Wegen $f\tilde{g} = \tilde{f}g$ und $r\tilde{s} = \tilde{r}s$ ist

$$(\tilde{f}\tilde{s} + \tilde{r}\tilde{g}) \cdot gs = \tilde{f}\tilde{s}gs + \tilde{r}\tilde{g}gs = \tilde{f}gs\tilde{s} + \tilde{r}sg\tilde{g}$$
$$= g\tilde{g}s\tilde{s} + r\tilde{s}g\tilde{g} = (gs + ry)\tilde{g}\tilde{s}$$

und $(\tilde{f}\tilde{r})(gs) = \tilde{f}g\tilde{r}s = g\tilde{g}r\tilde{s} = (gr)(\tilde{g}\tilde{s})$, d.h. auch die Ergebnisse sind äquivalent.

Man rechnet leicht nach (wie bei $\mathbb{Q}$), daß diese Äquivalenzklassen einen Ring bilden mit $\frac{0}{1}$ als Null und $\frac{1}{1}$ als Eins; er ist sogar ein Körper, denn für $f, g \neq 0$ ist $\frac{g}{s}$ ein multiplikatives Inverses zu $\frac{f}{g}$, da $(fg, fg) \sim (1, 1)$. Identifizieren wir schließlich ein Element $f \in R$ mit dem Bruch $\frac{f}{1}$, so können wir R in den Körper K einbetten.

Definition: Der so konstruierte Körper K heißt Quotientenkörper von R, in Zeichen $K = \text{Quot } R$.

Das Standardbeispiel ist natürlich $\mathbb{Q} = \text{Quot } \mathbb{Z}$, aber auch der Quotientenkörper $k(x) \underset{\text{def}}{=} \text{Quot } k[x]$ eines Polynomrings über einem Körper k ist wichtig: $k(x)$ heißt rationaler Funktionenkörper in einer Veränderlichen über k. Seine Elemente sind rationale Funktionen in x, d.h. Quotienten von Polynomen in x, wobei der Nenner natürlich nicht das Nullpolynom sein darf.

Für Polynome, die statt über einem Körper nur über einem faktoriellen Ring definiert sind, sind die beiden folgenden Begriffe sehr wesentlich:

Definition: *a)* Der *Inhalt* eines Polynoms $f = a_n x^n + \cdots + a_0 \in R[x]$ ist der größte gemeinsame Teiler $I(f)$ seiner Koeffizienten a_i.
b) f heißt *primitiv*, wenn die a_i zueinander teilerfremd sind.

Indem wir die sämtlichen Koeffizienten eines Polynoms durch deren gemeinsamen ggT dividieren sehen wir, daß sich jedes Polynom aus $R[x]$ als Produkt seines Inhalts mit einem primitiven Polynom schreiben läßt. Diese Zerlegung bleibt bei der Multiplikation zweier Polynome erhalten:

Lemma: R sei ein faktorieller Ring. Für zwei Polynome

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

und

$$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

aus $R[x]$ ist $I(fg) = I(f) \cdot I(g)$. Insbesondere ist das Produkt zweier primitiver Polynome wieder primitiv.

Beweis: Wir schreiben $f = I(f) \cdot f^*$ und $g = I(g) \cdot g^*$ mit primitiven Polynomen f^* und g^*; dann ist $fg = I(f) \cdot I(g) \cdot (f^* g^*)$. Falls $f^* g^*$ wieder ein primitives Polynom ist, folgt, daß $I(fg) = I(f) \cdot I(g)$ sein muß.

Es genügt daher, zu zeigen, daß das Produkt zweier primitiver Polynome wieder primitiv ist. Sei

$$fg = c_{n+m} x^{n+m} + c_{n+m-1} x^{n+m-1} + \cdots + c_1 x + c_0 \,;$$

dann ist $c_r = \sum_{i,j \text{ mit } i+j=r} a_i b_j$.

Angenommen, diese Koeffizienten c_r haben einen gemeinsamen Teiler, der keine Einheit ist. Wegen der Faktorialität von R gibt es dann auch ein irreduzibles Element p, das alle Koeffizienten c_r teilt.

Insbesondere ist p ein Teiler von $c_0 = a_0 b_0$; da p irreduzibel ist, muß mindestens einer der beiden Faktoren a_0, b_0 durch p teilbar sein. Da es im Lemma nicht auf die Reihenfolge von f und g ankommt, können wir o.B.d.A. annehmen, daß a_0 Vielfaches von p ist.

Da f ein primitives Polynom ist, kann nicht jeder Koeffizient a_i durch p teilbar sein; ν sei der kleinste Index, so daß a_ν kein Vielfaches von p ist. Genauso gibt es auch einen kleinsten Index $\mu \geq 0$, für den b_μ nicht durch p teilbar ist. In

$$c_{\mu+\nu} = \sum_{i,j \text{ mit } i+j=\mu+\nu} a_i b_j$$

ist dann der Summand $a_\nu b_\mu$ nicht durch p teilbar, denn für jeden anderen Summanden $a_i b_j$ ist entweder $i < \nu$ oder $j < \mu$, so daß mindestens einer der Faktoren und damit auch das Produkt durch p teilbar ist. Insgesamt ist daher $c_{\mu+\nu}$ nicht durch p teilbar, im Widerspruch zur Annahme.

Somit muß fg ein primitives Polynom sein. ∎

Satz von Gauß: R sei ein faktorieller Ring und $K = \operatorname{Quot} R$. Falls sich ein Polynom $f \in R[x]$ in $K[x]$ als Produkt zweier Polynome $g, h \in K[x]$ schreiben läßt, gibt es ein $\lambda \in K$, so daß $\widetilde{g} = \lambda g$ und $\widetilde{h} = \lambda^{-1} h$ in $R[x]$ liegen und $f = \widetilde{g} \cdot \widetilde{h}$.

Beweis: Durch Multiplikation mit einem gemeinsamen Vielfache aller Koeffizienten können wir aus einem Polynom mit Koeffizienten aus K eines mit Koeffizienten aus R machen. Dieses wiederum ist gleich seinem Inhalt mal einem primitiven Polynom. Somit läßt sich jedes Polynom aus $K[x]$ schreiben als Produkt eines Elements von K mit einem primitiven Polynom aus $R[x]$. Für g und h seien dies die Zerlegungen

$$g = cg^* \quad \text{und} \quad h = dh^* .$$

Dann ist $f = (cd)g^*h^*$, und nach dem Lemma ist g^*h^* ein primitives Polynom. Daher liegt $cd = I(f)$ in R, und wir können beispielsweise $\widetilde{g} = I(P)g^*$ und $\widetilde{h} = h^*$ setzen. ∎

Korollar: Ein primitives Polynom $f \in R[x]$ ist genau dann irreduzibel in $R[x]$, wenn es in $K[x]$ irreduzibel ist. ∎

CARL FRIEDRICH GAUSS (1777–1855) leistete wesentliche Beiträge zur Zahlentheorie, zur nichteuklidischen Geometrie, zur Differentialgeometrie und Kartographie, zur Fehlerrechnung und Statistik, zur Astronomie und Geophysik *usw.* Als Direktor der Göttinger Sternwarte baute er zusammen mit dem Physiker Weber den ersten Telegraphen. Er leitete die erste Vermessung und Kartierung des Königreichs Hannover, was sowohl seine Methode der kleinsten Quadrate als auch sein *Theorema egregium* motivierte, und zeitweise auch den Witwenfond der Universität Göttingen. Seine hierbei gewonnene Erfahrung nutzte er für erfolgreiche Spekulationen mit Aktien.

Aus dem Satz von GAUSS folgt induktiv sofort, daß seine Aussage auf für Produkte von mehr als zwei Polynomen gilt, und daraus folgt

Satz: Der Polynomring über einem faktoriellen Ring R ist faktoriell.

Beweis: Wir müssen zeigen, daß sich jedes $f \in R[x]$ bis auf Reihenfolge und Einheiten eindeutig als Produkt von Potenzen irreduzibler Elemente aus $R[x]$ und einer Einheit schreiben läßt. Dazu schreiben wir $f = I(f) \cdot f^*$ mit einem primitiven Polynom $f^* \in R[x]$ und zerlegen zunächst den Inhalt $I(f)$ in R. Da R nach Voraussetzung faktoriell ist, ist diese Zerlegung eindeutig bis auf Reihenfolge und Einheiten in R, und wie wir aus §2 wissen, sind die Einheiten von $R[x]$ gleich denen von R.

Als nächstes zerlegen wir das primitive Polynom f^* über dem Quotientenkörper K von R; dies ist möglich, da $K[x]$ als EUKLIDischer Ring faktoriell ist. Jedes der irreduziblen Polynome q_i, die in dieser Zerlegung vorkommen, läßt sich schreiben als $q_i = \lambda_i p_i$ mit einem $\lambda_i \in K^\times$ und einem primitiven Polynom $p_i \in R[x]$. Wir können daher annehmen, daß in der Zerlegung von f nur primitive Polynome aus $R[x]$ auftreten sowie eine Einheit aus K. Diese muß, da f^* Koeffizienten aus R hat und ein Produkt primitiver Polynome primitiv ist, in R liegen; da auch f^* primitiv ist, muß sie dort sogar eine Einheit sein.

Kombinieren wir diese Primzerlegung von f^* mit der Primzerlegung des Inhalts, haben wir eine Primzerlegung von f gefunden; sie ist (bis auf Reihenfolge und Einheiten) eindeutig, da entsprechendes für die Zerlegung des Inhalts, die Zerlegung von f^* sowie die Zerlegung eines Polynoms in Inhalt und primitiven Anteil gilt. ∎

Da wir einen Polynomring $R[x_1, \ldots, x_n]$ in n Veränderlichen als Polynomring $R[x_1, \ldots, x_{n-1}][x_n]$ in einer Veränderlichen über dem Polynomring $R[x_1, \ldots, x_{n-1}]$ in $n-1$ Veränderlichen auffassen können, folgt induktiv sofort:

Satz: Der Polynomring $R[x_1, \ldots, x_n]$ in n Veränderlichen über einem faktoriellen Ring R ist selbst faktoriell. Insbesondere sind $\mathbb{Z}[x_1, \ldots, x_n]$ sowie $k[x_1, \ldots, x_n]$ für jeden Körper k faktoriell. ∎

Damit wissen wir also, daß auch Polynome in mehreren Veränderlichen über $\mathbb{Z}$ oder über einem Körper in Produkte irreduzibler Polynome zer-

legt werden können; insbesondere existieren daher auch in dieser Ringen größte gemeinsame Teiler.

Der Beweis des obigen Satzes ist allerdings nicht konstruktiv; wir werden im nächsten Kapitel noch viel Arbeit investieren müssen, bevor wir Polynome über $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{F}_p$ oder anderen Körpern, in denen wir rechnen können, wirklich in ihre irreduziblen Faktoren zerlegen können.

§ 7: Resultanten

Wir wissen inzwischen, daß es auch in $\mathbb{Z}[x]$ größte gemeinsame Teiler gibt, und wir wissen auch, daß wir sie über den EUKLIDischen Algorithmus in $\mathbb{Q}[x]$ berechnen können. Wir wissen allerdings auch, daß der EUKLIDische Algorithmus in $\mathbb{Q}[x]$ bei der praktischen Durchführung seine Tücken hat und wollen daher eine Alternative finden, die stattdessen den EUKLIDischen Algorithmus in einem oder mehreren Polynomringen über endlichen Körpern benutzt. Hier haben wir allerdings auch Beispiele gesehen, wonach der ggT zweier Polynome aus $\mathbb{Z}[x]$ nicht einmal denselben Grad hat wie der der beiden Reduktionen modulo einer vorgegebenen Primzahl; insbesondere können Polynome, die in $\mathbb{Z}[x]$ und damit auch in $\mathbb{Q}[x]$ teilerfremd sind, modulo gewisser Primzahlen gemeinsame Teiler positiven Grades haben.

Um dieses Phänomen genauer zu untersuchen, wollen wir in diesem Paragraphen Kriterien dafür entwickeln, daß zwei Polynome einen größten gemeinsamen Teiler vom Grad d haben.

Was wir auf einfache Weise erhalten, ist ein Kriterium dafür, daß der ggT *mindestens* den Grad d hat. Wie üblich betrachten wir das Problem gleich über einem beliebigen faktoriellen Ring R; das wird uns später auch nützlich sein für die Lösung nichtlinearer Gleichungssysteme.

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

und

$$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

seien also zwei Polynome über $R[x]$ und nehmen an, es gebe ein Polynom $h \in R[x]$ vom Grad mindestens $d \geq 1$, das sowohl f als auch g

teilt. Dann ist

$$\frac{fg}{h} = \frac{f}{h} \cdot g = \frac{q}{h} \cdot f$$

ein gemeinsames Vielfaches von f und q, dessen Grad

$$\deg f + \deg g - \deg h = n + m - \deg h$$

höchstens gleich $n + m - d$.

Haben umgekehrt f und g ein gemeinsames Vielfaches vom Grad höchstens $n + m - d$, so hat auch ihr kleinstes gemeinsames Vielfaches S höchstens den Grad $n + m - d$. (Ein kleinstes gemeinsames Vielfaches existiert, da mit R auch $R[x]$ faktoriell ist.)

Zu S gibt es einerseits Polynome $u, v \in R[x]$, für die $S = uf = vg$ ist, andererseits ist p als *kleinstes* gemeinsames Vielfaches von f und g Teiler von fg, es gibt also ein Polynom $h \in R[x]$ mit $fg = Sh$. Für dieses ist

$$hv = \frac{fg}{S} \cdot v = f \cdot \frac{vg}{S} = f \quad \text{und} \quad hu = \frac{fg}{S} \cdot u = g \cdot \frac{uf}{S} = g\,,$$

es teilt also sowohl f als auch g und sein Grad $n + m - \deg S$ ist mindestens d. Damit ist gezeigt:

Lemma: Zwei Polynome $f, g \in R[x]$ haben genau dann einen gemeinsamen Teiler vom Grad mindestens d, wenn es nichtverschwindende Polynome $u, v \in R[x]$ gibt mit $\deg u \leq \deg g - d$ und $\deg v \leq \deg f - d$, so daß $uf = vg$ ist. ∎

Diese Bedingung schreiben wir um in ein lineares Gleichungssystem für die Koeffizienten von u und v: Da $\deg u \leq \deg g - d = m - d$ ist und $\deg v \leq \deg f - d = n - d$, lassen sich die beiden Polynome schreiben als

$$u = u_{m-d} x^{m-d} + u_{m-d-1} x^{m-d-1} + \cdots + u_1 x + u_0$$

und

$$v = v_{n-d} x^{n-d} + v_{n-d-1} x^{n-d-1} + \cdots + v_1 x + v_0\,.$$

Die Koeffizienten von x^r in uf und vg sind

$$\sum_{i,j \text{ mit } i+j=r} a_i u_j \quad \text{und} \quad \sum_{i,j \text{ mit } i+j=r} b_i v_j\,,$$

f und g haben daher genau dann einen gemeinsamen Teiler vom Grad mindestens d, wenn es nicht allesamt verschwindende Körperelemente $u_0, \ldots, u_{m-d}$ und $v_0, \ldots, v_{n-d}$ gibt, so daß

$$\sum_{i,j \text{ mit } i+j=r} a_i u_j - \sum_{i,j \text{ mit } i+j=r} b_i v_j = 0 \quad \text{für } r = 0, \ldots, n+m-d$$

ist. Dies ist ein homogenes lineares Gleichungssystem aus $n+m+1-d$ Gleichungen für die $n+m+2-2d$ Unbekannten $u_0, \ldots, u_{m-d}$ und $v_0, \ldots, v_{n-d}$; es hat genau dann eine nichttriviale Lösung, wenn seine Matrix kleineren Rang als $n+m+2-2d$ hat. Für $d = 1$, wenn die Matrix quadratisch ist, bedeutet dies einfach, daß ihre Determinante verschwindet; für $d > 1$ müssen wir d Determinanten von quadratischen Untermatrizen betrachten

Ausgeschrieben wird dieses Gleichungssystem, wenn wir mit dem Koeffizienten von x^{m+n-d} anfangen, zu

$$\begin{aligned}
a_n u_{m-d} - b_m v_{n-d} &= 0 \\
a_{n-1} u_{m-d} + a_n u_{m-d-1} - b_{m-1} v_{n-d} - b_m v_{n-d-1} &= 0 \\
a_{n-2} u_{m-d} + a_{n-1} u_{m-d-1} + a_n u_{m-d-2} & \\
- b_{m-2} v_{n-d} - b_{m-1} v_{n-d-1} b_m v_{n-d-2} &= 0 \\
&\ldots \\
a_0 u_3 + a_1 u_2 + a_2 u_1 + a_3 u_0 - b_0 v_3 - b_1 v_2 - b_2 v_1 - b_3 v_0 &= 0 \\
a_0 u_2 + a_1 u_1 + a_2 u_0 - b_0 v_2 - b_1 v_1 - b_2 v_0 &= 0 \\
a_0 u_1 + a_1 u_0 - b_0 v_1 - b_1 v_0 &= 0 \\
a_0 u_0 - b_0 v_0 &= 0
\end{aligned}$$

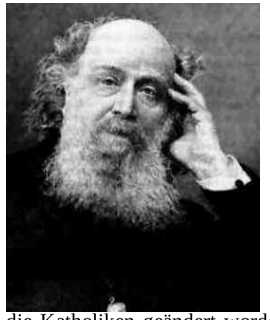
Natürlich ändert sich nichts an der nichttrivialen Lösbarkeit oder Unlösbarkeit dieses Gleichungssystems, wenn wir anstelle der Variablen v_j die Variablen $-v_j$ betrachten, womit alle Minuszeichen im obigen Gleichungssystem zu Pluszeichen werden; außerdem hat es sich – der größeren Übersichtlichkeit wegen – eingebürgert, die Transponierte der Matrix des Gleichungssystems zu betrachten. Dies führt auf die

$(n+m+2-2d) \times (n+m+1-d)$-Matrix

$$\begin{pmatrix}
a_n & a_{n-1} & a_{n-2} & \ldots & a_1 & a_0 & 0 & 0 & \ldots & 0 \\
0 & a_n & a_{n-1} & \ldots & a_2 & a_1 & a_0 & 0 & \ldots & 0 \\
0 & 0 & a_n & \ldots & a_3 & a_2 & a_1 & a_0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \ldots & a_0 \\
b_m & b_{m-1} & b_{m-2} & \ldots & b_2 & b_1 & b_0 & 0 & \ldots & 0 \\
0 & b_m & b_{m-1} & \ldots & b_3 & b_2 & b_1 & b_0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & 0 & b_m & b_{m-1} & b_{m-2} & \ldots & b_0
\end{pmatrix},$$

in der $m+1-d$ Zeilen aus Koeffizienten von f stehen und $n+1-d$ Zeilen aus Koeffizienten von g.

Für $d = 1$ ist diese Matrix quadratisch; man bezeichnet sie als SYLVESTER-Matrix und ihre Determinante als die *Resultante* $\mathrm{Res}(f, g)$ der beiden Polynome f und g. Falls man, etwa bei späteren Anwendungen auf Polynome mehrerer Veränderlicher, auf die Variable x hinweisen möchte, schreibt man auch $\mathrm{Res}_x(f, g)$. Die beiden Polynome f und g haben somit genau dann einen gemeinsamen Faktor positiven Grades, wenn $\mathrm{Res}(f, g)$ verschwindet.



JAMES JOSEPH SYLVESTER (1814–1897) wurde geboren als JAMES JOSEPH; erst als sein Bruder nach USA auswanderte und dazu einen dreiteiligen Namen brauchte, erweiterte er aus Solidarität auch seinem Namen. 1837 bestand er das berüchtigte Tripos-Examen der Universität Cambridge als Zweitbester, bekam aber keinen akademischen Abschluß, da er als Jude den dazu vorgeschriebenen Eid auf die 39 Glaubensartikel der Church of England nicht leisten konnte. Trotzdem wurde er Professor am University College in London; seine akademischen Grade bekam er erst 1841 aus Dublin, wo die Vorschriften gerade mit Rücksicht auf die Katholiken geändert worden waren. Während seiner weiteren Tätigkeit an sowohl amerikanischen als auch englischen Universitäten beschäftigte er sich mit Matrizen, fand die Diskriminante kubischer Gleichungen und entwickelte auch die allgemeine Theorie der Diskriminanten. In seiner Zeit an der Johns Hopkins University in Baltimore gründete er das American Journal of Mathematics, das noch heute mit die wichtigste mathematische Fachzeitschrift Amerikas ist.

Für $d > 1$ betrachten wir für $j = n+m+1-d, \ldots, n+m+2-2d$ jene quadratische Matrix M_j, die aus den ersten $n+m+2-d$ Spalten sowie der j-ten Spalte der obigen Matrix besteht. Offensichtlich hat letztere genau dann einen kleineren Rang als $n+m+1-d$, wenn alle d Matrizen M_j singulär sind, wenn also deren Determinanten verschwinden.

Sowohl die Resultante als auch die Determinanten der M_j sind Polynome in den Koeffizienten von f und g; wir haben daher den

Satz: Zwei Polynome $f, g \in R[X]$ über dem faktoriellen Ring R haben genau dann einen gemeinsamen Faktor vom Grad mindestens d, wenn gewisse Polynome in ihren Koeffizienten verschwinden. Insbesondere gibt es genau dann einen gemeinsamen Faktor positiven Grades, wenn die Resultante der beiden Polynome verschwindet. ∎

Die Resultante zweier Polynome der Grade 30 und 40 ist eine 70×70-Determinante – nichts, was man mit den aus der Linearen Algebra bekannten Algorithmen leicht und schnell ausrechnen könnte. Im Augenblick braucht uns das noch nicht sonderlich zu kümmern, da uns für den Algorithmus zur modularen Berechnung des ggT die bloße Existenz der Resultante genügt. Später, wenn wir Resultanten ernsthaft anwenden, werden wir sehen, daß sie sich erheblich effizienter berechnen lassen als andere Determinanten vergleichbarer Größe. Der Grund dafür liegt – wie eigentlich fast zu erwarten war – in der engen Beziehung zwischen Resultante und größtem gemeinsamen Teiler, die auch eine Beziehung zwischen Resultantenberechnung und EUKLIDischem Algorithmus liefert.

Für die ggT-Berechnung in $\mathbb{Z}[x]$ (und damit auch $\mathbb{Q}[x]$) sind Resultanten aus folgendem Grund für uns wichtig: 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 $\overline{f}, \overline{g} \in \mathbb{F}_p[x]$ 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 $\overline{h}, \overline{f_1}, \overline{g_1}$ die Reduktionen von h, f_1 und g_1 modulo p, so ist offensichtlich $\overline{f} = \overline{h}\,\overline{f_1}$ und $\overline{g} = \overline{h}\,\overline{g_1}$. Somit ist $\overline{h}$ auf jeden Fall ein gemeinsamer Teiler von $\overline{f}$ und $\overline{g}$, 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 teilerbar ist, hat $\overline{h}$ 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 $\overline{f}$ und $\overline{g}$. Wir werden gleich sehen, daß dies nicht immer so sein muß.

Zunächst aber wollen wir uns überlegen, wie wir ausschließen können, daß 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 mod p und g mod 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 mod p.

■

Falls unter diesen Bedingungen der ggT in $\mathbb{F}_p[x]$ denselben Grad hat wie der in $\mathbb{Z}[x]$, ist somit h mod p ein ggT in $\mathbb{F}_p[x]$. Wann das der Fall ist, sagen uns die Resultante *bzw.* die Determinanten der Matrizen M_j:

Angenommen, der ggT h von f und g in $\mathbb{Z}[x]$ hat den Grad $d \geq 0$. Dann haben f und g keinen gemeinsamen Teiler vom Grad mindestens $d + 1$; folglich ist im Falle $d = 0$ die Resultante eine von Null verschiedene ganze Zahl und für $d > 0$ hat mindestens eine der Matrizen M_j eine von null verschiedene Determinante.

Nun betrachten wir dasselbe Problem über $\mathbb{F}_p$. Da die Resultante und die Determinanten der M_j Polynome in den Koeffizienten der beiden Ausgangspolynome sind, führt ihre Berechnung über $\mathbb{F}_p$ zum selben Ergebnis wie die Berechnung über $\mathbb{Z}$ mit anschließender Reduktion modulo p. Somit gibt es modulo p genau dann einen gemeinsamen Teiler positiven Grades, wenn die Resultante durch p teilbar ist, und es gibt einen gemeinsamen Teiler vom Grad $d + 1$ mit $d > 0$, wenn die Determinanten *aller* Matrizen M_j durch p teilbar sind. Da eine ganze Zahl nur endlich viele Teiler hat, gibt es höchstens endlich viele solche Primzahlen.

Damit können wir das 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 $\bar{f}, \bar{g} \in \mathbb{F}_p[x]$ mit $\text{ggT}(\bar{f}, \bar{g}) = h^*$ gilt:
a) Falls p nicht die führenden Koeffizienten von sowohl f als auch g teilt, ist die Reduktion $\bar{h}$ von h ein Teiler von h^* und $\deg h^* \geq \deg h$.

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

■

§8: Die Landau-Mignotte-Schranke

In gewisser Weise ist der gerade bewiesene Satz das genaue Gegenteil von dem, was wir wollen: Wir wollen die schwierig zu berechnenden größten gemeinsamen Teiler in $\mathbb{Z}[x]$ zurückführen auf die leichter zu berechnenden über endlichen Körpern, Der obige Satz leistet das Umgekehrte.

Trotzdem können wir ihn zur Berechnung von ggTs in $\mathbb{Z}[x]$ verwenden, *falls* wir eine Schranke für die Beträge der Koeffizienten des ggT finden: Wenn wir wissen, daß alle Koeffizienten von h ganze Zahlen vom Betrag höchstens M sind und wir eine Primzahl $p \geq 2M + 1$ betrachten, so ist h durch h mod p eindeutig bestimmt.

Sofern wir eine solche Schranke M für den ggT zweier Polynome $f, g \in \mathbb{Z}[x]$ haben, können wir also eine Primzahl $p \geq 2M + 1$ wählen, die nicht beide führende Koeffizienten teilt, und den ggT $\bar{h} \in \mathbb{F}_p[x]$ von f mod p und g mod p berechnen. Zu $\bar{h}$ gibt es höchstens ein Polynom $h \in \mathbb{Z}[x]$, so daß h mod $p = \bar{h}$ ist. Falls es keines gibt, wissen wir, daß p eine der endlich vielen Ausnahmeprimzahlen ist; andernfalls müssen wir testen, ob h Teiler von f und g ist. Wenn ja, haben wir einen ggT von f und g gefunden, andernfalls folgt wieder, daß p eine Ausnahmeprimzahl war.

Im letzteren Fall müssen wir die Rechnung mit einer neuen Primzahl wiederholen; da es nur endlich viele Ausnahmeprimzahlen gibt, kann uns das höchstens endlich viele Male passieren.

Tatsächlich werden wir diesen Algorithmus im übernächsten Paragraphen noch etwas optimieren; aber damit er überhaupt funktioniert, brauchen wir als erstes eine Schranke für die Koeffizienten.

Eine solche Schranke brauchen wir auch im nächsten Kapitel für die Faktorisierung von Polynomen; deshalb fragen wir allgemeiner gleich

nach einer Schranke für die Koeffizienten eines beliebigen Teilers eines vorgegebenen Polynoms $f \in \mathbb{Z}[x]$.

$f \in \mathbb{Z}[x]$ 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: Am wichtigsten ist natürlich

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

die sogenannte *Höhe* des Polynoms. 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

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

und das letzte schließlich ist klar, denn

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

■

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 aus Kapitel 1, §6 bekannte Wurzelsatz von Viète, der die Koeffizienten a_i eines Polynoms

$$x^d + a_{d-1}x^{d-1} + \cdots + a_0 = \prod_{i=1}^{d}(x - z_i)$$

durch die Nullstellen z_i ausdrückt: Bis aufs Vorzeichen ist a_k die Summe aller Produkte aus jeweils $d-k$ der z_i.

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 ist bis aufs Vorzeichen die Summe aller Produkte von $d-k$ Nullstellen, und jedes einzelne solche Produkt 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 $f = \sum_{k=0}^{d} a_d x^d$ 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

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

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

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

■

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 $|z_j| > 1$ 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 $\mu(f) \le \|f\|_2$. ∎

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:

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

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

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

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 $f, g \in \mathbb{Z}[x]$

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

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.

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.

Als Beispiel betrachten wir noch einmal die beiden Polynome aus §3.

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

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.

Wir suchen eine Primzahl $p \geq 2 \cdot 510 + 1$, d.h. $p > 2 \cdot 510$:

```
> p := nextprime(2*510);
```

$$p := 1021$$

```
> 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 §3, hat sich abgesehen von den modularen Polynomdivisionen nichts wesentliches geändert, jedoch sind die Zwischenergebnisse erheblich angenehmer geworden.

§9: Der chinesische Restesatz

Zu Beginn des vorigen Paragraphen haben wir uns kurz überlegt, wie man grundsätzlich mit Hilfe der LANDAU-MIGNOTTE-Schranke und des modularen ggT größte gemeinsame Teiler in $\mathbb{Z}[x]$ berechnen kann. Bei nicht allzu großer LANDAU-MIGNOTTE-Schranke ist dies wahrscheinlich die schnellste Art und Weise, den ggT zu berechnen.

Bei großer LANDAU-MIGNOTTE-Schranke M wird allerdings eine Primzahl $p \geq 2M + 1$ nicht mehr in ein Maschinenwort passen, so daß alle Rechnungen in Langzahlarithmetik und damit recht langsam ausgeführt werden müssen.

Der Ausweg besteht darin, nicht modulo einer, sondern gleich modulo mehrerer Primzahlen zu rechnen. Die Idee dazu ist einfach: Wenn wir beispielsweise ein Zahl sowohl modulo zwei als auch modulo fünf kennen, kennen wir sie auch modulo zehn. Entsprechendes gilt allgemein:

Chinesischer Restesatz: Sind m, n zwei zueinander teilerfremde und a, b zwei beliebige Elemente eines EUKLIDischen Rings R, so gibt es Elemente $r \in R$ mit

$$r \equiv a \bmod m \quad \text{und} \quad r \equiv b \bmod n\,.$$

r ist modulo mn eindeutig bestimmt.

Beweis: Ausgangspunkt ist der erweiterte EUKLIDische Algorithmus: Da m und n teilerfremd sind, liefert er uns zwei Elemente $\alpha, \beta \in R$, so daß

$$\alpha m + \beta n = \mathrm{ggT}(m,n) = 1$$

ist. Somit ist

$$1 - \alpha m = \beta n \equiv \begin{cases} 1 & \bmod m \\ 0 & \bmod n \end{cases} \quad \text{und} \quad 1 - \beta n = \alpha m \equiv \begin{cases} 0 & \bmod m \\ 1 & \bmod n \end{cases},$$

also löst $r = \beta n a + \alpha m b \equiv \begin{cases} a & \bmod m \\ b & \bmod n \end{cases}$ das Problem.

Für jede andere Lösung s ist $r - s$ sowohl durch m als auch durch n teilbar; da beide teilerfremd sind, also durch mn. Umgekehrt ist klar, daß für jedes $\lambda \in R$ auch $r + \lambda mn$ eine Lösung ist. Die allgemeine

Lösung ist somit $r = (\beta a + \lambda m)n + (\alpha b - \lambda n)m$; insbesondere ist sie eindeutig modulo nm.

■

Bei der Lösung eines Systems

$$r \equiv a_i \bmod m_i \quad \text{für } i = 1, \ldots, N$$

können wir rekursiv vorgehen: Wir lösen die ersten beiden Kongruenzen $r \equiv a_1 \bmod m_1$ und $r \equiv a_2 \bmod m_2$ wie gerade besprochen; das Ergebnis ist eindeutig modulo $m_1 m_2$. Ist r_2 eine feste Lösung, so läßt sind die sämtlichen Lösung dieser beiden Kongruenzen gerade die Lösungen der einen Kongruenz

$$r \equiv r_2 \bmod m_1 m_2 \,.$$

Da die m_i paarweise teilerfremd sind, ist auch $m_1 m_2$ teilerfremd zu m_3. Mit dem erweiterten EUKLIDischen Algorithmus können wir daher wie oben das System

$$r \equiv r_2 \bmod m_1 m_2 \quad \text{und} \quad r \equiv a_3 \bmod m_3$$

lösen und zusammenfassen in einer Kongruenz

$$r \equiv r_3 \bmod m_1 m_2 m_3$$

und so weiter, bis wir schließlich ein r gefunden haben, das modulo aller m_i den gewünschten Wert hat und das modulo dem Produkt aller m_i eindeutig bestimmt ist.

Alternativ läßt sich die Lösung auch in einer geschlossenen Formel darstellen, allerdings um den Preis einer N-maligen statt $(N-1)$-maligen Anwendung des EUKLIDischen Algorithmus und größeren Zahlen schon von Beginn an: Um das System

$$r \equiv a_i \bmod m_i \quad \text{für} \quad i = 1, \ldots, N$$

zu lösen, berechne man zunächst für jedes i das Produkt

$$\widehat{m}_i = \prod_{j \neq i} m_j$$

der sämtlichen übrigen m_j und bestimme dazu Elemente $\alpha_i, \beta_i \in R$, für die gilt $\alpha_i m_i + \beta_i \widehat{m}_i = 1$. Dann ist

$$r = \sum_{j=1}^{N} \beta_j \widehat{m}_j a_j \equiv \beta_i \widehat{m}_i a_i = (1 - \alpha_i m_i) a_i \equiv a_i \bmod m_i \,.$$

Natürlich wird r hier – wie auch bei den obigen Formel – oft größer sein als das Produkt der m_i; um (in welchem Sinne auch immer) „kleine“ Lösungen zu finden, müssen wir also noch modulo diesem Produkt reduzieren.

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 lies sich die Gesamtzahl der Soldaten berechnen, wenn das Produkt der verschiedenen Reihenlängen größer war als diese Anzahl.

Es ist fraglich, ob die chinesischen Generäle wirklich soviel Mathematik konnten; Beispiele zu diesem Satz finden sich jedenfalls bereits 1247 in den *Mathematischen Abhandlungen in neun Bänden* von CH'IN CHIU-SHAO (1202–1261), allerdings geht es dort nicht um Soldaten, sondern um Reiskörner.

§ 10: 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. Zur ggT-Berechnung in $\mathbb{Z}[x]$ können wir den ggT der Inhalte problemlos nach dem klassischen EUKLIDischen Algorithmus bestimmen und multiplizieren den dann mit dem ggT der primitiven Anteile.

Seien also $f, g \in \mathbb{Z}[x]$ primitive Polynome. Die Grundidee des Algorithmus ist folgende:

a) Wir arbeiten nur mit Primzahlen, die nicht die führenden Koeffizienten sowohl von f als auch von g teilen. Nach dem Satz am Ende von §7 wissen wir dann, daß der ggT h_p von $f \bmod p$ und $g \bmod p$ mindestens denselben Grad hat wie $\mathrm{ggT}(f, g)$ und daß es nur endlich viele Primzahlen gibt, für die sich die beiden Grade unterscheiden. Für alle anderen p ist $h_p = \mathrm{ggT}(f, g) \bmod p$.

b) Die endlich vielen „schlechten“ Primzahlen, für die 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 p eine schlechte Primzahl sein. 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:

1. Schritt (Initialisierung): Berechne die LANDAU-MIGNOTTE-Schranke $\mathrm{LM}(f,g)$ und setze $M = 2\lceil \mathrm{LM}(f,g)\rceil + 1$. Außerdem wird $\mathcal{P} = \emptyset$ und $N = 1$ gesetzt

Da der Betrag eines jeden Koeffizienten des ggT höchstens gleich $\lceil \mathrm{LM}(f,g)\rceil$ ist, 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 führendem 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 mod p und g mod p. Falls dieser gleich eins 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 h_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 $\mathrm{LM}(f,g)$ sind. Falls das nicht möglich ist, haben wir bislang modulo lauter schlechten Primzahlen gerechnet, können also alle bisherigen Ergebnisse vergessen und gehen zurück zum zweiten Schritt.

Andernfalls wird überprüft, ob h sowohl f also 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 mod p und g mod 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 h_p ist.

Ist schließlich $\deg h = \deg h_p$, so konstruieren wir nach dem chinesischen Restesatz ein Polynom, das modulo N gleich h und modulo p gleich h_p ist und ersetzen N durch Np. Danach geht es weiter mit dem dritten Schritt.

Der Algorithmus muß enden, da es nur endlich viele schlechte Primzahlen p gibt, für die der in $\mathbb{F}_p[x]$ berechnete ggT nicht einfach die Reduktion von $\mathrm{ggT}(f,g)$ 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 $\mathrm{ggT}(f,g)$ 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 $\mathrm{ggT}(f, g) = x^2 + x + 1$.

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