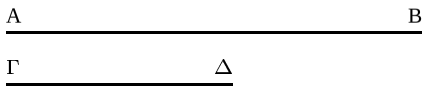
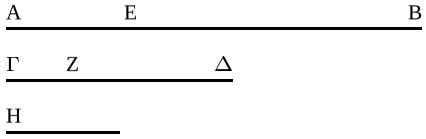
Kapitel 2
Grundalgorithmen

§ 1: Der Euklidische Algorithmus für ganze Zahlen

a) Der klassische Euklidische Algorithmus

Bei EUKLID, in Proposition 2 des siebten Buchs seiner *Elemente*, wird er so beschrieben:

> *Zu zwei gegebenen Zahlen, die nicht prim gegeneinander sind, ihr größtes gemeinsames Maß zu finden.*
>
> Die zwei gegebenen Zahlen, die nicht prim, gegeneinander sind, seien AB, ΓΔ. Man soll das größte gemeinsame Maß von AB, ΓΔ finden.
>
> 
>
>
> Wenn ΓΔ hier AB mißt – sich selbst mißt es auch – dann ist ΓΔ gemeinsames Maß von ΓΔ, AB. Und es ist klar, daß es auch das größte ist, denn keine Zahl größer ΓΔ kann ΓΔ messen.
>
> Wenn ΓΔ aber AB nicht mißt, und man nimmt bei AB, ΓΔ abwechselnd immer das kleinere vom größeren weg, dann muß (schließlich) eine Zahl übrig bleiben, die die vorangehende mißt. Die Einheit kann nämlich nicht übrig bleiben; sonst müßten AB, ΓΔ gegeneinander prim sein, gegen die Voraussetzung. Also muß eine Zahl übrig bleiben, die die vorangehende mißt. ΓΔ lasse, indem es BE mißt, EA, kleiner als sich selbst übrig; und EA lasse, indem es ΔZ mißt, ZΓ, kleiner als sich selbst übrig; und ΓZ messe AE.
>
> 
>

> Da ΓZ AE mißt und AE ΔZ, muß ΓZ auch ΔZ messen; es mißt aber auch sich selbst, muß also auch das Ganze ΓΔ messen. ΓΔ mißt aber BE; also mißt ΓZ auch BE; es mißt aber auch EA, muß also auch das Ganze BA messen. Und es mißt auch ΓΔ; ΓZ mißt also AB und ΓΔ; also ist ΓZ gemeinsames Maß von AB, ΓΔ. Ich behaupte, daß es auch das größte ist. Wäre nämlich ΓZ nicht das größte gemeinsame Maß von AB, ΓΔ, so müßte irgendeine Zahl größer ΓZ die Zahlen AB und ΓΔ messen. Dies geschehe; die Zahl sei H. Da H dann ΓΔ mäße und ΓΔ BE mißt, mäße H auch BE; es soll aber auch das Ganze BA messen, müßte also auch den Rest AE messen. AE mißt aber ΔZ; also müßte H auch ΔZ messen; es soll aber auch das Ganze ΔΓ messen, müßte also auch den Rest ΓZ messen, als größere Zahl die kleinere; dies ist unmöglich. Also kann keine Zahl größer ΓZ die Zahlen AB und ΓΔ messen; ΓZ ist also das größte gemeinsame Maß von AB, ΓΔ; dies hatte man beweisen sollen.

Was hier als erstes überrascht, ist die Beschränkung auf nicht zueinander teilerfremde Zahlen. Der Grund dafür liegt darin, daß die klassische griechische Philosophie und Mathematik die Eins nicht als Zahl betrachtete: Zahlen begannen erst bei zwei, und auch Mengen mußten mindestens zwei Elemente haben. Auch bei den Aristotelischen Syllogismen musste sich ein Prädikat auf mindestens zweielementige Klassen beziehen: Die oft als klassischer Syllogismus zitierte Schlußweise

> Alle Menschen sind sterblich
> SOKRATES ist ein Mensch
> Also ist SOKRATES sterblich

wäre von ARISTOTELES nicht anerkannt worden, denn es gab schießlich nur einen SOKRATES. Erst bei seinen Nachfolgern, den Peripatetikern, setzte sich langsam auch die Eins als Zahl durch. EUKLID macht noch brav eine Fallunterscheidung: In Proposition 1, unmittelbar vor der abgedruckten Proposition 2, führt er praktisch dieselbe Konstruktion durch für teilerfremde Zahlen. Außerdem fällt auf, daß EUKLID seine Konstruktion rein geometrisch durchführt; wenn er von einer Strecke eine andere Strecke abträgt solange es geht, ist das natürlich in unserer heutigen arithmetischen Sprache gerade die Konstruktion des Divisionsrests bei der Division der beiden Streckenlängen durcheinander.

In dieser Sprechweise wird der EUKLIDische Algorithmus für heutige Leser wohl auch klar: Wir suchen den größten gemeinsamen Teiler zweier natürlicher Zahlen a und b, d.h. die größte natürliche Zahl d, die

sowohl a als auch b teilt. Wir schreiben kurz

$$d = \mathrm{ggT}(a, b)\,.$$

Grundidee des EUKLIDischen Algorithmus ist die Anwendung der Division mit Rest: Für je zwei natürliche Zahlen x und y gibt es nichtnegative ganze Zahlen q und r, so daß

$$x = qy + r \quad \text{und} \quad 0 \le r < y$$

ist. Alsdann ist

$$\mathrm{ggT}(x, y) = \mathrm{ggT}(y, r)\,,$$

denn wegen der beiden Gleichungen

$$x = qy + r \quad \text{und} \quad r = x - qy$$

teilt jeder gemeinsame Teiler von x und y auch r, und jeder gemeinsame Teiler von y und r teilt auch x.

Der EUKLIDische Algorithmus nutzt dies aus, um die Zahlen, deren ggT bestimmt werden muß, sukzessive zu verkleinern, bis der ggT zweier Zahlen berechnet werden muß, von denen die eine Teiler der anderen ist; in diesem Fall ist natürlich die kleinere der beiden Zahlen gleich dem ggT.

Formal sieht der Algorithmus demnach folgendermaßen aus:

Schritt 0: Setze $r_0 = a$ und $r_1 = b$

Schritt i, $i \ge 1$**:** Falls $r_i = 0$ ist, endet der Algorithmus mit dem Ergebnis $\mathrm{ggT}(a, b) = r_{i-1}$; andernfalls dividiere man r_{i-1} mit Rest durch r_i und bezeichne den Divisionsrest mit r_{i+1}.

(Bei einer tatsächlichen Implementierung bieten sich natürlich einige offensichtliche Optimierungen an.)

Der Algorithmus muß nach endlich vielen Schritten enden, denn bei der Division mit Rest ist stets $0 \le r_{i+1} < r_i$, so daß r_i mit jedem Schritt kleiner wird, was bei natürlichen Zahlen nicht unbegrenzt möglich ist. Da außerdem in jedem Schritt

$$\mathrm{ggT}(r_{i-1}, r_i) = \mathrm{ggT}(r_i, r_{i+1})$$

ist und im letzten Schritt, wenn r_{i-1} den vorigen Wert r_{i-2} teilt,

$$\mathrm{ggT}(r_{i-1}, r_{i-2}) = r_{i-1}$$

ist, folgt induktiv

$$\mathrm{ggT}(a, b) = r_{i-1}\,,$$

so daß der Algorithmus das richtige Ergebnis liefert.

Es ist nicht ganz sicher, ob EUKLID wirklich gelebt hat; das nebenstehende Bild aus dem 18. Jahrhundert ist mit Sicherheit reine Phantasie. EUKLID ist vor allem bekannt als Autor der *Elemente*, in denen er u.a. die Geometrie seiner Zeit systematisch darstellte und (in gewisser Weise) auf wenige Definitionen sowie die berühmten fünf Postulate zurückführte. Diese Elemente entstanden um 300 v. Chr. und waren zwar nicht der erste, aber doch der erfolgreichste Versuch einer solchen Zusammenfassung. EUKLID arbeitete wohl am Museion in Alexandrien; außer den Elementen schrieb er noch ein Buch über Optik und weitere, teilweise verschollene Bücher.

b) Abschätzung des Rechenaufwands

Der obige Beweis, daß der EUKLIDische Algorithmus nach endlich vielen Schritten zum Ziele führt, nutzt aus, daß der Divisionsrest in jedem Schritt kleiner ist als im Schritt zuvor; die Anzahl der Divisionen ist als beschränkt durch das Minimum der beiden Zahlen, auf die wir den Algorithmus anwenden. In der Kryptographie gibt es Anwendungen, bei denen diese Zahlen etwa 600-stellig sind, und natürlich ist es undenkbar, 10^{600} Rechenoperationen auszuführen. Zum Glück ist der tatsächliche Aufwand deutlich geringer.

Um zu einer realistischeren Abschätzung zu kommen, suchen wir die kleinsten natürlichen Zahlen a, b, für die n Divisionen notwendig sind. Im Falle $n = 1$ sind dies offensichtlich $a = b = 1$; im Fall $a = b$ kommt man immer mit genau einer Division aus.

Dies ist allerdings ein eher untypischer Fall, der sich insbesondere nicht rekursiv verallgemeinern läßt, denn ab dem zweiten Schritt des EUKLIDischen Algorithmus ist der Divisor stets kleiner als der Dividend: Ersterer ist schließlich der Rest bei der vorangegangenen Division und

letzterer der Divisor. Die kleinsten natürlichen Zahlen $a \neq b$, für die man mit nur einer Division auskommt, sind $a = 2$ und $b = 1$.

Als nächstes Suchen wir die kleinsten Zahlen a, b, für die zwei Divisionen notwendig sind. Ist r der Rest bei der ersten Division, so ist $b : r$ die zweite Division. Für diese muß $r \geq 1$ und $b \geq 2$ sein, und $a = qb + r$, wobei q der Quotient bei der ersten Division ist. Dieser ist mindestens eins, die kleinstmöglichen Werte sind damit

$$r = 1, \quad b = 2 \quad \text{und} \quad a = b + r = 3\,.$$

Allgemeiner seien a_n und b_n mit $a_n > b_n$ die kleinsten Zahlen, für die n Divisionen notwendig sind, und r_n sei der Rest bei der Division von a_n durch b_n. Im nächsten Schritt des EUKLIDischen Algorithmus wird dann b_n durch r_n dividiert; da a_n und b_n die kleinstmöglichen Zahlen sind, muß dabei der Quotient gleich eins sein und $b_n = a_{n-1}$ sowie $r_n = b_{n-1}$. Also ist

$$a_n = b_n + r_n = a_{n-1} + b_{n-1} = a_{n-1} + a_{n-2} \quad \text{und} \quad b_n = a_{n-1}\,.$$

Da wir $a_1 = 2$ und $b_1 = 1$ kennen, können wir daraus alle a_n und b_n berechnen; was wir erhalten, sind die sogenannten FIBONACCI-Zahlen.

Sie sind durch folgende Rekursionsformel definiert:

$$F_0 = 0, \qquad F_1 = 1 \qquad \text{und} \qquad F_i = F_{i-1} + F_{i-2} \quad \text{für } i \geq 2\,.$$

Somit ist $a_1 = F_3$ und $b_1 = F_2$, und es folgt rekursiv, daß $a_n = F_{n+2}$ und $b_n = F_{n+1}$ ist.

Damit folgt

Satz von Lamé (1844)**:** Die kleinsten natürlichen Zahlen a, b, für die bei EUKLIDischen Algorithmus $n \geq 2$ Divisionen notwendig sind, sind $a = F_{n+2}$ und $b = F_{n+1}$. ∎

(Für $n = 1$ gilt der Satz nur, wenn wir zusätzlich voraussetzen, daß $a \neq b$ ist; für $n \geq 2$ ist dies automatisch erfüllt.)

GABRIEL LAMÉ (1795–1870) studierte von 1813 bis 1817 Mathematik an der Ecole Polytechnique, danach bis 1820 Ingenieurwissenschaften an der Ecole des Mines. Auf Einladung Zar Alexanders I. ging er 1820 nach Rußland, wo er Vorlesungen über Analysis, Physik, Chemie und Ingenierswissenschaften hielt. Nach seiner Rückkehr 1832 erhielt er einen Lehrstuhl für Physik an der Ecole Polytechnique, 1852 einen für mathematische Physik und Wahrscheinlichkeitstheorie an der Sorbonne. 1836/37 war er war auch wesentlich am Bau der Eisenbahnlinien Paris-Versailles und Paris-St. Germain beteiligt.

Um zu einer Aufwandsabschätzung zu kommen, müssen wir uns die FIBONACCI-Zahlen etwas genauer ansehen. FIBONACCI führte sie ein, um die Vermehrung einer Karnickelpopulation durch ein einfaches Modell zu berechnen. In seinem 1202 erschienenen Buch *Liber abaci* schreibt er:

Ein Mann bringt ein Paar Karnickel auf einen Platz, der von allen Seiten durch eine Mauer umgeben ist. Wie viele Paare können von diesem Paar innerhalb eines Jahres produziert werden, wenn man annimmt, daß jedes Paar jeden Monat ein neues Paar liefert, das vom zweiten Monat nach seiner Geburt an produktiv ist?

LEONARDO PISANO (1170–1250) ist heute vor allem unter seinem Spitznamen FIBONACCI bekannt; gelegentlich nannte er sich auch BIGOLLO, auf Deutsch *Tunichtgut* oder *Reisender.* Seine Bücher waren mit die ersten, die die indisch-arabischen Ziffern in Europa einführten. Er behandelt darin nicht nur Rechenaufgaben für Kaufleute, sondern auch zahlentheoretische Fragen, beispielsweise daß man die Quadratzahlen durch Aufaddieren der ungeraden Zahlen erhält. Auch betrachtet er Beispiele nichtlinearer Gleichungen, die er approximativ löst, und erinnert an viele in Vergessenheit geratene Ergebnisse der antiken Mathematik.

Um die Zahlen F_i durch eine geschlossene Formel darzustellen, betrachten wir die (formale) Potenzreihe

$$X(z) = \sum_{i=0}^{\infty} F_i z^i\,.$$

Auf Grund der Rekursionsformel $F_i = F_{i-1} + F_{i-2}$ für $i \geq 2$ ist

$$\sum_{i=2}^{\infty} F_i z^i = \sum_{i=2}^{\infty} F_{i-1} z^i + \sum_{i=2}^{\infty} F_{i-1} z^i = z \sum_{i=1}^{\infty} F_i z^i + z^2 \sum_{i=0}^{\infty} F_{i-1} z^i ,$$

was wir wegen $F_0 = 0$ und $F_1 = 1$ auch in der Form

$$X(z) - z = zX(z) + z^2 X(z)$$

schreiben können. Auflösen nach $X(z)$ führt auch

$$X(z) = \frac{z}{1 - z - z^2} .$$

Um die rechte Seite als Potenzreihe in z zu schreiben, versuchen wir, sie durch Terme der Form $\frac{1}{1-q}$ darzustellen, die wir als Summen geometrischer Reihen $\sum_{i=0}^{\infty} q^i$ schreiben können.

Da $z^2 + z - 1 = \left(z + \frac{1}{2}\right)^2 - \frac{5}{4}$ ist, verschwindet der Nenner für die beiden Werte

$$z = z_{1/2} = -\frac{1}{2} \pm \sqrt{\frac{5}{4}} = -\frac{1 \mp \sqrt{5}}{2} .$$

Nach dem Satz von VIÈTE ist $z_1 z_2 = z_1 + z_2 = -1$, also

$$1 - z - z^2 = -(z - z_1)(z - z_2) = \frac{(z - z_1)(z - z_2}{z_1 z_2}$$

$$= \left(1 - \frac{z}{z_1}\right)\left(1 - \frac{z}{z_2}\right) = (1 + z_2 z)(1 + z_1 z) .$$

Da wir die Summenformel der geometrischen Reihe besser anwenden können, wenn wir Terme der Form $(1 - q)$ haben, definieren wir die beiden neuen Zahlen

$$\phi = \frac{1 + \sqrt{5}}{2} \quad \text{und} \quad \overline{\phi} = \frac{1 - \sqrt{5}}{2} ;$$

dann ist

$$1 - z - z^2 = (1 - \phi z)(1 - \overline{\phi} z) .$$

Bemerkung: ϕ und $\overline{\phi}$ erfüllen die Gleichung $\phi^2 - \phi - 1 = 0$ oder $\phi^2 = \phi + 1$, d.h. ϕ ist das Verhältnis des *goldenen Schnitts:* Zwei Größen $a > b$ stehen bekanntlich in diesem Verhältnis, wenn sich $a + b$ zu a verhält wie a zu b. Für $\phi = a/b$ ist dies die Bedingung

$$1 + \phi^{-1} = 1 + \frac{b}{a} = \frac{a + b}{a} = \frac{a}{b} = \phi ,$$

die nach Multiplikation mit ϕ zu $\phi + 1 = \phi^2$ wird.

Nach diesen Vorbereitungen können wir mit der Partialbruchzerlegung von $X(z)$ beginnen: Nach der allgemeinen Theorie machen wir den Ansatz

$$X(z) = \frac{z}{1 - z - z^2} = \frac{\alpha}{1 - \phi z} + \frac{\beta}{1 - \overline{\phi} z} = \frac{(\alpha + \beta) - (\alpha\overline{\phi} + \beta\phi)z}{1 - z - z^2} ,$$

der auf die beiden Gleichungen

$$\alpha + \beta = 0 \quad \text{und} \quad \alpha\overline{\phi} + \beta\phi = -1$$

führt. Einsetzen von $\beta = -\alpha$ in die zweite Gleichung zeigt, daß

$$\alpha(\overline{\phi} - \phi) = -\alpha\sqrt{5} = -1 \quad \text{oder} \quad \alpha = \frac{1}{\sqrt{5}}$$

ist. Also ist

$$X(z) = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \phi z} - \frac{1}{1 - \overline{\phi} z} \right) .$$

Diese beiden Summanden können wir nun als Summen geometrischer Reihen interpretieren und erhalten

$$X(z) = \frac{1}{\sqrt{5}} \left(\sum_{i=0}^{\infty} \phi^i z^i + \sum_{i=0}^{\infty} \overline{\phi}^i z^i \right) = \frac{1}{\sqrt{5}} \sum_{i=1}^{\infty} (\phi^i + \overline{\phi}^i) .$$

Koeffizientenvergleich zeigt, daß

$$F_i = \frac{\phi^i + \overline{\phi}^i}{\sqrt{5}}$$

ist, womit wir die gesuchte explizite Formel gefunden hätten.

In Zahlen ist $\phi = \frac{1 + \sqrt{5}}{2} \approx 1{,}618034$, $\overline{\phi} = 1 - \phi \approx -0{,}618034$ und $\sqrt{5} \approx 2{,}236068$; der Quotient $\overline{\phi}^i / \sqrt{5}$ ist also für jedes i kleiner als $1/2$.

Daher können wir F_i auch einfacher berechnen als nächste ganze Zahl zu $\phi^i/\sqrt{5}$. Insbesondere folgt, daß F_i exponentiell mit i wächst.

Für $a = F_{n+2}$ und $b = F_{n+1}$, die beiden kleinsten Zahlen, für die beim EUKLIDischen Algorithmus n Divisionen notwendig sind, ist also

$$\begin{aligned} n &\approx \log_\phi \frac{b}{\sqrt{5}} = \log_\phi b - \log_\phi \sqrt{5} = \frac{\ln b}{\ln \phi} - \frac{\ln \sqrt{5}}{\ln \phi} \\ &\approx 2{,}078 \ln b - 1{,}672\,. \end{aligned}$$

Für beliebige Zahlen $a > b$ können nicht mehr Divisionen notwendig sein für die auf b folgenden nächstgrößeren FIBONACCI-Zahlen, also gibt obige Formel für jedes b eine obere Grenze. Die Anzahl der Divisionen wächst also nicht, wie bei der naiven Abschätzung im vorigen Abschnitt, mit b, sondern nur mit $\ln b$. Für sechshundertstellige Zahlen a, b müssen wir also nicht mit 10^{600} Divisionen rechnen, sondern mit weniger als drei Tausend, was auch für weniger leistungsfähige Computer problemlos und schnell möglich ist.

Tatsächlich ist natürlich auch noch 3 000 für die meisten sechshundertstelligen Zahlen eine gewaltige Überschätzung des tatsächlichen Aufwands, denn hier handelt es sich ja um eine obere Grenze, von der wir nur im Falle der FIBONACCI-Zahlen wissen, daß sie wirklich angenommen wird. Für zufällig gewählte Zahlen ist der Aufwand im Durchschnitt erheblich geringer, siehe dazu DONALD E. KNUTH: *The Art of Computer Programming 2: Seminumerical Algorithms,* Addison Wesley, viele Auflagen.

c) Der erweiterte Euklidische Algorithmus

Die Grundform des EUKLIDische Algorithmus reicht uns nicht aus; für viele Zwecke (nicht nur) der Computeralgebra ist mindestens genauso wichtig, den ggT als ganzzahlige Linearkombination der Ausgangsdaten darzustellen wie ihn zu berechnen. Daß eine solche Darstellung tatsächlich möglich ist, zeigt der erweiterte EUKLIDische Algorithmus, der diese Darstellung auch explizit liefert:

Ausgangspunkt ist wieder die Division mit Rest; die zugehörige Gleichung

$$r_{i-1} = q_i r_i + r_{i+1}$$

läßt sich umschreiben als

$$r_{i+1} = -q_i r_i + r_{i-1}\,,$$

so daß r_{i+1} eine ganzzahlige Linearkombination von r_i und r_{i-1} ist. Da entsprechend auch r_i Linearkombination von r_{i-1} und r_{i-2} ist, folgt induktiv, daß der ggT von a und b als ganzzahlige Linearkombination von $r_0 = a$ und $r_1 = b$ dargestellt werden kann.

Algorithmisch sieht dies folgendermaßen aus:

Schritt 0: Setze $r_0 = a$, $r_1 = b$, $\alpha_0 = \beta_1 = 1$ und $\alpha_1 = \beta_0 = 0$. Mit $i = 1$ ist dann

$$r_{i-1} = \alpha_{i-1} a + \beta_{i-1} b \quad \text{und} \quad r_i = \alpha_i a + \beta_i b\,.$$

Diese Relationen werden in jedem der folgenden Schritte erhalten:

Schritt i, $i \geq 1$**:** Falls $r_i = 0$ ist, endet der Algorithmus mit

$$\mathrm{ggT}(a, b) = r_{i-1} = \alpha_{i-1} a + \beta_{i-1} b\,.$$

Andernfalls dividiere man r_{i-1} mit Rest durch r_i mit dem Ergebnis

$$r_{i-1} = q_i r_i + r_{i+1}\,.$$

Dann ist

$$\begin{aligned} r_{i+1} = -q_i r_i + r_{i-1} &= -q_i(\alpha_i a + \beta_i b) + (\alpha_{i-1} a + \beta_{i-1} b) \\ &= (\alpha_{i-1} - q_i \alpha_i) a + (\beta_{i-1} - q_i \beta_i) b\,; \end{aligned}$$

man setze also

$$\alpha_{i+1} = \alpha_{i-1} - q_i \alpha_i \quad \text{und} \quad \beta_{i+1} = \beta_{i-1} - q_i \beta_i\,.$$

Genau wie oben folgt, daß der Algorithmus für alle natürlichen Zahlen a und b endet und daß am Ende der richtige ggT berechnet wird; außerdem sind die α_i und β_i so definiert, daß in jedem Schritt $r_i = \alpha_i a + \beta_i b$ ist, insbesondere ist also im letzten Schritt der ggT als Linearkombination der Ausgangszahlen dargestellt.

Als Beispiel wollen wir den ggT von 200 und 148 als Linearkombination darstellen. Im nullten Schritt haben wir 200 und 148 als die trivialen Linearkombinationen

$$200 = 1 \cdot 200 + 0 \cdot 148 \quad \text{und} \quad 148 = 0 \cdot 200 + 1 \cdot 148\,.$$

Im ersten Schritt dividieren wir, da 148 nicht verschwindet, 200 mit Rest durch 148:

$$200 = 1 \cdot 148 + 52 \Longrightarrow 52 = 1 \cdot 200 - 1 \cdot 148$$

Da auch $52 \neq 0$, dividieren wir im zweiten Schritt 148 durch 52 mit Ergebnis $148 = 2 \cdot 52 + 44$, d.h.

$$44 = 148 - 2 \cdot (1 \cdot 200 - 1 \cdot 148) = 3 \cdot 148 - 2 \cdot 200$$

Auch $44 \neq 0$, wir dividieren also weiter: $52 = 1 \cdot 44 + 8$ und

$$\begin{aligned} 8 &= 52 - 44 = (1 \cdot 200 - 1 \cdot 148) - (3 \cdot 148 - 2 \cdot 200) \\ &= 3 \cdot 200 - 4 \cdot 148\,. \end{aligned}$$

Im nächsten Schritt erhalten wir $44 = 5 \cdot 8 + 4$ und

$$\begin{aligned} 4 &= 44 - 5 \cdot 8 = (3 \cdot 148 - 2 \cdot 200) - 5 \cdot (3 \cdot 200 - 4 \cdot 148) \\ &= 23 \cdot 148 - 17 \cdot 200\,. \end{aligned}$$

Bei der Division von acht durch vier schließlich erhalten wir Divisionsrest Null; damit ist vier der ggT von 148 und 200 und kann in der angegebenen Weise linear kombiniert werden.

Der erweiterte EUKLIDische Algorithmus kann auch zur Lösung linearer diophantischer Gleichungen verwendet werden: Angenommen wir suchen ganzzahlige Lösungen (x, y) der linearen Gleichung

$$ax + by = c \quad \text{mit} \quad a, b, c \in \mathbb{Z}\,.$$

Da die linke Seite für alle x, y ein Vielfaches des ggT von a und b ist, kann es offensichtlich nur dann Lösungen geben, wenn $\mathrm{ggT}(a, b)$ ein Teiler von c ist. Falls dies gilt, können wir aus der linearen Darstellung

$$\mathrm{ggT}(a, b) = \alpha a + \beta b$$

durch Multiplikation mit $c/ggT(a, b)$ eine lineare Darstellung

$$c = xa + yb$$

konstruieren, also eine Lösung der Gleichung.

Dies ist allerdings nicht die einzige Lösung: Wegen $ba - ab = 0$ ist offensichtlich auch $(x+b, y-a)$ eine. Allgemeiner gilt $au+bv = 0$ auch für $u = b/gT(a, b)$ und $v = -a/ggT(a, b)$, und die allgemeine Lösung der Gleichung ist daher

$$\left(x + \frac{kb}{\mathrm{ggT}(a, b)},\ y - \frac{ka}{\mathrm{ggT}(a, b)}\right) \quad \text{mit} \quad k \in \mathbb{Z}\,.$$

Lineare diophantische Gleichungen mit mehr als zwei Unbekannten haben die Form

$$a_1 x_1 + \cdots + a_n x_n = c$$

mit ganzen Zahlen a_i, c; gesucht sind ganzzahlige Lösungen x_i. Auch eine solche Gleichung ist offensichtlich unlösbar, wenn der ggT der Koeffizienten a_i die rechte Seite nicht teilt. Wenn er sie teilt, können wir im wesentlichen wie im Fall zweier Veränderlichen vorgehen, indem wir zunächst den ggT als Linearkombination der a_i ausdrücken: Dazu berechnen wir zunächst den ggT d_2 von a_1 und a_2 und stellen diesen als Linearkombination von a_1 und a_2 dar. Sodann berechnen wir den ggT von d_2 und a_3; das ist gleichzeitig der ggT von a_1, a_2 und a_3. Wir stellen ihn als Linearkombination dieser Zahlen dar, indem wir ihn zunächst als Linearkombination von d_2 und a_3 schreiben und dann für d_2 die im vorigen Schritt berechnete Darstellung als Linearkombination von a_1 und a_2 einsetzen, und so weiter. Durch Multiplikation läßt sich aus dem Ergebnis eine Lösung der obigen Gleichung finden; weitere Lösungen erhält man durch Addition von Lösungen der homogenen Gleichung.

Löungen von Systemen linearer diophantischer Gleichungen findet man, indem man den GAUSS-Algorithmus ohne Divisionen anwendet: Möchte man aus einer Gleichung

$$a_{i1} x_1 + \cdots + a_{in} x_n = b_i \quad \text{mit} \quad a_{i1} \neq 0$$

die Variable x_1 eliminieren mittels der Gleichung

$$a_{j1} x_1 + \cdots + a_{jn} x_n = b_j \quad \text{mit} \quad a_{j1} \neq 0\,,$$

so subtrahiert man beim klassischen GAUSS-Algorithmus das a_{i1}/a_{j1}-fache dieser Gleichung von der Ausgangsgleichung, wodurch im allgemeinen Brüche ins Spiel kommen. Beim GAUSS-Algorithmus ohne

Divisionen bildet man stattdessen die Linearkombination a_{i1} mal zweite Gleichung minus a_{j1} mal erste Gleichung, in der x_1 ebenfalls nicht mehr vorkommt.

...

d) Der chinesische Restesatz

Hier geht es darum, eine ganze Zahl x zu finden derart, die modulo vorgegebener Zahlen $m_1, \ldots, m_r$ kongruent ebenfalls vorgegebener Zahlen $a_1, \ldots, a_r$ sind. Damit dieses Problem stets lösbar ist, werden die Zahlen $m_1, \ldots, m_r$ als paarweise teilerfremd vorausgesetzt.

Betrachten wir zunächst den Fall $r = 2$: Hier geht es darum, ein x zu finden mit

$$x \equiv a \bmod m \quad \text{und} \quad x \equiv b \bmod n$$

für zwei zueinander teilerfremde Zahlen m und n.

Da m und n teilerfremd sind, haben sie den ggT eins, der sich nach dem erweiterten EUKLIDischen Algorithmus als

$$1 = \alpha m + \beta n$$

schreiben läßt. 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

$$x = \beta n a + \alpha m b \equiv \begin{cases} a & \bmod m \\ b & \bmod n \end{cases}$$

das Problem.

Es ist natürlich nicht die einzige Lösung; wenn wir ein gemeinsames Vielfaches von m und n addieren, ändert sich nichts an den Kongruenzen. Da wir von teilerfremden Zahlen ausgegangen sind, ist das Produkt das kleinste gemeinsame Vielfache; die allgemeine Lösung ist somit

$$x + (\beta n + \lambda b)a + (\alpha m - \lambda a)b\,;$$

insbesondere ist die Lösung eindeutig modulo nm.

Bei mehr als zwei Kongruenzen geht man rekursiv vor: Man löst die ersten beiden Kongruenzen $x \equiv a_1 \bmod m_1$ und $x \equiv a_2 \bmod m_2$ wie

gerade besprochen; das Ergebnis ist eindeutig modulo $m_1 m_2$. Ist c_2 eine feste Lösung, so läßt sich die Lösung schreiben als Kongruenz

$$x \equiv c_2 \bmod m_1 m_2\,,$$

und da die m_i paarweise teilerfremd sind, ist auch $m_1 m_2$ teilerfremd zu m_3. Mit EUKLID können wir daher das System

$$x \equiv c_2 \bmod m_1 m_2 \quad \text{und} \quad x \equiv a_3 \bmod m_3$$

lösen und die Lösung schreiben als

$$x \equiv c_3 \bmod m_1 m_2 m_3$$

und so weiter, bis wir schließlich x modulo dem Produkt aller m_i kennen und somit das Problem gelöst haben.

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

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

zu lösen, berechnet man zunächst für jedes i das Produkt

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

der sämtlichen übrigen m_j und bestimmt dazu ganze Zahlen α_i, β_i, für die gilt $\alpha_i m_i + \beta_i \widehat{m}_i = 1$ Dann ist

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

Natürlich wird x hier – wie auch bei den obigen Formel – oft größer sein als das Produkt der m_i; um die kleinste Lösung zu finden, muß man 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 Reis.

§2: Der allgemeine Euklidische Algorithmus

Wenn wir uns den vorigen Paragraphen genau anschauen, sehen wir, daß von den vielen Eigenschaften der ganzen Zahlen vor allem eine wesentlich war: Die Division mit Rest. Division mit Rest gibt es beispielsweise auch für Polynome in einer Veränderlichen über einem Körper, so daß es möglich sein sollte, dieselben Algorithmen dafür zu formulieren. In der Tat spielt der EUKLIDische Algorithmus für Polynome in der Computeralgebra eine noch größere Rolle als der für Zahlen und wird uns im Rahmen dieser Vorlesung noch vielfach begegnen. Allerdings sind ganze Zahlen und Polynome erstens nicht die einzigen Beispiele, für die es einen EUKLIDischen Algorithmus gibt, und zweitens lassen sich viele Fragen simultan für beide Fälle klären, wenn wir den EUKLIDischen Algorithmus nur etwas abstrakter formulieren.

a) Grundbegriffe der Ringtheorie

Definition: *a)* Ein Ring ist eine Menge R zusammen mit zwei Rechenoperationen „+“ und „·“, so daß gilt:

1.) R bildet bezüglich „+“ eine abelsche Gruppe

2.) Die Verknüpfung „·“: $R \times R \to R$ erfüllt das Assoziativgesetz $x(yz) = (xy)z$ und es gibt ein Element $1 \in R$, so daß $1x = x1 = x$.

3.) „+“ und „·“ erfüllen die Distributivgesetze $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$..

b) Ein Ring heißt *kommutativ*, falls zusätzlich noch das Kommutativgesetz $xy = yx$ der Multiplikation erfüllt ist.

c) Ein Ring heißt *nullteilerfrei* wenn gilt: Falls ein Produkt $xy = 0$ verschwindet, muß mindestens einer der beiden Faktoren x, y gleich Null sein. Ein nullteilerfreier kommutativer Ring heißt *Integritätsbereich.*

d) Wir sagen, ein Element u eines Integritätsbereichs R sei *Teiler* von $x \in R$, in Zeichen $u|x$, wenn es ein $q \in R$ gibt, so daß $x = qu$.

e) $u \in R$ heißt *größter gemeinsamer Teiler* von x und y, wenn u Teiler von x und von y ist und wenn für jeden anderen gemeinsamen Teiler v von x und y gilt: $v|u$.

f) Ein Element $e \in R$ heißt *Einheit*, falls es ein $e' \in R$ gibt mit $ee' = 1$. Die Menge aller Einheiten von R bezeichnen wir mit $R^\times$.

g) Zwei Elemente $x, y \in R$ heißen assoziiert, wenn es eine Einheit $e \in R$ gibt, so daß $y = ex$.

Der Prototyp eines kommutativen Rings ist der Ring $\mathbb{Z}$ der ganzen Zahlen; er ist offensichtlich ein Integritätsbereich und seine einzigen Einheiten sind ± 1.

Der Menge aller $n \times n$-Matrizen über einem Körper ist ein Beispiel eines nichtkommutativen Rings. Er ist nicht nullteilerfrei, und seine Einheiten sind genau die invertierbaren Matrizen.

Auch die Polynome über einem Körper k bilden einen Ring, den Polynomring $k[X]$. Allgemeiner gilt sogar:

Lemma: Ist R ein Integritätsbereich, so auch der Polynomring

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; b \in \mathbb{N}_0, a_i \in R \right\} .$$

Seine Einheiten sind genau die Einheiten von R.

Beweis: Wenn wir Addition und Multiplikation nach den üblichen Regeln definieren, ist klar, daß $R[X]$ alle Ringaxiome erfüllt.

Um zu zeigen, daß $R[X]$ nullteilerfrei ist, betrachten wir zwei Polynome

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{und} \quad g = \sum_{j=0}^{m} b_j X^j ,$$

die beide von Null verschieden sind. Wir können etwa annehmen, daß n und m so gewählt sind, daß a_n und b_m beide nicht verschwinden.

Da R Integritätsbereich ist, kann dann auch das Produkt $a_n b_m$ nicht verschwinden, also ist der führende Term $a_n b_m X^{n+m}$ von fg von Null verschieden und damit auch fg selbst. Tatsächlich beweist dies sogar etwas mehr als die Nullteilerfreiheit, denn wir wissen nun, daß sich bei der Multiplikation zweier Polynome die Grade addieren.

Ist $f \in R[X]$ eine Einheit, so gibt es ein $g \in R[X]$ mit $fg = 1$; da das konstante Polynom 1 den Grad null hat, muß dasselbe auch für f und g gelten, d.h. $f, g \in R$ und damit in $R^\times$. ∎

Allgemein gilt:

Lemma: *a)* Die Menge $R^\times$ aller Einheiten von R ist eine abelsche Gruppe bezüglich der Multiplikation.

b) Ein kommutativer Ring R ist genau dann ein Integritätsbereich, wenn gilt: Ist $xz = yz$ für ein Element $z \neq 0$ und zwei beliebige Elemente x, y, so ist $x = y$.

c) Zwei Elemente x, y eines Integritätsbereich R sind genau dann assoziert, wenn $x|y$ und $y|x$.

d) Ein größter gemeinsamer Teiler, so er existiert, ist bis auf Assoziiertheit eindeutig bestimmt.

Beweis: a) Sind $e, f \in R$ Einheiten, so gibt es Elemente e', f' mit $ee' = ff' = 1$. Damit ist $(ef)(f'e') = e(ff')e' = ee' = 1$, d.h. auch ef ist eine Einheit. Außerdem ist jede Einheit invertierbar, denn offensichtlich ist e' ein multiplikatives Inverses zu e.

b) Ist R ein Integritätsbereich und $xz = yz$, so ist $(x - y)z = 0$; da $z \neq 0$ vorausgesetzt war, folgt $x - y = 0$, also $x = y$. Folgt umgekehrt aus $xz = yz$ und $z \neq 0$ stets $x = y$, so ist R nullteilerfrei, denn ist $xy = 0$ und $y \neq 0$, so ist $xy = 0y$, also $x = 0$.

c) Ist $y = ex$, so ist x ein Teiler von y. Da Einheiten invertierbar sind, ist auch $x = e^{-1}y$, d.h. $y|x$.

Ist umgekehrt $x|y$ und $y|x$, so gibt es Elemente q, r mit $x = qy$ und $y = rx$. Damit ist $1x = x = (qr)x$, also $qr = 1$. Somit ist q eine Einheit.

d) Sind u, v zwei größte gemeinsame Teiler von x, y, so ist nach Definition u Teiler von v und v Teiler von u, also sind u und v assoziiert. ∎

In Integritätsbereichen können wir somit einen Teilbarkeitsbegriff einführen, der den üblichen, von $\mathbb{Z}$ her gewohnten Regeln genügt. Manchmal können wir auch, wie in $\mathbb{Z}$, von einer eindeutigen Primzerlegung reden:

Definition: *a)* Ein Element x eines Integritätsbereichs R heißt *irreduzibel*, falls gilt: x ist keine Einheit, und ist $x = yz$ das Produkt zweier Elemente aus R, so muß y oder z eine Einheit sein.
b) Ein Integritätsbereich R heißt *faktoriell* oder *ZPE*-Ring, wenn gilt: Jedes Element $x \in R$ läßt sich bis auf Reihenfolge und Assoziiertheit eindeutig schreiben als Produkt $x = e\prod_{i=1}^{r} p_i^{s_i}$ mit einer Einheit $e \in R^\times$, irreduziblen Elementen $p_i \in R$ und natürlichen Zahlen s_i.
(*ZPE* steht für *Z*erlegung in *P*rimfaktoren *E*indeutig.)

Lemma: In einem faktoriellen Ring gibt es zu je zwei Elementen x, y einen größten gemeinsamen Teiler.

Beweis: Sind $x = u\prod_{i=1}^{r} p_i^{e_i}$ und $y = v\prod_{j=1}^{s} q_j^{f_j}$ mit $u, v \in R^\times$ und p_i, q_j irreduzibel die Zerlegungen von x und y in Primfaktoren, so können wir, indem wir nötigenfalls Exponenten Null einführen, o.B.d.A. annehmen, daß $r = s$ ist und $p_i = q_i$ für alle i. Dann ist offenbar $\prod_{i=1}^{r} p_i^{\min(e_i, f_i)}$ ein ggT von x und y, denn $z = \prod_{i=1}^{r} p_i^{g_i}$ ist genau dann Teiler von x, wenn $g_i \leq e_i$ für alle i, und Teiler von y, wenn $g_i \leq f_i$. ∎

b) Euklidische Ringe

EUKLIDische Ringe sind die Ringe, in denen es einen EUKLIDischen Algorithmus gibt. Wie wir gesehen haben, ist dazu die Division mit Rest das wichtigste Werkzeug, und wie sich in diesem Abschnitt herausstellen wird, brauchen wir kein weiteres. Wir definieren daher

Definition: Ein EUKLIDischer Ring ist ein Integritätsbereich R zusammen mit einer Abbildung $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$, so daß gilt: Ist $x|y$, so

ist $\nu(x) \leq \nu(y)$, und zu je zwei Elementen $x, y \in R$ gibt es Elemente $q, r \in R$ mit

$$x = qy + r \quad \text{und} \quad r = 0 \quad \text{oder} \quad \nu(r) < \nu(y)\,.$$

Wir schreiben auch $x : y = q$ Rest r und bezeichnen r als Divisionsrest bei der Division von x durch y.

Das Standardbeispiel ist natürlich der Ring $\mathbb{Z}$ der ganzen Zahlen mit $\nu(x) = |x|$. Ein anderes Beispiel ist der Polynomring $k[X]$ über einem Körper k: Hier können wir $\nu(f)$ für ein Polynom $f \neq 0$ als den Grad von f definieren; dann erfüllt auch die Polynomdivision mit Rest die Forderung an einen EUKLIDischen Ring.

Als letztes Beispiel schließlich kann sich der Leser überlegen, daß auch der Ring $\mathbb{Z}[i]$ der komplexen Zahlen mit ganzzahligen Real- und Imaginärteilen ein EUKLIDischer Ring ist; hier kann man $\nu(x+iy) = x^2 + y^2$ setzen.

Wie angekündigt, gilt

Lemma: In einem EUKLIDischen Ring R gibt es zu je zwei Elementen $x, y \in R$ einen ggT. Dieser kann nach dem EUKLIDischen Algorithmus berechnet werden und läßt sich als Linearkombination mit Koeffizienten aus R von x und y darstellen

Beweis: In jedem Integritätsbereich folgt aus der Gleichung $x = qy + r$ mit $x, y, q, r \in R$, daß die gemeinsamen Teiler von x und y gleich denen von y und r sind. Speziell in einem EUKLIDischen Ring können wir dabei r als Divisionsrest wählen und, wie beim klassischen EUKLIDischen Algorithmus, danach y durch r dividieren *usw.*, wobei wir eine Folge (r_i) von Divisionsresten erhalten mit der Eigenschaft, daß in jedem Schritt die gemeinsamen Teiler von x und y gleich denen von r_{i-1} und r_i sind. Außerdem ist stets entweder $r_i = 0$ oder $\nu(r_i) < \nu(r_{i-1})$, so daß die Folge nach endlich vielen Schritten mit einem $r_n = 0$ abbrechen muß. Auch hier sind die gemeinsamen Teiler von r_{n-1} und $r_n = 0$ genau die gemeinsamen Teiler von x und y. Da jede Zahl Teiler der Null ist, sind die gemeinsamen Teiler von r_{n-1} und Null aber genau die Teiler von r_{n-1}, und unter diesen gibt es natürlich einen größten, nämlich r_{n-1} selbst. Somit haben auch x und y einen größten gemeinsamen Teiler, nämlich den nach dem EUKLIDischen Algorithmus berechneten letzten von Null verschiedenen Divisionsrest r_{n-1}

Auch die lineare Kombinierbarkeit folgt wie im klassischen Fall: Bei jeder Division mit Rest ist der Divisionsrest als Linearkombination von Dividend und Divisor darstellbar; beim EUKLIDischen Algorithmus beginnen wir mit Dividend x und Divisor y, die natürlich beide als Linearkombinationen von x und y darstellbar sind, und induktiv folgt, daß auch alle folgenden Dividenden und Divisoren sind als Reste einer vorangegangenen Division Linearkombinationen von x und y sind, also ist es auch ihr Divisionsrest. Insbesondere ist auch der ggT als letzter nichtverschwindender Divisionsrest Linearkombination von x und y, und die Koeffizienten können wie im vorigen Paragraphen mit dem erweiterten EUKLIDischen Algorithmus berechnet werden. ∎

c) Eindeutige Primzerlegung in Euklidischen Ringen

Satz: Jeder EUKLIDische Ring ist faktoriell.

Beweis: Wir müssen zeigen, daß jedes Element $x \neq 0$ aus R bis auf Reihenfolge und Assoziiertheit eindeutig als Produkt aus einer Einheit und geeigneten Potenzen irreduzibler Elemente geschrieben werden kann. Wir beginnen damit, daß sich x überhaupt in dieser Weise darstellen läßt.

Dazu benutzen wir die Betragsfunktion $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$ des EUKLIDischen Rings R und beweisen induktiv, daß für $n \in \mathbb{N}_0$ alle $x \neq 0$ mit $\nu(x) \leq n$ in der gewünschten Weise darstellbar sind.

Ist $\nu(x) = 0$, so ist x eine Einheit: Bei der Division $1 : x = q$ Rest r ist nämlich entweder $r = 0$ oder aber $\nu(r) < \nu(x) = 0$. Letzteres ist nicht möglich, also ist $qx = 1$ und x eine Einheit. Diese kann als sich selbst mal dem leeren Produkt von Potenzen irreduzibler Elemente geschrieben werden.

Für $n > 1$ unterscheiden wir zwei Fälle: Ist x irreduzibel, so ist $x = x$ eine Darstellung der gewünschten Form, und wir sind fertig.

Andernfalls läßt sich $x = yz$ als Produkt zweier Elemente schreiben, die beide keine Einheiten sind. Da y und z Teiler von x sind, sind $\nu(y), \nu(z) \leq \nu(x)$. Wir wollen uns überlegen, daß sie tatsächlich sogar echt kleiner sind.

Dazu dividieren wir y mit Rest durch x; das Ergebnis sei q Rest r, d.h. $y = qx+r$ mit $r = 0$ oder $\nu(r) < \nu(x)$. Wäre $r = 0$, wäre y ein Vielfaches von x, es gäbe also ein $u \in R$ mit $y = ux = u(yz) = (uz)y$. Damit wäre $uz = 1$, also z eine Einheit, im Widerspruch zur Annahme. Somit ist $\nu(r) < \nu(x)$.

Weiter ist y ein Teiler von $r = y - qx = y(1 - qz)$, also folgt $\nu(y) \leq \nu(r) < \nu(x)$. Genauso folgt, daß auch $\nu(z) < \nu(x)$ ist.

Nach Induktionsvoraussetzung lassen sich daher y und z als Produkte von Einheiten und Potenzen irreduzibler Elemente schreiben, und damit läßt sich auch $x = yz$ so darstellen.

Als nächstes müssen wir uns überlegen, daß diese Darstellung bis auf Reihenfolge und Einheiten eindeutig ist. Das wesentliche Hilfsmittel hierzu ist die folgende Zwischenbehauptung:

Falls ein irreduzibles Element p ein Produkt xy teilt, teilt es mindestens einen der beiden Faktoren.

Zum *Beweis* betrachten wir den ggT von x und p. Dieser ist insbesondere ein Teiler von p, also bis auf Assoziiertheit entweder p oder 1. Im ersten Fall ist p Teiler von x und wir sind fertig; andernfalls können wir

$$1 = \alpha p + \beta x$$

als Linearkombination von p und x schreiben. Multiplikation mit y macht daraus $y = \alpha px + \beta xy$, und hier sind beide Summanden auf der rechten Seite durch p teilbar: Bei αpx ist das klar, und bei βxy folgt es daraus, daß nach Voraussetzung p ein Teiler von xy ist. Also ist p Teiler von y, und die Zwischenbehauptung ist bewiesen.

Induktiv folgt sofort:

Falls ein irreduzibles Element p ein Produkt $\prod_{i=1}^{r} x_i$ teilt, teilt es mindestens einen der Faktoren.

Um den Beweis des Satzes zu beenden, zeigen wir induktiv, daß für jedes $n \in \mathbb{N}_0$ alle Elemente mit $\nu(x) \leq n$ eine bis auf Reihenfolge und Einheiten eindeutige Primfaktorzerlegung haben.

Für $n = 0$ haben wir oben gesehen, daß x eine Einheit sein muß, und hier ist die Zerlegung $x = x$ eindeutig.

Seien nun

$$x = u \prod_{i=1}^{r} p_i^{e_i} = v \prod_{j=1}^{s} q_j^{f_j}$$

zwei Zerlegungen eines Elements $x \in R$, wobei wir annehmen können, daß alle $e_i, f_j \geq 1$ sind. Dann ist p_1 trivialerweise Teiler des ersten Produkts, also auch des zweiten. Wegen der Zwischenbehauptung teilt p_1 also mindestens eines der Elemente q_j, d.h. $p_1 = wq_j$ ist bis auf eine Einheit w gleich q_j. Da p_i keine Einheit ist, ist $\nu(x/p_i) < \nu(x)$; nach Induktionsannahme hat also $x/p_i = x/(wq_j)$ eine bis auf Reihenfolge und Einheiten eindeutige Zerlegung in irreduzible Elemente. Damit hat auch x diese Eigenschaft. ∎

Bemerkung: Die Umkehrung dieses Satzes gilt nicht: Wir werden gleich sehen, daß $\mathbb{Z}[X]$ oder auch Polynomringe in mehr als einer Veränderlichen über einem Körper faktoriell sind, aber keiner dieser Ringe ist EUKLIDisch, da sich weder der ggT 1 von 2 und X in $\mathbb{Z}[X]$ noch der ggT 1 von X und Y in $k[X, Y]$ als Linearkombination der Ausgangselemente schreiben läßt.

§3: Der Euklidische Algorithmus für Polynome

Aus dem vorigen Paragraphen wissen wir, daß der Polynomring über einem Körper EUKLIDisch ist, so daß auch dort größte gemeinsame Teiler existieren und nach dem EUKLIDischen Algorithmus berechnet werden können. Wir wollen uns zunächst überlegen, daß größte gemeinsame Teiler auch in Polynomringen in mehreren Veränderlichen über $\mathbb{Z}$ oder einem Körper existieren und dann sehen, wie man diese berechnen kann.

a) Der Satz von Gauß

Für einen beliebigen Integritätsbereich R ist der Polynomring $R[X]$ im allgemeinen nicht EUKLIDisch. Falls wir allerdings R in einen Körper K einbetten können, sind wir in einem EUKLIDischen Ring $K[X]$ und können dort den EUKLIDischen Algorithmus anwenden. Der Satz von GAUSS sagt uns, wie Faktorzerlegungen in $R[X]$ und in $K[X]$ miteinander zusammenhängen.

Zunächst brauchen wir einen geeigneten Kandidaten für einen Körper K, in den wir R einbetten können; dies ist der sogenannte *Quotientenkörper.* Seine Konstruktion ist völlig analog zur Konstruktion der rationalen Zahlen aus den ganzen Zahlen:

Wir betrachten für einen Integritätsbereich R auf der Menge aller Paare (r, s) mit $r, s \in R$ und $s \neq 0$ die Äquivalenzrelation

$$(r, s) \sim (u, v) \Longleftrightarrow rv = us\,;$$

die Äquivalenzklasse von (r, s) bezeichnen wir als den *Bruch* $\frac{r}{s}$.

Verknüpfungen zwischen diesen Brüchen werden nach den üblichen Regeln der Bruchrechnung definiert:

$$\frac{r}{s} + \frac{u}{v} = \frac{rv + us}{sv} \quad \text{und} \quad \frac{r}{s} \cdot \frac{u}{v} = \frac{ru}{sv}\,.$$

Dies ist wohldefiniert, denn sind $(r, s) \sim (r', s')$ und $(u, v) \sim (u', v')$, so ist

$$\frac{r'}{s'} + \frac{u'}{v'} = \frac{r'v' + u's'}{s'v'} \quad \text{und} \quad \frac{r'}{s'} \cdot \frac{u'}{v'} = \frac{r'u'}{s'v'}$$

und $rs' = r's$ sowie $uv' = u'v$. Damit ist auch

$$\begin{aligned}(r'v' + u's') \cdot sv &= r'v'sv + u's'sv = r'svv' + u'vss' \\ &= rs'vv' + uv'ss' = (rv + uy)s'v'\end{aligned}$$

und $(r'u')(sv) = r'su'v = rs'uv' = (ru)(s'v')$, 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 $r, s \neq 0$ ist $\frac{s}{r}$ ein multiplikatives Inverses zu $\frac{r}{s}$, da $(rs, rs) \sim (1, 1)$.

Identifizieren wir schließlich ein Element $r \in R$ mit dem Bruch $\frac{r}{1}$, 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 Integritätsbereich 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 ggT $I(f)$ der 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 Integritätsbereich. 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

$$fg = c_{n+m}X^{n+m} + c_{n+m-1}X^{n+m-1} + \ldots + c_1X + c_0\,;$$

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 vom Betrag größer eins. Dann gibt es auch ein irreduzibles Element p, das alle Koeffizienten c_r teilt.

Insbesondere ist p ein Teiler von $c_0 = a_0b_0$; da p irreduzibel ist, muß somit 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, ist nicht jeder Koeffizient a_i durch p teilbar; ν sei der kleinste Index, so daß a_ν kein Vielfaches von p ist. Da auch g primitiv ist, gibt es auch einen kleinsten Index μ, 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; für jeden anderen Summanden a_ib_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. ∎

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

Satz von Gauß: R sei ein Integritätsbereich 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. ∎

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 diesem Satz folgt induktiv sofort, daß dieselbe Aussage auf für Produkte von mehr als zwei Polynomen gilt. Damit folgt insbesondere

Satz: Der Polynomring über einem faktoriellen Ring R ist selbst 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*a)* 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 für Polynome in mehreren Veränderlichen über $\mathbb{Z}$ oder über einem Körper größte gemeinsame Teiler existieren. Der Rest des Paragraphen wird sich damit beschäftigen, wie wir diese effizient berechnen können.

Eine mögliche Strategie folgt aus den obigen Sätzen:

Ist R ein Integritätsbereich und sind $f, g \in R[X]$ zwei Polynome, so schreiben wir $f = I(f) \cdot f^*$ und $g = I(g) \cdot g^*$. Wegen der eindeutigen Primzerlegung in $R[X]$ ist

$$\mathrm{ggT}(f, g) = \mathrm{ggT}\big(I(f), I(g)\big) \cdot \mathrm{ggT}(f^*, g^*)\,.$$

Für den ersten Faktor müssen wir wissen, wie man den ggT in R ausrechnet; den zweiten Faktor können wir in $K[X]$ berechnen und dann durch seinen primitiven Anteil ersetzen, denn der ggT zweier primitiver Polynome ist als Teiler dieser Polynome insbesondere selbst primitiv.

b) Ein erstes Beispiel

Betrachten wir die beiden Polynome

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

und

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

aus $\mathbb{Z}[X]$. Offensichtlich sind beide primitiv, also ist auch ihr ggT primitiv. Wir berechnen ihn zunächst in $\mathbb{Q}[X]$, wo uns der EUKLIDische Algorithmus zur Verfügung steht:

Division von f durch g führt auf den Quotienten $X^2/3 - 2/9$ und Divisionsrest

$$r_2 = -\frac{5}{9}X^4 + \frac{1}{9}X^2 - \frac{1}{3}\,.$$

Division von g durch r_2 ergibt den Divisionsrest

$$r_3 = -\frac{117}{25}X^2 - 9X + \frac{441}{25}\,,$$

bei der Division von r_2 durch r_3 bleibt Rest

$$r_4 = \frac{233150}{6591}X - \frac{102500}{2197}\,,$$

und bei der letzten Division verbleibt als Rest der ggT

$$r_5 = \frac{1288744821}{543589225}\,.$$

Der primitive Anteil dieses „Polynoms“ ist Eins, also folgt

$$\mathrm{ggT}(f, g) = 1\,.$$

Leider folgte dies aber nur auf dem Umweg über sehr große Zwischenergebnisse. Wenn wir auch bei größeren Problemen noch effizient rechnen wollen, müssen wir einen Weg finden, um diese zu vermeiden.

Eine wichtige Beobachtung dazu ist folgende: Falls wir den EUKLIDischen Algorithmus statt über $\mathbb{Q}$ über einem endlichen Körper ausführen, kann es diese Explosion von Zwischenergebnissen nicht geben: Im Körper mit p Elementen wird jedes Element reprässentiert durch eine Zahl zwischen Null und $p-1$, und das gilt selbstverständlich auch für alle Zwischenergebnisse.

Hätten wir im obigen Beispiel etwa im Körper mit elf Elementen gerechnet, so wäre dort

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

und

$$g = 3X^6 + 5X^4 + 7X^2 + 2X + 10\,.$$

Division von f durch g führt auf den Quotienten $4X^2 + 1$ und Divisionsrest

$$r_2 = 8X^4 + 5X^2 + 7\,.$$

Division von g durch r_2 ergibt den Divisionsrest

$$r_3 = 5X^2 + 2X + 4\,,$$

bei der Division von r_2 durch r_3 bleibt Rest

$$r_4 = 10X + 10\,,$$

und bei der letzten Division verbleibt als Rest der ggT

$$r_5 = 7\,,$$

der in $\mathbb{F}_{11}$ natürlich eine Einheit ist, so daß die beiden Polynome auch dort teilerfremd sind.

Eine der beiden gebräuchlichen Strategien zur Berechnung des größten gemeinsamen Teilers zweier Polynome mit ganzzahligen Koeffizienten führt über den EUKLIDischen Algorithmus über endlichen Körpern, die andere (für die wir im Rahmen dieser Vorlesung keine Zeit haben) arbeitet mit sogenannten Subresultanten. Beide Methoden habe dieselbe asymptotische Laufzeit; die tatsächliche Laufzeit ist allerdings meist bei der modularen Methode deutlich besser als bei den Subresultantenalgorithmen.

c) Allgemeines zum Rechnen mit homomorphen Bildern

Modulare Methoden sind ein Spezialfall des Rechnens mit homomorphen Bildern, das wir in einem etwas anderen Zusammenhang auch später zur Bestimmung des ggTs zweier Polynome in mehreren Veränderlichen verwenden werden. Es lohnt sich daher, das Problem gleich abstrakt algebraisch zu formulieren:

Definition: *a)* Ein Homomorphismus $\varphi\colon R \to S$ von Ringen ist eine Abbildung, für die gilt

$$\varphi(r+s) = \varphi(r) + \varphi(s) \quad \text{und} \quad \varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$$

für alle $r, s \in \mathbb{R}$.
b) Der *Kern* eines Homomorphismus $\varphi\colon R \to S$ von Ringen ist die Menge aller $r \in R$ mit $\varphi(r) = 0$.
c) Eine Teilmenge $I \subseteq R$ heißt *Ideal* von R, in Zeichen $I \lhd R$, wenn gilt:
1.) I ist eine additive Untergruppe von R
2.) Für $r \in R$ und $s \in I$ ist auch rs ein Element von I.
d) Die Menge $(a) = \{ra | r \in R\}$ aller Vielfachen eines Elements $a \in R$ heißt das von a erzeugte *Hauptideal*.

Bei der modularen Berechnung des ggT verwenden wir für geeignete Primzahlen p den Homomorphismus

$$\varphi_p\colon \begin{cases} \mathbb{Z} \to \mathbb{F}_p \\ x \mapsto x \bmod p \end{cases};$$

sein Kern ist offensichtlich das von p erzeugte Hauptideal. Später werden wir oft auch *Einsetzungsmorphismen* betrachten, die ein Polynom an einer vorgegebenen Stelle auswerten: Für ein festes Element $a \in R$ eines Integritätsbereichs R betrachten wir hier den Homomorphismus

$$\varphi_a\colon \begin{cases} R[X] \to R \\ f \mapsto f(a) \end{cases}.$$

Sein Kern besteht aus allen Polynomen, die an der Stelle a verschwinden; das ist offenbar gerade das von $X - a$ erzeugte Hauptideal.

Es ist kein Zufall, daß es sich in beiden Fällen um Hauptideale handelt, denn allgemein gilt

Lemma: Jedes Ideal eines EUKLIDischen Rings ist ein Hauptideal.

Beweis: Das Nullideal ist ein Hauptideal, und für jedes andere Ideal I betrachten wir die Menge

$$M = \left\{ \nu(r) \;\middle|\; r \in I \setminus \{0\} \right\}.$$

Diese hat als Teilmenge von $\mathbb{N}_0$ ein minimales Element m; wir wählen ein $a \in I$ mit $\nu(a) = m$.

Für jedes Element $x \in I$ können wir x mit Rest durch a dividieren; das Ergebnis sei q Rest r. Falls $r = 0$ liegt $x = qa$ in (a); andernfalls ist $\nu(r) < \nu(a)$. Letzteres ist aber nicht möglich, denn $r = x - qa$ liegt in I, so daß $\nu(r) \geq \nu(a)$ sein müßte. Somit ist $I = (a)$. ∎

Ideale spielen bei Ringen genau dieselbe Rolle wie Normalteiler bei Gruppen, d.h. es gilt:

Lemma: Zu einem Ring R und einer Teilmenge $I \subseteq R$ gibt es genau dann einen Homomorphismus $\varphi\colon R \to S$ mit Kern I, wenn I ein Ideal von R ist.

Beweis: Ist I Kern des Homomorphismus $\varphi\colon R \to S$, so ist I natürlich eine additive Untergruppe von R, da φ insbesondere auch ein Gruppenhomomorphismus ist. Für $r \in R$ und $s \in I$ ist $\varphi(s) = 0$, also auch $\varphi(rs) = \varphi(r)\varphi(s) = 0$. Somit ist I ein Ideal.

Ist umgekehrt I ein Ideal von R, so können wir auf R eine Äquivalenzrelation definieren durch $r \sim s$ genau dann, wenn $r - s \in I$. Die Äquivalenzklasse von r bezeichnen wir mit $\overline{r}$, die Menge aller Äquivalenzklassen mit $\overline{R} = R/I$.

Für $r, r', s, s' \in R$ mit $r \sim r'$ und $s \sim s'$ liegt mit $r - r'$ und $s - s'$ auch $r + s - r' - s'$ in I, d.h. $\overline{r+s} = \overline{r} + \overline{s}$. Genauso ist auch $\overline{r \cdot s} = \overline{r} \cdot \overline{s}$, denn ist $r' = r + i$ und $s' = s + j$ mit $i, j \in I$, so ist

$$r' \cdot s' = (r + i)(s + j) = rs + is + rj + ij\,,$$

und wegen der Idealeigenschaft von i liegen rs, is und rj allesamt in I. Somit ist $\overline{R}$ ein Ring, und die Abbildung $\varphi\colon R \to \overline{R}$, die jedes $r \in R$ auf seine Äquivalenzklasse $\overline{r}$ in $\overline{R}$ abbildet, ist ein Homomorphismus, dessen Kern natürlich I ist. ∎

Die Ideale haben ihren Namen von KUMMER, der sie als *ideale Zahlen* betrachtete: KUMMER glaubte zunächst, er habe einen Beweis der FERMAT-Vermutung gefunden, allerdings war er davon ausgegangen, daß der Ring $\mathbb{Z}[\zeta_p]$, wobei p eine primitive p-te Einheitswurzel bezeichnet, faktoriell ist. Dies ist zwar für unendlich viele Primzahlen p der Fall, aber eben nicht für alle. KUMMER konnte aber zeigen, daß es auf dem Niveau der Ideale eine eindeutige Primzerlegung gibt – nur reichte das leider nicht aus, um seinen Beweis auch für die Primzahlen zu retten für die $\mathbb{Z}[\zeta_p]$ nicht faktoriell ist.

Natürlich definiert jeder Homomorphismus $\varphi\colon R \to S$ einen Homomorphismus

$$\varphi\colon \begin{cases} R[X] \to S[X] \\ a_n X^n + \cdots + a_0 \mapsto \varphi(a_n) X^n + \cdots + \varphi(a_0) \end{cases}$$

zwischen den Polynomringen darüber; die Grundidee beim Rechnen mit homomorphen Bildern besteht darin, ein Problem für Polynome über S auf das entsprechende Problem über S zurückzuführen.

d) Zusammenhang zwischen ggT und modularem ggT

Wir gehen aus von zwei Polynomen

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

und

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

mit Koeffizienten aus R und wollen die Berechnung des ggT von f und g zurückführen auf die des ggT von $\varphi(f)$ und $\varphi(g)$. Um zu sehen, was dabei zu beachten ist, betrachten wir einen Teiler

$$h = c_r X^r + c_{r-1} X^{r-1} + \cdots + c_1 X + c_0$$

von f und g. Dazu gibt es Kofaktoren $F, G \in R[X]$, für die $f = hF$ und $g = hG$ ist; da φ auch auf dem Niveau der Polynomringe ein Homomorphismus ist, folgt

$$\varphi(f) = \varphi(h)\varphi(F) \quad \text{und} \quad \varphi(g) = \varphi(h)\varphi(G)\,.$$

Damit ist also auch $\varphi(h)$ ein gemeinsamer Teiler von $\varphi(f)$ und $\varphi(g)$.

Falls der führende Koeffizient von h im Kern von φ liegt (und nur dann) ist allerdings der Grad von $\varphi(h)$ kleiner als der von h. Als Beispiel dazu können wir die beiden Polynome $p = 3X^6 + 3X^5 + X + 1$ und $q = 3X^6 - 3X^5 + X - 1$ betrachten. Hier ist

$$p : q = 1 \quad \text{Rest } 6X^5 + 2$$

und

$$q : (6X^5 + 2) = \frac{X}{2} - \frac{1}{2} \quad \text{Rest } 0\,,$$

also ist das primitive Polynom $h = 3X^5 + 1$ zu $6X^5 + 2$ ein ggT von p und q in $\mathbb{Z}[X]$. Die Polynome $p \bmod 3 = X + 1$ und $q \bmod 3 = X - 1$ sind aber teilerfremd, und natürlich ist auch $h \bmod 3 = 1$.

Andererseits kann es auch gemeinsame Teiler von $\varphi(f)$ und $\varphi(g)$ geben, die nicht von einem gemeinsamen Teiler von f und g kommen. Für die im vorigen Paragraphen betrachteten Polynome f und g passiert dies beispielsweise modulo sieben: Dort ist

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

und

$$g = 3X^6 + 5X^4 + 3X^2 + 5X\,.$$

Division von f durch g in $\mathbb{F}_7[X]$ führt auf den Divisionsrest

$$r_2 = X^4 + 4X^2 + 2\,,$$

Division von g durch r_2 ergibt den Divisionsrest

$$r_3 = 4X^2 + 5X\,,$$

und bei der Division von r_2 durch r_3 bleibt Rest

$$r_4 = 3X + 2\,,$$

was über $\mathbb{F}_7$ ein Teiler von r_3 ist. Somit ist hier der ggT gleich dem linearen Polynom $3X + 2$, während f und g in $\mathbb{Z}[X]$ teilerfremd sind.

Das erste Problem, daß der ggT von $\varphi(f)$ und $\varphi(g)$ kleineren Grad hat als der von f und g, läßt sich leicht vermeiden: Liegt nämlich der

führende Koeffizient von $h = \text{ggT}(f, g)$ im Kern von φ, so müssen auch die führenden Koeffizienten von f und g dort liegen; denn der führende Koeffizient eines Vielfachen von h muß ein Vielfaches des führenden Koeffizienten von h sein. Um dieses Problem zu vermeiden, müssen wir somit einfach alle Homomorphismen ausschließen, die die führenden Koeffizienten von f und g auf Null abbilden. Falls wir als Homomorphismen die Abbildungen $\varphi_p\colon \mathbb{Z} \to \mathbb{F}_p$ verwenden, müssen wir also alle Primzahlen vermeiden, die beide führende Koeffizienten teilen.

Schwieriger ist es mit dem Problem, daß der ggT von $\varphi(f)$ und $\varphi(g)$ größeren Grad haben kann als der von f und g. Um dieses Problem in den Griff zu bekommen, müssen wir zunächst untersuchen, wann zwei Polynome über einem Körper überhaupt einen (nichtkonstanten) gemeinsamen Teiler haben.

e) Die Resultante

Wir gehen aus von einem faktoriellen Ring R mit Quotientenkörper K und zwei Polynomen

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

und

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

aus $R[X]$. Ist $h \in R[X]$ ein Polynom positiven Grades, das sowohl f als auch g teilt, ist

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

ein gemeinsames Vielfaches von f und q, dessen Grad

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

echt kleiner ist als $\deg f + \deg g = n + m$.

Haben umgekehrt f und g ein gemeinsames Vielfaches, dessen Grad kleiner ist als $n + m$, so hat auch ihr kleinstes gemeinsames Vielfaches p einen kleineren Grad als $n + m$. (Ein kleinstes gemeinsames Vielfaches existiert, da wir in Abschnitt *a)* gesehen haben, daß mit R auch $R[X]$ faktoriell ist.)

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

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

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

Lemma: Zwei Polynome $f, g \in R[X]$ haben genau dann einen gemeinsamen Teiler positiven Grades, wenn es nichtverschwindende Polynome $u, v \in R[X]$ gibt mit $\deg u < \deg g$ und $\deg v < \deg f$, so daß $uf = vg$ ist. ∎

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

$$u = u_{m-1}X^{m-1} + u_{m-2}X^{m-2} + \ldots + u_1X + u_0$$

und

$$v = v_{n-1}X^{n-1} + v_{n-2}X^{n-2} + \ldots + v_1X + v_0\,,$$

und im Polynom uf hat die Potenz X^r den Koeffizienten

$$\sum_{i,j \text{ mit } i+j=r} a_i u_j\,,$$

während sie im Polynom vg den Koeffizienten

$$\sum_{i,j \text{ mit } i+j=r} b_i v_j$$

hat. f und g haben daher genau dann einen gemeinsamen Teiler positiven Grades, wenn es nicht allesamt verschwindende Körperelemente $u_0, \ldots, u_{m-1}$ und $v_0, \ldots, v_{n-1}$ gibt, so daß

$$\sum_{i,j \text{ mit } i+j=r} a_i u_j - \sum_{i,j \text{ mit } i+j=r} b_i v_j = 0 \qquad \text{für } r = 0, \ldots, n+m-1$$

ist. Dies ist ein homogenes lineares Gleichungssystem aus $n + m$ Gleichungen für die $n + m$ Unbekannten $u_0, \ldots, u_{m-1}$ und $v_0, \ldots, v_{n-1}$; es

hat genau dann eine nichttriviale Lösung, falls seine Matrix singulär ist, falls also deren Determinante verschwindet.

Ausgeschrieben wird dieses Gleichungssystem, wenn wir mit dem Koeffizienten von X^{m+n-1} anfangen, zu

$$\begin{gathered}
a_n u_{m-1} - b_m v_{n-1} = 0 \\
a_{n-1}u_{m-1} + a_n u_{m-2} - b_{m-1}v_{n-1} - b_m v_{n-2} = 0 \\
a_{n-2}u_{m-1} + a_{n-1}u_{m-2} + a_n u_{m-3} - b_{m-2}v_{n-1} - b_{m-1}v_{n-2} b_m v_{n-3} = 0 \\
\ldots \\
a_0u_2 + a_1u_1 + a_2u_0 - b_0v_2 - b_1v_1 - b_2v_0 = 0 \\
a_0u_1 + a_1u_0 - b_0v_1 - b_1v_0 = 0 \\
a_0u_0 - b_0v_0 = 0
\end{gathered}$$

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 Determinante

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

Die Matrix dazu bezeichnet man als SYLVESTER-Matrix, ihre Determinante als *Resultante* $\operatorname{Res}(f, g)$ 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 Resultante ist offensichtlich ein Polynom in den a_i und den b_j, das genau dann verschwindet, wenn f und g einen gemeinsamen Faktor haben.

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 Rücksichtauf 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 auch heute noch mit die wichtigste mathematische Zeitschrift Amerikas ist.

f) Die Landau-Mignotte-Schranke

$f \in \mathbb{Z}[X]$ sei 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 zunächst jedem Polynom

$$f = \sum_{k=0}^{d} a_k X^k$$

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 wird es sich als nützlich erweisen, zunächst Polynome mit beliebigen *komplexen* Koeffizienten zu betrachtet; für diese können wir genau wie oben ihre Höhe definieren. Zusätzlich werden 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 Größe 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 liefern die sogenannten *elementarsymmetrische* Funktionen $\psi_k(z_1, \ldots, z_n)$, die definiert sind als Summe Summe aller möglicher Produkte von k Werten z_j mit verschiedenen Indizes.

Wurzelsatz von Viète: Hat das Polynom $\sum_{k=0}^{d} a_k X^k$ die Nullstellen $z_1, \ldots, z_d$, so ist $a_k = (-1)^{d-k} a_d \psi_k(z_1, \ldots, z_n)$, wobei $\psi_k(z_1, \ldots, z_n)$.

(Die Funktionen ψ_k bezeichnet man in der Algebra als *elementarsymmetrische Funktionen;* man kann zeigen, daß sich jedes in n Variablen symmetrische Polynom als Polynom in diesen elementarsymmetrischen Funktionen schreiben läßt.)

Der *Beweis* des Satzes von VIEÈTE ist fast trivial: Man muß einfach $\prod_{j=1}^{d}(X - z_j)$ ausmultiplizieren. Dabei entstehen 2^d Summanden, die jeweils Produkte von d Faktoren sind: Aus jedem der Faktoren $(X - z_j)$ wird entweder das X genommen oder $(-z_j)$. Die Summanden, in denen X in der k-ten Potenz steht, haben somit $n - k$ Faktoren der Form $(-z_j)$, d.h. insgesamt steht im Produkt vor X^k der Term $(-1)^{n-k}\psi_{n-k}(z_1, \ldots, z_n)$. ∎

(Ohne Beweis sei an den *Fundamentalsatz der Algebra* erinnert, wonach sich jedes Polynom über den komplexen Zahlen als Produkt von Linearfaktoren schreiben läßt.)

FRANÇOIS VIÈTE (1540–1603) . . .

Um die Koeffizienten eines Polynoms durch die Nullstellen abschätzen zu können, brauchen wir 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:

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

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:

$$a_k = (-1)^k a_d\, \psi_k(z_1, \ldots, z_d)$$

ist eine Summe von Termen, von denen jeder einzelne höchstens den Betrag $\mu(f)$ hat. Die Anzahl dieser Terme 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

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

∎

Um umgekehrt das Maß durch eine Norm abschätzen zu können, 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 $f = \sum_{k=0}^{d} X^d$.

Dann ist $(X - z)f = a_d X^{d+1} + \sum_{k=1}^{d} (za_k - a_{k-1})X^k - a_0 z$ und

$\|(X - z)f\|_2^2$ als Summe aller Koeffizientenquadrate errechnet sich zu

$$a_d\,\overline{a_d} + \sum_{k=1}^{d} (za_k - a_{k-1})\,\overline{(za_k - a_{k-1})} + a_0\overline{a_0}$$

$$= |a_d|^2 + \sum_{k=1}^{d} \left(|a_k|^2 |z|^2 - 2\,\mathfrak{Re}(za_k\overline{a_{k-1}}) + \left|a_{k-1}\right|^2 \right) + |a_0|^2$$

$$= (1 + |z|^2) \sum_{k=0}^{d} |a_k|^2 - 2 \sum_{k=1}^{d} \mathfrak{Re}(za_k\overline{a}_{k-1})\,.$$

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 $\|(\overline{z}X - 1)f\|_2^2$ wird zu

$$a_d\overline{z} \cdot \overline{a_d} z + \sum_{k=1}^{d} (\overline{z}a_{k-1} - a_k)(z\overline{a_{k-1}} - \overline{a_k}) + a_0\overline{a_0}$$

$$= |za_d|^2 + \sum_{k=1}^{d} \left(\left|za_{k-1}\right|^2 - 2\,\mathfrak{Re}(za_k\overline{a_{k-1}}) + |a_k|^2 \right) + |a_0|^2$$

$$= (1 + |z|^2) \sum_{k=0}^{d} |a_k|^2 - 2 \sum_{k=1}^{d} \mathfrak{Re}(za_k\overline{a}_{k-1})\,.$$

Also stimmen die beiden Normen überein. ∎

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

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

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 boykotierten seine Vorlesungen, da sie meinten, sie könnten Mathematik nur von einem Professor ihrer eigenen Rasse 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.

g) Die modulare Berechnung des ggT

Der Algorithmus zur modularen Berechnung des ggT zweier Polynome $f, g \in \mathbb{Z}[X]$ mit ganzzahligen Koeffizienten geht nun folgendermaßen:

1. Schritt: Berechne die LANDAU-MIGNOTTE-Schranke $\mathrm{LM}(f,g)$ und setze $M = 2\,\mathrm{LM}(f,g) + 1$. Außerdem wird $\mathcal{P} = \emptyset$ gesetzt, d.h. die Menge der bereits betrachteten Primzahlen ist noch leer.

Da der Betrag eines jeden Koeffizienten des ggT höchstens gleich $\mathrm{LM}(f,g)$ 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 weder den führenden Koeffizienten von f noch den von g teilt, und berechne in $\mathbb{F}_p[X]$ den ggT 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 $h \in \mathbb{Z}[X]$ sei ein Polynom, dessen Reduktion modulo p gleich dem in $\mathbb{F}_p[X]$ berechneten ggT ist. Außerdem ersetze man $\mathcal{P}$ durch $\mathcal{P} \cup \{p\}$.

(Die Zahl N soll jeweils so gewählt werden, daß wir in jeder Phase des Algorithmus die Koeffizienten des ggT modulo N kennen oder zumindest zu kennen glauben. $N = 1$ bedeutet, daß wir nichts darüber wissen und uns dessen auch bewußt sind.)

3. Schritt: Falls $N \geq M$ ist, ändere man die Koeffizienten von h modulo N nötigenfalls so ab, daß ihre Beträge höchstens gleich LM(f, g) sind. Falls das nicht möglich ist, 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 geht es ebenfalls zurück zum zweiten Schritt.

4. Schritt: Im Fall $N < M$ wähle man eine zufällige Primzahl $p \notin \mathcal{P}$, die weder den führenden Koeffizienten von f noch den von g teilt, ersetze $\mathcal{P}$ durch $\mathcal{P} \cup \{p\}$ und berechne in $\mathbb{F}_p[X]$ den ggT von f mod p und g mod p. Falls dieser gleich eins ist, endet der Algorithmus und ggT$(f, g) = 1$. Falls sein Grad größer als der von h ist, wiederhole man den vierten Schritt, falls er kleiner ist, setze man $N = p$ und $\mathcal{P} = \{p\}$; alsdann geht es weiter mit dem dritten Schritt. Sind schließlich die beiden Grade gleich, so konstruiere man nach dem chinesischen Restesatz ein Polynom, das modulo N gleich h ist und modulo p gleich dem gerade berechneten ggT. N wird ersetzt durch Np, und es geht 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 ggT(f, g) modulo p ist, und nach endlich vielen Durchläufen sind genügend viele davon zusammengekommen, daß ihr Produkt die Zahl M übersteigt. Da der ggT in $\mathbb{F}_p[X]$ für Primzahlen, die keinen der führenden Koeffizienten teilen, höchstens höheren Grad als ggT(f, g) haben kann, ist auch klar, daß der Algorithmus mit einem korrekten Ergebnis abbricht.

h) Die Berechnung der Resultante

Angenommen, wir wollen die Resultante zweier Polynome der Grade dreißig und vierzig bestimmen. Das ist die Determinante einer 70×70-Matrix, und eine solche Determinante hat nach LAGRANGE 70! Summanden; das sind geringfügig mehr als 10^{100}. So viele Rechenoperationen sind weit jenseits der Möglichkeiten selbst der besten heutigen Supercomputer.

Tatsächlich verwendet natürlich niemand den Entwicklungssatz von LAGRANGE um eine Determinante zu berechnen – außer vielleicht bei

einigen kleineren Spielzeugdeterminanten in Mathematikklausuren. In allen anderen Fällen wird man die Matrix durch Zeilen- und/oder Spaltenoperationen auf Dreiecksform bringen und dann die Determinante einfach als Produkt der Diagonaleinträge berechnen. Das dauert für die SYLVESTER-Matrix zweier Polynome der Grade dreißig und vierzig auf heutigen Computern weniger als eine halbe Minute.

Stellt man allerdings keine Matrix auf, sondern verlangt von einem Computeralgebrasystem einfach, daß es die Resultante der beiden Polynome berechnen soll, hat man das Ergebnis nach weniger als einem Zehntel der Zeit. Einer der Schlüssel dazu ist wieder der EUKLIDische Algorithmus.

Angenommen, wir haben zwei Polynome f, g in einer Variablen X über einem Körper k:

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad \text{und}$$
$$g = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0 \quad \text{mit} \quad n \leq m\,.$$

Falls $f = a_0$ konstant ist, also $n = 0$, gibt es in der SYLVESTER-Matrix null Zeilen aus Koeffizienten von g und m Zeilen aus Koeffizienten von f; die Matrix ist also einfach a_0 mal der $m \times m$-Einheitsmatrix und die Resultante als ihre Determinante ist a_0^m.

Andernfalls dividieren wir g durch f und erhalten einen Rest h:

$$g : f = q \text{ Rest } h \quad \text{oder} \quad h = g - qf\,.$$

Der zentrale Punkt beim EUKLIDischen Algorithmus ist, daß die gemeinsamen Teiler von f und g genau dieselben sind wie die von f und h. Insbesondere haben also f und g genau dann einen gemeinsamen Teiler von positivem Grad, wenn f und h einen haben, d.h. $\mathrm{Res}_x(f, g)$ verschwindet genau dann, wenn $\mathrm{Res}_x(f, h)$ verschwindet. Damit sollte es also einen Zusammenhang zwischen den beiden Resultanten geben, und den können wir zur Berechnung von $\mathrm{Res}_x(f, g)$ ausnützen, denn natürlich ist $\mathrm{Res}_x(f, h)$ kleiner und einfacher als $\mathrm{Res}_x(f, g)$.

Überlegen wir uns, was bei der Polynomdivision mit den Koeffizienten passiert.

Wir berechnen eine Folge von Polynomen $g_0 = g, g_1, \ldots, g_r = h$, wobei g_i aus seinem Vorgänger dadurch entsteht, daß wir ein Vielfaches von $X^j f$ subtrahieren, wobei $j = \deg g_i - \deg f$ ist. Der maximale Wert, den j annehmen kann, ist offenbar $\deg g - \deg f = m - n$.

Die Zeilen der SYLVESTER-Matrix sind Vektoren in k^{n+m}; die ersten m sind die Koeffizientenvektoren von $X^{m-1}f, \ldots, Xf, f$, danach folgen die von $X^{n-1}g, \ldots, Xg, g$.

Im ersten Divisionschritt subtrahieren wir von g ein Vielfaches $\lambda X^j f$ mit $j = m - n$; damit subtrahieren wir auch von jeder Potenz $X^i g$ das Polynom $\lambda X^{i+j} f$. Für $0 \le i < n$ und $0 \le j \le m+n$ ist $0 \le i+j < m$, was wir subtrahieren entspricht auf dem Niveau der Koeffizientenvektoren also stets einem Vielfachen einer Zeile der SYLVESTER-Matrix. Damit ändert sich nichts am Wert der Determinanten, wenn wir den Koeffizientenvektor von g nacheinander durch den von $g_1, \ldots, g_r = h$ ersetzen.

Die Resultante ändert sich also nicht, wenn man in der SYLVESTER-Matrix entsteht jede Zeile mit Koeffizienten von g ersetzt durch die entsprechende Zeilen mit Koeffizientenvon h, wobei h als ein Polynom vom Grad m behandelt wird, dessen führende Koeffizienten verschwinden. Ist $h = c_s x^s + \cdots + c_0$, so ist also $\mathrm{Res}_x(f, g)$ gleich

$$\begin{vmatrix}
a_n & a_{n-1} & a_{n-2} & \ldots & a_1 & a_0 & 0 & 0 & \ldots & 0 \\
0 & a_n & a_{n-1} & \ldots & a_2 & a_1 & a_0 & 0 & \ldots & 0 \\
0 & 0 & a_n & \ldots & a_3 & a_2 & a_1 & a_0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \ldots & a_0 \\
c_m & c_{m-1} & c_{m-2} & \ldots & c_2 & c_1 & c_0 & 0 & \ldots & 0 \\
0 & c_m & c_{m-1} & \ldots & c_3 & c_2 & c_1 & c_0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & 0 & c_m & c_{m-1} & c_{m-2} & \ldots & c_0
\end{vmatrix},$$

wobei die Koeffizienten $c_m, \ldots, c_{s+1}$ alle verschwinden.

Somit beginnt im unteren Teil der Matrix jede Zeile mit $m - s$ Nullen.

In den ersten $m-s$ Spalten der Matrix stehen daher nur noch Koeffizienten von f: In der ersten ist dies ausschließlich der führende Koeffizient a_n von f in der ersten Zeile. Entwickeln wir nach der ersten Zeile, können wir also einfach die erste Zeile und die erste Zeile streichen; die Determinante ist dann a_n mal der Determinante der übrigbleibenden Matrix. Diese hat (falls $m > s + 1$) wieder dieselbe Gestalt, wir können also wieder einen Faktor a_n ausklammern und bekommen eine Determinante mit einer Zeile und einer Spalte weniger *uws.;* das Ganze funktioniert $m - s$ mal, dann ist der führende Koeffizient von h in die erste Spalte gerutscht und die übriggebliebene Matrix ist die Sylvestermatrix von f und h – falls etwas übrigbleibt.

Offensichtlich bleibt genau dann nichts übrig, wenn h das Nullpolynom ist: Dann sind die unteren m Zeilen Null, d.h. die Resultante verschwindet.

Andernfalls ist

$$\mathrm{Res}_x(f, g) = a_n^{m-s} \mathrm{Res}_x(f, h),$$

und da diese Formel auch für $h = 0$ gilt, haben wir gezeigt

Lemma: Hat f keinen größeren Grad als g und ist h der Divisionsrest von g durch f, der den Grad s habe, so ist $\mathrm{Res}(f, g) = a_n^{m-s} \mathrm{Res}(f, h)$. ∎

Dies läßt sich nun nach Art des EUKLIDischen Algorithmus iterieren: Berechnen wir wie dort die Folge der Reste $r_1 = h$ der Division von g durch f und dann (mit $r_0 = g$) weiter r_{i+1} gleich dem Rest bei der Division von r_i durch r_{i-1}, so können wie die Berechnung von $\mathrm{Res}_x(f, g)$ durch Multiplikation mit Potenzen der führenden Koeffizienten der Divisoren zurückführen auf die viel kleineren Resultanten $\mathrm{Res}_x(r_i, r_{i+1})$. Sobald r_{i+1} eine Konstante ist, egal ob Null oder nicht, haben wir eine explizite Formel und der Algorithmus endet. Für den Fall, daß f größeren Grad als g hat brauchen wir noch

Lemma: Für ein Polynom, f vom Grad n und ein Polynom g vom Grad n ist $\mathrm{Res}(f, g) = (-1)^{nm} \mathrm{Res}(g, f)$.

Beweis: Wir müssen in der SYLVESTER-Matrix m Zeilen zu f mit den n Zeilen zu g vertauschen. Dies kann beispielsweise so realisiert werden, daß wir die unterste f-Zeile nacheinander mit jeder der g-Zeilen vertauschen, bis sie nach n Vertauschungen schließlich unten steht. Dies müssen wir wiederholen, bis alle f-Zeilen unten stehen, wir haben also insgesamt nm Zeilenvertauschungen. Somit ändert sich das Vorzeichen der Determinante um den Faktor $(-1)^{nm}$. ∎

i) Resultanten und homomorphe Bilder

Ein aufmerksamer Leser muß sich an dieser Stelle (mindestens) zwei Fragen stellen:

1.) Die Resultante sagt uns, ob zwei Polynome einen gemeinsamen Teiler haben oder nicht. Um dies zu entscheiden, berechnen wir den größten gemeinsamen Teiler und je nachdem, welchen Grad dieser hat, setzen wir die Resultante auf Null oder einen anderen Wert. Wozu brauchen wir, wenn wir ohnehin den ggT berechnen, dann überhaupt eine Resultante?

2.) Da der Algorithmus à la EUKLID die Folge der sukkzessiven Reste berechnet, bekommen wir genau dieselben Probleme mit explodierenden Zwischenergebnissen wie bei EUKLIDischen Algorithmus. Dort hielten wir diese für inakzeptabel; warum sollten wir sie hier tolerieren?

Tatsächlich ist kaum eine Situation vorstellbar, in der es sonderlich sinnvoll wäre, die Resultante zweier konkret gegebener Polynome aus $\mathbb{Q}[X]$ zu berechnen: Wenn wir wissen wollen, ob sie gemeinsame Nullstellen haben, berechnen wir ihren ggT.

Die wahre Nützlichkeit von Resultanten kommt von Situationen wie der, für die wir Resultanten bereits angewandt haben: Wir haben Resultanten für Polynome mit ganzzahligen Koeffizienten berechnet und daraus geschlossen, modulo welcher Primzahlen zwei Polynome einen gemeinsamen Teiler haben. Dort ging es in erster Linie um den Beweis, daß das ggT-Problem nur modulo endlich vieler Primzahlen schlechte Reduktion hat.

Dort ging es zwar nur um einen abstrakten Beweis, aber entsprechende Situationen lassen sich auch für algorithmische Anwendungen nutzen.

Das Grundprinzip, das uns auf beide Fragen eine Antwort geben wird, ist das bereits beim modularen EUKLIDischen Algorithmus betrachtete Rechnen modulo homomorpher Bilder.

Zunächst einige Begriffe aus der Algebra:

Definition: *a)* Ein Homomorphismus $\varphi\colon R \to S$ von Ringen ist eine Abbildung, für die gilt

$$\varphi(r+s) = \varphi(r) + \varphi(s) \quad \text{und} \quad \varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$$

für alle $r, s \in \mathbb{R}$.
b) Der *Kern* eines Homomorphismus $\varphi\colon R \to S$ von Ringen ist die Menge aller $r \in R$ mit $\varphi(r) = 0$.
c) Eine Teilmenge $I \subseteq R$ heißt *Ideal* von R, in Zeichen $I \lhd R$, wenn gilt:

1.) I ist eine additive Untergruppe von R
2.) Für $r \in R$ und $s \in I$ ist auch rs ein Element von I.

Ideale spielen bei Ringen genau dieselbe Rolle wie Normalteiler bei Gruppen, d.h. es gilt:

Lemma: Zu einem Ring R und einer Teilmenge $I \subseteq R$ gibt es genau dann einen Homomorphismus $\varphi\colon R \to S$ mit Kern I, wenn I ein Ideal von R ist.

Beweis: Ist I Kern des Homomorphismus $\varphi\colon R \to S$, so ist I natürlich eine additive Untergruppe von R, da φ insbesondere auch ein Gruppenhomomorphismus ist. Für $r \in R$ und $s \in I$ ist $\varphi(s) = 0$, also auch $\varphi(rs) = \varphi(r)\varphi(s) = 0$. Somit ist I ein Ideal.

Ist umgekehrt I ein Ideal von R, so können wir auf R eine Äquivalenzrelation definieren durch $r \sim s$ genau dann, wenn $r - s \in I$. Die Äquivalenzklasse von r bezeichnen wir mit $\overline{r}$, die Menge aller Äquivalenzklassen mit $\overline{R} = R/I$.

Für $r, r', s, s' \in R$ mit $r \sim r'$ und $s \sim s'$ liegt mit $r - r'$ und $s - s'$ auch $r + s - r' - s'$ in I, d.h. $\overline{r+s} = \overline{r} + \overline{s}$. Genauso ist auch $\overline{r \cdot s} = \overline{r} \cdot \overline{s}$, denn ist $r' = r + i$ und $s' = s + j$ mit $i, j \in I$, so ist

$$r' \cdot s' = (r+i)(s+j) = rs + is + rj + ij\,,$$

und wegen der Idealeigenschaft von i liegen rs, is und rj allesamt in I. Somit ist $\overline{R}$ ein Ring, und die Abbildung $\varphi\colon R \to \overline{R}$, die jedes $r \in R$ auf seine Äquivalenzklasse $\overline{r}$ in $\overline{R}$ abbildet, ist ein Homomorphismus, dessen Kern natürlich I ist. ∎

Die Ideale haben ihren Namen von KUMMER, der sie als *ideale Zahlen* betrachtete: KUMMER glaubte zunächst, er habe einen Beweis der FERMAT-Vermutung gefunden, allerdings war er davon ausgegangen, daß der Ring $\mathbb{Z}[\zeta_p]$, wobei p eine primitive p-te Einheitswurzel bezeichnet, faktoriell ist. Dies ist zwar für unendlich viele Primzahlen p der Fall, aber eben nicht für alle. KUMMER konnte aber zeigen, daß es auf dem Niveau der Ideale eine eindeutige Primzerlegung gibt – leider reichte das aber nicht aus, um seinen Beweis auch für die Primzahlen zu retten für die $\mathbb{Z}[\zeta_p]$ nicht faktoriell ist.

Natürlich definiert jeder Homomorphismus $\varphi\colon R \to S$ einen Homomorphismus

$$\varphi\colon \begin{cases} R[X] \to S[X] \\ a_n X^n + \cdots + a_0 \mapsto \varphi(a_n)X^n + \cdots + \varphi(a_0) \end{cases}$$

zwischen den Polynomringen darüber, und da die Resultante zweier Polynome als Summe von Produkten von Koeffizienten der beiden Polynome dargestellt werden kann, ist

$$\operatorname{Res}_X\big(\varphi(f), \varphi(g)\big) = \varphi\big(\operatorname{Res}_X(f, g)\big)\,.$$

Diese Formel hatten wir bereits im Fall $R = \mathbb{Z}$ und $S = \mathbb{F}_p$ angewandt; für praktische Anwendungen interessanter sind aber Fälle wie die Abbildungen

$$\varphi_a\colon \begin{cases} R[X] \to R \\ X \mapsto a \end{cases} \quad \text{für ein Element } a \in R\,.$$

...