des Misserfolgs, da konstante a in Schritt 2 und 4 ohnehin $\gcd(\ldots, f) \in \{1, f\}$ hervorbringen.

Offenbar ergibt oben angegebener Algorithmus 7 keinen Sinn für gerade q. Es lässt sich jedoch eine ähnliche Idee auf Körper der Charakteristik 2 anwenden:

Algorithmus 10 (*Equal-degree*-Aufspaltung für *gerade* q)**.**
Eingabe. $q = 2^k$ Primzahlpotenz, $f \in \mathbb{F}_q[X]$ vom Grad n quadratfrei und normiert das Produkt irreduzibler Polynome gleichen Grades $d < n$.
Ausgabe. Im Erfolgsfall ein echter Teiler von f, sonst nichts.

1. Wähle $a \in \mathbb{F}_q[X]$ mit $\deg a < n$ zufällig und gleichverteilt.
2. $b := \sum_{i=0}^{dk-1} a^{2^i} \bmod f$.
3. $g_2 := \gcd(b, f)$. Falls $g_2 \notin \{1, f\}$, **return** g_2.
4. **fail**.

Lemma 11. Algorithmus 10 findet mit Wahrscheinlichkeit $\geqslant \frac{1}{2}$ einen echten Teiler von f.

Beweis. Der Beweis verläuft im Wesentlichen analog zu dem von Lemma 8.

Definiere für $m \in \mathbb{N}$ das Polynom $T_m = \sum_{i=0}^{m-1} X^{2^i} \in \mathbb{F}_2[X]$. Für alle m gilt, wobei die Summationsvariablen stets von 0 bis $m-1$ laufen,

$$\begin{aligned}
& T_m(T_m+1) \\
= \; & \sum_i \sum_j X^{2^i} X^{2^j} + \sum_i X^{2^i} \\
= \; & \left(\sum_i \sum_j \delta_{(j<i)} X^{2^i+2^j} + \sum_i \sum_j \delta_{(j>i)} X^{2^i+2^j} \right) + \left(\sum_i X^{2^i+2^i} + \sum_i X^{2^i} \right) \\
= \; & \left(\sum_i \sum_j \delta_{(j<i)} X^{2^i+2^j} + \sum_j \sum_i \delta_{(i>j)} X^{2^j+2^i} \right) + \sum_i \left(X^{2^i} + X^{2^{i+1}} \right) \\
= \; & 0 + \left(X^{2^0} + 0 + X^{2^{(m-1)+1}} \right) \\
= \; & X^{2^m} + X.
\end{aligned}$$

Für alle $\alpha \in \mathbb{F}_{2^m}$ gilt daher nach dem kleinen Satz von Fermat

$$T_m(\alpha)(T_m(\alpha)+1) = \alpha^{2^m} + \alpha = 0$$

und somit, da $\mathbb{F}_{2^m}$ nullteilerfrei ist, $0 \in \{T_m(\alpha), T_m(\alpha)+1\}$. Insgesamt folgt

$$\forall \alpha \in \mathbb{F}_{2^m}.\ T_m(\alpha) \in \{0,1\} = \mathbb{F}_2.$$

Da $\operatorname{char} \mathbb{F}_{2^m} = 2$, ist $(\alpha+\beta)^{2^i} = \alpha^{2^i} + \beta^{2^i}$ für $\alpha, \beta \in \mathbb{F}_{2^m}$ und es folgt, dass die durch T_m induzierte Abbildung $\mathbb{F}_{2^m} \to \mathbb{F}_2$ ein $\mathbb{F}_2$-Vektorraumhomomorphismus ist. Nach dem Basisergänzungssatz gibt es eine $\mathbb{F}_2$-Basis $\{b_1, \ldots, b_m\}$ von $\mathbb{F}_{2^m}$ mit $b_1 = 1$. Mit $F = \langle b_2, \ldots, b_m \rangle \subseteq \mathbb{F}_{2^m}$ gilt $F \dot\cup (1+F) = \mathbb{F}_{2^m}$ und $|F| = |1+F|$, also folgt für α auf $\mathbb{F}_{2^m}$ gleichverteilt

$$\begin{aligned}
& \Pr[T_m(\alpha) = 0] \\
= \; & \Pr[T_m(\alpha) = 0 \mid \alpha \in F] \cdot \Pr[\alpha \in F] + \Pr[T_m(\alpha) = 0 \mid \alpha \in 1+F] \cdot \Pr[\alpha \in 1+F] \\
= \; & \Pr[T_m(\alpha) = 0 \mid \alpha \in F] \cdot \frac{1}{2} + \Pr[T_m(1+\alpha) = 1 + T_m(\alpha) = 0 \mid \alpha \in F] \cdot \frac{1}{2} \\
= \; & \Pr[T_m(\alpha) \in \mathbb{F}_2 \mid \alpha \in F] \cdot \frac{1}{2} \\
= \; & \frac{1}{2}.
\end{aligned}$$

Betrachte einen der Homomorphismen $\chi_i \colon R \to R_i$ des chinesischen Restsatzes. Es gilt

$$\chi_i(\overline{b}) = \chi_i(\overline{T_{kd}(a)}) = \chi_i\left(\overline{\sum_{i=0}^{kd-1} a^{2^i}} \right) = \sum_{i=0}^{kd-1} \chi_i(\overline{a})^{2^i} = T_{kd}(\chi_i(\overline{a})),$$

und da $\chi_i(\overline{a})$ gleichverteilt ist auf $R_i \cong \mathbb{F}_{q^d} = \mathbb{F}_{2^{kd}}$, ist $\chi_i(\overline{b})$ gleich 0 bzw. gleich 1 für jeweils genau die Hälfte der a.

Der Rest des Beweises entspricht Wort für Wort dem zu Lemma 8. □

Um mithilfe dieser Verfahren nicht nur einen, sondern alle irreduziblen Faktoren zu extrahieren, bietet sich folgender naheliegende Algorithmus an:

Algorithmus 12 (*Equal-degree*-Faktorisierung)**.**
Eingabe. q Primzahlpotenz, $f \in \mathbb{F}_q[X]$ vom Grad n quadratfrei und normiert das Produkt irreduzibler Polynome gleichen Grades $d \leqslant n$.
Ausgabe. Die Menge der irreduziblen Faktoren von f.

1. Falls $d = n$, **return** $\{f\}$.
2. Rufe wiederholt Algorithmus 7 bzw. 10 auf, bis er ein Ergebnis g liefert.
3. **return** $\mathfrak{rec}(g) \cup \mathfrak{rec}(f/g)$, wobei $\mathfrak{rec}$ einen rekursiven Aufruf dieses Algorithmus mit neuem f bezeichne.

Lemma 13. Algorithmus 12 arbeitet korrekt. *(Beweis klar.)*

2.3 Bestimmung der Vielfachheiten

Die bisher beschriebenen Verfahren finden lediglich eine Faktorisierung des *quadratfreien Teils* eines Polynoms. Wie bereits in Abschnitt 1 angedeutet, lassen sich die Vielfachheiten jedoch ganz einfach durch wiederholte Division bestimmen:

Algorithmus 14 (Bestimmung der Vielfachheiten)**.**
Eingabe. $f \in \mathbb{F}_q[X]$ normiert sowie die Menge seiner irreduziblen Faktoren $(g_1, \ldots, g_r) \subseteq \mathbb{F}_q[X]$.
Ausgabe. Vielfachheiten $(e_1, \ldots, e_r) \subseteq \mathbb{N}$, sodass $f = \prod_{i=1}^{r} g_i^{e_i}$.

1. $i := 1$.
2. $e_i := 0$.
3. $e_i := e_i + 1$; $f := f/f_i$. Falls $f \bmod f_i = 0$, **goto** 3.
4. $i := i + 1$. **goto** 2.

Lemma 15. Algorithmus 14 arbeitet korrekt. *(Beweis klar.)*

3 Faktorisierung über $\mathbb{Z}$

Es stellt sich heraus, dass wir zur Faktorisierung von Polynomen mit ganzzahligen Koeffizienten die bisher entwickelten Verfahren für endliche Körper wiederverwenden können: Ist $f \in \mathbb{Z}[X]$ ein Polynom über $\mathbb{Z}$, so sind für einen hinreichend großen Modulus m die Koeffizienten von f gerade die symmetrischen Repräsentanten der Koeffizienten von $f + m\mathbb{Z}[X]$.

3.1 Quadratfreie Zerlegung

Im gesamten Abschnitt sei K ein Körper der Charakteristik 0.

Definition 16 (Formale Ableitung)**.** Sei $f = \sum_{i=0}^{n} f_i X^i \in K[X]$. Definiere die *formale Ableitung* $f' \in K[X]$ von f als

$$f' = \sum_{i=0}^{n-1} (i+1) f_{i+1} X^i.$$

Für die formale Ableitung gelten viele der Rechenregeln für die „richtige" Ableitung aus der Differentialrechnung; unter anderem die folgenden Lemmata, die ohne ihre (einfachen) Beweise wiedergegeben werden.

Lemma 17 (Produktregel)**.** Für $f, g \in K[X]$ gilt $(fg)' = f'g + fg'$. *(ohne Beweis.)*

Lemma 18 (Kettenregel)**.** Für $f, g \in K[X]$ gilt $(f(g))' = f'(g)g'$. *(ohne Beweis.)*

Mithilfe der formalen Ableitung lässt sich der folgende einfache Algorithmus zur quadratfreien Zerlegung formulieren.

Algorithmus 19 (quadratfreie Zerlegung (Charakteristik 0))**.**
Eingabe. $f \in K[X]$ normiert vom Grad $\geqslant 1$.
Ausgabe. Der quadratfreie Teil von f.

1. **return** $f/\gcd(f, f')$.

Lemma 20. Algorithmus 19 arbeitet korrekt.

Beweis. Sei $f = \prod_{i=1}^{m} f_i^{e_i} \in K[X]$ mit $m \in \mathbb{N}$, paarweise verschiedenen irreduziblen Polynomen $f_i \in K[X]$ und positiven Vielfachheiten $e_i \in \mathbb{Z}$. Unter Verwendung von Lemmata 17 und 18 erhält man (wobei Summationen und Produkte, sofern nicht anders angegeben, von 1 bis m laufen)

$$f' = \sum_i (f_i^{e_i})' \prod_{j \neq i} f_j^{e_j} = \sum_i (e_i f_i^{e_i - 1} f_i') \prod_{j \neq i} f_j^{e_j} = \sum_i e_i f_i' \prod_j f_j^{e_j - \delta_{(j=i)}}.$$

Sei $k \in \{1, \ldots, m\}$. Es folgt weiter

$$f' = \underbrace{e_k f_k' \prod_j f_j^{e_j - \delta(j=k)}}_{\in \langle f_k^{e_k - 1} \rangle \setminus \langle f_k^{e_k} \rangle} + \sum_{i \neq k} e_i f_i' \underbrace{\prod_j f_j^{e_j - \delta_{(j=i)}}}_{\in \langle f_k^{e_k} \rangle},$$

also $f_k^{e_i - 1} \mid f'$, aber $f_i^{e_i} \nmid f'$. Insgesamt ergibt sich

$$f/\gcd(f, f') = f/\prod_i f_i^{e_i - 1} = \prod_i f_i.$$

□

Ist eine quadratfreie Zerlegung über $\mathbb{Z}$ gefunden, so lässt sich der quadratfreie Teil über einem endlichen Körper faktorisieren. Stellt man sicher, dass der Modulus *nicht* von der Diskriminante des Polynoms geteilt wird, so ist das reduzierte Polynom ebenfalls wieder quadratfrei und die Bestimmung der Vielfachheiten (Abschnitt 2.3) kann weggelassen werden:

Lemma 21. Ist $f \in \mathbb{Z}[X]$ quadratfrei und gilt $m \nmid \operatorname{Disk} f$, so ist $f + m\mathbb{Z}[X]$ ebenfalls quadratfrei.

Beweis. Hat $f + m\mathbb{Z}$ einen wiederholten Teiler vom Grad $\geqslant 1$, so ist $\operatorname{Disk}(f + m\mathbb{Z}[X]) = \operatorname{Disk} f + m\mathbb{Z} = 0$ und es folgt $m \mid \operatorname{Disk} f$ im Widerspruch zur Annahme. □

3.2 Henselsches Lemma

Wie in Abschnitt 1 angedeutet, existiert ein effizientes Verfahren, mit dem sich aus einer Faktorisierung modulo einer kleinen Primzahl eine Faktorisierung modulo einer beliebig großen Potenz dieser Zahl gewinnen lässt. Dieses Verfahren ist das *Hensel-Lifting*, welches aus wiederholter Anwendung des folgenden Algorithmus besteht.

Algorithmus 22 (Hensel-Schritt)**.**
Eingabe. $q = p^e > 1$ Primzahlpotenz und $u, v, w, a, b \in \mathbb{Z}[X]$ mit [(a)] v normiert, $\deg b < \deg v$, [(b)] $\deg a < \deg w$ und [(c)] $\deg u = \deg v + \deg w$, sodass [(d)] $u \equiv vw \pmod{q}$ sowie [(e)] $av + bw \equiv 1 \pmod{p}$.
Ausgabe. Polynome $v^*, w^* \in \mathbb{Z}[X]$, die die Bedingungen (a)–(e) mit $e + 1$ anstelle von e erfüllen.

1. $f := u - vw$.
2. Division mit Rest liefert t, r mit $bf = tv + r$ und $\deg r < \deg v$.
3. $v^* := v + r$.
4. $w^* := (w + af + tw) \bmod pq$.
5. **return** v^*, w^*.

Für den Korrektheitsbeweis zeigen wir zunächst das folgende einfache Hilfslemma.

Lemma 23. Sei R ein Integritätsring und $m \in R$. Sei $b \in R[X]$ normiert und sei $a \in R[X]$ Vielfaches von m. Dann sind Quotient $q \in R[X]$ und Rest $r \in R[X]$ der Division von a durch b ebenfalls Vielfache von m.

Beweis. Es existieren $\bar{q}, \bar{r} \in R[X]$ mit $\deg \bar{r} < \deg b$ und $a/m = \bar{q}b + \bar{r}$. Aus $\deg(m\bar{r}) = \deg \bar{r} < b$ und $a = m\bar{q}b + m\bar{r}$ folgt mit der Eindeutigkeit von q und r die Behauptung $q = m\bar{q} \in \langle m \rangle$ und $r = m\bar{r} \in \langle m \rangle$. □

Lemma 24. Algorithmus 22 arbeitet korrekt.

Beweis. Wir zeigen für jede der Eigenschaften (a)–(e), dass v^* und w^* sie (mit pq anstelle von p) ebenfalls erfüllen.

(d) Aus $f \in \langle q \rangle$ folgt mit Lemma 23 auch $t, r \in \langle q \rangle$. Modulo pq gilt daher

$$\begin{aligned} u - v^*w^* &\equiv u - (v + bf - tv)(w + af + tw) \\ &\equiv (u - vw) - v(af + tw) - w(bf - tv) - \underbrace{(bf - tv)}_{\in\langle q\rangle}\underbrace{(af + tw)}_{\in\langle q\rangle} \\ &\equiv f - vaf - vtw - wbf + wtv \\ &\equiv \underset{\langle q\rangle}{\underset{\cap}{f}}\underbrace{(1 - av - bw)}_{\in\langle p\rangle} \equiv 0 \end{aligned}$$

und es folgt $u \equiv v^*w^* \pmod{pq}$.

(e) Modulo p gilt

$$\begin{aligned} av^* + bw^* &\equiv a(v + r) + b(w + af + tw) \\ &\equiv av + bw + \underbrace{ar + b(af + tw)}_{\in\langle q\rangle} \\ &\equiv av + bw, \end{aligned}$$

was zu zeigen ist.

(a) Nach Definition von r ist $\deg r < \deg v$ und somit $\operatorname{lc} v^* = \operatorname{lc}(v + r) = \operatorname{lc} v = 1$ sowie $\deg v^* = \deg v > \deg b$ (wobei lc für den Leitkoeffizienten steht).

(c) Wir zeigen $\deg w^* = \deg w$. Da w^* in Schritt 4 des Algorithmus 22 modulo pq reduziert wird, ist $\operatorname{lc} w^* \notin \langle pq \rangle$, weswegen $\deg(w^* + \langle pq \rangle) = \deg w^*$ gilt. Außerdem folgt mit $\operatorname{lc}(u + \langle pq \rangle) = \operatorname{lc}(w^* + \langle pq \rangle) \neq 0$ auch $\operatorname{lc} u \notin \langle pq \rangle$ und hieraus $\deg(u + \langle pq \rangle) = \deg u$. Mit (a) und (d) ergibt sich

$$\begin{aligned} \deg u &= \deg(v^*w^* + \langle pq \rangle) \\ &= \deg(v^* + \langle pq \rangle) + \deg(w^* + \langle pq \rangle) \\ &= \deg v + \deg w^*, \end{aligned}$$

und dies impliziert wegen $\deg u = \deg v + \deg w$ die Behauptung.

(b) folgt aus $\deg w^* = \deg w$, was im vorherigen Punkt gezeigt wurde.

□

3.3 Mignotte-Schranke

Inzwischen können wir Faktorisierungen von Polynomen modulo beliebig großer Primzahlpotenzen erzeugen. Eine Antwort auf die entscheidende Frage, *wie* groß diese sein müssen, damit garantiert alle irreduziblen Teiler über $\mathbb{Z}$ gefunden werden, gibt die Mignotte-Schranke, die in diesem Abschnitt hergeleitet wird.

Bemerkung 25 (Normen für Polynome)**.** Für $p \in (0, \infty]$ übertragen sich die p-Normen $\|\cdot\|_p$ durch Anwendung auf den Koeffizientenvektor auf Polynome $f = f_0 + f_1X + \cdots + f_nX^n \in \mathbb{C}[X]$, i. e.

$$\|f\|_p = \left(\sum_{j=0}^{n} |f_j|^p\right)^{1/p} \quad \text{bzw.} \quad \|f\|_\infty = \max\{\, |f_j| \mid j \in \{0, \ldots, n\}\}.$$

Lemma 26. Sei $f \in \mathbb{C}[X]$ ein Polynom und $z \in \mathbb{C}$ eine Konstante. Dann gilt

$$\|(X - z)f\|_2 = \|(\overline{z}X - 1)f\|_2.$$

Beweis. Sei $n = \deg f$. Definiere zur Vereinfachung der Schreibweise $f_{-1} = f_{n+1} = 0$. Es gilt

$$\begin{aligned}
\|(X-z)f\|_2^2 \;=\; \sum_{j=0}^{n+1} |f_{j-1} - f_j z|^2 \;&=\; \sum_{j=0}^{n+1} \left(f_{j-1} - f_j z\right)\left(\overline{f_{j-1}} - \overline{f_j z}\right) \\
&= \sum_{j=0}^{n+1} \left(|f_{j-1}|^2 - \overline{f_{j-1}} f_j z - f_{j-1}\overline{f_j z} + |f_j z|^2\right) \\
&= \sum_{j=0}^{n+1} \left(|f_{j-1} z|^2 - \overline{f_{j-1}} f_j z - f_{j-1}\overline{f_j z} + |f_j|^2\right) \\
&= \sum_{j=0}^{n+1} \left(\overline{z} f_{j-1} - f_j\right)\left(z\overline{f_{j-1}} - \overline{f_j}\right) \\
&= \|(\overline{z}X - 1)f\|_2^2.
\end{aligned}$$

Aus der Nichtnegativität der 2-Norm folgt damit die Behauptung. □

Definition 27. Sei $f \in \mathbb{C}[X]$ ein Polynom vom Grad n und $z_1, \ldots, z_n \in \mathbb{C}$ die (nicht notwendigerweise verschiedenen) Nullstellen von f. Definiere $M(f)$ als

$$M(f) = |f_n| \cdot \prod_{j=1}^{n} \max\{1, |z_j|\}.$$

Lemma 28 (Landau-Ungleichung)**.** Sei $f \in \mathbb{C}[X]$ ein Polynom. Dann gilt

$$M(f) \leqslant \|f\|_2.$$

Beweis. Sei $n = \deg f$. Es gibt ein $k \in \{0, \ldots, n\}$ und eine Sortierung der Nullstellen $z_1, \ldots, z_n \in \mathbb{C}$ von f, sodass $|z_j| > 1$ für alle $j \leqslant k$ und $|z_j| \leqslant 1$ für alle $j > k$. Setze

$$g = f_n \cdot \prod_{j=1}^{k} (\overline{z_j}X - 1) \cdot \prod_{j=k+1}^{n} (X - z_j).$$

Dann gilt

$$\begin{aligned}
M(f)^2 = \left|f_n \cdot \prod_{j=1}^{k} z_j \cdot \prod_{j=k+1}^{n} 1\right|^2 \;=\; |\operatorname{lc} g|^2 \;\leqslant\; \|g\|_2^2 \;&=\; \left\|\frac{g}{\overline{z_1}X - 1} \cdot (X - z_1)\right\|_2^2 \\
&= \ldots \\
&= \left\|\frac{g}{\prod_{j=1}^{k}(\overline{z_j}X - 1)} \cdot \prod_{j=1}^{k}(X - z_j)\right\|_2^2 \\
&= \left\|f_n \cdot \prod_{j=1}^{n}(X - z_j)\right\|_2^2 \\
&= \|f\|_2^2,
\end{aligned}$$

wobei die Gleichheit $\|g\|_2^2 = \|f\|_2^2$ durch k-malige Anwendung von Lemma 26 gezeigt wird. Es folgt die Behauptung. □

Lemma 29. Sei $f \in \mathbb{C}[X]$ ein Polynom und $h \in \mathbb{C}[X]$ ein Teiler von f. Seien $n = \deg f$ und $m = \deg h$. Dann gilt

$$\|h\|_2 \leqslant 2^m M(h) \leqslant \left|\frac{h_m}{f_n}\right| 2^m \|f\|_2.$$

Beweis. Seien $u_1, \ldots, u_m \in \mathbb{C}$ die Nullstellen von h und $k \in \{1, \ldots, m\}$. Sei $\mathcal{S}$ die Menge der $(m-k)$-elementigen Teilmengen von $\{1, \ldots, m\}$. Nach dem Satz von Vieta ist

$$h_k = (-1)^{m-k} h_m \sum_{S \in \mathcal{S}} \prod_{j \in S} u_j,$$

also

$$|h_k| \leqslant |h_m| \sum_{S \in \mathcal{S}} \prod_{j \in S} |u_j| \leqslant |h_m| \binom{m}{m-k} \prod_{j=1}^{m} \max\{1, |u_j|\} = \binom{m}{k} M(h).$$

Es folgt

$$\|h\|_2 \leqslant \|h\|_1 = \sum_{k=0}^{m} |h_k| \leqslant \sum_{k=0}^{m} \binom{m}{k} M(h) = 2^m M(h).$$

Mit der Landau-Ungleichung (Lemma 28) ergibt sich die zweite Abschätzung daraus, dass jede Nullstelle von h auch Nullstelle von f ist. □

Corollar 30 (Mignotte-Schranke)**.** Sei $f \in \mathbb{Z}[X]$ vom Grad n. Ist $h \in \mathbb{Z}[X]$ vom Grad m ein Teiler von f, so gilt

$$\|h\|_\infty \leqslant \sqrt{n+1} \cdot 2^m \|f\|_\infty.$$

Beweis. Offenbar ist $\|h\|_\infty \leqslant \|h\|_2$. Mit Lemmata 28 und 29 erhält man daher $\|h\|_\infty \leqslant \left|\frac{h_m}{f_n}\right| 2^m \|f\|_2$. Über $\mathbb{Z}$ impliziert $\operatorname{lc} h \mid \operatorname{lc} f$, dass $|\operatorname{lc} h|$ durch $|\operatorname{lc} f|$ beschränkt ist, also folgt die Behauptung aus der Abschätzung

$$\|f\|_2 = \sqrt{\sum_{j=0}^{n} f_j^2} \leqslant \sqrt{\sum_{j=0}^{n} \|f\|_\infty^2} = \sqrt{(n+1)\|f\|_\infty^2} = \sqrt{n+1} \cdot \|f\|_\infty.$$

□

3.4 Faktorkombination

Es verbleibt das in Abschnitt 1 erwähnte Problem, dass Faktoren eines modulo p^e reduzierten Polynoms nicht unbedingt „echten" Teilern des ursprünglichen Polynoms über $\mathbb{Z}$ entsprechen. Am einfachsten löst man dieses Problem wie folgt (wobei $\mathcal{P}$ die Potenzmenge bezeichne):

Algorithmus 31 (Faktorkombination, naiv)**.**
Eingabe. $f \in \mathbb{Z}[X]$ vom Grad n normiert, $q \geqslant \sqrt{n+1} \cdot 2^{n+1} \|f\|_\infty$ Primzahlpotenz, $g_1, \ldots, g_r \in (\mathbb{Z}/q\mathbb{Z})[X]$ irreduzibel mit $f \bmod q = \prod_{i=1}^{r} g_i$.
Ausgabe. Ein irreduzibler Teiler (über $\mathbb{Z}$) von f.

1. $k := 2$; $(\mathcal{S}_2, \ldots, \mathcal{S}_{2^r}) := \mathcal{P}(\{1, \ldots, r\}) \backslash \varnothing$ in aufsteigender Kardinalität.
2. $g := \mathfrak{z}(\prod_{i \in \mathcal{S}_k} g_i)$, wobei $\mathfrak{z}\colon (\mathbb{Z}/q\mathbb{Z})[X] \to \mathbb{Z}[X]$ die Koeffizienten unter Verwendung symmetrischer Repräsentanten als ganze Zahlen interpretiere.
3. Falls $g \mid f$, **return** g.
4. $k := k + 1$; **goto** 2.

Durch Iteration dieses Verfahrens in naheliegender Weise lässt sich eine vollständige irreduzible Faktorisierung von f über $\mathbb{Z}$ finden.

Lemma 32. Algorithmus 31 arbeitet korrekt.

Beweis. Ist $g \in \mathbb{Z}[X]$ ein irreduzibler Teiler von f, so existiert wegen $g \bmod q \mid f \bmod q$ und nach der Eindeutigkeit der Zerlegung in irreduzible Elemente ein k, sodass $|\mathcal{S}_k|$ kleinstmöglich ist und

$$g \equiv \prod_{i \in \mathcal{S}_k} g_i \pmod{q}.$$

Nach der Bedingung $q \geqslant \sqrt{n+1} \cdot 2^{n+1} \|f\|_\infty$ folgt dann mit Corollar 30, dass $g' = \mathfrak{z}(\prod_{i \in \mathcal{S}_k} g_i)$ ein Teiler von f ist. Wäre g' nicht irreduzibel, so würde vom Algorithmus 31 bereits ein k mit kleinerem $|\mathcal{S}_k|$ gefunden, das einen der Faktoren von g' beschreibt; ergo ist $g' = g$.

Anschließend lässt sich der Algorithmus mit f/g', q und der Liste der g_i mit $i \notin \mathcal{S}_k$ als Eingabe erneut anwenden, bis alle Faktoren von g gefunden sind. □

Da k im schlimmsten Fall über alle nichtleeren Teilmengen von $\{1, \ldots, r\}$ iteriert, bis ein Faktor von f bestimmt werden konnte, ist die Laufzeit von Algorithmus 31 theoretisch exponentiell in r. Es stellt sich allerdings heraus, dass für „typische" Polynome bei weitem nicht der theoretisch benötigte Suchraum ausgeschöpft wird, sodass dieses Verfahren für viele Anwendungen durchaus praktisch verwendbar ist.

Wie bereits in Abschnitt 1 erwähnt, wurden beginnend 1982 auf Gitterreduktion basierende Algorithmen zur Faktorkombination vorgestellt [7], die zwar theoretisch effizienter, aber nicht praxisrelevant sind. Mit dem 2002 vorgestellten [8] und 2011 verbesserten [4] Algorithmus nach van Hoeij wurden Gitter-Verfahren zur Faktorkombination effizient und damit praktisch nutzbar gemacht.

Literatur

[1] BERLEKAMP, Elwyn R.: Factoring Polynomials Over Finite Fields. In: *Bell Systems Technical Journal* 46 (1967), S. 1853–1859

[2] BERLEKAMP, Elwyn R.: Factoring Polynomials Over Large Finite Fields. In: *Mathematics of Computation* 24 (1970), S. 713–735

[3] CANTOR, David G. ; ZASSENHAUS, Hans: A new algorithm for factoring polynomials over finite fields. In: *Mathematics of Computation* 36 (1981), S. 587–592

[4] HART, William ; VAN HOEIJ, Mark ; NOVOCIN, Andrew: Practical Polynomial Factoring in Polynomial Time. In: *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, ACM, 2011 (ISSAC '11). – ISBN 978–1–4503–0675–1, S. 163–170

[5] HOLT, Derek F. ; EICK, Bettina ; O'BRIEN, Eamonn A.: *Handbook of computational group theory*. Chapman & Hall/CRC, 2005 (Discrete mathematics and its applications). – ISBN 1–584–88372–3

[6] KNUTH, Donald E.: *The Art of Computer Programming, Volume II: Seminumerical Algorithms*. 2nd Edition. Addison-Wesley Longman Publishing Co., Inc., 1981. – ISBN 0–201–89684–2

[7] LENSTRA, Arjen K. ; LENSTRA, JR., Hendrik W. ; LOVÁSZ, László: Factoring polynomials with rational coefficients. In: *Mathematische Annalen* 261 (1982), S. 515–534

[8] VAN HOEIJ, Mark: Factoring Polynomials and the Knapsack Problem. In: *Journal of Number Theory* 95 (2002), S. 167–189