Kapitel 2
Grundalgorithmen

§1: Der Euklidische Algorithmus für ganze Zahlen

a) Der klassische Euklidische Algorithmus

Beginnen wir mit dem einfachsten Fall, für den der Algorithmus schon im zehnten Buch von EUKLIDs Elementen zu finden ist: 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 EUKLIDische Algorithmus zur Berechnung des ggT zweier natürlicher Zahlen a und b 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 offensichtlich $a = 2$ 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 die kleinsten Zahlen, für die n Divisionen notwendig sind, und r sei der Rest bei der ersten Division. Für die zweite Division $b : r$ ist dann $b_n \geq a_{n-1}$ und $r \geq b_{n-1}$; die kleinstmöglichen Werte sind damit

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

Da wir $a_1 = 2$ und $b_1 = 1$ kennen, können wir somit 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 $\phi = \dfrac{1+\sqrt{5}}{2} \approx 1{,}618034$, $\overline{\phi} = 1 - \phi \approx -0{,}618034$ 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.

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

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

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 $u = b/ggT(a, b)$ 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

$$a_1x_1 + \cdots + a_nx_n = c$$

mit ganzen Zahlen a_i, c, für die ganzzahlige Lösungen x_i gesucht sind. Auch eine solche Gleichung ist offensichtlich unlösbar, wenn der ggT der Koeffizienten a_i die rechte Seite nicht teilt.

Auch der ggT mehrerer Zahlen a_i kann aus diesen linear kombiniert werden: 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.

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

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

das Problem.

Es ist natürlich nicht die einzige Lösung; da m und n teilerfremd sind, ist die allgemeine Lösung

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

Die Lösung ist also 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_1m_2. Ist c_2 eine feste Lösung, so läßt sich die Lösung schreiben als Kongruenz

$$x \equiv c_2 \bmod m_1m_2\,,$$

und da die m_i paarweise teilerfremd sind, ist auch m_1m_2 teilerfremd zu m_3. Mit EUKLID können wir daher das System

$$x \equiv c_2 \bmod m_1m_2 \quad \text{und} \quad x \equiv a3 \bmod m_3$$

lösen und die Lösung schreiben als

$$x \equiv c_3 \bmod m_1m_2m_3$$

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

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: Ganzzahlige Polynome

a) Der Euklidische Algorithmus für Polynome

Zunächst sei k ein Körper und

$$A = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

sowie

$$B = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$$

seien Polynome mit Koeffizienten a_i, b_i aus k; falls a_n und b_m nicht verschwinden, bezeichnen wir

$$n = \deg A \quad \text{und} \quad m = \deg B$$

als die Grade von A und B.

Da wir Koeffizienten aus einem Körper haben, läßt sich das Polynom A nach dem bekannten Algorithmus mit Rest durch B dividieren, d.h. man kann Polynome Q, R finden, für die

$$A = QB + R \quad \text{ist mit} \quad \deg R < \deg B\,.$$

Mit dieser Division lassen sich sowohl der gewöhnliche als auch der erweiterte EUKLIDische Algorithmus sofort verallgemeinern auf Polynome; da der Grad von R kleiner ist als der von B und Grade als nichtnegative ganze Zahlen nicht unbegrenzt kleiner werden können, folgt daß der Algorithmus auch für Polynome stets nach endlich vielen Schritten endet, und hier ist die naive obere Schranke für die Anzahl von Divisionen, der Grad von B, sogar bereits realistisch.

b) Probleme bei der praktischen Durchführung

Wirklich explizit durchführbar ist der Algorithmus natürlich nur, wenn wir im Körper k rechnen können, also beispielsweise für $k = \mathbb{Q}$ oder einen endlichen Körper.

Das Ergebnis kann allerdings gerade über den rationalen Zahlen und ihren Erweiterungskörpern unerwartet ausfallen:

Betrachten wir etwa die beiden Polynome

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

und

$$Q = 3X^6 + 5X^4 - 4X^2 - 9X + 21\,.$$

Division von P durch Q 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 Q durch R_2 ergibt

$$R_3 = -\frac{117}{25}X^2 - 9X + \frac{441}{25}\,,$$

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

$$R_5 = \frac{1288744821}{543589225}\,.$$

c) Was ist „der“ ggT zweier Polynome?

Da beide Ausgangspolynome ganzzahlige Koeffizienten haben, erscheint ein ggT mit einem so großen Nenner seltsam. In der Tat ist jedes Polynom durch jede von Null verschiedene Konstante teilbar; ist also ein Polynom P Teiler eines Polynoms Q, so ist auch jedes von Null verschiedene skalare Vielfache von P Teiler von Q. Somit können wir hier nicht sinnvoll von *dem* größten gemeinsamen Teiler zweier Polynome reden.

Wir haben bislang noch nicht definiert, wann ein Polynom *größer* sein soll als ein anderes: Bei zwei natürlichen Zahlen ist klar, welche größer ist, aber schon bei reellen Polynomen ist alles andere als klar, ob etwa $x + 2$ größer sein soll als $2x + 1$ oder umgekehrt. Wir werden dieses Problem ignorieren und einfach sagen, P sei *ein* größter gemeinsamer Teiler von A und B, wenn P ein gemeinsamer Teiler ist und jeder andere gemeinsamen Teiler ein Teiler von P ist.

Der größte gemeinsame Teiler, den uns der EUKLIDISCHE Algorithmus für Polynome liefert, hat diese Eigenschaft, denn da dieser ggT als Linearkombination von A und B geschrieben werden kann, muß jedes Polynom, das sowohl A als auch B teilt, auch den ggT teilen.

Problematischer ist, daß es viele solche größten gemeinsamen Teiler geben kann: Zumindest jedes von Null verschiedene skalare Vielfache eines ggT ist selbst einer. Zum Glück ist das aber auch schon alles, was passieren kann: Sind nämlich P und Q zwei größte gemeinsame Teiler von A und B, so muß nach Definition P ein Teiler von Q sein und umgekehrt. Da der Grad eines Teilers stets kleiner oder gleich dem des Polynoms ist, haben die beiden also insbesondere denselben Grad, und ihr Quotient, egal in welcher Reihenfolge, hat Grad Null und ist somit eine Konstante.

Der größte gemeinsame Teiler zweier Polynome über einem Körper ist also eindeutig bis auf Multiplikation mit einer nichtverschwindenen Konstanten; diese Konstante kann nach Belieben gewählt werden und wird meist so gewählt, daß das Ergebnis in irgendeinem Sinne einfach wird.

Auf das obige Beispiel angewendet heißt das, daß mit

$$R_5 = \frac{1288744821}{543589225}$$

auch eins ein ggT von A und B ist und man daher im allgemeinen sagen würde, „der“ ggT von A und B sei eins.

Im nächsten Paragraphen werden wir Verfahren diskutieren, die uns dieses Ergebnis direkter liefern als der direkte EUKLIDische Algorithmus.

d) Der Satz von Gauß

Bei Polynomen mit ganzzahligen Koeffizienten können wir auch verlangen, daß ein Polynom nur dann als Teiler eines anderen bezeichnet werden soll, wenn der Quotient der beiden wieder ein Polynom mit ganzzahligen Koeffizienten ist. In diesem Sinne ist dann zwar $X+1$ ein Teiler von X^2-1, nicht aber $2X+2$.

Sind P und Q zwei Polynome mit ganzzahligen Koeffizienten, so bezeichnen wir ein Polynom T mit ganzzazhligen Koeffizienten als einen größten gemeinsamen Teiler von P und Q in $\mathbb{Z}[X]$, wenn es einerseits Teiler von P und Q ist und andererseits jeder weitere Teiler H von P und Q Teiler von T ist – jeweils im gerade definieren Sinne.

Es ist nicht klar, daß ein solcher ggT existiert: Der EUKLIDische Algorithmus für $\mathbb{Q}[X]$ wird ihn jedenfalls im allgemeinen nicht liefern. Falls er allerdings existiert, ist er bis auf den Faktor ± 1 eindeutig bestimmt, denn sind T_1 und T_2 zwei größte gemeinsame Teiler, so muß jeder der beiden den anderen teilen, so unterscheiden sich also nur um einen skalaren Faktor, und der kann, wenn jedes das andere teilen soll, nur ± 1 sein.

Der Satz von GAUSS zeigt, daß größte gemeinsame Teiler in $\mathbb{Z}[X]$ existieren und daß sie über den EUKLIDischen Algorithmus auch berechnet werden können.

Wir bezeichnen ein Polynom $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ mit ganzzahligen Koeffizienten als *primitiv,* wenn der ggT seiner sämtlichen Koeffizienten eins ist, wenn die Koeffizienten also keinen gemeinsamen Teiler vom Betrag größer eins haben. Für ein beliebiges ganzzahliges Polynom bezeichnen wir den ggT seiner Koeffizienten als seinen *Inhalt* $I(P)$. Jedes Polynom P läßt sich somit schreiben als $P = I(P) \cdot P^*$, wobei P^* ein primitives Polynom ist.

Lemma: Für zwei Polynome $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ und $Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$ mit ganzzahligen Koeffizienten ist $I(PQ) = I(P) \cdot I(Q)$. Insbesondere ist das Produkt zweier primitiver Polynome wieder primitiv.

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

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

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

dann ist

$$c_r = \sum_{i,j \text{ mit } i+j=r} a_ib_j\,.$$

Angenommen, diese Koeffizienten c_r haben einen gemeinsamen Teiler vom Betrag größer eins. Dann gibt es auch eine Primzahl p, die alle Koeffizienten c_r teilt.

Insbesondere ist p ein Teiler von $c_0 = a_0b_0$; da p Primzahl ist, muß einer der beiden Faktoren a_0, b_0 durch p teilbar sein. Da es im Lemma nicht auf die Reihenfolge von P und Q ankommt, können wir o.B.d.A. annehmen, daß a_0 Vielfaches von p ist.

Da P 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 Q 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 $a_i b_j$ ist entweder $i < \nu$ oder $j < \mu$, so daß mindestens einer der Faktoren und damit auch das Produkt durch p teilbar ist. Insgesamt ist daher $c_{\mu+\nu}$ nicht durch p teilbar, im Widerspruch zur Annahme.

Somit muß PQ ein primitives Polynom sein. ■

Satz von Gauß: Läßt sich ein ganzzahliges Polynom P als Produkt zweier Polynome Q_1, Q_2 mit rationalen Koeffizienten schreiben, so gibt es skalare Vielfache $\widetilde{Q}_1$ und $\widetilde{Q}_2$ von Q_1 und Q_2 mit ganzzahligen Koeffizienten, so daß $P = \widetilde{Q}_1 \cdot \widetilde{Q}_2$ ist.

Beweis: Durch Multiplikation mit dem Hauptnenner aller Koeffizienten können wir aus einem Polynom mit rationalen Koeffizienten eines mit ganzzahligen Koeffizienten machen. Dieses wiederum ist gleich seinem Inhalt mal einem primitiven Polynom. Somit läßt sich jedes Polynom mit rationalen Koeffizienten schreiben als Produkt einer rationalen Zahl mit einem primitiven ganzzahligen Polynom. Für Q_1 und Q_2 sei dies die Zerlegung

$$Q_1 = c_1 Q_1^* \quad \text{und} \quad Q_2 = c_2 Q_2^* \,.$$

Dann ist $P = (c_1c_2)Q_1^*Q_2^*$, und nach dem Lemma ist $Q_1^*Q_2^*$ ein primitives Polynom. Daher ist $c_1c_2 = I(P)$ eine ganze Zahl, und wir können beispielsweise $\widetilde{Q}_1 = I(P)Q_1^*$ und $\widetilde{Q}_2 = Q_2^*$ setzen. ■

Korollar: Ist für zwei Polynome P, Q mit ganzzahligen Koeffizienten das Polynom T mit rationalen Koeffizienten ein ggT in $\mathbb{Q}[X]$, so hat T ein skalares Vielfaches T^* mit ganzzahligen Koeffizienten, das ggT von P und Q in $\mathbb{Z}[X]$ ist.

Im nächsten Paragraphen werden wir eine Methode kennenlernen. wie man T^* ohne den Umweg über $\mathbb{Q}[X]$ berechnen kann.

§3: Resultanten und die modulare Berechnung des ggT

Das Problem mit den immer größer werdenden Koeffizienten kann über endlichen Körpern nicht auftreten, da es dort nur endlich viele Elemente gibt. Es liegt daher nahe, zur Berechnung des größten gemeinsamen Teilers zweier Polynome mit ganzzahligen Koeffizienten das entsprechende Problem modulo geeigneter Primzahlen p zu lösen und aus diesen Lösungen auf den ggT über $\mathbb{Z}$ zu schließen.

a) Zusammenhang zwischen ggT und modularem ggT

$$P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

und

$$Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$$

seien zwei Polynome mit ganzzahligen Koeffizienten. Ist

$$T = c_rX^r + c_{r-1}X^{r-1} + \cdots + c_1X + c_0$$

ein Teiler von P und Q, so ist natürlich auch für jede Primzahl p das Polynom $T \bmod p$ ein Teiler von $P \bmod p$ und $Q \bmod p$, wobei das Polynom modulo p einfach das Polynom mit modulo p reduzierten Koeffizienten bedeuten soll.

Das Polynom $T \bmod p$ kann allerdings kleineren Grad als T haben; dies ist genau dann der Fall, wenn der führende Koeffizient von T durch p teilbar ist.

Für $P = 3X^6+3X^5+X+1$ und $Q = 3X^6-3X^5+X-1$ beispielsweise ist

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