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 imaginärquadratische 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

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

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 $\log|\alpha| \leq M$ und $\log|\overline{\alpha}| \leq M$. Ist $\log R = M$, so ist also $|\alpha| \leq R$ und $|\overline{\alpha}| \leq R$. Damit ist $|\mathrm{Sp}(\alpha)| \leq 2R$ und $|\mathrm{N}(\alpha)| \leq R^2$.

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 $s \geq 0$ beschränken.

Für einen solchen Punkt $\lambda(\beta) = (s, -s)$ gibt es jedenfalls ein größtes $n \in \mathbb{N}_0$, so daß $nr \leq s$ 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 $0 \leq s - nr < r$; 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 eine geeignete Einheit $\alpha \in \mathcal{O}_D^\times$.

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 wurde, 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.

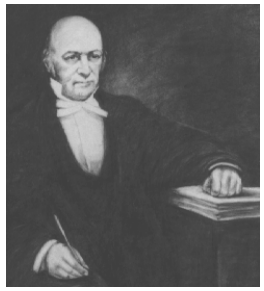
Die damaligen Mathematiker waren jedoch bescheidener: Ihnen genügte es, einfach irgendeine Art von Multiplikation zu finden, die nicht unbedingt den Körperaxiomen genügte – von Körpern sprach damals ohnehin noch niemand.

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 $n \leq 8$ 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 uber 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 für 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

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

Kapitel 5
Quadratische Formen

Eine quadratische Form ist ein Ausdruck der Form

$$F(x, y) = Ax^2 + Bxy + Cy^2 \quad \text{mit} \quad A, B, C \in \mathbb{Z} ;$$

die Zahlentheorie interessiert sich vor allem dafür, welche Werte $F(x, y)$ für $x, y \in \mathbb{Z}$ annimmt.

§ 1: Summen zweier Quadrate

Der einfachste Fall ist die Form $F(x, y) = x^2 + y^2$. Er hängt eng zusammen mit der Hauptordnung $\mathbb{Z}[i]$ von $\mathbb{Q}[i]$, denn

$$x^2 + y^2 = (x + iy)(x - iy)$$

ist die Norm von $x + iy$. Eine ganze Zahl n ist also genau dann als Summe zweier Quadrate darstellbar, wenn sie die Norm einer GAUSSschen ganzen Zahl ist.

Modulo vier ist $0^2 \equiv 2^2 \equiv 0$ und $1^2 \equiv 3^2 \equiv 1$; somit ist jede Summe zweier Quadrate kongruent null, eins oder zwei modulo vier. Eine Zahl kongruent drei modulo vier kann somit nicht als Summe zweier Quadratzahlen auftreten.

Auf der Suche nach positiven Ergebnissen können wir uns auf Primzahlen beschränken, denn wie FIBONACCI bereits im dreizehnten Jahrhundert zeigte, gilt:

Lemma: Sind zwei Zahlen $n, m \in \mathbb{N}$ darstellbar als Summen zweier Quadrate, so gilt dasselbe für ihr Produkt nm.

Beweis: Wenn n und m als Summen zweier Quadrate darstellbar sind, gibt es $\alpha, \beta \in \mathbb{Z}[i]$, so daß $n = \mathrm{N}(\alpha)$ und $m = \mathrm{N}(\beta)$ ist. Wegen der Multiplikativität der Norm ist dann $nm = \mathrm{N}(\alpha\beta)$ ebenfalls eine Norm und damit als Summe zweier Quadrate darstellbar. ∎

(FIBONACCI bewies dieses Lemma natürlich nicht mit Normen GAUSSsche Zahlen; er fand eine explizite Formel für die Darstellung des Produkts als Summe zweier Quadrate. Es handelt sich dabei um dieselbe Formel, zu der wir durch Ausmultiplizieren der Gleichun $\mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) = \mathrm{N}(\alpha\beta)$ für $\alpha = a + ib$ und $\beta = c + id$) kämen.)

Da $2 = 1^2 + 1^2$ als Summe zweier Quadrate darstellbar ist, müssen wir nur die ungeraden Primzahlen untersuchen, und hier wissen wir bereits, daß die Primzahlen kongruent drei modulo vier nicht als solche Summen auftreten.

Satz: Eine ungerade Primzahl p ist genau dann darstellbar als Summe zweier Quadrate, wenn $p \equiv 1 \bmod 4$. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Summanden.

Beweis: Aus Kapitel I, §7 wissen wir, daß die multiplikative Gruppe des Körper $\mathbb{F}_p$ von einem einzigen Element g erzeugt wird. Für $p = 4k + 1$ ist dann $g^{4k} = 1$, also $g^{2k} = -1$. Somit ist $-1 = p - 1$ in $\mathbb{F}_p$ das Quadrat von g^k.

In $\mathbb{Z}$ gibt es daher Zahlen x, für die $x^2 \equiv -1 \bmod p$ ist oder, anders ausgedrückt, $x^2 + 1 = kp$ für ein $k \in \mathbb{N}$. Da jede Restklasse modulo p einen Vertreter mit Betrag kleiner $p/2$ enthält, können wir dabei annehmen, daß $|x| < p/2$ ist; dann ist mit einer geeigneten natürlichen Zahl k

$$x^2 + 1^2 = kp < \frac{p^2}{4} + 1 < \frac{p^2}{2} \Longrightarrow k < p\,.$$

Es gibt also eine natürliche Zahl $1 \le k < p$, so daß kp darstellbar ist als Summe zweier Quadrate. Die kleinste solche Zahl sei m; wir müssen zeigen, daß sie gleich eins ist.

Zunächst ist klar, daß m eine ungerade Zahl sein muß, denn aus der Formel $x^2 + y^2 = mp$ mit geradem m folgt, daß x und y entweder beide

gerade oder beide ungerade sind; $x \pm y$ sind also gerade und

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = \frac{x^2+y^2}{2} = \frac{m}{2}p\,,$$

im Widerspruch zur Minimalität von m.

Falls die Behauptung falsch wäre, müßte somit $m \ge 3$ sein. Wir definieren zwei neue Zahlen u, v durch die Bedingungen

$$|u| < \frac{m}{2}, \quad |v| < \frac{m}{2}, \quad u \equiv x \bmod m \quad \text{und} \quad v \equiv y \bmod m\,.$$

Offensichtlich können nicht beide dieser Zahlen verschwinden, denn sonst wären x und y beide durch m teilbar, also wäre $x^2 + y^2 = mp$ durch m^2 teilbar. Das kann aber nicht sein, denn p ist prim und $m < p$. Weiter ist

$$u^2 + v^2 \equiv x^2 + y^2 = mp \equiv 0 \bmod m\,,$$

also gibt es eine natürliche Zahl ℓ, so daß $u^2 + v^2 = \ell m$ ist. Da $u^2 + v^2$ kleiner ist als $\frac{1}{2}m^2$, ist $\ell < \frac{m}{2}$.

Nach der zu Beginn des Paragraphen zitierten Formel von FIBONACCI, d.h. also durch explizite Berechnung von $(u+iv)(x+iy)$ und Berechnung der Norm davon, erhalten wir die Formel.

$$(\ell m)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2\,.$$

Dabei ist

$$xu + yv \equiv x^2 + y^2 \equiv 0 \bmod m \text{ und } xv - yu \equiv xy - yx \equiv 0 \bmod m\,,$$

beide Zahlen sind also durch m teilbar. Somit gibt es natürliche Zahlen X, Y mit

$$(\ell m)(mp) = m^2\ell p = (mX)^2 + (mY)^2 \quad \text{oder} \quad \ell p = X^2 + Y^2\,.$$

Da $\ell < \frac{m}{2}$, widerspricht dies der Minimalität von m.

Damit haben wir gezeigt, daß $m = 1$ sein muß, d.h. p läßt sich als Summe zweier Quadrate darstellen. Wir müssen uns noch überlegen, daß diese Darstellung bis auf die Reihenfolge der Faktoren eindeutig ist.

Angenommen, es gibt zwei Darstellungen $p = x^2 + y^2 = u^2 + v^2$. In $\mathbb{Z}[i]$ ist dann

$$p = (x + iy)(x - iy) = (u + iv)(u - iv)\,.$$

Alle Faktoren haben Norm p und sind somit irreduzibel, und aus Kapitel IV, §5 wissen wir, daß $\mathbb{Z}[i]$ ein EUKLIDischer, insbesondere also faktorieller Ring ist. Daher unterscheiden sich die beiden Zerlegungen nur durch Einheiten von $\mathbb{Z}[i]$. Auch diese kennen wir aus Kapitel IV: Nach dem Lemma aus §6 sind es genau die Elemente ± 1 und $\pm i$. Somit ist entweder $x^2 = u^2$ und $y^2 = v^2$ oder umgekehrt, womit die Eindeutigkeit bewiesen wäre. ∎

Als erste Anwendung davon können wir die Primzahlen im Ring $\mathbb{Z}[i]$ der GAUSSschen Zahlen bestimmen:

Korollar: Eine Primzahl $p \in \mathbb{N}$ ist genau dann irreduzibel in $\mathbb{Z}[i]$, wenn $p \equiv 3 \bmod 4$. Andernfalls zerfällt sie in das Produkt zweier konjugiert komplexer irreduzibler Elemente $r \pm is$ mit $r^2 + s^2 = p$.

Beweis: $p = 2 = (1+i)(1-i)$ zerfällt offensichtlich, und dies ist bereits die Primzerlegung, denn $N(1 \pm i) = 2$ hat keine echten Teiler.

Falls eine ungerade Primzahl p einen echten Teiler $r + is$ hat, ist sie auch durch $r - is$ teilbar. Da die Norm von p gleich p^2 ist und $r \pm is$ keine Einheiten, muß $N(r \pm is) = p$ sein. Damit folgt zunächst, daß $r \pm is$ prim sind, denn ein echter Teiler müßte als Norm einen echten Teiler von p haben. Außerdem folgt, daß sich $(r + is)(r - is) = r^2 + s^2$ höchstens durch eine Einheit von p unterscheidet; da beides positive Zahlen sind, muß diese aber gleich eins sein, d.h. die Primzerlegung von p in $\mathbb{Z}[i]$ ist

$$p = (r + is)(r - is) = r^2 + s^2 \,.$$

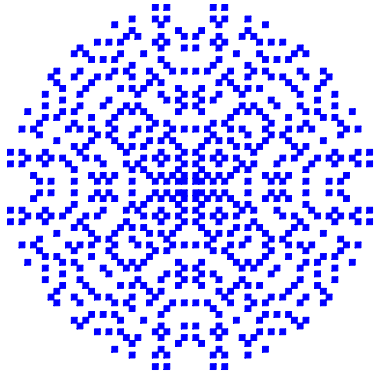
Nach dem Satz ist daher $p \equiv 1 \bmod 4$.

Ist umgekehrt $p \equiv 1 \bmod 4$, so gibt es nach dem Satz zwei ganze Zahlen r, s, so daß $p = r^2 + s^2$ ist, d.h. $p = (r+is)(r-is)$ zerfällt in $\mathbb{Z}[i]$, und das Argument aus dem vorigen Abschnitt zeigt, daß dies die Primzerlegung ist.

Somit zerfallen genau die Primzahlen $p \equiv 1 \bmod 4$ und die Zwei, d.h. genau die $p \equiv 3 \bmod 4$ bleiben prim. ∎

In der Abbildung sind die GAUSSschen Primzahlen $a + ib$ der Norm höchstens 1000 durch Quadrate um den Punkt $(a, b) \in \mathbb{R}^2$ dargestellt.

Mancher Leser wird hier ein gelegentlich von Designern verwendetes Muster erkennen.



Kehren wir zurück zur Ausgangsfrage, wann eine beliebige natürliche Zahl als Summe zweier Quadrate dargestellt werden kann:

Satz: Eine natürliche Zahl n läßt sich genau dann als Summe zweier Quadrate schreiben, wenn jede Primteiler $p \equiv 3 \bmod 4$ mit einer gerader Potenz in der Primzerlegung von n auftritt.

Beweis: Zunächst ist die Bedingung hinreichend, denn da mit n auch jedes Produkt $c^2 n$ als Summe zweier Quadrate darstellbar ist, können wir die Primteiler $p \equiv 3 \bmod 4$ ignorieren. Nach dem gerade bewiesenen Satz wissen wir, daß jede Primzahl $p \equiv 1 \bmod 4$ Summe zweier Quadrate ist, und natürlich gilt dies auch für $2 = 1^2 + 1^2$. Damit ist nach dem obigen Lemma auch jedes Produkt solcher Primzahlen als Summe zweier Quadrate darstellbar.

Umgekehrt sei

$$n = x^2 + y^2 \quad \text{und} \quad d = \mathrm{ggT}(x, y) \,.$$

Mit $x = du$, $y = dv$ und $n = d^2 m$ ist dann $m = u^2 + v^2$, und m enthält genau dann einen Primteiler $p \equiv 3 \bmod 4$ in ungerader Potenz, wenn dies für m der Fall ist. Sei p ein solcher Primteiler. Dann ist p ein Teiler

von

$$u^2 + v^2 = (u + iv)(u - iv)$$

im Ring $\mathbb{Z}[i]$ der GAUSSschen Zahlen. Falls p auch dort eine Primzahl ist, muß es mindestens einen der beiden Faktoren teilen; komplexe Konjugation zeigt, daß es dann auch den anderen teilt. Damit teilt es auch deren Summe $2u$ und Differenz $2iv$; da p ungerade ist und i eine Einheit, teilt p also die zueinander teilerfremden Zahlen u und v, ein Widerspruch.

Somit ist p in $\mathbb{Z}[i]$ keine Primzahl; nach obigem Korollar muß daher $p = 2$ oder $p \equiv 1 \bmod 4$ sein. Damit ist jeder Primteiler $p \equiv 3 \bmod 4$ von n zugleich ein Teiler von d, tritt in n also mit einer geraden Potenz auf. ∎

Für zusammengesetzte Zahlen ist die Darstellung als Summe zweier Quadrate im allgemeinen nicht mehr eindeutig. Über die Primzerlegung in $\mathbb{Z}[i]$ läßt sich die Anzahl verschiedener Darstellungen leicht erkennen: Natürlich entsprechen auch für eine beliebige natürliche Zahl n die Darstellungen als Summe zweier Quadrate den Darstellungen von n als Norm eines Elements von $\mathbb{Z}[i]$, wobei assoziierte Elemente auf dieselbe Zerlegung führen.

Aus der Primzerlegung von n in $\mathbb{Z}$ können wir leicht auf die Primzerlegung in $\mathbb{Z}[i]$ schließen: Primzahlen kongruent drei modulo vier bleiben nach obigem Korollar auch in $\mathbb{Z}[i]$ irreduzibel, die kongruent eins modulo vier sind Produkte zweier konjugierter Elemente $x \pm iy$. Die beiden Faktoren sind nicht assoziert, denn sonst wäre $|x| = |y|$ und $p = x^2 + y^2$ wäre gerade. Die Zwei schließlich ist Produkt der beiden irreduziblen Elemente $1 \pm i$, und die sind assoziiert zueinander, denn $(1 - i) \cdot i = 1 + i$.

Wir sortieren daher in der Primzerlegung von n nach den Kongruenzklassen modulo vier der Primfaktoren:

$$n = 2^e \prod_{j=1}^{r} p_j^{f_j} \prod_{k=1}^{s} q_k^{2g_k} \quad \text{mit} \quad p_j \equiv 1 \bmod 4, \quad q_k \equiv 3 \bmod 4\,.$$

Für jedes p_j wählen wir ein $\pi_j \in \mathbb{Z}[i]$ derart, daß $\pi_j \cdot \overline{\pi}_j = p_j$ ist; dann ist n in $\mathbb{Z}[i]$ assoziiert zu

$$(1 + i)^{2e} \prod_{j=1}^{r} \pi_j^{f_j} \prod_{j=1}^{r} \overline{\pi}_j^{f_j} \prod_{k=1}^{s} q_k^{2g_k}\,.$$

Ein Element $\alpha \in \mathbb{Z}[i]$, für das $\mathrm{N}(\alpha) = n$ sein soll, hat daher bis auf eine Einheit die Form

$$\alpha = (1 + i)^e \prod_{j=1}^{r} \pi_j^{h_j} \prod_{j=1}^{r} \overline{\pi}_j^{f_j - h_j} \prod_{k=1}^{s} q_k^{g_k}\,,$$

mit $0 \le h_j \le f_j$. Die Anzahl verschiedener Möglichkeiten ist somit gleich dem Produkt der $(f_j + 1)$, wobei hier allerdings die Darstellungen $n = x^2 + y^2$ und $n = y^2 + x^2$ für $x \neq y$ als verschieden gezählt werden.

Die im Vergleich zur Größe von n meisten verschiedenen Darstellungen gibt es offenbar dann, wenn n ein Produkt verschiedener Primzahlen ist, die allesamt kongruent eins modulo vier sind. In diesem Fall ist die Anzahl der Darstellungen gleich zwei hoch Anzahl der Faktoren.

§2: Anwendung auf die Berechnung von π

Aus der Analysis I ist bekannt, daß gilt

$$\arctan x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} - \frac{x^{11}}{11} + \frac{x^{13}}{13} - \frac{x^{15}}{15} + \cdots\;;$$

falls es jemand nicht mehr weiß: Die Ableitung des Arcustangens ist $1/(1 + x^2)$, und nach der Summenformel für die geometrische Reihe ist

$$\frac{1}{1 + x^2} = 1 - x^2 + x^4 - x^6 + x^8 - x^{10} + x^{12} - x^{14} + \cdots\,.$$

Durch gliedweise Integration folgt wegen $\arctan 0 = 0$ die obige Formel. Eine bekannte Anwendung davon ist der Spezialfall $x = 1$:

$$\frac{\pi}{4} = \arctan 1 = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15} + \cdots\,.$$

Zur praktischen Berechnung von π ist diese Formel allerdings völlig unbrauchbar und der Alptraum eines jeden Numerikers: Zunächst einmal

sind alternierende Summen grundsätzlich problematisch, allerdings ist das hier vergleichsweise harmlos: Wenn wir jeden negativen Summanden von seinem Vorgänger subtrahieren, bekommen wir eine Reihe

$$\frac{\pi}{4} = \frac{2}{1\cdot 3} + \frac{2}{5\cdot 7} + \frac{2}{9\cdot 11} + \frac{2}{13\cdot 15} + \cdots$$

mit lauter positiven Gliedern. Die Summanden sind jedoch immer noch monoton fallend, so daß die Rundungsfehler der ersten Additionen bei hinreichend langer Summation größer sind als die hinteren Summanden. Man muß also, wenn man eine endliche Teilsumme berechnen will, von hinten nach vorne summieren und damit bereits vor Beginn der Rechnung die Anzahl der Terme festlegen. Bei jeder Erhöhung der Anzahl der Summanden muß die gesamte Rechnung von vorne beginnen.

Dazu kommt, daß die Reihe extrem langsam konvergiert: Berechnet man für

$$\frac{\pi}{8} = \sum_{n=0}^{\infty} \frac{1}{(4n+1)(4n+3)}$$

die Teilsummen

$$S_N = \sum_{n=0}^{N} \frac{1}{(4n+1)(4n+3)},$$

so erhält man für die ersten Zehnerpotenzen N die folgenden Fehler:

N	10	100	1 000	10 000
$\frac{\pi}{8} - S_N$	$5{,}68\cdot 10^{-3}$	$6{,}19\cdot 10^{-4}$	$6{,}24\cdot 10^{-5}$	$6{,}25\cdot 10^{-6}$
N	100 000	1 000 000	10 000 000	
$\frac{\pi}{8} - S_N$	$6{,}25\cdot 10^{-7}$	$6{,}26\cdot 10^{-7}$	$6{,}4\cdot 10^{-8}$	

Man muß also für jede weitere Dezimalstelle den Rechenaufwand ungefähr verzehnfachen. Angesichts der Tatsache, daß heute mehrere Billionen Ziffern von π bekannt sind, kann das wohl kaum der beste Weg zur Berechnung von π sein.

Zahlen mit einer großen Anzahl verschiedener Darstellungen als Summen von Quadraten können uns hier zu besseren Ergebnissen helfen: Die Reihe für den Arcustangens konvergiert sicherlich umso besser, je kleiner der Wert von x ist. Wenn wir also den Winkel $\frac{\pi}{4}$ aufteilen können

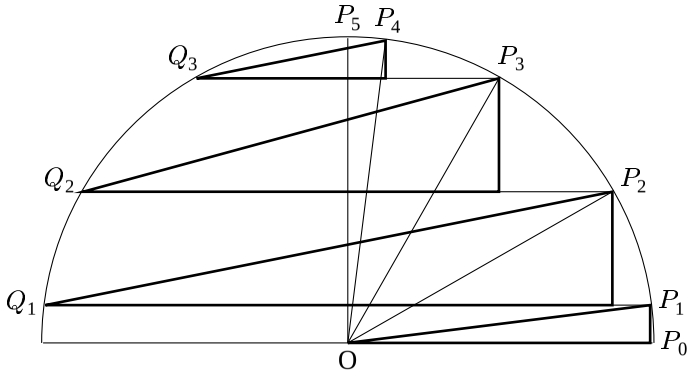
in mehrere kleine Winkel, deren Tangens wir kennen, sollten bessere Ergebnisse zu erwarten sein. Genau das können wir mit solchen Zahlen erreichen.

Angenommen, wir haben für eine Zahl n die r verschiedenen Darstellungen

$$n = x_1^2 + y_1^2 = \cdots = x_r^2 + y_r^2$$

als Summen von Quadraten, wobei $y_1 < \cdots < y_r$ sei. Dann ist $x_i = y_{r-i}$, denn wir können ja in jeder Darstellung die Reihenfolge der Faktoren vertauschen. Wir wollen außerdem voraussetzen, daß n nicht das Doppelte eines Quadrats ist, so daß stets $x_i \neq y_i$ und somit r eine gerade Zahl ist.

Die Punkte $P_i = (x_i, y_i)$ und $Q_i = (-x_i, y_i)$ für $i = 1, \ldots, r$ liegen auf der Kreislinie $x^2 + y^2 = N^2$ um den Nullpunkt O, genauso die drei Punkte $P_0 = (\sqrt{n}, 0)$, $Q_0 = (-\sqrt{n}, 0)$ und $P_{r+1} = (0, \sqrt{n})$.



Da die y-Koordinaten y_i der P_i der Größe nach geordnet sind, ist

$$\frac{\pi}{2} = \sum_{i=0}^{r} \measuredangle OP_iP_{i+1} = 2\sum_{i=0}^{r/2-1} \measuredangle OP_iP_{i+1} + \measuredangle OP_{r/2}P_{r/2+1}.$$

Leider ist keines der Dreiecke $\triangle OP_iP_{i+1}$ rechtwinklig, so daß uns die ganzzahligen Koordiaten der (meisten) P_i bei der Berechnung der Winkel $\measuredangle OP_iP_{i+1}$ nichts nützen.

Nun lehrt uns aber ein Satz der Elementargeometrie, der (im Anhang zu diesem Paragraphen bewiesene) Satz vom Innenwinkel, daß der Winkel $\measuredangle OP_iP_{i+1}$ doppelt so groß ist wie der Winkels $\measuredangle Q_iP_iP_{i+1}$. Letzterer gehört zu einem rechtwinkligen Dreieck, denn natürlich ändert sich nichts am Winkel, wenn wir den Punkt P_i ersetzen durch die senkrechte Projektion $P_i' = (x_{i+1}, y_i)$ von P_{i+1} auf die Gerade Q_iP_i. Somit ist

$$\frac{\pi}{2} = 2\measuredangle OP_0'P_1 + 4\sum_{i=1}^{r/2-1} \measuredangle Q_iP_i'P_{i+1} + 2\measuredangle Q_{r/2}P_{r/2}'P_{r/2+1}\,.$$

Division durch zwei macht daraus

$$\frac{\pi}{4} = \measuredangle OP_0'P_1 + 2\sum_{i=1}^{r/2-1} \measuredangle Q_iP_i'P_{i+1} + \measuredangle Q_{r/2}P_{r/2}'P_{r/2+1}\,.$$

In dieser Darstellung sind die drei Punkte, die den Winkel bestimmen, in allen Fällen die Eckpunkte eines rechtwinkligen Dreiecks, sie haben allesamt ganzzahlige Koordinaten, und zumindest die Katheten der Dreiecke haben ganzzahlige Längen. Somit können wir alle auftretenden Winkel ausdrücken durch Arcustangenswerte rationaler Zahlen.

Als Beispiel betrachten wir das kleinste Produkt dreier verschiedener Primzahlen kongruent eins modulo vier, also $N = 5\cdot 13\cdot 17 = 1105$. Aus den Darstellungen

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2 \quad \text{und} \quad 17 = 1^2 + 4^2$$

verschafft man sich leicht die vier Darstellungen

$$1105 = 4^2 + 3^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2\,,$$

zu denen natürlich auch noch vier mit vertauschten Faktoren kommen. Wir haben also

$$P_1 = (33,4)\,,\ P_2 = (32,9)\,,\ P_3 = (31,12)\,,\ P_4 = (24,23)\,,$$
$$P_8 = (4,33)\,,\ P_7 = (9,32)\,,\ P_6 = (12,31)\,,\ P_5 = (23,24)\,;$$

dazu kommen noch die beiden Randpunkte $P_0 = (\sqrt{1105}, 0)$ sowie $P_9 = (0, \sqrt{1105})$.

Die Q_i für $1 \le i \le 8$ unterscheiden sich von den P_i nur durch das Vorzeichen der Abszisse. Damit können wir die Tangenten aller Winkel bei O berechnen:

$$\tan\measuredangle OP_0P_1 = \tan\measuredangle OP_8P_9 = \frac{y_1}{x_1} = \frac{4}{33}$$
$$\tan\measuredangle OP_1P_2 = \tan\measuredangle OP_7P_8 = \tan 2\measuredangle Q_1P_1P_2 = \frac{y_2-y_1}{x_1+x_2} = \frac{5}{65} = \frac{1}{13}$$
$$\tan\measuredangle OP_2P_3 = \tan\measuredangle OP_6P_7 = \tan 2\measuredangle Q_2P_2P_3 = \frac{y_3-y_2}{x_2+x_3} = \frac{3}{63} = \frac{1}{21}$$
$$\tan\measuredangle OP_3P_4 = \tan\measuredangle OP_5P_6 = \tan 2\measuredangle Q_3P_3P_4 = \frac{y_4-y_3}{x_3+x_4} = \frac{11}{55} = \frac{1}{5}$$
$$\tan\measuredangle OP_4P_5 = \tan 2\measuredangle Q_4P_4P_5 = \frac{y_5-y_4}{x_4+x_5} = \frac{1}{47}$$

Die Summe aller dieser Winkel ist

$$\frac{\pi}{4} = \arctan\frac{4}{33} + 2\arctan\frac{1}{13} + 2\arctan\frac{1}{21} + 2\arctan\frac{1}{5} + \arctan\frac{1}{47}\,.$$

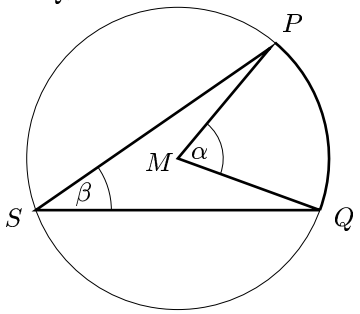
Berechnen wir das Summation von 0 bis n in der TAYLOR-Reihe, erhalten wir folgende (auf eine geltende Ziffer gerundeten) Abweichungen Δ_n von π:

n	1	2	3	4	5
Δ_n	$5\cdot 10^{-4}$	$1\cdot 10^{-5}$	$4\cdot 10^{-7}$	$1\cdot 10^{-8}$	$5\cdot 10^{-10}$
n	6	7	8	9	10
Δ_n	$2\cdot 10^{-11}$	$6\cdot 10^{-13}$	$2\cdot 10^{-14}$	$8\cdot 10^{-16}$	$3\cdot 10^{-17}$

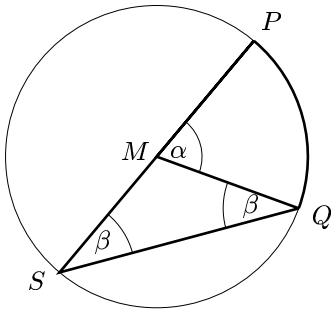
Anhang: Der Satz vom Innenwinkel

Da der Satz vom Innenwinkel in Deutschland anscheinend nicht zum Standardstoff im Geometrieunterricht der Schulen zählt, sei er hier noch einmal genauer formuliert und bewiesen:

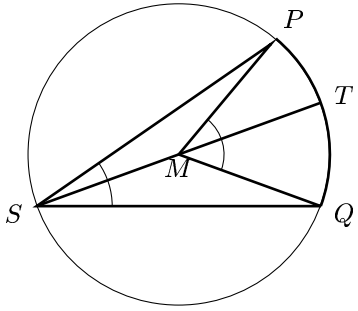
Satz: P, Q, S seien Punkte auf einer Kreisline mit Mittelpunkt M. Dann ist $\angle MPQ = 2\angle SPQ$.



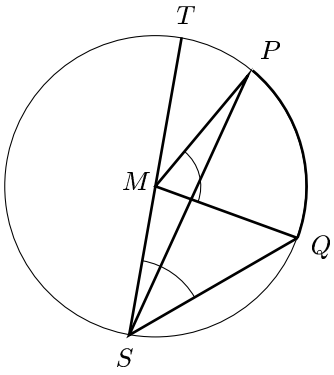
Beweis: Am einfachsten ist der Fall, daß M auf der Verbindungsstrecke von S mit einem der beiden Punkte P und Q liegt; wir nehmen an, er liege auf $\overline{SP}$. (Der andere Fall ist spiegelsymmetrisch dazu und geht genauso.) Dann ist das Dreieck $\triangle MSQ$ gleichschenklig, d.h. wir haben bei S und bei Q denselben Winkel β. Der verbleibende Dreieckswinkel bei M ist somit $\pi - 2\beta$. Andererseits ist dies aber der Komplementärwinkel zu $\alpha = \angle MPQ$, also ist $\alpha = 2\beta$, wie behauptet.



Der allgemeine Fall kann auf diesen Spezialfall zurückgeführt werden: Liegen P und Q auf verschiedenen Seiten des Durchmessers durch S, dessen anderer Endpunkt T sei, so erfüllen auch die Punkte S, P, T, M sowie die Punkte S, Q, T, M die Voraussetzung des Satzes, und in beiden Fällen sind wir in der Situation des bereits bewiesenen Spezialfalls. Addition der Ergebnisse für diese beiden Fälle liefert das Ergebnis für die Punkte S, P, Q, M.



Bleibt noch der Fall, daß P und A auf derselben Seite des Durchmessers $\overline{ST}$ liegen. Auch in diesem Fall erfüllen wieder sowohl die Punkte S, P, T, M als auch die Punkte S, Q, T, M die Voraussetzungen des Satzes, und beides Mal sind wir in der Situation des eingangs bewiesenen Spezialfalls. Dieses Mal führt die Subtraktion dieser beiden Ergebnisse zum gewünschten Resultat für die Ausgangssituation mit den Punkten S, P, Q, M.



Damit ist der Satz vollständig bewiesen. ∎

§3: Der Satz von Lagrange

Es ist nicht möglich, eine beliebige natürliche Zahl als Summe von höchstens drei Quadratzahlen zu schreiben; das kleinste Gegenbeispiel ist die Sieben. Wie EULER vermutete und LAGRANGE bewies, kommt man aber immer mit höchstens vier Quadratzahlen aus.

Der Beweis ist recht ähnlich zu dem des Zweiquadratesatzes aus §1; statt mit dem Ring $\mathbb{Z}[i]$ der GAUSSschen Zahlen arbeiten wir aber mit dem Ring

$$\mathbb{Z} \oplus \mathbb{Z}\mathbf{i} \oplus \mathbb{Z}\mathbf{j} + \oplus \mathbb{Z}\mathbf{k}$$

der ganzen Quaternionen. Auch hier haben wir eine Normabbildung, und eine ganze Zahl n ist offensichtlich genau dann als Summe von vier Quadraten darstellbar, wenn sie Norm einer ganzen Quaternion ist. Wegen der Multiplikativität der Norm reicht es also wieder, wenn wir Primzahlen p betrachten.

Zur Vorbereitung zeigen wir zunächst

Lemma: Zu jeder Primzahl p gibt es ganze Zahlen $x, y, z \in \mathbb{Z}$ und eine natürliche Zahl $m < p$, so daß gilt: $mp = x^2 + y^2 + z^2$

Beweis: Für $p = 2$ ist $2 = 1^2 + 1^2 + 0^2$; sei also p ungerade.

Von den Zahlen a^2 mit $0 \le a \le \frac{1}{2}(p-1)$ sind keine zwei kongruent modulo p, denn $a^2 - b^2 = (a+b)(a-b)$, und falls $0 \le a, b < \frac{1}{2}p - 1$ sind beide Faktoren kleiner als p. Damit gibt es auch in den Mengen

$$\mathcal{M}_1 = \left\{ -a^2 \;\middle|\; 0 \le a \le \tfrac{1}{2}(p-1) \right\}$$

und

$$\mathcal{M}_2 = \left\{ 1 + a^2 \;\middle|\; 0 \le a \le \tfrac{1}{2}(p-1) \right\}$$

keine zwei Elemente, die modulo p kongruent sind. Da die beiden Mengen disjunkt sind und jede davon $\frac{1}{2}(p+1)$ Elemente hat, enthält ihre Vereinigung $p+1$ Elemente; hier muß es also mindestens zwei Elemente geben, die modulo p kongruent sind. Es gibt also Zahlen $x, y \in \mathbb{Z}$ mit $-x^2 \equiv 1 + y^2 \bmod p$, d.h. $x^2 + y^2 + 1 = mp$ ist durch p teilbar. Da $x, y \le \frac{1}{2}(p-1)$, ist dabei $m < p$. Da $1 = 1^2$ ein Quadrat ist, ist damit das Lemma bewiesen. ∎

Lemma: Jede Primzahl p läßt sich als Summe von höchstens vier Quadraten schreiben.

Beweis: Für $p = 2$ wissen wir das; sei also p wieder ungerade. Nach dem vorigen Lemma gibt es eine natürliche Zahl $m < p$ derart, daß mp als Summe von sogar höchstens drei Quadraten darstellbar ist; k sei die kleinste natürliche Zahl, für die kp als Summe von höchstens vier Quadraten darstellbar ist. Natürlich ist dann auch $k < p$.

Wäre k eine gerade Zahl, so wäre auch die Summe der vier Quadrate gerade, und dazu gibt es drei Möglichkeiten: Entweder alle Summanden sind gerade oder alle sind ungerade oder zwei davon sind gerade, der Rest ungerade. Im letzteren Fall wollen wir die vier Zahlen w, x, y, z so anordnen, daß w und x gerade sind, y und z dagegen ungerade. Dann sind in allen drei Fällen $w \pm x$ und $y \pm z$ gerade, und

$$\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = \frac{w^2+x^2+y^2+z^2}{2} = \frac{k}{2}p\,,$$

im Widerspruch zur Minimalität von k. Also ist k ungerade, und falls das Lemma falsch wäre, müßte $k \ge 3$ sein.

Wir betrachten die modulo k zu w, x, y, z kongruenten ganzen Zahlen W, X, Y, Z vom Betrag kleiner $k/2$. Wie schon beim Zwei-Quadrate-Satz können diese nicht allesamt verschwinden, denn sonst wären w, x, y, z durch k teilbar, also ihre Quadratsumme kp durch k^2, was wegen $k < p$ für eine Primzahl p nicht möglich ist.

Somit ist $0 < W^2 + X^2 + Y^2 + Z^2 < 4 \cdot \left(\frac{k}{2}\right)^2 = k^2$. Andererseits ist aber

$$W^2 + X^2 + Y^2 + Z^2 \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \bmod k\,;$$

also ist

$$W^2 + X^2 + Y^2 + Z^2 = k\ell \quad \text{mit} \quad 1 \le \ell < k\,.$$

Damit haben die Quaternionen

$$q = w + ix + jy + kz \quad \text{und} \quad Q = W + iX + jY + kZ$$

die Normen $\mathrm{N}(q) = kp$ und $\mathrm{N}(Q) = k\ell$, ihre Produkt hat also die Norm $k^2\ell p$. Zumindest von der Norm her spricht also nichts dagegen, daß dieses Produkt durch k teilbar sein könnte.

Tatsächlich ist $q\overline{Q}$ durch k teilbar, und das sieht man am schnellsten durch brutales Nachrechnen: In

$$\begin{aligned} q\overline{Q} = {} & (wW + xX + yY + zZ) \\ & + (-wX + xW - yZ + zY)\mathbf{i} \\ & + (-wY + yW - zX + xZ)\mathbf{j} + (-wZ + zW - xY + yX)\mathbf{k} \end{aligned}$$

sind alle vier Klammern durch k teilbar, denn modulo k sind alle Großbuchstaben gleich den entsprechenden Kleinbuchstaben, so daß die Koeffizienten von $\mathbf{i}, \mathbf{j}, \mathbf{k}$ trivialerweise modulo k verschwinden, und für den Realteil haben wir

$$wW + xX + yY + zZ \equiv w^2 + x^2 + y^2 + z^2 = kp \equiv 0 \bmod k\,.$$

Somit ist

$$\frac{q\overline{Q}}{k} = A + B\mathbf{i} + C\mathbf{j} + D\mathbf{k}$$

eine Quaternion mit ganzzahligen Koeffizienten, und

$$A^2 + B^2 + C^2 + D^2 = \mathrm{N}\left(\frac{q\overline{Q}}{k}\right) = \frac{\mathrm{N}(q\overline{Q})}{k^2} = \frac{\mathrm{N}(q)\mathrm{N}(Q)}{k^2} = \ell p\,.$$

Dies widerspricht aber der Minimalität von k.

Somit muß $k = 1$ sein, und der Satz ist bewiesen. ∎

Satz (LAGRANGE)**:** Jede natürliche Zahl läßt sich als Summe von höchstens vier Quadraten schreiben.

Beweis: Wie wir in Kapitel IV, §7 gesehen haben, läßt sich eine Zahl n genau dann als Summe von höchstens vier Quadraten schreiben, wenn sie Norm einer ganzen Quaternion ist. Da wir gerade gesehen haben, daß sich jede Primzahl als Summe von höchstens vier Quadraten schreiben läßt (und die Eins natürlich auch), folgt die Behauptung aus der Multiplikativität der Norm. ∎

§4: Quadratische Formen und Matrizen

Nachdem wir in den vorigen Paragraphen gesehen haben, daß die spezielle quadratische Form $x^2 + y^2$ vielfältige Beziehungen sowohl zum Zahlkörper $\mathbb{Q}[i]$ als auch zu Anwendungen außerhalb der Zahlentheorie haben, wollen wir uns nun etwas mit der allgemeinen Theorie dieser Formen beschäftigen. In den nächsten Paragraphen werden wir sie dann auf quadratische Zahlkörper und die PELLsche Gleichung anwenden.

Viele abstrakte Aussagen über quadratische Formen werden einfacher, wenn wir sie in lineare Algebra übersetzen. In Matrixschreibweise ist

$$Ax^2 + Bxy + Cy^2 = \begin{pmatrix} x & y \end{pmatrix} Q \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{mit} \quad Q = \begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix},$$

die quadratische Form kann also auch durch die symmetrische Matrix Q beschrieben werden.

Die Determinante von Q ist $AC - \frac{1}{4}B^2$; bis auf einen Faktor -4 ist das die Zahl $B^2 - 4AC$, die wir in Kapitel IV, §2 als Diskriminante eines Elements eines quadratisches Zahlkörpers definiert haben. Wir können also hoffen, daß uns die lineare Algebra via Determinantentheorie Aussagen über die Werte einer quadratischen Form sowie über Zusammenhänge zwischen den Diskriminanten verschiedener Elemente eines quadratischen Zahlkörpers gibt.

Die Werte, die eine quadratische Form annehmen kann, hängen nicht davon ab, in welcher Basis wir das Argument $\binom{x}{y}$ darstellen; wir können die Basis daher bei Bedarf beliebig ändern.

Das ist zum Beispiel nützlich bei der Frage, wann eine quadratische Form nur positive oder nur negative Werte annimmt:

Definition: Eine symmetrische Matrix $Q \in \mathbb{R}^{2\times 2}$ sowie die dadurch definierte quadratische Form $f_Q(x,y) = (x\ y)Q\binom{x}{y}$ heißen $\left\{\begin{matrix}\text{positiv}\\ \text{negativ}\end{matrix}\right\}$ semidefinit, wenn $f_Q(x,y)\ \left\{\begin{matrix}\geq\\ \leq\end{matrix}\right\}\ 0$ für alle $x, y \in \mathbb{R}$. Sie heißt $\left\{\begin{matrix}\text{positiv}\\ \text{negativ}\end{matrix}\right\}$ definit, wenn zusätzlich $f(x,y) = 0$ nur gilt für $x = y = 0$.

Wie aus der linearen Algebra bekannt ist, gibt es zu einer symmetrischen reellen Matrix stets eine Basis aus Eigenvektoren; bezüglich derer hat die Matrix Diagonalgestalt, wobei in der Diagonale die beiden (reellen) Eigenwerte stehen. Das Produkt dieser Eigenwerte ist die Determinante der Matrix, ihre Summe die Spur.

Offensichtlich ist eine Diagonalmatrix genau dann positiv semidefinit, wenn beide Eigenwerte ≥ 0 sind und genau dann positiv definit, wenn sie sogar echt positiv sind. Entsprechendes gilt für negativ (semi-)definite Matrizen. Für eine positiv oder negativ semidefinite Matrix muß daher die Determinante ≥ 0 sein; bei einer definiten Matrix muß sie positiv sein. Ob sie positiv oder negativ definit ist, sagt uns dann die Spur, denn da die beiden Eigenwerte (falls $\neq 0$) dasselbe Vorzeichen haben, ist dieses auch das Vorzeichen ihrer Summe, der Spur. Wenn die Determinante $AC - \frac{1}{4}B^2$ positiv ist, müssen A und C dasselbe Vorzeichen haben; da auch $A + C$ gleich der Spur der Matrix ist, folgt

Lemma: *a)* Eine symmetrische 2×2-Matrix ist genau dann positiv oder negativ definit, wenn ihre Determinante positiv ist. Sie ist positiv definit, wenn der Eintrag links oben positiv ist, andernfalls ist sie negativ definit.
b) Die quadratische Form $Ax^2+Bxy+Cy^2$ ist genau dann definit, wenn ihre Diskriminante $B^2 - 4AC$ negativ ist. Im Falle $A > 0$ ist sie dann positiv, sonst negativ definit. ∎

So nützlich der Wechsel zu einer Basis aus Eigenvektoren in diesem Fall auch war, für die meisten zahlentheoretischen Fragen werden uns nur

solche Basiswechsel helfen, die ganzzahlige Punkte wieder in ganzzahlige Punkte überführen. Hier gilt

Lemma: Die lineare Abbildung

$$\varphi: \begin{cases} \mathbb{R}^2 \to \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} \mapsto M \begin{pmatrix} x \\ y \end{pmatrix} \end{cases}$$

definiert genau dann eine Bijektion $\mathbb{Z}^2 \to \mathbb{Z}^2$, wenn alle Einträge der Matrix A ganzzahlig sind und $\det M = \pm 1$ ist.

Beweis: Da die Spaltenvektoren von M die Bilder der Basisvektoren $\binom{1}{0}$ und $\binom{0}{1}$ sind, ist klar, daß $\varphi(\mathbb{Z}^2)$ genau dann in $\mathbb{Z}^2$ liegt, wenn alle Einträge von M ganzzahlig sind. Das Gleichheitszeichen gilt genau dann, wenn auch $\varphi^{-1}(\mathbb{Z}^2) \subseteq \mathbb{Z}^2$ ist, d.h. wenn auch M^{-1} lauter ganzzahlige Einträge hat. In diesem Fall sind $\det M$ und $\det M^{-1}$ beide ganzzahlig mit Produkt eins, also ist $\det M = \pm 1$.

Hat umgekehrt eine Matrix M mit ganzzahligen Einträgen Determinante ± 1, so hat auch M^{-1} ganzzahlige Einträge, denn die Spaltenvektoren von M^{-1} sind die Lösungen der linearen Gleichungssysteme $M\binom{x}{y} = \binom{1}{0}$ und $M\binom{x}{y} = \binom{0}{1}$, die wir nach der CRAMERschen Regel ausdrücken können durch Brüche mit ganzzahligen Zählern und $\det M$ im Nenner. ∎

Setzen wir für so eine Matrix M das Bild $M\binom{x}{y}$ an Stelle von $\binom{x}{y}$ in die quadratische Form ein, erhalten wir das Ergebnis

$${}^t\left(M\begin{pmatrix} x \\ y \end{pmatrix}\right) \cdot Q \cdot M\begin{pmatrix} x \\ y \end{pmatrix} = (x \;\; y)\left({}^tMQM\right)\begin{pmatrix} x \\ y \end{pmatrix},$$

das wir auch erhalten hätten, wenn wir $\binom{x}{y}$ in die quadratische Form zur Matrix ${}^tMQM$ eingesetzt hätten. Da $\binom{x}{y} \mapsto M\binom{x}{y}$ eine Bijektion von $\mathbb{Z}^2$ nach $\mathbb{Z}^2$ definiert, nehmen die quadratischen Formen zu Q und zu ${}^tMQM$ also dieselben Werte an. Deshalb definieren wir

Definition: Die quadratischen Formen mit Matrizen Q_1 und Q_2 heißen *äquivalent,* wenn es eine Matrix M mit ganzzahligen Einträgen und $\det M = \pm 1$ gibt, so daß $Q_2 = {}^tMQ_1M$.

Lemma: Zwei äquivalente quadratische Formen haben dieselbe Diskriminante.

Beweis: Bis auf den Faktor -4 ist die Diskriminante gleich der Determinante der Matrix und

$$\det Q_2 = \det {}^tM \cdot \det Q_1 \cdot \det M = \det Q_1,$$

da $\det M = \det {}^tM = \pm 1$ ist. ∎

§5: Kettenbruchentwicklung quadratischer Irrationalitäten

Die rationalen Zahlen sind genau diejenigen reellen Zahlen, deren Kettenbruchentwicklung nach endlich vielen Schritten abbricht. Wir wollen sehen, daß wir auch quadratische Irrationalitäten, d.h. Elemente eines quadratischen Zahlkörpers, die nicht in $\mathbb{Q}$ liegen, durch ihre Kettenbruchentwicklung charakterisieren können.

In den Beispielen der Kettenbruchentwicklungen von $\sqrt{2}$ und $\sqrt{3}$ kamen wir in Kapitel III auf periodische Folgen. Wie sich zeigen wird, ist dies charakteristisch für quadratische Irrationalitäten.

Nach der Formel am Ende von §2 von Kapitel III gilt für die Zahlen α_n aus dem Algorithmus zur Kettenbruchentwickung die Gleichung

$$\alpha = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}},$$

wobei p_n und q_n Zähler und Nenner der n-ten Konvergente sind. Zähler und Nenner des rechtsstehenden Bruchs sind die beiden Komponenten des Vektors

$$M\begin{pmatrix} \alpha_n \\ 1 \end{pmatrix} \quad \text{mit} \quad M = \begin{pmatrix} p_{n-2} & p_{n-1} \\ q_{n-2} & q_{n-1} \end{pmatrix},$$