Kapitel 3
Modulare Methoden

§1: Rechnen mit homomorphen Bildern

In Kapitel I, §2, haben wir gesehen, daß selbst ein theoretisch so einfaches Verfahren wie der EUKLIDische Algorithmus schon bei zwei relativ kleinen Polynomen mit ggT eins zu riesigen Zwischenergebnissen führen kann. Diese Explosion der Zwischenergebnisse ist ein wohlbekanntes Problem der Computeralgebra, das beileibe nicht nur beim EUKLIDischen Algorithmus auftritt; es ist auch der Grund dafür, daß in der Computeralgebra die Speichergröße oft wichtiger ist als die Rechengeschwindigkeit.

Natürlich bemühten sich Mathematiker, seitdem sie Computer für symbolisches Rechnen benutzen, mit diesem Problem fertig zu werden, und haben eine ganze Reihe von Ansätze entwickelt. Zwei relativ universell einsetzbare Verfahren sollen in diesem und dem nächsten Kapitel vorgestellt werden.

Die Grundidee ist in beiden Fällen dieselbe: Wenn wir über $\mathbb{Z}$ oder über einem Polynomring $R[X]$ rechnen, kommen wir immer wieder an eine Stelle, an der wir dividieren müssen, und ab dann haben wir Nenner, die in vielen interessanten Fällen leider sehr schnell größer werden.

Rechnen wir allerdings statt in $\mathbb{Z}$ modulo einer Primzahl, also im Körper $\mathbb{F}_p = \mathbb{Z}/p = \mathbb{Z}/(p)$, so erhalten wir auch als Zwischenergebnisse Elemente aus $\mathbb{F}_p$ statt aus $\mathbb{Q}$, wir bleiben also immer in $\mathbb{F}_p$ – es sei denn, wir müssen in $\mathbb{Z}$ durch ein Vielfaches von p dividieren. Wenn wir modulo p rechnen, können wir hoffen, daß das so berechnete Ergebnis

gleich dem wirklich interessierenden Ergebnis modulo p ist. Das muß natürlich nicht der Fall sein; in solchen Fällen reden wir von schlechter Reduktion, andernfalls von guter Reduktion modulo p.

Im Falle guter Reduktion kennen wir das gesuchte Ergebnis modulo p. Falls wir wissen, daß alle dort vorkommenden Zahlen betragsmäßig kleiner sind als $p/2$, reicht das, um das Ergebnis zu rekonstruieren, denn zwischen $-p/2$ und $p/2$ gibt es keine zwei Zahlen, die dieselbe Restklasse modulo p haben. Für die Anwendung modularer Methoden ist es daher wesentlich, daß wir eine Schranke für den Betrag der vorkommenden Größen haben.

Oft wird diese Schranke ziemlich groß sein, und dann wird auch das Rechnen modulo einer Primzahl, die mehr als doppelt so groß sein muß, schnell teuer.

Zur Lösung dieses Problems gibt es zwei Ansätze: Entweder wir rechnen modulo mehrerer Primzahlen und versuchen, die Ergebnisse irgendwie zusammenzusetzen – darum geht es bei den modularen Methoden in diesem Kapitel. Alternativ können wir uns auf eine Primzahl p beschränken und dann versuchen, die Ergebnisse hochzuheben zu Ergebnissen modulo $p^2, p^3, p^4, \ldots$, bis wir über dem doppelten der Schranke liegen. Mit diesen sogenannten p-adischen Methoden werden wir uns im nächsten Kapitel beschäftigen.

Auch wenn wir zum Rechnen in einem Polynomring für eine der Variablen einen Wert einsetzen, haben wir dieselben beiden Möglichkeiten: Für nichtkonstante Polynome reicht es natürlich nie, nur einen Wert einzusetzen, aber die wohlbekannten Interpolationsverfahren erlauben uns, ein Polynom vom Grad höchstens d zu rekonstruieren, wenn wir seinen Wert an $d+1$ Stellen kennen – das ist hier die modulare Methode. Bei der p-adischen Methode beachten wir, daß der Wert eines Polynoms an der Stelle $X = c$ gerade das Polynom modulo $X - c$ ist. Können wir daraus das Polynom modulo $(X-c)^2$ und so weiter rekonstruieren, kennen wir ein Polynom vom Grad d, sobald wir es modulo $(X - c)^{d+1}$ kennen.

In diesem Kapitel geht es, wie gesagt, nur um modulare Methoden; im nächsten Paragraphen wollen wir deren Grundlage möglichst allgemein herleiten.

§2: Der chinesische Restesatz

Um sowohl $\mathbb{Z}$ als auch Polynomringe in einer Veränderlichen zusammenzufassen und in einer verallgemeinerungsfähigen Weise zu behandeln, beginnen wir ganz abstrakt:

Wir gehen aus von einem Ring R, wie üblich kommutativ und mit Einselement, und Idealen $I_j \lhd I$ für $j = 1, \ldots, r$.

Definition: Die Ideale $I_1, \ldots, I_r \lhd R$ heißen *paarweise erzeugend*, wenn es für je zwei Indizes $i \neq j$ Elemente $n_i^{(j)} \in I_i$ und $n_j^{(i)} \in I_j$ gibt, so daß $n_i^{(j)} + n_j^{(i)} = 1$ ist.

Für Ideale $(m_1), \ldots, (m_r) \lhd \mathbb{Z}$ ist jedes Element aus (m_i) von der Form am_i mit $a \in \mathbb{Z}$; diese Ideale sind also paarweise erzeugend, wenn es $a_i^{(j)} \in \mathbb{Z}$ gibt, so daß für $i \neq j$ gilt: $a_i^{(j)} m_i + a_j^{(i)} m_j = 1$. Dann müssen m_i und m_j teilerfremd sein, denn jeder gemeinsame Teiler ist auch ein Teiler der Eins. Sind umgekehrt m_i und m_j teilerfremd, so liefert uns der erweiterte EUKLIDische Algorithmus ganze Zahlen $a_i^{(j)}$ und $a_j^{(i)}$ derart, daß $a_i^{(j)} m_i + a_j^{(i)} m_j = 1$ ist. Hier bedeutet paarweise erzeugend also einfach, daß die Erzeugenden der Ideale paarweise teilerfremd sind.

Der chinesische Restesatz in seiner allgemeinsten Form besagt:

Satz: Sind $I_1, \ldots, I_r$ paarweise erzeugend, so ist

$$R/\bigcap_{j=1}^{r} I_j \cong \bigoplus_{j=1}^{r} R/I_j \,.$$

Zum *Beweis* betrachten wir die Abbildung

$$\Phi\colon \begin{cases} R \to \displaystyle\bigoplus_{j=1}^{r} R/I_j \\ f \mapsto (f + I_1, \ldots, f + I_r) \end{cases},$$

wobei $f + I_j$ die Restklasse von f modulo I_j bezeichnet. Diese ist genau dann das Nullelement von R/I_j, wenn f in I_j liegt; der Kern von Φ ist also der Durchschnitt der Ideale I_j.

Als nächstes wollen wir uns überlegen, daß Φ surjektiv ist: Wir gehen also aus von irgendwelchen Elementen $f_1, \ldots, f_r \in R$ und suchen ein Element $f \in R$ derart, daß modulo jedem der Ideale I_j die Elemente f und f_j die gleiche Restklasse haben.

Diese können wir uns wie im Beweis gegen Ende des letzten Kapitels mit einer Verallgemeinerung der LAGRANGE-Formel zur Interpolation verschaffen: Wir konstruieren uns für jedes j ein Element e_j, das modulo I_j die Eins von R/I_j ist und modulo der restlichen I_i die Null von R/I_i. Da die Ideale paarweise erzeugend sind, gibt es für $i \neq j$ Elemente $n_i^{(j)} \in I_i$ und $n_j^{(i)} \in I_j$ derart, daß $n_i^j + n_j^{(i)} = 1$ ist. Das Produkt

$$e_j = \prod_{\substack{i=1 \\ i \neq j}}^{r} n_i^{(j)}$$

liegt somit in allen Idealen I_i mit $i \neq j$, denn es ist ein Vielfaches von $n_i^{(j)}$. Außerdem ist

$$n_i^{(j)} = 1 - n_j^{(i)} \quad \text{mit} \quad n_j^{(i)} \in I_j \, ;$$

modulo I_j sind daher alle $n_i^{(j)}$ gleich dem Einselement von R/I_j. Damit ist auch e_j als Produkt dieser Elemente modulo I_j gleich eins. Setzen wir nun

$$f = \sum_{j=1}^{r} f_j e_j \, ,$$

so liegt

$$f - f_j e_j = \sum_{\substack{i=1 \\ i \neq j}}^{r} f_i e_i$$

in I_j, da alle e_i mit $i \neq j$ dort liegen. Modulo I_j ist f also $f_j e_j$, und da e_j modulo I_j das Einselement ist, folgt, daß f und f_j die gleiche Restklasse in R/I_j haben. Dies zeigt die Surjektivität von Φ, und da wir den Kern bereits als Durchschnitt der I_j identifiziert haben, folgt die Behauptung aus dem Homomorphiesatz. ∎

Speziell für $R = \mathbb{Z}$ erhalten wir die traditionelle Version des chinesischen Restesatzes:

Satz: Sind $m_1, \ldots, m_r$ paarweise teilerfremde natürliche Zahlen und ist m das Produkt der m_i, so ist

$$\mathbb{Z}/m \cong \bigoplus_{i=1}^{r} \mathbb{Z}/m_i \,.$$

Für beliebig vorgegebene ganze Zahlen x_i gibt es stets ein $x \in \mathbb{Z}$, so daß $x \equiv x_i \bmod m_i$ für alle i; diese Lösung x ist eindeutig modulo m. ∎

Die explizite Konstruktion von x verwendet natürlich den erweiterten EUKLIDischen Algorithmus: Im Falle von nur zwei Moduln m_1, m_2 liefert er ganze Zahlen a_1, a_2, für die $a_1 m_1 + a_2 m_2 = 1$ ist. Dann ist

$$e_1 = a_2 m_2 = 1 - a_1 m_1 \equiv \begin{cases} 1 \bmod m_1 \\ 0 \bmod m_2 \end{cases}$$

und

$$e_2 = a_1 m_1 = 1 - a_2 m_2 \equiv \begin{cases} 0 \bmod m_1 \\ 1 \bmod m_2 \end{cases}$$

und $x = e_1 x_1 + e_2 x_2$ ist eine Lösung.

Bei mehr als zwei Moduln m_i kann man entweder die Konstruktion aus dem Beweis des obigen Satzes nachmachen, oder aber schrittweise vorgehen: Man konstruiert zunächst ein

$$x^{(2)} \equiv \begin{cases} x_1 \bmod m_1 \\ x_2 \bmod m_2 \end{cases},$$

dann ein

$$x^{(3)} \equiv \begin{cases} x^{(2)} \bmod m_1 m_2 \\ x_3 \bmod m_3 \end{cases},$$

und so weiter.

Imitiert man die Konstruktion im obigen Beweis, berechnet man zunächst für jedes j das Produkt

$$\widehat{m}_j = \prod_{i \neq j} m_i$$

und bestimmt dazu Elemente $\alpha_j, \beta_j \in R$, für die gilt $\alpha_j m_j + \beta_j \widehat{m}_j = 1$. Dann ist

$$x = \sum_{i=1}^{r} \beta_i \widehat{m}_i a_i \equiv \beta_j \widehat{m}_j a_j = (1 - \alpha_j m_j) a_j \equiv a_j \bmod m_j .$$

Ein Nachteil dieser Vorgehensweise ist, daß der EUKLIDische Algorithmus hier einmal mehr angewendet werden muß und daß man schon von Anfang an mit größeren Zahlen rechnen muß.

Der chinesische Restesatz hat seinen Namen daher, daß angeblich chinesische Generäle ihre Truppen in Zweier-, Dreier-, Fünfer-, Siebenerreihen *usw.* antreten ließen und jeweils nur die (i.a. unvollständige) letzte Reihe abzählten. Aus den Ergebnissen ließ sich die Gesamtzahl der Soldaten berechnen, wenn das Produkt der verschiedenen Reihenlängen größer war als diese Anzahl.

Es ist zwar fraglich, ob es in China wirklich Generäle gab, die diesen Satz kannten und anwendeten, aber Beispiele dazu finden sich bereits in einem chinesischen Lehrbuch des dreizehnten Jahrhunderts, den 1247 erschienenen *Mathematischen Abhandlungen in neun Bänden* von CH'IN CHIU-SHAO (1202–1261). Dort geht es allerdings nicht um Soldaten, sondern um Reiskörner.

Im Falle eines Polynomrings $R[X]$ sind vor allem Ideale der Form $I_j = (X - x_j)$ interessant; die Restklasse eines Polynoms f in R/I_j ist dann umkehrbar eindeutig bestimmt durch $f(x_j)$. Gesucht ist daher ein $f \in R[X]$, so daß $f(x_j)$ für jedes j gleich einem vorgegebene Wert $x_j \in R$ ist: Wir müssen also ein klassisches Interpolationsproblem lösen.

§3: Modulare Berechnung der Resultante

Beginnen wir mit der Resultante zweier Polynome

$$f = a_d X^d + \cdots + a_1 X + a_0 \quad \text{und} \quad g = b_e X^e + \cdots + b_1 X + b_0$$

in einer Veränderlichen mit ganzzahligen Koeffizienten. Ihre Resultante

$$\mathrm{Res}_Y(f,g) = \begin{vmatrix} a_d & & \cdots & & a_0 & & \\ & \ddots & & & & \ddots & \\ & & a_d & & \cdots & & a_0 \\ b_e & & \cdots & & b_0 & & \\ & \ddots & & & & \ddots & \\ & & & b_e & & \cdots & b_0 \end{vmatrix}$$

ist als Determinante einer ganzzahligen Matrix selbst ganzzahlig, läßt sich aber schon für moderat große Grade d und e nicht mehr mit einem realistischen Aufwand über den LAPLACEschen Entwicklungssatz berechnen. Die Berechnung nach Art des EUKLIDischen Algorithmus in $\mathbb{Q}[X]$ aus Kapitel I, §6, erfordert deutlich weniger Rechenoperationen, führt allerdings meist relativ schnell zu rationalen Zahlen mit riesigen Nennern. Wenn wir modulo einer Primzahl p rechnen, wenden wir diesen Algorithmus in $\mathbb{F}_p[X]$ an, und dort haben natürlich auch alle Zwischenergebnisse Koeffizienten aus $\mathbb{F}_p$.

Sei also p prim; wir betrachten

$$f^{(p)} = (a_d \bmod p)X^d + \cdots + (a_1 \bmod p)X + (a_0 \bmod p) \in \mathbb{F}_p[X]$$

und

$$g^{(p)} = (b_e \bmod p)X^e + \cdots + (b_1 \bmod p)X + (b_0 \bmod p) \in \mathbb{F}_p[X]\,.$$

Wenn a_d durch p teilbar ist, hat $f^{(p)}$ einen kleineren Grad als f, und wenn b_e durch p teilbar ist, hat $g^{(p)}$ einen kleineren Grad als g. In beiden Fällen hat die SYLVESTER-Matrix von $f^{(p)}$ und $g^{(p)}$ eine andere Gestalt als die von f und g; wir können daher nicht erwarten, daß $\mathrm{Res}_X(f,g)$ und $\mathrm{Res}_X(f^{(p)},g^{(p)})$ viel miteinander zu tun haben. In diesen Fällen sagen wir, das Problem habe schlechte Reduktion bei p.

Wenn p keinen der beiden führenden Koeffizienten teilt, ist auch $\deg f^{(p)} = d$ und $\deg g^{(p)} = e$; die Resultante der beiden Polynome sieht also genauso aus wie die obige Determinante, nur daß wir alle Einträge modulo p betrachten. Da die Determinante ein Polynom in ihren Einträgen ist, erhalten wir genau das gleiche Ergebnis, wenn wir sie zunächst in $\mathbb{Z}$ berechnen und dann zur Restklasse modulo p übergehen. Somit ist

$$\mathrm{Res}_X(f^{(p)},g^{(p)}) = \mathrm{Res}_X(f,g) \bmod p$$
$$\text{falls } p \text{ kein Teiler von } a_d \text{ oder } b_e \text{ ist.}$$

In diesen Fällen sagen wir, das Problem habe gute Reduktion modulo p.

Um die Resultante modular berechnen zu können, brauchen wir noch eine obere Schranke für ihren Betrag.

Betrachten wir zunächst die Determinante einer beliebigen $r \times r$-Matrix $A = (a_{ij})$. Für jeden Index i sei eine Schranke b_i gegeben derart, daß $\left|a_{ij}\right| \leq b_i$ für alle j. Dann ist

$$\begin{aligned} |\det A| &= \left| \sum_{\pi \in S_r} \operatorname{sgn} \pi \cdot a_{1\pi(1)} \cdots a_{r\pi(r)} \right| \leq \sum_{\pi \in S_r} \left|a_{1\pi(1)}\right| \cdots \left|a_{r\pi(r)}\right| \\ &\leq \sum_{\pi \in S_r} b_1 \cdots b_r = r! \cdot b_1 \cdots b_r \end{aligned}$$

Um dies auf den Fall einer Resultanten anzuwenden, brauchen wir Schranken für die Koeffizienten eines Polynoms.

Definition: Die *Höhe* $H(P)$ eines Polynoms $P = c_m X^m + \cdots c_1 X + c_0$ aus $\mathbb{C}[X]$ ist das Maximum der Beträge der Koeffizienten $c_0, \ldots, c_m$.

Die ersten e Spalten der Resultante von f und g haben Koeffizienten von f als Einträge; ihre Beträge sind kleiner oder gleich der Höhe $H(f)$ von f. Die restlichen d Zeilen enthalten Koeffizienten von g, deren Beträge durch $H(g)$ beschränkt sind. Somit ist

$$|\operatorname{Res}_X(f, g)| \leq (d + e)! \cdot H(f)^e \cdot H(g)^d .$$

Damit ist klar, wie wir die Resultante modular berechnen können:

1. Ansatz: Wir wählen eine Primzahl $p > 2(d + e)! \cdot H(f)^e \cdot H(g)^d$. Da $H(f) \geq |a_d|$ und $H(g) \geq |b_e|$, kann p für positive d und e kein Teiler von a_d oder b_e sein, es gibt also keine schlechte Reduktion. Wir berechnen daher $\operatorname{Res}_X(f^{(p)}, g^{(p)})$, und $\operatorname{Res}_X(f, g)$ ist die einzige ganze Zahl mit Betrag höchstens $(d + e)! \cdot H(f)^e \cdot H(g)^d$, die modulo p diese Restklasse hat.

2. Ansatz: Wir wählen verschiedene Primzahlen $p_1, \ldots, p_r$, modulo derer das Problem gute Reduktion hat und deren Produkt N größer ist als $2(d + e)! \cdot H(f)^e \cdot H(g)^d$. Für jede der Primzahlen p_i berechnen wir $\operatorname{Res}_X(f^{(p_i)}, g^{(p_i)})$ und setzen die Ergebnisse nach dem chinesischen Restesatz zusammen zu einer Restklasse modulo N. Wieder ist die Resultante die einzige Zahl mit Betrag höchstens $(d + e)! \cdot H(f)^e \cdot H(g)^d$, die modulo N diese Restklasse hat.

Auch Resultanten von Polynomen in mehreren Veränderlichen lassen sich modular berechnen: Seien etwa $f, g \in \mathbb{Z}[X, Y]$ zwei Polynome zweier Veränderlichen, deren Resultante bezüglich Y wir berechnen wollen. Dazu fassen wir bekanntlich f und g auf als Polynome in Y mit Koeffizienten aus $\mathbb{Z}[X]$, also

$$f = f(X, Y) = a_d(X)Y^d + \cdots + a_1(X)Y + a_0(X)$$

und

$$g = g(X, Y) = b_e(X)Y^e + \cdots + b_1(X)Y + b_0(X)\,;$$

die Resultante ist die Determinante der SYLVESTER-Matrix mit diesen Koeffizienten als Einträgen.

Setzen wir für X eine ganze Zahl c ein, werden

$$f(c, Y) = a_d(c)Y^d + \cdots + a_1(c)Y + a_0(c) \in \mathbb{Z}[Y]$$

und

$$g(c, Y) = b_e(c)Y^e + \cdots + b_1(c)Y + b_0(c) \in \mathbb{Z}[Y]$$

zu Polynomen in einer Veränderlichen, deren Resultante

$$\begin{vmatrix}
a_d(c) & & \cdots & & a_0(c) & & \\
& \ddots & & & & \ddots & \\
& & a_d(c) & \cdots & & & a_0(c) \\
b_e(c) & & \cdots & b_0(c) & & & \\
& \ddots & & & \ddots & & \\
& & & b_e(c) & \cdots & & b_0(c)
\end{vmatrix}$$

wir nach obigem Algorithmus modular berechnen können.

Auch hier müssen wir darauf achten, daß wir keine schlechte Reduktion haben, daß der Grad von $f(c, Y)$ also nicht kleiner wird als der Y-Grad von f und entsprechend für g. Der eingesetzte Wert c darf also weder eine Nullstelle von a_d noch eine von b_e sein.

Alsdann hat die SYLVESTER-Matrix von $f(c, Y)$ und $g(c, Y)$ bezüglich Y dieselbe Gestalt wie die von f und g, und wieder gilt: Zumindest vom Ergebnis her ist es gleichgültig, ob wir zunächst die Resultante von f und g als Polynom aus $\mathbb{Z}[X]$ bestimmen und dann den Wert c einsetzen,

oder ob wir c gleich in alle Einträge einsetzen und dann die Resultante als ganze Zahl berechnen:

$$\text{Res}_Y(f,g)(c) = \text{Res}_Y\big(f(c,Y), g(c,Y)\big)$$
$$\text{falls } a_d(c) \neq 0 \quad \text{und} \quad b_e(c) \neq 0\,.$$

Falls $\text{Res}_Y(f,g) \in \mathbb{Z}[X]$ den Grad n hat, benötigen wir $n+1$ solche Werte c, um das Polynom durch Interpolation zu bestimmen. Für einen Algorithmus zur Berechnung von $\text{Res}_Y(f,g)$ fehlt also noch eine obere Schranke für den Grad der Resultante.

Beginnen wir wieder mit der Determinante einer beliebigen $r \times r$-Matrix mit Polynomen in Y als Einträgen. Falls alle Einträge der i-ten Zeile höchstens den Grad n_i haben, hat jedes der Produkte aus dem LAPLACEschen Entwicklungssatz höchstens die Summe der n_i als Grad, und da sich der Grad durch Addition nicht erhöhen kann, ist diese Summe auch eine obere Schranke für den Grad der Determinante.

Hat also jeder der Koeffizienten $a_i = a_i(Y) \in \mathbb{Z}[Y]$ höchstens den Grad n und jeder der Koeffizienten b_j höchstens den Grad m, so hat die Resultante höchstens den Grad $ne + md$. Wir können die Resultante daher als Interpolationspolynom vom Grad höchstens $ne + md$ bestimmen, wenn wir die Resultante von $f(c,Y)$ und $g(c,Y)$ für $ne + md + 1$ verschiedene Werte c berechnen, wobei diese allesamt weder Nullstellen von a_d noch von b_e sein dürfen.

Resultanten von Polynomen in drei Veränderlichen kann man mit der gleichen Strategie zurückführen auf solche in zwei Veränderlichen, solche in vier auf solche in drei, und so weiter. Wenn man sich überlegt, wie viele Berechnungen von Resultanten ganzzahliger Polynome in einer Veränderlichen hinter dieser Vorgehensweise stehen, mag dies als eine sehr ineffiziente Methode erscheinen, aber GEORGE E. COLLINS hat 1971 die verschiedenen bekannten Methoden verglichen und kam zum Schluß, daß dies die effizienteste Vorgehensweise ist; sie

> GEORGE E. COLLINS: The Calculation of Multivariate Polynomial Resultants, *J. ACM.* **18** (1971), S. 515–532

(Das *Journal of the ACM* (Association for Computing Machinery) ist im Netz der Universität Mannheim online verfügbar und steht auch als Papierausgabe in der Bibliothek.)

Seit 1971 gab es natürlich viele Fortschritte in der Computeralgebra und Verbesserungen an allen bekannten Verfahren, aber soweit ich weiß, gab es nichts, was eine andere Vorgehensweise besser als die modulare Berechnung werden ließ.

§4: Die Landau-Mignotte-Schranke

Als nächstes Beispiel für die Anwendung modularer Methoden wollen wir die Berechnung des größten gemeinsamen Teilers betrachten. Hier wird sich herausstellen, daß die Identifikation der Stellen schlechter Reduktion sehr viel schwieriger ist als im Falle der Resultantenberechnung; daher soll die modulare Berechnung des ggT auf mehrere Abschnitte verteilt werden. Hier im ersten geht es um eine Schranke für die Koeffizienten des ggT zweier ganzzahliger Polynome in einer Veränderlichen. Da wir später auch Schranken für die Koeffizienten der irreduziblen Faktoren eines Polynoms benötigen werden, beginnen wir mit der allgemeineren Frage nach Schranken für beliebige Teiler.

$f \in \mathbb{Z}[X]$ sei also ein bekanntes Polynom mit ganzzahligen Koeffizienten, und $g \in \mathbb{Z}[X]$ sei ein (im allgemeinen noch unbekannter) Teiler von f. Wir wollen eine obere Schranke für die Koeffizienten von g finden.

Dazu ordnen wir jedem Polynom

$$f = \sum_{k=0}^{d} a_k X^k \in \mathbb{C}[X]$$

mit komplexen Koeffizienten a_k eine Reihe von Maßzahlen für die Größe der Koeffizienten zu: Wir kennen bereits die Höhe

$$H(f) = \max_{k=0}^{d} |a_k| \ ,$$

und unser Ziel ist es, für ein gegebenes Polynom $f \in \mathbb{Z}[X]$ die Höhe seiner Teiler abzuschätzen. Auf dem Weg zu dieser Abschätzung werden

uns noch eine Reihe anderer Größen nützlich sein, darunter die L^1- und die L^2-Norm

$$\|f\|_1 = \sum_{k=0}^{d} |a_k| \quad \text{und} \quad \|f\|_2 = \sqrt{\sum_{k=0}^{d} a_k \overline{a_k}} = \sqrt{\sum_{k=0}^{d} |a_k|^2}\,.$$

Für die drei bislang definierten Größen gilt

Lemma 1: $H(f) \le \|f\|_2 \le \|f\|_1 \le \sqrt{d+1}\ \|f\|_2 \le (d+1)H(f)$

Beweis: Ist a_ν der betragsgrößte Koeffizient von f, so ist

$$H(f) = |a_\nu| = \sqrt{|a_\nu|^2}$$

offensichtlich kleiner oder gleich $\|f\|_2$. Dies wiederum ist nach der Dreiecksungleichung kleiner oder gleich $\|f\|_1$, denn schreiben wir in $\mathbb{C}^{d+1}$ den Koeffizientenvektor von f als Summe von Vielfachen der Basisvektoren, d.h.

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} a_0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ a_d \end{pmatrix},$$

so steht links ein Vektor der Länge $\|f\|_2$, und rechts stehen Vektoren, deren Längen sich zu $\|f\|_1$ summieren.

Das nächste Ungleichheitszeichen ist die CAUCHY-SCHWARZsche Ungleichung, angewandt auf die Vektoren

$$\begin{pmatrix} |a_0| \\ |a_1| \\ \vdots \\ |a_d| \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Das Skalarprodukt dieser beiden Vektoren ist die Summe der $|a_i|$, also die L^1-Norm $\|f\|_1$; die Länge des ersten Vektors ist gleich $\|f\|_2$, und die des zweiten ist $\sqrt{d+1}$.

Schließlich ist noch

$$\|f\|_2 = \sqrt{\sum_{j=0}^{d} |a_j|^2} \leq \sqrt{\sum_{j=0}^{d} |a_\nu|^2} = \sqrt{d+1}\,|a_\nu| = \sqrt{d+1}\,H(f)\,;$$

■

multipliziert man diese Ungleichung mit $\sqrt{d+1}$ folgt die letzte Ungleichung aus der Behauptung.

■

Es ist alles andere als offensichtlich, wie sich die drei bislang definierten Maßzahlen für einen Teiler eines Polynoms durch die entsprechende Größen für das Polynom selbst abschätzen lassen, denn über die Koeffizienten eines Teilers können wir leider nur sehr wenig sagen. Über seine Nullstellen allerdings schon: Die Nullstellen eines Teilers bilden natürlich eine Teilmenge der Nullstellen des Polynoms. Also sollten wir versuchen, auch die Nullstellen ins Spiel zu bringen.

Den Zusammenhang zwischen Nullstellen und Koeffizienten liefert uns der Wurzelsatz von VIÈTE.

FRANÇOIS VIÈTE (1540–1603) studierte Jura an der Universität Poitiers, danach arbeitete er als Hauslehrer. 1573, ein Jahr nach dem Massaker an den Hugenotten, berief ihn CHARLES IX (obwohl VIÈTE Hugenotte war) in die bretonische Regierung; unter HENRI III wurde er geheimer Staatsrat. 1584 wurde er auf Druck der katholischen Liga vom Hofe verbannt und betrieb fünf Jahre lang nur Mathematik. Unter HENRI IV arbeitete er wieder am Hof und knackte u.a. verschlüsselte Botschaften an den spanischen König PHILIP II. In seinem Buch *In artem analyticam isagoge* rechnete er als erster systematisch mit symbolischen Größen.

Angenommen, wir haben ein Polynom

$$f = X^d + a_{d-1}d^{n-1} + a_{d-2}X^{d-2} + \ldots + a_2X^2 + a_1X + a_0\,,$$

mit höchstem Koeffizienten eins und mit (nicht notwendigerweise verschiedenen) Nullstellen $z_1, \ldots, z_d$. Dann ist auch

$$f = (X - z_1)(X - z_2)\cdots(X - z_d)\,.$$

Ausmultiplizieren und Koeffizientenvergleich liefert

$$\begin{aligned} a_{d-1} &= -(z_1 + \cdots + z_d) \\ a_{d-2} &= \sum_{i<j} z_i z_j \\ a_{d-3} &= -\sum_{i<j<k} z_i z_j z_k \\ &\vdots \qquad\qquad \vdots \\ a_0 &= (-1)^d z_1 \cdots z_d \,. \end{aligned}$$

Allgemein ist a_{d-k} bis aufs Vorzeichen gleich der Summe alle Produkte aus k Werten z_i mit verschiedenem Index, a_k also eine aus $d-k$ Werten z_i. Diese Summen bezeichnet man als die *elementarsymmetrischen Funktionen* in $z_1, \ldots, z_n$ und die obigen Gleichungen als den Wurzelsatz von VIÈTE.

Um die Koeffizienten eines Polynoms durch die Nullstellen abschätzen zu können, brauchen wir also obere Schranken für die Beträge der Produkte aus k Nullstellen. Natürlich ist jedes solche Produkt ein Teilprodukt des Produkts $z_1 \cdots z_d$ aller Nullstellen, aber das führt zu keiner Abschätzung, da unter den fehlenden Nullstellen auch welche sein können, deren Betrag kleiner als eins ist. Um eine obere Schranke für den Betrag zu kommen, müssen wir diese Nullstellen im Produkt $z_1 \cdots z_d$ durch Einsen ersetzen; dann können wir sicher sein, daß kein Produkt von k Nullstellen einen größeren Betrag hat als das so modifizierte Produkt. Diese Überlegungen führen auf die

Definition: Das *Maß* $\mu(f)$ eines nichtkonstanten Polynoms

$$f = a_d \prod_{j=1}^{d} (X - z_j)$$

ist das Produkt der Beträge aller Nullstellen von Betrag größer eins mal dem Betrag des führenden Koeffizienten a_d von f:

$$\mu(f) = |a_d| \prod_{j=1}^{d} \max\bigl(1, |z_j|\bigr) \,.$$

Dieses Maß ist im allgemeinen nur schwer explizit berechenbar, da man dazu die sämtlichen Nullstellen des Polynoms explizit kennen muß. Es hat aber den großen Vorteil, daß für zwei Polynome f und g trivialerweise gilt

$$\mu(f \cdot g) = \mu(f) \cdot \mu(g) .$$

Auch können wir es nach dem Wurzelsatz von VIÈTE leicht für eine Abschätzung der Koeffizienten verwenden: a_k/a_d ist bis aufs Vorzeichen die Summe aller Produkte von $d-k$ Nullstellen, und jedes einzelne solche Produkt mal $|a_d|$ hat höchstens den Betrag $\mu(f)$. Die Anzahl der Summanden ist die Anzahl von Möglichkeiten, aus d Indizes eine k-elementige Teilmenge auszuwählen, also $\binom{d}{k}$. Damit folgt

Lemma 2: Für ein nichtkonstantes Polynom $f = \sum_{k=0}^{d} a_k X^k \in \mathbb{C}[X]$ ist

$$|a_k| \le \binom{d}{k} \mu(f) .$$

∎

Der größte unter den Binomialkoeffizienten $\binom{d}{k}$ ist bekanntlich der mittlere *bzw.* sind die beiden mittleren, und die Summe aller Binomialkoeffizienten $\binom{d}{k}$ ist, wie die binomische Formel für $(1+1)^d$ zeigt, gleich 2^d. Damit folgt

Korollar: Für ein nichtkonstantes Polynom $f \in \mathbb{C}[X]$ ist

$$H(f) \le \binom{d}{[d/2]} \mu(f) \quad \text{und} \quad H(f) \le \|f\|_1 \le 2^d \mu(f) .$$

∎

Zur Abschätzung des Maßes durch eine Norm zeigen wir zunächst

Lemma 3: Für jedes Polynom $f \in \mathbb{C}[X]$ und jede komplexe Zahl z ist

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

Beweis durch explizite Berechnung der beiden Seiten: Sei $f = \sum_{k=0}^{d} a_k X^d$.

Das Quadrat von $\|(X-z)f\|_2 = \left\| a_d X^{d+1} + \sum_{k=1}^{d} (z a_k - a_{k-1}) X^k - a_0 z \right\|_2$

ist die Summe aller Koeffizientenquadrate, also

$$\begin{aligned} & a_d\,\overline{a_d} + \sum_{k=1}^{d} (z a_k - a_{k-1})\,\overline{(z a_k - a_{k-1})} + a_0 z \overline{a_0 z} \\ = {} & |a_d|^2 + \sum_{k=1}^{d} \left(|a_k|^2 |z|^2 - 2\,\mathfrak{Re}(z a_k \overline{a_{k-1}}) + \left|a_{k-1}\right|^2 \right) + |a_0|^2 |z|^2 \\ = {} & (1 + |z|^2) \sum_{k=0}^{d} |a_k|^2 - 2 \sum_{k=1}^{d} \mathfrak{Re}(z a_k \overline{a}_{k-1})\,. \end{aligned}$$

Entsprechend ist $(\overline{z}X - 1)f = a_d \overline{z} X^{d+1} + \sum_{k=1}^{d} (\overline{z} a_{k-1} - a_k) X^k - a_0$ und auch $\|(\overline{z}X - 1)f\|_2^2$ wird zu

$$\begin{aligned} & a_d \overline{z} \cdot \overline{a_d} z + \sum_{k=1}^{d} (\overline{z} a_{k-1} - a_k)(z \overline{a_{k-1}} - \overline{a_k}) + a_0 \overline{a_0} \\ = {} & |z a_d|^2 + \sum_{k=1}^{d} \left(\left|z a_{k-1}\right|^2 - 2\,\mathfrak{Re}(z a_k \overline{a_{k-1}}) + |a_k|^2 \right) + |a_0|^2 \\ = {} & (1 + |z|^2) \sum_{k=0}^{d} |a_k|^2 - 2 \sum_{k=1}^{d} \mathfrak{Re}(z a_k \overline{a}_{k-1})\,. \end{aligned}$$

■

Für das Polynom $f = a_d \prod_{j=1}^{d} (X - z_j)$ bedeutet dies, daß wir den Faktor $(X - z_j)$ durch $(\overline{z}_j X - 1)$ ersetzen können, ohne daß sich die L^2-Norm ändert. Wenden wir dies an auf alle Faktoren $(X - z_j)$, für die $\left|z_j\right| > 1$ ist, erhalten wir ein Polynom, dessen sämtliche Nullstellen Betrag kleiner oder gleich eins haben, denn $\overline{z}_j X - 1$ verschwindet für $X = 1/\overline{z}_j$, was für $|z|_j > 1$ einen Betrag kleiner Eins hat. Das Maß des modifizierten Polynoms ist also gleich dem Betrag des führenden Koeffizienten, und dieser wiederum ist natürlich kleiner oder gleich der L^2-Norm. Andererseits ist das Maß des modifizierten Polynoms gleich dem des ursprünglichen, denn für jeden Faktor $(X - z_j)$ wird der führende Koeffizient bei der Modifikation mit $\overline{z}_j$ multipliziert, was denselben Betrag hat wie z_j. Damit folgt:

Lemma 4: Für ein nichtkonstantes Polynom $f \in \mathbb{C}[X]$ ist

$$\mu(f) \leq \|f\|_2 \ .$$

■

Nach diesen Vorbereitungen können wir uns an die Abschätzung der Koeffizienten eines Teilers machen. Sei dazu

$$g = \sum_{j=0}^{e} b_j X^j \quad \text{Teiler von} \quad f = \sum_{i=0}^{d} a_i X^i \ .$$

Da jede Nullstelle von g auch Nullstelle von f ist, lassen sich die Maße der beiden Polynome leicht vergleichen:

$$\mu(g) \leq \left|\frac{b_e}{a_d}\right| \cdot \mu(f) \, .$$

Kombinieren wir dies mit dem Korollar zu Lemma 2 und mit Lemma 4, erhalten wir die LANDAU-MIGNOTTE-Schranke:

$$H(g) \leq \binom{e}{[e/2]} \left|\frac{b_e}{a_d}\right| \|f\|_2 \quad \text{und} \quad \|g\|_1 \leq 2^e \left|\frac{b_e}{a_d}\right| \|f\|_2 \ .$$

Der ggT zweier Polynome f und g muß diese Abschätzung für beide Polynome erfüllen, allerdings kennen wir *a priori* weder den Grad noch den führenden Koeffizienten des ggT. Falls wir Polynome mit ganzzahligen Koeffizienten betrachten und einen ggT in $\mathbb{Z}[X]$ suchen, wissen wir nur, daß sein führender Koeffizient die führenden Koeffizienten sowohl von f als auch von g teilen muß, und daß sein Grad natürlich weder den von f noch den von g übersteigen kann. Damit erhalten wir die LANDAU-MIGNOTTE-Schranke für den ggT zweier Polynome: Schreiben wir f und g wie oben, so ist für $f, g \in \mathbb{Z}[X]$

$$H\big(\mathrm{ggT}(f,g)\big) \leq \|\mathrm{ggT}(f,g)\|_1$$
$$\leq \mathrm{LM}(f,g) \underset{\text{def}}{=} 2^{\min(d,e)} \, \mathrm{ggT}(a_d, b_e) \min\left(\frac{\|f\|_2}{|a_d|}, \frac{\|g\|_2}{|b_e|}\right) \ .$$

MAURICE MIGNOTTE arbeitet am Institut de Recherche Mathématique Avancée der Universität Straßburg; sein Hauptforschungsgebiet sind diophantische Gleichungen. Er ist Autor mehrerer Lehrbücher, unter anderem aus dem Gebiet der Computeralgebra.

EDMUND GEORG HERMANN LANDAU (1877–1938) wurde in Berlin geboren und studierte an der dortigen Universität, wo er auch von 1899 bis 1909 lehrte. Dann bekam er einen Ruf an die damals führende deutsche Mathematikfakultät in Göttingen. 1933 verlor er seinen dortigen Lehrstuhl, denn die Studenten boykottierten seine Vorlesungen, da sie meinten, sie könnten Mathematik unmöglich bei einem jüdischen Professor lernen. LANDAUS zahlreiche Publikationen beschäftigen sich vor allem mit der Zahlentheorie, über die er auch ein bedeutendes Lehrbuch schrieb. Sehr bekannt sind insbesondere seine Arbeiten über Primzahlverteilung.

Als Beispiel betrachten wir noch einmal die beiden Polynome aus Kapitel 1, §2.

$$f = X^8 + X^6 - 3X^4 - 3X^3 + 8X^2 + 2X - 5$$

hat die L^2-Norm

$$\|f\|_2 = \sqrt{1^2 + 1^2 + 3^2 + 3^2 + 8^2 + 2^2 + 5^2} = \sqrt{113}$$

und den führenden Koeffizienten eins; für

$$g = 3X^6 + 5X^4 - 4X^2 - 9X + 21$$

haben wir führenden Koeffizienten drei und

$$\|g\|_2 = \sqrt{3^2 + 5^2 + 4^2 + 9^2 + 21^2} = \sqrt{572} = 2\sqrt{143}\,.$$

Da $3^2 \cdot 113 > 900$ größer ist als $2^2 \cdot 143 < 600$, ist die LANDAU-MIGNOTTE-Schranke für diese beiden Polynome

$$\mathrm{LM}(f, g) = 2^6 \cdot \frac{2}{3}\sqrt{143} \approx 510{,}2191249\,.$$

Da die Koeffizienten des ggT ganze Zahlen sind, kann der Betrag eines jeden Koeffizienten also höchstens gleich 510 sein.

§5: Gute und schlechte Reduktion beim ggT

Nachdem wir eine obere Schranke für die Koeffizienten des größten gemeinsamen Teilers zweier Polynome aus $\mathbb{Z}[X]$ gefunden haben, stellt sich als nächstes die Frage, bei welchen Primzahlen wir gute Reduktion haben.

Angenommen, f und g aus $\mathbb{Z}[X]$ sind zwei Polynome mit ganzzahligen Koeffizienten. Ihr ggT $h \in \mathbb{Z}[X]$ ist bis auf eine Einheit eindeutig bestimmt, also bis aufs Vorzeichen. Sein Grad sei d.

Nun sei p eine Primzahl und $f^{(p)}, g^{(p)} \in \mathbb{F}_p[X]$ seien die Polynome, die aus f und g entstehen, wenn wir alle Koeffizienten modulo p reduzieren. Wann wissen wir, daß auch deren ggT in $\mathbb{F}_p[X]$ den Grad d hat?

Ist $f = hf_1$, $g = hg_1$, und sind $h^{(p)}, f_1^{(p)}, g_1^{(p)}$ die Reduktionen von h, f_1 und g_1 modulo p, so ist offensichtlich $f^{(p)} = h^{(p)} f_1^{(p)}$ und $g^{(p)} = h^{(p)} g_1^{(p)}$. Somit ist $h^{(p)}$ auf jeden Fall ein gemeinsamer Teiler von $f^{(p)}$ und $g^{(p)}$, muß also deren größten gemeinsamen Teiler teilen. Daraus folgt nun aber nicht, daß dessen Grad mindestens gleich d sein muß, denn wenn der führende Koeffizient von h durch p teilbar ist, hat $h^{(p)}$ kleineren Grad als h. Ein Beispiel dafür können wir uns leicht mit Maple konstruieren:

```
> h := 3*X+1: f1 := (X^3 - X^2 + 2): g1 := (X^2+X+1):
```

```
> f := expand(h*f1); g := expand(h*g1);
```

$$f := 3X^4 - 2X^3 + 6X - X^2 + 2$$

$$g := 3X^3 + 4X^2 + 4X + 1$$

```
> gcd(f, g);
```

$$3X + 1$$

```
> Gcd(f, g) mod 3;
```

$$1$$

Das Kommando `Gcd` mit großem `G` ist die „träge“ Form des `gcd`-Kommandos, die erst vom `mod`-Operator ausgewertet wird, so daß die ggT-Berechnung über $\mathbb{F}_3$ erfolgt. Im vorliegenden Beispiel freilich hätten wir auch mit `gcd` dasselbe Ergebnis bekommen, denn hier ist h mod p der ggT von $f^{(p)}$ und $g^{(p)}$. Wir werden gleich sehen, daß dies nicht immer so sein muß.

Zunächst aber wollen wir uns überlegen, wann der Grad von h mod p kleiner ist als der von h. Das ist offensichtlich dann und nur dann

der Fall, wenn der führende Koeffizient von h durch p teilbar ist. Da wir h erst ausrechnen wollen, hat dieses Kriterium freilich keinen großen praktischen Nutzen.

Nun ist aber $f = hf_1$ und $g = hg_1$; der führende Koeffizient von f *bzw.* g ist also das Produkt der führenden Koeffizienten von h und von f_1 *bzw.* g_1. Wenn daher der führende Koeffizient von h durch p teilbar ist, so gilt dasselbe auch für die führenden Koeffizienten von f und von g. Die Umkehrung dieser Aussage gilt natürlich nicht, aber da wir eine große Auswahl an Primzahlen haben, stört uns das nicht weiter. Wir können also festhalten:

Lemma: Falls für die beiden Polynome $f, g \in \mathbb{Z}[X]$ die Primzahl p nicht beide führende Koeffizienten teilt, hat der ggT von $f^{(p)}$ und $g^{(p)}$ in $\mathbb{F}_p[X]$ mindestens denselben Grad wie $h = \text{ggT}(f, g) \in \mathbb{Z}[X]$ und ist ein Vielfaches von $h^{(p)}p$.

■

Falls er unter diesen Bedingungen größeren Grad als $h^{(p)}$ hat, müssen $f^{(p)}/h^{(p)} = (f/h)^{(p)}$ und $g^{(p)}/h^{(p)} = (g/h)^{(p)}$ einen gemeinsamen Faktor positiven Grades haben, d.h.

$$\text{Res}_X(f^{(p)}/h^{(p)}, g^{(p)}/h^{(p)}) = \text{Res}_X(f/h, g/h) \bmod p$$

muß verschwinden, Falls p keinen der führenden Koeffizienten von f und g teilt, teilt es auch keinen der führenden Koeffizienten von f/h und g/h, so daß diese Resultante gleich $\text{Res}_X(f/h, g/h) \bmod p$ ist, d.h. p muß Teiler dieser Resultanten sein. Da wir h nicht kennen, können wir sie nicht ausrechnen; aber wir wissen nun, daß höchstens für endlich viele Primzahlen p der ggT von $f^{(p)}$ und $g^{(p)}$ etwas anderes als $\text{ggT}(f, g) \bmod p$ sein kann.

Damit können wir das bisherige Ergebnis dieses Paragraphen für Zwecke der ggT-Berechnung in $\mathbb{Z}[X]$ folgendermaßen zusammenfassen:

Satz: Für zwei Polynome $f, g \in \mathbb{Z}[X]$ mit $\text{ggT}(f, g) = h$ und ihre Reduktionen $f^{(p)}, g^{(p)} \in \mathbb{F}_p[X]$ mit $\text{ggT}(f^{(p)}, g^{(p)}) = h^*$ gilt:
a) Falls p nicht die führenden Koeffizienten von sowohl f als auch g teilt, ist die Reduktion $h^{(p)}$ von h ein Teiler von h^* und $\deg h^* \geq \deg h$.

b) Es gibt höchstens endlich viele Primzahlen p, für die $h^{(p)}$ nicht gleich dem ggT von $f^{(p)}$ und $g^{(p)}$ ist.

■

Nun haben wir nur noch eine Schwierigkeit: Da $\mathbb{F}_p$ ein Körper ist, können wir den modulo p berechneten ggT stets so normieren, daß er führenden Koeffizienten eins hat. Für Polynome mit ganzzahligen Koeffizienten ist das nicht möglich: Der ggT von

$$f = (2X+1)^2 = 4X^2+4X+1 \quad \text{und} \quad g = (2X+1)(2X-1) = 4X^2-1$$

ist $h = 2X+1$, was wir in $\mathbb{Z}[X]$ nicht zu $X+\frac{1}{2}$ kürzen können. Berechnen wir dagegen in $\mathbb{F}_5[X]$ den ggT der beiden Reduktionen modulo fünf, so ist $X+3$ ein genauso akzeptables Ergebnis wie $2(X+3) = 2X+1$ oder $3(X+3) = 3X+4$ oder $4(X+3) = 4X+2$. Welches dieser Polynome sollen wir nach $\mathbb{Z}[X]$ hochheben?

Wir wissen, daß der führende Koeffizient des ggT in $\mathbb{Z}[X]$ den führenden Koeffizienten beider Polynome teilen muß; er muß daher ein Teiler des ggT c dieser beiden führenden Koeffizienten sein. Wie wir am obigen Beispiel sehen, ist er freilich im Allgemeinen nicht gleich diesem ggT. Wenn wir von zwei primitiven Polynomen ausgehen, können wir trotzdem den modulo p berechneten ggT so liften, daß er c als führenden Koeffizienten hat; im obigen Beispiel bekämen wir also das Polynom $4X+2$.

Da wir von zwei primitiven Polynomen f und g ausgehen, muß nach den Ergebnissen aus Kapitel I, §4 auch deren ggT h primitiv sein. Wenn h den echten Teiler c_0 von c als führenden Koeffizienten hat, so ist $\widetilde{h} = \frac{c}{c_0}h$ ein Polynom mit führendem Koeffizienten c, das modulo p ein ggT von f mod p und g mod p ist. Sein primitiver Anteil ist der korrekte ggT h; im obigen Beispiel ist das $2X+1$.

§6: Die modulare Berechnung des ggT

Nach vielen Vorbereitungen sind wir nun endlich in der Lage, einen Algorithmus zur modularen Berechnung des ggT in $\mathbb{Z}[X]$ oder $\mathbb{Q}[X]$ zu formulieren. Wesentlich ist für beide Fälle nur die Berechnung des ggT zweier primitiver Polynome aus $\mathbb{Z}[X]$: Zwei Polynome aus $\mathbb{Q}[X]$

lassen sich stets schreiben als λf und μg mit $\lambda, \mu \in \mathbb{Q}^\times$ und primitiven Polynomen $f, g \in \mathbb{Z}[X]$, und sie haben denselben ggT wie f und g. Für Polynome aus $\mathbb{Z}[X]$ sind $\lambda, \mu \in \mathbb{Z}$ die Inhalte, und der ggT in $\mathbb{Z}[X]$ ist $\mathrm{ggT}(\lambda, \mu) \cdot \mathrm{ggT}(f, g)$; für Polynome aus $\mathbb{Q}[X]$ kommt es auf nicht auf Konstanten an, und wir können $\mathrm{ggT}(f, g)$ als ggT nehmen.

Seien nun also $f, g \in \mathbb{Z}[X]$ primitive Polynome.

a) Wir arbeiten nur mit Primzahlen, die nicht die führenden Koeffizienten sowohl von f als auch von g teilen. Wie wir in §5 gesehen haben, hat dann der ggT h_p von $f^{(p)}$ und $g^{(p)}$ mindestens denselben Grad hat wie $\mathrm{ggT}(f, g)$ und es gibt nur endlich viele Primzahlen, für die sich die beiden Grade unterscheiden. Für alle anderen p ist $h_p = \mathrm{ggT}(f, g)^{(p)}$.

b) Diese endlich vielen Primzahlen, für die das Problem h_p größeren Grad hat, lassen sich nicht schon *a priori* ausschließen. Wir können sie aber anhand zweier Kriterien nachträglich erkennen: Falls wir eine Primzahl q (die nicht beide führende Koeffizienten teilt) finden, für die $\deg h_q < \deg h_p$ ist, muß das Problem bei p schlechte Reduktion haben. Wenn wir mehrere Primzahlen haben, die uns modulare ggTs desselben Grads liefern, so können wir diese nach dem chinesischen Restesatz zusammensetzen. Falls wir hier keine Lösung finden, bei der sämtliche Koeffizienten einen Betrag unterhalb der LANDAU-MIGNOTTE-Schranke liegen, oder wenn wir eine solche Lösung finden, diese aber kein gemeinsamer Teiler von f und g ist, dann waren alle betrachteten Primzahlen schlecht.

Um die Übersicht zu behalten fassen wir bei der Rechnung alle bereits betrachteten Primzahlen zusammen zu einer Menge $\mathcal{P}$ und wir berechnen auch in jedem Schritt das Produkt N aller Elemente von $\mathcal{P}$, die wir noch nicht als schlecht erkannt haben. Falls sie wirklich nicht schlecht sind, kennen wir den ggT modulo N.

Diese Ideen führen zu folgendem Rechengang zur modularen Berechnung des ggT zweier primitiver Polynome aus $\mathbb{Z}[X]$:

1. Schritt (Initialisierung): Berechne den ggT c der führenden Koeffizienten von f und g sowie die LANDAU-MIGNOTTE-Schranke $\mathrm{LM}(f, g)$ und setze $M = 2c\big\lceil \mathrm{LM}(f, g) \big\rceil + 1$. Setze außerdem $\mathcal{P} = \emptyset$ und $N = 1$.

Da der Betrag eines jeden Koeffizienten des ggT höchstens gleich $\big[\mathrm{LM}(f,g)\big]$ ist und wir höchstens das c-fache dieses ggT berechnen, kennen wie die Koeffizienten in $\mathbb{Z}$, sobald wir sie modulo M kennen.

2. Schritt: Wähle eine zufällige Primzahl $p \notin \mathcal{P}$, die nicht die führenden Koeffizienten von sowohl f als auch g teilt, ersetze $\mathcal{P}$ durch $\mathcal{P} \cup \{p\}$ und berechne in $\mathbb{F}_p[X]$ den ggT h_p von $f^{(p)}$ und $g^{(p)}$; dieser sei so normiert, daß sein höchster Koeffizient gleich eins ist. Falls $h_p = 1$ ist, endet der Algorithmus und $\mathrm{ggT}(f,g) = 1$. Andernfalls wird $N = p$ gesetzt und ein Polynom $h \in \mathbb{Z}[X]$ berechnet, dessen Reduktion modulo p gleich ch_p ist.

3. Schritt: Falls $N \geq M$ ist, ändere man die Koeffizienten von h modulo N nötigenfalls so ab, daß ihre Beträge höchstens gleich $c\,\mathrm{LM}(f,g)$ sind. Falls das nicht möglich ist, haben wir bislang modulo lauter schlechter Primzahlen gerechnet, können also alle bisherigen Ergebnisse vergessen und gehen zurück zum zweiten Schritt.

Andernfalls wird h durch seinen primitiven Anteil ersetzt und wir überprüfen, ob h sowohl f als auch g teilt. Falls ja, ist h der gesuchte ggT, und der Algorithmus endet; andernfalls müssen wir ebenfalls zurück zum zweiten Schritt und dort von Neuem anfangen.

4. Schritt: Im Fall $N < M$ wählen wir eine zufällige Primzahl $p \notin \mathcal{P}$, die nicht die führenden Koeffizienten von sowohl f als auch g teilt, ersetzen $\mathcal{P}$ durch $\mathcal{P} \cup \{p\}$ und berechnen in $\mathbb{F}_p[X]$ den ggT h_p von $f^{(p)}$ und $g^{(p)}$. Falls dieser gleich eins ist, endet der Algorithmus und $\mathrm{ggT}(f,g) = 1$. Falls sein Grad größer als der von h ist, war p eine schlechte Primzahl; wir vergessen h_p und gehen zurück an den Anfang des vierten Schritts, d.h. wir wiederholen die Rechnung mit einer neuen Primzahl,

Falls der Grad von h_p kleiner ist als der von h, waren alle bisher betrachteten Primzahlen mit der eventuellen Ausnahme von p schlecht; wir setzen N deshalb zurück auf p und konstruieren ein Polynom $h \in \mathbb{Z}[X]$, dessen Reduktion modulo p gleich ch_p ist.

Ist schließlich $\deg h = \deg h_p$, so konstruieren wir nach dem chinesischen Restesatz ein neues Polynom h, das modulo N gleich dem alten h

und modulo p gleich ch_p ist. Danach geht es weiter mit dem dritten Schritt.

Der Algorithmus muß enden, da es nur endlich viele Primzahlen p gibt, für die der in $\mathbb{F}_p[X]$ berechnete ggT nicht einfach die Reduktion von ggT(f, g) modulo p ist, und nach endlich vielen Durchläufen sind genügend viele gute Primzahlen zusammengekommen, daß ihr Produkt die Zahl M übersteigt. Da der ggT in $\mathbb{F}_p[X]$ für Primzahlen, die nicht beide führende Koeffizienten teilen, höchstens höheren Grad als ggT(f, g) haben kann, ist auch klar, daß der Algorithmus mit einem korrekten Ergebnis abbricht.

Betrachten wir dazu ein Beispiel:

```
> f := X^6-124*X^5-125*X^4-2*X^3+248*X^2+249*X+125:
```

```
> g := X^5+127*X^4+124*X^3-255*X^2-381*X-378:
```

Eine einfache, aber langweilige Rechnung zeigt, daß die LANDAU-MIGNOTTE-Schranke von f und g ungefähr den Wert 13199,21452 hat; wegen möglicher Rundungsfehler sollten wir zur Sicherheit vielleicht besser von 13200 ausgehen. Die Zahl, modulo derer wir die Koeffizienten mindestens kennen müssen, ist somit $M = 26401$.

Als erste Primzahl wählen wir zum Beispiel $p = 107$ und berechnen

```
> Gcd(f, g) mod 107;
```

$$X^3 + 90X^2 + 90X + 89$$

Damit ist $\mathcal{P} = \{107\}$ und $N = 107 < M$. Also wählen wir eine weitere Primzahl, etwa $p = 271$:

```
> Gcd(f, g) mod 271;
```

$$X^3 + 127X^2 + 127X + 126$$

Auch dieser modulare ggT hat Grad drei, wir können die beiden also zusammensetzen, indem wir den chinesischen Restesatz auf die Koeffizienten anwenden:

```
> chrem([90, 127], [107, 271]);
```

$$5547$$

```
> chrem([89, 126], [107, 271]);
```

$$5546$$

Damit ist also $h = X^3 + 5547X^2 + 5547X + 5546$, $\mathcal{P} = \{107, 271\}$ und $N = 107 \times 271 = 28997$.

Dies ist größer als M, und alle Koeffizienten von h liegen unterhalb der LANDAU-MIGNOTTE-Schranke, also müssen wir untersuchen, ob h Teiler von f und von g ist:

```
> rem(f, X^3 + 5547*X^2 + 5547*X + 5546, X);
```

$$967384732340761X^2 + 967384732340761X + 967384732340761$$

Offensichtlich nicht; somit sind 107 und 271 für dieses Problem schlechte Primzahlen. Versuchen wir unser Glück als nächstes mit $p = 367$:

```
> Gcd(f, g) mod 367;
```

$$X^2 + X + 1$$

Also wird $\mathcal{P} = \{107, 271, 367\}$ und $N = 367$; wir erwarten, daß der gesuchte ggT modulo 367 gleich $X^2 + X + 1$ ist. Um von 367 aus über die Schranke M zu kommen reicht eine relativ kleine Primzahl, z.B. $p = 73$.

```
> Gcd(f, g) mod 73;
```

$$X^3 + 22X^2 + 22X + 21$$

Dieser ggT hat zu großen Grad, also ist auch 73 schlecht für uns. Wir lassen daher $N = 367$ und haben nun $\mathcal{P} = \{73, 107, 271, 367\}$.

Die nächste Primzahl nach 73 ist 79.

```
> Gcd(f, g) mod 79;
```

$$X^2 + X + 1$$

Wieder erhalten wir ein quadratisches Polynom, also setzen wir

$$N = 367 \times 79 = 44503, \qquad \mathcal{P} = \{73, 79, 107, 271, 367\}$$

und natürlich $h = X^2 + X + 1$. Da $N > M$ ist und alle Koeffizienten von h unter der LANDAU-MIGNOTTE-Schranke liegen, müssen wir nun testen, ob h Teiler von f und von g ist:

```
> rem(f, X^2+X+1, X);
```

0

```
> rem(g, X^2+X+1, X);
```

0

Damit ist ggT$(f, g) = X^2 + X + 1$.

Bei diesem Beispiel habe ich natürlich absichtlich möglichst viele schlechte Primzahlen verwendet; wählt man seine Primzahlen wirklich zufällig, wird man nur selten eine erwischen.

Auch für das Beispiel aus Kapitel I, §2 mit

$$f = X^8 + X^6 - 3X^4 - 3X^3 + 8X^2 + 2X - 5$$

und

$$g = 3X^6 + 5X^4 - 4X^2 - 9X + 21$$

können wir den ggT nach der modularen Methode ausrechnen: In §4 hatten wir bereits die LANDAU-MIGNOTTE-Schranke

$$\mathrm{LM}(f, g) = 2^6 \cdot \frac{2}{3}\sqrt{143} \approx 510{,}2191249$$

berechnet; da der ggT der führenden Koeffizienten gleich eins ist, reicht es also, den ggT modulo 1021 zu kennen. Da dies eine Primzahl ist, die gut in ein Maschinenwort paßt, können wir als erstes die modulare Berechnung nur mit $p = 1021$ durchführen:

```
> f := X^8+X^6-3*X^4-3*X^3+8*X^2+2*X-5 mod p;
```

$$f := X^8 + X^6 + 1018 * X^4 + 1018 * X^3 + 8 * X^2 + 2 * X + 1016$$

```
> g := 3*X^6 + 5*X^4 - 4*X^2 - 9*X + 21 mod p;
```

$$g := 3X^6 + 5X^4 + 1017X^2 + 1012X + 21$$

```
> r2 := Rem(f, g, X) mod p;
```

$$r2 := 907X^4 + 227X^2 + 340$$

```
> r3 := Rem(g, r2, X) mod p;
```

$$r3 := 77X^2 + 1012X + 181$$

```
> r4 := Rem(r2, r3, X) mod p;
```

$$r4 := 405X + 581$$

```
> r5 := Rem(r3, r4, X) mod p;
```

$$r5 := 956$$

```
> r6 := Rem(r4, r5, X) mod p;
```

$$r6 := 0$$

Somit ist 956 ein ggT in $\mathbb{F}_{1021}[X]$, und damit natürlich auch die Eins. Nach dem, was wir in diesem Paragraphen gesehen haben, folgt daraus, daß auch der ggT von f und g in $\mathbb{Z}[X]$ gleich eins ist.

Vergleicht man mit dem Rechengang in Kapitel I §2, hat sich abgesehen von den modularen Polynomdivisionen nichts wesentliches geändert, jedoch sind die Zwischenergebnisse erheblich angenehmer geworden.

Die Resultante von f und g ist in diesem Fall $260708 = 2^2 \cdot 7 \cdot 9311$; für diese Primzahlen gibt uns Maple

$$\text{ggT}(f^{(2)}, g^{(2)}) = X^2 + X + 1, \quad \text{ggT}(f^{(7)}, g^{(7)}) = X + 3$$
$$\text{und} \quad \text{ggT}(f^{(9311)}, g^{(9311)}) = X - 820\,;$$

für alle anderen Primzahlen p ist $\text{ggT}(f^{(p)}, g^{(p)}) = 1$.

§7: Polynome in mehreren Veränderlichen

Wie wir aus Kapitel II wissen, ist auch der Polynomring in mehreren Veränderlichen über den ganzen Zahlen oder über einem Körper faktoriell; somit existieren auch dort größte gemeinsame Teiler. Im vorigen Paragraphen haben wir gesehen, wie sich diese im Falle einer Veränderlichen berechnen lassen; hier soll nun im wesentlichen die gleiche Technik angewendet werden, um die ggT-Bestimmung für Polynome in n Veränderlichen zurückzuführen auf die in $n-1$ Veränderlichen.

Wir betrachten also zwei Polynome f, g in $n \geq 2$ Veränderlichen $X_1, \ldots, X_n$ über einem Körper oder über faktoriellen Ring k; wichtig sind vor allem die Fälle $k = \mathbb{Z}$, $k = \mathbb{Q}$ und $k = \mathbb{F}_p$. Wie beim GAUSSschen

Lemma betrachten wir die Polynome aus $R_n = k[X_1, \ldots, X_n]$ als Polynome in der einer Veränderlichen X_n über dem Polynomring $R_{n-1} = k[X_1, \ldots, X_{n-1}]$, schreiben also $R_n = R_{n-1}[X_n]$. Durch ggT-Berechnungen in R_{n-1} können wir diese Polynome zerlegen in ihre Inhalte und primitiven Anteile; der ggT der Inhalte läßt sich wieder in R_{n-1} berechnen.

Bleibt noch der ggT der primitiven Anteile; diese seien f und g, jeweils aufgefaßt als Polynome in X_n mit Koeffizienten aus R_{n-1}. Um deren ggT zu berechnen, könnten wir den EUKLIDischen Algorithmus über dem Quotientenkörper von R_{n-1} anwenden, allerdings steigen hier die Grade von Zähler und Nenner der Koeffizienten sowie *deren* Koeffizienten im allgemeinen so stark an, daß dies nur bei wenigen Variablen und sehr kleinen Graden praktisch durchführbar ist. Daher müssen wir auch hier wieder nach Alternativen suchen.

Im vorigen Paragraphen hatten wir, um die Explosion der Koeffizienten beim EUKLIDischen Algorithmus in $\mathbb{Q}[X]$ zu vermeiden, den Umweg über die ganzen Zahlen modulo einer Primzahl p genommen, also zunächst einen ggT (oder mehrere) in Körpern $\mathbb{F}_p[X]$ berechnet. Wie wir uns schon in den ersten beiden Paragraphen überlegt haben, können wir genauso auch die Variablenanzahl reduzieren, indem wir für eine der Variablen Werte einsetzen, z.B. für X_{n-1}. Wir betrachten also anstelle eines Polynoms $f \in R_n = R_{n-1}[X_n]$ das Polynom

$$f^{(c)} = f(X_1, \ldots, X_{n-2}, c, X_n) \in k[X_1, \ldots, X_{n-2}, X_n] = R_{n-2}[X_n]\,,$$

in dem für X_{n-1} der Wert c eingesetzt wird; jeder Koeffizient $a_j \in R_{n-1}$ wird also ersetzt durch $a_j(X_1, \ldots, X_{n-2}, c) \in R_{n-2}$. Auch hier stellt sich die Frage, was der ggT von $f^{(c)}$ und $g^{(c)}$ mit dem von f und g zu tun hat.

Ist $h \in R_{n-1}[X]$ ein Teiler von f, etwa $f = qh$, so ist $f^{(c)} = q^{(c)}h^{(c)}$, d.h. auch $h^{(c)}$ ist ein Teiler von $f^{(c)}$. Dieser Teiler könnte aber einen kleineren Grad haben als h; dies passiert offensichtlich genau dann, wenn der führende Koeffizient von h durch Einsetzen von $X_{n-1} = c$ zum Nullpolynom aus R_{n-2} wird. Da der führende Koeffizient von f das Produkt der führenden Koeffizienten von h und q ist, gilt dann dasselbe auch für den führenden Koeffizienten von f; wir können dieses

Problem also vermeiden, indem wir c so wählen, daß der führende Koeffizient von f durch Einsetzen von $X_{n-1} = c$ nicht zum Nullpolynom wird. Wenn wir das für f *oder* g sicherstellen, wissen wir daher, daß $\mathrm{ggT}(f,g)^{(c)}$ ein Teiler von $f^{(c)}$ und $g^{(c)}$, also auch von $\mathrm{ggT}(f^{(c)}, g^{(c)})$ ist, und daß beide größte gemeinsame Teiler denselben Grad in X_n haben. Da die führenden Koeffizienten von f und g als Polynome in X_{n-1} geschrieben werden können, gibt es nur endlich viele Werte von c, die wir vermeiden müssen, und diese lassen sich einfach identifizieren.

Auch dann wissen wir allerdings nur, daß $h^{(c)} = \mathrm{ggT}(f,g)^{(c)}$ ein Teiler von $\mathrm{ggT}(f^{(c)}, g^{(c)})$ ist. $h^{(c)}$ ist genau dann ein echter Teiler, wenn $f^{(c)}/h^{(c)}$ und $g^{(c)}/h^{(c)}$ einen gemeinsamen Faktor haben, der keine Einheit ist, wenn also die Resultante von $f^{(c)}/h^{(c)}$ und $g^{(c)}/h^{(c)}$ bezüglich X_n verschwindet. Bezeichnet h den ggT von f und g, so entsteht diese Resultante im Falle, daß *keiner* der führenden Koeffizienten von f oder g an der Stelle $X_{n-1} = c$ verschwindet, aus $\mathrm{Res}_{X_n}(f/h, g/h) \in R_{n-1}$ durch Einsetzen von $X_{n-1} = c$. Da diese Resultante als Polynom in X_{n-1} geschrieben werden kann, gibt es daher wieder höchstens endlich viele Werte von c, für die dies der Fall ist. Da wir h nicht kennen, können wir diese Werte allerdings nicht im voraus identifizieren – ganz analog zur Situation bei der modularen Berechnung des ggT in $\mathbb{Z}[X]$.

Als nächstes stellt sich das Problem, was wir aus der Kenntnis von $\mathrm{ggT}(f^{(c)}, g^{(c)})$ für $\mathrm{ggT}(f,g)$ folgern können. Offensichtlich nicht sonderlich viel, denn wenn wir ein Polynom nur an einer Stelle $X_{n-1} = c$ kennen, gibt uns das noch kaum Information. Wenn wir allerdings ein Polynom vom Grad d in X_{n-1} an $d+1$ verschiedenen Punkten kennen, dann kennen wir es vollständig.

Die theoretisch einfachste Konstruktion des Polynoms aus seinen Funktionswerten an $d+1$ verschiedenen Stellen geht auf JOSEPH-LOUIS COMTE DE LAGRANGE zurück und benutzt dieselbe Strategie, die wir vom chinesischen Restesatz her kennen: Ist R ein Integritätsbereich und suchen wir ein Polynom $h \in R[X]$ vom Grad d, das an den Stellen $c_i \in R$ für $i = 0, \ldots, d$ die Werte $h_i \in R$ annimmt, so konstruieren wir zunächst Polynome α_i mit $\alpha_i(c_i) = 1$ und $\alpha_i(c_j) = 0$ für $j \neq i$. Das Verschwinden an den Stellen c_j können wir erreichen, indem wir die

Linearfaktoren $(X - c_j)$ für $j \neq i$ miteinander multiplizieren. Um an der Stelle c_i den Wert eins zu erhalten, müssen wir allerdings noch durch das Produkt der $(c_i - c_j)$ dividieren, und damit kommen wir eventuell aus R hinaus und müssen im Quotientenkörper rechnen. Mit den so definierten Polynomen

$$\alpha_i(X) = \frac{\prod_{j \neq i}(X - c_j)}{\prod_{j \neq i}(c_i - c_j)}$$

ist das Interpolationspolynom dann $f(X) = \sum_{i=1}^{d} \alpha_i(X) h_i$.

(Das Interpolationsverfahren von LAGRANGE ist zwar einfach zu verstehen und führt auf eine elegante Formel, es gibt jedoch effizientere Verfahren, die auch hier anwendbar sind, z.B. das von ISAAC NEWTON. Für Einzelheiten sei auf die Numerik-Vorlesung verwiesen.)

Die Nenner in der LAGRANGEschen (oder auch NEWTONschen) Interpolationsformel stören uns nicht besonders, da wir ja spezialisieren, indem wir für X_{n-1} jeweils Konstanten einsetzen, die c_i liegen also alle im Ring k der Konstanten. Falls es sich dabei um einen Körper handelt, haben wir überhaupt keine Probleme mit den Divisionen; im wohl wichtigsten Fall, daß wir über den ganzen Zahlen arbeiten, erhalten wir zwar Interpolationspolynome mit rationalen Koeffizienten, können diese aber zerlegen in einen konstanten Faktor mal einem ganzzahligen Polynom mit teilerfremden Koeffizienten, das für die Berechnung des ggT zweier primitiver ganzzahliger Polynome an Stelle des Interpolationspolynoms verwendet werden kann.

JOSEPH-LOUIS LAGRANGE (1736–1813) wurde als GIUSEPPE LODOVICO LAGRANGIA in Turin geboren und studierte dort zunächst Latein. Erst eine alte Arbeit von HALLEY über algebraische Methoden in der Optik weckte sein Interesse an der Mathematik, woraus ein ausgedehnter Briefwechsel mit EULER entstand. In einem Brief vom 12. August 1755 berichtete er diesem unter anderem über seine Methode zur Berechnung von Maxima und Minima; 1756 wurde er, auf EULERs Vorschlag, Mitglied der Berliner Akademie; zehn Jahre später zog er nach Berlin und wurde dort EULERs Nachfolger als mathematischer Direktor der dortigen Akademie

1787 wechselte er an die Pariser Académie des Sciences, wo er bis zu seinem Tod blieb und unter anderem an der Einführung des metrischen Systems beteiligt war. Seine Arbeiten umspannen weite Teile der Analysis, Algebra und Geometrie.

Damit ergibt sich folgender Algorithmus zur Zurückführung des ggT zweier Polynome in n Veränderlichen auf die Berechnung von ggTs von Polynomen in $n-1$ Veränderlichen:

Wir gehen aus von zwei Polynomen $F, G \in R_n = k[X_1, \ldots, X_n]$, mit $k = \mathbb{Z}, \mathbb{Q}$ oder $\mathbb{F}_p$ (oder sonst einem faktoriellen Ring, über dem wir den ggT zweier Polynome in einer Veränderlichen berechnen können).

1. Schritt (Initialisierung): Schreibe

$$F = \sum_{i=0}^{d} a_i(X_1, \ldots, X_{n-1}) X_n^i \quad \text{und}$$

$$G = \sum_{j=0}^{e} b_j(X_1, \ldots, X_{n-1}) X_n^j ,$$

wobei die führenden Koeffizienten a_d und b_e nicht identisch verschwinden sollen. Weiter sei $\mathcal{C} = \emptyset$ die Menge aller bislang betrachteten Spezialisierungen und $\mathcal{M} = \emptyset$ die Teilmenge der nach unserem jeweiligen Erkenntnisstand „guten“ Spezialisierungen.

Als nächstes werden die Inhalte $I(F)$ und $I(G)$ von F und G bezüglich obiger Darstellung berechnet, d.h. $I(F)$ ist der ggT der $a_i(X_1, \ldots, X_{n-1})$ und $I(G)$ der von $b_0(X_1, \ldots, X_{n-1})$ bis $b_e(X_1, \ldots, X_{n-1})$. Beides kann bestimmt werden durch eine Folge von ggT-Berechnungen in $n-1$ Veränderlichen, ebenso auch der ggT I_0 dieser beiden Inhalte. Weiter seien $f = F/I(F)$ und $g = G/I(G)$ die primitiven Anteile von F und G. Der ggT von F und G ist I_0 mal dem in den folgenden Schritten berechneten ggT von f und g.

2. Schritt: Wähle so lange ein neues zufälliges Element $c \in k \setminus \mathcal{C}$ und ersetze $\mathcal{C}$ durch $\mathcal{C} \cup \{c\}$, bis $a_d(X_1, \ldots, X_{n-2}, c)$ und $b_e(X_1, \ldots, X_{n-2}, c)$ nicht beide gleich dem Nullpolynom sind. (Meist wird dies bereits beim

ersten Versuch der Fall sein.) Berechne dann den ggT h_c von

$$f^{(c)} = \sum_{i=0}^{d} a_i(X_1, \ldots, X_{n-2}, c)X_n^i \quad \text{und}$$

$$g^{(c)} = \sum_{j=0}^{e} b_j(X_1, \ldots, X_{n-2}, c)X_n^j .$$

Falls $h_c = 1$, endet der Algorithmus mit dem Ergebnis $\text{ggT}(f, g) = 1$. Andernfalls wird $\mathcal{M} = \{c\}$ und $N = \deg_{X_n} h_c$ und m wird eins mehr als das Maximum der Grade der a_i und der b_j in der Variablen X_{n-1}.

3. Schritt: Falls die Elementanzahl $\#\mathcal{M}$ von $\mathcal{M}$ gleich m ist, wird das Interpolationspolynom $h \in k[X_1, \ldots, X_n]$ berechnet, das für jedes $c \in \mathcal{M}$ die Gleichung

$$h(X_1, \ldots, X_{n-1}, c, X_n) = h_c(X_1, \ldots, X_{n-2}, X_n)$$

erfüllt. *Falls* h sowohl f als auch g teilt, ist $h = \text{ggT}(f, g)$ und der Algorithmus endet mit diesem Ergebnis. Andernfalls waren alle bisherigen Spezialisierungen schlecht, und wir müssen von Neuem mit Schritt 2 beginnen.

4. Schritt: Falls $\#\mathcal{M} < m$, wählen wir ein zufälliges $c \in k \setminus \mathcal{C}$ solange, bis $a_d(X_1, \ldots, X_{n-2}, c)$ und $b_e(X_1, \ldots, X_{n-2}, c)$ nicht beide gleich dem Nullpolynom sind. Wir berechnen wieder den ggT h_c von

$$f^{(c)} = \sum_{i=0}^{d} a_i(X_1, \ldots, X_{n-2}, c)X_n^i \quad \text{und}$$

$$g^{(c)} = \sum_{j=0}^{e} b_j(X_1, \ldots, X_{n-2}, c)X_n^j .$$

Falls $h_c = 1$, endet der Algorithmus mit dem Ergebnis $\text{ggT}(f, g) = 1$.

Falls $\deg_{X_n} h_c > N$ ist, haben wir ein schlechtes c gewählt und gehen zurück zum Anfang des vierten Schritts.

Falls $\deg_{X_n} h_c < N$ ist, waren alle zuvor betrachteten Werte von c schlecht; wir setzen $\mathcal{M} = \{c\}$ und $N = \deg_{X_n} h_c$.

Falls schließlich $\deg_{X_n} h_c = N$ ist, ersetzen wir $\mathcal{M}$ durch $\mathcal{M} \cup \{c\}$, und es geht weiter mit Schritt 3.

Da es nur endlich viele schlechte Werte für c gibt, muß der Algorithmus nach endlich vielen Schritten enden.

Als Beispiel wollen wir den ggT der beiden Polynome

$$f = X^3 + X^2Y + X^2Z + XYZ + Y^2Z + YZ^2$$

und

$$g = X^3 + X^2Y + X^2Z + XY^2 + XZ^2 + Y^3 + Y^2Z + YZ^2 + Z^3$$

aus $\mathbb{Z}[X, Y, Z]$ berechnen. Wir fassen Sie zunächst auf als Polynome in Z mit Koeffizienten aus $\mathbb{Z}[X, Y]$:

$$f = YZ^2 + (X^2 + XY + Y^2)Z + X^3 + X^2Y$$

und

$$g = Z^3 + (X + Y)Z^2 + (X^2 + Y^2)Z + X^3 + X^2Y + XY^2 + Y^3$$

Der führende Koeffizient von f ist Y, der von g ist eins. Wie man leicht sieht, sind beide Polynome bereits primitiv.

Der höchste Y-Grad eines Koeffizienten ist drei; wir brauchen daher vier zufällig gewählte Spezialisierungen. Der Einfachheit und vor allem der Übersichtlichkeit halber seien hierfür die (nicht gerade „zufälligen“) Werte $c = 1, 2, 3$ und 4 gewählt.

Für $c = 1$ ist

$$f(X, 1, Z) = Z^2 + (X^2 + X + 1)Z + X^3 + X^2$$

und

$$g(X, 1, Z) = Z^3 + (X + 1)Z^2 + (X^2 + 1)Z + X^3 + X^2 + X + 1\,;$$

wir müssen den ggT dieser beiden Polynome berechnen.

Dies leistet der entsprechende Algorithmus für Polynome in zwei Veränderlichen; da die Polynome wieder primitiv sind und der höchste

X-Grad eines Koeffizienten gleich drei ist, müssen wir vier Spezialisierungen für X betrachten. Auch diese seien zufälligerweise gerade $1, 2, 3$ und 4. Wir erhalten folgende Ergebnisse:

d	$f(d, 1, Z)$	$g(d, 1, Z)$	ggT
1	$Z^2 + 3Z + 2$	$Z^3 + 2Z^2 + 2Z + 4$	$Z + 2$
2	$Z^2 + 7Z + 12$	$Z^3 + 3Z^2 + 5Z + 15$	$Z + 3$
3	$Z^2 + 13Z + 36$	$Z^3 + 4Z^2 + 10Z + 40$	$Z + 4$
4	$Z^2 + 21Z + 80$	$Z^3 + 5Z^2 + 17Z + 85$	$Z + 5$

Auch ohne Interpolationsformel sehen wir, daß

$$h_1(X, Z) = X + 1 + Z$$

das Interpolationspolynom ist. Division zeigt, daß

$$\frac{f(X, 1, Z)}{h_1(X, Z)} = X^2 + Z \quad \text{und} \quad \frac{g(X, 1, Z)}{h_1(X, Z)} = X^2 + Z^2 + 1$$

beides Polynome sind; somit ist

$$\text{ggT}\big(f(X, 1, Z), g(X, 1, Z)\big) = X + 1 + Z\,.$$

Als nächstes setzen wir $c = 2$ für Y ein; wir erhalten

$$f(X, 2, Z) = 2Z^2 + (X^2 + 2X + 4)Z + X^3 + 2X^2$$

und

$$g(X, 2, Z) = Z^3 + (X + 2)Z^2 + (X^2 + 4)Z + X^3 + 2X^2 + 4X + 8$$

und spezialisieren darin wieder X zu $1, 2, 3, 4$:

d	$f(d, 2, Z)$	$g(d, 2, Z)$	ggT
1	$2Z^2 + 7Z + 3$	$Z^3 + 3Z^2 + 5Z + 15$	$Z + 3$
2	$2Z^2 + 12Z + 16$	$Z^3 + 4Z^2 + 8Z + 32$	$Z + 4$
3	$2Z^2 + 19Z + 45$	$Z^3 + 5Z^2 + 13Z + 65$	$Z + 5$
4	$2Z^2 + 28Z + 96$	$Z^3 + 6Z^2 + 20Z + 120$	$Z + 6$

Hier ist unser ggT-Kandidat somit $h_2(X, Z) = X + 2 + Z$, und wieder zeigt Division, daß dies tatsächlich ein Teiler beider Polynome und somit deren ggT ist.

Für $c = 3$ ist

$$f(X, 3, Z) = 3Z^2 + (X^2 + 3X + 9)Z + X^3 + 3X^2$$

und

$$g(X, 3, Z) = Z^3 + 4Z^2 + 10Z + 40\,.$$

Die Spezialisierungen in X und ihre größten gemeinsamen Teiler sind

d	$f(d, 3, Z)$	$g(d, 3, Z)$	ggT
1	$3Z^2 + 13Z + 4$	$Z^3 + 4Z^2 + 10Z + 40$	$Z + 4$
2	$3Z^2 + 19Z + 20$	$Z^3 + 5Z^2 + 13Z + 65$	$Z + 5$
3	$3Z^2 + 27Z + 54$	$Z^3 + 6Z^2 + 18Z + 108$	$Z + 6$
4	$3Z^2 + 37Z + 112$	$Z^3 + 7Z^2 + 25Z + 175$	$Z + 7$

Hier ist entsprechend $h_3(X, Z) = X + 3 + Z$.

Für $c = 4$ schließlich erhalten wir

$$f(X, 4, Z) = 4Z^2 + (X^2 + 4X + 16)Z + X^3 + 4X^2$$

und

$$g(X, 4, Z) = Z^3 + (X + 4)Z^2 + (X^2 + 16)Z + X^3 + 4X^2 + 16X + 64\,.$$

Die Spezialisierungen in X und ihre größten gemeinsamen Teiler sind

d	$f(d, 4, Z)$	$g(d, 4, Z)$	ggT
1	$4Z^2 + 21Z + 5$	$Z^3 + 5Z^2 + 17Z + 85$	$Z + 5$
2	$4Z^2 + 28Z + 24$	$Z^3 + 6Z^2 + 20Z + 120$	$Z + 6$
3	$4Z^2 + 37Z + 63$	$Z^3 + 7Z^2 + 25Z + 175$	$Z + 7$
4	$4Z^2 + 48Z + 128$	$Z^3 + 8Z^2 + 32Z + 256$	$Z + 8$

Dies führt auf $h_4(X, Z) = X + 4 + Z$.

Auch das Polynom $h(X, Y, Z)$ mit $h(X, c, Z) = h_c(X, Z)$ für die Werte $c = 1, 2, 3, 4$ läßt sich ohne Interpolationsformel leicht erraten: Offensichtlich ist

$$h(X, Y, Z) = X + Y + Z\,.$$

Division zeigt, daß

$$\frac{f}{h} = X^2 + YZ \quad \text{und} \quad \frac{g}{h} = X^2 + Y^2 + Z^2$$

ist; somit ist

$$\mathrm{ggT}(f, g) = h = X + Y + Z\ .$$

Dieses Ergebnis hätten wir natürlich schon sehr viel früher erraten können, und in der Tat wird der Algorithmus oft so implementiert, daß man bereits nach eigentlich zu wenigen Spezialisierungen interpoliert und nachprüft, ob man einen gemeinsamen Teiler gefunden hat; wenn ja, ist dies der ggT. Falls nein, läßt sich aber noch nicht schließen, daß alle bisherigen Spezialisierungen schlecht waren; vielleicht waren auch nur die Grade einiger Koeffizienten zu klein, was sich nur durch weitere Spezialisierungen und Interpolationen feststellen läßt.