§9 Der 4-Quadrate-Satz

Satz von Lagrange: Jede natürliche Zahl ist Summe von vier Quadraten, d.h. jedes $n \in \mathbb{N}$ hat eine Darstellung der Gestalt

(1) $$n = x_1^2 + x_2^2 + x_3^2 + x_4^2 \quad \text{mit } x_i \in \mathbb{Z}$$

Def. Für jedes $n \in \mathbb{N}$ sei $r_4(n)$ die Anzahl der Quadrupel $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ mit (1).

Der Satz von Lagrange folgt aus der

Formel von Jacobi: Es gilt

(2) $$r_4(n) = \begin{cases} 8\sigma(n) & \text{falls } n \text{ ungerade} \\ 3 \cdot 8\sigma(\ddot{u}) & \text{falls } n \text{ gerade,} \end{cases}$$

wobei $\ddot{u}$ den ungeraden Teil von n bezeichnet, also $\ddot{u} = n/2^{w_2(n)}$.

Bem. 1: Den Satz von Lagrange kann man auch ohne Rekurs auf die Formel von Jacobi beweisen (z.B. wie in Vorlesung SS 13, §9, siehe Anhang A1–A5 in diesem Skript).

Bem. 2: Jacobi hat seine Formel (2) in Zusammenhang mit ziemlich tiefen Methoden der Analysis entdeckt.

Beweis der Formel von Jacobi: Vorbereitend stellen wir zuerst einige leicht ablesbare Eigenschaften der Funktion $r(n) := r_4(n)$ zusammen. Zunächst ist für bel. n die Relation

(3) $$r(4n) = r(2n)$$

erfüllt: In jeder Darstellung $4n = x_1^2+x_2^2+x_3^2+x_4^2$ sind x_1, x_2, x_3, x_4 entweder alle gerade oder alle sind ungerade. Oder sind

$$(4)\qquad y_1 := \frac{x_1+x_2}{2},\ y_2 := \frac{x_1-x_2}{2},\ y_3 := \frac{x_3+x_4}{2},\ y_4 := \frac{x_3-x_4}{2}$$

sämtlich in $\mathbb{Z}$, und sie erfüllen $y_1^2+y_2^2+y_3^2+y_4^2 = 2n$. Umgekehrt: Ausgehend von einer Darstellung $2n = y_1^2+y_2^2+y_3^2+y_4^2$ mit $y_i \in \mathbb{Z}$, gibt es offenbar eindeutig bestimmte x_1, x_2, x_3, x_4 aus $\mathbb{Z}$ mit (4); diese erfüllen $x_1^2+x_2^2+x_3^2+x_4^2 = 4n$. Es folgt (3). –

Weiter behaupten wir, daß jedes ungerade $n = \tilde{u}$ die Relation

$$(5)\qquad r(2\tilde{u}) = 3\,r(\tilde{u})$$

erfüllt: In jeder Darstellung $2\tilde{u} = x_1^2+x_2^2+x_3^2+x_4^2$ sind genau zwei der x_i gerade, und die restlichen beiden ungerade. Die Anzahl der entspr. (x_1, x_2, x_3, x_4), bei denen speziell x_1, x_2 gerade (und x_3, x_4 ungerade sind, ist offenbar $\frac{1}{6}r_4(2\tilde{u})$. Die genannten Quadrupel (x_1, x_2, x_3, x_4) entsprechen dabei gemäß (4) genau den Quadrupeln (y_1, y_2, y_3, y_4) mit

$$y_1^2+y_2^2+y_3^2+y_4^2 = \tilde{u},$$

für die y_1+y_2 gerade und y_3+y_4 ungerade sind, d. h. $y_1 \equiv y_2 \bmod 2$ und $y_3 \not\equiv y_4 \bmod 2$. Deren Anzahl ist $\frac{1}{2}r(\tilde{u})$, wie man sich unschwer klar macht, cf. A.*) Es folgt $\frac{1}{6}r(2\tilde{u}) = \frac{1}{2}r(\tilde{u})$, also (5). –

---

*) Für jedes $y = (y_1, y_2, y_3, y_4)$, welches $\tilde{u}$ darstellt, ist auch $y' = (y_3, y_4, y_1, y_2)$ ein solches Quadrupel; und weil $\tilde{u}$ ungerade hat man $y_1 \equiv y_2 \bmod 2 \Leftrightarrow y_3 \not\equiv y_4 \bmod 2$. Dabei hat ein Darstellungstupel y von n genau dann die beiden obengenannten Eigenschaften, wenn y' sie nicht erfüllt. Wegen $(y')' = y$ folgt nun die Beh.

Für ungerades $\check{u}$ sind in jeder Darstellung

(6) $\qquad 4\check{u} = x_1^2 + x_2^2 + x_3^2 + x_4^2$

entweder alle x_i gerade oder alle x_i ungerade. Sind alle x_i gerade und setzt man $y_i = \frac{x_i}{2}$, so erhält man $y_1^2 + y_2^2 + y_3^2 + y_4^2 = u$ mit $y_i \in \mathbb{Z}$. Umgekehrt liefert jede solche Darstellung vermöge $x_i = 2y_i$ eine Darstellung (6), bei der alle x_i gerade sind. Insgesamt gilt daher

(7) $\qquad r(4\check{u}) = r(\check{u}) + R(\check{u})$,

wenn $R(\check{u})$ die Anzahl der Darstellungen (6) bezeichnet, bei denen alle x_i ungerade sind. Zunächst kommt es nun auf die Bestimmung von $R(u)$ an. Denn nach (5) und (3) ist ja

$3r(\check{u}) = r(2\check{u}) = r(4\check{u}) = r(\check{u}) + R(\check{u})$, also

$$r(\check{u}) = \frac{1}{2} R(\check{u})$$

Zum Beweis der Formel (2) von Jacobi ist also jedenfalls

(8) $\qquad R(\check{u}) = 16\,\sigma(\check{u})$

zu zeigen. Ist das einmal erledigt, so ergibt (5) auch $r(2\check{u}) = 3r(\check{u}) = 3 \cdot 8\,\sigma(u)$. Zum vollständigen Beweis von (2) ist also noch $n = 2^k\check{u}$ für $k \geq 2$ zu betrachten. Mit (3) ergibt Induktion $r(2^k\check{u}) = r(2^{k-1}\check{u}) = 3 \cdot 8\,\sigma(\check{u})$. Alles läuft also auf die Beh. (8) hinaus, also die Anzahl der Darstellungen

(9) $\qquad 4\check{u} = x_1^2 + x_2^2 + x_3^2 + x_4^2$ mit ungeraden $x_i \in \mathbb{Z}$.

Dabei sind $x_1^2 + x_2^2$ und $x_3^2 + x_4^2$ gerade, aber $\not\equiv 0 \bmod 4$, also

$$x_1^2 + x_2^2 = 2s \text{ und } x_3^2 + x_4^2 = 2t \text{ mit } s, t \in \mathbb{N}_{\text{ung.}} \uparrow,$$

und mit $r_2(m) = 4 \sum_{d \mid m} \chi(d)$ – vgl. Satz 2, §8 (S. 142) – gilt also

$$R(\tilde{u}) = \sum_{\substack{s+t=2\tilde{u} \\ \text{ungerade}}} r_2(2s)\, r_2(2t) = 16 \sum_{\substack{s+t=2\tilde{u} \\ \text{ungerade}}} \Big(\sum_{a \mid s}{}' \chi(a) \sum_{b \mid t}{}' \chi(b) \Big) = 16 \sum_{\substack{s+t=2\tilde{u} \\ \text{ungerade}}} \sum_{a \mid s,\, b \mid t}{}' \chi(ab)$$

wobei wir $\chi(x) = 0$ für $2 \mid x$ benutzt haben. Wir erhalten

$$R(u) = 16 \sum_{ac+bd=2\tilde{u}}{}' \chi(ab)$$

mit Summation über alle $(a,b,c,d) \in \mathbb{N}^4_{\text{ung.}}$ mit $ac+bd = 2\tilde{u}$.

Betrachten wir zuerst die Quadrupel mit $a = b$, so liefern diese den Beitrag

$$16 \sum_{a(c+d)=2\tilde{u}} \chi(a)^2 = 16 \sum_{a \mid u}{}' \sum_{\substack{c,d \text{ ungerade} \\ c+d = 2\frac{u}{a}}} 1 = 16 \sum_{a \mid u}{}' \frac{u}{a} = 16\, \sigma(u),$$

so daß zu zeigen ist, daß die Summe über die Quadrupel mit $a \neq b$ verschwindet. Aus Symmetriegründen genügt es zu zeigen, daß

$$(10) \qquad \sum_{\substack{ac+bd=2\tilde{u} \\ a>b}}{}' \chi(ab) = 0$$

gilt, wobei über alle Quadrupel $(a,b,c,d) \in \mathbb{N}^4_{\text{ung}}$ mit $ab+cd = 2\tilde{u}$ und $a > b$ summiert wird. Dazu werden wir zeigen, daß man die genannten Quadrupel so in Paare $(a,b,c,d), (a',b',c',d')$ einteilen kann, daß jeweils $\chi(ab) + \chi(a'b') = 0$ gilt. Dabei sei (a',b',c',d') aus (a,b,c,d) mittels einer 4×4-Matrix M der Gestalt

$$M = \begin{pmatrix} 0 & X \\ X^{-1} & 0 \end{pmatrix} \quad \text{mit einem } X \in SL_2(\mathbb{Z})$$

der Gestalt $X = \begin{pmatrix} k+2 & k+1 \\ k+1 & k \end{pmatrix}$ mit $k \in \mathbb{N}_0$ hervor. Es ist also

$$(11)\qquad \begin{pmatrix} a' \\ b' \\ c' \\ d' \end{pmatrix} = \begin{pmatrix} 0 & 0 & k+2 & k+1 \\ 0 & 0 & k+1 & k \\ -k & k+1 & 0 & 0 \\ k+1 & -(k+2) & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} (k+2)c + (k+1)d \\ (k+1)c + kd \\ -ka + (k+1)b \\ (k+1)a - (k+2)b \end{pmatrix},$$

wobei k noch geeignet zu verfügen ist. Jedenfalls sind die a', b', c', d' alle ganzzahlig und alle ungerade; ferner gilt $a' > b'$. Mit $2\ddot{u} = ac + bd = (a,b)\begin{pmatrix} c \\ d \end{pmatrix} = {}^t\!\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix}$ ist auch ${}^t\!\begin{pmatrix} a' \\ b' \end{pmatrix}\begin{pmatrix} c' \\ d' \end{pmatrix} = {}^t\!\left(X\begin{pmatrix} c \\ d \end{pmatrix}\right) X^{-1}\begin{pmatrix} a \\ b \end{pmatrix} = (c,d)\,{}^t\!X\,X^{-1}\begin{pmatrix} a \\ b \end{pmatrix} = (c,d)\begin{pmatrix} a \\ b \end{pmatrix} = 2\ddot{u}$. Nach (11) sind $a', b' > 0$, und es bleibt also, auch $c' > 0$, $d' > 0$ sicherzustellen, also

$$-ka + (k+1)b > 0 \text{ und } (k+1)a - (k+2)b > 0, \text{ d. h.}$$
$$b - k(a-b) > 0 \text{ und } (k+1)(a-b) - b > 0, \text{ d. h.}$$

$$(12)\qquad \frac{b}{a-b} - 1 < k < \frac{b}{a-b}$$

Da $\frac{b}{a-b}$ nicht ganzzahlig ist (denn b ist ungerade, aber $a-b$ gerade), besagt (12) nichts anderes als

$$(13)\qquad k = \left[\frac{b}{a-b}\right]$$

Für dieses – und nur für dieses k ist also (a', b', c', d') ein Quadrupel der verlangten Art. Wobei k allerdings von (a,b,c,d) abhängt. Da für die Matrix $M = M_k$ wegen $MM = \begin{pmatrix} 0 & X \\ X^{-1} & 0 \end{pmatrix}\begin{pmatrix} 0 & X \\ X^{-1} & 0 \end{pmatrix} = \begin{pmatrix} E_2 & 0 \\ 0 & E_2 \end{pmatrix} = E_4$ aber $M^{-1} = M$ gilt und ferner

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

ist die entspr. Matrix M', die (a', b', c', d') in (a,b,c,d) überführt, identisch mit M. Oder kann ein weiteres, von (a,b,c,d) und (a',b',c',d') verschiedenes Quadrupel (e,f,g,h) nicht auf ein Quadrupel (e',f',g',h') führen, welches wieder mit (a,b,c,d) noch (a',b',c',d') übereinstimmt. – Jetzt bleibt aber noch $\chi(a'b') = -\chi(ab)$ zu zeigen. Modulo 4 ist

$1-a-b+ab=(1-a)(1-b)\equiv 0$ u. entspr. $1-a'-b'+a'b'\equiv 0$,

also

$$ab+a'b' \equiv a+b-1+a'+b'-1 \overset{(11)}{\equiv} a+b+(k+2)c+(k+1)d+(k+1)c+kd-2$$

$$\equiv a+b+2kc+2c+2kd+d+c-2$$

$$\equiv a+b+c+d+2k(c+d)+2(c-1)$$

$$\equiv a+b+c+d \bmod 4 \quad \text{(denn } c+d \text{ und } c-1 \text{ sind gerade)}$$

s.o.

$$\equiv ac-1+bd-1 = 2u-2 = 2(u-1)\equiv 0 \bmod 4,$$

denn u ist ungerade. Es ist also

$$ab \equiv -a'b' \bmod 4$$

und daher

$$\chi(ab)=\chi(-a'b')=\chi(-1)\chi(a'b')=-\chi(a'b'). \qquad \square$$

Bem. $1=1^2$, $2=1^2+1^2$, $3=1^2+1^2+1^2$, $4=2^2$, $5=2^2+1^2$, $6=2^2+1^2+1^2$

x $7=2^2+1^2+1^2+1^2$ | $8=2^2+2^2$, $9=3^2$, $10=3^2+1^2$, $11=3^2+1^2+1^2$, $12=2^2+2^2+2^2$, $13=3^2+2^2$

o $14=3^2+2^2+1^2$

x $15=3^2+2^2+1^2+1^2$ | $16=$ ....

x $23=3^2+3^2+2^2+1^2$ | $24=$ ....

x $28=5^2+1^2+1^2+1^2$ | $29=$

o $30=5^2+2^2+1^2$

x $31=5^2+2^2+1^2+1^2$

Welche n lassen sich als 3 Quadraten in $\mathbb{Z}$ (d.h. $n=x_1^2+x_2^2+x_3^2$ mit $x_i\in\mathbb{Z}$, zulässig $x_i=0$) ?