Der 3-Quadrate-Satz

F1: Ist n eine natürliche Zahl der Gestalt

(*) $\qquad n = 4^j(8k+7)$ mit $j,k \in \mathbb{N}_0$,

so ist n keine Summe von 3 Quadraten in $\mathbb{Z}$.

Bew. Quadrate in $\mathbb{Z}/8$: $\{\bar{0}, \bar{1}, \bar{4}\}$, $\Longrightarrow$

$$x^2+y^2+z^2 \not\equiv 7 \bmod 8 \qquad \text{[für alle } x,y,z \in \mathbb{Z}\text{]}$$

Also kein n der Gestalt $n = 8k+7$ ist Summe von 3 Quadraten in $\mathbb{Z}$.
Jetzt Induktion nach j. $j=0$ ✓ Sei $j \geq 1$.
Dann $n = 4m$, und nach I.A. ist m keine Summe von 3 Qu'n.

Ann. $\qquad 4m = n = x^2+y^2+z^2$, $\Longrightarrow$
$x^2+y^2+z^2 \equiv 0 \bmod 4$, $\Longrightarrow$ x,y,z alle gerade, $\Longrightarrow$
$m = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$ W!

3-Quadrate-Satz (Legendre, Gauß): Jede natürliche Zahl n, die nicht von der in F1 genannten Gestalt (*) ist, ist Summe von 3 Quadraten in $\mathbb{Z}$, d.h. n hat eine Darstellung der Gestalt

(1) $\qquad n = x_1^2 + x_2^2 + x_3^2 \qquad$ mit $x_i \in \mathbb{Z}$.

Ist zudem n nicht durch 4 teilbar (also $n \equiv 1,2,3,5$ oder $6 \bmod 8$), so existiert stets auch eine primitive Darstellung der Gestalt (1), d.h. eine mit

(2) $\qquad \mathrm{ggT}(x_1, x_2, x_3) = 1$ $\qquad \square$

Der 3-Quadrate-Satz liegt anscheinend viel tiefer als der 4-Quadrate-Satz, der aus dem 3-Quadrate-Satz unmittelbar folgt: Sei $n \in \mathbb{N}$ bel.

Wir können annehmen, daß n die Gestalt $n = 4^s m$ mit $m \equiv 7 \bmod 8$ hat (denn andernfalls ist n ja schon Summe von 3 Quadraten in $\mathbb{Z}$). Dann ist $m - 1 \equiv 6 \bmod 8$, also ist $m-1$ Summe von 3 Quadraten und somit m Summe von 4 Quadraten. Aber dann ist auch $n = 4^s m$ Summe von 4 Quadraten. – allerdings ohne den Zusatz (2) –

Der 3-Quadratesatz folgt aus einem allgemeinen Prinzip der "Algebraischen Zahlentheorie" (→ Lokal-Global-Prinzip von Hasse). Was eine möglichst direkte Begründung des 3-Quadratesatzes (ohne den Zusatz (2)) angeht, so sind derzeit kursierende Beweise insofern "nicht elementar", als sie (anders als Gauß) den nachstehenden 'Satz von Dirichlet' benützen, dessen Beweis essentiell auf Methoden der komplexen Analysis beruht.

'Satz von Dirichlet' (1798 von Legendre formuliert, aber erst 1837 von Dirichlet bewiesen):
Für bel. $m > 1$ aus $\mathbb{N}$ und jedes zu m prime a aus $\mathbb{Z}$ gibt es unendlich viele Primzahlen p mit

$$p \equiv a \bmod m .$$

Weitere Bemerkungen:

1) Auf den Zusatz (2) im 3-Quadratesatz legte schon Legendre Wert. Man beachte: Während z.B. $45 = 6^2 + 3^2$ i.w. die einzige Darstellung von 45 als Summe von 2 Quadraten ist (und diese nicht primitiv ist), hat 45 neben $45 = 6^2 + 3^2 + 0^2$ auch die primitive Darstellung $45 = 5^2 + 4^2 + 2^2$ als Summe von 3 Quadraten.

2) Gauß hat auch über die Anzahl $r_3(n)$ der Darstellungen $n = x_1^2 + x_2^2 + x_3^2$ bzw. die Anzahl $R_3(n)$ der entsprechenden primitiven Darstellungen interessante Aussagen gemacht.

3) Unabhängig von Gauß erhält man durch einfaches Abzählen der (x_1, x_2, x_3, x_4) mit $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ für $x_4 = 0$, $x_4 = 1$, $x_4 = 2, \ldots$ die 'banale Formel':

$$(3) \qquad r_4(n) = r_3(n) + 2r_3(n-1^2) + 2r_3(n-2^2) + 2r_3(n-3^2) + \cdots$$

Mit der Formel von Jacobi für $r_4(n)$ – vgl. S. 155 – liefert (3) eine gute Rekursionsformel für die $r_3(n)$. Aber dieser Rekursionsformel läßt sich nicht entnehmen – jedenfalls nicht auf einfache Weise – daß $r_3(n)$ stets $\neq 0$ ausfällt, wenn n nicht von der Gestalt $n = 4^j(8k+7)$ ist.

4) Was nun den Gaußschen Beweis für den 3-Quadrate-Satz angeht, so will ich versuchen, davon eine gewisse Idee zu geben, in der Extra-Vorlesung am 3. Febr. um 12 Uhr.

5) Gegeben eine natürliche Zahl $k > 1$. Für jedes $n \in \mathbb{N}$ sei $r_k(n)$ die Anzahl aller k-Tupel $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ mit $n = x_1^2 + \ldots + x_k^2$; die Anzahl der entsprechenden primitiven k-Tupel, d.h. solcher mit $ggT(x_1, \ldots, x_k) = 1$, bezeichnen wir mit $R_k(n)$. Offenbar gilt

$$(4) \qquad r_k(n) = \sum_{d^2 \mid n} R_k\left(\frac{n}{d^2}\right)$$

Im Fall $k = 4$ ist $r_k(n)$ bekannt (Formel von Jacobi, S. 155); die Relation (4) liefert dann eine Rekursionsformel für $R_4(n)$. Ob es auch eine 'geschlossene Formel' für $R_4(n)$ gibt, weiß ich nicht. Es sei aber bemerkt, daß $R_4(n)$ genau dann von 0 verschieden ist, wenn $n \not\equiv 0 \bmod 8$ ist:

Zusatz zum 4-Quadratesatz: Unter den ganzzahligen Darstellungen

$$(5) \qquad n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

gibt es genau dann eine primitive, d.h. eine mit

$$(6) \qquad \operatorname{ggT}(x_1, x_2, x_3, x_4) = 1 ,$$

wenn $n \not\equiv 0 \bmod 8$ ist.

Beweis: 1) O.E. sei $n > 1$. Hat $n-1$ nicht die Gestalt $4^j(8k+7)$, so ist $n-1$ Summe dreier Quadrate in $\mathbb{Z}$, also gilt (5) mit $x_1 = 1$, und dafür ist (6) erfüllt.

2) Sei also $n = 1 + 4^j(8k+7)$. Für $j \geq 1$ ist $n \equiv 1 \bmod 4$, und nach dem 3-Quadratesatz (S. 161) gibt es eine Darstellung $n = x_1^2 + x_2^2 + x_3^2$ mit $\operatorname{ggT}(x_1, x_2, x_3)$. Also gilt (5) mit $x_4 = 0$, und (6) ist erfüllt.

3) In (2) verbleibt der Fall $j = 1$, d.h. der Fall $n \equiv 0 \bmod 8$. In einer beliebigen Darstellung der Gestalt (5) müssen dann alle x_i gerade sein (andernfalls die rechte Seite $\equiv 1, 2, 3$ oder $4 \bmod 8$ ausfallen würde), also ist (6) für $n \equiv 0 \bmod 8$ nicht erfüllbar.