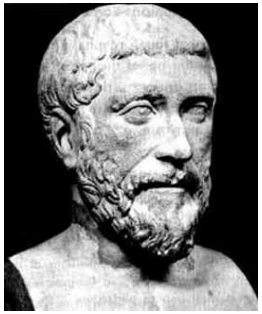
Kapitel 1
Ganze Zahlen und ihre Primzerlegung

§0: Rationale und irrationale Zahlen

Die Zahlentheorie beschäftigt sich, wie schon ihr Name sagt, mit Zahlen. Nun würde allerdings eine Umfrage wohl ergeben, daß sich nach Ansicht eines Großteils der Bevölkerung die gesamte Mathematik mit Zahlen beschäftigt – auch wenn beispielsweise im neunbändigen Analysislehrbuch von JEAN DIEUDONNÉ abgesehen von den dreiteiligen Abschnittsnummern praktisch keine Zahlen außer 0, 1 und 2 vorkommen.

Die Zahlentheorie unterscheidet sich dadurch von anderen Teilen der Mathematik, daß es dort vor allem um *ganze* Zahlen geht, oft sogar einfach um die natürlichen Zahlen $1, 2, 3, \ldots$. Die frühe griechische Philosophie der Pythagoräer beispielsweise stand unter dem Motto *Alles ist Zahl*. Sie konnten die musikalischen Harmonien auf einfache Verhältnisse natürlicher Zahlen zurückführen und waren überzeugt, daß dies auch für alle anderen Proportionen galt.

Umso größer war der Schock, als um 450 v.Chr. einer von ihnen, wahrscheinlich HIPPASSOS VON METAPONT, herausfand, daß es in der Geometrie Längenverhältnisse gibt, die sich *nicht* so beschreiben lassen. Schlimmer noch: Ein Beispiel dafür bietet ausgerechnet das Wahrzeichen der Pythagoräer, das Pentagramm. HIPPASSOS VON METAPONT nahm deshalb auch ein schlimmes Ende: Nach einigen Überlieferungen wurde er von den erzürnten Pythagoräern ertränkt, nach anderen ließen ihn die Götter als Strafe für seine Schandtat bei einem Schiffsuntergang ertrinken.



PYTHAGORAS VON SAMOS lebte etwa von 569 bis 475. Als ungefähr 18-Jähriger besuchte er Thales in Milot und ging auf dessen Rat 535 nach Ägypten, um mehr über Mathematik und Astronomie zu lernen. Im Tempel von Diospolis wurde er nach der dafür vorgesehen Ausbildung in die Priesterschaft aufgenommen. 525, bei der persischen Invasion Ägyptens, geriet er in Gefangenschaft und wurde nach Babylon gebracht, was er nutzte er, um die dortige Mathematik zu erlernen. 520 kam er frei und kehrte zurück nach Samos, zog aber schon bald weiter nach Croton in Süditalien, wo er eine religiöse und philosophische Schule gründete, die Pythagoräer.

Wir wollen uns hier zunächst mit einem einfacheren Fall als dem Pentagramm beschäftigen, beschäftigen, dem Verhältnis zwischen der Diagonale und der Seite eines Quadrats. In einem Quadrat der Seitenlänge a kann die Diagonale aufgefaßt werden als Hypothenuse eines gleichschenkligen rechtwinkligen Dreiecks mit Katheten der Länge a; sie hat daher nach dem Satz des PYTHAGORAS (der tatsächlich wohl einige hundert Jahre älter als PYTHAGORAS sein dürfte) die Länge $a\sqrt{2}$, und das gesuchte Verhältnis ist $\sqrt{2}$.

Wäre $\sqrt{2}$ als Verhältnis a/b zweier natürlicher Zahlen darstellbar, so könnten wir ohne Beschränkung der Allgemeinheit annehmen, daß mindestens eine der beiden Zahlen a und b ungerade ist: Andernfalls müßten wir einfach so lange durch zwei kürzen, bis dies der Fall ist.

Quadrieren wir beide Seiten der Gleichung $a/b = \sqrt{2}$, so erhalten wir die neue Gleichung $a^2/b^2 = 2$; demnach müßte $a^2 = 2b^2$ eine gerade Zahl sein. Damit müßte aber auch a gerade sein, denn das Quadrat einer ungeraden Zahl ist ungerade. Wenn aber a durch zwei teilbar ist, ist $a^2 = 2b^2$ durch vier teilbar, also wäre auch b^2 und damit auch b gerade, ein Widerspruch. Somit ist $\sqrt{2}$ keine rationale Zahl.

Auch das Verhältnis zwischen Umfang und Durchmesser eines Kreises, für das wir heute die Bezeichnung π verwenden, ist nicht rational, allerdings erfordert der Beweis dafür etwas mehr Arbeit. Ich möchte ihn trotzdem hier vorstellen, denn er zeigt sehr schön, wie zahlentheoretische Aussagen teilweise nur auf Umwegen über andere Gebiete der Mathematik bewiesen werden können. Beim folgenden Beweis führt

dieser Umweg über die relle Analysis:

Wir gehen zunächst aus von einem beliebigen Polynom $P(x)$ mit reellen Koeffizienten von einem geraden Grad $2n$. Dazu definieren wir das Polynom

$$Q(x) = P(x) - P''(x) + P^{(4)}(x) - \cdots + (-1)^n P^{(2n)}(x)$$

als die alternierende Summe der Ableitungen gerader Ordnung von P. Weiter betrachten wir die Funktion $S(x) = Q'(x)\sin x - Q(x)\cos x$; ihre Ableitung ist

$$\begin{aligned} S'(x) &= Q''(x)\sin x + Q'(x)\cos x - Q'(x)\cos x + Q(x)\sin x \\ &= \big(Q''(x) + Q(x)\big)\sin x\,. \end{aligned}$$

In $Q''(x) = P''(x) - P^{(4)}(x) + \cdots + (-1)^{n-1}P^{(2n)}(x)$ kommen bis auf $P(x)$ genau dieselben Terme vor wie in $Q(x)$, allerdings mit dem jeweils anderen Vorzeichen. Daher ist $Q''(x) + Q(x) = P(x)$ und $S'(x) = P(x)\sin x$.

Somit ist $S(x) = Q'(x)\sin x - Q(x)\cos x$ eine Stammfunktion von $P(x)\sin x$, und wir erhalten die

Formel von Hermite:

$$\int_0^\pi P(x)\sin x\,dx = S(\pi) - S(0) = Q(\pi) + Q(0)\,,$$

denn $\sin 0 = \sin\pi = 0$, $\cos 0 = 1$ und $\cos\pi = -1$.

Wir nehmen nun an, $\pi = a/b$ sei eine rationale Zahl und wenden die gerade bewiesene Formel an auf das spezielle Polynom

$$P(x) = \frac{x^n(a-bx)^n}{n!}\,;$$

wir erhalten

$$I_n \underset{\text{def}}{=} \int_0^\pi P(x)\sin x\,dx = Q(\pi) + Q(0)\,.$$

$P(x)$ ist im Intervall $(0,\,\pi)$ genau wie die Sinusfunktion überall positiv; daher ist auch $I_n > 0$. Außerdem ist $P(x)$ symmetrisch zu $\pi/2$, denn

$$P(\pi - x) = (\pi - x)^n\big(a - b(\pi - x)\big)^n = \Big(\frac{a}{b} - x\Big)^n (bx)^n = x^n(a-bx)^n\,.$$

Das Maximum von P in $(0,\,\pi)$ wird an derselben Stelle angenommen wie das der Funktion $f(x) = x(a-bx)$; wegen $f'(x) = a - 2bx$ handelt es sich dabei um die Intervallmitte $a/2b = \pi/2$, und der Funktionswert dort ist

$$P\Big(\frac{a}{2b}\Big) = \frac{1}{n!}\Big(\frac{a}{2b}\Big)^n\Big(\frac{ab}{2b}\Big)^n = \frac{1}{n!}\frac{a^{2n}}{(4b)^n}\,.$$

Schätzen wir das Integral ab durch Intervallänge mal Maximum des Integranden, erhalten wir daher die Ungleichung

$$I_n \le \pi\cdot\frac{1}{n!}\frac{a^{2n}}{(4b)^n}$$

und sehen, daß I_n für $n\to\infty$ gegen Null geht; denn $n!$ wächst stärker als jede Potenz einer reellen Zahl. Somit ist

$$\lim_{n\to\infty} I_n = 0\,.$$

Andererseits ist aber $I_n = Q(0) + Q(\pi)$, was in diesem Fall wegen der Symmetrie von P einfach $2Q(0)$ ist. Wir wollen uns überlegen, daß $Q(0)$ eine ganze Zahl ist. Dazu reicht es zu zeigen, daß alle Ableitungen von $P(x)$ an der Stelle Null ganzzahlige Werte annehmen. Nach der binomischen Formel ist

$$P(x) = \frac{x^n(a-bx)^n}{n!} = \frac{1}{n!}\sum_{i=0}^{n}\binom{n}{i}a^{n-i}(-b)^i x^{n+i}\,;$$

die k-te Ableitung verschwindet also für $k < n$ an der Stelle Null. Für $k = n + i \ge n$ ist

$$P^{(k)}(0) = \frac{1}{n!}\binom{n}{i}a^{n-i}(-b)^i(n+i)!$$

ebenfalls eine ganze Zahl, da der Nenner $n!$ Teiler von $(n+i)!$ ist und ansonsten nur ganze Zahlen dastehen.

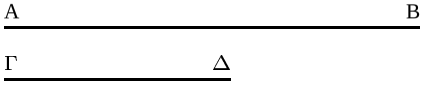
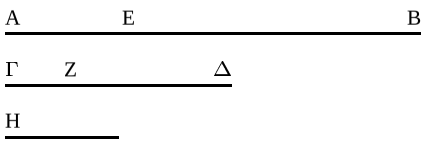
Somit ist also I_n für jedes $n\in\mathbb{N}$ eine positive ganze Zahl. Der Limes einer Folge positiver ganzer Zahlen kann aber unmöglich Null sein,

also führt die Annahme, $\pi = a/b$ sei eine rationale Zahl, zu einem Widerspruch, d.h. π ist irrational.

Wenn man schon dabei ist, kann man leicht auch noch viele anderere wichtige Zahlen als irrational erkennen; auf dem ersten Übungsblatt ist ein Beweis für die Irrationalität der EULERschen Zahl e skizziert, und mit nur wenig mehr Aufwand als im Fall der Quadratwurzel aus zwei läßt sich auch leicht zeigen, daß *jede* Quadratwurzel einer natürlichen Zahl entweder ganzzahlig oder irrational ist. Dasselbe gibt für höhere Wurzeln und sogar für Nullstellen gewisser Polynome mit ganzzahligen Koeffizienten, allerdings brauchen wir für allgemeine Beweis einen Satz, den zwar fast jeder kennt, dessen Beweis man aber nur selten sieht: Die eindeutige Primzerlegung der natürlichen Zahlen. Der Beweis dieses Satzes wiederum verwendet eine Konstruktion, die wahrscheinlich bereits den Pythagoräern bekannt war und die wir heute als EUKLIDischen Algorithmus bezeichnen. Wie sich zeigen wird, ist er zusammen mit einer ganzen Reihe von Varianten ein nicht nur in der Zahlentheorie allgegenwärtiges Werkzeug; es lohnt sich also, ihn gleich jetzt zum Beginn der Vorlesung etwas ausführlicher zu betrachten.

§ 1: Der Euklidische Algorithmus

Bei EUKLID, in Proposition 2 des siebten Buchs seiner *Elemente*, wird er (in der Übersetzung von CLEMENS THAER in Oswalds Klassikern der exakten Wissenschaft) 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.

Aus heutiger Sicht erscheint hier die Voraussetzung, daß die betrachteten Größen nicht teilerfremd sein dürfen, seltsam. Sie erklärt sich daraus, daß in der griechischen Philosophie und Mathematik die Einheit eine Sonderrolle einnahm und nicht als Zahl angesehen wurde: Die Zahlen begannen erst mit der Zwei. Dementsprechend führt EUKLID in Proposition 1 des siebten Buchs fast wörtlich dieselbe Konstruktion durch für den Fall von teilerfremden Größen. Schon wenig später wurde die Eins auch in Griechenland als Zahl anerkannt, und für uns heute ist die Unterscheidung ohnehin bedeutungslos. Wir können die Bedingung, daß der ggT ungleich eins sein soll, also einfach ignorieren.

Das dem EUKLIDischen Algorithmus zugrunde liegende Prinzip der *Wechselwegnahme* oder wechselseitigen Subtraktion war in der griechischen Mathematik spätestens gegen Ende des fünften vorchristlichen Jahrhunderts bereits wohlbekannt unter dem Namen Antanairesis

(ἀνταναιρεσις) oder auch Anthyphairesis (ἀνθυφαιρεσις), und auch der Algorithmus selbst geht mit ziemlicher Sicherheit, wie so vieles in den Elementen, *nicht* erst auf EUKLID zurück: Seine *Elemente* waren das wohl mindestens vierte Buchprojekt dieses Namens, und alles spricht dafür, daß er vieles von seinen Vorgängern übernommen hat. Seine Elemente waren dann aber mit Abstand die erfolgreichsten, so daß die anderen in Vergessenheit gerieten und verloren gingen; EUKLID wurde schließlich als *der* Stoichist bekannt nach dem griechischen Titel στοιχεῖα der Elemente.

Es ist nicht ganz sicher, ob EUKLID wirklich gelebt hat; es ist möglich, wenn auch sehr unwahrscheinlich, daß EUKLID wie BOURBAKI einfach ein Pseudonym für eine Autorengruppe ist. (Das nebenstehende Bild aus dem 18. Jahrhundert ist reine Phantasie.) EUKLID ist vor allem bekannt als Autor der *Elemente*, in denen er die Geometrie seiner Zeit systematisch darstellte und (in gewisser Weise) auf wenige Definitionen sowie die berühmten fünf Postulate zurückführte; sie entstanden um 300 v. Chr. EUKLID arbeitete wohl am Museion in Alexandrien; außer den Elementen schrieb er noch ein Buch über Optik und weitere, teilweise verschollene Bücher.

Wenn wir nicht mit Zirkel und Lineal arbeiten, sondern rechnen, können wir die mehrfache „Wegnahme“ einer Strecke von einer anderen einfacher beschreiben durch eine Division mit Rest: Sind a und b die (als natürliche Zahlen vorausgesetzten) Längen der beiden Strecken und ist $a : b = q$ Rest r, so kann man q mal die Strecke b von a wegnehmen, und übrig bleibt eine Strecke der Länge r.

EUKLIDs Konstruktion wird dann zu folgendem Algorithmus:

Gegeben seien zwei natürliche Zahlen a, b.

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

Schritt i, $i \geq 1$**:** Falls r_i verschwindet, endet der Algorithmus mit $\mathrm{ggT}(a, b) = r_{i-1}$; andernfalls sei r_{i+1} der Rest bei der Division von r_{i-1} durch r_i.

EUKLID behauptet, daß dieser Algorithmus stets endet und daß das Ergebnis der größte gemeinsame Teiler der Ausgangszahlen a, b ist, d.h.

die größte natürliche Zahl, die sowohl a als auch b teilt.

Da der Divisionsrest r_{i+1} stets echt kleiner ist als sein Vorgänger r_i und eine Folge immer kleiner werdender nichtnegativer ganzer Zahlen notwendigerweise nach endlich vielen Schritten die Null erreicht, muß der Algorithmus in der Tat stets enden. Daß er mit dem richtigen Ergebnis endet, ist ebenfalls leicht zu sehen, denn im i-ten Schritt ist

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

so daß jeder gemeinsame Teiler von r_i und r_{i+1} auch ein Teiler von r_{i-1} ist und umgekehrt jeder gemeinsame Teiler von r_{i-1} und r_i auch r_{i+1} teilt. Somit haben r_i und r_{i-1} diesselben gemeinsamen Teiler wie r_i und r_{i+1}, insbesondere haben sie denselben größten gemeinsamen Teiler. Durch Induktion folgt, daß in jedem Schritt $\mathrm{ggT}(r_i, r_{i-1}) = \mathrm{ggT}(a, b)$ ist. Im letzten Schritt ist $r_i = 0$; da jede natürliche Zahl Teiler der Null ist, ist dann $r_{i-1} = \mathrm{ggT}(r_i, r_{i-1}) = \mathrm{ggT}(a, b)$, wie behauptet.

§ 2: Der erweiterte Euklidische Algorithmus

Mehr als zwei Tausend Jahre nach der Entdeckung von Anthyphairesis und EUKLIDischem Algorithmus, 1624 in Bourg-en-Bresse, stellte BACHET DE MÉZIRIAC in der zweiten Auflage seines Buchs *Problèmes plaisants et délectables qui se fonts par les nombres* Aufgaben wie die folgende:

Il y a 41 personnes en un banquet tant hommes que femmes et enfants qui en tout dépensent 40 sous, mais chaque homme paye 4 sous, chaque femme 3 sous, chaque enfant 4 deniers. Je demande combien il y a d'hommes, combien de femmes, combien d'enfants.

(Bei einem Bankett sind 41 Personen, Männer, Frauen und Kinder, die zusammen vierzig Sous ausgeben, aber jeder Mann zahlt vier Sous, jede Frau drei Sous und jedes Kind 4 Deniers. Ich frage, wie viele Männer, wie viele Frauen und wie viele Kinder es sind.)

CLAUDE GASPAR BACHET SIEUR DE MÉZIRIAC (1581-1638) verbrachte den größten Teil seines Lebens in seinem Geburtsort Bourg-en-Bresse. Er studierte bei den Jesuiten in Lyon und Milano und trat 1601 in den Orden ein, trat aber bereits 1602 wegen Krankheit wieder aus und kehrte nach Bourg zurück. Sein Buch erschien 1612; 1959 brachte der Verlag Blanchard eine vereinfachte Ausgabe heraus. Am bekanntesten ist BACHET für seine lateinische Übersetzung der *Arithmetika* von DIOPHANTOS. In einem Exemplar davon schrieb FERMAT seine Vermutung an den Rand. Auch Gedichte von BACHET sind erhalten. 1635 wurde er Mitglied der französischen Akademie der Wissenschaften.

Sobald man weiß, daß zwölf Deniers ein Sou sind (und zwanzig Sous ein Pfund), kann man dies in ein lineares Gleichungssystem übersetzen: Ist x die Zahl der Männer, y die der Frauen und z die der Kinder, so muß gelten $x + y + z = 41$ und $4x + 3y + \frac{1}{3}z = 40$.

Zur Lösung kann man zunächst die erste Gleichung nach z auflösen und in die zweite Gleichung einsetzen; dies führt auf die Gleichung

$$\frac{11}{3}x + \frac{8}{3}y = \frac{79}{3} \quad \text{oder} \quad 11x + 8y = 79\,.$$

Bei einer solchen Gleichung ist *a priori* nicht klar, ob es überhaupt Lösungen gibt: Die Gleichung $10x + 8y = 79$ beispielsweise kann keine haben, denn für ganze Zahlen x, y ist $10x + 8y$ stets gerade. Allgemein kann $ax + by = c$ höchstens dann ganzzahlige Lösungen haben, wenn der ggT von a und b Teiler von c ist.

BACHET DE MÉZIRIAC hat bewiesen, daß sie in diesem Fall auch stets Lösungen hat; das Kernstück dazu ist seine Proposition XVIII, wo er zu zwei teilerfremden Zahlen a, b ganze Zahlen x, y konstruiert, für die $ax - by = 1$ ist: *Deux nombres premiers entre eux estant donnéz, treuuer le moindre multiple de chascun d'iceux, surpassant de l'unité un multiple de l'autre.* Die Methode ist eine einfache Erweiterung des EUKLIDischen Algorithmus, und genau wie letzterer nach EUKLID benannt ist, da ihn dieser rund 150 Jahre nach seiner Entdeckung in seinem Lehrbuch darstellte, heißt auch BACHETs Satz heute *Identität von* BÉZOUT, weil dieser ihn 142 Jahre später, im Jahre 1766, in seinem Lehrbuch beschrieb (und auf Polynome verallgemeinerte).

ETIENNE BÉZOUT (1730-1783) wurde in Nemours in der Ile-de-France geboren, wo seine Vorfahren Magistrate waren. Er ging stattdessen an die Akademie der Wissenschaften; seine Hauptbeschäftigung war die Zusammenstellung von Lehrbüchern für die Militärausbildung. Im 1766 erschienenen dritten Band (von vier) seines *Cours de Mathématiques à l'usage des Gardes du Pavillon et de la Marine* ist die Identität von BÉZOUT dargestellt. Seine Bücher waren so erfolgreich, daß sie auch ins Englische übersetzt und als Lehrbücher z.B. in Harvard benutzt wurden. Heute ist er vor allem auch bekannt durch seinen Beweis, daß sich zwei Kurven der Grade n und m in höchstens nm Punkten schneiden können.

Zur Lösung von Problemen wie dem von BACHET wollen wir gleich allgemein den größten gemeinsamen Teiler zweier Zahlen als Linearkombination dieser Zahlen darstellen. Dazu ist nur eine kleine Erweiterung des EUKLIDischen Algorithmus notwendig, so daß man oft auch einfach vom erweiterten EUKLIDischen Algorithmus spricht.

Die Gleichung

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

läßt sich umschreiben als

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

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 a und 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 verschwindet, endet der Algorithmus mit

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

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

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

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 wird 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:

$$200 = 1\cdot 148 + 52 \quad \text{und} \quad 52 = 1\cdot 200 - 1\cdot 148\,.$$

Da auch $52 \neq 0$, dividieren wir im zweiten Schritt 148 durch 52:

$148 = 2\cdot 52 + 44$ und $44 = 148 - 2\cdot(1\cdot 200 - 1\cdot 148) = 3\cdot 148 - 2\cdot 200$.

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

$8 = 52 - 44 = (1\cdot 200 - 1\cdot 148) - (3\cdot 148 - 2\cdot 200) = 3\cdot 200 - 4\cdot 148$.

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

$4 = 44 - 5\cdot 8 = (3\cdot 148 - 2\cdot 200) - 5\cdot(3\cdot 200 - 4\cdot 148) = 23\cdot 148 - 17\cdot 200$.

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

Zur Lösung des Problems von BACHET müssen wir die Gleichung $11x + 8y = 79$ betrachten. Dazu stellen wir zunächst den ggT von 11 und 8 als Linearkombination dieser Zahlen dar.

Elf durch acht ist eins Rest drei, also ist $3 = 1\cdot 11 - 1\cdot 8$.

Im nächsten Schritt dividieren wir acht durch drei mit dem Ergebnis zwei Rest zwei, also ist $2 = 1\cdot 8 - 2\cdot 3 = 1\cdot 8 - 2\cdot(1\cdot 11 - 1\cdot 8) = -2\cdot 11 + 3\cdot 8$.

Im letzten Schritt wird daher drei durch zwei dividiert und wir sehen erstens, daß der ggT gleich eins ist (was hier keine Überraschung ist), und zweitens, daß gilt $1 = 3 - 2 = (1\cdot 11 - 1\cdot 8) - (-2\cdot 11 + 3\cdot 8) = 3\cdot 11 - 4\cdot 8$.

Damit haben wir auch eine Darstellung von 79 als Linearkombination von elf und acht:

$$79 = 79\cdot(3\cdot 11 - 4\cdot 8) = 237\cdot 11 - 316\cdot 8\,.$$

Dies ist allerdings nicht die gesuchte Lösung: BACHET dachte sicherlich nicht an 237 Männer, -316 Frauen und 119 Kinder.

Nun ist aber die obige Gleichung $1 = 3\cdot 11 - 4\cdot 8$ nicht die einzige Möglichkeit zur Darstellung der Eins als Linearkombination von acht und elf: Da $8\cdot 11 - 11\cdot 8$ verschwindet, können wir ein beliebiges Vielfaches dieser Gleichung dazuaddieren und bekommen die allgemeinere Lösung

$$(3 + 8k)\cdot 11 - (4 + 11k)\cdot 8 = 1\,.$$

Entsprechend können wir auch ein beliebiges Vielfaches dieser Gleichung zur Darstellung von 79 addieren:

$$79 = (237 + 8k)\cdot 11 - (316 + 11k)\cdot 8\,.$$

Wir müssen k so wählen, daß sowohl die Anzahl $237 + 8k$ der Männer als auch die Anzahl $-(316 + 11k)$ der Frauen positiv oder zumindest nicht negativ wird, d.h. $-\frac{237}{8} \le k \le -\frac{316}{11}$. Da k ganzzahlig sein muß, kommt nur $k = -29$ in Frage; es waren also fünf Männer, drei Frauen und dazu noch $41 - 5 - 3 = 33$ Kinder. Ihre Gesamtausgaben belaufen sich in der Tat auf $5\cdot 4 + 3\cdot 3 + 33\cdot\frac{1}{3} = 40$ Sous.

Entsprechend kann der erweiterte EUKLIDische Algorithmus zur Lösung anderer diophantischer Gleichungen verwendet werden, von Gleichungen also, bei denen nur ganzzahlige Lösungen interessieren. Wir betrachten nur die einfache lineare Gleichung

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

für zwei Unbekannte $x, y \in \mathbb{Z}$.

Der größte gemeinsame Teiler $d = \text{ggT}(a, b)$ von a und b teilt offensichtlich jeden Ausdruck der Form $ax + by$ mit $x, y \in \mathbb{Z}$; falls d kein Teiler von c ist, kann es also keine ganzzahlige Lösung geben.

Ist aber $c = rd$ ein Vielfaches von d und ist $d = \alpha a + \beta b$ die lineare Darstellung des ggT nach dem erweiterten EUKLIDischen Algorithmus, so haben wir mit $x = r\alpha$ und $y = r\beta$ offensichtlich eine Lösung gefunden.

Ist (x', y') eine weitere Lösung, so ist

$$a(x - x') + b(y - y') = c - c = 0 \quad \text{oder} \quad a(x - x') = b(y' - y)\,.$$

$v = a(x-x') = b(y'-y)$ ist also ein gemeinsames Vielfaches von a und b und damit auch ein Vielfaches des kleinsten gemeinsamen Vielfachen von a und b. Dieses kleinste gemeinsame Vielfache ist ab/d, es muß also eine ganze Zahl m geben mit

$$x - x' = m \cdot \frac{b}{d} \quad \text{und} \quad y' - y = m \cdot \frac{a}{d}\,.$$

Die allgemeine Lösung der obigen Gleichung ist somit

$$x = r\alpha - m \cdot \frac{b}{d} \quad \text{und} \quad y = r\beta + m \cdot \frac{a}{d} \quad \text{mit} \quad m \in \mathbb{Z}\,.$$

§ 3: Der Aufwand des Euklidischen Algorithmus

Im Beweis, daß der EUKLIDische Algorithmus stets nach endlich vielen Schritten abbricht, hatten wir argumentiert, daß der Divisionsrest stets kleiner ist als der Divisor, so daß er irgendwann einmal null werden muß; dann endet der Algorithmus.

Damit haben wir auch eine obere Schranke für den Rechenaufwand zur Berechnung von $\text{ggT}(a, b)$: Wir müssen höchstens b Divisionen durchführen.

Das erscheint zwar auf den ersten Blick als ein recht gutes Ergebnis; wenn man aber bedenkt, daß der EUKLIDische Algorithmus heute in der Kryptographie auf über 600-stellige Zahlen angewendet wird, verliert diese Schranke schnell ihre Nützlichkeit: Da unser Universum ein geschätztes Alter von zehn Milliarden Jahren, also ungefähr $3 \cdot 10^{18}$ Sekunden hat, ist klar, daß auch der schnellste heutige Computer, der zu Beginn des Universum zu Rechnen begann, bis heute nur einen verschwindend kleinen Bruchteil von 10^{600} Divisionen ausgeführt hätte; Wäre 10^{600} eine realistische Aufwandsabschätzung, könnten wir an eine Anwendung des EUKLIDischen Algorithmus auf 600-stellige Zahlen nicht einmal denken.

Tatsächlich ist 10^{600} aber natürlich nur eine obere Schranke, von der wir bislang noch nicht wissen, wie realistisch sie ist. Um dies zu entscheiden, suchen wir die kleinsten natürlichen Zahlen a, b, für die n Divisionen notwendig sind; dies wird uns zurückführen auf ein Problem aus dem 13. Jahrhundert.

Im Falle $n = 1$ sind offensichtlich $a = b = 1$ die kleinstmöglichen Zahlen; wenn $a = b$ ist, 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

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

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:

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

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.* Er ging in Nordafrika zur Schule, kam aber 1202 zurück nach Pisa. 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.

Wie wir gerade gesehen haben, kann man mit den FIBONACCI-Zahlen nicht nur Karnickelpopulationen beschreiben, sondern – wie GABRIEL LAMÉ 1844 entdeckte – auch eine Obergrenze für den Aufwand beim EUKLIDischen Algorithmus angeben:

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

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 Alexanders I. kam er 1820 nach Rußland, wo er in St. Petersburg als Professor und Ingenieur unter anderem Vorlesungen über Analysis, Physik, Chemie und Ingenierswissenschaften hielt. 1832 erhielt er einen Lehrstuhl für Physik an der Ecole Polytechnique in Paris, 1852 einen für mathematische Physik und Wahrscheinlichkeitstheorie an der Sorbonne. 1836/37 war er wesentlich am Bau der Eisenbahnlinien Paris-Versailles und Paris–St. Germain beteiligt.

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

Um die Zahlen F_n durch eine geschlossene Formel darzustellen, können wir (genau wie man es auch für die rekursive Berechnung per Computer tun würde) die Definitionsgleichung der FIBONACCI-Zahlen als

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} \quad \text{mit} \quad A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

schreiben; dann ist

$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = A^{n-1} \begin{pmatrix} F_1 \\ F_0 \end{pmatrix} = A^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Das charakteristische Polynom von A ist

$$\det(A - \lambda E) = (1 - \lambda)(-\lambda) - 1 = \lambda^2 - \lambda - 1\,;$$

die Eigenwerte von A sind daher $\lambda_{1/2} = \frac{1}{2} \pm \frac{1}{2}\sqrt{5}$. Bezeichnet B die Matrix, deren Spalten aus den zugehörigen Eigenvektoren besteht, so ist also $A = B^{-1} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} B$ und

$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = A^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = B^{-1} \begin{pmatrix} \lambda_1^{n-1} & 0 \\ 0 & \lambda_2^{n-1} \end{pmatrix} B \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Auch ohne die Matrix B zu berechnen, wissen wir somit, daß sich F_n in der Form $F_n = a\lambda_1^{n-1} + b\lambda_2^{n-1}$ darstellen läßt. Für $n = 1$ und $n = 2$ erhalten wir die beiden Bedingungen

$$1 = a\lambda_1^0 + b\lambda_2^0 = a + b \quad \text{und} \quad 1 = a\lambda_1 + b\lambda_2 .$$

Damit ist $b = 1 - a$, und die zweite Gleichung wird zu

$$a(\lambda_1 - \lambda_2) + \lambda_2 = a\sqrt{5} + \lambda_2 = 1 \Longrightarrow a = \frac{1-\lambda_2}{\sqrt{5}} = \frac{\lambda_1}{\sqrt{5}} .$$

Also ist $b = 1 - a = -\lambda_2/\sqrt{5}$ und

$$F_n = \frac{\lambda_1^n - \lambda_2^n}{\sqrt{5}} .$$

Numerisch ist

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \approx 1{,}618034, \quad \lambda_2 = 1 - \lambda_1 = \frac{1-\sqrt{5}}{2} \approx -0{,}618034$$

und $\sqrt{5} \approx 2{,}236068$; der Quotient $\lambda_2^n/\sqrt{5}$ ist also für jedes n kleiner als $1/2$. Daher können wir F_n auch einfacher berechnen als nächste ganze Zahl zu $\lambda_1^n/\sqrt{5}$. Insbesondere folgt, daß F_n exponentiell mit n wächst.

Die Gleichung $\lambda^2 - \lambda - 1 = 0$ läßt sich umschreiben als $\lambda(\lambda - 1) = 1$ oder $\lambda : 1 = 1 : (\lambda - 1)$. Diese Gleichung charakterisiert den *goldenen Schnitt:* Stehen zwei Strecken a und b in diesem Verhältnis, so auch die beiden Strecken b und $a - b$. Die positive Lösung λ_1 wird traditionell mit dem Buchstaben ϕ bezeichnet; F_n ist also der zur nächsten ganzen Zahl gerundete Wert von $\phi^n/\sqrt{5}$.

Die beiden kleinsten Zahlen, für die wir n Divisionen brauchen, sind nach LAMÉ $a = F_{n+2}$ und $b = F_{n+1}$. Aus der geschlossenen Formel für die FIBONACCI-Zahlen folgt

$$\begin{aligned} n &\approx \log_\phi \sqrt{5}\, b - 1 = \log_\phi b + \log_\phi \sqrt{5} - 1 = \frac{\ln b}{\ln \phi} + \frac{\ln \sqrt{5}}{\ln \phi} - 1 \\ &\approx 2{,}078 \ln b + 0{,}672 . \end{aligned}$$

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

Tatsächlich gibt natürlich auch die hier berechnete Schranke nur selten den tatsächlichen Aufwand wieder; fast immer werden wir mit erheblich weniger auskommen. Im übrigen ist auch alles andere als klar, ob wir den ggT auf andere Weise nicht möglicherweise schneller berechnen können. Da wir aber für Zahlen der Größenordnung, die in heutigen Anwendungen interessieren, selbst mit der Schranke für den schlimmsten Fall ganz gut leben können, sei hier auf diese Fragen nicht weiter eingegangen. Interessenten finden mehr dazu z.B. in den Abschnitten 4.5.2+3 des Buchs

DONALD E. KNUTH: The Art of Computer Programming, *vol. 2:* Seminumerical Algorithms, *Addison-Wesley,* ^{2}1981

§4: Die multiplikative Struktur der ganzen Zahlen

Eine Primzahl ist bekanntlich eine natürliche Zahl p, die genau zwei Teiler hat, nämlich die Eins und sich selbst. Der erweiterte EUKLIDische Algorithmus liefert eine wichtige Folgerung aus dieser Definition:

Lemma: Wenn eine Primzahl das Produkt ab zweier natürlicher Zahlen teilt, teilt sie mindestens einen der Faktoren.

Beweis: Angenommen, die Primzahl p sei kein Teiler von a, teile aber ab. Da der ggT von a und p Teiler von p und ungleich p ist, muß er notgedrungen gleich eins sein; es gibt also eine Darstellung

$$1 = \alpha a + \beta p \quad \text{mit} \quad \alpha, \beta \in \mathbb{Z} .$$

Dann ist $b = \alpha ab + \beta pb$ durch p teilbar, denn sowohl ab also auch pb sind Vielfache von p. ∎

Daraus folgt induktiv

Satz: Jede natürliche Zahl läßt sich bis auf Reihenfolge eindeutig als ein Produkt von Primzahlpotenzen schreiben.

Beweis: Wir zeigen zunächst, daß sich jede natürliche Zahl überhaupt als Produkt von Primzahlpotenzen schreiben läßt. Falls dies nicht der Fall wäre, gäbe es ein minimales Gegenbeispiel M. Dies kann nicht die Eins sein, denn die ist ja das leere Produkt, und es kann auch keine Primzahl sein, denn die ist ja das Produkt mit sich selbst als einzigem Faktor. Somit hat M einen echten Teiler N, d.h. $1 < N < M$. Da M das minimale Gegenbeispiel war, lassen sich N und M/N als Produkte von Primzahlpotenzen schreiben, also auch $M = N \times M/N$.

Bleibt noch zu zeigen, daß die Produktdarstellung bis auf die Reihenfolge der Faktoren eindeutig ist. Auch hier gäbe es andernfalls wieder ein minimales Gegenbeispiel M, das somit mindestens zwei verschiedene Darstellungen

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

hätte. Da die Eins durch kein Produkt dargestellt werden kann, in dem wirklich eine Primzahl vorkommt, ist $M > 1$ und somit steht in jedem der beiden Produkte mindestens eine Primzahl.

Da p_1 Teiler von M ist, teilt es auch das rechtsstehende Produkt, also nach dem gerade bewiesenen Lemma mindestens einen der Faktoren, d.h. mindestens ein q_j. Da q_j eine Primzahl ist, muß dann $p_1 = q_j$ sein. Da M als minimales Gegenbeispiel vorausgesetzt war, unterscheiden sich die beiden Produkte, aus denen dieser gemeinsame Faktor gestrichen wurde, höchstens durch die Reihenfolge der Faktoren, und damit gilt dasselbe für die beiden Darstellungen von M. ∎

Als erste Anwendung dieses Satzes können wir zeigen

Satz: Die reelle Zahl x erfülle die Gleichung

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0\,.$$

Dann ist x entweder ganzzahlig oder irrational.

Beweis: Ist x eine rationale Zahl, so können wir es als Quotient $x = p/q$ zweier zueinander teilerfremder ganzer Zahlen p, q schreiben. Multiplikation der Gleichung

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

mit q^n führt auf die Gleichung

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0\,,$$

also ist

$$\begin{aligned} p^n &= -a_{n-1}p^{n-1}q - \cdots - a_1 pq^{n-1} - a_0 q^n \\ &= q(-a_{n-1}p^{n-1} - \cdots - a_1 pq^{n-s21} - a_0 q^{n-1})\,. \end{aligned}$$

Damit muß q Teiler von p^n sein, was wegen der Eindeutigkeit der Primfaktorzerlegung von p^n sowie der vorausgesetzten Teilerfremdheit von p und q nur für $q = \pm 1$ der Fall sein kann. Somit ist x eine ganze Zahl, wie behauptet. ∎

§5: Kongruenzenrechnung

Zwei ganze Zahlen lassen sich im allgemeinen nicht durcheinander dividieren. Trotzdem – oder gerade deshalb – spielen Teilbarkeitsfragen in der Zahlentheorie eine große Rolle. Das technische Werkzeug zu ihrer Behandlung ist die Kongruenzenrechnung.

Definition: Wir sagen, zwei ganze Zahlen $x, y \in \mathbb{Z}$ seien kongruent modulo m für eine natürliche Zahl m, in Zeichen

$$x \equiv y \bmod m\,,$$

wenn $x - y$ durch m teilbar ist.

Die Kongruenz modulo m definiert offensichtlich eine Äquivalenzrelation auf $\mathbb{Z}$: Jede ganze Zahl ist kongruent zu sich selbst, denn $x - x = 0$ ist durch jede natürliche Zahl teilbar; wenn $x - y$ durch m teilbar ist, so auch $y - x = -(x - y)$, und ist schließlich $x \equiv y \bmod m$ und $y \equiv z \bmod m$, so sind $x - y$ und $y - z$ durch m teilbar, also auch ihre Summe $x - z$, und damit ist auch $x \equiv z \bmod m$.

Zwei Zahlen $x, y \in \mathbb{Z}$ liegen genau dann in derselben Äquivalenzklasse, wenn sie bei der Division durch m denselben Divisionsrest haben; es gibt somit m Äquivalenzklassen, die den m möglichen Divisionsresten $0, 1, \ldots, m-1$ entsprechen.

Lemma: Ist $x \equiv x' \bmod m$ und $y \equiv y' \bmod m$, so ist auch

$$x \pm y \equiv x' \pm y' \bmod m \quad \text{und} \quad x'y' \equiv xy \bmod m\,.$$

Beweis: Sind $x - x'$ und $y - y'$ durch m teilbar, so auch

$$(x \pm y) - (x' \pm y') = (x - x') \pm (y - y') \qquad \text{und}$$
$$xy - x'y' = x(y - y') + y'(x - x')$$

■

Im folgenden wollen wir das Symbol „mod“ nicht nur in Kongruenzen wie $x \equiv y \bmod m$ benutzen, sondern auch – wie in vielen Programmiersprachen üblich – als Rechenoperation:

Definition: Für eine ganze Zahl x und eine natürliche Zahl m bezeichnet $x \bmod m$ jene ganze Zahl $0 \le r < m$ mit $x \equiv r \bmod m$.

$x \bmod m$ ist also einfach der Divisionsrest bei der Division von x durch m.

Da nach dem gerade bewiesenen Lemma die Addition, Subtraktion und Multiplikation mit Kongrenzen vertauschbar sind, können wir auf der Menge aller Äquivalenzklassen Rechenoperationen einführen. Übersichtlicher wird das, wenn wir statt dessen die Menge

$$\mathbb{Z}/m \underset{\text{def}}{=} \{0, 1, \ldots, m-1\}$$

betrachten. Wir definieren eine Addition durch

$$x \oplus y = (x + y) \bmod m = \begin{cases} x + y & \text{falls } x + y < m \\ x + y - m & \text{sonst} \end{cases}$$

und entsprechend eine Multiplikation gemäß

$$x \odot y = (xy) \bmod m\,.$$

Für $m = 4$ haben wir also folgende Operationen:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

und

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Um diese Tabellen zu interpretieren, sollten wir uns an einige Grundbegriffe aus der Algebra erinnern:

Definition: *a)* Eine Gruppe ist eine Menge G zusammen mit einer Verknüpfung $\times\colon G \times G \to G$, für die gilt
1.) $(x \times y) \times z = x \times (y \times z)$ für alle $x, y, z \in G$.
2.) Es gibt ein Element $e \in G$, so daß $e \times x = x \times e = x$ für alle $x \in G$.
3.) Zu jedem $x \in G$ gibt es ein $x' \in G$, so daß $x \times x' = x' \times x = e$ ist.

Die Gruppe heißt kommutativ oder abelsch, wenn zusätzlich noch gilt

4.) $x \times y = y \times x$ für alle $x, y \in G$.

b) Eine Abbildung $\varphi\colon G \to H$ zwischen zwei Gruppen G und H mit Verknüpfungen $\times$ und $\otimes$ heißt (Gruppen-)Homomorphismus, falls für alle $x, y \in G$ gilt: $\varphi(x \times y) = \varphi(x) \otimes \varphi(y)$. Ist φ zusätzlich bijektiv, reden wir von einem Isomorphismus. Die Gruppen G und H heißen isomorph, in Zeichen $G \cong H$, wenn es einen Isomorphismus $\varphi\colon G \to H$ gibt.

c) Ein Ring ist eine Menge R zusammen mit zwei Verknüpfungen $+, \cdot\colon R \times R \to R$, so daß gilt
1.) Bezüglich + ist R eine abelsche Gruppe.
2.) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle $x, y, z \in R$.
3.) Es gibt ein Element $1 \in R$, so daß $1 \cdot x = x \cdot 1 = x$ für alle $x \in R$.
4.) $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x + y) \cdot z = x \cdot z + y \cdot z$ für alle $x, y, z \in R$.
Der Ring heißt kommutativ, wenn zusätzlich noch gilt
5.) $x \cdot y = y \cdot x$ für alle $x, y \in R$.

d) Eine Abbildung $\varphi\colon R \to S$ zwischen zwei Ringen heißt (Ring-) Homomorphismus, wenn für alle $x, y \in R$ gilt

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

wobei + und $\cdot$ auf der linken Seite jeweils die Operationen von R bezeichnen und rechts die von S. Auch hier reden wir von einem Isomorphismus, wenn φ bijektiv ist, und bezeichnen $R \cong S$ als isomorph, wenn es einen Isomorphismus $\varphi\colon R \to S$ gibt.

Lemma: Für jedes $m \in \mathbb{N}$ ist $\mathbb{Z}/m$ mit den Operationen $\oplus$ und $\odot$ ein Ring.

Beweis: Wir betrachten die Abbildung

$$\varphi\colon \begin{cases} \mathbb{Z} \to \mathbb{Z}/m \\ x \mapsto x \bmod m \end{cases}.$$

Nach dem obigen Lemma ist

$$\varphi(x + y) = \varphi(x) \oplus \varphi(y) \quad \text{und} \quad \varphi(xy) = \varphi(x) \odot \varphi(y)\,.$$

Da $\mathbb{Z}$ bezüglich + eine abelsche Gruppe ist, gilt somit dasselbe für $\mathbb{Z}/m$ bezüglich $\oplus$: Wenn zwei ganze Zahlen gleich sind, sind schließlich auch ihre Divisionsreste modulo m gleich. Das Neutralelement ist $\varphi(0) = 0$, und das additive Inverse ist $\varphi(-x) = m - \varphi(x)$. Auch die Eigenschaften von $\odot$ folgen sofort aus den entsprechenden Eigenschaften der Multiplikation ganzer Zahlen; das Neutralelement ist $\varphi(1) = 1$. ∎

Man beachte, daß $\mathbb{Z}/m$ im allgemeinen kein Körper ist: In $\mathbb{Z}/4$ beispielsweise ist $2 \odot 2 = 0$, und in einem Körper kann ein Produkt nur verschwinden, wenn mindestens einer der beiden Faktoren verschwindet.

Im folgenden werden wir die Rechenoperationen in $\mathbb{Z}/m$ einfach mit + und $\cdot$ bezeichnen, wobei jedesmal aus dem Zusammenhang klar sein sollte, ob wir von der Addition und Multiplikation in $\mathbb{Z}/m$ oder der in $\mathbb{Z}$ reden. Der Malpunkt wird dabei, wie üblich, oft weggelassen.

§6: Der chinesische Restesatz

Der Legende nach zählten chinesische Generäle ihre Truppen, indem sie diese mehrfach antreten ließen in Reihen verschiedener Breiten $m_1, \ldots, m_r$ und jedesmal nur die Anzahl a_r der Soldaten in der letzten Reihe zählten. Aus den r Relationen

$$x \equiv a_1 \bmod m_1, \quad \ldots, \quad x \equiv a_r \bmod m_r$$

bestimmten sie dann die Gesamtzahl x der Soldaten.

Ob es im alten China wirklich Generäle gab, die soviel Mathematik konnten, sei dahingestellt; Beispiele zu diesem Satz finden sich jedenfalls bereits 1247 in den chinesischen *Mathematischen Abhandlungen in neun Bänden* von CH'IN CHIU-SHAO (1202–1261), allerdings geht es dort nicht um Soldaten, sondern um Reis.

CH'IN CHIU-SHAO oder QIN JIUSHAO wurde 1202 in der Provinz Sichuan geboren. Auf eine wilde Jugend mit vielen Affairen folgte ein wildes und alles andere als gesetztreues Berufsleben in Armee, öffentlicher Verwaltung und illegalem Salzhandel. Als Jugendlicher studierte er an der Akademie von Hang-chou Astronomie, später brachte ihm ein unbekannter Lehrer Mathematik bei. Insbesondere studierte er die in vorchristlicher Zeit entstandenen *Neun Bücher der Rechenkunst*, nach deren Vorbild er 1247 seine deutlich anspruchsvolleren *Mathematischen Abhandlungen in neun Bänden* publizierte, die ihn als einen der bedeutendsten Mathematiker nicht nur Chinas ausweisen. Zum chinesischen Restesatz schreibt er, daß er ihn von den Kalendermachern gelernt habe, diese ihn jedoch nur rein mechanisch anwendeten ohne ihn zu verstehen. CH'IN CHIU-SHAO starb 1261 in Meixian, wohin er nach einer seiner vielen Entlassungen wegen krimineller Machenschaften geschickt worden war.

Wir wollen uns zunächst überlegen, unter welchen Bedingungen ein solches Verfahren überhaupt funktionieren kann. Offensichtlich können die obigen r Relationen eine natürliche Zahl nicht eindeutig festlegen, denn ist x eine Lösung und M irgendein gemeinsames Vielfaches der sämtlichen m_i, so ist $x + M$ auch eine – M ist schließlich modulo aller m_i kongruent zur Null.

Außerdem gibt es Relationen obiger Form, die unlösbar sind, beispielsweise das System

$$x \equiv 2 \bmod 4 \quad \text{und} \quad x \equiv 3 \bmod 6\,,$$

dessen erste Gleichung nur gerade Lösungen hat, während die zweite nur ungerade hat. Das Problem hier besteht darin, daß zwei ein gemeinsamer Teiler von vier und sechs ist, so daß jede der beiden Kongruenzen auch etwas über x mod 2 aussagt, wobei diese beiden Aussagen hier einander widersprechen.

Dieses Problem können wir dadurch umgehen, daß wir nur Moduln m_i zulassen, die paarweise teilerfremd sind. Dies hat auch den Vorteil, daß jedes gemeinsame Vielfache der m_i Vielfaches des Produkts aller m_i sein muß, so daß wir x modulo einer vergleichsweise großen Zahl kennen.

Chinesischer Restesatz: Das System von Kongruenzen

$$x \equiv a_1 \bmod m_1, \quad \ldots, \quad x \equiv a_r \bmod m_r$$

hat für paarweise teilerfremde Moduln m_i genau eine Lösung x mit $0 \le x < m_1 \cdots m_r$. Jede andere Lösung $y \in \mathbb{Z}$ läst sich in der Form $x + km_1 \cdots m_r$ schreiben mit $k \in \mathbb{Z}$.

Mit den Begriffen aus dem vorigen Paragraphen läßt sich dies auch anders formulieren: Die Zahl x mod m_i können wir auffassen als Element von $\mathbb{Z}/m_i$, das r-Tupel aus allen diesen Zahlen also als Element von $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$. Man überlegt sich leicht, daß das kartesische Produkt von zwei oder mehr Gruppen wieder eine Gruppe ist: Die Verknüpfung wird einfach komponentenweise definiert, und das Neutralelement ist dasjenige Tupel, dessen sämtliche Komponenten Neutralelemente der jeweiligen Faktoren sind. Genauso folgt, daß das kartesische Produkt von zwei oder mehr Ringen wieder ein Ring ist.

In algebraischer Formulierung haben wir dann die folgende Verschärfung des obigen Satzes:

Chinesischer Restesatz *(Algebraische Form)***:** Die Abbildung

$$\varphi\colon \begin{cases} \mathbb{Z}/m_1 \cdots m_r \to Z/m_1 \times \cdots \times \mathbb{Z}/m_r \\ \qquad\qquad x \mapsto (x \bmod m_1, \ldots, x \bmod m_r) \end{cases}$$

ist ein Isomorphismus von Ringen.

Wir *beweisen* den Satz in dieser algebraischen Form:

Zunächst ist

$$\psi\colon \begin{cases} \mathbb{Z} \to \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \\ x \mapsto (x \bmod m_1, \ldots, x \bmod m_r) \end{cases}$$

ein Ringhomomorphismus, denn nach dem Lemma aus dem vorigen Paragraphen ist der Übergang zu den Restklassen modulo jeder der Zahlen m_i mit Addition und Multiplikation vertauschbar. Da $\psi(x)$ nur von x mod $m_1 \cdots m_r$ abhängt, folgt daraus, daß auch φ ein Ringhomomorphismus ist.

φ ist injektiv, denn ist $\varphi(x) = \varphi(y)$, so ist $x \bmod m_i = y \bmod m_i$ für alle i; da die m_i paarweise teilerfremd sind, ist $x - y$ somit durch das Produkt der m_i teilbar, was für $x, y \in \mathbb{Z}/m_1 \cdots m_r$ nur im Fall $x = y$ möglich ist.

Nun ist φ aber eine Abbildung zwischen endlichen Mengen, die beide aus je $m_1 \cdots m_r$ Elementen bestehen. Jede injektive Abbildung zwischen zwei gleichmächtigen endlichen Mengen ist zwangsläufig auch surjektiv, also bijektiv, und somit ist φ ein Isomorphismus. ∎

Aus Sicht der chinesischen Generäle ist dieser Beweis enttäuschend: Angenommen, ein General weiß, daß höchstens Tausend Soldaten vor ihm stehen. Er läßt sie in Zehnerreihen antreten; in der letzten Reihe stehen fünf Soldaten. Bei Elferreihen sind es neun, bei Dreizehnerreihen sechs. Da $10 \cdot 11 \cdot 13 = 1430$ größer ist als Tausend, weiß er, daß dies die Anzahl eindeutig festlegt. Er weiß aber nicht, wie viele Soldaten nun tatsächlich vor ihm stehen. Als General hat er natürlich die Möglichkeit, einige Soldaten abzukommandieren, die für jede Zahl bis Tausend die Divisionsreste modulo $9, 10$ und 13 berechnen müssen, bis sie auf das Tripel $(5, 9, 6)$ stoßen. Wir als Mathematiker sollten jedoch eine effizientere Methode finden.

Dazu verhilft uns der erweiterte EUKLIDische Algorithmus:

Wir beginnen mit dem Fall zweier Kongruenzen

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

mit zueinander teilerfremden Zahlen m und n. Ihr ggT eins läßt sich nach dem erweiterten EUKLIDischen Algorithmus als $1 = \alpha m + \beta n$ schreiben. Somit ist

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

also löst

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

das Problem.

x 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 daher

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

Insbesondere ist die Lösung eindeutig modulo nm.

Als Beispiel betrachten wir die beiden Kongruenzen

$$x \equiv 1 \mod 17 \quad \text{und} \quad x \equiv 5 \mod 19\,.$$

Wir müssen als erstes den erweiterten EUKLIDischen Algorithmus auf die beiden Moduln 17 und 19 anwenden:

$$19 : 17 = 1 \text{ Rest } 2 \Longrightarrow 2 = 19 - 17$$

$$17 : 2 = 8 \text{ Rest } 1 \Longrightarrow 1 = 17 - 8 \cdot 2 = 9 \cdot 17 - 8 \cdot 19$$

Also ist $9 \cdot 17 = 153 \equiv 0 \mod 17$ und $\equiv 1 \mod 19$; außerdem ist $-8 \cdot 19 = -152$ durch 19 teilbar und $\equiv 1 \mod 17$. Die Zahl

$$x = -152 \cdot 1 + 153 \cdot 5 = 613$$

löst somit das Problem. Da 613 größer ist als $17 \cdot 19 = 323$, ist allerdings nicht 613 die kleinste positive Lösung, sondern $613 - 323 = 290$.

Bei mehr als zwei Kongruenzen gehen wir rekursiv vor: Wir lösen die ersten beiden Kongruenzen $x \equiv a_1 \mod m_1$ und $x \equiv a_2 \mod m_2$ 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

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

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

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

lösen und die Lösung schreiben als

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

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

Im Beispiel des oben angesprochenen Systems

$$x \equiv 5 \mod 10, \quad x \equiv 9 \mod 11, \quad x \equiv 6 \mod 13$$

lösen wir also zunächst nur das System

$$x \equiv 5 \mod 10 \quad \text{und} \quad x \equiv 9 \mod 11\,.$$

Da $1 = 11 - 10$, ist $11 \equiv 0 \mod 11$ und $11 \equiv 1 \mod 10$; entsprechend ist $-10 \equiv 0 \mod 10$ und $-10 \equiv 1 \mod 11$. Also ist

$$x = 5 \cdot 11 - 9 \cdot 10 = -35$$

eine Lösung; die allgemeine Lösung ist $-35 + 110k$ mit $k \in \mathbb{Z}$. Die kleinste positive Lösung ist $-35 + 110 = 75$.

Unser Ausgangssystem ist somit äquivalent zu den beiden Kongruenzen

$$x \equiv 75 \mod 110 \quad \text{und} \quad x \equiv 6 \mod 13\,.$$

Um es zu lösen, müssen wir zunächst die Eins als Linearkombination von 110 und 13 darstellen. Hier bietet sich keine offensichtliche Lösung an, also verwenden wir den erweiterten EUKLIDischen Algorithmus:

$$110 : 13 = 8 \text{ Rest } 6 \Longrightarrow 6 = 110 - 8 \cdot 13$$

$$13 : 6 = 2 \text{ Rest } 1 \Longrightarrow 1 = 13 - 2 \cdot 6 = 17 \cdot 13 - 2 \cdot 110$$

Also ist $17 \cdot 13 = 221 \equiv 1 \mod 110$ und $\equiv 0 \mod 13$; genauso ist $-2 \cdot 110 = 220 \equiv 1 \mod 13$ und $\equiv 9 \mod 110$. Eine ganzzahlige Lösung unseres Problems ist somit

$$75 \cdot 221 - 6 \cdot 220 = 15\,255\,.$$

Die allgemeine Lösung ist

$$15\,255 + k \cdot 110 \cdot 13 = 15\,255 + 1\,430k \quad \text{mit} \quad k \in \mathbb{Z}\,.$$

Da $15\,255 : 1\,430 = 10$ Rest 955 ist, hatte der General also 955 Soldaten vor sich stehen.

Alternativ läßt sich die Lösung eines Systems aus r Kongruenzen auch in einer geschlossenen Form 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, berechnen wir zunächst für jedes i das Produkt

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

der sämtlichen übrigen m_j und bestimmen 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, müssen wir also noch modulo diesem Produkt reduzieren.

Im obigen Beispiel wäre

$$\begin{array}{lll} m_1 = 10 & \widehat{m}_1 = 11 \cdot 13 = 143 & 1 = 43 \cdot 10 - 3 \cdot 143 \\ m_2 = 11 & \widehat{m}_2 = 10 \cdot 13 = 130 & 1 = -59 \cdot 11 + 5 \cdot 130 \\ m_3 = 13 & \widehat{m}_3 = 10 \cdot 11 = 110 & 1 = 17 \cdot 13 - 2 \cdot 110 \,, \end{array}$$

also

$$x = -3 \cdot 143 \cdot 5 + 5 \cdot 130 \cdot 9 - 2 \cdot 110 \cdot 6 = -2145 + 5850 - 1320 = 2385 \,.$$

Modulo $10 \cdot 11 \cdot 13$ erhalten wir natürlich auch hier wieder 955.

Damit kennen wir nun auch zwei konstruktive Beweise des chinesischen Restesatzes und wissen, wie man Systeme von Kongruenzen mit Hilfe des erweiterten EUKLIDischen Algorithmus lösen kann.

§ 7: Prime Restklassen

Wie wir gesehen haben, können wir auch in $\mathbb{Z}/m$ im allgemeinen nicht dividieren. Allerdings ist Division doch sehr viel häufiger möglich als in den ganzen Zahlen. Dies wollen wir als nächstes genauer untersuchen:

Lemma: Zu zwei gegebenen natürlichen Zahlen a, m gibt es genau dann ein $x \in \mathbb{N}$, so daß $ax \equiv 1 \bmod m$, wenn ggT$(a, m) = 1$ ist.

Beweis: Wenn es ein solches x gibt, gibt es dazu ein $y \in \mathbb{N}$, so daß $ax = 1 + my$, d.h. $1 = ax - my$. Damit muß jeder gemeinsame Teiler von a und m Teiler der Eins sein, a und m sind also teilerfremd.

Sind umgekehrt a und m teilerfremd, so gibt es nach dem erweiterten EUKLIDischen Algorithmus $x, y \in \mathbb{Z}$ mit $ax + my = 1$. Durch (gegebenenfalls mehrfache) Addition der Gleichung $am - ma = 0$ läßt sich nötigenfalls erreichen, daß a positiv wird, und offensichtlich ist $ax \equiv 1 \bmod m$. ∎

Definition: Ein Element $a \in \mathbb{Z}/m$ heißt prime Restklasse, wenn ggT$(a, m) = 1$ ist.

Nach dem gerade bewiesenen Lemma gibt es somit zu jeder primen Restklasse a ein $x \in \mathbb{Z}/m$, so daß dort $ax = 1$ ist. Damit ist das folgende Lemma nicht verwunderlich:

Lemma: Die primen Restklassen aus $\mathbb{Z}/m$ bilden bezüglich der Multiplikation eine Gruppe.

Beweis: Wir müssen uns zunächst überlegen, daß das Produkt zweier primer Restklassen wieder eine prime Restklasse ist. Sind $a, b \in \mathbb{Z}/m$ beide teilerfremd zu m, so auch ab, denn wäre p ein gemeinsamer Primteiler von ab und m, so wäre p als Primzahl auch Teiler von a oder b, also gemeinsamer Teiler von a und m oder von b und m. Die Eins ist natürlich eine prime Restklasse, und auch die Existenz von Inversen ist kein Problem: Nach dem vorigen Lemma gibt es ein $x \in \mathbb{Z}$, so daß $ax \equiv 1 \bmod m$ ist, und die andere Richtung dieses Lemmas zeigt, daß auch $x \bmod m$ eine prime Restklasse ist. Das Assoziativgesetz der Multiplikation gilt für alle Elemente von $\mathbb{Z}/m$, erst recht also für die primen Restklassen. ∎

Definition: Die Gruppe $(\mathbb{Z}/m)^\times$ der primen Restklassen heißt *prime Restklassengruppe,* ihre Ordnung wird mit $\varphi(m)$ bezeichnet. $\varphi : \mathbb{N} \to \mathbb{N}$ heißt EULERsche φ-Funktion.

LEONHARD EULER (1707–1783) wurde in Basel geboren und ging auch dort zur Schule und, im Alter von 14 Jahren, zur Universität. Dort legte er zwei Jahre später die Magisterprüfung in Philosophie ab und begann mit dem Studium der Theologie; daneben hatte er sich seit Beginn seines Studium unter Anleitung von JOHANN BERNOULLI mit Mathematik beschäftigt. 1726 beendete er sein Studium in Basel und bekam eine Stelle an der Petersburger Akademie der Wissenschaften, die er 1727 antrat. Auf Einladung FRIEDRICHS DES GROSSEN wechselte er 1741 an die preußische Akademie der Wissenschaften; nachdem sich das Verhältnis zwischen den beiden dramatisch verschlechtert hatte, kehrte er 1766 nach St. Petersburg zurück. Im gleichen Jahr erblindete er vollständig; trotzdem schrieb er rund die Hälfte seiner zahlreichen Arbeiten (Seine gesammelten Abhandlungen umfassen 73 Bände) danach. Sie enthalten bedeutende Beiträge zu zahlreichen Teilgebieten der Mathematik, Physik, Astronomie und Kartographie.

Lemma: *a)* Für zwei zueinander teilerfremde Zahlen $n, m \in \mathbb{N}$ ist $\varphi(nm) = \varphi(n)\varphi(m)$.
b) Für $m = \prod_{i=1}^{r} p_i^{e_i}$ ist $\varphi(m) = \prod_{i=1}^{r} \left(p_i^{e_i-1}(p_i - 1)\right)$.

Beweis: a) Eine Zahl a ist genau dann teilerfremd zum Produkt nm, wenn a mod n teilerfremd zu n und a mod m teilerfremd zu m ist. Da nach dem chinesischen Restesatz $\mathbb{Z}/nm \cong \mathbb{Z}/n \times \mathbb{Z}/m$ ist, ist daher auch $(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$.

b) Wegen *a)* genügt es, dies für Primzahlpotenzen p^e zu beweisen. Eine Zahl a ist genau dann teilerfremd zu p^e, wenn sie kein Vielfaches von p ist. Unter den Zahlen von 1 bis p^e gibt es genau p^{e-1} Vielfache von p, also ist $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. ∎

Korollar: $\mathbb{Z}/m$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Beweis: Das einzige, was $\mathbb{Z}/m$ zu einem Körper eventuell fehlt, ist die Existenz von multiplikativen Inversen für alle von null verschiedenen Elemente. Dies ist offenbar äquivalent zur Formel $\varphi(m) = m - 1$, und die gilt nach dem Lemma genau dann, wenn m prim ist. ∎

Der Körper $\mathbb{Z}/p$ mit p Elementen wird üblicherweise mit $\mathbb{F}_p$ bezeichnet; die zugehörige prime Restklassengruppe $(\mathbb{Z}/p)^\times = \mathbb{F}_p \setminus \{0\}$ entsprechend als $\mathbb{F}_p^\times$. Dabei steht das „$\mathbb{F}$“ für *finit*. Im Englischen werden endliche Körper gelegentlich auch als *Galois fields* bezeichnet, so daß man hier auch die Abkürzung GF(p) sieht. *Field* ist das englische Wort für Körper; das gelegentlich in Informatikbüchern zu lesende Wort *Galoisfeld* ist also ein Übersetzungsfehler.

Wir wollen uns als nächstes überlegen, daß die multiplikative Gruppe dieses Körpers aus den Potenzen eines einzigen Elements besteht. Dazu brauchen wir zunächst noch ein Lemma aus der Gruppentheorie:

Definition: Die Ordnung eines Elements a einer (multiplikativ geschriebenen) Gruppe G ist die kleinste natürliche Zahl r, für die a^r gleich dem Einselement ist. Falls es keine solche Zahl gibt, sagen wir, a habe unendliche Ordnung.

Lemma (LAGRANGE): In einer endlichen Gruppe teilt die Ordnung eines jeden Elements die Gruppenordnung.

Beweis: Die Potenzen des Elements a bilden zusammen mit der Eins eine Untergruppe H von G, deren Elementanzahl gerade die Ordnung r von H ist. Wir führen auf G eine Äquivalenzrelation ein durch die Vorschrift $g \sim h$, falls gh^{-1} in H liegt. Offensichtlich besteht die Äquivalenzklasse eines jeden Elements $g \in G$ aus genau r Elementen, nämlich $g, ga, \ldots, ga^{r-1}$. Da G die Vereinigung aller Äquivalenzklassen ist, muß die Gruppenordnung somit ein Vielfaches von r sein. ∎

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

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

Korollar: Für zwei zueinander teilfremde Zahlen a, m ist

$$a^{\varphi(m)} \equiv 1 \bmod m\,.$$

Beweis: Klar, denn $\varphi(m)$ ist die Ordnung der primen Restklassengruppe modulo m. ∎

Für eine Primzahl $N = p$ bezeichnet man diese Aussage auch als den *kleinen Satz von* FERMAT:

Satz (FERMAT): Für jede nicht durch die Primzahl p teilbare natürliche Zahl a ist $a^{p-1} \equiv 1 \bmod p$. Für alle $a \in \mathbb{Z}$ ist $a^p \equiv a \bmod p$.

Beweis: Die erste Aussage ist klar, da $\varphi(p) = p - 1$ ist. Für die zweite müssen wir nur noch beachten, daß für durch p teilbare Zahlen a sowohl a^p als auch a kongruent null modulo p sind. ∎

Der französische Mathematiker PIERRE DE FERMAT (1601–1665) wurde in Beaumont-de-Lomagne im Departement Tarn et Garonne geboren. Bekannt ist er heutzutage vor allem für seine 1994 von ANDREW WILES bewiesene Vermutung, wonach die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ keine ganzzahlige Lösung mit $xyz \neq 0$ hat. Dieser „große“ Satzes von FERMAT, von dem FERMAT lediglich in einer Randnotitz behauptete, daß er ihn beweisen könne, erklärt den Namen der obigen Aussage. Obwohl FERMAT sich sein Leben lang sehr mit Mathematik beschäftigte und wesentliche Beiträge zur Zahlentheorie, Wahrscheinlichkeitstheorie und Analysis lieferte, war er hauptberuflich Jurist.

Satz: Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.

Beweis: Da die multiplikative Gruppe eines Körpers mit q Elementen aus allen Körperelementen außer der Null besteht, hat sie die Ordnung $q-1$, d.h. nach LAGRANGE ist die Ordnung eines jeden Elements ein Teiler

von $q - 1$. Wir müssen zeigen, daß es mindestens ein Element gibt, dessen Ordnung *genau* $q - 1$ ist.

Für jeden Primteiler p_i von $q - 1$ hat die Polynomgleichung

$$x^{(q-1)/p_i} = 1$$

höchstens $(q - 1)/p_i$ Lösungen im Körper; es gibt also zu jedem p_i ein Körperelement a_i mit $a_i^{(q-1)/p_i} \neq 1$.

q_i sei die größte Potenz von p_i, die $q - 1$ teilt, und $g_i = a_i^{(q-1)/q_i}$ die $(q - 1)/q_i$-te Potenz von a_i. Dann ist

$$g_i^{q_i} = a_i^{q-1} = 1 \quad \text{und} \quad g_i^{\frac{q_i}{p_i}} = a_i^{\frac{q-1}{p_i}} \neq 1\,;$$

g_i hat also die Ordnung q_i. Da die verschiedenen q_i Potenzen verschiedener Primzahlen p_i sind, hat daher das Produkt g aller g_i das Produkt aller q_i als Ordnung, also $q - 1$. Damit ist die multiplikative Gruppe des Körpers zyklisch. ∎

Definition: Ein Element g eines endlichen Körpers k heißt *primitive Wurzel*, wenn es die zyklische Gruppe $k^\times$ erzeugt.

Selbst im Fall der Körper $\mathbb{F}_p$ gibt es keine Formel, mit der man eine solche primitive Wurzel explizit in Abhängigkeit von p angeben kann. Üblicherweise wählt man zufällig ein Element aus und testet, ob es die Ordnung $p - 1$ hat. Die Wahrscheinlichkeit dafür ist offenbar $\varphi(p - 1) : (p - 1)$, was für die meisten Werte von p recht gut ist. Der Test, ob die Ordnung gleich $p - 1$ ist, läßt sich allerdings nur dann effizient durchführen, wenn die Primteiler p_i von $p - 1$ bekannt sind, denn dann kann man einfach testen, ob alle Potenzen mit den Exponenten $(p - 1)/p_i$ von eins verschieden sind. Für große Werte von p, wie sie in der Kryptographie benötigt werden, kann dies ein Problem sein, so daß man hier im allgemeinen von faktorisierten Zahlen r ausgeht und dann testet, ob $r + 1$ prim ist. Im Kapitel über Primzahlen werden wir geeignete Tests kennenlernen.

Kapitel 6
Quadratische Zahlkörper

Ein Zahlkörper ist ein Körper K, der den Körper $\mathbb{Q}$ der rationalen Zahlen enthält und als $\mathbb{Q}$-Vektorraum endlichdimensional ist. Im zweidimensionalen Fall reden wir von quadratischen Zahlkörpern. Die algebraische Zahlentheorie untersucht die (noch zu definierenden) ganzen Zahlen eines solchen Zahlkörpers. In dieser Vorlesung geht es zwar eher um elementare als um algebraische Zahlentheorie, jedoch werden wir im nächsten Kapitel sehen, daß ein Umweg über quadratische Zahlen auch bei rein ganzzahligen Problemen gelegentlich hilfreich sein kann.

§ 1: Grundbegriffe der Ringtheorie

Als erstes wollen wir uns überlegen, in welchen Zahlbereichen außer $\mathbb{Z}$ wir noch sinnvoll von Teilbarkeit und eventuell auch Division mit Rest reden können. Wir brauchen dazu selbstverständlich zumindest eine Addition und eine Multiplikation, d.h. einen der bereits im ersten Kapitel definierten *Ringe*. Wenn wir eindeutige Quotienten wollen, müssen wir aber noch zusätzlich voraussetzen, daß es keine sogenannten *Nullteiler* gibt, d.h. von null verschiedene Elemente r, s, deren Produkt gleich null ist. Ist nämlich $y = qs$, so ist dann auch $y = (q + r)s$, was unserer Vorstellung von Teilbarkeit mit eindeutig bestimmtem Quotienten widerspricht.

Definition: *a)* Ein Ring heißt *nullteilerfrei* wenn gilt: Ist $x \cdot y = 0$, so muß mindestens einer der beiden Faktoren x, y verschwinden. Ein nullteilerfreier kommutativer Ring heißt *Integritätsbereich* (englisch *domain*).

b) 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 $x = q \cdot u$.
c) $u \in R$ 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: $v|u$.
d) Ein Element $e \in R$ heißt *Einheit*, falls es ein $e' \in R$ gibt mit $e \cdot e' = 1$. Die Menge aller Einheiten von R bezeichnen wir mit $R^\times$.
e) Zwei Elemente $x, y \in R$ heißen assoziiert, wenn es eine Einheit $e \in R$ gibt, so daß $y = e \cdot x$.

Der Prototyp eines kommutativen Rings ist der Ring $\mathbb{Z}$ der ganzen Zahlen; er ist ein Integritätsbereich mit ± 1 als einzigen Einheiten. Zwei ganze Zahlen sind somit genau dann assoziiert, wenn sie denselben Betrag haben.

Der Ring $\mathbb{Z}/m$ ist genau dann nullteilerfrei, wenn m prim ist; in diesem Fall ist er sogar ein Körper. Ist aber $m = ab$ eine Zerlegung (in $\mathbb{N}$) von m in ein Produkt mit $a, b > 1$, so ist in $\mathbb{Z}/m$ zwar $ab = 0$, aber $a, b \neq 0$.

Der Menge aller $n \times n$-Matrizen über einem Körper ist ein Beispiel eines nichtkommutativen Rings. Er ist nicht nullteilerfrei, enthält aber viele invertierbare Elemente.

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

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

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 die folgende *Kürzungsregel* erfüllt ist: Gilt für $x, y, z \in R$ und $z \neq 0$ die Gleichung $xz = yz$, so ist $x = y$.
c) Zwei Elemente x, y eines Integritätsbereich R sind genau dann assoziiert, 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. $y|x$.
Gilt 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 $x = u \prod_{i=1}^{r} p_i^{e_i}$ mit einer Einheit $u \in R^\times$, irreduziblen Elementen $p_i \in R$ und natürlichen Zahlen e_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: Wir wählen zunächst aus jeder Klasse assoziierter irreduzibler Elemente einen Vertreter; für die Zerlegung eines Elements in ein Produkt irreduzibler Elemente reicht es dann, wenn wir nur irreduzible Elemente betrachten, die Vertreter ihrer Klasse sind.

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 entsprechenden 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 $g_i \leq f_i$. ∎

§2: Die Elemente quadratischer Zahlkörper

Ein quadratischer Zahlkörper ist ein Zahlkörper, der als $\mathbb{Q}$-Vektorraum betrachtet die Dimension zwei hat. Es gibt daher ein von der Eins linear unabhängiges Element α. Die drei Elemente $1, \alpha, \alpha^2$ müssen aber linear

abhängig sein; es gibt also rationale p, q, r, so daß $p\alpha^2 + q\alpha + r$ verschwindet. Indem wir mit dem Hauptnenner von p, q, r multiplizieren, erhalten wir eine entsprechende Gleichung mit ganzzahligen Koeffizienten, und wenn wir dann noch durch deren ggT dividieren, erhalten wir teilerfremde ganze Zahlen A, B, C, so daß $A\alpha^2 + B\alpha + C = 0$ ist.

Nach der Lösungsformel für quadratische Gleichungen folgt

$$\alpha = -\frac{B}{2A} \pm \frac{\sqrt{B^2 - 4AC}}{2A} .$$

Den Ausdruck $\Delta = B^2 - 4AC$ unter der Wurzel bezeichnen wir als die *Diskriminante* von α. Für $\alpha = \sqrt{W}$ mit $W \in \mathbb{Z}$ beispielsweise ist $A = 1, B = 0$ und $C = -W$, also $\delta = 4W$. Für $\alpha = \frac{1}{3} + \frac{1}{5}\sqrt{2}$ haben wir die Gleichung

$$\alpha^2 - \frac{2}{3}\alpha + \frac{1}{9} - \frac{2}{25} = \alpha^2 - \frac{2}{3}\alpha + \frac{7}{225} = 0 \Longrightarrow 225\alpha^2 - 150\alpha + 7 = 0 ;$$

hier ist die Diskriminante somit $\Delta = 150^2 - 4 \cdot 225 \cdot 7 = 16200$.

Wegen der Irrationalität von α muß auch $\sqrt{\Delta}$ irrational sein, d.h. Δ ist kein Quadrat. Wegen der Eindeutigkeit der Primzerlegung in $\mathbb{Z}$ können wir ganze Zahlen $Q, D \in \mathbb{Z}$ finden, so daß $\Delta = Q^2 D$ und $\sqrt{\Delta} = Q\sqrt{D}$ ist mit einer quadratfreien Zahl D, d.h. einer Zahl D, die durch keine Quadratzahl ungleich eins teilbar ist. Somit läßt sich α in der Form $r + s\sqrt{D}$ schreiben mit $r, s \in \mathbb{Q}$. Da K als $\mathbb{Q}$-Vektorraum zweidimensional ist, läßt sich jedes Element von K so schreiben, als Vektorraum ist also $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$.

Umgekehrt ist $\mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$ für jedes Nichtquadrat D ein Körper, denn natürlich liegen Summe und Differenz zweier Elemente wieder in diesem Vektorraum und wegen

$$(r + s\sqrt{D})(u + v\sqrt{D}) = (ru + svD) + (rv + su)\sqrt{D}$$

auch das Produkt. Für den Quotienten können wir wie bei den komplexen Zahlen über die dritte binomische Formel argumentieren:

$$\frac{r + s\sqrt{D}}{u + v\sqrt{D}} = \frac{(r + s\sqrt{D})(u - v\sqrt{D})}{(u + v\sqrt{D})(u - v\sqrt{D})} = \frac{ru + svD}{u^2 - v^2 D} + \frac{rv + su}{u^2 - v^2 D} .$$

Wir bezeichnen diesen Körper kurz mit $K = \mathbb{Q}[\sqrt{D}]$.

Für $D > 0$ ist $\mathbb{Q}[\sqrt{D}]$ ein Teilkörper von $\mathbb{R}$; wir reden in diesem Fall von einem *reellquadratischen* Zahlkörper. Falls $D < 0$, gibt es in $\mathbb{Q}[\sqrt{D}]$ auch imaginäre Elemente; hier reden wir von einem *imaginärquadratischen* Zahlkörper.

§3: Die Hauptordnung eines Zahlkörpers

Jede rationale Zahl ist Lösung einer linearen Gleichung $aX + b = 0$ mit ganzzahligen Koeffizienten a, b, von denen der erste nicht verschwinden darf; sie ist genau dann eine ganze Zahl, wenn man $a = 1$ wählen kann.

Entsprechend ist jedes Element x eines Zahlkörpers K Lösung einer Polynomgleichung

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = 0 \quad \text{mit} \quad a_i \in \mathbb{Z} ,$$

denn da K nach Definition ein endlichdimensionaler $\mathbb{Q}$-Vektorraum ist, können die Potenzen von x nicht allesamt linear unabhängig sein. Es gibt also für irgendein n eine lineare Abhängigkeit

$$\lambda_n x^n + \lambda_{n-1} x^{n-1} + \cdots + \lambda_1 x + \lambda_0 = 0 \quad \text{mit} \quad \lambda_i \in \mathbb{Q} .$$

Multiplikation mit dem Hauptnenner der Koeffizienten λ_i macht daraus eine Polynomgleichung mit ganzzahligen Koeffizienten.

Definition: Eine Element x eines Zahlkörpers K heißt *ganz*, wenn es einer Polynomgleichung

$$X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = 0$$

mit ganzzahligen Koeffizienten $a_i \in \mathbb{Z}$ und höchstem Koeffizienten eins genügt.

Man kann relativ einfach zeigen, daß die ganzen Zahlen in einem Zahlkörper K einen Ring bilden; da wir uns hier aber auf quadratische Zahlkörper beschränken, bei denen wir dies ganz explizit sehen können, sie hier auf einen solche Beweis verzichtet.

Wir betrachten also einen quadratischen Zahlkörper $K = \mathbb{Q}[\sqrt{D}]$. Ein Element $\alpha = r + s\sqrt{D}$ mit $r, s \in \mathbb{Z}$ ist genau dann ganz, wenn es einer Gleichung der Form $x^2 + ax + b$ mit $a, b \in \mathbb{Z}$ genügt. Da

$$x^2 = (r + s\sqrt{D})^2 = (r^2 + s^2 D) + 2rs\sqrt{D}$$

ist, genügt x der Gleichung

$$x^2 - 2rx + (r^2 - s^2 D) = 0\,.$$

Somit müssen $c = 2r$ und $d = r^2 - s^2 D$ ganze Zahlen sein.

Für $r \in \mathbb{Z}$ ist die erste Bedingung trivialerweise erfüllt und die zweite genau dann, wenn auch s eine ganze Zahl ist: Da D keinen Nenner hat, ist der Nenner von $r^2 - s^2 D$ in diesem Fall das Quadrat des Nenners von s.

Falls r keine ganze Zahl ist, muß es wegen der ersten Bedingung von der Form $r = c/2$ sein mit einer ungeraden Zahl r. Notwendige Bedingung für die Ganzheit von $r^2 - s^2 D$ ist dann, daß auch $s = e/2$ von dieser Form ist. Dann ist

$$r^2 - s^2 D = \frac{c^2 - e^2 D}{4} \in \mathbb{Z} \Longrightarrow c^2 - e^2 D \equiv 0 \bmod 4\,.$$

c und e sind ungerade Zahlen; ihre Quadrate sind also kongruent eins modulo vier. Somit ist $r^2 - s^2 D$ genau dann ganz, wenn $D \equiv 1 \bmod 4$ ist.

In $\mathbb{Q}[\sqrt{D}]$ ist ein Element $r + s\sqrt{D}$ daher für $D \not\equiv 1 \bmod 4$ genau dann ganz, wenn r und s beide ganz sind; die Menge der ganzen Zahlen ist also $\mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$. Diese Menge ist offensichtlich eine abelsche Gruppe bezüglich der Addition, und da das Quadrat von $\sqrt{D}$ die ganze Zahl D ist, ist sie auch abgeschlossen bezüglich der Multiplikation; die ganzen Zahlen bilden also einen Ring.

Im Fall $D \equiv 1 \bmod 4$ ist $r + s\sqrt{D}$ auch noch dann ganz, wenn r und s beide die Hälfte einer ungeraden Zahl sind. Insbesondere ist also auch

$$\beta_D = \frac{1 + \sqrt{D}}{2}$$

eine ganze Zahl, und offensichtlich sind die ganzen Zahlen genau die Zahlen, die sich als $u + \beta_D$ mit $u, v \in \mathbb{Z}$ schreiben lassen. Die Menge der ganzen Zahlen ist also $\mathbb{Z} \oplus \mathbb{Z}\beta_D$. Auch dies ist ein Ring, denn

$$\beta_D^2 = \frac{1 + 2\sqrt{D} + D}{4} = \frac{D-1}{4} + \frac{1 + \sqrt{D}}{2} = \frac{D-1}{4} + \beta_D$$

liegt wieder in dieser Menge, da $(D-1)/4$ im Fall $D \equiv 1 \bmod 4$ eine ganze Zahl ist.

Die ganzen Zahlen in $\mathbb{Q}[\sqrt{D}]$ bilden also in jedem Fall einen Ring; diesen Ring bezeichnen wir als die *Hauptordnung* $\mathcal{O} = \mathcal{O}_D$ von $\mathbb{Q}[\sqrt{D}]$. Wie wir gerade gesehen haben, ist also

$$\mathcal{O}_D = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}\sqrt{D} & \text{falls } D \not\equiv 1 \bmod 4 \\ \mathbb{Z} \oplus \mathbb{Z}\beta_D \;\text{ mit }\; \beta_D = \frac{1}{2}(1 + \sqrt{D}) & \text{falls } D \equiv 1 \bmod 4 \end{cases}.$$

Beim Körper $K = \mathbb{Q}[i]$ der komplexen Zahlen mit rationalem Real- und Imaginärteil ist $D = -1 \equiv 3 \bmod 4$, also ist die Hauptordnung hier einfach $\mathcal{O}_{-1} = \mathbb{Z} \oplus \mathbb{Z}i$, die sogenannten ganzen GAUSSschen Zahlen. Für $D = -3 \equiv 1 \bmod 4$ dagegen ist auch $\beta_{-3} = \frac{1}{2}(1 + \sqrt{-3})$ eine ganze Zahl und $\mathcal{O}_{-3} = \mathbb{Z} \oplus \mathbb{Z}\beta_{-3}$.

Dieses Beispiel wirft die Frage auf, ob unsere Definition ganzer Zahlen wirklich so geschickt war: Wir hätten schließlich auch einfach definieren können, daß $r + s\sqrt{D}$ genau dann ganz heißen soll, wenn r und s ganze Zahlen sind.

Einer der Gründe ist sicherlich, daß wir in nichtquadratischen Zahlkörpern keine ausgezeichneten Elemente wie $\sqrt{D}$ haben, und selbst im quadratischen Fall ist $\sqrt{D}$ nicht immer das einzige ausgezeichnete Element. Im Falle $D = -3$ beispielsweise ist $\beta_{-3} = \frac{1}{2}(1 + \sqrt{-3})$ eine primitive sechste Einheitswurzel, und es gibt keinen Grund, diese als „weniger ganz“ oder „weniger ausgezeichnet“ zu betrachten als $\sqrt{-3}$.

Viel wichtiger ist aber, daß wir nur bei dieser Definition der Ganzheit eine Chance auf eindeutige Primzerlegung in der Hauptordnung haben:

Definition: *a)* Sind $R \leq S$ Integritätsbereiche, so heißt ein Element $x \in S$ ganz über R, wenn es einer Gleichung

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 = 0 \quad \text{mit} \quad r_i \in R$$

genügt.
b) R heißt ganzabgeschlossen oder normal, wenn jedes über R ganze Element des Quotientenkörpers K von R in R liegt.

Satz: Ein faktorieller Ring ist ganzabgeschlossen.

Beweis: Jedes Element x des Quotientenkörpers eines Rings R kann als Quotient $x = p/q$ mit $p, q \in R$ dargestellt werden. Falls R faktoriell ist, können wir dabei annehmen, daß p und q teilerfremd sind. x ist genau dann ganz über R, wenn es ein $n \in \mathbb{N}$ und Elemente $r_0, \ldots, r_{n-1} \in R$ gibt derart, daß

$$x^n = -r_{n-1}x^{n-1} - \cdots - r_1 x - r_0$$

ist. Multiplikation mit q^n macht daraus die Gleichung

$$p^n = -r_{n-1}p^{n-1}q - \cdots - r_1 pq^{n-1} - r_o q^n \,.$$

Hier ist die rechte Seite durch q teilbar, also auch die linke. Da p und q als teilerfremd vorausgesetzt war, ist das nur möglich, wenn q eine Einheit ist, d.h. $x = p/q$ liegt in R. ∎

§4: Normen und Spuren in quadratischen Zahlkörpern

Beginnen wir mit einem Beispiel: Die Hauptordnung von $K = \mathbb{Q}[\sqrt{-5}]$ ist $\mathcal{O}_{-5} = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{-5}]$, und dort haben wir die beiden Produktzerlegungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \,.$$

Folgt daraus, daß $\mathcal{O}_{-5}$ nicht faktoriell ist?

Bevor wir diese Frage beantworten können, müssen wir zunächst wissen, ob möglicherweise die Faktoren auf der rechten Seite noch weiter zerlegt werden können. Solche Fragen lassen sich oft entscheiden, indem man die *Normen* der beteiligten Elemente betrachtet.

Definition: *a)* Für ein Elements $\alpha = r + s\sqrt{D}$ von $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$ heißt $\overline{\alpha} = r - s\sqrt{D}$ das zu α konjugierte Element.
b) Die Norm von α ist

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = (r + s\sqrt{D})(r - s\sqrt{D}) = r^2 - s^2 D \in \mathbb{Q} \,.$$

c) Die Spur von α ist $\quad \mathrm{Sp}(\alpha) = \alpha + \overline{\alpha} = 2r \,.$

Lemma: *a)* Für $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$ ist $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$.
b) Für $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$ ist $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$.
c) $\alpha \in \mathbb{Q}[\sqrt{D}]$ ist Wurzel der quadratischen Gleichung

$$X^2 - \mathrm{Sp}(\alpha)X + \mathrm{N}(\alpha) = 0 \,.$$

d) $\alpha \in \mathbb{Q}[\sqrt{D}]$ ist genau dann ganz, wenn $\mathrm{N}(\alpha)$ und $\mathrm{Sp}(\alpha)$ in $\mathbb{Z}$ liegen.
e) $\alpha \in \mathcal{O}_D$ ist genau dann eine Einheit, wenn $\mathrm{N}(\alpha) = \pm 1$ ist.

Beweis: a) Folgt sofort durch direktes Nachrechnen: Für $\alpha = r + s\sqrt{D}$ und $\beta = u + v\sqrt{D}$ ist

$$\overline{\alpha\beta} = \overline{(ru + svD) + (rv + su)\sqrt{D}} = (ru + svD) - (rv + su)\sqrt{D}$$
$$= (r - s\sqrt{D})(u - v\sqrt{D}) = \overline{\alpha}\overline{\beta} \,.$$

b) Nach Definition ist

$$\mathrm{N}(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha} \cdot \beta\overline{\beta} = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) \,.$$

c) Ist offensichtlich, denn nach dem Satz von VIÈTE sind α und $\overline{\alpha}$ Nullstellen der Gleichung

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - \mathrm{Sp}(\alpha)X + \mathrm{N}(\alpha) = 0 \,.$$

d) folgt sofort aus *c)* und der Definition der Ganzheit.

e) Ist $\alpha \in \mathcal{O}_D^\times$ eine Einheit, so gibt es ein dazu inverses ganzes Element $\beta \in \mathcal{O}_D$, und wegen $\alpha\beta = 1$ ist auch $\mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = 1$. Die Norm ist also eine Einheit von $\mathbb{Z}$, d.h. $\mathrm{N}(\alpha) = \pm 1$.

Ist umgekehrt $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = \pm 1$, so ist $\alpha \cdot (\pm\overline{\alpha}) = 1$, wir haben also ein ganzes Inverses. ∎

Das können wir beispielsweise anwenden auf die eingangs betrachteten Zerlegungen $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. In $\mathbb{Q}[\sqrt{-5}]$ ist

$$\mathrm{N}(2) = 2 \cdot 2 = 4, \quad \mathrm{N}(3) = 3 \cdot 3 = 9, \quad \mathrm{N}(1 \pm \sqrt{-5}) = 1 + 5 = 6 \,.$$

Echte Primteiler einer dieser Zahlen müßten also Norm ± 2 oder ± 3 haben. Wegen

$$\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2$$

müßte für solche Elemente $b = 0$ und $a^2 = 2$ oder 3 sein, was für ein $a \in \mathbb{Q}$ offensichtlich nicht möglich ist. Somit sind die Elemente $2, 3$ und $1 \pm \sqrt{-5}$ allesamt irreduzibel, und die Zahl sechs läßt sich auf zwei verschiedene Weisen als Produkt irreduzibler Elemente schreiben. (Es ist klar, daß 2 und 3 nicht zu $1 \pm \sqrt{-5}$ assoziiert sein können, denn die Normen assoziierter Elemente unterscheiden sich höchstens im Vorzeichen.)

Damit haben wir gezeigt, daß die Hauptordnung von $\mathbb{Q}[\sqrt{-5}]$ nicht faktoriell ist.

§5: Euklidische Ringe

In Kapitel I bewiesen wir die eindeutige Primzerlegung in $\mathbb{Z}$ mit Hilfe des EUKLIDischen Algorithmus. Wenn wir Beispiele für faktorielle Ringe $\mathcal{O}_D$ suchen, liegt es daher nahe, nach Ringen zu suchen, in denen es einen EUKLIDischen Algorithmus gibt. Solche Ringe heißen EUKLIDische Ringe.

Wie wir gesehen haben, ist die Division mit Rest das wichtigste Werkzeug beim EUKLIDischen Algorithmus, 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 $\nu: R \setminus \{0\} \to \mathbb{N}_0$, 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.

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 in Kapitel I mit dem erweiterten EUKLIDischen Algorithmus berechnet werden. ∎

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 $\nu(r) < \nu(x)$.

Als Teiler von x ist y auch Teiler von $r = y - qx = y(1 - qz)$, also muß $\nu(y) \leq \nu(r) < \nu(x)$ sein. 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 x_i.

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: Beispielsweise sind nach einem Satz von GAUSS auch $\mathbb{Z}[X]$ sowie Polynomringe in mehr als einer Veränderlichen über $\mathbb{Z}$ oder einem Körper faktoriell, aber

keiner dieser Ringe ist EUKLIDisch, da sich weder der ggT eins von 2 und X in $\mathbb{Z}[X]$ noch der ggT eins von X und Y in $k[X,Y]$ als Linearkombination der Ausgangselemente schreiben läßt.

Wir interessieren uns in diesem Kapitel vor allem für quadratische Zahlkörper; daher wollen wir uns fragen, wann die Hauptordnung eines solchen Körpers EUKLIDisch ist.

Für einen EUKLIDischen Ring brauchen wir zunächst eine Abbildung ν nach $\mathbb{N}_0$. Für $\mathbb{Z}$ konnten wir einfach den Betrag nehmen; für die Hauptordnung eines quadratischen Zahlkörpers können wir unser Glück versuchen mit dem Betrag der Norm.

Falls die Hauptordnung $\mathcal{O}_D$ von $\mathbb{Q}[\sqrt{D}]$ zusammen mit dieser Abbildung ein EUKLIDischer Ring ist, muß es zu je zwei Elementen $r, s \in \mathcal{O}_D$ mit $s \neq 0$ ein Element $q \in \mathcal{O}_D$ geben, so daß $|\mathrm{N}(r - sq)| < |\mathrm{N}(s)|$ ist. Division durch s macht daraus die Ungleichung

$$\left|\mathrm{N}\left(\frac{r}{s} - q\right)\right| < |\mathrm{N}(1)| = 1\,.$$

Da sich jedes Element von $\mathbb{Q}[\sqrt{D}]$ als so ein Quotient r/s darstellen läßt, muß es also zu jedem $x \in \mathbb{Q}[\sqrt{D}]$ ein $q \in \mathcal{O}_D$ geben, so daß $|\mathrm{N}(x-q)| < 1$ ist. Dies zeig auch, wie man im EUKLIDischen Fall die Division mit Rest durchführt: Man berechnet den Quotienten x/y zunächst im Körper $\mathbb{Q}[\sqrt{D}]$ und nimmt dann das bezüglich der Norm nächstgelegene Element von $\mathcal{O}_D$.

Betrachten wir als Beispiel die Division von $23 + 9i$ durch $2 - 3i$ im Ring $\mathbb{Z}[i]$ der GAUSSschen Zahlen. In $\mathbb{Q}[i]$ ist

$$\frac{23+9i}{2-3i} = \frac{(23+9i)(2+3i)}{13} = \frac{19}{13} + \frac{87}{13}i\,.$$

Da $19 : 13 = 1$ Rest 6 und $87 : 13 = 6$ Rest 9 ist, liegt das Element $1 + 7i$ aus $\mathbb{Z}[i]$ am nächsten bei dieser Zahl. Die Norm von

$$\frac{19}{13} + \frac{87}{13}i - (1+7i) = \frac{6}{13} - \frac{4}{13}i$$

ist $(6^2 + 4^2)/13^2 = 52/169$ und damit deutlich kleiner als eins. Somit ist

$$(23+9i) : (2-3i) = (1+7i) \text{ Rest } -2i$$

ein mögliches Ergebnis der Division mit Rest. Ein anderes wäre

$$(23+9i) : (2-3i) = (1+6i) \text{ Rest } 3\,,$$

denn auch die Norm von 3 ist kleiner als die von $2+3i$. (Der Rest wurde jeweils als Dividend minus Divisor mal Quotient berechnet.) Da in der Definition eines EUKLIDischen Rings von Eindeutigkeit keine Rede war, ist dies kein Problem. (Auch beim EUKLIDischen Algorithmus wird nie gebraucht, daß das Ergebnis der Division mit Rest eindeutig ist; in der Tat läßt sich der sogar für $\mathbb{Z}$ gelegentlich dadurch etwas beschleunigen, daß man bei der Division mit Rest auch negative Reste zuläßt und stets das Ergebnis nimmt, bei dem der Betrag des Rests minimal ist.)

Um zu sehen, in welchen der Ringe $\mathcal{O}_D$ eine solche Division mit Rest stets möglich ist, betrachten wir die Situation geometrisch. Wir beschränken uns dabei zunächst auf den imaginärquadratischen Fall.

Um besser zu sehen, welche Terme in den folgenden Rechnungen positiv und welche negativ sind, schreiben wir den Körper als $\mathbb{Q}[\sqrt{-D}]$ mit $D > 0$; seine Elemente lassen sich dann in der Form $x+iy\sqrt{D}$ darstellen, wobei $i = \sqrt{-1}$ die imaginäre Einheit bezeichnet.

Wir betrachten $\mathbb{Q}[\sqrt{-D}]$ als Teilmenge der komplexen Zahlenebene $\mathbb{C}$; dann ist

$$\mathrm{N}(r + is\sqrt{D}) = (r + is\sqrt{D})(r - is\sqrt{D}) = r^2 + s^2 D = \left|r + is\sqrt{D}\right|^2$$

einfach das Quadrat des üblichen komplexen Betrags. $\mathcal{O}_{-D}$ ist also genau dann ein EUKLIDischer Ring mit der Norm als Betragsfunktion, wenn es zu jedem Element $x \in \mathbb{Q}[\sqrt{-D}]$ ein $q \in \mathcal{O}_{-D}$ gibt, so daß $|x - q| < 1$ ist. Da $\mathbb{Q}[\sqrt{-D}]$ dicht in $\mathbb{C}$ liegt, müssen dazu die Kreisscheiben mit Radius eins um die Punkte aus $\mathcal{O}_{-D}$ die ganze komplexe Zahlenebene überdecken. Bei den Punkten, die nur auf Rändern solcher Kreisscheiben liegen, muß zudem überprüft werden, daß sie nicht in $\mathbb{Q}[\sqrt{-D}]$ liegen: Andernfalls sind das Körperelemente, für die obige Ungleichung nicht erfüllt ist.

Die Punkte aus $\mathcal{O}_D$ bilden ein Gitter in $\mathbb{C}$; für jeden der Gitterpunkte $q \in \mathcal{O}_D$ definieren wir dessen *Wirkungsbereich* oder VORONOI-Bereich

als den Abschluß der Menge aller $z \in \mathbb{C}$, die näher bei q liegen als bei jedem der anderen Gitterpunkte:

$$W(q) = \left\{ z \in \mathbb{C} \;\middle|\; \forall q' \in \mathcal{O}_{-D} : |z-q| \le |z-q'| \right\}$$

Offensichtlich liegt jedes $z \in \mathbb{C}$ in mindestens einem dieser Wirkungsbereiche, und falls

$$W(q) \subseteq \left\{ z \in \mathbb{C} \;\middle|\; |z-q| < 1 \right\},$$

folgt insbesondere, daß jedes Element von $\mathbb{Q}[\sqrt{-D}]$ im Innern einer Kreisscheibe mit Radius eins um einen Gitterpunkt liegt: Dann ist der Ring $\mathcal{O}_{-D}$ EUKLIDisch.

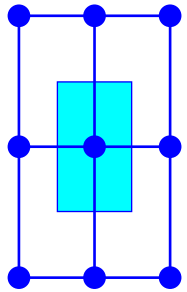
Der Wirkungsbereich eines Gitterpunkts z unterscheidet sich von dem des Nullpunkts nur durch eine Verschiebung um z; entsprechendes gilt auch für die Kreise mit Radius eins um die beiden Punkte. Daher reicht es, zu untersuchen, wann der Wirkungsbereich des Nullpunkts ganz im Innern des Einheitskreises liegt.

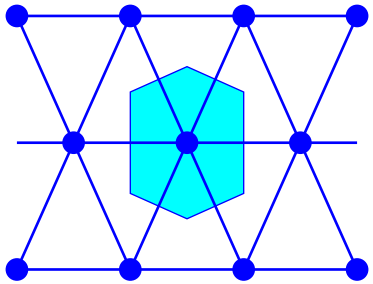
Die Struktur des Wirkungsbereichs hängt ab von $D \bmod 4$: Falls $D \not\equiv -1 \bmod 4$, d.h. $D \not\equiv 3 \bmod 4$, ist $\mathcal{O}_{-D} = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{-D}]$. In der komplexen Zahlenebene bilden diese Punkte ein Rechteckgitter mit den Gitterpunkten $q = r + is\sqrt{D}$ zu $r, s \in \mathbb{Z}$. Der Wirkungsbereich des Nullpunkts ist daher das Rechteck mit Ecken $\pm\frac{1}{2} \pm \frac{i}{2}\sqrt{D}$, und die am weitesten von der Null entfernte Punkte sind die Ecken mit Abstand

$$\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{D}}{2}\right)^2} = \frac{\sqrt{1+D}}{2}\,.$$

Dies ist genau dann echt kleiner als eins, wenn $D \le 2$ ist, d.h. $D = 1$ oder $D = 2$.

Für $D = 3$ überdecken zwar die abgeschlossenen Kreisscheiben mit Radius eins um die Gitterpunkte ganz $\mathbb{C}$, aber die gerade betrachteten Eckpunkte sind Elemente des Körpers $\mathbb{Q}[\sqrt{-3}]$, die in keiner offenen Kreisscheibe um einen Gitterpunkt liegen. Das ist allerdings hier kein Problem, denn in $\mathbb{Q}[\sqrt{-3}]$ sind diese Eckpunkte ja selbst Gitterpunkte: Für $D \equiv 3 \bmod 4$ gibt es schließlich mehr ganze Zahlen in $\mathbb{Q}[\sqrt{-D}]$.





Hier wird das Gitter $\mathcal{O}_{-D}$ erzeugt von der Eins und von $\frac{1}{2}(1 + i\sqrt{D})$. Der Nullpunkt hat somit sechs nächste Nachbarn, nämlich ± 1 und $\pm\frac{1}{2} \pm \frac{i}{2}\sqrt{D}$. Die Wirkungsbereiche der Null und von ± 1 werden getrennt durch die Geraden $x = \pm\frac{1}{2}$, und auch für die vier anderen Punkte müssen wir die Mittelsenkrechte zur Verbindungsstrecke betrachten. Diese geht durch den Streckenmittelpunkt, also durch $\pm\frac{1}{4} \pm \frac{i}{4}\sqrt{D}$, und sie steht senkrecht auf dieser Strecke.

Eine Drehung um 90° kann in der komplexen Zahlenebene realisiert werden durch Multiplikation mit i; wir haben also die vier Geraden

$$\left\{ \left(\pm\frac{1}{2} \pm \frac{i}{2}\sqrt{D}\right) + \left(\mp\frac{\sqrt{D}}{2} \pm \frac{i}{2}\right) t \;\middle|\; t \in \mathbb{R} \right\}\,.$$

Zwei der Ecken des Wirkungsbereichs liegen (aus Symmetriegründen) auf der imaginären Achse; Einsetzen in die Geradengleichungen ergibt, daß deren Imaginärteile gleich $\pm\frac{1}{4}(\sqrt{D} + 1/\sqrt{D})$ sind. Die restlichen vier Ecken liegen auf den Geraden $x = \pm\frac{1}{2}$, haben also Realteil $\pm\frac{1}{2}$; hier führt die Rechnung auf die Imaginärteile $\pm\frac{1}{4}(\sqrt{D} - 1/\sqrt{D})$.

Der Abstand dieser Punkte vom Nullpunkt ist

$$\sqrt{\left(\frac{1}{2}\right)^2 + \frac{(\sqrt{D} - 1/\sqrt{D})^2}{16}} = \frac{1}{4}\sqrt{4 + D - 2 + \frac{1}{D}} = \frac{1}{4}\sqrt{2 + D + \frac{1}{D}}\,;$$

dies ist genau dann kleiner als eins, wenn gilt

$$2 + D + \frac{1}{D} < 4^2 = 16 \quad \text{oder} \quad D + \frac{1}{D} < 14\,.$$

Die einzigen $D \equiv 3 \bmod 4$, die dies erfüllen, sind $D = 3, D = 7$ und $D = 11$. Für diese ist auch $\frac{1}{4}(\sqrt{D} + 1/\sqrt{D}) < 1$, so daß dann und nur dann der gesamte Wirkungsbereich der Null im Einheitskreis liegt.

Die einzigen imaginärquadratischen Zahlkörper $\mathbb{Q}[\sqrt{D}]$, deren Hauptordnung bezüglich der Norm EUKLIDsch ist, sind somit die mit

$$D \in \{-1, -2, -3, -7, -11\} ;$$

von diesen wissen wir damit auch, daß ihre Hauptordnung faktoriell ist.

Es ist nicht bekannt, ob es andere $D < 0$ gibt, für die die Hauptordnung bezüglich einer anderen Funktion $\nu\colon \mathcal{O}_D \setminus \{0\} \to \mathbb{N}_0$ EUKLIDisch ist. Bekannt ist aber, daß die einzigen weiteren faktoriellen Hauptordnungen $\mathcal{O}_D$ die sind mit $D \in \{-19, -43, -67, -163\}$: *siehe* H. STARK: A complete determination of the complex fields of class numbers one, *Michigan J. of Math.* **14** (1967), 1–27. Die Methoden seines Beweises liegen deutlich über dem Niveau dieser Vorlesung.

Im reellquadratischen Fall wird die Ungleichung $|\mathrm{N}(z - q)| - 1$ für $z = x + y\sqrt{D}$ und $q = r + s\sqrt{D}$ zu

$$\left|(x - r)^2 - (y - v)^2 D\right| < 1 .$$

Betrachten wir für festes $q = r + s\sqrt{D} \in \mathcal{O}_D$ die Menge Z_q aller $(x, y) \in \mathbb{R}^2$, für die $z = x + y\sqrt{D}$ diese Ungleichung erfüllt, erhalten wir also einen Bereich, der durch Hyperbeln begrenzt wird, und wir müssen zeigen, daß die Vereinigung aller Z_q für $q \in \mathcal{O}_D$ ganz $\mathbb{R}^2$ ist. Durch mühsames Abhaken vieler Einzelfälle folgt aus einer ganzen Reihe von Arbeiten, daß dies genau dann der Fall ist, wenn

$$D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\} .$$

Die letzten offenen Fälle wurden 1950 untersucht in H. CHATLAND, H. DAVENPORT: Euclid's algorithm in real quadratic fields, *Canadian J. Math.* **2** (1950), 289–296; dort sind auch die weiteren Arbeiten zitiert, aus denen zusammen schließlich das obige Ergebnis folgt.

Genau für diese D ist also $\mathcal{O}_D$ EUKLIDisch bezüglich der Norm. Es gibt zahlreiche weitere positive D, für die $\mathcal{O}_D$ faktoriell ist; vermutungsweise sind es sogar unendlich viele. Ob einige dieser Ringe möglicherweise

bezüglich einer anderen Abbildung $\nu\colon R \setminus \{0\} \to \mathbb{N}_0$ EUKLIDisch sind, ist nicht bekannt, und die Nichtexistenz einer solchen Abbildung ist natürlich nur schwer zu beweisen.

§6: Einheiten in quadratischen Zahlkörpern

Ist $x + y\sqrt{D}$ eine Einheit in $\mathcal{O}_D$ (man spricht auch kurz, aber schlampig, von einer Einheit des Zahlkörpers $\mathbb{Q}[\sqrt{D}]$), so muß die Norm $x^2 - Dy^2$ eine Einheit in $\mathbb{Z}$ sein, also gleich ± 1.

Im imaginärquadratischen Fall ist $x^2 - Dy^2$ die Summe zweier positiver Terme; hier kommt also nur der Wert +1 in Frage. Die einzigen ganzzahligen Lösungen sind offensichtlich $(x, y) = (\pm 1, 0)$, sowie im Fall $D = -1$ der GAUSSschen Zahlen $(x, y) = (0, \pm 1)$. Für $D \equiv 1 \bmod 4$ sind auch echt halbzahlige Werte für sowohl x als auch y zugelassen; dies führt offensichtlich nur für $D = -3$ zu weiteren Lösungen, nämlich $x = \pm\frac{1}{2}$ und $y = \pm\frac{1}{2}$. Damit haben wir gezeigt:

Lemma: In einem imaginärquadratischen Zahlkörper $\mathbb{Q}[\sqrt{D}]$ gibt es für $D \neq -1$ und $D \neq -3$ nur die Einheiten ± 1. In $\mathbb{Q}[i]$ gibt es zusätzlich noch die Einheiten $\pm i$, und in $\mathbb{Q}[\sqrt{-3}]$ sind die Einheiten genau die sechsten Einheitswurzeln ± 1 und $\pm\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$. ∎

In reellquadratischen Körpern führt die Bedingung $\mathrm{N}(x) = \pm 1$ auf die Gleichung $x^2 - Dy^2 = \pm 1$ mit einem positiven D; hier können wir nicht ausschließen, daß es unendlich viele Lösungen gibt.

Betrachten wir zunächst den Fall, daß $x^2 - Dy^2 = 1$ ist. Diese Gleichung bezeichnet man als die PELLsche Gleichung.

JOHN PELL (1611–1685) wurde im englischen Sussex geboren und ging auch dort zur Schule. Bereits 1624 begann er sein Studium an der Universität Cambridge; 1628 erhielt er seinen Bachelor und 1630 seinen Master. Danach arbeitete er meist als Lehrer. Von 1654–1658 war er als Diplomat im Auftrag CROMWELLs in Zürich. In einem dort von JOHANN HEINRICH RAHN (1622–1676) verfaßten Buch, an dem PELL wesentlich mitwirkte, ist ein Beispiel der obigen Gleichung zu finden, weshalb sie EULER (1707–1783) nach PELL benannte. Tatsächlich wurde sie wohl erstmalig von dem indischen Mathematiker und Astronom BRAHMAGUPTA (598–670) untersucht; die vollständige Theorie dazu geht

zurück auf LAGRANGE (1736–1813), der die Gleichung als ein Problem bezeichnet, das FERMAT den englischen Mathematikern stellte. Nach seiner Rückkehr aus Zürich wurde PELL Priester. 1663 wählte ihn die Royal Society zum Mitglied, 1675 wurde er deren Vizepräsident.

Mit der PELLschen Gleichung werden wir uns im nächsten Kapitel genauer beschäftigen, und wir werden sehen, daß sie stets unendlich viele Lösungen hat. Als Vorbereitung dazu wollen wir uns hier etwas genauer mit der Struktur der Einheitengruppe beschäftigen. Dazu betrachten wir die Abbildung

$$\lambda\colon \begin{cases} \mathcal{O}_D^\times \to \mathbb{R}^2 \\ \alpha \mapsto (\log|\alpha|, \log|\overline{\alpha}|) \end{cases}$$

Da eine Einheit Norm ± 1 hat, ist $|\alpha| \cdot |\overline{\alpha}| = 1$, das Bild von λ liegt also auf der zweiten Winkelhalbierenden $y = -x$ von $\mathbb{R}^2$. Außerdem sind α und $\overline{\alpha}$ reell, so daß α genau dann im Kern von λ liegt, wenn $\alpha = \pm 1$ ist.

Das Bild von λ ist diskret, denn hat $\lambda(\alpha)$ höchstens den Abstand M vom Nullpunkt, so ist $\log|\alpha| \le M$ und $\log|\overline{\alpha}| \le M$. Ist $\log R = M$, so ist also $|\alpha| \le R$ und $|\overline{\alpha}| \le R$. Damit ist $|\mathrm{Sp}(\alpha)| \le 2R$ und $|\mathrm{N}(\alpha)| \le R^2$. Da Norm und Spur ganzzahlig sind, gibt es also für beide nur endlich viele Möglichkeiten, und da für ein ganzes Element Norm und Spur zusammen mit dem führenden Koeffizienten eins die Koeffizienten der quadratischen Gleichung sind, gibt es auch nur endlich viele quadratische Gleichungen und damit nur endlich viele Möglichkeiten für α.

Somit gibt es im Bild von λ ein Element $\lambda(\alpha) = (r, -r)$ mit *minimalem* $r > 0$. Wir wollen uns überlegen, daß das jeder andere Punkt im Bild ein ganzzahliges Vielfaches davon ist. Da mit $(s, -s)$ auch $(-s, s)$ im Bild liegt, können wir uns dabei auf Punkte $(s, -s)$ mit $s \ge 0$ beschränken.

Für einen solchen Punkt $\lambda(\beta) = (s, -s)$ gibt es jedenfalls ein größtes $n \in \mathbb{N}_0$, so daß $nr \le s$ ist. Dann ist

$$\lambda(\beta\alpha^{-n}) = \lambda(\beta) - n\lambda(\alpha) = (s, -s) - n(r, -r) = (s - nr, nr - s),$$

so daß auch dieser Punkt im Bild liegt. Nach Wahl von n ist aber $0 \le s - nr < r$; wegen der Minimalität von r ist also $s - nr = 0$, d.h. $s = nr$ und $\beta = \alpha^n$.

Damit haben wir bewiesen

Satz: Falls es im reellquadratischen Zahlkörper $K = \mathbb{Q}[\sqrt{D}]$ ein Element aus $\mathcal{O}_D^\times$ gibt, dessen Norm größer als eins ist, gibt es auch ein entsprechendes Element α mit kleinster Norm, und die Einheiten von $\mathcal{O}_D$ sind genau die Elemente $\pm\alpha^n$ mit $n \in \mathbb{Z}$. Insbesondere ist dann die Einheitengruppe unendlich.

■

Im nächsten Kapitel werden wir sehen, daß jeder reellquadratische Zahlkörper eine solche „Grundeinheit“ α hat; die Einheitengruppe eines reellquadratischen Zahlkörpers besteht also stets genau aus den Elemente der Form $\pm\alpha^n$ mit $n \in \mathbb{Z}$ und $\alpha \in \mathcal{O}_D^\times$.

Bevor wir das im einzelnen untersuchen, wollen wir zum Abschluß dieses Kapitels und zur Vorbereitung auf das nächste noch ein Beispiel einer nichtkommutativen Variante eines Zahlkörpers betrachten.

§ 7: Quaternionen

Nachdem durch die komplexen Zahlen $\mathbb{R}^2$ mit der Struktur eines Körpers versehen war, versuchten viele Mathematiker ähnliches auch für $\mathbb{R}^3$ zu erreichen. Natürlich kann weder $\mathbb{R}^3$ noch sonst ein $\mathbb{R}^n$ mit $n > 2$ zu einem Körper gemacht werden, denn ein solcher Körper wäre eine algebraische Erweiterung von $\mathbb{R}$; da aber der algebraische Abschluß von $\mathbb{R}$ gleich $\mathbb{C}$ ist, muß dann $n = 1$ oder $n = 2$ sein.

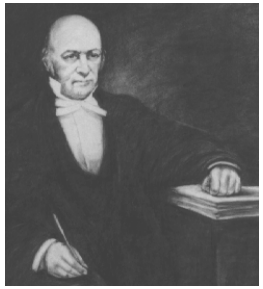
Die damaligen Mathematiker waren jedoch bescheidener: Ihnen genügte es, einfach irgendeine Art von Multiplikation zu finden, die nicht unbedingt allen Körperaxiomen genügte – von Körpern sprach damals ohnehin noch niemand.

Erst 1940 konnte HEINZ HOPF (1894–1971) (auf dem Umweg über Vektorfelder auf Sphären) zeigen werden, daß das nicht möglich ist: Selbst eine bilineare Abbildung $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ kann nur dann existieren, wenn n eine Zweierpotenz ist, und 1958 zeigten dann unabhängig voneinander und mit verschiedenen Methoden JOHN MILNOR und MICHEL KERVAIRE, daß auch noch $n \le 8$ sein muß, so daß nur die vier Möglichkeiten $n = 1, 2, 4$ und 8 in Frage kommen. Genau in diesen Fällen waren auch bereits entsprechende Produkte bekannt:

Für $n = 1$ und 2 haben wir natürlich die reelle *bzw.* komplexe Multiplikation. Den Fall $n = 4$ löste HAMILTON 1843: Er fand eine Multiplikation auf $\mathbb{R}^4$, die zwar nicht kommutativ ist, ansonsten aber alle Körperaxiome erfüllt. Man spricht in so einem Fall von einem *Schiefkörper* oder, in der neueren Literatur, einer *Divisionsalgebra.* HAMILTON bezeichnete seine vierdimensionalen Zahlen als *Quaternionen.* Kurz danach konstruierte ARTHUR CAYLEY (1821–1895) ein nicht-assoziatives Produkt auf $\mathbb{R}^8$; die so erhaltenen „Zahlen“ nannte er *Oktaven.*

HAMILTON wählte eine Basis von $\mathbb{H} = \mathbb{R}^4$, die aus der Eins sowie drei „imaginären Einheiten“ $\mathbf{i}, \mathbf{j}, \mathbf{k}$ besteht, d.h. $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$. Außerdem postulierte er, daß $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ sein sollte; daraus lassen sich dann über das Assoziativgesetz auch die anderen Produkte imaginärer Einheiten berechnen.

Damit ist, wenn man die Gültigkeit des Distributivgesetzes postuliert, eine Multiplikation auf $\mathbb{R}^4$ definiert; der Beweis, daß hierbei alle Körperaxiome außer der Kommutativität der Multiplikation erfüllt sind, enthält wie üblich nur einen etwas schwierigeren Punkt, die Existenz von Inversen; der Rest ist mühsame Abhakerei.



WILLIAM ROWEN HAMILTON (1805–1865) wurde in Dublin geboren; bereits mit fünf Jahren sprach er Latein, Griechisch und Hebräisch. Mit dreizehn begann er, mathematische Literatur zu lesen, mit 21 wurde er, noch als Student, Professor der Astronomie am Trinity College in Dublin. Er verlor allerdings schon bald sein Interesse an der Astronomie und beschäftigte sich stattdessen mit mathematischen und physikalischen Problemen. Am bekanntesten ist er für seine Entdeckung der Quaternionen, vorher publizierte er aber auch bedeutende Arbeiten über Optik, Dynamik und Algebra.

Zum Glück fand CAYLEY 1858 einen einfacheren Weg: Die vier komplexen 2×2-Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ und } K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

erfüllen dieselben Relationen

$$I^2 = J^2 = K^2 = -E \quad \text{und} \quad IJ = -JI = K\,;$$

wir können also die Quaternion $a + bi + cj + dk$ identifizieren mit der Matrix

$$aE + bI + cJ + dK = \begin{pmatrix} a + di & b + ci \\ -b + ci & a - di \end{pmatrix} \in \mathbb{C}^{2\times 2}\,.$$

Da für Matrizen das Assoziativgesetz wie auch das Distributivgesetz gelten, ist klar, daß das Produkt zweier solcher Matrizen wieder von derselben Form ist und daß auch die Quaternionenmultiplikation Assoziativ- und Distributivgesetz erfüllt.

Die Quaternionen entsprechen somit genau den komplexen 2×2-Matrizen der Form

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \quad \text{mit} \quad \alpha = a + di, \beta = b + ci\,.$$

Die Determinante dieser Matrix ist

$$\alpha\overline{\alpha} + \beta\overline{\beta} = a^2 + b^2 + c^2 + d^2\,.$$

Definieren wir in Analogie zum Fall der quadratischen Zahlkörper wieder das konjugierte Element zu $\gamma = a + bi + cj + dk$ als die Quaternion $\overline{\gamma} = a - bi - cj - dk$, so entspricht $\overline{\gamma}$ der Matrix

$$\begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} = (\alpha\overline{\alpha} + \beta\overline{\beta})E\,.$$

Damit folgt insbesondere, daß $\gamma\overline{\gamma}$ eine reelle Zahl ist, die genau dann verschwindet, wenn $\gamma = 0$ ist. Wir bezeichnen diese Zahl wieder als die *Norm* $\mathrm{N}(\gamma)$ der Quaternion γ, und wieder ist $\overline{\gamma}/\mathrm{N}(\gamma)$ das multiplikative Inverse zu γ – sowohl für die Links- wie auch die Rechtsmultiplikation.

$\mathrm{N}(\gamma)$ ist gleichzeitig die Determinante der γ zugeordneten Matrix; aus dem Multiplikationssatz für Determinanten folgt daher sofort die Formel

$$\mathrm{N}(\gamma\delta) = \mathrm{N}(\gamma)\mathrm{N}(\delta)\,.$$