WiSe '21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ 13: Summen von Quadraten

Stichworte: Pythagoras, Summe von 2 □en und $\mathbb{Z}[i]$, 3-Quadratesatz von Legendre, 4-Quadrate-Satz von Lagrange, andere quadratische Formen und pythagoräische Quadrupel

13.1. Einleitung: Ganzzahlige Lösungen der Gleichung $x^2+y^2=z^2$ heißen pythagoräische Tripel. Mit den indischen Formeln können alle diese Lösungen angegeben werden. Darüberhinaus stellt sich die Frage, welche natürlichen Zahlen als Summe zweier Quadratzahlen geschrieben werden können. Durch Untersuchung der Primelemente im Gaußschen Zahlring $\mathbb{Z}[i]$ kann diese beantwortet werden. Wir gehen auch kurz auf andere quadratische Formen und insb. den 4-Quadratesatz von Lagrange ein.

13.2. Def.: Ein Tripel $(x,y,z)\in\mathbb{N}^3$ natürlicher Zahlen heißt pythagoräisches Tripel, wenn $x^2+y^2=z^2$ ist. Kurz: pyth. Tripel. Ein pyth. Tripel (x,y,z) heißt primitiv, falls $(x,y,z)=1$ ist.

13.3. Bem.: Ein pyth. Tripel (x,y,z) ist genau dann primitiv, falls $(x,y)=1$ gilt. Dann: $2\mid x \vee 2\mid y$.
[„$\Leftarrow$": mit $p\mid(x,y,z)$ folgt $p\mid(x,y)=1$ ↯, „$\Rightarrow$": • wäre $p\mid(x,y)$, folgte $p\mid x^2+y^2=z^2$ und $p\mid(x,y,z)=1$ ↯.]
• Weiter $2\mid x$ (oder $2\mid y$), sonst $x^2\equiv y^2\equiv 1\ (4)$, $z^2\equiv 2\ (4)$, ↯ denn Quadrate sind nur $\equiv 0\ (4)$ oder $\equiv 1\ (4)$.
OE sei $2\mid x$.

13.4. Satz (indische Formeln): Es gilt
$$\{(x,y,z)\in\mathbb{N}^3;\ (x,y)=1,\ 2\mid x,\ x^2+y^2=z^2\}=\{(2uv,\ u^2-v^2,\ u^2+v^2);\ u,v\in\mathbb{N},\ u>v,\ u+v\equiv 1\ (2),\ (u,v)=1\}.$$

13.5. Bem.: • Man erhält also alle primitiven pyth. Tripel (x,y,z) durch Parametrisierung mit $u,v\in\mathbb{N}$, $u>v$, $u+v\equiv 1\ (2)$, $(u,v)=1$, nämlich $x:=2uv$, $y:=u^2-v^2$, $z:=u^2+v^2$.
• Alle pyth. Tr. erhält man aus den primitiven pyth. Tripeln (x,y,z) durch Multiplikation mit $d\in\mathbb{N}$, also in der Form (dx,dy,dz).
• Wir betrachten OE nur Tripel mit $x,y,z\in\mathbb{N}$, nicht $\in\mathbb{Z}$. Und Tripel $(x,0,x)$ sind trivial.

Bew.: „$\subseteq$": Seien $x,y,z \in \mathbb{N}$, $2|x$, $(x,y)=1$ und $x^2+y^2=z^2$. Dann ist $2\nmid z$, $2\nmid y$, also sind $\frac{z-y}{2}, \frac{z+y}{2} \in \mathbb{Z}$ und $\left(\frac{z-y}{2}, \frac{z+y}{2}\right)=1$. $\ulcorner p \mid \frac{z-y}{2}, p \mid \frac{z+y}{2} \Rightarrow p \mid z,y, x$ ↯. $\lrcorner$
Haben $\left(\frac{x}{2}\right)^2 = \frac{z+y}{2}\cdot\frac{z-y}{2}$. Aus der Teilerfremdheit folgt: $\frac{z+y}{2}=u^2$, $\frac{z-y}{2}=v^2$ für $u,v\in\mathbb{N}$.
Somit ist $z=u^2+v^2$, $y=u^2-v^2$, $u>v$, $(u,v)=1$.
Aus $x^2+y^2=z^2$ ergibt sich $x=2uv$. Weiter ist $u+v \equiv u^2+v^2 \equiv z \equiv 1 \ (2)$.

„$\supseteq$": • Seien $u,v\in\mathbb{N}$, $u>v$, $u+v\equiv 1(2)$, $(u,v)=1$, $x:=2uv$, $y:=u^2-v^2$, $z:=u^2+v^2$. Dann gilt $x,y\in\mathbb{N}$ wegen $u>v$,
$z\in\mathbb{N}$, $2|x$ wegen $x=2uv$
und $x^2+y^2=(2uv)^2+(u^2-v^2)^2 = u^4+2u^2v^2+v^4=(u^2+v^2)^2=z^2$.

• Sei $d:=(x,y)$. Dann teilt d^2 auch z^2, und deshalb teilt d auch z. $\ulcorner$PFZ! $\lrcorner$
Wegen $d|y$, $d|z$ teilt d auch die Differenz und Summe von y und z,
d.h. $d\,|\,2u^2$, $d\,|\,2v^2$, also $d \mid (2u^2,2v^2)=2(u^2,v^2) \underset{(u,v)=1}{=} 2$,
es folgt $d|2$, also $d\in\{1,2\}$.
Nun folgt aus $u+v\equiv 1(2)$ aber $y=u^2-v^2\equiv 1\ (2)$,
und mit $d|y$ bleibt nur noch $d=1$. □

13.6. Bem.: • Die zulässigen Tripel (x,y,z) und Paare u,v sind einander bijektiv zugeordnet.
Die ersten (u,v) ergeben:

u	2	3	4	4	...
v	1	2	1	3	...
x	4	12	8	24	...
y	3	5	15	7	...
z	5	13	17	25	...

Die pythagoreische Gleichung $x^2+y^2=z^2$ hat demnach unendlich viele Lösungen in $\mathbb{N}^3$.
• Die indischen Formeln Satz 13.4 zeigen, welche Quadratzahlen z^2 sich als Summe zweier Quadrate schreiben lassen. Es soll noch untersucht werden, für welche $n\in\mathbb{N}$ dies überhaupt zutrifft.
Ziel ist nun eine Charakterisierung aller nat. Zahlen, die als Summe von zwei Quadraten darstellbar sind: der Satz von Euler über die Summe von zwei Quadraten, s.u. Satz 13.21.1.

Eine unmittelbare, leicht einzusehende Feststellung ist schonmal:

13.7. Satz (Fermat): Eine PZ p ist als $p=x^2+y^2$ darstellbar, genau wenn $p\equiv 1\,(4)$ oder $p=2$.
Bew.: „$\Rightarrow$": Sei $p=x^2+y^2$, und mit $p|y$ folgt $p|x$ ↯. Ⓔ $p\nmid y \Rightarrow x^2\equiv -y^2\,(p) \overset{p\neq 2}{\Rightarrow} 1=\left(\frac{-y^2}{p}\right)=\left(\frac{-1}{p}\right) \underset{1.\,EG}{=} (-1)^{\frac{p-1}{2}} \Rightarrow p\equiv 1(4)$.

„⇐": Laut Ü Bl.8 Aufg.5 ist $r^2 \equiv -1\ (p)$ für $p \equiv 1\ (4)$ explizit lösbar durch $r \equiv \pm \left(\frac{p-1}{2}\right)!\ (p)$.

Von den $>p$ vielen $xr+y$ für $0 \le x,y < \sqrt{p}$ müssen 2 mod p kongruent sein: $x_1 r + y_1 \equiv x_2 r + y_2\ (p)$

$\Rightarrow x := x_1 - x_2,\ y := y_1 - y_2$ (nicht $x=y=0$) erfüllen $xr+y \equiv 0\ (p)$, und $x^2+y^2 \equiv x^2 + (-xr)^2 = x^2(1+r^2) \equiv 0\ (p) \overset{0<x^2+y^2<2p}{\Longrightarrow} x^2+y^2 = p$. □

Wir verwenden im folgenden einen algebraischen Ansatz durch Betrachtung des Gaußschen Zahlrings.

13.8. Def.: Der Ring $\mathbb{Z}[i] := \{a+bi;\ a,b \in \mathbb{Z}\}$ mit $i = \sqrt{-1} \in \mathbb{C}$,

d.h. mit der Multiplikation $(a+bi)(u+vi) := (au - bv) + i(av + bu)$,

heißt Gaußscher Zahlring. Die Abb. $N: \mathbb{Z}[i] \to \mathbb{Z},\ N(a+bi) := \underbrace{a^2+b^2}_{\text{Summe zweier Quadrate!}}$

heißt Norm bzw. Normabbildung von $\mathbb{Z}[i]$.

13.9. Bem.: Haben: $N(a+bi) = (a+bi)\cdot\overline{(a+bi)} = (a+bi)(a-bi)$.

13.10 Satz: Die Norm N auf $\mathbb{Z}[i]$ ist multiplikativ, d.h. $\forall \alpha,\beta \in \mathbb{Z}[i]: N(\alpha\beta) = N(\alpha)N(\beta)$.

Bew.: $N((a+bi)(u+vi)) = N((au-bv)+i(av+bu)) = (au-bv)^2 + (av+bu)^2$

$= a^2u^2 - 2abuv + b^2v^2 + a^2v^2 + 2abuv + b^2u^2 = (a^2+b^2)\cdot(u^2+v^2) = N(a+bi)\cdot N(u+vi)$. □

13.11. Bem.: $\mathbb{Z}[i]$ hat die Einheitengruppe $\mathbb{Z}[i]^\times = \{1,-1,i,-i\}$,

⌐$\alpha \in \mathbb{Z}[i]$ heißt Einheit, falls $\exists \beta \in \mathbb{Z}[i]$ mit $\alpha\beta = 1$. D.h. die Einheiten sind die Teiler der 1.⌋

Bew.: Ist $a+bi \in \mathbb{Z}[i]^\times$ eine Einheit, so ex. $u+vi \in \mathbb{Z}[i]$ mit $(a+bi)(u+vi) = 1$, also folgt $1 = N(1) \overset{13.10}{=} N(a+bi)\,N(u+vi) = (a^2+b^2)\cdot(u^2+v^2)$, also $a^2+b^2 = 1$, d.h. $(a,b) \in \{(0,\pm 1),(\pm 1,0)\}$. □

13.12. Satz: $\mathbb{Z}[i]$ ist euklidischer Ring mit der Norm als euklidischer Funktion,

d.h. $\forall \beta,\alpha \in \mathbb{Z}[i],\ \alpha \neq 0,\ \exists \gamma,\rho \in \mathbb{Z}[i]: \beta = \gamma\alpha + \rho$ und $N(\rho) < N(\alpha)$.

"Division von β durch α" "mit Rest ρ von kleinerer Norm als die Norm von α"

Bew.: Genügt, z.z.: Beh. ⊛: $\forall \eta \in \mathbb{Q}(i) := \{x+yi;\ x,y \in \mathbb{Q}\}\ \exists \gamma \in \mathbb{Z}[i]: N(\eta - \gamma) < 1$.

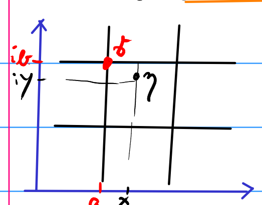
⌐Denn mit $\eta := \frac{\beta}{\alpha} \in \mathbb{Q}(i)$, denn $\mathbb{Q}(i)$ ist Körper ⌐!⌋, und γ laut Beh. ⊛

folgt für $\rho := \beta - \gamma\alpha \in \mathbb{Z}[i]$, dass $N(\rho) = N(\beta - \gamma\alpha) = N(\eta\alpha - \gamma\alpha) = N((\eta-\gamma)\alpha)$

$\overset{\text{Multipl. Satz 13.10}}{=} N(\eta-\gamma)\,N(\alpha) < N(\alpha)$.⌋

Bew. der Beh. ⊛: Sei $\eta = x+yi \in \mathbb{Q}(i),\ x,y \in \mathbb{Q}$. Dann $\exists a \in \mathbb{Z}: |x-a| \le \frac{1}{2}$,

$\exists b \in \mathbb{Z}: |y-b| \le \frac{1}{2}$.



Dann ist $\gamma := a+bi \in \mathbb{Z}[i]$ und $\eta - \gamma = r + si$ mit $|r|,|s| \le \frac{1}{2}$,

also $N(\eta-\gamma) = N(r+si) = r^2+s^2 \le \frac{1}{4}+\frac{1}{4} = \frac{1}{2} < 1$. □

13.13. Bem.: $\mathbb{Z}[i]$ ist also ein faktorieller Ring, da er euklidisch ist, vgl. [Algebra, A13.16/A13.17]

In ihm ist von jedem $\alpha \in \mathbb{Z}[i]$ eine eind. PFZ in Primelemente möglich.

13.14. Def.: $\pi \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$ (d.h. π keine Einheit) heißt Primelement, falls $\forall \alpha, \beta \in \mathbb{Z}[i]: \pi \mid \alpha\beta \Rightarrow \pi \mid \alpha \vee \pi \mid \beta$.

13.15. Satz: Sei $\pi \neq 0$ ein Primelement von $\mathbb{Z}[i]$. Dann gibt es genau eine Primzahl $p \in \mathbb{P}$ mit $\pi \mid p$ ⌜in $\mathbb{Z}[i]$⌟. Es gilt entweder $N(\pi) = p$ oder $N(\pi) = p^2$.

Bew.: $N(\pi) = \pi\bar{\pi} \Rightarrow \pi \mid N(\pi)$, $N(\pi) \in \mathbb{N}$ keine Einheit in $\mathbb{Z}$.
Sei $N(\pi) = p_1 \cdots p_r$ mit Primzahlen p_j, $r \geq 1$, die PFZ von $N(\pi)$.
Da π Primelement, teilt π ein $p_j =: p \in \mathbb{P}$. Aus $\pi \mid p$ folgt $N(\pi) \mid N(p) = p^2$, also ist $N(\pi) = p$ oder $N(\pi) = p^2$.
Dabei ist p eindeutig: $\pi \mid q \Rightarrow N(\pi) \mid N(q) = q^2 \Rightarrow p \mid q^2 \Rightarrow p = q$. □

13.16. Zur Auffindung der Primelemente in $\mathbb{Z}[i]$ sind also die Zerlegungen der $p \in \mathbb{P}$ in $\mathbb{Z}[i]$ zu untersuchen. Zur Unterscheidung: Die $p \in \mathbb{P}$ heißen rationale Primzahlen, die π heißen Gaußsche Primzahlen. (Hier: "Primelemente".)

13.17. Def.: $\alpha, \beta \in \mathbb{Z}[i]$ heißen assoziiert, falls $\alpha = \beta\varepsilon$ für ein $\varepsilon \in \mathbb{Z}[i]^\times$. Kurz: $\alpha \mathrel{\hat{=}} \beta$.

13.18. Satz: Sei $p \in \mathbb{P}$ und π ein Primfaktor von p in $\mathbb{Z}[i]$ (d.h. Primel. $\pi \mid p$).
Dann gibt es drei Fälle:
(1.) $p \mathrel{\hat{=}} \pi^2$, d.h. p verzweigt in $\mathbb{Z}[i]$,
(2.) $p \mathrel{\hat{=}} \pi$, d.h. p träge in $\mathbb{Z}[i]$ (da p Primel. bleibt),
(3.) $p = \pi\bar{\pi}$ mit $\pi \not\mathrel{\hat{=}} \bar{\pi}$, d.h. p zerfällt in $\mathbb{Z}[i]$.

Dabei gilt:
(1.) $\Leftrightarrow p = 2$,
(2.) $\Leftrightarrow N(\pi) = p^2 \Leftrightarrow p \equiv 3\ (4)$.
(3.) $\Leftrightarrow N(\pi) = p \Leftrightarrow p \equiv 1\ (4)$.

Bew.: Sei $p = \gamma\pi$ mit $\gamma \in \mathbb{Z}[i]$. Dann ist $p^2 = N(\gamma)N(\pi)$.
1. Fall: $N(\pi) = p^2$, d.h. $N(\gamma) = 1 \Leftrightarrow \gamma$ Einheit $\Leftrightarrow p \mathrel{\hat{=}} \pi$.
2. Fall: $N(\pi) = p$, d.h. $\pi\bar{\pi} = p$, $\bar{\pi}$ auch Primelement (da $\mathbb{Q}(i) \to \mathbb{Q}(i)$, $\alpha \mapsto \bar{\alpha}$ Auto), und: $\pi \mathrel{\hat{=}} \bar{\pi} \Leftrightarrow p \mathrel{\hat{=}} \pi^2$.

Sei $\pi = a + bi$, dann ist $(a,b) = 1$. Gelte $\pi \mathrel{\hat{=}} \bar{\pi} \Rightarrow \pi \mid \pi + \bar{\pi}$, $\pi \mid \pi - \bar{\pi} \Rightarrow \pi \mid 2a$, $\pi \mid 2b$
$\Rightarrow p \mid 2a$, $p \mid 2b \Rightarrow p \mid 2 \Rightarrow p = 2$. ⌜Denn: $\pi \mid c \in \mathbb{Z} \Rightarrow N(\pi) \mid N(c) \Rightarrow p \mid c^2 \Rightarrow p \mid c$⌟
Haben $2 = (1+i)(1-i)$ und $1 - i = -i(1+i) \mathrel{\hat{=}} 1+i$, ist Primel. ⌜!⌟
→ 2 ist verzweigt. → ⌜$N(1+i) = 2$ prim $\Rightarrow 1+i$ irred., also prim im faktoriellen $\mathbb{Z}[i]$⌟

Bleibt z.z.: Für $p \neq 2$ gilt $N(\pi) = p \Leftrightarrow p \equiv 1\ (4)$.

- Sei $N(\pi) = p \Rightarrow a^2 + b^2 = p \overset{13.7.}{\Rightarrow} p \equiv 1\ (4)$.
- Sei $p \equiv 1\ (4)$ und es gelte nicht $N(\pi) = p$. Dann (nach 13.15) ist $N(\pi) = p^2$,
  $\overset{s.o.}{\Rightarrow}$ p Primel. in $\mathbb{Z}[i]$. Wegen $p \equiv 1\ (4)$ ex. (nach 13.7) ein $a \in \mathbb{Z}$ mit $a^2 \equiv -1\ (p)$,
  also $p \mid a^2 + 1 = (a+i)(a-i) \overset{p\ \text{Primel.}}{\Rightarrow} p \mid a+i$ oder $p \mid a-i$, ↯.
  $\ulcorner a \pm i = p(x+yi) \Rightarrow py = \pm 1 \Rightarrow p \mid \pm 1$ ↯ $\lrcorner$. □

13.19 Bsp.: 7 ist Primel. auch in $\mathbb{Z}[i]$, 5 dagegen nicht $\leadsto 5 = N(2+i) = (2+i)(2-i) = 2^2 + 1^2$.

13.20. Kor. (Satz von Euler/Fermat): Sei p prim. Ist $p \equiv 1\ (4)$, so ex. $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$.
Bis auf Vertauschung von x, y ist diese Darstellung eindeutig. (Ferner notwendig $(x,y) = 1$.)
Ist p umgekehrt als $p = x^2 + y^2$ darstellbar, so ist $p \equiv 1\ (4)$ oder $p = 2$.

Bew.: 1.) $p = N(\pi)$ nach Satz 13.18. Mit $\pi = x + yi$, $x, y \in \mathbb{Z}$, folgt $p = x^2 + y^2 = (\pm x)^2 + (\pm y)^2$, $x \neq 0 \neq y$.
2.) Zur Eindeutigkeit der Darstellung: Sei neben $p = x^2 + y^2$, OE $x, y \in \mathbb{N}$, noch
$p = u^2 + v^2$ mit $u, v \in \mathbb{N}$, also $p = N(u + vi) = N(\pi')$ mit $\pi' := u + vi$,
wo π' prim (Satz 13.18.),
mit $\pi \cdot \overline{\pi} = p = \pi' \cdot \overline{\pi'} \underset{\mathbb{Z}[i]\ \text{faktoriell}}{\Longrightarrow} \pi' \hat{=} \pi$ oder $\pi' \hat{=} \overline{\pi}$

$$\Rightarrow \exists \varepsilon \in \{1, -1, i, -i\}: u + vi = \varepsilon(x \pm yi) = \begin{cases} \pm x \pm yi \\ \mp y \pm xi \end{cases} \overset{x,y,u,v>0}{\Longrightarrow} \begin{cases} u = x, v = y \\ u = y, v = x \end{cases}$$ □

13.21. Satz: 1. (Satz von Euler/Fermat über die Summe von zwei Quadraten):
Genau dann ist $n \in \mathbb{N}$ Summe von 2 Quadraten in $\mathbb{Z}$, wenn
in der PFZ von n alle Primteiler p von n, für die $p \equiv 3\ (4)$ gilt, in gerader
Potenz auftreten. D.h.: $n = \prod_p p^{\alpha_p}$, $\alpha_p \in \mathbb{N}_0 \Rightarrow \forall p \in \mathbb{P}, p \equiv 3\ (4): \alpha_p \equiv 0\ (2)$.

2. Besitzt n eine primitive Darstellung als Summe von 2 Quadraten, d.h.
$n = a^2 + b^2$ mit teilerfremden $a, b \in \mathbb{Z}$, so folgt:
$\boxtimes$ n hat keine Primteiler $p \equiv 3\ (4)$, und es ist $4 \nmid n$.

3. Umgekehrt gilt: Gilt $\boxtimes$ und bezeichne s die Anzahl der ungeraden Primteiler von n,
so hat $n > 2$ genau 2^{s-1} primitive Darstellungen als Summe von 2 Quadraten
(wenn nur wesentlich verschiedene Darstellungen gewählt werden).

Bem.: n kann in 3. außerdem noch nicht-primitive Darstellungen haben, z.B. $50 = 7^2 + 1^2 = 5^2 + 5^2$.

Bew.: Zu 2.: Es gelte $n=a^2+b^2$ mit $(a,b)=1$. Sei $p\mid n$, Ann.: $p\equiv 3\ (4)$.
Dann ist p Primel. in $\mathbb{Z}[i]$. Mit $p\mid n=\alpha\bar\alpha$, wo $\alpha=a+bi\in\mathbb{Z}[i]$ ist, folgt $p\mid\alpha$ oder $p\mid\bar\alpha$, also $p\mid a\pm bi$, also $p\mid a$ und $p\mid b$ im ↯ zu $(a,b)=1$.
Ann.: $4\mid n=a^2+b^2 \overset{(a,b)=1}{\Longrightarrow} a\equiv b\equiv 1\ (2) \Rightarrow a^2\equiv b^2\equiv 1\ (4) \Rightarrow a^2+b^2\equiv 2\ (4)$, ↯.

Zu 1.: Sei $n=m^2n_0$ mit quadratfreiem n_0, d.h. $p\mid n_0\Rightarrow p^2\nmid n_0$.
Zu „$\Leftarrow$“: Sei $n_0=p_1p_2\cdots p_r$ mit $p_i\equiv 1\ (4)$, ev. bis auf $p_1=2$ (falls n_0 gerade).
Nach Satz 13.18 ist $p_i=N(\pi_i)$, also $n_0=N(\pi_1)N(\pi_2)\cdots N(\pi_r)=N(\underbrace{\pi_1\cdots\pi_r}_{=:\alpha=c+di})$,
also $n_0=c^2+d^2$, $n=m^2(c^2+d^2)=a^2+b^2$.
Zu „$\Rightarrow$“: Sei $n=a^2+b^2$ und $d:=(a,b)\neq 0$, sei $\hat a:=\frac{a}{d}$, $\hat b:=\frac{b}{d}$.
Dann ist $n=d^2(\hat a^2+\hat b^2)=d^2\hat m^2 n_0$, also $\hat m^2 n_0=\hat a^2+\hat b^2$, $(\hat a,\hat b)=1$.
Nach 2. gehen in $\hat m n_0$ nur $p=2$ oder $p\equiv 1\ (4)$ auf,
folglich gehen auch in n_0 nur solche p auf. Sei $w_p(k)$ der p-Exponent in $k\in\mathbb{N}$.
Für jedes $p\equiv 3\ (4)$ ist also $w_p(n)=2w_p(m)+w_p(n_0)=2w_p(m)$ gerade.

Zu 3.: Für beliebiges $n\in\mathbb{N}$ definiere

$$R(n):=\#\{(a,b)\in\mathbb{Z}^2;\ n=a^2+b^2,\ (a,b)=1\}$$

$$M_n:=\{\alpha\in\mathbb{Z}[i];\ n=N(\alpha),\ p\nmid\alpha \text{ für alle } p\},\quad \text{also } R(n)=\#M_n,$$

z.B. $R(1)=4$, $R(2)=4$. Weiter sei $r(n):=\#\{(a,b)\in\mathbb{Z}^2;\ n=a^2+b^2\}$.

Für $n\in\mathbb{N}$ sei jetzt Bedingung $\boxed{\times}$ erfüllt (und s sei die # der Primteiler $\neq 2$ von n).
Es gen. z.z.: $R(n)=2^{s+2}$ für alle $n\in\mathbb{N}$.
⌜Denn für $n>2$, d.h. $s\geq 1$, gilt: Ist $\alpha=a+bi\in M_n$, so sind die Elemente $\pm a\pm bi$, $\pm ai\pm b$ acht verschiedene Elemente von M_n; man beachte $a\neq b$ und $a,b\neq 0$.
Somit ist $\frac{R(n)}{8}=2^{s-1}$.⌟

Bew. durch Ind. nach s: Für $s=0$ ist dies richtig, da $R(1)=4$, $R(2)=4$.
Für $s>0$ sei $p\mid n$, $p\neq 2$. Wegen $\boxed{\times}$ ist $p=\pi\bar\pi$, $\pi\not\sim\bar\pi$ (π fest gewählt), $\alpha\in M_n$. Mit $p\mid n=N(\alpha)=\alpha\bar\alpha$ folgt $\pi\mid\alpha$ oder $\pi\mid\bar\alpha$,
d.h. $\pi\mid\alpha$ oder $\bar\pi\mid\alpha$, d.h. $\frac{\alpha}{\pi}$ oder $\frac{\alpha}{\bar\pi}$ in $\mathbb{Z}[i]$.
Dann ist $N(\frac{\alpha}{\pi})=\frac{N(\alpha)}{N(\pi)}=\frac{n}{p}$ oder $N(\frac{\alpha}{\bar\pi})=\frac{n}{p}$, also $\frac{\alpha}{\pi}\in M_{n/p}$ oder $\frac{\alpha}{\bar\pi}\in M_{n/p}$.
Es folgt $M_n=\pi M_{n/p}\,\dot\cup\,\bar\pi M_{n/p}$ als disjunkte Vereinigung ⌜sonst $\pi\mid\alpha \wedge \bar\pi\mid\alpha \Rightarrow p=\pi\bar\pi\mid\alpha$, ↯ zu $\alpha\in M_n$⌟
Somit $\#M_n=2\,\#M_{n/p}$, d.h. $R(n)\overset{IV}{=}2\cdot 2^{(s-1)+2}=2^{s+2}$. □

Es folgt die Umkehrung des Korollars 13.20 zu Satz 13.18:

13.22. Kor.: Es sei $n \in \mathbb{N}_{>1}$ ungerade. Besitzt n im wesentlichen nur eine einzige Darstellung als Summe von 2 Quadraten, und ist diese Darstellung primitiv, so ist n eine Primzahl.

Bew.: Nach Satz 13.21.3 hat n nur einen einzigen Primteiler p, d.h. $n = p^k$, und es ist $p \equiv 1\ (4)$. Wäre $k \geq 2$, so hätte man $n = p^2 \cdot p^{k-2} \underset{\text{Satz 13.21.}}{=} p^2(a^2+b^2) = (pa)^2 + (pb)^2$, ↯ zur Vor. □

13.23. Bem.: • $45 = 6^2 + 3^2$ ist die einzige Darstellung von 45 als Summe von 2 Quadraten. Doch diese ist nicht primitiv.

• Im übrigen ist die Vor. "ungerade" wesentlich: Für $n = 10$ ist $n = 3^2 + 1^2$ die im wesentlichen einzige Darstellung als Summe von 2 Quadraten, und diese ist auch primitiv, aber $10 \notin \mathbb{P}$.

Der Fall der Summe dreier Quadrate ist wesentlich schwieriger und kann hier nur knapp diskutiert werden. Der Hauptgrund ist, dass keine Multiplikationsformel der Art

$$(x_1^2+y_1^2+z_1^2)\cdot(x_2^2+y_2^2+z_2^2) = L_1^2(x_1,\dots,z_2) + L_2^2(x_1,\dots,z_2) + L_3^2(x_1,\dots,z_2)$$

existiert: A. Hurwitz zeigte, dass es solche Formeln nur für 1, 2, 4 oder 8 Summanden gibt.

Für Summen von 3 Quadraten kann folgender Satz gezeigt werden:

13.24. Satz (von Legendre über Summen von 3 Quadraten):

Für alle $n \in \mathbb{N}$ sind äquivalent: 1. Es gibt $x, y, z \in \mathbb{N}_0$ mit $n = x^2 + y^2 + z^2$,
2. $n \notin \{4^a(8b+7);\ a, b \in \mathbb{N}_0\}$.

Bew.: Nur von 1. ⇒ 2., d.h. ¬2. ⇒ ¬1. Sei dazu $n = 4^a(8b+7)$ mit $a, b \in \mathbb{N}_0$,
Ann.: $n = x^2 + y^2 + z^2$. Wir setzen die modulare Brille mod 8 auf: Da $x^2 \equiv 0, 1$ oder $4\ (8)$, ist $x^2+y^2+z^2 \equiv 0, 1, 2, 3, 4, 5$ oder $6\ (8)$, insb. ist $x^2+y^2+z^2$ niemals $\equiv 7\ (8)$. Mit $\frac{n}{4^a} = 8b+7$ kann also $\frac{n}{4^a}$ nicht Summe 3er Quadrate sein, wir haben aber $\frac{n}{4^a} = \left(\frac{x}{2^a}\right)^2 + \left(\frac{y}{2^a}\right)^2 + \left(\frac{z}{2^a}\right)^2$, ↯. □

13.25. Bem.: • Die Richtung 2. ⇒ 1. erfordert einiges aus der Theorie der ternärquadratischen Formen $Q(x_1, x_2, x_3) = \sum_{j,k=1}^{3} a_{jk} x_j x_k$ mit $a_{jk} \in \mathbb{Z}$ und dem Satz von Dirichlet (aus der Vorlesung "Analytische Zahlentheorie"), dass in jeder reduzierten Restklasse $a + q\mathbb{Z}$ mit $(a, q) = 1$, $a \in \mathbb{Z}$, $q \in \mathbb{N}$, unendlich viele Primzahlen liegen.

• Legendres Beweis 2. ⇒ 1. stellte sich als falsch heraus. Der erste korrekte Beweis stammt von Gauß.

Der Fall der Summen von 4 (oder mehr) Quadraten ist hingegen einfach, denn es gilt:

13.26. Satz (Euler-Identität für die Summe von 4 Quadraten): Für $a,b,c,d, w,x,y,z \in \mathbb{R}$ gilt

$$(a^2+b^2+c^2+d^2)\cdot(x^2+y^2+z^2+w^2)$$
$$=(ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+(az+cx+dy-bw)^2+(aw+dx+bz-cy)^2.$$

Bew.: z.B. durch Ausmultiplizieren und Vergleichen beider Seiten. Anders so: Wir fassen jede Seite als Polynom in x auf. Der Koeff. vor x^2 beider Seiten ist $a^2+b^2+c^2+d^2$.
Der Koeff. vor x ist $=0$ auf der l.S., und hebt sich weg auf der r.S.
Es bleibt der "konstante" Term, der sich durch Setzen von $x=0$ ergibt, und die Wiederholung des Arguments für y, dann für z, und zuletzt für w, führt zur Beh. $\square$

Dies führt zum folgenden Satz, dessen Aussage möglicherweise schon in der Antike bekannt war:

13.27. Satz (von Lagrange über die Summe von 4 Quadraten, 4-Quadrate-Satz):
Jedes $n \in \mathbb{N}_0$ ist Summe von 4 Quadraten $\in \mathbb{N}_0$.

Bew.: Laut Satz 13.26 gen. z.z.: Jedes $p \in \mathbb{P}$ ist Summe von 4 Quadraten. Klar: $2=1^2+1^2+0^2+0^2$.
Sei also $p>2$. 1.) Ist $2|m$ und m Summe von 4 Quadraten, so ist $\frac{m}{2}$ Summe von 4 Quadraten.
⌜ $m=a^2+b^2+c^2+d^2$ gerade. Eine Summe von ~~geraden~~ ungeraden ungeraden Quadraten wäre ungerade, daher haben zwei Paare der Summanden dieselbe Parität, etwa a,b und c,d.
Somit ist $\frac{m}{2}=\left(\frac{a+b}{2}\right)^2+\left(\frac{a-b}{2}\right)^2+\left(\frac{c+d}{2}\right)^2+\left(\frac{c-d}{2}\right)^2$ auch Summe von 4 Quadraten. ⌟

2.) Ist $p>2$, so ex. $a,b,c,d \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $0<a^2+b^2+c^2+d^2=mp<\frac{p^2}{2}$.
⌜ Die $\frac{p+1}{2}$ vielen Quadrate $0^2, 1^2, \dots, \left(\frac{p-1}{2}\right)^2$ sind p.w. inkongruent mod p.
Somit liegen die $\frac{p+1}{2}$ vielen u^2 mit $0 \le u \le \frac{p-1}{2}$ in verschiedenen Restklassen mod p, und die $\frac{p+1}{2}$ vielen $-v^2-1$ mit $0 \le v \le \frac{p-1}{2}$ in verschiedenen Restklassen mod p.
Da $\frac{p+1}{2}+\frac{p+1}{2}=p+1>p$, ex. mind. eine Restklasse mod p in beiden Listen, d.h.
ex. u,v mit $u^2 \equiv -v^2-1\ (p)$. Diese können nicht beide 0 sein, und $0<u^2+v^2+1 \le \frac{p^2-2p+3}{2}<\frac{p^2}{2}$. ⌟

3.) Nach 2) ex. ein $m \in \mathbb{N}$ mit $m<p$, so dass $a^2+b^2+c^2+d^2=mp$, OE sei m minimal so.
Nach 1.) ist $2 \nmid m$. Für $m=1$ fertig, sei also $m>1$. Würde m jede der Zahlen a,b,c,d teilen, so wäre $m|p$ im Wz zu $m<p$. Wähle x,y,z,w mit $x \equiv a\ (m)$, $y \equiv -b\ (m)$, $z \equiv -c\ (m)$, $w \equiv -d\ (m)$ und $|x|,|y|,|z|,|w|<\frac{m-1}{2}$, und nicht alle der x,y,z,w können $=0$ sein.

Weiter ist $x^2+y^2+z^2+w^2 \equiv 0\ (m)$, also $0 < x^2+y^2+z^2+w^2 = mn \le 4\left(\frac{m-1}{2}\right)^2 = (m-1)^2$.
Also ist $0<n<m$. Nun ist $ax-by-cz-dw \equiv a^2+b^2+c^2+d^2 \equiv 0\ (m)$,

$$ay+bx+cw-dz \equiv -ab+ab-cd+dc \equiv 0\ (m),$$
$$az+cx+dy-bw \equiv -ac+ac-db+db \equiv 0\ (m),$$
$$aw+dx+bz-cy \equiv -ad+ad-bc+bc \equiv 0\ (m).$$

Nach der Euler-Identität 13.26 ist m^2np die Summe von 4 Quadraten, und jedes der Quadrate ist durch m^2 teilbar. Also ist np Summe von 4 Quadraten, was der Minimalität von m widerspricht. □

13.28 Bem.: • Der 4-Quadrate-Satz wurde hier elementar bewiesen mit der Grundidee aus 13.7, einen (Dirichletschen) Schubfachschluss zu verwenden. Diese Idee geht auf A. Thue zurück. Man kann den Satz auch mit der Normabbildung auf dem ganzzahligen Quaternionenring $\mathbb{Z}[i,j,k]$ beweisen, ähnlich wie der 2-Quadrate-Satz mit $\mathbb{Z}[i]$, wie dies oben im Beweis für Satz 13.18 / Kor. 13.20 durchgeführt wurde.

• Der Thue-Ansatz funktioniert auch für Zahlen der Form x^2+2y^2 oder x^2+3y^2, denn hier gilt $(x^2+\lambda y^2)\cdot(X^2+\lambda Y^2) = (xX-\lambda yY)^2 + \lambda(xY+yX)^2$ für $\lambda=2,3$.
Dieses Phänomen tritt bei binärquadratischen Formen $ax^2+bxy+cy^2$ i.a. nicht auf; die Frage führt auf das Klassenzahlproblem quadratischer Zahlkörper (s. "algebraische ZT").

• Ganzzahlige Lösungen der Gleichung $d^2 = a^2+b^2+c^2$ heißen pythagoräische Quadrupel. Ähnlich wie bei den indischen Formeln können pyth. Quadrupel mit Parameter-Quadrupeln erzeugt werden. Die damit erzeugten pyth. Quadrupel müssen nicht notwendig primitiv sein; eine Verschärfung der Parameterbedingungen erzeugt dann nur primitive pyth. Quadrupel.