Bachelorarbeit
zur Erlangung des Abschlusses
Bachelor of Science (B.Sc.) in Mathematik

Summe von Quadraten und die Anzahl ihrer Darstellungen

eingereicht bei: Herrn Prof. Dr. rer. nat. Holger Brenner
Herrn Prof. Dr. rer. nat. Tim Römer
Fachbereich Mathematik/Informatik

von Autorin: Volha Baranouskaya
vbaranou@uos.de
49080 Osnabrück, Jahnplatz 6

Osnabrück, den 9. September 2009

Inhaltsverzeichnis

Einleitung

Eine Darstellung einer natürlichen Zahl als Summe von zwei Quadraten ist aus der Schule bekannt als z. B. der Satz von PYTHAGORAS[1] für rechtwinklige Dreiecke

$$25 \;=\; (\pm 3)^2 + (\pm 4)^2.$$

Weitere Beispiele kann man sich leicht überlegen. Als Summe von zwei Quadraten können die Zahlen

$$5 = (\pm 1)^2 + (\pm 2)^2 \quad \text{und} \quad 65 = (\pm 4)^2 + (\pm 7)^2$$

genannt werden. Andererseits gibt es Zahlen, die nicht als Summe von zwei Quadraten geschrieben werden können, sondern nur als Summe von drei oder vier Quadraten, z.B. die Zahl

$$62 = (\pm 2)^2 + (\pm 3)^2 + (\pm 7)^2 \quad \text{oder} \quad 7 = (\pm 2)^2 + (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2.$$

Außerdem haben die meisten Zahlen nicht nur eine Darstellung sondern mehrere, wobei in der Darstellung das Vorzeichen und die Reihenfolge der Summanden berücksichtigt wird. Für die oben gegebene Zahl 65 gibt es zum Beispiel 16 verschiedene Darstellungen, nämlich

$$\begin{aligned} 65 &= (\pm 4)^2 + (\pm 7)^2 \\ &= (\pm 7)^2 + (\pm 4)^2 \\ &= (\pm 1)^2 + (\pm 8)^2 \\ &= (\pm 8)^2 + (\pm 1)^2. \end{aligned}$$

Das Interesse der Mathematiker an der Klärung, warum es solche Darstellungen gibt und wie viele Darstellungen für eine natürliche Zahl existieren geht auf die Zeit von DIOPHANT zurück. Die ersten Erklärungen der Darstellung einer natürlichen Zahl als Summe von zwei Quadraten können mit der Formulierung der Theorie der komplexen Zahlen angesehen werden, die BOMBELLI 1572 in seinem Buch „Algebra“ dargelegt

[1] Pythagoras von Samos (* um 570 v. Chr.; †nach 510 v. Chr. in Metapont in der Basilicata) war ein antiker griechischer Philosoph (Vorsokratiker) und Gründer einer einflussreichen religiös-philosophischen Bewegung.

hat. Die Eigenschaft der imaginären Einheit (nämlich $i^2 = -1$) fand zunächst keine Anerkennung in der Wissenschaft, obwohl die Mathematiker mit diesen Zahlen einsehen könnten, dass eine Primzahl kongruent 1 modulo 4 als Summe von zwei Quadraten darstellbar ist. PIERRE DE FERMAT[2] ging anders vor. Er hat seine „Methode des Abstieges“ benutzt, um die Darstellungen solcher Primzahlen als Summe zweier Quadrate zu begründen. Den Satz für Primzahlen $p \equiv 1 \bmod 4$ und $p = 2$ hat EULER zwischen 1742 und 1747 bewiesen, und hat im Beweis die Theorie der komplexen Zahlen und die Überlegungen von FERMAT verwendet. Nachdem er den Satz bewiesen hat, war es ihm nicht aufwändig zu zeigen, dass eine natürliche Zahl als Summe von zwei Quadraten mit einem Primteiler auch als Summe von zwei Quadraten eine abgeleitete Darstellung von ihren beiden Primteilern ist, wobei zweiter auch Summe von zwei Quadraten ist.

Die Geschichte der Darstellung einer natürlichen Zahl als Summe von drei Quadraten ist im Grunde die Geschichte der Darstellung einer ternären quadratischen Formen mit bestimmten Eigenschaften in solcher Form. Es wurde zuerst die Theorie der binären quadratischen Formen untersucht, deren Schöpfer FERMAT war [vgl.[14], IV §IV]. LAGRANGE UND GAUSS haben die Begriffe (äquivalent, definit, indefinit, reduziert usw.) der Eigenschaften von quadratischen Formen eingeführt und viele Sätze in diesem Bereich bewiesen. Als Ergebnis dieser Leistungen war der Beweis des „Drei-Quadrate-Satz“ von LEGENDRE 1798, der eine Ungenauigkeit hatte. Diese Ungenauigkeit wurde später von GAUSS beseitigt.

Die Aussage, dass eine beliebige natürliche Zahl sich als Summe von vier Quadraten schreiben lässt, wurde schon im Jahre 1621 von BACHET erkannt. Auch 1640 hat FERMAT Gleiches vermutet. Weiter, wie aus der Korrespondenz von EULER an GOLDBACH zu entnehmen ist, dass bis 1751 keiner einen Beweis der Aussage geben konnte [vgl.[14], III. Anhang II]. Die Anwendung des „Zwei-Quadrate-Satzes“ führte auch nicht zum gewünschten Ergebnis. Aber schon im Jahre 1770 hat LAGRANGE den Erfolgt gehabt. Im Beweis dieses Satzes hat er nicht nur die Summe von zwei Quadraten sondern auch Summe von drei Quadraten und quadratische Formen verwendet. Unabhängig von LAGRANGE entdeckte HAMILTON viele Jahre später – genauer 1843 – die vierdimensionalen Zahlen, die den „Vier-Quadrate-Satz“ eine typische Produktregel ist.

Seitdem FERMAT die Vermutung geäußert hat, dass eine Primzahl $p = 4k + 1$ mit $k \in \mathbb{N}$ nur eine einzelne Darstellung als Summe von zwei Quadraten hat, fragte er nach der Anzahl der Darstellungen für eine beliebige natürliche Zahl in dieser Form

[2] Pierre de Fermat (* vermutlich Ende 1607 oder Anfang 1608 in Beaumont-de-Lomagne; †12. Januar 1665 in Castres) war ein französischer Mathematiker und Jurist.

und suchte eine Methode, um diese Anzahl zu finden. In einem halben Jahr ist er zu vielen Behauptungen gekommen, die er nicht beweisen konnte. Eine davon lautet, dass eine Primzahl $p = 4k - 1$ nicht die Summe zweier teilerfremden Quadrate teilen kann, d.h., dass -1 ein nicht quadratischer Rest modulo dieser p ist. Später, als EULER den Satz für Primzahlen $p \equiv 1 \bmod 4$ bewiesen hat, ist klar geworden, dass die Anzahl der Darstellungen einer natürlichen Zahl durch die Komposition aus der Zerlegung in Primfaktoren berechnet werden kann. Für eine natürliche Zahl, die Summe von vier Quadraten ist, hat CARL GUSTAV JACOB JACOBI[3] die Anzahl der Darstellungen 1828 berechnet.

Das Ziel dieser Arbeit besteht darin, die natürlichen Zahlen als Summe von zwei, drei und vier Quadraten zu betrachten und die Anzahl der Darstellungen der Summe von zwei und vier Quadraten zu berechnen.

Im Rahmen des ersten Kapitels erfolgt die Betrachtung der natürlichen Zahlen als Summe von zwei Quadraten. Zuerst werden die Voraussetzungen untersucht, unter denen sich eine natürliche Zahl in dieser Form schreiben lässt. Dafür werden die GAUSSschen Zahlen eingeführt und betrachtet. Von besonderem Interesse ist hier der Begriff der „Norm“. Mit der Norm wird in dem darauffolgenden Abschnitt gezeigt, dass eine Primzahl $p \equiv 1 \bmod 4$ und $p = 2$ die Summe von zwei Quadraten ist. Im letzten Abschnitt des Kapitels wird gezeigt, welche Bedingungen erfüllt werden müssen, um eine natürliche Zahl als Summe von zwei Quadraten darzustellen.

Im zweiten Kapitel werden die Quaternionen[4] eingeführt, die im vierdimensionalen $\mathbb{R}$-Vektorraum definiert sind. Die Quaternionen sind die hyperkomplexen Zahlen mit drei imaginären Teilen. In Analogie zu den komplexen Zahlen werden ihre wichtigsten Eigenschaften betrachtet. Auf der Basis dieser Zahlen wird der Satz von LAGRANGE bewiesen, der sagt, dass sich jede natürliche Zahl als Summe von höchstens vier Quadratzahlen schreiben lässt.

Im Kapitel 3 erfolgt die Betrachtung der natürlichen Zahlen als Summe von drei Quadraten. Dafür werden in den ersten drei Abschnitten die Vorbereitungen gemacht, nämlich die Betrachtung der quadratischen Formen allgemein und danach der binären und der ternären quadratischen Formen. Am Ende des dritten Kapitels wird gezeigt, wann eine ternäre quadratische Form äquivalent zur Summe von drei Quadraten ist. Die Sätze und Methoden wie z. B. das JACOBI-Symbol, der Satz von DIRICHLET, das

[3] Carl Gustav Jacob Jacobi (* 10. Dezember 1804 in Potsdam; †18. Februar 1851 in Berlin), war ein deutscher Mathematiker.

[4] lat. quaternio -Vierheit.

Reziprozitätsgesetz und der Chinesische Restsatz werden in dieser Arbeit ohne Beweise verwendet. Mit ihrer Hilfe und mit Hilfe der ternären quadratischen Formen wird die Darstellung einer natürliche Zahl n als Summe von drei Quadraten bewiesen, die nicht in der Form $n = 4^a(8k + 7)$ mit $a, k \in \mathbb{N}$ darstellbar ist.

Im Kapitel 4 wird die Anzahl der Darstellungen einer natürlichen Zahl als Summe von zwei und vier Quadraten berechnet. Zu Beginn wird die Anzahl der Darstellungen einer natürlichen Zahl als Summe von zwei Quadraten mit teilerfremden Summanden untersucht. Im folgenden Abschnitt werden die Hilfsmittel wie die zahlentheoretischen Funktionen, die Charaktere und die Faltung mit ihren Eigenschaften vorgestellt. Auf diesen Grundlagen wird im nächsten Abschnitt die Anzahl der Darstellungen einer natürlichen Zahl $n = x^2 + y^2$ mit nicht notwendig teilerfremden x und y berechnet. Im letzten Abschnitt des Kapitels wird der Satz von JACOBI bewiesen, der die Anzahl der Darstellungen einer natürlichen Zahl als Summe von vier Quadraten berechnet.

Im letzten Abschnitt der Arbeit wird das WARINGsche Problem formuliert und ohne Beweis erwähnt, dass es lösbar ist. Danach werden Spezialfälle vorgestellt, wobei der „Vier-Quadrate-Satz“ aus dem Kapitel 2 ein Sonderfall davon ist. Abschließend wird auf offene Fragen eingegangen.

1 Die Gausschen Zahlen und Summe zweier Quadrate

Die Geschichte von der Suche und der Erklärung der Lösung $i = \sqrt{-1}$ für die Gleichung $x^2 + 1 = 0$ ist sehr spannend und geht in das 16. Jahrhundert zurück. Die komplexen Zahlen haben den Mathematikern und Philosophen der Vergangenheit große Schwierigkeiten bereitet. So konnte z.B. Euler[1] die imaginären Zahlen nicht erklären, obwohl er mit ihnen jahrzehntelang meisterhaft gerechnet hat. Er betonte auch: „So ist es klar, dass die Quadrat-Wurzeln von Negativen-Zahlen nicht einmal unter die möglichen Zahlen berechnet werden können: folglich müssen wir sagen, dass dieselben ohnmögliche Zahlen sind. Und dieser Umstand leitet uns auf den Begriff von solchen Zahlen, welche ihrer Natur nach ohnmöglich sind, und gemeiniglich *imaginäre*, oder *eingebildete* Zahlen genannt werden, weil sie bloß allein in der Einbildung statt finden“[vgl.[3], 3. §1.4].

Wir beschäftigen uns im ersten Kapitel mit diesen imaginären Zahlen. Wir fangen mit der Betrachtung der Gausschen Zahlen und ihrer Eigenschaften an. Danach zeigen wir, wann eine Primzahl Summe von zwei Quadraten ist und am Schluss des Kapitels beweisen wir, wann eine natürliche Zahl als Summe von zwei Quadraten dargestellt werden kann.

1.1 Die Gausschen Zahlen und ihre Eigenschaften

Wir gehen davon aus, dass dem Leser die komplexen Zahlen $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$ mit den Operationen der Addition und Multiplikation bekannt sind. 1799 hat Carl Friedrich Gauss[2] die komplexen Zahlen $\mathbb{C}$ erstmals in seiner Dissertation erfasst. Die Elemente $a + bi \in \mathbb{C}$ mit $a, b \in \mathbb{Z}$ nennt man *ganze* Gausssche *Zahlen* und bezeichnet sie mit $\mathbb{Z}[i]$.

[1] Leonhard Euler (* 15. April 1707 in Basel; †18. September 1783 in Sankt Petersburg) war Schweizer Mathematiker und Physiker.

[2] Johann Carl Friedrich Gauss (* 30. April 1777 in Braunschweig; †23. Februar 1855 in Göttingen) war ein deutscher Mathematiker, Astronom, Geodät und Physiker.

Definition 1.1. $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ heißt die *Menge der* Gausszschen Zahlen.

Gauss hat in seinem Werk „Theoria Residuorum Biguadraticorum, Commentatio Secunda“(Werke 2, 93-148) die eindeutige Darstellung der komplexen Zahlen als Punkte in der *komplexen Zahlenebene* dargelegt. In dieser Ebene bilden die Gausszschen Zahlen ein sogenanntes Gitter [siehe Abbildung. 1.1].

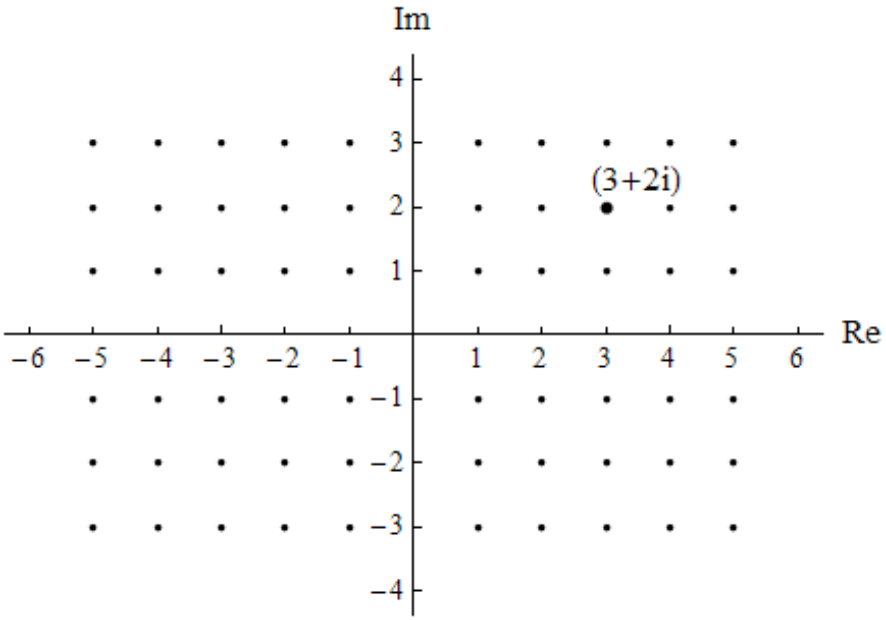

Abbildung 1.1: Die komplexe Zahlenebene.

Im Folgenden wollen wir die Eigenschaften von $\mathbb{Z}[i]$ betrachten.

Satz 1.2. *Sei* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ *die Menge der* Gausszschen Zahlen. *Dann ist* $\mathbb{Z}[i]$ *ein kommutativer Unterring von* $\mathbb{C}$.

Beweis. In $\mathbb{Z}[i]$ rechnet man mit ganzen Zahlen, wobei $i^2 = -1 \in \mathbb{Z}$ ist. In $\mathbb{C}$ rechnet man mit reellen Zahlen $\mathbb{R}$, wobei $(\mathbb{R}, +, \cdot)$ ein Körper ist [vgl. [10], Beispiel 2.11(i)]. Die Rechenregeln für $\mathbb{Z}$ stimmen mit den jeweiligen Rechenregeln von $\mathbb{R}$ überein, da $\mathbb{Z} \subset \mathbb{R}$ ist. Deswegen gelten die Assoziativität, die Kommutativität bezüglich Addition und Multiplikation und die Distributivität von komplexen Zahlen. Aus dem gleichen Grund ist 1 das Einselement in $\mathbb{Z}[i]$. Es bleibt nur die Abgeschlossenheit bezüglich Addition und Multiplikation zu zeigen.

Seien $x = a + bi$, $y = c + di$ Gausszsche Zahlen, mit $a, b, c, d \in \mathbb{Z}$ und $i \in \mathbb{C}$ mit $i^2 = -1$.

$(\mathbb{Z}[i], +)$ ist *abgeschlossen*: $x + y = (a + c) + (b + d)i \in \mathbb{Z}[i]$.

$(\mathbb{Z}[i], \cdot)$ ist *abgeschlossen*: $x \cdot y = (a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i \in \mathbb{Z}[i]$. $\square$

Mit der Betrachtung von $\mathbb{Z}[i]$ als Unterring von $\mathbb{C}$ ist es offensichtlich, dass die Begriffe von komplexen Zahlen für Gausssche Zahlen gelten, wenn $\mathbb{Z}$ statt $\mathbb{R}$ betrachtet wird. So stimmen z.B. die Konjugationsabbildung und die Rechnenregeln mit dem konjugierten Element mit denen der komplexen Zahlen überein. Der Betrag von komplexen Zahlen für Gausssschen Zahlen nennt man Norm. Wegen der Wichtigkeit des Begriffes für diese Arbeit, definieren wir ihn gesondert.

Definition 1.3. Für jede komplexe Zahl $x = a + bi$ mit $a, b \in \mathbb{Z}$ heißt

$$N(x) = |x|^2 = x\overline{x} = a^2 + b^2$$

die *Norm* von x.

Die Norm ist multiplikativ:

$$N(xy) = xy\overline{xy} = xy(\overline{yx}) = x(y\overline{y})\overline{x} = x\overline{x}y\overline{y} = N(x)N(y)$$

mit $x, y \in \mathbb{Z}[i]$.
In $\mathbb{C}$ haben alle Elemente außer 0 ein Inverses aus $\mathbb{C}$ bezüglich der Multiplikation d.h. sie sind Einheiten [vgl.[5], Definition 4.17(f)]. In $\mathbb{Z}[i]$, der ein Ring ist, sind nur 4 solche Elemente vorhanden.

Definition 1.4. $\mathbb{Z}[i]^* := \{1, -1, i, -i\}$ heißt *Menge der Einheiten von* Gausss*chen Zahlen.*

Lemma 1.5. *Ist* $x \in \mathbb{Z}[i]^*$*, dann gilt* $N(x) = 1$.

Beweis. Ist $N(x) = a^2 + b^2 = 1$ mit $a, b \in \mathbb{Z}$, dann gilt

$$\begin{aligned} \text{entweder} \quad & x = \pm i \quad \text{mit } a = 0 \text{ und } b = \pm 1, \\ \text{oder} \quad & x = \pm 1 \quad \text{mit } a = \pm 1 \text{ und } b = 0. \end{aligned}$$

$\square$

Satz 1.6. *Der Ring* $\mathbb{Z}[i]$ *ist euklidisch, d.h. zu* $x, y \in \mathbb{Z}[i]$ *mit* $y \neq 0$ *gibt es* $q, r \in \mathbb{Z}[i]$ *mit*

$$x = yq + r \quad \textit{und} \quad N(r) \leq \tfrac{1}{2}N(y).$$

Beweis. Der Ring $\mathbb{Z}[i]$ hat keinen anderen Nullteiler außer 0, er ist nullteilerfrei.
Sei $z = \frac{x}{y} = c + id \quad \text{mit} \quad c, d \in \mathbb{Q}$. Zu c, d gibt es eine Approximation $c', d' \in \mathbb{Z}$ derart, dass $|c - c'| \leq \frac{1}{2} \quad \text{und} \quad |d - d'| \leq \frac{1}{2}$ gilt. Wir schreiben den ganzen Teil von z als $q = c' + id' \in \mathbb{Z}[i]$ auf. Es sei $r = x - yq$. Dann gilt

$$|z - q|^2 = |(c - c') + i(d - d')|^2 = |c - c'|^2 + |d - d'|^2 \leq (\tfrac{1}{2})^2 + \left(\tfrac{1}{2}\right)^2 = \tfrac{1}{2}.$$

Also ist $N(r) = |r|^2 = |x - yq|^2 = |y(\frac{x}{y} - q)|^2 = |y|^2|z - q|^2 \leq \frac{1}{2}|y|^2 = \frac{1}{2}N(y)$. □

Der euklidische Zahlenring $\mathbb{Z}[i]$ ist ein Hauptidealring. Somit ist jedes irreduzible Element in $\mathbb{Z}[i]$ auch ein Primelement, und es gilt der Satz von der eindeutigen Primfaktorzerlegung [vgl.[5], Satz 11.6, 11.12, 11.14].

Definition 1.7. Die Primelemente von $\mathbb{Z}[i]$ heißen Gausssche *Primzahlen.*

Satz 1.8. *Wenn $x \in \mathbb{Z}[i]$ und $N(x)$ eine Primzahl in $\mathbb{Z}$ ist, dann ist x eine* Gausssche *Primzahl.*

Beweis. Sei $p = N(x)$ eine Primzahl und $x = yz$ mit $y, z \in \mathbb{Z}[i]$. Wegen $N(x) = N(yz) = N(y)N(z)$ ist entweder $N(y) = 1$ oder $N(z) = 1$, da $N(x)$ prim aus $\mathbb{N}$ und irreduzibel ist. Gemäß Lemma 1.5 ist y oder z eine Einheit und dann ist $x \in \mathbb{Z}[i]$ irreduzibel. □

Satz 1.9. *Sei $p \in \mathbb{N}$ eine ungerade Primzahl. Dann ist p entweder prim in $\mathbb{Z}[i]$ oder die Norm von einer* Gausssche *Primzahl in der Form $p = q\overline{q}$, wobei $q, \overline{q}$ zueinander nicht assoziierte* Gausssche *Primzahlen sind und $p = q\overline{q}$ eine Primfaktorzerlegung ist.*

Beweis. Die Primzahl p aus $\mathbb{N}$ ist in $\mathbb{Z}[i]$ in das Produkt der Primfaktoren

$$p = uq_1q_2 \dots q_n$$

mit $u \in \mathbb{Z}[i]^*$ und Gausschen Primzahlen q_i zerlegbar. Gemäß Lemma 1.5 gilt

$$p^2 = N(p) = N(uq_1q_2 \dots q_n) = N(q_1)N(q_2) \dots N(q_n).$$

Ist $0 \neq p \in \mathbb{N}$ und $N(q_j)$ keine Einheit ist, dann ist $0 \neq N(q_j)$ aus $\mathbb{N}$. Daraus folgt, dass

$$p^2 = \prod_{j \in \mathbb{N}} N(q_j)$$

ist, mit $1 \leq j \leq 2$.

Wir betrachten zwei Fälle.
1. Fall: Sei $j = 1$ und $p = uq_1$.
Hier ist q_1 eine GAUSSsche Primzahl und u ist eine Einheit, dann sind p und q_1 zueinander assoziiert und p ist auch eine GAUSSsche Primzahl.
2. Fall: Sei $j = 2$ und $p = uq_1q_2$.
Es ist $p^2 = N(p) = N(q_1)N(q_2)$. Somit ist $q_1\overline{q_1} = N(q_1) = p = N(q_2) = q_2\overline{q_2}$ mit $N(q_1), N(q_2) \neq 1$. Sei q_1 und q_2 die GAUSSschen Primzahlen d.h. $q_1 \neq q_2$, dann ist offensichtlich q_1 zu $\overline{q_2}$ assoziiert (bzw. q_2 zu $\overline{q_1}$ assoziiert) und es gilt, dass $\overline{q_1}, \overline{q_2}$ GAUSSsche Primzahlen sind. Wir setzen $q = q_1$, daher ist $p = q\overline{q}$. Diese Bezeichnung wenden wir im Beweis weiter an.
Nehmen wir an, dass q und $\overline{q}$ zueinander assoziiert sind, dann gilt $uq = \overline{q}$ mit $q = a + bi \in \mathbb{Z}[i]$. Wir führen den Beweis weiter mit der Fallunterscheidung für die Einheit u.
2.a. Fall: Sei $u = \pm 1$.
Hier gilt entweder $p = q\overline{q} = q^2 = (a + bi)^2$ bei $u = 1$ oder $p = q\overline{q} = -q^2 = -(a + bi)^2$ bei $u = -1$. Es ist $p \in \mathbb{N}$, deswegen muss $a = 0$ oder $b = 0$ sein. Also ist entweder $p = a^2$ bei $b = 0$ und $u = 1$ oder $p = b^2$ bei $a = 0$ und $u = -1$. Aber dies widerspricht der Annahme, dass p eine Primzahl ist.
2.b. Fall: Sei $u = \pm i$.
Dann ist entweder $p = q\overline{q} = (a + bi)(-b + ai) = -2ab + (a^2 - b^2)i$ bei $u = i$ oder $p = q\overline{q} = (a+bi)(b-ai) = 2ab+(-a^2+b^2)i$ bei $u = -i$. Da $p \in \mathbb{N}$ ungerade ist und es gilt weiter entweder $p = 2a^2$ bei $a = -b$ und $u = i$ oder $p = 2b^2$ bei $a = b$ und $u = -i$. Also ist p nicht prim. Dies ist ein Widerspruch zur Annahme. □

Darstellung der GAUSSschen Zahlen durch 2×2 Matrizen

Die GAUSSsche Zahl $x = a + bi$ kann als eine Zahl, ein Zahlenpaar oder eine 2×2 Matrix aufgefasst werden.
Die Darstellung von GAUSSschen Zahlen als 2×2 Matrix bezieht sich auf die Darstellung von komplexen Zahlen. Sei

$$\Psi = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

die *Menge der reellen Matrizen, die komplexe Zahlen darstellen* [vgl.[3], § 2.3.5].

Die $\mathbb{R}$-lineare Abbildung

$$F : \mathbb{C} \to \Psi, \quad a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

ist ein *Körperisomorphismus* mit $I := F(i) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad I^2 = -E.$

Das Produkt der Multiplikation von zwei beliebigen Matrizen A $= \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ und B $= \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$ aus Ψ ist

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix}. \tag{1.1}$$

Wenn man mit Matrizen rechnet, dann fordert die Multiplikation immer eine besondere Beachtung, weil sie im Allgemeinen nicht kommutativ ist. Das Produkt aus Gleichung (1.1) ist kommutativ, wie man leicht nachrechnen kann. Daher ist Ψ bezüglich der Matrizenaddition, Matrizenmultiplikation ein *Körper* mit der Einheitsmatrix E als Einselement.

Definition 1.10. Die Menge $\mathbb{G} := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ heißt *die Menge der Matrizen der* Gausschen Zahlen.

Satz 1.11. $(\mathbb{G}, +, \cdot)$ *ist ein kommutativer Unterring von* Ψ.

Beweis. Wegen des Körperisomorphismus F und $\mathbb{Z}[i] \subset \mathbb{C}$ gilt, dass der kommutative Ring $\mathbb{Z}[i]$ in $\mathbb{G}$ übergeht. □

Definition 1.12. $\mathbb{G}^* := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$ heißt *Einheitsmenge der Matrizen der* Gausschen Zahlen.

1.2 Primzahlen als Summe zweier Quadrate

Nach der Betrachtung der Gaussschen Zahlen beschäftigen wir uns in diesem Abschnitt mit Primzahlen als Summe von zwei Quadraten, die mit Hilfe der Gaussschen Zahlen berechnet werden. Wir betrachten auch die Elemente im Restklassenring $\mathbb{Z}/(p)$ als Summe von zwei Quadraten.

1.2.1 Primzahl als Summe zweier Quadrate

Satz 1.13. *Eine Primzahl p kann genau dann als Summe zweier Quadrate geschrieben werden, wenn entweder $p \equiv 1$ mod 4 oder $p = 2$ ist. Eine solche Darstellung ist bis auf die Reihenfolge eindeutig.*

Beweis. Die quadratischen Reste modulo 4 sind 0 und 1. Die Summen von zwei quadratischen Resten sind $0, 1, 2$. Dann muss für eine Primzahl $p = a^2 + b^2$ entweder $p \equiv 0 \bmod 2$, was nur der Zahl $p = 2 = 1^2 + 1^2$ entspricht, oder $p \equiv 1 \bmod 4$ gelten. Umgekehrt, sei $p \equiv 1 \bmod 4$. Wir betrachten die Gleichung $t^2 \equiv -1 \bmod p$. Die prime Restklassengruppe $(\mathbb{Z}/(p))^*$ ist zyklisch der Ordnung $p - 1$ [vgl.[9], Folgerung 6.2.2, Korollar 6.1.2]. Wegen der Zyklizität besitzt $(\mathbb{Z}/(p))^*$ mindestens ein primitives Element g, so dass $g^j \not\equiv 1 \bmod p$ für $1 \leq j \leq p - 2$. Das primitive Element heißt *das erzeugende Element*, weil es für jedes $a \in (\mathbb{Z}/(p))^*$ ein eindeutig bestimmtes j gibt mit $0 \leq j \leq p - 2$ und $g^j \equiv a \bmod p$, d.h. es wird eine Potenz j zu jedem Element $a \in (\mathbb{Z}/(p))^*$ zugeordnet.
Für die Existenz eines solchen j zu $\sqrt{-1}$ wenden wir einen Gruppenisomorphismus an [vgl.[1], Bemerkung 5.6]:

$$\begin{array}{ccc} \big(\mathbb{Z}/(p-1), +\big) & \longrightarrow & \big((\mathbb{Z}/(p))^*, \cdot\big), \\ j & \longmapsto & g^j. \end{array} \tag{1.2}$$

Sei $p = 4k + 1$ mit $k \in \mathbb{N}$, dann sieht die Abbildung (1.2) folgendermaßen aus

$$\frac{p-1}{2} = 2k \mapsto -1,$$

da dies das einzige Element $\neq 1$ ist, dessen Quadrat 1 ist. Und

$$k \mapsto \sqrt{-1}.$$

Also ist die Kongruenz $t^2 \equiv -1 \bmod p$ lösbar, d.h. es gibt ein $m \in \mathbb{N}$, so dass $mp = t^2 + 1$ ist. Die Gleichung $mp = t^2 + 1$ in $\mathbb{Z}[i]$ sieht folgendermaßen aus:

$$mp = t^2 + 1 = (t + i)(t - i).$$

Wäre p eine Gausssche Primzahl, dann gelte $p|t + i$ oder $p|t - i$. Aber es gibt

$$\begin{array}{rll} \text{weder} & t + i = p(u + vi) = pu + pvi & \text{mit } pv = 1 \\ \text{noch} & t - i = p(z + wi) = pz + pwi & \text{mit } pw = 1, \end{array}$$

wobei $u + vi, z + wi \in \mathbb{Z}[i]$. Also ist p keine GAUSSsche Primzahl und gemäß Satz 1.9 eine Norm, die eine Summe von zwei Quadraten ist.
Wir kommen zur Eindeutigkeit.
Es ist $p = a^2 + b^2 = N(x) = x \cdot \overline{x}$ mit $x = a + bi$. Nach Satz 1.9 ist x eine GAUSSsche Primzahl. Die Zahl $p = q_1 q_2$ in $\mathbb{Z}[i]$ keine GAUSSsche Primzahl, dann sind die Faktoren q_1, q_2 zueinander nicht assoziiert. Wir setzen $q = q_1$, dann ist $p = q\overline{q}$.
Also muss wegen der Eindeutigkeit der Primfaktorzerlegung von p die Zahl x eine zu q oder $\overline{q}$ assoziierte GAUSSsche Zahl sein und $\overline{x}$ assoziiert zu der anderen der beiden. □

1.2.2 Elemente im Restklassenring $\mathbb{Z}/(p)$ als Summe zweier Quadrate

In nächstem Kapitel, wo wir die natürlichen Zahlen als Summe von vier Quadraten betrachten, brauchen wir die Darstellung der Elemente aus dem Ring $\mathbb{Z}/(p)$ als Summe von zwei Quadraten.

Satz 1.14. *Sei p eine Primzahl. Zu jedem x im Restklassenring $\mathbb{Z}/(p)$ gibt es $a, b \in \mathbb{Z}/(p)$ mit $x = a^2 + b^2$ in $\mathbb{Z}/(p)$.*

Beweis. $p = 2$: Dann ist jedes Element aus $\mathbb{Z}/(2)$ ein Quadrat. Deshalb gibt es für jedes Element trivialerweise eine Darstellung als Summe von zwei Quadraten.
$p > 2$: Um eine Darstellung als Summe von zwei Quadraten für eine ungerade Primzahl zu erhalten, verwenden wir die Abbildung

$$\varphi : \mathbb{Z}/(p) \longrightarrow \mathbb{Z}/(p), \quad a \mapsto a^2,$$

und erhalten dadurch als Bild der Abbildung alle Quadrate in $\mathbb{Z}/(p)$. Die Anzahl der Bildelemente beträgt $\frac{p+1}{2}$ [vgl.[1], Satz 7.1]. Als Nächstes wählen wir die Abbildung

$$\psi : \mathbb{Z}/(p) \longrightarrow \mathbb{Z}/(p), \quad z \mapsto x - z.$$

Die Funktion ψ ist bijektiv. Wir komponieren die beiden Abbildungen zu

$$\psi \circ \varphi : \mathbb{Z}/(p) \longrightarrow \mathbb{Z}/(p), \quad a \mapsto x - a^2.$$

Das Bild dieser Abbildung enthält wieder $\frac{p+1}{2}$ Elemente, da ψ bijektiv ist und die Anzahl der Bildelemente sich nicht verändert. Ist x ein Quadratrest modulo p, dann sind wir fertig.
Das Bild der komponierten Abbildung liefert wieder $\frac{p+1}{2}$ Elemente und davon gibt es höchstens $\frac{p-1}{2}$ Nichtquadrate. Also gibt es mindestens $\frac{p+1}{2} - \frac{p-1}{2} = 1$ Quadrate vom Bild. □

1.3 Natürliche Zahlen als Summe zweier Quadrate

Nach dem Fundamentalsatz der Arithmetik hat jede natürliche Zahl n eine eindeutige Primfaktorzerlegung. Alle Primfaktoren, die als Summe von zwei Quadraten darstellbar sind, haben wir im Abschnitt 1.2 bestimmt. In diesem Abschnitt zeigen wir, welche natürlichen Zahlen sich als Summe zweier Quadrate darstellen lassen und die Rolle der anderen Primfaktoren in einer solchen Darstellung.

Satz 1.15. *Eine natürliche Zahl n ist genau dann eine Summe zweier Quadrate, wenn der Exponent von jedem Primfaktor $p \equiv 3 \mod 4$ in der Primfaktorzerlegung von n gerade ist.*

Beweis. Sei $n = m \cdot x$ mit

$$\begin{aligned} &m \text{ ist das Produkt von allen Primfaktoren} \quad p \equiv 3 \bmod 4 \quad \text{und} \\ &x \text{ ist das Produkt von allen Primfaktoren} \quad p \not\equiv 3 \bmod 4, \end{aligned}$$

wobei $m, x \in \mathbb{N}$.
Die Primfaktoren $p \not\equiv 3 \bmod 4$ sind keine Gausschen Primzahlen und sind gemäß Satz 1.9 Normen. Dann ist

$$x = p_1 \cdot \ldots \cdot p_s = N(p_1^{'}) \cdot \ldots \cdot N(p_s^{'}) = N(p_1^{'} \cdot \ldots \cdot p_s^{'}) = a^2 + b^2$$

mit $p_j \in \mathbb{Z}[i]$. Also ist x eine Summe zweier Quadrate.

Sei m eine Quadratzahl, $m = c^2$ d.h. dass der Exponent von allen Primfaktoren $p \equiv 3 \bmod 4$ in n gerade ist, dann ist

$$n = c^2(a^2 + b^2) = (ca)^2 + (cb)^2$$

Also ist n Summe von zwei Quadraten.
Umgekehrt, sei $n = a^2 + b^2$ und $\mathrm{ggT}(a, b) = d$. Dann gilt $d^2 | \, n$.

$$n_1 = \frac{n}{d^2} = \frac{a^2}{d^2} + \frac{b^2}{d^2} = {a_1}^2 + {b_1}^2 \text{ mit } \mathrm{ggT}(a_1, b_1) = 1.$$

Es ist $\mathrm{ggT}(n_1, a_1 b_1) = 1$. Ist nämlich p ein Primteiler von n_1 und wäre p auch ein Teiler von a_1, so wäre $p | n - a_1^2 = b_1^2$ und damit wäre $p | b_1$ im Widerspruch zur Teilerfremdheit von a_1 und b_1, also $p \nmid a_1 b_1$.
Der Restklassenring $\mathbb{Z}/(p)$ ist ein Körper und sei $[b_1] \in \mathbb{Z}/(p)$ die Restklasse. Daraus

folgt, dass für die Restklasse $[b_1]$ eine inverse Restklasse $[k] \in \mathbb{Z}/(p)$ existiert, so dass $[b_1][k] = [1]$ ist. Dann ist $b_1 k \equiv 1 \bmod p$. Es ist $p|{a_1}^2 + {b_1}^2$ d.h.

$$\begin{aligned} {a_1}^2 + {b_1}^2 &\equiv 0 \bmod p \\ (a_1 k)^2 + (b_1 k)^2 &\equiv 0 \bmod p \\ (a_1 k)^2 + 1 &\equiv 0 \bmod p \\ (a_1 k)^2 &\equiv -1 \bmod p. \end{aligned}$$

Also gibt es einen quadratischen Rest -1 modulo p. Dies ist aber für $p \equiv 3 \bmod 4$ nicht möglich wegen einer ähnlichen Überlegung wie im Beweis von Satz 1.13. Also hat die Zahl n_1 keine Primfaktoren $p \equiv 3 \bmod 4$. Sie können in d^2 und nur mit einem geraden Exponenten vorkommen. □

2 Quaternionen und Summe von vier Quadraten

Das Ziel dieses Kapitels ist die Betrachtung der Darstellung einer beliebigen natürlichen Zahl n als Summe von vier Quadraten. Dafür lernen wir die Quaternionen kennen, die als Zahlen im vierdimensionalen $\mathbb{R}$-Vektorraum definiert sind. Danach definieren wir die Verknüpfungen Addition und Multiplikation anschließend betrachten wir einige wichtige Eigenschaften. Am Ende des Kapitels beweisen wir den Satz von Lagrange, den „Vier-Quadrate-Satz“, mit Hilfe der neu gelernten Zahlen und eines weiteren Satzes.

2.1 Quaternionen - Hamiltonsche Zahlen

William Rowan Hamilton[1] hatte die komplexen Zahlen als Zahlenpaare angegeben. Dieses war der Ausgangspunkt des Interesses an der Frage, ob eine entsprechende Form im Raum $\mathbb{R}^3$ existiert. Hamilton hat jahrelang gehofft, eine Multiplikation für reelle Tripel mit guten Eigenschaften zu finden; heute weiß man, dass keine solche existiert [vgl.[3], 7. §1.1]. Am 16. Oktober 1843 hat Sir Hamilton auf dem Wege zur Sitzung der Royal Irish Academy einen genialen Einfall gehabt. Er hat verstanden, dass diese Produktregel gilt, wenn man bereit ist, die Kommutativität zu opfern und damit in eine neue Dimension zu springen.
Die weitere Details der Entdeckungsgeschichte der Quaternionen kann in der Broschüre „Hamiltons Entdeckung der Quaternionen, Erweiterte Fassung einen Vortrages“ [13] von Bartel Leendert van der Waerden nachgelesen werden.

Die neu entdeckten Quaternionen[2], welche mit einem Realteil und drei Imaginärteilen eine Erweiterung der komplexen Zahlen bilden, nennt man Hamilton zu Ehren Hamilton-*Zahlen* und wir bezeichnet sie mit $\mathbb{H}$.

Nach der Entdeckung der Quaternionen-Algebra ist klar geworden, dass man die Rechengesetze für Quaternionen schon früher besessen hatte. So z.B. treten die Quaternionenformeln in einer kurzen Note über *Mutationen des Räumes* von Gauss 1819 auf,

[1] Sir William Rowan Hamilton (* 4. August 1805 in Dublin; †2. September 1865 in Dunsink, bei Dublin) war ein irischer Mathematiker und Physiker.
[2] von lat. quaternio - Vierheit.

auch ist der Vier-Quadrate-Satz eine typische Produktregel für Quaternionen.

Definition 2.1. Seien $a_1, a_2, a_3, a_4 \in \mathbb{R}$ und i, j, k Symbole. Die Zahl

$$x := (a_1, a_2, a_3, a_4) := a_1 + a_2 i + a_3 j + a_4 k,$$

heißt eine *Quaternion*.

Die HAMILTON-Zahlen sind die geordneten reellen Quadrupel im vierdimensionalen $\mathbb{R}$-Vektorraum $\mathbb{R}^4$ mit Standardbasis

$$1 := (1,0,0,0),\ i := (0,1,0,0),\ j := (0,0,1,0) \text{ und } k := (0,0,0,1).$$

Wir definieren die Verknüpfungen *Addition, Multiplikation* und die Relation *Gleichheit* für die HAMILTON-Zahlen.

Definition 2.2. Seien $x = a_1 + a_2 i + a_3 j + a_4 k,\ y = b_1 + b_2 i + b_3 j + b_4 k$ Quaternionen und $c \in \mathbb{R}$.

1. *Zwei Quaternionen sind dann gleich*, wenn sie in allen Komponenten übereinstimmen:

$$x = y \quad \Leftrightarrow \quad a_1 = b_1,\ a_2 = b_2,\ a_3 = b_3,\ a_4 = b_4.$$

2. *Die Addition von Quaternionen* ist komponentenweise definiert:

$$x + y = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k.$$

3. *Die Multiplikation einer Quaternion mit Skalar* ist komponentenweise definiert:

$$cx = ca_1 + ca_2 i + ca_3 j + ca_4 k.$$

4. Die Rechenregeln

$$\begin{aligned} i \cdot j &= k \quad \text{und} \quad j \cdot i = -k \\ j \cdot k &= i \quad \text{und} \quad k \cdot j = -i \\ k \cdot i &= j \quad \text{und} \quad i \cdot k = -j \end{aligned}$$

$$i^2 = j^2 = k^2 = ijk = -1$$

heißen HAMILTON*sche Regeln*.

5. *Die Multiplikation von zwei Quaternionen* wird definiert durch assoziierte Fortsetzung der HAMILTONschen Regeln:

$$\begin{aligned} x \cdot y &= (a_1 + a_2 i + a_3 j + a_4 k) \cdot (b_1 + b_2 i + b_3 j + b_4 k) \\ &= a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4 \\ &\quad + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) \cdot i \\ &\quad + (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) \cdot j \\ &\quad + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) \cdot k. \end{aligned}$$

Bemerkung 2.3. *Die Multiplikation der Imaginärteile aus* $\mathbb{H}$ *ist nicht kommutativ.*

Definition 2.4. Die Menge

$$\mathbb{H} := \{(a_1, a_2, a_3, a_4) \,|\, a_i \in \mathbb{R} \quad \text{für alle } i = 1, \ldots, 4\}$$

mit den in Definition 2.2 definierten Verknüpfungen heißt die *Menge der Quaternionen.*

Jetzt möchten wir die Darstellung einer Quaternion in der Matrixform betrachten. Dies erleichtert den Nachweis ihrer Eigenschaften.

Quaternion in der Form 4×4 Matrix

Außer der Darstellung einer Quaternion $x = a_1 + a_2 i + a_3 j + a_4 k$ als Zahl kann x als eine Matrix im Raum $\mathbb{R}^{4\times 4}$ geschrieben werden. Dazu multiplizieren wir die HAMILTON-Zahl x mit den Basisvektoren $(1, i, j, k)$. Danach werden die Ergebnisse in die Standard-Reihenfolge gebracht. Dies ergibt die Spalten der Matrix $M(x)$. Es ist

$$\begin{aligned} (a_1 + a_2 i + a_3 j + a_4 k) \cdot 1 &= a_1 + a_2 i + a_3 j + a_4 k \\ (a_1 + a_2 i + a_3 j + a_4 k) \cdot i &= a_1 i - a_2 - a_3 k + a_4 j \\ (a_1 + a_2 i + a_3 j + a_4 k) \cdot j &= a_1 j + a_2 k - a_3 - a_4 i \\ (a_1 + a_2 i + a_3 j + a_4 k) \cdot k &= a_1 k - a_2 j + a_3 i - a_4. \end{aligned}$$

Also sieht die Matrix folgendermaßen aus:

$$M(x) = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & -a_4 & a_3 \\ a_3 & a_4 & a_1 & -a_2 \\ a_4 & -a_3 & a_2 & a_1 \end{pmatrix}.$$

Bei den Quaternionen war anfangs nicht klar, ob die Multiplikation der Imaginärteile assoziativ ist. Wir wissen, dass die Matrizenmultiplikation assoziativ ist, weil $Mat(n \times n, \mathbb{R})$ ein Ring ist. Wir zeigen, dass $M(xy) = M(x)M(y)$ gilt und können daraus schließen, dass die Quaternionen- Multiplikation assoziiert ist.

Zuerst berechnen wir das Produkt von Matrizen von zwei Quaternionen. Sei

$$M(x) = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & -a_4 & a_3 \\ a_3 & a_4 & a_1 & -a_2 \\ a_4 & -a_3 & a_2 & a_1 \end{pmatrix}, \quad M(y) = \begin{pmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & -b_4 & b_3 \\ b_3 & b_4 & b_1 & -b_2 \\ b_4 & -b_3 & b_2 & b_1 \end{pmatrix}$$

mit $x, y \in \mathbb{H}$ und $a_i, b_i \in \mathbb{R}$ für alle $i = 1, \ldots, 4$.

Dann ist das Produkt von Matrizen M(x)M(y) =

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix},$$

wobei

$c_{11} = a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4, \quad c_{12} = -a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3,$
$c_{21} = a_1b_2 + a_2b_1 + a_3b_4 - a_3b_4, \quad c_{22} = a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4,$
$c_{31} = a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2, \quad c_{32} = a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1,$
$c_{41} = a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1, \quad c_{42} = -a_1b_3 + a_2b_4 - a_3b_1 - a_4b_2,$

$c_{13} = -a_1b_3 + a_2b_4 - a_3b_1 - a_4b_2, \quad c_{14} = -a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1,$
$c_{23} = -a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1, \quad c_{24} = a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2,$
$c_{33} = a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4, \quad c_{34} = -a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3,$
$c_{43} = a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3, \quad c_{44} = a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4$

mit $c_{ij} \in \mathbb{R}$ und $i, j = 1, \ldots, 4$ sind.

Als Nächstes berechnen wir die Matrix vom Produkt zweier Quaternionen. Dafür multiplizieren wir die Quaternionen x und y als Zahlen und stellen das Produkt als Matrix nach dem oben benutzten Verfahren.

$$\begin{aligned} z = x \cdot y &= (a_1 + a_2 i + a_3 j + a_4 k) \cdot (b_1 + b_2 i + b_3 j + b_4 k) \\ &= a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4 \\ &\quad + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) \cdot i \\ &\quad + (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) \cdot j \\ &\quad + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) \cdot k, \end{aligned}$$

$$\begin{aligned} z \cdot i &= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) \cdot i \\ &\quad - a_1 b_2 - a_2 b_1 - a_3 b_4 + a_4 b_3 \\ &\quad + (-a_1 b_3 + a_2 b_4 - a_3 b_1 - a_4 b_2) \cdot k \\ &\quad + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) \cdot j \\ &= - a_1 b_2 - a_2 b_1 - a_3 b_4 + a_4 b_3 \\ &\quad + (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) \cdot i \\ &\quad + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) \cdot j \\ &\quad + (-a_1 b_3 + a_2 b_4 - a_3 b_1 - a_4 b_2) \cdot k, \end{aligned}$$

$$\begin{aligned} z \cdot j &= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) \cdot j \\ &\quad + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) \cdot k \\ &\quad - a_1 b_3 + a_2 b_4 - a_3 b_1 - a_4 b_2 \\ &\quad + (-a_1 b_4 - a_2 b_3 + a_3 b_2 - a_4 b_1) \cdot i \\ &= - a_1 b_3 + a_2 b_4 - a_3 b_1 - a_4 b_2 \\ &\quad + (-a_1 b_4 - a_2 b_3 + a_3 b_2 - a_4 b_1) \cdot i \\ &\quad + (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) \cdot j \\ &\quad + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) \cdot k, \end{aligned}$$

$$\begin{aligned} z \cdot k &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) \cdot k \\ &\quad +(-a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3) \cdot j \\ &\quad +(a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2) \cdot i \\ &\quad -a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1 \\ &= -a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1 \\ &\quad +(a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2) \cdot i \\ &\quad +(-a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3) \cdot j \\ &\quad +(a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) \cdot k. \end{aligned}$$

Wie man leicht sehen kann, gilt Folgendes:

$$\begin{aligned} z \cdot 1 &= c_{11} + c_{21}i + c_{31}j + c_{41}k \\ z \cdot i &= c_{12} + c_{22}i + c_{32}j + c_{42}k \\ z \cdot j &= c_{13} + c_{23}i + c_{33}j + c_{43}k \\ z \cdot k &= c_{14} + c_{24}i + c_{34}j + c_{44}k \end{aligned}$$

d.h. M(xy) =

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}.$$

Wichtige Eigenschaften der Quaternionen

Die HAMILTON-Zahlen sind die Erweiterung der komplexen Zahlen $\mathbb{C}$ und werden auch die *hyperkomplexen Zahlen* genannt, da sie drei Imaginärteile haben. Die Darstellung einer Quaternion in komplexer Zahlenform kann durch Adjunktion von $j \in \mathbb{H}$ zu $\mathbb{C}$ gewonnen werden [vgl.[4], 29.2].

Bemerkung 2.5. *Sei* $\alpha = a_1 + a_2i, \beta = a_3 + a_4i \in \mathbb{C}$ *und* $x = a_1 + a_2i + a_3j + a_4k \in \mathbb{H}$, *wobei* $j, k \notin \mathbb{C}$. *Dann gilt*

$$x = (a_1 + a_2i) + (a_3 + a_4i)j = \alpha + \beta j \text{ für alle } x \in \mathbb{H}.$$

Die meisten Eigenschaften der Quaternionen und Abbildungen über Quaternionen übertragen sich von komplexen Zahlen, z.B. die Konjugation und die Norm einer Qua-

ternion.

Definition 2.6. Seien $a_1, a_2, a_3, a_4 \in \mathbb{R}$ und $x = (a_1, a_2, a_3, a_4) \in \mathbb{H}$. Die *Konjugationsabbildung* wird definiert durch

$$\mathbb{H} \longrightarrow \mathbb{H}, \quad x \longmapsto \overline{x},$$

wobei

$$\begin{aligned} \overline{x} &= \overline{(a_1, a_2, a_3, a_4)} = \overline{a_1 + a_2 i + a_3 j + a_4 k} = a_1 - a_2 i - a_3 j - a_4 k \\ &= (a_1, -a_2, -a_3, -a_4). \end{aligned}$$

Es gelten die folgenden Rechenregeln:
Seien $x = a_1 + a_2 i + a_3 j + a_4 k$ und $y = b_1 + b_2 i + b_3 j + b_4 k$. Dann ist

$$\begin{aligned} \overline{x+y} &= \overline{a_1 + a_2 i + a_3 j + a_4 k + b_1 + b_2 i + b_3 j + b_4 k} \\ &= \overline{a_1 + b_1 + (a_2 + b_2) \cdot i + (a_3 + b_3) \cdot j + (a_4 + b_4) \cdot k} \\ &= a_1 + b_1 - (a_2 + b_2) \cdot i - (a_3 + b_3) \cdot j - (a_4 + b_4) \cdot k \\ &= a_1 + b_1 - a_2 i - b_2 i - a_3 j - b_3 j - a_4 k - b_4 k \\ &= \underbrace{a_1 - a_2 i - a_3 j - a_4 k}_{\overline{x}} + \underbrace{b_1 - b_2 i - b_3 j - b_4 k}_{\overline{y}} \\ &= \overline{x} + \overline{y}. \end{aligned}$$

Aber es gilt in $\mathbb{H}$ im Gegensatz zu $\mathbb{C}$:

$$\begin{aligned}
\overline{x \cdot y} &= \overline{(a_1 + a_2 i + a_3 j + a_4 k) \cdot (b_1 + b_2 i + b_3 j + b_4 k)} \\
&= a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4 \\
&\quad -(a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) \cdot i \\
&\quad -(a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) \cdot j \\
&\quad -(a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) \cdot k \\
&= (b_1 - b_2 i - b_3 j - b_4 k) \cdot a_1 \\
&\quad -(b_2 + b_1 i - b_4 j + b_3 k) \cdot a_2 \\
&\quad -(b_3 + b_4 i + b_1 j - b_2 k) \cdot a_3 \\
&\quad -(b_4 - b_3 i + b_2 j + b_1 k) \cdot a_4 \\
&= (b_1 - b_2 i - b_3 j - b_4 k) \cdot a_1 \\
&\quad -(-b_2 i + b_1 - b_4 k - b_3 j) \cdot a_2 i \\
&\quad -(-b_3 j - b_4 k + b_1 - b_2 i) \cdot a_3 j \\
&\quad -(-b_4 k - b_3 j - b_2 i + b_1) \cdot a_4 k \\
&= \underbrace{(b_1 - b_2 i - b_3 j - b_4 k)}_{\overline{y}} \cdot \underbrace{(a_1 - a_2 i - a_3 j - a_4 k)}_{\overline{x}} \\
&= \overline{y} \cdot \overline{x}.
\end{aligned}$$

Man spricht in einem solchen Fall von einem *Antiautomorphismus*.

Definition 2.7. Seien $a_1, a_2, a_3, a_4 \in \mathbb{R}$ und $x = (a_1, a_2, a_3, a_4) \in \mathbb{H}$. Die Abbildung N heißt *Norm* und wird definiert durch

$$N : \mathbb{H} \longrightarrow \mathbb{H} \quad \text{mit} \quad N(x) := x \cdot \overline{x} \quad \text{für alle } x \in \mathbb{H}.$$

Bemerkung 2.8. *Sei $N(x)$ die Norm von $x \in \mathbb{H}$. Dann gilt*

$$N(x) = x \cdot \overline{x} = \overline{x} \cdot x \quad \textit{für alle } x \in \mathbb{H}.$$

Man rechnet

$$\begin{aligned} N(x) &= x \cdot \overline{x} \\ &= (a_1, a_2, a_3, a_4) \cdot (a_1, -a_2, -a_3, -a_4) \\ &= (a_1a_1 + a_2a_2 + a_3a_3 + a_4a_4, \\ &\quad -a_1a_2 + a_2a_1 - a_3a_4 + a_4a_3, \\ &\quad -a_1a_3 + a_3a_1 - a_4a_2 + a_2a_4, \\ &\quad -a_1a_4 + a_4a_1 - a_2a_3 + a_3a_2) \\ &= (\sum_{i=1}^{4} a_i^2, 0, 0, 0). \end{aligned}$$

Wie wir sehen, ist $N(x)$ eine Quaternion, in der die imaginären Teile gleich Null sind. Es erlaubt uns $N(x) \in \mathbb{H}$ mit einer Zahl aus $\mathbb{R}_+$ zu identifizieren. Also $N(x) \in \mathbb{R}_+$.

Man sieht, dass die Norm einer Quaternion eine Zahl als eine Summe von vier Quadraten gut beschreibt.

Satz 2.9. *Die Norm ist multiplikativ, d.h. es gilt*

$$N(x \cdot y) = N(x) \cdot N(y) \text{ für } x, y \in \mathbb{H}.$$

Beweis. Es gilt

$$N(xy) = x \cdot y \cdot \overline{x \cdot y} = x \cdot y \cdot \overline{y} \cdot \overline{x} = x \cdot N(y) \cdot \overline{x} = x \cdot \overline{x} \cdot N(y) = N(x) \cdot N(y).$$

□

Satz 2.10. $(\mathbb{H}, +, \cdot)$ *ist ein Schiefkörper.*

Beweis. Seien $x, y, z \in \mathbb{H}$ mit $x = (a_1, a_2, a_3, a_4)$, $y = (b_1, b_2, b_3, b_4), z = (c_1, c_2, c_3, c_4)$ und für alle $a_i, b_i, c_i \in \mathbb{R}$ mit $i = 1, \ldots, 4$.

$(\mathbb{H}, +)$ ist eine *abelsche Gruppe*:

$(\mathbb{H}, +)$ ist *abgeschlossen*:
Es ist $(\mathbb{R}, +)$ eine abelsche Gruppe. Und dann gilt mit Definition 2.2 im Punkt 2

$$x + y = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4) \in \mathbb{H}$$

$(\mathbb{H}, +)$ ist *assoziativ und kommutativ*:
Oben haben wir die Darstellung der Quaternionen als 4×4 Matrizen gesehen. Nach der Assoziativität, der Kommutativität der Rechenregeln von Matrizen gilt es, dass $(\mathbb{H}, +)$ assoziativ uns kommutativ ist.
$(\mathbb{H}, +)$ besitzt *ein neutrales Element*:
Durch $a_1 = a_2 = a_3 = a_4 = 0$ erhält man die Nullmatrix bzw. das Element

$$(0, 0, 0, 0) = 0 \in \mathbb{R}.$$

$(\mathbb{H}, +)$ besitzt zu jedem beliebigen Element ein *Negatives*:
Dies folgt ebenfalls aus der Eigenschaft, dass die reellen Zahlen einen Körper bilden. Es lautet $-x = (-a_1, -a_2, -a_3, -a_4) \in \mathbb{H}$.

$(\mathbb{H}, \cdot)$ ist *eine (nicht kommutative) Gruppe*:

$(\mathbb{H}, \cdot)$ ist *abgeschlossen*:
Da sowohl die a_s als auch die b_s nach Voraussetzung reell sind, sind die Einträge der Produkt-Quaternion in Definition 2.2 im Punkt 5 wieder reell, da $(\mathbb{R}, +, \cdot)$ ein Körper ist.
$(\mathbb{H}, \cdot)$ ist *assoziativ*:
Wegen der Matrizendarstellung der Quaternionen und der Assoziativität der Matrizenmultiplikation gilt, dass $(\mathbb{H}, \cdot)$ assoziativ ist.
$(\mathbb{H}, \cdot)$ besitzt *ein neutrales Element*:
Man erhält die Einheitsmatrix mit $a_1 = 1$ und $a_2 = a_3 = a_4 = 0$, was auf der Ebene der Zahlen gesprochen, dem Element $(1, 0, 0, 0) = 1 \in \mathbb{R} \subset \mathbb{H}$ entspricht.
Zu jedem von Null verschiedenem Element $x \in \mathbb{H}$ existiert ein *Inverses* $x^{-1} \in \mathbb{H}$:
Das multiplikative Inverse x^{-1} zu x kann leicht mit der Norm Abbildung [vgl. Definition 2.7] gefunden werden. Sei $x \neq 0$, dann ist mindestens ein $a_i \neq 0$ in x. Und folglich

$$N(x) = x\overline{x} = \sum_{i=1}^{4} a_i^2 > 0.$$

Also

$$\begin{aligned} x^{-1} &= \frac{\overline{x}}{\sum_{i=1}^{4} a_i^2} \\ &= \frac{a_1 - a_2 i - a_3 j - a_4 k}{a_1^2 + a_2^2 + a_3^2 + a_4^2} \in \mathbb{H}. \end{aligned}$$

Es gilt das *Links- bzw. Rechtsdistributivgesetz:*
Wegen der Nichtkommutativität bzgl. der Multiplikation muss man hier zwischen Multiplikation von links und rechts unterscheiden. Beides folgt aus den Distributivgesetzen für Matrizen. □

Jetzt definieren wir analog zum GAUSSschen Zahlenring $\mathbb{Z}[i] \subseteq \mathbb{C}$ einen Unterring des Schiefkörpers, nämlich $\mathbb{H}_\mathbb{Z}$.

Definition 2.11. Der *Ring der ganzen Quaternionen* wird durch

$$\mathbb{H}_\mathbb{Z} := \{(a_1, a_2, a_3, a_4) \,|\, a_i \in \mathbb{Z}, \text{ für alle } i = 1, \ldots, 4\}$$

definiert. Die Elemente des Ringes $\mathbb{H}_\mathbb{Z}$ heißen *ganze Quaternionen.*

Die Norm einer ganzen Quaternion ist offenbar eine natürliche Zahl. Gemäß Satz 2.9 gilt weiter, dass das Produkt von zwei natürlichen Zahlen m und n, die jeweils eine Summe von vier Quadraten sind, auch eine Summe von vier Quadraten ist.

Für das Weitere brauchen wir den Begriff der Teilbarkeit und den der modularen Äquivalenz zweier Elemente in $\mathbb{H}_\mathbb{Z}$. Diese Definition lehnt sich an die Definitionen an, wie wir sie bereits für kommutative Ringe kennen.

Definition 2.12. Seien $x, y \in \mathbb{H}_\mathbb{Z}$ mit $x = (a_1, a_2, a_3, a_4)$ und $y = (b_1, b_2, b_3, b_4)$. Sei weiter $m \in \mathbb{Z}$.

1. Dann heißt m ein *Teiler* von x, wenn m jede Komponente von x teilt:

   $$m|x \iff m|a_s \qquad \text{für alle } s = 1, \ldots, 4$$

   d.h. es gibt ein $z \in \mathbb{H}_\mathbb{Z}$ mit

   $$x = m \cdot z.$$

2. Zwei ganze Quaternionen heißen zueinander *äquivalent modulo* m, wenn sie denselben Rest bzgl. des Teilers m besitzen:

   $$x \equiv y \bmod m \iff m|x - y$$

   d.h., dass die Division durch m der einzelnen Komponenten von x und y den gleichen Rest geben:

   $$a_s \equiv b_s \bmod m$$

   für $s = 1, \ldots, 4$.

Lemma 2.13. *Seien $n \in \mathbb{Z}$ und x, y, y' ganze Quaternionen. Dann folgt aus*

$$y \equiv y' \bmod m$$

bereits

$$xy \equiv xy' \bmod m.$$

Beweis. Nach dem Punkt 2 der vorhergehenden Definition lässt sich wegen der Äquivalenz von y und y' ein $z \in \mathbb{H}_{\mathbb{Z}}$ finden, derart, dass

$$y - y' = m \cdot z.$$

Dann ist

$$xy - xy' = x \cdot (y - y') = x \cdot m \cdot z = m \cdot (x \cdot z),$$

was der obigen Behauptung entspricht. □

2.2 Natürliche Zahlen als Summe von vier Quadraten

Im ersten Kapitel der Arbeit haben wir die natürlichen Zahlen als Summe von zwei Quadraten beleuchtet. Und damit haben wir gesehen, dass nicht jede natürliche Zahl sich in dieser Form schreiben lässt. In diesem Abschnitt zeigen wir, dass jede beliebige natürliche Zahl als Summe von vier Quadraten darstellbar ist. Wir fangen mit einem Hilfssatz an.

Satz 2.14. *Zu jeder Primzahl $p \geq 3$ gibt es $a, b, m \in \mathbb{N}$ derart, dass*

$$a^2 + b^2 + 1 = mp,$$

wobei $0 < m < \frac{p}{2}$.

Beweis. Nach Satz 1.14 existiert für jedes Element in $\mathbb{Z}/(p)$ eine Darstellung als Summe von zwei Quadraten. Wir haben also insbesondere die Gleichung

$$a'^2 + b'^2 \equiv -1 \bmod p \Longleftrightarrow a'^2 + b'^2 + 1 \equiv 0 \bmod p,$$

wobei $a', b' \in \mathbb{Z}$ sind. Da wir modulo p rechnen können, wählen wir a' und b' aus dem ganzzahligen Intervall $[0, p-1]$. Da wir negative Zahlen zulassen, können wir auch aus dem Intervall $[\frac{-p+1}{2}, \frac{p-1}{2}]$ wählen. Da a'^2 und b'^2 natürliche Zahlen sind, setzen wir $a = |a'|$ und $b = |b'|$, so dass $a^2 = a'^2$ und $b^2 = b'^2$ ist. Dann gibt es ein $m \in \mathbb{N}$, so dass

$a^2 + b^2 + 1 = mp$ gilt.

Wir schätzen dieses m ab:

$$mp = a^2 + b^2 + 1 \leq 2 \cdot \left(\frac{p-1}{2}\right)^2 + 1 = \frac{p^2 - 2p + 3}{2} \leq \frac{p^2 - 6 + 3}{2} < \frac{p^2}{2}.$$

Daraus folgt, dass $0 < m < \frac{p}{2}$ ist. □

Wie beweisen jetzt den Satz von Lagrange.

Satz 2.15 (Lagrange)**.** *Jede natürliche Zahl ist Summe von vier Quadraten natürlicher Zahlen.*

Beweis. Nach dem Fundamentalsatz der Arithmetik hat jede natürliche Zahl n eine eindeutige Primfaktorzerlegung und wegen Satz 2.9 genügt es zu beweisen, dass die Primfaktoren eine Darstellung als Summe von vier Quadraten besitzen. Für $n = 0, 1, 2$ ist die Aussage trivial.

$$0 = 0 + 0 + 0 + 0$$
$$1 = 1 + 0 + 0 + 0$$
$$2 = 1 + 1 + 0 + 0.$$

Sei p eine ungerade Primzahl. Nach Satz 2.14 gibt es eine natürliche Zahl $n = mp$ als Summe von drei Quadraten mit $0 < m < \frac{p}{2}$. Sei nun $m_0 < \frac{p}{2}$ und $m_0 \in \mathbb{N}$ minimal mit der Eigenschaft, dass

$$m_0 p = a_1^2 + a_2^2 + a_3^2 + a_4^2 \quad \text{mit ganzen Zahlen } a_i \text{ und } i = 1, \ldots, 4 \text{ ist.} \tag{2.1}$$

Zunächst nehmen wir an, dass m_0 gerade ist, dann ist das Produkt $m_0 \cdot p$ wieder gerade. Dann müssen keine, zwei oder alle Zahlen $a_1, \ldots, a_4$ gerade sein. Nach Permutationen gilt, dass die Quotienten

$$\frac{a_1 + a_2}{2}, \frac{a_1 - a_2}{2}, \frac{a_3 + a_4}{2}, \frac{a_3 - a_4}{2} \text{ aus } \mathbb{Z} \text{ sind.}$$

Aber dann ist

$$\begin{aligned} & \left(\frac{a_1+a_2}{2}\right)^2+\left(\frac{a_1-a_2}{2}\right)^2+\left(\frac{a_3+a_4}{2}\right)^2+\left(\frac{a_3-a_4}{2}\right)^2 \\ = \; & \frac{1}{4}\cdot((a_1+a_2)^2+(a_1-a_2)^2+(a_3+a_4)^2+(a_3-a_4)^2) \\ = \; & \frac{1}{2}\cdot(a_1^2+a_2^2+a_3^2+a_4^2)=\frac{m_0}{2}\cdot p. \end{aligned}$$

Das ist ein Widerspruch zur Annahme der Minimalität von m_0. Also muss m_0 ungerade sein. Im Fall $m_0 = 1$ sind wir fertig. Wir nehmen jetzt an, dass $m_0 > 1$ ist. Wir führen die Division mit Rest für jedes a_i aus (2.5) durch m_0

$$a_i = m_0 \cdot q_i + b_i, \tag{2.2}$$

wobei $q_i, b_i \in \mathbb{Z}$ und b_i der Rest aus dem Intervall $]-\frac{m_0}{2}, \frac{m_0}{2}[$ ist. Wir betrachten nun $x = (a_1, a_2, a_3, a_4)$ und $y = (b_1, b_2, b_3, b_4)$ mit x, y aus $\mathbb{H}_\mathbb{Z}$. Die Norm von y ist die Summe der Quadratreste:

$$N(y) = \sum_{i=1}^{4} b_i^2 < 4 \cdot (\frac{m_0}{2})^2 = m_0^2.$$

Wegen $a_i = m_0 \cdot q_i + b_i$ gilt, dass

$$a_i^2 = m_0^2 \cdot q_i^2 + 2 \cdot m_0 \cdot q_i \cdot b_i + b_i^2 = m_0 \cdot (m_0 \cdot q_i^2 + 2 \cdot q_i \cdot b_i) + b_i^2$$

ist. Die Norm von x ist die Summe der a_i^2 aus (2.5):

$$\begin{aligned} N(x) &= \sum_{i=1}^{4} a_i^2 = \sum_{i=1}^{4} (m_0 \cdot (m_0 q_i^2 + 2 q_i \cdot b_i) + b_i^2) \\ &= m_0 \cdot \underbrace{\sum_{i=1}^{4} (m_0 q_i^2 + 2 q_i \cdot b_i)}_{=:c} + \sum_{i=1}^{4} b_i^2 = m_0 \cdot c + N(y). \end{aligned}$$

Wir erhalten, dass

$$N(x) - N(y) = m_0 \cdot c \Longrightarrow N(x) \equiv N(y) \equiv 0 \bmod m_0.$$

Dann gibt es ein $m_1 \in \mathbb{N}$ derart, dass $N(y) = m_1 \cdot m_0$. Und wegen $N(y) < m_0^2$, muss $m_1 < m_0$ sein.

Wäre $m_1 = 0$, dann $y = 0$ und damit sämtliche $b_i = 0$. Gemäß 2.9 wäre

$$m_0 \cdot p = N(x) = \sum_{i=1}^{4} a_i^2 = \sum_{i=1}^{4} (m_0 \cdot q_i)^2 = m_0^2 \sum_{i=1}^{4} q_i^2$$

und es wäre

$$p = m_0 \sum_{i=1}^{4} q_i^2.$$

Da aber p eine Primzahl ist und $m_0 > 1$ und $m_0 < \frac{p}{2}$ ist, ist dies ein Widerspruch. Also muss $m_1 \neq 0$ sein. Es ist $a_i - b_i = m_0 \cdot q_i$, d.h. $a_i \equiv b_i \bmod m_0$ und gemäß Definition 2.12 und Lemma 2.13 gilt

$$\begin{aligned} x &\equiv y \bmod m_0 \\ \overline{x} \cdot x &\equiv \overline{x} \cdot y \bmod m_0. \end{aligned}$$

Weil $\overline{x} \cdot x = N(x) \equiv 0 \bmod m_0$ ist, ist dann auch $\overline{x} \cdot y \equiv 0 \bmod m_0$. Dann gibt es ein $z \in \mathbb{H}_{\mathbb{Z}}$, so dass

$$\overline{x} \cdot y = z \cdot m_0 \quad \text{und} \quad z = \frac{1}{m_0} \cdot \overline{x} \cdot y \text{ gilt.}$$

Die Norm von z ist

$$\begin{aligned} N(z) &= N\left(\frac{1}{m_0}\overline{x} \cdot y\right) = \frac{1}{m_0^2} \cdot N(\overline{x}y) = \frac{1}{m_0^2} \cdot N(\overline{x}) \cdot N(y) \\ &= \frac{1}{m_0^2} \cdot N(x) \cdot N(y) = \frac{1}{m_0^2} \cdot m_0 \cdot p \cdot m_1 \cdot m_0 = m_1 \cdot p \end{aligned}$$

was ein Widerspruch zur minimalen Wahl von m_0 ergibt. □

3 Ternäre quadratische Formen und Summe von drei Quadraten

In diesem Kapitel interessieren wir uns für die natürlichen Zahlen, die als Summe von drei Quadraten ganzer Zahlen darstellbar sind. Um zu betrachten, welche natürliche Zahlen Summe von drei Quadraten sind, führen wir den Begriff von ternären quadratischen Formen ein. Dieser Begriff ist eine Erweiterung der binären quadratischen Formen.

Am Anfang des Kapitels werden die quadratischen Formen allgemein definiert, die im zweiten und dritten Abschnitt als binäre und ternäre quadratische Formen betrachtet werden. Im dritten Abschnitt kommen wir unmittelbar zum Beweis der Darstellung einer natürlichen Zahl als Summe von drei Quadraten.

3.1 Quadratische Formen

In diesem und nächsten Abschnitten verwenden wir zwei Schriftarten. Mit lateinischen Buchstaben bezeichnen wir Matrizen und mit kalligraphischen Buchstaben quadratische Formen.

Definition 3.1. a) Ein Polynom der Form

$$\sum_{u,v=1}^{n} a_{uv}x_u x_v = \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

mit symmetrischer Matrix $A = (a_{uv})$ und $A \in \mathbb{Z}^{n\times n}$ heißt *quadratische Form.*

b) Die Zahl

$$D = \det A$$

heißt die *Determinante der quadratischen Form.*

Diese quadratische Form kann man noch in der Form

$$x^T Ax \text{ mit } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ schreiben.}$$

Definition 3.2. Eine quadratische Form $\sum_{u,v=1}^{n} a_{uv} x_u x_v$ heißt *positiv definit*, wenn $x^T Ax \geq 0$ und $x^T Ax = 0$ nur dann, wenn $x = 0$ ist.

Wenn in die quadratische Form bestimmte ganze Zahlen x, y eingesetzt werden, dann enthält man eine ganze Zahl n, und man sagt, dass die Form diese Zahl darstellt. Es ist

$$U = \begin{pmatrix} u_{11} & \dots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{n1} & \dots & u_{nn} \end{pmatrix}$$

eine ganzzahlige Matrix mit $D = \pm 1$, dann ist auch U^{-1} eine solche und die Abbildung

$$y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = U \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{bzw.} \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = U^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \tag{3.1}$$

bildet $\mathbb{Z}^n$ bijektiv auf sich selbst ab. Ist x eine Basis, dann ist y eine neue Basis.
Eine solche Matrix bzw. lineare Abbildung heißt *unimodular* [vgl.[12], IV. 8].

Definition 3.3. Zwei quadratische Formen mit Matrizen H und H' heißen *äquivalent,* wenn eine unimodulare Matrix U existiert, so dass

$$H = U^T H' U$$

gilt, wobei U^T die transponierte Matrix von U ist.

Es seien zwei quadratischen Formen x^TAx und $y^TA'y$, die äquivalent durch eine unimodulare Matrix U aus Gleichung (3.1) sind. Dann ist

$$\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ äquivalent zu}$$

$$\begin{aligned} &\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} \begin{pmatrix} u_{11} & \dots & u_{n1} \\ \vdots & \ddots & \vdots \\ u_{1n} & \dots & u_{nn} \end{pmatrix} \begin{pmatrix} a'_{11} & \dots & a'_{1n} \\ \vdots & \ddots & \vdots \\ a'_{1n} & \dots & a'_{nn} \end{pmatrix} \begin{pmatrix} u_{11} & \dots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{n1} & \dots & u_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\ &= \begin{pmatrix} x_1 \cdot u_{11} + \ldots + x_n \cdot u_{1n} \\ \vdots \\ x_1 \cdot u_{n1} + \ldots + x_n \cdot u_{nn} \end{pmatrix}^T \begin{pmatrix} a'_{11} & \dots & a'_{1n} \\ \vdots & \ddots & \vdots \\ a'_{1n} & \dots & a'_{nn} \end{pmatrix} \begin{pmatrix} x_1 \cdot u_{11} + \ldots + x_n \cdot u_{1n} \\ \vdots \\ x_1 \cdot u_{n1} + \ldots + x_n \cdot u_{nn} \end{pmatrix} \\ &= \begin{pmatrix} y_1 & \dots & y_n \end{pmatrix} \begin{pmatrix} a'_{11} & \dots & a'_{1n} \\ \vdots & \ddots & \vdots \\ a'_{1n} & \dots & a'_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \end{aligned}$$

Satz 3.4. *Äquivalente Formen stellen dieselben Zahlen dar und haben dieselbe Determinante.*

Beweis. Es sei U eine unimodulare Matrix und x, y aus Gleichung (3.1). Seien H und $H^{'}$ zueinander äquivalente Matrizen. Dann gilt

$$\begin{aligned} x^THx &= x^T(U^TH^{'}U)x \\ &= (x^TU^T)H^{'}(Ux) \\ &= (Ux)^TH^{'}(Ux) \\ &= y^TH^{'}y \end{aligned}$$

Es gilt nach dem Determinantenmultiplikationssatz

$$\begin{aligned} \det H^{'} &= \det(U^THU) \\ &= \det U^T \cdot \det H \cdot \det U \\ &= \det H \cdot \det U^2 \\ &= \det H. \end{aligned}$$

□

Bemerkung 3.5. *a) Jede quadratische Form ist zu sich selbst äquivalent.*

b) Zwei quadratische Formen, die zu einer dritten äquivalent sind, sind untereinander äquivalent.
c) Alle quadratische Formen mit Determinante D zerfallen in Klassen äquivalenter Formen. (Da es sich um eine Äquivalenzrelation handelt.)

3.2 Binäre quadratische Formen

Wir fangen mit der Definition einer binären quadratischen Form, die aus der allgemeinen Definition folgt. Danach betrachten wir, wann eine binäre quadratische Form positiv definit ist und zeigen die Äquivalenz zwischen zwei binären quadratischen Formen. Am Ende des Abschnittes betrachten wir eine reduzierte quadratische Form.

Ein Polynom aus Definition (3.1) mit $n = 2$ ist

$$a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{13}x_2^2 = (x_1 \;\; x_2)\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

und heißt *binär*. Die Determinante von der binären quadratischen Form ist

$$D = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}^2.$$

Die binäre quadratische Form x^TAx kann noch in der Form $\mathcal{A}(x_1, x_2)$ aufgefasst werden. Wir setzen

$$a = a_{11}, \;\; b = a_{12} \text{ und } c = a_{22}.$$

Im Folgenden werden wir uns an diese Bezeichnung halten. Sei eine binäre quadratische Form $\mathcal{A}(x_1, x_2)$ mit

$$a(ax_1^2 + 2bx_1x_2 + cx_2^2) = (ax_1 + bx_2)^2 + Dx_2^2. \tag{3.2}$$

Bemerkung 3.6. *Eine binäre quadratische Form $\mathcal{A}(x_1, x_2)$ mit Determinante D ist genau dann positiv definit, wenn $a > 0$ und $D > 0$ gilt.*

Beweis. Die rechte Seite der Gleichung (3.2) ist bei $D > 0$ immer ≥ 0 ist, d.h. dass eine quadratische Form bei $D > 0$ ausschließlich Zahlen ≥ 0 darstellen, wenn $a > 0$ ist. Die quadratische Form stellt die Zahl 0 nur für $x_1 = x_2 = 0$ dar. □

Satz 3.7. *Jede definite Form $ax_1^2 + 2bx_1x_2 + cx_2^2$ mit positiver Determinante D ist äquivalent zu einer Form $a'y_1^2 + 2b'y_1y_2 + c'y_2^2$ mit*

$$2|b'| \leq a' \leq c'.$$

Beweis. Es sei $ax_1^2 + 2bx_1x_2 + cx_2^2$ eine binäre quadratische Form. Und es sei $\tilde{a}$ die kleinste darstellbare positive Zahl durch diese Form. Dann existieren ganze Zahlen α, γ, so dass

$$\tilde{a} = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \quad \text{mit} \quad \text{ggT}(\alpha, \gamma) = 1$$

gilt. Wenn $\text{ggT}(\alpha, \gamma) > 1$ wäre, so wäre $\tilde{a}$ nicht die kleinste Zahl. Es sind Zahlen β, δ bestimmbar, so dass

$$\alpha\delta - \beta\gamma = 1$$

gilt, d.h. dass eine Matrix $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit Determinante 1 existiert.

Durch die durch U definierte Substitution geht die Form $ax_1^2 + 2bx_1x_2 + cx_2^2$ in die äquivalente Form $a''z_1^2 + 2b''z_1z_2 + c''z_2^2$ über. Der erste Koeffizient der neuen Form ist

$$\begin{aligned}
\begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \cdot \begin{pmatrix} a'' & b'' \\ b'' & c'' \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^T \cdot \begin{pmatrix} a & b \\ b & c \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} \alpha \\ \gamma \end{pmatrix}^T \cdot \begin{pmatrix} a & b \\ b & c \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} \\
&= \tilde{a}.
\end{aligned}$$

Wir wollen eine weitere Substitution mit einer Matrix der Form $G = \begin{pmatrix} 1 & \beta'' \\ 0 & 1 \end{pmatrix}$ durchführen, der Koeffizient β'' wird später genauer bestimmt. Dabei geht die Form $a''z_1^2 + 2b''z_1z_2 + c''z_2^2$ in die Form $a'y_1^2 + 2b'y_1y_2 + c'y_2^2$ über.

Die Einträge in der ersten Spalte vom Produkt $\begin{pmatrix} 1 & 0 \\ \beta'' & 1 \end{pmatrix} \begin{pmatrix} a'' & b'' \\ b'' & c'' \end{pmatrix} \begin{pmatrix} 1 & \beta'' \\ 0 & 1 \end{pmatrix}$ sind

$$\begin{aligned}
a' &= \tilde{a} \\
b' &= \tilde{a}\beta'' + b''.
\end{aligned}$$

Wegen $|b'| = |\tilde{a}\beta'' + b''|$ kann β'' so gewählt werden, dass

$$\begin{aligned} |b'| &\leq \frac{\tilde{a}}{2} \\ &= \frac{a'}{2} \end{aligned}$$

gilt. Da c' durch $a'y_1^2 + 2b'y_1y_2 + c'y_2^2$ auch darstellbar ist, d.h. $a' \leq c'$ gilt und daher ist

$$2|b'| \leq a' \leq c'.$$

□

Definition 3.8. Eine definite Form $ax_1^2 + 2bx_1x_2 + cx_2^2$ mit positiver Determinante heißt *reduziert,* wenn

$$2|b| \leq a \leq c$$

ist.

Nach der Definition 3.8 und Satz 3.7 gilt, dass zu jeder binären quadratischen Form eine äquivalente reduzierte Form existiert.

Satz 3.9. *Sei $ax_1^2 + 2bx_1x_2 + cx_2^2$ eine reduzierte Form mit Determinante D. Dann gilt*

$$a \leq \frac{2}{\sqrt{3}}\sqrt{D}.$$

Beweis. Die Determinante dieser Form ist

$$ac - b^2 = D > 0.$$

Nach Voraussetzung ist $a \leq c$, daher gilt

$$\begin{aligned} a^2 &\leq ac \\ &= b^2 + D \\ &\leq \frac{a^2}{4} + D, \quad \text{daher ist} \\ \frac{3}{4}a^2 &\leq D \qquad\quad \text{und somit} \\ a &\leq \frac{2}{\sqrt{3}}\sqrt{D}. \end{aligned}$$

□

Korollar 3.10. *Sei $ax_1^2+2bx_1x_2+cx_2^2$ eine reduzierte Form mit Determinante 1. Dann gilt*

$$a = c = 1 \quad \textit{und} \quad b = 0.$$

Beweis. Es sei $ax_1^2+2bx_1x_2+cx_2^2$ eine reduzierte Form. Wegen $D = 1$ und des vorherigen Satzes gilt

$$a \leq \frac{2}{\sqrt{3}}.$$

Da a aus $\mathbb{Z}$ ist, ist dann $a = 1$. Weiter gilt, dass $b \leq \frac{1}{2}$ ist, daher ist $b = 0$. Dann ist

$$c = \frac{D + b^2}{a} = 1.$$

□

3.3 Ternäre quadratische Formen

Wir definieren eine ternäre quadratische Form und ihre Determinante. Danach werden ihre wichtigsten Eigenschaften betrachtet und am Ende des Abschnittes beweisen wir einen Hilfssatz, der sagt, dass eine positiv definite ternäre quadratische Form mit Determinante 1 zu einer Summe von drei Quadraten äquivalent ist. Dieser Satz ist ein Hilfsmittel für den nächsten Abschnitt.

Mit $n = 3$ ist allgemeine quadratische Form eine *ternäre quadratische Form*

$$\sum_{u,v=1}^{3} a_{uv}x_ux_v = \mathcal{H}(x_1, x_2, x_3) = x^THx = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 + 2a_{13}x_1x_3 + 2a_{23}x_2x_3 + a_{33}x_3^2$$

mit

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \text{ und } \quad H = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

wobei x_1, x_2, x_3 aus $\mathbb{Z}$ sind und H eine symmetrische Matrix mit ganzzahligen Koeffizienten ist. Sei $\mathcal{H}(x_1, x_2, x_3)$ eine ternäre quadratische Form mit Matrix $H = (a_{ij})$ aus

$\mathbb{Z}^{3\times 3}$. Dann ist die Zahl

$$D = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{array}{l} a_{11}a_{22}a_{33} + a_{12}a_{32}a_{13} + a_{21}a_{23}a_{31} \\ \\ -a_{31}a_{22}a_{13} - a_{23}a_{32}a_{11} - a_{12}a_{21}a_{33} \end{array}$$

die *Determinante der ternären quadratischen Form.*

Von allen ternären quadratischen Formen sind die positiv definiten für uns von besonderem Interesse, weil sie nur die Zahlen ≥ 0 darstellen. Jetzt zeigen wir, welche Bedingungen von einer ternären quadratischen Form erfüllt sind, wenn sie positiv definit ist.

Lemma 3.11. *Sei $\mathcal{H}(x_1, x_2, x_3) = \sum_{u,v=1}^{3} a_{uv}x_u x_v$ eine ternäre quadratische Form. Dann ist $\mathcal{H}(x_1, x_2, x_3)$ positiv definit genau dann, wenn*

$$a_{11} > 0, \quad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0 \quad \textit{und} \quad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} > 0 \ \textit{gilt.}$$

Beweis. Es ist

$$\begin{aligned} a_{11}\mathcal{H}(x_1, x_2, x_3) &= a_{11}^2x_1^2 + a_{11}a_{22}x_2^2 + a_{11}a_{33}x_3^2 + 2a_{11}a_{12}x_1x_2 + 2a_{11}a_{13}x_1x_3 + 2a_{11}a_{23}x_2x_3 \\ &= a_{11}^2x_1^2 + a_{11}a_{22}x_2^2 + a_{11}a_{33}x_3^2 + 2a_{11}a_{12}x_1x_2 + 2a_{11}a_{13}x_1x_3 + 2a_{11}a_{23}x_2x_3 \\ &\quad + a_{12}^2x_2^2 - a_{12}^2x_2^2 + 2a_{12}a_{13}x_2x_3 - 2a_{12}a_{13}x_2x_3 + a_{13}^2x_3^2 - a_{13}^2x_3^2 \\ &= \underbrace{a_{11}^2x_1^2 + a_{12}^2x_2^2 + a_{13}^2x_3^2 + 2(a_{11}a_{12}x_1x_2 + a_{11}a_{13}x_1x_3 + a_{12}a_{13}x_2x_3)} \\ &\quad + a_{11}a_{22}x_2^2 - a_{12}^2x_2^2 + 2a_{11}a_{23}x_2x_3 - 2a_{12}a_{13}x_2x_3 + a_{11}a_{33}x_3^2 - a_{13}^2x_3^2 \\ &= (\underbrace{a_{11}x_1 + a_{12}x_2 + a_{13}x_3})^2 + (a_{11}a_{22} - a_{12}^2)x_2^2 + 2(a_{11}a_{23} - a_{12}a_{13})x_2x_3 \\ &\quad + (a_{11}a_{33} - a_{13}^2)x_3^2 \qquad (3.3) \\ &= (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + \mathcal{H}'(x_2, x_3), \end{aligned}$$

wobei $\mathcal{H}'(x_2, x_3)$ die binäre quadratische Form

$$(a_{11}a_{22} - a_{12}^2)x_2^2 + 2(a_{11}a_{23} - a_{12}a_{13})x_2x_3 + (a_{11}a_{33} - a_{13}^2)x_3^2$$

ist. Die Determinante von $\mathcal{H}'(x_2, x_3)$ ist

$$\begin{vmatrix} a_{11}a_{22} - a_{12}^2 & a_{11}a_{23} - a_{12}a_{13} \\ a_{11}a_{23} - a_{12} & a_{11}a_{33} - a_{13}^2 \end{vmatrix} = (a_{11}a_{22} - a_{12}^2)(a_{11}a_{33} - a_{13}^2) - (a_{11}a_{22} - a_{12}^2)^2$$
$$= a_{11} \det H > 0,$$

wobei H die Matrix von $\mathcal{H}(x_1, x_2, x_3)$ ist.
Sei zuerst $\mathcal{H}(x_1, x_2, x_3)$ positiv definit. Die Zahl a_{11} eine darstellbare Zahl. Also ist $a_{11} \geq 0$. Ist $a_{11} = 0$, dann ist die Zahl 0 für $x_1 = 1$ und $x_2 = x_3 = 0$ darstellbar, was nicht erlaubt ist. Deswegen muss $a_{11} > 0$ sein. Wir nehmen an, dass $\mathcal{H}'(x_2, x_3) = 0$ mit $(x_2, x_3) \neq (0, 0)$. Es kann ein solches x_1 ausgewählt werden, dass $a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = 0$ ist. Somit ist $\mathcal{H}(x_1, x_2, x_3)$ gleich Null. Aber das ist ein Widerspruch zur Annahme. Ist die Form $\mathcal{H}'(x_2, x_3) < 0$, dann entspricht sie dem negativen Wert von $\mathcal{H}(x_1, x_2, x_3)$, was nicht möglich ist. Daraus folgt, dass $\mathcal{H}(x_1, x_2, x_3)$ nur dann größer gleich Null ist, wenn $\mathcal{H}'(x_2, x_3)$ positiv definit ist. Gemäß Bemerkung 3.6 ist

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0.$$

Daraus folgt, dass die Determinante von H positiv ist.
Umgekehrt, seien

$$a_{11} > 0, \quad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0 \quad \text{und} \quad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} > 0,$$

Also ist $\mathcal{H}'$ positiv definit. Sei $\mathcal{H}'(x_2, x_3) = 0$, dann ist $x_2 = x_3 = 0$. Und die Gleichung (3.3) ist $a_{11}\mathcal{H}(x_1, x_2, x_3) = a_{11}x_1$. Wegen $a_{11} > 0$ kann $\mathcal{H}(x_1, x_2, x_3)$ nur dann gleich Null sein, wenn $x_1 = x_2 = x_3 = 0$ gilt. □

Satz 3.12. *Jede positiv definite ternäre quadratische Form mit Determinante D ist äquivalent zu einer Form in einer geeigneten Basis, für deren Matrix $A = (a_{uv})$ gilt*

$$2|a_{12}| \leq a_{11}, \quad 2|a_{13}| \leq a_{11}, \quad a_{11} \leq \frac{4}{3}\sqrt[3]{D}.$$

Beweis. Sei a'_{11} die kleinste darstellbare natürliche Zahl von einer Form $\mathcal{H}(x_1, x_2, x_3)$ aus der Klasse aller äquivalenten Formen. Man kann zunächst die gegebene Form durch eine äquivalente Form ersetzen, in welcher der erste Koeffizient dieses kleinste a'_{11} ist. Es ist nämlich

$$a'_{11} = \mathcal{H}(c_{11}, c_{21}, c_{31}) \quad \text{mit} \quad \text{ggT}(c_{11}, c_{21}, c_{31}) = 1,$$

denn wenn $\mathrm{ggT}(c_{11}, c_{21}, c_{31}) > 1$ wäre, wäre a'_{11} nicht die kleinste darstellbare Zahl. Nun sei $\mathrm{ggT}(c_{11}, c_{21}) = d$. Es gilt daher $c_{12}, c_{22}, \alpha, \beta$ aus $\mathbb{Z}$, so dass

$$c_{11}c_{22} - c_{12}c_{21} = d \quad \text{und} \quad d\alpha - c_{31}\beta = 1 \text{ gilt.}$$

Dann ist die Determinante

$$\begin{aligned}
\det C = \begin{vmatrix} c_{11} & c_{12} & \frac{c_{11}}{d}\beta \\ c_{21} & c_{22} & \frac{c_{21}}{d}\beta \\ c_{31} & 0 & \alpha \end{vmatrix} &= c_{31} \cdot (\frac{c_{12}c_{21}}{d}\beta - \frac{c_{11}c_{22}}{d}\beta) + \alpha \cdot (c_{11}c_{22} - c_{12}c_{21}) \\
&= \alpha \cdot d - c_{31} \cdot \beta \\
&= 1.
\end{aligned}$$

Daraus folgt, dass die gegebene Form $\mathcal{H}(x_1, x_2, x_3)$ zur Form $\mathcal{B}(x_1, x_2, x_3)$ mit der Matrix $x^T(C^THC)x$ äquivalent ist. Sei $B = (b_{ij})$ diese Matrix von $\mathcal{B}$. Dann gilt, dass der Koeffizient

$$\begin{aligned}
b_{11} &= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}^T \cdot B \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}^T \cdot \begin{pmatrix} C^T\ H\ C \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} c_{11} \\ c_{21} \\ c_{31} \end{pmatrix}^T \cdot H \cdot \begin{pmatrix} c_{11} \\ c_{21} \\ c_{31} \end{pmatrix} \\
&= a'_{11}
\end{aligned}$$

ist. Wir konstruieren eine ganzzahlige Matrix

$$G = \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix}$$

mit der Eigenschaft $tw - uv = 1$ und $\det G = 1$. Die Koeffizienten werden später genauer bestimmt. Wir setzen

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = G \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

und enthalten eine neue äquivalente Form

$$\mathcal{A}(y_1, y_2, y_3) = y^T(G^T BG)y$$

mit der Matrix $A = G^T BG = (a_{nm})$. Die Elemente in der ersten Spalte von A, also das Produkt $(b_{11}\, b_{12}\, b_{13}) \cdot G$, sind

$$\begin{aligned} a_{11} &= a'_{11}, \\ a_{12} &= ra'_{11} + tb_{12} + vb_{13} \\ a_{13} &= sa'_{11} + ub_{12} + wb_{13}. \end{aligned}$$

Andererseits gilt

$$\begin{aligned} b_{11}x_1 + b_{12}x_2 + b_{13}x_3 &= \begin{pmatrix} b_{11} & b_{12} & b_{13} \end{pmatrix} \cdot G \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \qquad (3.4) \\ &= \begin{pmatrix} b_{11} & b_{12} & b_{13} \end{pmatrix} \cdot \begin{pmatrix} y_1 + ry_2 + sy_3 \\ ty_2 + uy_3 \\ vy_2 + wy_3 \end{pmatrix} \\ &= b_{11}(y_1 + ry_2 + sy_3) + b_{12}(ty_2 + uy_3) + b_{13}(vy_2 + wy_3) \\ &= b_{11}y_1 + (rb_{11} + tb_{12} + vb_{13})y_2 + (sb_{11} + ub_{12} + wb_{13})y_3 \\ &\overset{b_{11}=a_{11}}{=} a_{11}y_1 + a_{12}y_2 + a_{13}y_3. \end{aligned}$$

Nach Multiplikation wie in Gleichung (3.3) gilt weiter

$$\begin{aligned} b_{11}\mathcal{B}(x_1, x_2, x_3) &= (b_{11}x_1 + b_{12}x_2 + b_{13}x_3)^2 + \mathcal{B}'(x_2, x_3), \\ a_{11}\mathcal{A}(y_1, y_2, y_3) &= (a_{11}y_1 + a_{12}y_2 + a_{13}y_3)^2 + \mathcal{A}'(y_2, y_3). \end{aligned}$$

Wegen der Gleichung (3.4) sind beide Quadrate gleich. Durch die unimodulare Substitution $\begin{pmatrix} t & u \\ v & w \end{pmatrix}$ geht $\mathcal{B}'(x_2, x_3)$ in $\mathcal{A}'(y_2, y_3)$ über. Die beiden Formen sind positiv definit. Es ist

$$\mathcal{A}'(y_2, y_3) = (a_{11}a_{22} - a_{12}^2)y_2^2 + 2(a_{11}a_{23} - a_{12}a_{13})y_2y_3 + (a_{11}a_{33} - a_{13}^2)y_3^2$$

mit Determinante $a_{11} \det A$.
Man kann so die Transformation wählen, dass $\mathcal{A}'(y_2, y_3)$ in eine reduzierte quadratische Form übergeht [vgl. Satz 3.7 und Definition 3.8]. Wir nehmen also an, dass $\mathcal{A}'(y_2, y_3)$

reduziert ist. Gemäß Satz 3.9 gilt

$$\begin{aligned} 2|a_{11}a_{23} - a_{12}a_{13}| &\leq a_{11}a_{22} - a_{12}^2 \leq a_{11} - a_{33}a_{13}^2 \\ a_{11}a_{22} - a_{12}^2 &\leq \frac{2}{\sqrt{3}}\sqrt{a_{11} \cdot \det A}. \end{aligned}$$

Wir wählen r so, dass

$$|a_{12}| \leq \frac{1}{2}a_{11}$$

und s so, dass

$$|a_{13}| \leq \frac{1}{2}a_{11}$$

gilt. Da a_{11} die kleinste darstellbare Zahl und a_{22} auch darstellbar ist, ist dann $a_{11} \leq a_{22}$. Weiter gilt

$$\begin{aligned} a_{11}^2 &\leq a_{11}a_{22} \\ &= a_{11}a_{22} + a_{12}^2 - a_{12}^2 \\ &\leq \frac{2}{\sqrt{3}}\sqrt{a_{11} \cdot \det A} + \frac{1}{4}a_{11}^2 \\ \frac{3}{4}a_{11}^2 &\leq \frac{2}{\sqrt{3}} \cdot \sqrt{a_{11} \cdot \det A} \\ (a_{11})^{\frac{3}{2}} &\leq \frac{8}{3\sqrt{3}} \cdot \sqrt{\det A} \\ a_{11} &\leq \sqrt[3]{\frac{64}{27}} \cdot \sqrt[3]{\det A} \\ a_{11} &\leq \frac{4}{3}\sqrt[3]{\det A}. \end{aligned}$$

□

Wir sind zum Hilfssatz des Kapitels gekommen.

Korollar 3.13. *Jede positiv definite ternäre quadratische Form $\mathcal{H}(x_1, x_2, x_3)$ mit Determinante 1 ist äquivalent zu $x_1^2 + x_2^2 + x_2^2$.*

Beweis. Sei $\mathcal{H}(x_1, x_2, x_3)$ eine ternäre quadratische Form mit der Determinante 1. Gemäß Satz 3.12 gibt es zu $\mathcal{H}(x_1, x_2, x_3)$ eine äquivalente Form mit Matrix $A = (a_{ij})$ und mit

$$0 < a_{11} \leq \tfrac{4}{3}\sqrt[3]{\det A}.$$

Da $\mathcal{A}$ und $\mathcal{H}$ äquivalent sind, haben sie dieselbe Determinante. Es gilt $a_{11} \leq \frac{4}{3}$, also $a_{11} = 1$. Für die ganzen Zahlen

$$|a_{12}| \leq \frac{1}{2} \quad \text{und} \quad |a_{13}| \leq \frac{1}{2}$$

gilt weiter, dass $a_{12} = a_{13} = 0$ und wegen der Symmetrie auch $a_{21} = a_{31} = 0$ sind. Also ist

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix}.$$

Es ist

$$\begin{aligned} a_{11}\mathcal{A} - (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 &= (a_{11}a_{22} - a_{12}^2)x_2^2 + 2(a_{11}a_{23} - a_{12}a_{13})x_2x_3 \\ &\quad +(a_{11}a_{33} - a_{13}^2)x_3^2 \\ &= a_{22}x_2^2 + 2a_{23}x_2x_3 + a_{33}x_3^2 \end{aligned}$$

eine reduzierte quadratische Form mit der Determinante 1 [vgl. Beweis von Satz 3.13]. Gemäß Korollar 3.10 für eine reduzierte quadratische Form mit Determinante 1 gilt

$$a_{22} = 1, \qquad a_{23} = 0 \qquad \text{und} \qquad a_{33} = 1.$$

□

3.4 Natürliche Zahlen als Summe von drei Quadraten

Satz 3.14. *Eine natürliche Zahl n ist genau dann als Summe von drei Quadraten darstellbar, wenn sie nicht in der Form $n = 4^a(8m + 7)$ mit $a, m \in \mathbb{N}_0$ darstellbar ist.*

Beweis. Die Quadrate modulo 8 gleich $0, 1, 4$. Die Summe von drei Quadraten modulo

8 ist eine Zahl $0, 1, 2, 3, 4, 5$ oder 6, aber nie 7,

$$\begin{aligned}
0+0+0 &\equiv 0 \bmod 8\\
0+0+1 &\equiv 1 \bmod 8\\
0+1+1 &\equiv 2 \bmod 8\\
1+1+1 &\equiv 3 \bmod 8\\
0+0+4 &\equiv 4 \bmod 8\\
0+4+4 &\equiv 0 \bmod 8\\
4+4+4 &\equiv 4 \bmod 8\\
1+1+4 &\equiv 6 \bmod 8\\
1+4+4 &\equiv 1 \bmod 8\\
0+1+4 &\equiv 5 \bmod 8.
\end{aligned}$$

Daher ist $8m+7$ mit $m \in \mathbb{N}_0$ nicht die Summe von drei Quadraten. Wenn für ein $a \geq 1$

$$n = 4^a(8m+7) = x_1^2 + x_2^2 + x_3^2$$

wäre, d.h. durch 4 teilbar, dann wären die Zahlen x_1, x_2, x_3 gerade, wie es die obigen Kongruenzen zeigen. Mit $x_i = 2x_i^{'}$ für $i = 1, 2, 3$ und $x_i^{'}$ aus $\mathbb{N}$ würde gelten

$$\begin{aligned}
4^a(8m+7) &= (2x_1^{'})^2 + (2x_2^{'})^2 + (2x_3^{'})^2\\
4^{a-1}(8m+7) &= (x_1^{'})^2 + (x_2^{'})^2 + (x_3^{'})^2.
\end{aligned}$$

Induktiv führt es zu einer Lösung

$$8m+7 = (\tilde{x}_1^{'})^2 + (\tilde{x}_2^{'})^2 + (\tilde{x}_3^{'})^2,$$

die zum Widerspruch zum Fall $a = 0$ steht.
Jetzt möchten wir zeigen, dass eine Zahl $n \neq 4^a(8m+7)$ als Summe von drei Quadraten darstellbar ist.
Es darf ohne Beschränkung der Allgemeinheit angenommen werden, dass die Zahl n ungerade oder das Doppelte einer ungeraden Zahl ist, denn $4^a n$ mit $4 \not| n$ kann als Summe von drei Quadraten genau dann dargestellt werden, wenn das für n gilt. Also ist

$$n \equiv 1, 2, 3, 5, 6 \bmod 8.$$

Nach dem vorherigen Abschnitt genügt es nur zu beweisen, dass eine positiv definite ternäre quadratische Form $\sum_{u,v=1}^{3} a_{uv} y_u y_v$ mit der Determinante 1 existiert, welche die

Zahl n darstellt, denn dann ist n auch durch die äquivalente Form $x_1^2 + x_2^2 + x_3^2$ darstellbar ist. Es müssen also die folgenden Relationen erfüllt sein:

1) $n = a_{11}y_1^2 + 2a_{12}y_1y_2 + a_{22}y_2^2 + 2a_{13}y_1y_3 + 2a_{23}y_2y_3 + a_{33}y_3^2$

2) $a_{11} > 0$

3) $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0 \quad \text{mit} \quad a_{12} = a_{21}$

4) $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = 1.$

Wir werden sehen, dass es mit

$$a_{23} = a_{32} = 0, \;\; a_{13} = a_{31} = 1 \quad \text{und} \quad y_1 = y_2 = 0, \;\; y_3 = 1$$

geht. Dann ist $n = a_{33}$. Wir setzen

$$\begin{aligned} a &= a_{11}, \\ b &= a_{12} = a_{12}, \\ c &= a_{22}. \end{aligned}$$

Also ist

$$\begin{vmatrix} a & b & 1 \\ b & c & 0 \\ 1 & 0 & n \end{vmatrix} = n(ac - b^2) - c = 1,$$

d.h. die Bedingungen werden zu

$$a > 0, \quad ac - b^2 = d > 0 \quad \text{und} \quad c = dn - 1.$$

Sei $n = 1$, dann gelten alle Relationen mit z.B. $a = 3, b = c = 1$ und $d = 2$.

Sei $n > 1$, dann ist wegen $d > 0$

$$\begin{aligned} c &= dn - 1 \\ &> 0 \\ ac &> 0 \\ a &> 0. \end{aligned}$$

Also, es muss gelten

$$ac - b^2 = d > 0 \quad \text{und} \quad c = dn - 1.$$

Daraus folgt, dass $b^2 \equiv -d \bmod c$ ist, d.h. dass $-d$ ein quadratischer Rest modulo $dn - 1$ ist. Dann bleibt zu beweisen:
Für jedes $n > 1$ mit $n \equiv 1, 2, 3, 5, 6 \bmod 8$ gibt es ein $d > 0$, so dass $-d$ ein quadratischer Rest modulo $dn - 1$ ist. Wir betrachten zwei Fälle.
1. Fall: Es sei $n \equiv 2$ oder $6 \bmod 8$.
Es ist $\mathrm{ggT}(4n, n - 1) = 1$. Nach dem Satz von Dirichlet existiert eine Primzahl p mit

$$p = 4nv + n - 1 = (4v + 1)n - 1,$$

wobei v aus $\mathbb{N}$ ist [vgl.[8], Satz 1.3]. Wir setzen $d = 4v+1$, dann ist $d > 0$ und $p = dn-1$. Wie wir sehen, ist d ungerade. Daher ist für ein gegebenes n dieses $p \equiv 1 \bmod 4$, d.h. dass das Jacobi-Symbol $(\frac{-1}{p}) = 1$ ist.
Für jedes solches p ist das Jacobi-Symbol

$$\left(\frac{-d}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{p}{d}\right) = \left(\frac{dn-1}{d}\right) = \left(\frac{-1}{d}\right) = 1.$$

[vgl.[1], Satz 8.8(2)].
2. Fall: Es sei $n \equiv 1$ oder 3 oder $5 \bmod 8$.
Wie setzen

$$e = \begin{cases} 1, & \text{falls } n \equiv 3 \bmod 8, \\ 3, & \text{falls } n \equiv 1 \text{ oder } 5 \bmod 8 \end{cases}$$

Die Zahl $\frac{en-1}{2}$ ist ungerade, daher ist $\mathrm{ggT}(4n, \frac{en-1}{2}) = 1$. Nach dem Satz von Dirichlet existiert eine Primzahl p mit

$$p = 4nv + \frac{en-1}{2} = \frac{8nv + en - 1}{2} = \frac{1}{2}((8v + e)n - 1),$$

wobei $v \in \mathbb{N}$ ist. Wir setzen $d = 8v + e$, dann ist $2p = dn - 1$. Nun ist

$$\begin{aligned}
&\text{für } n \equiv 1 \bmod 8: \quad d \equiv 3 \bmod 8 \text{ und } p \equiv 1 \bmod 4;\\
&\text{für } n \equiv 3 \bmod 8: \quad d \equiv 1 \bmod 8 \text{ und } p \equiv 1 \bmod 4;\\
&\text{für } n \equiv 5 \bmod 8: \quad d \equiv 3 \bmod 8 \text{ und } p \equiv 3 \bmod 4.
\end{aligned}$$

In jedem dieser Fälle hat das JACOBI -Symbol $(\frac{-2}{d})$ den Wert 1 [vgl.[1], Satz 8.8]. Daher gilt

$$\Big(\frac{-d}{p}\Big) = \Big(\frac{-1}{p}\Big)\Big(\frac{d}{p}\Big) = \Big(\frac{-1}{p}\Big) \cdot (-1)^{\frac{d-1}{2}\cdot\frac{p-1}{2}}\Big(\frac{p}{d}\Big).$$

Für alle Fälle ist $\Big(\frac{-1}{p}\Big)(-1)^{\frac{d-1}{2}\cdot\frac{p-1}{2}} = 1$. Dann gilt weiter

$$\Big(\frac{-d}{p}\Big) = \Big(\frac{p}{d}\Big) \cdot 1 = \Big(\frac{p}{d}\Big)\Big(\frac{-2}{d}\Big) = \Big(\frac{-2p}{d}\Big) = \Big(\frac{1-dn}{d}\Big) = \Big(\frac{1}{d}\Big) = 1.$$

Also ist $-d$ quadratischer Rest modulo p und auch modulo $2p$. Die konkreten Lösungen können jetzt leicht ausgerechnet werden. □

4 Anzahl der Darstellungen als Summe von Quadraten

In den vorherigen drei Kapiteln haben wir die Darstellungen einer natürlichen Zahl als eine Summe von zwei, drei und vier Quadraten kennengelernt. In diesem Kapitel bestimmen wir die Anzahl der Darstellungen als Summe von zwei und vier Quadraten. Wegen des beschränkten Umfanges der Bachelorarbeit und des Schwierigkeitsgrades des Beweises für die Anzahl der Darstellungen der Summe von drei Quadraten wird die Anzahl der Darstellungen von drei Quadraten nicht betrachtet.

Es kann eine natürliche Zahl $n = x^2+y^2$ mit $\mathrm{ggT}(x, y) = 1$ oder $\mathrm{ggT}(x, y) \neq 1$ sein. Die Anzahl ihrer Darstellungen hängt stark von $\mathrm{ggT}(x, y)$ ab. Wir betrachten die Anzahl der Darstellungen von $n = x^2 + y^2$ mit $\mathrm{ggT}(x, y) = 1$ im ersten Abschnitt und mit $\mathrm{ggT}(x, y) \geq 1$ im dritten Abschnitt des Kapitels. Im vierten Abschnitt wird der Satz über die Anzahl der Darstellungen für n als Summe von vier Quadraten bewiesen.

In den meisten Beweisen der Anzahl der Darstellungen werden die Begriffe von zahlentheoretischen Funktionen, Charakter und Faltung, verwendet. Für das leichtere Verständnis der Beweise geben wir einen kurzen Überblick über diese Begriffe im zweiten Abschnitt.

4.1 Anzahl der Darstellungen einer natürlichen Zahl als Summe zweier Quadrate mit teilerfremden Summanden

Wir fangen mit einem Hilfssatz an.

Satz 4.1. *a) Es sei $n > 1$ und $4 \nmid n$. Für alle Primfaktoren p von n gelte $p \not\equiv 3 \bmod 4$ und es sei s die Anzahl der ungeraden verschiedenen Primteiler von n. Dann hat die Kongruenz $t^2 \equiv -1 \bmod n$ genau 2^s verschiedene Lösungen.*
b) Es sei $n > 1$ und $t^2 \equiv -1 \bmod n$. Dann ist n eindeutig in der Form $n = x^2 + y^2$ mit $(x, y) \in \mathbb{N}^2$, $\mathrm{ggT}(x, y) = 1$ und $y \equiv tx \bmod n$ darstellbar.

Beweis. a) Sei $n = 2$, dann gibt es nur eine Lösung der Kongruenz mit $t = 1$.
Für ein ungerades $n \in \mathbb{N}$ unterscheiden wir drei Fälle.

1. Fall für $n = p$, wobei $p \equiv 1 \bmod 4$ eine Primzahl:
Sei $f(t) = t^2 + 1$ das Polynom zweiten Grades. Dann kann die Polynomkongruenz $t^2 \equiv -1 \bmod p$ maximal 2 inkongruente Lösungen in $\mathbb{Z}/(p)$ haben [vgl. [9], Korollar 5.3.4]. Sei t_0 eine Lösung, dann ist $-t_0$ die zweite Lösung, so dass $t \neq -t_0$. Sonst würde gelten

$$\begin{aligned} t_0 &\equiv -t_0 \bmod p \\ 2t_0 &\equiv 0 \bmod p. \end{aligned}$$

Wäre in diesem Fall $t_0 \neq 0$, dann wäre $2t_0 \not\equiv 0 \bmod p$. Wäre $t_0 = 0$, dann wäre die Kongruenz $t^2 \equiv -1 \bmod p$ unmöglich.
Also hat die Kongruenz $t^2 \equiv -1 \bmod p$ entweder keine Lösung oder genau 2 Lösungen. Im Beweis von Satz 1.13 haben wir gezeigt, dass die Kongruenz $t^2 \equiv -1 \bmod p$ für $p \equiv 1 \bmod 4$ lösbar ist. Dann hat sie genau 2 Lösungen.

2. Fall für $n = p^v$ mit $p \equiv 1 \bmod 4$ und $v \in \mathbb{N}$:
Wie man leicht sehen kann, hat die Kongruenz $t^2 \equiv -1 \bmod p^v$ in Analogie zur Kongruenz $t^2 \equiv -1 \bmod p$ auch entweder keine Lösung oder genau 2 Lösungen.
Sei -1 aus $(\mathbb{Z}/(p^v))^*$. Die Restklassengruppe $(\mathbb{Z}/(p^v))^*$ ist zyklisch der Ordnung $p^{v-1}(p-1)$ und besitzt also ein Element g, das alle andere Elemente in $(\mathbb{Z}/(p^v))^*$ erzeugt [vgl.[9], 6.2.3]. Sei

$$(\mathbb{Z}/(p^v)^* \longrightarrow (\mathbb{Z}/(p))^* \tag{4.1}$$

der kanonische Homomorphismus, der surjektiv ist [vgl.[1], Lemma 5.9]. Im Beweis von Satz 1.13 haben wir die wichtigen Eigenschaften der Einheitsgruppe $(\mathbb{Z}/(p))^*$ genannt. Wir wenden sie hier an. Also sind die beiden Einheitsgruppen $(\mathbb{Z}/(p^v))^*, (\mathbb{Z}/(p))^*$ zyklisch, damit gilt, dass ein Erzeuger aus $(\mathbb{Z}/(p^v))^*$ durch dem Homomorphismus (4.1) auf einen Erzeuger aus $(\mathbb{Z}/(p))^*$ abgebildet wird. Wegen des Isomorphismus zwischen

$$(\mathbb{Z}/(p^{v-1}(p-1)) \cong (\mathbb{Z}/(p^v))^* \quad \text{und} \quad (\mathbb{Z}/(p-1)) \cong (\mathbb{Z}/(p))^*$$

gilt, dass

$$\begin{aligned} (\mathbb{Z}/(p^{v-1}(p-1)), +) &\longrightarrow (\mathbb{Z}/(p-1))^*, +), \\ j &\mapsto i \end{aligned}$$

auch ein surjektiver Gruppenhomomorphismus ist.
Die Existenz eines geraden $i \in \mathbb{Z}/(p-1)$, das dem quadratischen Rest $-1 \in (\mathbb{Z}/(p))^*$ zugeordnet ist [vgl. Beweis von Satz 1.13], folgt daraus, dass ein gerades $j \in \mathbb{Z}/(p^{v-1}(p-1))$ existiert.
Die Elemente p und $p-1$ sind teilerfremd, dann ist nach dem Chinesischen Restsatz

$$\mathbb{Z}/(p^{v-1}(p-1)) \cong \mathbb{Z}/(p^{v-1}) \times \mathbb{Z}/(p-1),$$

wobei $j = (j_1, j_2)$ ein Zahlenpaar mit $j_1 \in \mathbb{Z}/(p^{v-1})$ und $j_2 \in \mathbb{Z}/(p-1)$ ist.
Es sei $j_2 = i$ und jede i in $\mathbb{Z}/(p^{v-1})$ ist auch gerade. Da modulo der ungeraden Zahl p^{v-1} jede Zahl ein Vielfaches von 2 ist, ist auch j_1 gerade und so muss insgesamt j gerade sein [vgl.[1], Satz 6.5].
Also ist die Kongruenz $t^2 \equiv -1 \bmod p^v$ lösbar und hat genau 2 Lösungen.

3. Fall für ein $n = \prod_{i=1}^{s} {p_i}^{v_i}$ mit verschiedenen $p_i \equiv 1 \bmod 4$ und $s, v_i, i \in \mathbb{N}$:
Die Primfaktoren ${p_i}^{v_i}, {p_j}^{v_j}$ mit $i \neq j$ sind paarweise teilerfremd. Nach dem Chinesischen Restsatz besitzt ein Element

$$t = (t_1, \ldots, t_s) \quad \text{aus} \quad \mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{v_1}) \times \ldots \times \mathbb{Z}/(p_s^{v_s})$$

die Eigenschaft, dass $t^2 \equiv -1 \bmod n$ genau dann gilt, wenn

$$t_i^2 \equiv -1 \bmod p_i^{v_i}$$

für alle $i = 1, \ldots, s \in \mathbb{N}$ gilt [vgl.[1], Satz 4.13]. Aus der Kombinatorik folgt, dass die Anzahl solcher t gleich 2^s ist.
b) Sei $k = \lfloor \sqrt{n} \rfloor$. Nach dem Approximationssatz von Dirichlet [vgl.[12], Satz 1.10.27] gibt es für jedes $k \in \mathbb{N}$ natürliche Zahlen a, b mit $\mathrm{ggT}(a,b) = 1$, so dass

$$\Big| -\frac{t}{n} - \frac{a}{b} \Big| = \Big| \frac{tb + na}{nb} \Big| \leq \frac{1}{b(k+1)} \text{ mit } b \leq k \text{ gilt.}$$

Dann

$$\begin{aligned}\left|\frac{tb+na}{nb}\right| &\leq \frac{1}{b([\sqrt{n}]+1)}\\ |tb+na| &\leq \frac{|nb|}{b([\sqrt{n}]+1)}\\ &\leq \frac{|n|}{[\sqrt{n}]+1}\\ &< \sqrt{n} \quad \text{mit } b \leq \sqrt{n}.\end{aligned}$$

Wie setzen $c = tb + na$, dann gilt

$$c \equiv tb \bmod n \text{ und } |c| < \sqrt{n}.$$

Wegen $b \leq \sqrt{n}$ und $|c| < \sqrt{n}$ gilt, dass $b^2 + c^2 < 2n$ ist. Wegen $b^2 \leq n$ gilt weiter, dass $b^2 + c^2 \equiv b^2 + t^2b^2 \equiv b^2(1 + t^2) \equiv 0 \bmod n$ und daher $b^2 + c^2 = n$ ist.
Es ist

$$\begin{aligned}1 = \frac{b^2+c^2}{n} &= \frac{b^2+t^2b^2+2tbna+n^2a^2}{n}\\ &= \frac{b^2(1+t^2)}{n} + 2tba + na^2\\ &= \Big(\frac{b(1+t^2)}{n} + ta\Big)\cdot b + \underbrace{tba+na^2}_{=a\cdot c}.\end{aligned}$$

Aus dieser Gleichung folgt $\mathrm{ggT}(b, c) = 1$. Wegen $n > 1$ und $\mathrm{ggT}(b, c) = 1$ ist $c \neq 0$. Ist $c > 0$, so setzen wir $x = b$ und $y = c$, dann ist $y \equiv tx \bmod n$. Ist $c < 0$, so setzen wir $x = -c$ und $y = b$. Aus $b^2 + c^2 \equiv 0 \bmod n$ folgt

$$\begin{aligned}b^2 &\equiv -t^2b^2 \bmod n\\ y \equiv\ b &\equiv -t^2b \bmod n\\ &\equiv -tc \bmod n\\ &\equiv tx \bmod n.\end{aligned}$$

Jetzt beweisen wir die Eindeutigkeit der Lösung $(x, y) \in \mathbb{N}$. Seien (x_1, y_1) und (x_2, y_2) zwei Lösungen. Dann ist

$$\begin{aligned}n^2 = (x_1^2+y_1^2)(x_2^2+y_2^2) &= x_1^2x_2^2 + y_1^2y_2^2 + x_1^2y_2^2 + y_1^2x_2^2\\ &= (x_1x_2 + y_1y_2)^2 + (x_1y_2 - y_1x_2)^2.\end{aligned}$$

Für jede Lösung (x_i, y_i) gilt die Kongruenz $y_i \equiv tx_i \bmod n$ mit $i = 1, 2$. Dann

$$x_1x_2 + y_1y_2 \equiv x_1x_2 + t^2x_1x_2 \equiv x_1x_2(1 + t^2) \bmod n.$$

Nach der Bedingung $t^2 \equiv -1 \bmod n$ gilt $x_1x_2(1 + t^2) \equiv 0 \bmod n$. Deshalb ist $x_1x_2 + y_1y_2 = n \cdot m$ mit $m \in \mathbb{N}$. In der obigen Gleichung hat $x_1x_2 + y_1y_2$ die Potenz 2 und diese Gleichung ist nur dann gültig, wenn $m = 1$ und $(x_1y_2 - y_1x_2)^2 = 0$ ist. Weiter gilt

$$\begin{aligned} x_1 \cdot n &= x_1(\underbrace{x_1x_2 + y_1y_2}_{n}) - y_1(\underbrace{x_1y_2 - y_1x_2}_{=0}) \\ &= x_1^2x_2 + y_1y_2x_1 - y_1y_2x_1 + y_1^2x_2 \\ &= x_2(x_1^2 + y_1^2) \\ &= x_2 \cdot n \end{aligned}$$

Also ist $x_1 = x_2$ und $y_1 = y_2$. □

In diesem Abschnitt interessieren wir uns für die natürlichen Zahlen $n = x^2 + y^2$ mit $\mathrm{ggT}(x, y) = 1$. Mit den zwei folgenden Lemmata zeigen wir, welche natürlichen Zahlen genau diese Bedingung erfüllen.

Lemma 4.2. *Sei n eine natürliche Zahl, die durch 4 teilbar ist, und $n = x^2 + y^2$ mit $x, y \in \mathbb{N}$. Dann sind x, y gerade und insbesondere gilt* $\mathrm{ggT}(x, y) \neq 1$.

Beweis. Es sei $n = 4k$ mit $k \in \mathbb{N}$ und sei $n = x^2 + y^2$. Wäre $x = 2u + 1$ und $y = 2v + 1$ mit $u, v \in \mathbb{N}$, dann würde gelten

$$x^2 + y^2 = 4u^2 + 2u + 4v^2 + 2v + 2 \text{ und } 4 \not| x^2 + y^2.$$

Deswegen müssen x, y gerade sein. □

Lemma 4.3. *Sei n eine natürliche Zahl in der Form $n = a^2b = x^2 + y^2$, wobei $a, b \in \mathbb{N}$, a das Produkt von Primfaktoren $q \equiv 3$ mod 4 ist. Es sei b das Produkt von Primfaktoren $p \equiv 1, 2$ mod 4, die alle einfach vorkommen mögen.*
a) Für $a > 1$ gilt, dass $\mathrm{ggT}(x, y) \neq 1$.
b) Für $a = 1$ gilt, dass $\mathrm{ggT}(x, y) = 1$.

Beweis. a) Sei $n = a^2b = x^2 + y^2$ eine natürliche Zahl mit $x, y, a, b \in \mathbb{N}$. Sei weiter

$$n = (\underbrace{q_1^2 \cdot \ldots \cdot q_r^2}_{a^2}) \cdot \underbrace{2^v \cdot (p_1 \cdot \ldots \cdot p_s)}_{b}$$

mit $q_i \equiv 3 \bmod 4, p_j \equiv 1 \bmod 4$ und $v = 0, 1$ mit $v, r, s \in \mathbb{N}$.
Gemäß Satz 1.9 ist q_i eine Gaußsche Primzahl und 2 und p_j sind die Normen

$$p_j = N(p_j^{'}), \quad \text{und} \quad 2 = N(1+i),$$

wobei $p_j^{'}$ und $1+i$ Gaußsche Primzahlen für alle $j = 1, \ldots, s$ sind. Dann hat die Zahl n in $\mathbb{Z}[i]$ eine eindeutige Primfaktorzerlegung

$$n = (q_1 q_1 \cdot \ldots \cdot q_r q_r)(1+i)^v (1-i)^v (p_1^{'}\overline{p_1^{'}} \cdot \ldots \cdot p_s^{'}\overline{p_s^{'}}). \tag{4.2}$$

Für jedes $q_m \equiv 3 \bmod 4$ gilt auch

$$q_m^2 \equiv 1 \bmod 4 \ \text{ und } \ q_m^2 = N(q_m),$$

weil $q_m = \overline{q_m}$ in $\mathbb{Z}[i]$ für alle $m = 1, \ldots, r$ ist. Wir schreiben

$$n = x^2 + y^2 = (x+iy)(x-iy) \text{ mit } (x \pm iy) \in \mathbb{Z}[i]. \tag{4.3}$$

a) Sei $a > 1$, dann gibt es ein $q_m = q$. Nach der Primfaktorzerlegung (4.2) gilt

$$q|(x+iy) \quad \text{und} \quad q|(x-iy).$$

Wegen der Summation gilt

$$\begin{aligned} 2q &\mid (x+iy)+(x-iy) \\ 2q &\mid 2x \\ q &\mid x. \end{aligned}$$

Wie wir sehen q teilt die Zahlen x und y. Somit ist $\mathrm{ggT}(x, y) \neq 1$.
b) Sei $a = 1$, dann ist

$$n = x^2 + y^2 = 2^v \cdot p_1 \cdot \ldots \cdot p_s,$$

wobei $p_j \equiv 1 \bmod 4$ mit $j = 1, \ldots, s \in \mathbb{N}$ und $v = 0, 1$. Wenn $\mathrm{ggT}(x, y) = d > 1$ wäre, dann gelte $d^2|n$, was nicht sein kann, da alle Primfaktoren einfach vorkommen. □

Jetzt möchten wir die Anzahl der Darstellungen für eine natürliche Zahl $n = x^2 + y^2$

mit $\mathrm{ggT}(x,y) = 1$ berechnen. Mit $R_2(n)$ bezeichnen wir die Anzahl der Zahlenpaare $(x,y) \in \mathbb{Z}^2$ mit $n = x^2 + y^2$ und mit $\mathrm{ggT}(x,y) = 1$.

Satz 4.4. *Es sei n eine natürliche Zahl und $4 \nmid n$. Weiter sei n durch keine Primzahl $q \equiv 3 \bmod 4$ teilbar und sei s die Anzahl der ungeraden verschiedenen Primteiler von n, die alle einfach vorkommen mögen. Dann ist $R_2(n) = 2^{s+2}$.*

Beweis. Sei $n = 1 = (\pm 1)^2 + 0$. Dann ist $R_2(1) = 4$. Sei $n = 2 = (\pm 1)^2 + (\pm 1)^2$, dann ist $R_2(2) = 4$. Sei n eine natürliche Zahl großer 2, die keine Primfaktoren $q \equiv 3 \bmod 4$ hat. Dann ist gemäß Satz 1.15 dieses n eine Summe von zwei Quadraten. Es seien die ungeraden Primfaktoren verschieden. Es sei

$$n = 2^a \cdot p_1 \cdot \ldots \cdot p_s = ((\pm 1)^2 + (\pm 1)^2)^a (x^2 + y^2),$$

wobei $p_i \equiv 1 \bmod 4$ für alle $a, i = 1, \ldots, s \in \mathbb{N}$ und $x, y \in \mathbb{Z}$.
Die Zahl n ist nicht durch 4 teilbar, deswegen ist der Exponent a entweder 0 oder 1 und in beiden Fällen gilt

$$n = ((\pm 1)^2 + (\pm 1)^2)^a (x^2 + y^2) = x^2 + y^2.$$

Gemäß Lemma 4.3(b) gilt $\mathrm{ggT}(x,y) = 1$. Dann ist $R_2(n)$ das Vierfache der Anzahl der Lösungspaare $(x,y) \in \mathbb{N}^2$ mit $x^2 + y^2 = n$ und $\mathrm{ggT}(x,y) = 1$. Jedes solches Paar bestimmt eindeutig ein t modulo n mit $y \equiv tx \bmod n$. Es ist daher auch x und n teilerfremd.

$$\begin{aligned} x^2 + y^2 &\equiv x^2 + t^2 x^2 \bmod n \\ &\equiv x^2(1 + t^2) \equiv 0 \bmod n. \end{aligned}$$

Dann ist $t^2 \equiv -1 \bmod n$. Gemäß Satz 4.1(a) ist die Anzahl der Lösungen der Kongruenz $t^2 \equiv -1 \bmod n$ gleich 2^s. Wir bezeichnen diese Anzahl der Lösungen mit $\varrho(n)$.
Umgekehrt sei $t^2 \equiv -1 \bmod n$. Nach Satz 4.1.(b) existiert zu jedem t genau ein Paar $(x,y) \in \mathbb{N}^2$ mit $\mathrm{ggT}(x,y) = 1$ und $y \equiv tx \bmod n$ und $n = x^2 + y^2$. Also ist $R_2(n) = 4\varrho(n) = 4 \cdot 2^s = 2^{s+2}$. □

4.2 Zahlentheoretische Funktionen, Charaktere und Faltung als Hilfsmittel

In diesem Abschnitt geben wir einen kurzen Überblick über die zahlentheoretischen Funktionen, die Charaktere und die Faltung. Diese Begriffe und ihre Eigenschaften

sind in Verbindung mit anderen Begriffen der Zahlentheorie ein wichtiges Hilfsmittel für die Beweise des Kapitels.

Zahlentheoretische Funktionen

Eine Abbildung

$$f : \mathbb{N} \longrightarrow \mathbb{C}$$

heißt eine *zahlentheoretische Funktion* [vgl.[2], 1.§ 4.1].
Die Werte von vielen zahlentheoretischen Funktionen liegen in $\mathbb{Z}$ oder in $\mathbb{N}$. Als Beispiel zahlentheoretischer Funktionen können bekannte Funktionen genannt werden:

$\tau(n)$	Anzahl der Teiler von n,	$\tau(n) = \sum_{d\|n} 1$,
$\sigma(n)$	Summe der Teiler von n,	$\sigma(n) = \sum_{d\|n} d$,
$\varphi(n)$	Anzahl der primen Restklassen modulo n,	Euler-Funktion

wobei d die Teiler von n sind [vgl.[12], V.1]. In den zwei nächsten Abschnitten des Kapitels werden außer den oben genannten noch andere zahlentheoretischen Funktionen verwendet, z.B.

a) $\alpha(n)$ beschreibt, ob die Zahl n eine Quadratzahl ist. Es ist

$$\alpha(n) = \begin{cases} 1, \text{ wenn } n \text{ Quadratzahl ist,} \\ 0 \text{ sonst.} \end{cases}$$

b) $\iota(n) = 1$ für alle $n \in \mathbb{N}$.

c) $\lambda(n \bmod m)$ Restklassencharakter modulo m, der später definiert wird.

Jetzt definieren wir zwei Eigenschaften von zahlentheoretischen Funktionen, die uns besonders wichtig sind.

Eine zahlentheoretische Funktion f heißt *(schwach) additiv,* wenn

$$f(nm) = f(n) + f(m) \text{ für alle } n, m \in \mathbb{N} \text{ mit } \operatorname{ggT}(n, m) = 1 \tag{4.4}$$

gilt. Gilt (4.4) ohne Beschränkung, so heißt f *stark additiv.*

Eine zahlentheoretische Funktion f heißt *(schwach) multiplikativ,* wenn

$$f(nm) = f(n) \cdot f(m) \text{ für alle } n, m \in \mathbb{N} \text{ mit } \operatorname{ggT}(n, m) = 1 \tag{4.5}$$

gilt. Hat (4.5) keine Beschränkung, dann heißt f *stark multiplikativ* [vgl.[2], 1. § 4.2]

Charaktere

Es sei $(\mathbb{Z}/(m))^*$ die prime Restklassengruppe modulo m. Diese Gruppe ist eine endliche abelsche Gruppe der Ordnung $\varphi(m)$, wobei $\varphi(m)$ die Euler-Funktion ist. Ein Gruppenhomomorphismus

$$\chi : (\mathbb{Z}/(m))^* \longrightarrow \mathbb{C}^*,$$

wobei $\mathbb{C}^*$ die komplexe Einheitsgruppe ist, heißt *Charakter.*

Wie wir sehen, ist ein Charakter für eine prime Restklasse der Einheitsgruppe $(\mathbb{Z}/(m))^*$ erklärt. Die Menge der Charaktere bilden eine multiplikative abelsche Gruppe, die zur Gruppe $(\mathbb{Z}/(m))^*$ isomorph ist [vgl.[6], 3.3]. Diese Charaktere erweitern wir zu einem *Restklassencharakter modulo* m für alle $n \in \mathbb{Z}$ durch

$$\chi(n) = \begin{cases} \chi(n \bmod m) & \text{falls } \operatorname{ggT}(n, m) = 1 \\ 0 & \text{falls } \operatorname{ggT}(n, m) > 1. \end{cases}$$

Das Legendre-Symbol $(\frac{a}{p})$ mit $a \in \mathbb{Z}$ und Primzahl p ordnet sich dem Begriff des Restklassencharakters unter, wenn man $(\frac{a}{p}) = 0$ für $\operatorname{ggT}(a, p) > 1$ setzt und $(\frac{a}{p}) \in \{-1, 0, 1\} \subseteq \mathbb{C}^*$ auffasst.
Wegen der Ordnung der Gruppe $(\mathbb{Z}/(m))^*$ gilt, dass es $\varphi(m)$ Restklassencharaktere modulo m gibt. Es besteht die Relation für alle Restklassencharaktere modulo m

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(m) & \text{für } n \equiv 1 \bmod m \\ 0 & \text{für } n \not\equiv 1 \bmod m. \end{cases}$$

Faltung

Es seien f und g zwei zahlentheoretischen Funktionen. Außer den gewöhnlichen Verknüpfungen $\cdot$ und $+$ für die zahlentheoretischen Funktionen ist die Verknüpfung $*$ von größter Bedeutung. Sie wird folgendermaßen definiert

$$(f * g)(n) := \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big).$$

Dabei bedeutet die Bedingung $d|n$ stets, dass über alle positiven Teiler d von n zu summieren ist. Das Produkt $f * g$ heißt *Faltung* [vgl.[2], § 4.6.(1)].

Satz 4.5. *Seien $f(n)$ und $g(n)$ multiplikative zahlentheoretische Funktionen, dann ist die Faltung $f * g$ auch multiplikativ.*

Beweis. Seien $n = n_1 \cdot n_2 \in \mathbb{N}$ mit $\mathrm{ggT}(n_1, n_2) = 1$. Dann gilt

$$(f * g)(n_1 n_2) = \sum_{t|n_1 n_2} f(t) g\Big(\frac{n_1 n_2}{t}\Big),$$

wobei $t \in \mathbb{N}$ die Teiler von n sind. Wegen der Teilerfremdheit kann jedes $t = t_1 \cdot t_2$ so zerlegt werden, dass t_1 ein Teiler von n_1 und t_2 ein Teiler von n_2 mit $\mathrm{ggT}(t_1, t_2) = 1$ ist. Wegen der Multiplikativität der zahlentheoretischen Funktionen f und g gilt

$$\begin{aligned}
(f * g)(n_1 n_2) &= \sum_{t_1|n_1} \sum_{t_2|n_2} f(t_1) f(t_2) \cdot g\Big(\frac{n_1}{t_1}\Big) g\Big(\frac{n_2}{t_2}\Big) \\
&= \sum_{t_1|n_1} f(t_1) g\Big(\frac{n_1}{t_1}\Big) \cdot \sum_{t_2|n_2} f(t_2) g\Big(\frac{n_2}{t_2}\Big) \\
&= (f * g)(n_1) \cdot (f * g)(n_2)
\end{aligned}$$

□

Man beachte, dass bei stark multiplikativen zahlentheoretischen Funktionen die Faltung im Allgemeinen nicht stark multiplikativ ist [vgl.[6], 5.1].

4.3 Anzahl der Darstellungen einer natürlichen Zahl als Summe von zwei Quadraten mit nicht notwendig teilerfremden Summanden

In diesem Abschnitt sind die natürlichen Zahlen $n = x^2 + y^2$ mit $\text{ggT}(x, y) \geq 1$ zur Betrachtung zugelassen. Sie können beliebige Primfaktoren modulo 4 besitzen. Die Anzahl der Darstellungen von n mit Primfaktoren $p \equiv 3 \bmod 4$ mit geradem Exponent wird getrennt von anderen Fällen bewiesen.

Mit $r_2(n)$ bezeichnen wir die Anzahl der Zahlenpaare $(x, y) \in \mathbb{Z}^2$ mit $x^2 + y^2 = n$ und $\text{ggT}(x, y) \geq 1$.

Satz 4.6. *Es sei $n = 2^a m$, wobei alle Primfaktoren von m den Rest $1 \bmod 4$ haben. Dann ist $r_2(n) = 4\tau(m)$, wobei $\tau(m)$ die Anzahl der Teiler von m ist.*

Beweis. Es sei

$$n = 2^a m = 2^a p_1^{v_1} \cdot \ldots \cdot p_s^{v_s}$$

mit $p_i \equiv 1 \bmod 4$ für alle $i = 1, \ldots, s$ und v_i, a aus $\mathbb{N}_0$. Gemäß Satz 1.15 ist n Summe von zwei Quadraten $n = x^2 + y^2$. Es sei $\text{ggT}(x, y) = d$. Dann gilt

$$n = x^2 + y^2 = d^2(x'^2 + y'^2) \text{ mit } \text{ggT}(x', y') = 1.$$

Also ist d^2 ein Teiler von n. Dann ist die Anzahl der Darstellungen der Zahl n gleich

$$r_2(n) = \sum_{d^2|n} R_2\Big(\frac{n}{d^2}\Big)$$

und die einzelnen Summanden können gemäß Satz 4.4 ausgerechnet werden.
Außer d^2 gibt es noch die anderen Teiler von n, die keine Quadrate sind. Die Funktion $\varrho(n)$ aus dem Beweis vom Satz 4.4 ist eine zahlentheoretische Funktion, weil Definitions- und Wertebereich der Funktion natürliche Zahlen sind [vgl.[9], § 2.3.1].
Mit $R_2(n) = 4\varrho(n)$ und der zahlentheoretischen Funktion α [vgl. Abschnitt 4.2(a)], gilt

$$r_2(n) = \sum_{d^2|n} R_2\Big(\frac{n}{d^2}\Big) = \sum_{d^2|n} 4\varrho\Big(\frac{n}{d^2}\Big) = 4 \cdot \sum_{u|n} \alpha(u)\varrho\Big(\frac{n}{u}\Big) = 4(\alpha * \varrho)(n)$$

wobei $(\alpha * \varrho)$ eine Faltung und $u \in \mathbb{N}$ alle Teiler von n durch läuft. Die Funktionen α und ϱ sind (schwach) multiplikativ [vgl. 4.5]. Daher ist die Faltung $\alpha * \varrho$ auch (schwach)

multiplikativ.
Wegen der Eindeutigkeit der Primfaktorzerlegung von n genügt es, die Gleichung $(\alpha * \varrho)(n) = \tau(m)$ für $n = 2^a m$ mit den angegebenen Bedingungen nur für die Primzahlenpotenzen p^r mit $p = 2$ oder $p \equiv 1 \bmod 4$ mit $r \geq 0$ nachzuweisen.

Für eine Zahl 2^i mit $i > 1$ gibt es keine Lösung $t^2 \equiv -1 \bmod 2^i$ d.h. $\varrho(2^i) = 0$ für alle $i > 1$ und die Teilsumme der Faltung ist $\sum_{i=2}^{a} \alpha(2^i)\varrho(2^{a-i}) = 0$. Ist die Potenz $i = 0, 1$ in der Zahl 2^i, dann ist $\varrho(2^0) = \varrho(1) = 1$ und $\varrho(2^1) = 1$. Andererseits ist entweder $\alpha(2^a)$ oder $\alpha(2^{a-1})$ gleich 1. Also gilt insgesamt

$$(\alpha * \varrho)(2^a) = \sum_{i=0}^{a} \alpha(2^i)\varrho(2^{a-i}) = \alpha(2^a) + \alpha(2^{a-1}) = 1.$$

Für jede Primzahl $p \equiv 1 \bmod 4$ gilt

$$\begin{aligned}
(\alpha * \varrho)(p^{2r}) &= \alpha(1)\varrho(p^{2r}) + \alpha(p)\varrho(p^{2r-1}) + \ldots + \alpha(p^{2r})\varrho(1) \\
&= \varrho(p^{2r}) + \varrho(p^{2r-2}) + \ldots + \varrho(1) \\
&= 2r + 1, \\
(\alpha * \varrho)(p^{2r+1}) &= \alpha(1)\varrho(p^{2r+1}) + \alpha(p)\varrho(p^{2r}) + \ldots + \alpha(p^{2r+1})\varrho(1) \\
&= \varrho(p^{2r+1}) + \varrho(p^{2r-1}) + \ldots + \varrho(p^3) + \varrho(p) \\
&= (2r + 1) + 1.
\end{aligned}$$

Daher ergibt sich für jeden Primfaktor $p_i^{v_i}$

$$(\alpha * \varrho)(p_i^{v_i}) = v_i + 1 = \tau(p_i^{v_i})$$

wobei $\tau(p_i^{v_i})$ die Anzahl der Teiler von $(p_i^{v_i})$ ist. Aus der Multiplikativität der Faltung folgt

$$r_2(n) = 4 \cdot (\alpha * \varrho)(n) = 4 \cdot (\alpha * \varrho)(2^a m) = 4 \cdot 1 \cdot \tau(p_1^{v_1}) \cdot \ldots \cdot \tau(p_s^{v_s}) = 4\tau(m).$$

□

Wir kommen zum Fall, wann eine natürliche Zahl $n = x^2 + y^2$ mit $\mathrm{ggT}(x, y) \geq 1$ Primfaktoren $p \equiv 1 \bmod 4$ mit $r \geq 1$ und Primfaktoren $p \equiv 3 \bmod 4$ mit geradem Exponent besitzt.

Satz 4.7. *Sei n eine natürliche Zahl, die die Summe von zwei Quadraten ist, und es*

sei

$$\lambda(d) = \begin{cases} 0 & \text{für } d \equiv 0 \bmod 2 \\ 1 & \text{für } d \equiv 1 \bmod 4 \\ -1 & \text{für } d \equiv 3 \bmod 4. \end{cases}$$

der Restklassencharakter modulo 4. *Dann gilt*

$$r_2(n) = 4 \sum_{d|n} \lambda(d).$$

Beweis. Im Beweis zu Satz 4.6 haben wir gezeigt, dass die Faltung $(\alpha * \varrho)(n) = \frac{1}{4} r_2(n)$ multiplikativ ist. Mit der zahlentheoretischen Funktion $\iota(n) = 1$ aus dem vorherigen Abschnitt gilt

$$\sum_{d|n} \lambda(d) = \sum_{d|n} \lambda(d) \cdot \iota\Big(\frac{n}{d}\Big) = (\lambda * \iota)(n).$$

Wegen $(\alpha * \varrho)(n) = \frac{1}{4} r_2(n)$ genügt es zu zeigen, dass die Beziehung

$$(\lambda * \iota)(n) = (\alpha * \varrho)(n)$$

gilt. Die Funktionen λ und ι sind multiplikativ, damit ist auch das Produkt $\lambda * \iota$ multiplikativ. Wegen der Eindeutigkeit der Primfaktorzerlegung für jede Zahl $n \in \mathbb{N}$ und wegen der Multiplikativität der beiden Funktionen genügt es, den Beweis nur für die Primzahlpotenzen p^r mit $r \geq 1$ zu zeigen.
Sei $p = 2$:

$$\begin{aligned} (\lambda * \iota)(2^r) &= \lambda(1) \cdot \iota(2^r) + \lambda(2) \cdot \iota(2^{r-1}) + \ldots + \lambda(2^r) \cdot \iota(1) \\ &= 1 + 0 + 0 + \ldots + 0 \\ &= 1. \end{aligned}$$

Also ist $(\lambda * \iota)(2^r) = (\alpha * \varrho)(2^r)$ [vgl. Beweis von Satz 4.6].
Sei $p \equiv 1 \bmod 4$: Es ist $\lambda(p^r) = 1$ für alle $r \in \mathbb{N}$ und

$$\begin{aligned} (\lambda * \iota)(p^r) &= \lambda(1) \cdot \iota(p^r) + \lambda(p) \cdot \iota(2^{r-1}) + \lambda(p^2) \cdot \iota(2^{r-2}) + \ldots + \lambda(p^r) \cdot \iota(1) \\ &= 1 + 1 + 1 + \ldots + 1 = r + 1. \end{aligned}$$

Die Beziehung $(\lambda * \iota)(p^r) = (\alpha * \varrho)(p^r)$ gilt [vgl. Beweis von Satz 4.6].
Sei $p \equiv 3 \bmod 4$: Es ist $\lambda(p^r) = 1$ für alle geraden $r \in \mathbb{N}$ und $\lambda(p^r) = -1$ für alle

ungeraden $r \in \mathbb{N}$. Dann ist

$$\begin{aligned}(\lambda * \iota)(p^r) &= \lambda(1)\cdot\iota(p^r) + \lambda(p)\cdot\iota(2^{r-1}) + \lambda(p^2)\cdot\iota(2^{r-2}) + \ldots + \lambda(p^r)\cdot\iota(1)\\ &= 1\underbrace{-1+1-1\ldots+1}_{r \text{ mal}}.\end{aligned}$$

Zu geradem r ist $(\lambda * \iota)(p^r) = 1$ und bei ungeradem r ist $(\lambda * \iota)(p^r) = 0$.
Mit $p \equiv 3 \bmod 4$ ist die Funktion $\varrho(p^r) = 0$. Und folglich ist die Faltung $(\alpha * \varrho)(p^r) = 0$.
Gemäß des Beweises von Satz 4.6 ist $(\lambda * \iota)(p^r) = (\alpha * \varrho)(p^r)$ und

$$r_2(n) = 4\sum_{d|n}\lambda(d).$$

□

4.4 Anzahl der Darstellungen einer natürlichen Zahl als Summe von vier Quadraten

In diesem Abschnitt betrachten wir die Anzahl der Darstellungen für eine natürliche Zahl n, die eine Summe von vier Quadraten ist. Den Beweis der Anzahl der Darstellungen von n zerlegen wir in drei Sätze.

Ist u ungerade, dann bezeichnen wir mit $s(u)$ die Anzahl der Darstellungen
$4u = u_1^2 + u_2^2 + u_3^2 + u_4^2$ mit $u_i \in \mathbb{N}$ ungerade für alle $i = 1, \ldots, 4$. Mit $r_4(n)$ bezeichnen wir die Anzahl der Quadrupel $(u_1, u_2, u_3, u_4) \in \mathbb{Z}^4$ mit
$u_1^2 + u_2^2 + u_3^2 + u_4^2 = n$.

Satz 4.8. *Es sei u eine positive ungerade Zahl. Dann ist $s(u) = \sigma(u)$, wobei σ die Teilersummenfunktion ist.*

Beweis. Sei

$$4u = u_1^2 + u_2^2 + u_3^2 + u_4^2 \quad \text{mit ungeraden } u_i \text{ für } i = 1, \ldots, 4.$$

Je zwei dieser Quadrate ergeben zusammen eine gerade Zahl. Wir setzen

$2v = u_1^2 + u_2^2$ und $2w = u_3^2 + u_4^2$. Dabei sind v, w ungerade und $2(v + w) = 4u$.

Aus Satz 4.7 folgt, dass die Anzahl der Darstellungen für $2v$ und $2w$ mit Nebenbedingung u_i aus $\mathbb{N}$ sind

$$\frac{1}{4}r_2(2v) = (\lambda * \iota)(2v) \quad \text{und} \quad \frac{1}{4}r_2(2w) = (\lambda * \iota)(2w).$$

Es ergibt sich für die Zerlegung $4u = 2v + 2w$ genau

$$\frac{1}{16}r_2(2v) \cdot r_2(2w) = (\lambda * \iota)(2v) \cdot (\lambda * \iota)(2w) \text{ Quadrupel } (u_1, u_2, u_3, u_4) \in \mathbb{N}^4.$$

Dann ist

$$\begin{aligned}
s(u) &= \sum_{2v+2w=4u} (\lambda * \iota)(2v) \cdot (\lambda * \iota)(2w) \\
&= \sum_{2v+2w=4u} \underbrace{(\lambda * \iota)(2)}_{=1} \cdot (\lambda * \iota)(v) \cdot \underbrace{(\lambda * \iota)(2)}_{=1} (\lambda * \iota)(w). \\
&= \sum_{v+w=2u} (\lambda * \iota)(v) \cdot (\lambda * \iota)(w) \\
&= \sum_{v+w=2u} \big(\sum_{a|v} \lambda(a) \cdot \sum_{b|w} \lambda(b) \big) \\
&= \sum_{v+w=2u} \sum_{\substack{a|v \\ b|w}} \lambda(ab) \\
&= \sum_{ac+bd=2u} \lambda(ab)
\end{aligned}$$

Zuerst rechnen wir die Summe mit $a = b$ aus. Die Zahl a ist ungerade als Teiler von v, ebenso c, d, daher ist a^2 auch ungerade und $\lambda(a^2) = 1$. Also ist

$$\sum_{a(c+d)=2u} \lambda(ab) = \sum_{a(c+d)=2u} \lambda(a^2) = \sum_{a(c+d)=2u} 1.$$

Die Zahl a teilt $2u$, daher teilt a auch u. Es gilt

$$\sum_{a(c+d)=2u} 1 = \sum_{a|u} \sum_{\frac{2u}{a}=c+d} 1 = \sum_{a|u} \frac{u}{a} = \sigma(u),$$

wobei $\sigma(u)$ die Summe der Teiler von u ist.
Jetzt zeigen wir, dass die verbliebene Summen $\sum_{ac+bd=2u} \lambda(ab)$ mit einerseits $a > b$ oder andererseits $a < b$ gleich Null sind. Die Summe mit Nebenbedingung $a > b$ ist symmetrisch zur Summe mit $a < b$. Deswegen beschränken wir uns auf dem Fall $a > b$.

Wir ordnen die Lösungen der Gleichung $ac+bd = 2u$ paarweise an, so dass einer Lösung

(a,b,c,d) eindeutig eine Lösung $(a^{'},b^{'},c^{'},d^{'})$ mit $\lambda(ab)+\lambda(a^{'}b^{'})=0$ entspricht. Dafür bilden wir eine bijektive Abbildung Υ abhängig von $k\in\mathbb{N}$ durch

$$\Upsilon:\begin{pmatrix}a\\b\\c\\d\end{pmatrix}\longmapsto\begin{pmatrix}0&0&k+2&k+1\\0&0&k+1&k\\-k&k+1&0&0\\k+1&-(k+2)&0&0\end{pmatrix}\begin{pmatrix}a\\b\\c\\d\end{pmatrix}.$$

Diese Abbildungsmatrix nennen wir M. Das Quadrat von M ist die Einheitsmatrix, d.h. dass M bijektiv ist. Wir setzen

$$\begin{pmatrix}a^{'}\\b^{'}\\c^{'}\\d^{'}\end{pmatrix}=\begin{pmatrix}0&0&k+2&k+1\\0&0&k+1&k\\-k&k+1&0&0\\k+1&-(k+2)&0&0\end{pmatrix}\cdot\begin{pmatrix}a\\b\\c\\d\end{pmatrix}=\begin{pmatrix}(k+2)c+(k+1)d\\(k+1)c+kd\\-ka+(k+1)b\\(k+1)a-(k+2)b\end{pmatrix}.$$

Wegen $c+d>0$ gilt, dass $a^{'}>b^{'}$ ist. Für jedes beliebige k sind $a^{'},b^{'},c^{'},d^{'}$ ungerade. Die Zahlen $a^{'},b^{'}$sind positiv und sollen

$$\begin{aligned}c^{'}&=-ka+(k+1)b=b-k(a-b)>0\text{ und}\\d^{'}&=(k+1)a-(k+2)b=(k+1)(a-b)-b>0\text{ sein.}\end{aligned}$$

Also soll

$$\frac{b}{a-b}-1<k<\frac{b}{a-b}$$

sein. Wir wählen daher

$$k=\Big[\frac{b}{a-b}\Big].$$

Es gilt

$$\begin{aligned}a^{'}c^{'}+b^{'}d^{'}&=((k+2)c+(k+1)d)(-ka+(k+1)b)+((k+1)c+kd)((k+1)a-(k+2)b)\\&=-k(k+2)ca+(k+1)(k+2)cb-k(k+1)ad+(k+1)^2bd\\&\quad+(k+1)^2ca-(k+1)(k+2)cb+k(k+1)da-k(k+2)db\\&=ac(-k(k+2)+(k+1)^2)+bd((k+1)^2-k(k+2))\\&=(ac+bd)((k+1)^2-k(k+2))\\&=ac+bd=2u.\end{aligned}$$

Durch die Gleichung

$$\left[\frac{b'}{a'-b'}\right] \;=\; \left[\frac{k(c+d)+c}{c+d}\right] = k$$

werden die Zahlen a, b, c, d aus den Zahlen a', b', c', d' durch die gleiche Matrix gewonnen. Für ungerade $x, y \in \mathbb{N}$ gilt $xy \equiv x + y - 1 \bmod 4$. Daher gilt

$$\begin{aligned} ab + a'b' &\equiv a + b - 1 + a' + b' - 1 \\ &\equiv a + b + (k+2)c + (k+1)d + (k+1)c + kd - 2 \\ &\equiv a + bc + d + 2kc + 2kd + 2c - 2 \\ &\equiv a + bc + d + 2k(c+d) + 2(c-1) \\ &\equiv 0 \bmod 4. \end{aligned}$$

Da $c-1$ und $c+d$ gerade sind, sind $2(c-1)$ und $2k(c+d) \equiv 0 \bmod 4$, und daher auch $a + bc + d \equiv 0 \bmod 4$. Also ist $ab + a'b' \equiv 0 \bmod 4$ und damit $\lambda(ab) = -\lambda(a'b')$. □

Satz 4.9. *Sei u eine ungerade natürliche Zahl. Dann ist $r_4(2u) = 3r_4(u)$.*

Beweis. Die Zahl $2u = u_1^2 + u_2^2 + u_3^2 + u_4^2$ mit ungeradem u ist kongruent 2 modulo 4. Daher sind genau zwei der u_i mit $i = 1, \ldots, 4$ gerade (bzw. ungerade). Wir fordern zusätzlich

$$u_1, u_2 \equiv 0 \bmod 2 \text{ und } u_3, u_4 \equiv 1 \bmod 2.$$

Wegen $\binom{4}{2} = 6$ ergeben sich $\frac{1}{6}r_4(2u)$ Lösungen für ein solches Quadrupel. Wir machen die Substitution

$$y_1 = \frac{u_1 + u_2}{2}, \;\; y_2 = \frac{u_1 - u_2}{2}, \;\; y_3 = \frac{u_3 + u_4}{2}, \;\; y_4 = \frac{u_3 - u_4}{2}. \tag{4.6}$$

Es ist $u = y_1^2 + y_2^2 + y_3^2 + y_4^2$ mit $y_1 + y_2 \equiv 0 \bmod 2$ und $y_3 + y_4 \equiv 1 \bmod 2$ entsprechend den Bedingungen an u_1, u_2, u_3, u_4. Dann ist die Anzahl der Lösungen $(y_1, \ldots, y_4)$ mit diesen Nebenbedingungen ebenfalls $\frac{1}{6}r_4(2u)$. Andererseits gibt es $r_4(u)$ Lösungen für u ohne diese Nebenbedingungen. Die Zahl u ist ungerade, deswegen kann entweder $y_1 + y_2 \equiv 0 \bmod 2$ und $y_3 + y_4 \equiv 1 \bmod 2$ oder umgekehrt sein, d.h. es gibt nur zwei Möglichkeiten. Es gilt also

$$\frac{1}{2}r_4(u) = \frac{1}{6}r_4(2u).$$

Daraus folgt, dass $3r_4(u) = r_4(2u)$ ist. □

Jetzt beweisen wir die Formel für die Anzahl der Darstellungen einer Zahl als Summe von vier Quadratren.

Satz 4.10. *(Jacobi) Es sei n eine natürliche Zahl. Dann gilt*

$$r_4(n) = \begin{cases} 8 \cdot \sigma(n) & \text{für } n \not\equiv 0 \bmod 4 \\ 8 \cdot \sigma(n) - 32 \cdot \sigma\left(\frac{n}{4}\right) & \text{für } n \equiv 0 \bmod 4. \end{cases}$$

Beweis. Es sei

$$4n = x_1^2 + x_2^2 + x_3^2 + x_4^2 \text{ mit } n, x_i \in \mathbb{N} \text{ für } i = 1, \ldots, 4.$$

Diese Zahl $4n$ ist durch 4 teilbar, daher sind alle x_i gerade oder ungerade. Mit $u_i = x_i$ in der Substitution (4.6) gilt

$$2n = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

mit allen y_i gerade oder ungerade.
Im Beweis von Satz 4.9 haben wir gesehen, dass die Anzahl der Darstellungen von $4n$ und $2n$ mit den dortigen Nebenbedingungen gleich sind. Also ist $r_4(4n) = r_4(2n)$.
Da der Beweis der Anzahl der Darstellungen von n auf der Restklasse modulo 4 basiert, betrachten wir alle Reste von n modulo 4.
1. Fall: Es sei n eine ungerade natürliche Zahl.
Es ist

$$4n = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Dann ist die Anzahl der Darstellungen $r_4(4n)$ die Summe der Anzahl der Darstellungen mit allen x_i gerade oder ungerade.
Nach Satz 4.8 gibt es $s(n) = \sigma(n)$ Lösungen mit ungeraden x_i aus $\mathbb{N}$. Und für x_i ungerade aus $\mathbb{Z}$ gibt es $16 \cdot \sigma(n)$ Darstellungen der Zahl $4n$.
Für die Lösungen mit geradem x_i und mit $x_i' = \frac{1}{2}x_i$ ist

$$\begin{aligned} 4n &= 4({x_1'}^2 + {x_2'}^2 + {x_3'}^2 + {x_4'}^2) \\ n &= {x_1'}^2 + {x_2'}^2 + {x_3'}^2 + {x_4'}^2. \end{aligned}$$

Die Anzahl dieser Lösungen ist $r_4(n)$. Dann ergeben sich insgesamt

$$r_4(4n) = r_4(n) + 16 \cdot \sigma(n) \text{ Darstellungen von } 4n.$$

Aus Satz 4.9 folgt

$$3r_4(n) = r_4(2n) = r_4(4n) = r_4(n) + 16 \cdot \sigma(n).$$

Also ist

$$\begin{aligned} 2r_4(n) &= 16 \cdot \sigma(n) \text{ und somit} \\ r_4(n) &= 8 \cdot \sigma(n). \end{aligned}$$

2. Fall: Es sei $n \equiv 2 \bmod 4$.
Gemäß Satz 4.9 gilt

$$\begin{aligned} r_4(n) &= 3 \cdot r_4\Big(\frac{n}{2}\Big) \\ &= 3 \cdot 8 \cdot \sigma\Big(\frac{n}{2}\Big) \\ &= 8 \cdot \sigma(2) \cdot \sigma\Big(\frac{n}{2}\Big) \\ &= 8 \cdot \sigma(n), \end{aligned}$$

da die Funktion σ eine multiplikative zahlentheoretische Funktion ist und $\mathrm{ggT}(2, \frac{n}{2}) = 1$ ist.
3. Fall: Es sei $n \equiv 0 \bmod 4$.
Wir setzen $n = 2^k u$, wobei $k \geq 2$ und u eine ungerade Zahl ist. Dann ist

$$\begin{aligned} r_4(2^k u) &= r_4(2^{k-1}u) = \ldots = r_4(2^{k-(k-2)}u) \\ &= r_4(4u) \\ &= r_4(2u) \\ &= 24 \cdot \sigma(u) \\ &= 8 \cdot 3 \cdot \sigma(u) \\ &= 8 \cdot [\sigma(2^k) - 4\sigma(2^{k-2})] \cdot \sigma(u) \\ &= 8 \cdot \sigma(2^k) \cdot \sigma(u) - 32 \cdot \sigma\Big(\frac{2^k}{4}\Big) \cdot \sigma(u) \\ &= 8 \cdot \sigma(n) - 32 \cdot \sigma\Big(\frac{n}{4}\Big), \end{aligned}$$

da $\mathrm{ggT}(2^k, u) = \mathrm{ggT}(\frac{2^k}{4}, u) = 1$ und σ multiplikativ ist.

□

Am Ende des Kapitels möchten wir zwei Beispiele zur Berechnung von Anzahl der Darstellungen der Zahl n als Summe von vier Quadraten geben.

Beispiel 4.11. Sei $n = 170$.

Die Teiler von n sind $1, 2, 5, 10, 17, 34, 85, 170$. Also ist

$$\sigma(170) = 1 + 2 + 5 + 10 + 17 + 34 + 85 + 170 = 324.$$

Da n nicht durch vier teilbar ist, gilt die erste Bedingung des Satzes 4.10 und wir erhalten

$$r_4(170) = 8 \cdot 324 = 2592$$

Möglichkeiten, die Zahl 170 als Summe von vier Quadraten darzustellen.

Beispiel 4.12. Sei $n = 4$. Die Teiler von n sind $1, 2$ und 4. Daher ist $\sigma(4) = 7$. Und die Anzahl der Darstellungen von 4 gemäß der zweiten Behauptung des Satzes 4.10 ist

$$r_4(4) = 8 \cdot 7 - 32 = 24.$$

Die Zahl 4 hat genau 16 Darstellungen mit Summanden ± 1

$$4 = (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2$$

und 8 Darstellungen mit einem Summand ± 2 und anderen Nullen. Es ist eine von 8 Darstellungen

$$4 = 0 + 0 + 0 + (\pm 2)^2.$$

Bemerkung 4.13. *Die Behauptung des Satzes 13 des Kapitels VII.8 im Buch „Zahlentheorie“ [12] von* Harald Scheid

$$r_4(n) = \begin{cases} 8 \cdot \sigma(n) & \text{wenn } 2 \nmid n, \\ 24 \cdot \sigma(n) & \text{wenn } 2 | n \end{cases}$$

ist nur für $4|n$ nicht richtig.

Nach der zweiten Aussage der Behauptung aus Bemerkung 4.13 gilt, dass

$$r_4(4) = 24 \cdot 7 = 168$$

ist. Dies stimmt mit dem Ergebnis von Beispiel (4.12) nicht überein.

5 Ausblick auf das WARINGsche Problem

In der Vergangenheit haben sich Mathematiker in der Zahlentheorie mit natürlichen Zahlen beschäftigt, die sich als Summe von Quadraten, Kuben, Biquadraten usw. schreiben lassen. Der englische Mathematiker EDWARD WARING[1] hat in seinem Buch „*Meditationes Algebraicae*“ behauptet, dass jede natürliche Zahl als Summe von höch stens neun dritten Potenzen, als Summe von höchstens neunzehn vierten Potenzen usw. darstellbar ist. Diese Behauptung hat er nicht bewiesen und wurde daher als das WARINGsche Problem bekannt, welches sich folgendermaßen formulieren lässt: Zu jedem k existiert ein (minimales) $g(k)$ derart, dass jedes n als Summe von höchstens $g(k)$ k-ten Potenzen dargestellt werden kann. Neben der Existenz gehört zum WARINGschen Problem auch die Frage, wie man $g(k)$ bestimmen bzw. gute Abschätzungen finden kann. Der Satz von LAGRANGE, der in dieser Arbeit betrachtet wurde, ist ein Spezialfall vom WARINGschen Problem, er besagt $g(2) = 4$.

Einen bedeutenden Fortschritt in der Lösung des WARINGschen Problems hat DAVID HILBERT[2] 1909 geleistet. Er hat die WARINGsche Vermutung vollständig bewiesen. Daher bezeichnet man den Satz als den Satz von WARING-HILBERT. Im gleichen Jahr bewiest A.J.A. WIEFERICH, dass maximal neun Summanden benötigt werden, um eine beliebige natürliche Zahl als Summe von Kuben darzustellen.
Nachdem die Existenz eines $g(k)$ für jedes $k \geq 2$ bewiesen war, beschäftigen sich die Mathematiker mit der Ermittlung des kleinsten ausreichenden $g(k)$.
Offensichtlich muss $g(k)$ mit k anwachsen. Eine Abschätzung der Zahl $g(k)$ nach unten wird in folgendem Satz beschrieben, den wir ohne Beweis erwähnen.

Satz 5.1. *Für jede natürliche Zahl $k \geq 2$ gilt*

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

Der rechte Seite der Behauptung im Satz 5.1 bezeichnen wir mit $g^*(k)$. Daraus ergibt sich bei kleinem k die Tabelle 5.1 der unteren Schranken $g^*(k)$ von $g(k)$.

[1] Edward Waring (* 1736 in Old Heath nahe Shrewsbury; †15. August 1798 in Pontesbury, Shropshire).
[2] David Hilbert (23. Januar 1862 in Königsberg; †14. Februar 1943 in Göttingen) war einer der bedeutendsten Mathematiker der Neuzeit.

k	2	3	4	5	6	7	8	9	10	...
$g^*(k)$	4	9	19	37	73	143	279	548	1079	...

Tabelle 5.1: Untere Schranken $g^*(k)$ von $g(k)$ bei kleinem k

Die Mathematiker des 20. Jahrhunderts haben den Satz von Waring-Hilbert mit anderen Beweismethoden gezeigt: In den 1920er Jahren haben G.H. Hardy und J.E. Littlewood auf der Basis der Werke von L.E. Dickson, S.S. Pillai und anderen eine analytische Methode entwickelt, die den Satz von Waring-Hilbert bestätigt und auch eine gute Abschätzung von $g(k)$ gibt (nämlich $g(k) \leq k \cdot 2^{k-1}$) [vgl.[7], Sechster Teil, Einleitung].

Man hat bereits beweisen können, dass $g(k) = g^*(k)$ für $k \leq 471\,600\,000$ gilt. L.E. Dickson hat einen Beweis für $6 \leq k \leq 400$ schon 1936 gegeben. Nach diesem Ergebnis konnte R.M. Stemmler für jedes k aus dem Intervall $400 < k \leq 200\,000$ die minimale Anzahl der Summanden in der Darstellung einer beliebigen natürlichen Zahl n als Summe von k-ten Potenzen nachweisen. Für $k = 4$ haben R. Balasubramanian, J.-M. Deshouillers, F. Dress 1985 und für $k = 5$ hat J.-R. Chen 1964 die Zahl $g(k)$ bestimmt. Im Jahr 1990 konnten J.M. Kubina und M.C. Wunderlich die Gleichheit bis 471 600 000 nachweisen.

In Zukunft soll noch bewiesen werden, dass die Gültigkeit der Gleichung $g(k) = g^*(k)$ für *alle* $k \in \mathbb{N}$ gilt, obwohl man im Bereich $k > 471\,600\,000$ fast vollständige Klarheit hat. So konnte K. Mahler 1957 nachweisen, dass $g(k) > g^*(k)$ höchstens endlich oft möglich ist [vgl.[2], 4 § 1.7].

Anhang

Zusammenfassung

Ziel dieser Arbeit war es, die natürlichen Zahlen aus dem Blickwinkel der Zahlentheorie zu betrachten. Es wurde untersucht, wann die natürlichen Zahlen sich als Summe von zwei, drei bzw. vier Quadraten schreiben lassen. Außerdem wurde die Anzahl der Darstellungen von natürlichen Zahlen als Summe von zwei bzw. vier Quadraten berechnet.

Abstract

The aim of this thesis was to examine natural numbers from the point of view of Number theory. It was described in which cases natural numbers can be written in the form of the sum of two, three or four squares. Finally, the number of representations of natural numbers was calculated as the sum of two or four squares.

Literaturverzeichnis

[1] Brenner H.: *Zahlentheorie - Skript*. in: Institut für Mathematik, Osnabrück, 2008.

[2] Bundschuh P.: *Einführung in die Zahlentheorie*. Springer, 2002.

[3] Ebbinghaus H.-D., K. Mainzer, M. Koecher, R. Remmert: *Zahlen*. Springer, 1992.

[4] Hornfeck B.: *Algebra*. Walter de Gruyter, 1976.

[5] Ischebeck F.: *Einladung zur Zahlentheorie*. Wissenschaftsverlag, 1992.

[6] Krätzel E.: *Zahlentheorie*. VEB Deutscher Verlag der Wissenschaften, 1981.

[7] Landau E.: *Vorlesungen über Zahlentheorie, Vol.1, Sechster Teil*. Chelsea Publishing Company, 1954.

[8] Müller-Stach S./Piontkowski J.: *Elementare und algebraische Zahlentheorie, ein moderner Zugang zu klassischen Themen*. Vieweg & Sohn Verlag, 2006.

[9] Remmert R., P. Ullrich: *Elementare Zahlentheorie*. Birkhäuser Verlag, 1987.

[10] Römer T.: *Elementare Zahlentheorie WS 2004/05 - Skript*. in: Institut für Mathematik, Universität Osnabrück, 2004.

[11] Römer T.: *Einführung in die Algebra SS07 - Skript*. in: Fachbereich Mathematik/Informatik, Universität Osnabrück, 2007.

[12] Scheid H.: *Zahlentheorie*. Wissenschaftsverlag, 1994.

[13] van der Waerden B.L.: *Hamiltons Entdeckung der Quaternionen, Erweiterte Fassung einen Vortrages*. Hubert & Co., Göttingen, 1973.

[14] Weil A.: *Zahlentheorie, ein Gang durch die Geschichte von Hammurapi bis Legendre*. Birkhäuser Verlag, 1992.

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Arbeit selbstständig und unter ausschließlicher Verwendung der angegebenen Literatur und Hilfsmittel erstellt zu haben.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Osnabrück, 9. September 2009 _____

Unterschrift

Abbildungsverzeichnis

Das Bild „Die komplexe Zahlenebene“ (siehe Abbildung 1.1, Seite 6) wurde mit dem Programm „Mathematica“ von Autorin erstellt und unter der Lizenz CC-by-sa 3.0 gestellt.