10. Summen von zwei und vier Quadraten

10.1. Satz. *Eine Primzahl p ist genau dann die Summe zweier Quadratzahlen,*

$$p = u^2 + v^2, \quad u, v \in \mathbb{Z},$$

wenn $p = 2$ oder $p \equiv 1 \bmod 4$.

Beweis. Da $2 = 1^2 + 1^2$, brauchen wir nur ungerade Primzahlen zu betrachten.
a) Die Bedingung $p \equiv 1 \bmod 4$ ist notwendig, denn für das Quadrat einer ganzen Zahl n gilt stets $n^2 \equiv 0, 1 \bmod 4$.

b) Um zu zeigen, dass die Bedingung auch hinreicht, verwenden wir den ersten Ergänzungssatz zum quadratischen Reziprozitätsgesetz. Aus $p \equiv 1 \bmod 4$ folgt $(\frac{-1}{p}) = 1$, es gibt also eine ganze Zahl x mit $x^2 \equiv -1 \bmod p$, d.h.

$$x^2 + 1^2 \equiv 0 \bmod p. \tag{1}$$

Wir wenden nun auf die Zahl x den im Anschluss bewiesenen Satz von Thue an. Danach gibt es ganze Zahlen u, v mit $0 < |u|, |v| < \sqrt{p}$, so dass

$$vx \equiv u \bmod p.$$

Multiplizieren wir Kongruenz (1) mit v^2, ergibt sich

$$u^2 + v^2 \equiv 0 \bmod p,$$

also $u^2 + v^2 = kp$ mit einer ganzen Zahl k. Wegen der Größenabschätzung für u und v ist $0 < u^2 + v^2 < 2p$ und es folgt

$$u^2 + v^2 = p.$$

Damit ist Satz 10.1 bewiesen bis auf den noch ausstehenden Beweis des folgenden Satzes von Thue.

10.2. Satz (Thue). *Sei p eine ungerade Primzahl und $x \in (\mathbb{Z}/p)^*$. Dann existieren ganze Zahlen u, v mit $0 < |u| < \sqrt{p}$ und $0 < |v| < \sqrt{p}$, so dass*

$$vx \equiv u \bmod p.$$

Bemerkung. Im Körper $\mathbb{F}_p = \mathbb{Z}/p$ hat man also $x = u/v$ und Zähler und Nenner lassen sich so durch ganze Zahlen $u, v \in \mathbb{Z}$ repräsentieren, dass die Ungleichungen $|u|, |v| < \sqrt{p}$ erfüllt sind.

Beweis. Wir betrachten die Menge

$$X := \{(u, v) \in \mathbb{Z} \times \mathbb{Z} : 0 \leqslant u, v < \sqrt{p}\}.$$

Es gibt $\lfloor \sqrt{p} \rfloor + 1$ ganze Zahlen n mit $0 \leqslant n < \sqrt{p}$. Daraus folgt $\#X > p$. Deshalb ist die Abbildung

$$X \longrightarrow \mathbb{Z}/p, \quad (u, v) \mapsto (vx - u) \bmod p$$

nicht injektiv, es gibt also in X mindestens zwei Paare $(u_1, v_1) \neq (u_2, v_2)$ mit

$$(v_1 x - u_1) \equiv (v_2 x - u_2) \bmod p \quad \Longrightarrow \quad (v_1 - v_2)x \equiv (u_1 - u_2) \bmod p.$$

Es ist $v_1 \neq v_2$, denn andernfalls wäre $u_1 \equiv u_2 \bmod p$, sogar $u_1 = u_2$, also $(u_1, v_1) = (u_2, v_2)$, Widerspruch. Mit

$$u := u_1 - u_2, \quad v := v_1 - v_2$$

gilt daher die Behauptung des Satzes von Thue.

Wir kommen jetzt zu der Frage, welche allgemeinen natürlichen Zahlen $n \in \mathbb{N}_1$ sich als Summe von zwei Quadratzahlen darstellen lassen. Mithilfe des folgenden Satzes kann man das Problem auf den Fall von Primzahlen zurückführen.

10.3. Satz. *Seien $n_1, n_2 \in \mathbb{N}_1$ natürliche Zahlen, die sich als Summe zweier Quadratzahlen darstellen lassen. Dann ist auch $n := n_1 n_2$ Summe zweier Quadratzahlen.*

Beweis. Sei $n_1 = x_1^2 + y_1^2$ und $n_2 = x_2^2 + y_2^2$ mit ganzen Zahlen x_ν, y_ν. Wir betrachten die ganzen Gaußschen Zahlen

$$z_1 := x_1 + iy_1 \in \mathbb{Z}[i], \quad z_2 := x_2 + iy_2 \in \mathbb{Z}[i].$$

Es gilt $n_1 = |z_1|^2 = x_1^2 + y_1^2$ und $n_2 = |z_2|^2 = x_2^2 + y_2^2$. Das Produkt $z_3 := z_1 z_2$ ist ebenfalls eine ganze Gaußsche Zahl, $z_3 = x_3 + iy_3$. Da $|z_3|^2 = |z_1|^2 \cdot |z_2|^2$, folgt

$$n = n_1 n_2 = x_3^2 + y_3^2, \quad \text{q.e.d.}$$

10.4. Satz. *Eine natürliche Zahl $n \in \mathbb{N}_1$ ist genau dann Summe von zwei Quadratzahlen, wenn in der kanonischen Primfaktor-Zerlegung*

$$n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$$

alle Primfaktoren mit $p_j \equiv 3 \bmod 4$ einen geraden Exponenten k_j haben.

Beweis. a) Wir zeigen zunächst, dass die angegebene Bedingung hinreicht. Wir stellen n dar als $n = m^2 n'$, wobei n' nur Primfaktoren $p = 2$ oder $p \equiv 1 \bmod 4$ enthält. Jeder dieser Primfaktoren von n' ist nach Satz 10.1 Summe zweier Quadratzahlen, also nach Satz 10.3 auch n', d.h.

$$n' = x^2 + y^2 \quad \text{mit } x, y \in \mathbb{Z}.$$

Daraus folgt $n = (mx)^2 + (my)^2$, q.e.d.

b) Zum Beweis der Umkehrung setzen wir voraus, dass $n = x^2 + y^2$ mit $x, y \in \mathbb{Z}$. Sei $p \mid n$ ein Primteiler mit $p \equiv 3 \bmod 4$. Wir müssen zeigen, dass p mit gerader Vielfachheit in n vorkommt. Sei $k \in \mathbb{N}_0$ der maximale Exponent, so dass

$$p^k \mid x \quad \text{und} \quad p^k \mid y,$$

also $x = p^k x_1$, $y = p^k y_1$ mit ganzen Zahlen x_1, y_1. Wegen der Maximaleigenschaft von k ist entweder x_1 oder y_1 nicht durch p teilbar. O.B.d.A. sei $p \nmid x_1$. Es gilt

$$n = x^2 + y^2 = p^{2k}(x_1^2 + y_1^2).$$

Angenommen, die Vielfachheit von p in n wäre ungerade, so würde daraus folgen, dass $p \mid x_1^2 + y_1^2$, d.h.

$$x_1^2 + y_1^2 \equiv 0 \bmod p.$$

Da $x_1 \not\equiv 0 \bmod p$, besitzt x_1 ein Inverses modulo p, es gibt also eine ganze Zahl u mit $ux_1 \equiv 1 \bmod p$. Multipliziert man die obige Kongruenz mit u^2, erhält man mit $z := uy_1$ eine Lösung der Kongruenz

$$z^2 \equiv -1 \bmod p.$$

Das heißt aber, dass -1 quadratischer Rest modulo p ist, was wegen $p \equiv 3 \bmod 4$ im Widerspruch zum ersten Ergänzungssatz des quadratischen Reziprozitätsgesetzes steht. Also ist die Annahme falsch und damit Satz 10.4 bewiesen.

Nach Satz 10.4 kann man nur spezielle natürliche Zahlen als Summe von zwei Quadratzahlen darstellen. Für die Darstellung beliebiger natürlicher Zahlen benötigt man mehr Quadrate. Auch drei Quadrate reichen im Allgemeinen nicht aus. Z.B. ist leicht zu sehen, dass sich die Zahl 7 nicht als Summe von drei Quadratzahlen darstellen lässt. Wir werden auf die genauen Bedingungen, welche natürlichen Zahlen sich als Summe von drei Quadratzahlen darstellen lassen, in Kap.**??** zurückkommen. Im Rest dieses Paragraphen beweisen wir den Satz von Lagrange, dass sich jede natürliche Zahl als Summe von vier Quadratzahlen darstellen lässt.

10.5. Quaternionen. So wie im Fall der Summendarstellung durch zwei Quadrate die ganzen Gaußschen Zahlen nützlich waren, sind es im Fall der Summen von vier Quadraten die ganzzahligen Quaternionen. Die von Hamilton erfundenen Quaternionen $\mathbb{H}$ bilden einen 4-dimensionalen Vektorraum über $\mathbb{R}$. Außer der Vektorraum-Addition ist noch eine Multiplikation definiert. Mit diesen zwei Verknüpfungen wird $\mathbb{H}$ zu einem sog. Schiefkörper, d.h. es sind alle Körperaxiome bis auf das Kommutativ-Gesetz der Multiplikation erfüllt.

Wir benötigen hier nur die ganzzahligen Quaternionen, die wir mit $\mathbb{H}_\mathbb{Z}$ bezeichnen. Als additive Gruppe ist $\mathbb{H}_\mathbb{Z}$ isomorph zu $\mathbb{Z}^4$ mit komponentenweiser Addition.

$$\mathbb{H}_\mathbb{Z} \mathrel{\widehat{=}} \{(x_0, x_1, x_2, x_3) : x_\nu \in \mathbb{Z}\} = \mathbb{Z}^4.$$

Zur Definition der Multiplikation ist eine Matrix-Schreibweise der Quaternionen nützlich. Wir identifizieren $\mathbb{H}_\mathbb{Z}$ mit folgender Menge von 2×2-Matrizen:

$$\begin{aligned}\mathbb{H}_\mathbb{Z} &= \left\{ \begin{pmatrix} x_0 + ix_1 & x_2 + ix_3 \\ -x_2 + ix_3 & x_0 - ix_1 \end{pmatrix} : x_0, x_1, x_2, x_3 \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : z, w \in \mathbb{Z}[i] \right\}.\end{aligned}$$

Es ist leicht nachzurechnen, dass das Produkt zweier Matrizen aus $\mathbb{H}_\mathbb{Z}$ wieder in $\mathbb{H}_\mathbb{Z}$ liegt, woraus folgt, dass $\mathbb{H}_\mathbb{Z}$ einen Ring bildet. Mit den Definitionen

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I_1 := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad I_2 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad I_3 := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

lässt sich jedes Element $X \in \mathbb{H}_\mathbb{Z}$ eindeutig schreiben als

$$X = x_0 E + x_1 I_1 + x_2 I_2 + x_3 I_3 \quad \text{mit } x_0, x_1, x_2, x_3 \in \mathbb{Z}.$$

E ist das Einselement von $\mathbb{H}_\mathbb{Z}$ und es gelten die Rechenregeln

$$I_1^2 = I_2^2 = I_3^2 = -E,$$
$$I_1 I_2 = -I_2 I_1 = I_3, \quad I_2 I_3 = -I_3 I_2 = I_1, \quad I_3 I_1 = -I_1 I_3 = I_2.$$

Die konjugierte Quaternion X^σ ist definiert durch

$$X^\sigma := x_0 E - x_1 I_1 - x_2 I_2 - x_3 I_3.$$

Die konjugierte Quaternion lässt sich auch darstellen als

$$X^\sigma = \overline{X}^\top \quad \text{(Transponierte der konjugiert komplexen Matrix)}.$$

Wir definieren eine Normabbildung durch

$$\mathrm{N} : \mathbb{H}_\mathbb{Z} \to \mathbb{N}_0, \quad X \mapsto \det(X).$$

Für $X = \begin{pmatrix} x_0 + ix_1 & x_2 + ix_3 \\ -x_2 + ix_3 & x_0 - ix_1 \end{pmatrix}$ ist

$$\mathrm{N}(X) = \det(X) = x_0^2 + x_1^2 + x_2^2 + x_3^2$$

sowie

$$X X^\sigma = \mathrm{N}(X) \cdot E \quad \text{und} \quad \mathrm{N}(X^\sigma) = \mathrm{N}(X).$$

Aus dem Determinanten-Multiplikationssatz folgt

$$\mathrm{N}(XY) = \mathrm{N}(X)\mathrm{N}(Y) \quad \text{für alle } X, Y \in \mathbb{H}_\mathbb{Z}.$$

10.6. Satz. *Sind n_1, n_2 zwei natürliche Zahlen, die sich als Summe von vier Quadratzahlen darstellen lassen. Dann ist auch das Produkt $n = n_1 n_2$ Summe von vier Quadratzahlen.*

Beweis. Eine natürliche Zahl ist genau dann die Summe von vier Qudratzahlen, wenn sie gleich der Norm einer ganzzahligen Quaternion ist. Es gibt also $X, Y \in \mathbb{H}_\mathbb{Z}$, so dass

$$n_1 = \mathrm{N}(X), \quad n_2 = \mathrm{N}(Y).$$

Da $n = n_1 n_2 = \mathrm{N}(X)\mathrm{N}(Y) = \mathrm{N}(XY)$, ist n die Norm von $XY \in \mathbb{H}_\mathbb{Z}$, q.e.d.

10.7. Lemma. *Sei p eine Primzahl mit $p \equiv 3 \bmod 4$. Dann gibt es ganze Zahlen $x, y \in \mathbb{Z}$, so dass*

$$x^2 + y^2 \equiv -1 \bmod p.$$

Beweis. Unter den Zahlen $1, 2, ..., p-1$ gibt es ebenso viele quadratische Rest modulo p wie Nichtreste. Die Zahl 1 ist ein quadratischer Rest. Es gibt deshalb eine natürliche Zahl k mit $1 \leqslant k < p-1$, so dass k quadratischer Rest modulo p ist, aber $k+1$ quadratischer Nichtrest. Da $p \equiv 3 \bmod 4$, ist -1 quadratischer Nichtrest modulo p. Deshalb ist $(-1)(k+1) = -k-1$ quadratischer Rest modulo p. Es gibt also ganze Zahlen x, y, so dass

$$x^2 \equiv k \bmod p \quad \text{und} \quad y^2 \equiv -k-1 \bmod p.$$

Addiert man die beiden Kongruenzen, erhält man

$$x^2 + y^2 \equiv -1 \bmod p,$$

und damit die Behauptung von Lemma 10.7.

10.8. Satz (Lagrange). *Jede natürliche Zahl n lässt sich als Summe von vier Quadratzahlen darstellen.*

Beweis. Wegen Satz 10.6 genügt es, den Satz für Primzahlen zu beweisen. Außerdem ist nach Satz 10.1 nur noch der Fall $p \equiv 3 \bmod 4$ zu behandeln.

Nach Lemma 10.7 gibt es ganze Zahlen x_0, x_1 mit $x_0^2 + x_1^2 \equiv -1 \bmod p$, d.h. mit $x_2 = 1$ und $x_3 = 0$ haben wir

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = kp \tag{2}$$

mit einer ganzen Zahl $k \geqslant 1$. Falls $k = 1$, sind wir fertig. Für den allgemeinen Fall $k > 1$ verwenden wir die sog. *Abstiegsmethode*, die darin besteht, aus der Darstellung (2) eine analoge Darstellung mit einem kleineren k zu konstruieren. Nach endlich vielen Schritten ist man dann bei $k = 1$ angelangt.

i) Zunächst können wir, indem wir die x_ν durch ihre absolut kleinsten Reste modulo p ersetzen, o.B.d.A. annehmen, dass $|x_\nu| < p/2$ für alle ν. Dann ist $\sum_{\nu=0}^{3} x_\nu^2 < p^2$, d.h. in (2) ist $k < p$.

ii) Ist k gerade, so ist die Anzahl der ungeraden x_ν gerade. Daraus folgt, dass wir nach evtl. Umnummerierung voraussetzen können, dass

$$x_0 \equiv x_1 \bmod 2, \quad \text{und} \quad x_2 \equiv x_3 \bmod 2.$$

Dann sind $(x_0 \pm x_1)/2$ und $(x_2 \pm x_3)/2$ ganze Zahlen und

$$\begin{aligned}&\Big(\frac{x_0+x_1}{2}\Big)^2+\Big(\frac{x_0-x_1}{2}\Big)^2+\Big(\frac{x_2+x_3}{2}\Big)^2+\Big(\frac{x_2-x_3}{2}\Big)^2\\&=\frac{1}{2}(x_0^2+x_1^2+x_2^2+x_3^2)=\frac{k}{2}\cdot p,\end{aligned}$$

wir haben also eine Halbierung von k erreicht.

iii) Sei nun $k>1$ ungerade. Sei $X \in \mathbb{H}_\mathbb{Z}$ die Quaternion mit den Koeffizienten x_ν. Weiter sei $\widetilde{x}_\nu$ der absolut kleinste Rest von x_ν modulo k, also $\widetilde{x}_\nu \equiv x_\nu \bmod k$ und $|\widetilde{x}_\nu| < k/2$. Wir fassen die $\widetilde{x}_\nu$ zu $\widetilde{X} \in \mathbb{H}_\mathbb{Z}$ zusammen. Es ist $\widetilde{X} \neq 0$, denn andernfalls wären alle x_ν durch k teilbar, also $k^2 \mid \mathrm{N}(X) = kp$, was wegen $\gcd(k,p)=1$ unmöglich ist. Nun ist

$$\mathrm{N}(\widetilde{X}) = \sum_{\nu=0}^{3} \widetilde{x}_\nu^2 =: m < k^2 \quad \text{mit } m \in \mathbb{N}_1, \tag{3}$$

und es existiert ein $V \in \mathbb{H}_\mathbb{Z}$, so dass $\widetilde{X} = X + kV$. Wir definieren nun

$$Y := X\widetilde{X}^\sigma = XX^\sigma + kXV^\sigma. \tag{4}$$

Da $XX^\sigma = \mathrm{N}(X)E = kpE$, folgt mit $Z := pE + XV^\sigma$

$$Y = kpE + kXV^\sigma = k(pE + XV^\sigma) = kZ \tag{5}$$

Aus (4) und (5) folgt

$$\mathrm{N}(Y) = \mathrm{N}(X)\mathrm{N}(\widetilde{X}^\sigma) = kp \cdot m \quad \text{und} \quad \mathrm{N}(Y) = k^2\mathrm{N}(Z), \tag{6}$$

also $k \mid pm$. Da $\gcd(k,p)=1$, ist k ein Teiler vom m und aus (3) ergibt sich $m = k'k$ mit einer natürlichen Zahl $k' < k$. Aus (6) folgt nun der gewünschte Abstieg

$$\mathrm{N}(Z) = k'p.$$

Damit ist Satz 10.8 bewiesen.

Aufgaben

10.1. Man gebe einen Beweis des Satzes 10.1, der anstelle des Satzes 10.2 von Thue die Abstiegsmethode verwendet.

10.2. Dass -1 für eine ungerade Primzahl p genau dann quadratischer Rest ist, wenn $p \equiv 1 \bmod 4$, lässt sich auch mit einer Variante des Satzes von Wilson zeigen. Man beweise dazu:

Sei p eine ungerade Primzahl. Dann gilt

$$\left(\tfrac{p-1}{2}!\right)^2 \equiv (-1)^{(p+1)/2} \bmod p.$$

10.3. Man stelle die Zahlen $n = 1, 2, 3, \ldots, 32$ jeweils als Summe einer kleinstmöglichen Anzahl von Quadraten dar.

10.4. Sei $Q_8 := \{X \in \mathbb{H}_\mathbb{Z} : \mathrm{N}(X) = 1\}$. Man zeige:

a) Bzgl. der Multiplikation von Quaternionen ist Q_8 eine Gruppe mit 8 Elementen, die sog. Quaternionengruppe.

b) Q_8 besitzt genau drei zyklische Untergruppen der Ordnung 4.

c) Je zwei solche Untergruppen sind konjugiert, d.h. sind $G_1, G_2 \subset Q_8$ zyklische Untergruppen der Ordnung 4, so gibt es ein Element $\alpha \in Q_8$ mit

$$\alpha G_1 \alpha^{-1} = G_2.$$