Anhang A1–A5

§9 Der 4-Quadrate-Satz

F1: Sei n eine natürliche Zahl mit $4 \nmid n$. Zu jedem $a \in \mathbb{Z}$ mit $(a,n)=1$ gibt es $r,s \in \mathbb{Z}$ mit

$$a \equiv r^2 + s^2 \bmod n$$

("2-Quadrate-Satz mod n") [1]

Bew. 1) Genügt der Fall $n = p^\nu$ ($p \neq 2$, $\nu \geq 1$) bzw. $n=2$. (trivial)
(Chinesischer Restsatz, üA).

2) Genügt der Fall $n = p$ ($p \neq 2$):

$a \equiv r^2 + s^2 \bmod p$, o.E. $(r,p)=1$ $\Rightarrow$ $a - s^2 \equiv r^2 \bmod p$, $(a-s^2, p) = 1$ $\Rightarrow$

$a - s^2$ quadr. Rest mod p, $\overset{\S 6}{\Longrightarrow}$ $a-s^2$ quadr. Rest mod p^ν,

$\Rightarrow \exists\, r' \in \mathbb{Z}$ mit $a - s^2 \equiv r'^2 \bmod p^\nu$. ✓

3) Sei also $n = p$ ($p \neq 2$). Ist a quadr. Rest mod p, so fertig.
Sei also a quadr. Nichtrest mod p. Betrachte

$$a - s^2 \quad \text{für alle primen Reste } s \bmod p$$

Das liefert $\frac{p-1}{2}$ prime Reste mod p, und alle diese sind $\not\equiv a \bmod p$. Da a QNR ist (und es gibt $\frac{p-1}{2}$ QNR'e gibt), muß ein $a - s^2$ QR sein, d.h. es ex. $r \in \mathbb{Z}$ mit

$$a - s^2 \equiv r^2 \bmod p. \qquad \Rightarrow \text{Beh.}$$

---

[1] die Voraus. $4 \nmid n$ ist notwendig, da $r^2 + s^2 \not\equiv -1 \bmod 4$ für alle r, s

1736-1813

Satz 1 (Lagrange, Fermat): Jede natürliche Zahl n ist Summe von vier Quadraten:

$$n = a^2 + b^2 + c^2 + d^2 \quad \text{mit } a,b,c,d \in \mathbb{N} \cup \{0\}.$$

Beweis: ① o.E. n quadratfrei ∨ o.E. n ungerade

⌜Denn: Sei $2 \mid n$. Dann $n = 2m$, $2 \nmid m$. Nach Vor.
$n = 2(a^2+b^2+c^2+d^2) = (a+b)^2 + (a-b)^2 + (c+d)^2 + (c-d)^2$ ⌟

Nach F1 gibt es $r,s \in \mathbb{Z}$ mit

$$(1) \qquad r^2 + s^2 \equiv -1 \bmod n$$

Vorbetrachtung: Wir müssen wenigstens

$$a^2 + b^2 + c^2 + d^2 \overset{z}{\equiv} 0 \bmod n$$

(nicht-trivial) erfüllen, also $c^2 + d^2 \equiv -(a^2+b^2) \bmod n$, und somit

$$(*) \qquad c^2 + d^2 \equiv (r^2+s^2)(a^2+b^2) \bmod n$$

Daher betrachte die Menge M aller $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in \mathbb{Z}^4 \subseteq \mathbb{R}^4$ mit

$$(2) \qquad \begin{pmatrix} c \\ d \end{pmatrix} \equiv \begin{pmatrix} r & -s \\ s & r \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \bmod n, \quad \text{d.h.}$$

$$(2') \qquad \begin{aligned} c &\equiv ra - sb \bmod n \\ d &\equiv sa + rb \bmod n \end{aligned}$$

M ist Untergruppe von $\mathbb{Z}^4$. ("Gitter") *). Es gilt

$$(3) \qquad \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in M \implies a^2+b^2+c^2+d^2 \equiv 0 \bmod n$$

Denn: $c^2+d^2 \overset{(2')}{\equiv} (ra-sb)^2 + (sa+rb)^2 = r^2a^2 + s^2b^2 + s^2a^2 + r^2b^2 =$
$(r^2+s^2)(a^2+b^2) \equiv -(a^2+b^2) \bmod n.$

*) Es ist $M \neq \{0\}$, denn $\begin{pmatrix} n \\ n \\ n \\ n \end{pmatrix} \in M$, aber z.B. auch $\begin{pmatrix} 1 \\ 1 \\ r-s \\ r+s \end{pmatrix} \in M$

② Aus (2') folgt

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \\ r \\ s \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \\ -s \\ r \end{pmatrix} + x\begin{pmatrix} 0 \\ 0 \\ n \\ 0 \end{pmatrix} + y\begin{pmatrix} 0 \\ 0 \\ 0 \\ n \end{pmatrix} \quad \text{mit } x,y \in \mathbb{Z}$$

alle $\beta_i \in M$

β_1 β_2 β_3 β_4

Betrachte die Matrix

$$B := (\beta_1, \beta_2, \beta_3, \beta_4) \in M_4(\mathbb{Z}), \quad B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ * & * & n & 0 \\ * & * & 0 & n \end{pmatrix}, \Rightarrow$$

(4) $\det(B) = n^2$, mit $\beta_1, \beta_2, \beta_3, \beta_4$ Basis von $\mathbb{R}^4$
$\beta_1, \beta_2, \beta_3, \beta_4$ $\mathbb{Z}$-Basis von M

$$M = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \mathbb{Z}\beta_3 + \mathbb{Z}\beta_4$$

③ Wichtige Beobachtung:

$$\omega = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in M \Rightarrow \begin{pmatrix} -b \\ a \\ -d \\ c \end{pmatrix}, \begin{pmatrix} -c \\ d \\ a \\ -b \end{pmatrix}, \begin{pmatrix} -d \\ -c \\ b \\ a \end{pmatrix} \in M$$

ω_1 ω_2 ω_3 ω_4

mit (2) bzw. (2') nachrechnen (beachte $r^2+s^2 \equiv -1 \bmod n$, $\det\begin{pmatrix} r & -s \\ s & r \end{pmatrix}$)

④ Vektoren $\omega_1, \omega_2, \omega_3, \omega_4$ wie in ③ sind paarw. orthogonal bzgl. $\langle , \rangle$. Leicht nachzuprüfen.

$A := (\omega_1, \omega_2, \omega_3, \omega_4)$. Dann ${}^tA A = (a^2+b^2+c^2+d^2) E_4$, $\Rightarrow$

(5) $\det(A) = \pm (a^2+b^2+c^2+d^2)^2$ [in der Tat +]

⑤ Unter allen Elementen $\neq 0$ aus M wähle ein $\omega \in M$ mit kleinster Länge:

$$\omega = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in M, \quad 0 \neq a^2+b^2+c^2+d^2 \text{ minimal.}$$

Dann $\omega_1 = \omega$, $\omega_2, \omega_3, \omega_4$ wie in ③.

Wir behaupten:

(6) $M = \mathbb{Z}w_1 + \mathbb{Z}w_2 + \mathbb{Z}w_3 + \mathbb{Z}w_4$

d.h. $(w_1, \dots, w_4)$ ist $\mathbb{Z}$-Basis von M !

Bew. $\alpha \in M$, $\alpha = x_1w_1 + x_2w_2 + x_3w_3 + x_4w_4$, $x_i \in \mathbb{R}$

(denn $w_1, \dots, w_4$ $\mathbb{R}$-Basis von $\mathbb{R}^4$ nach ④).

$x_i = q_i + r_i$ mit $-\frac{1}{2} < r_i \leq \frac{1}{2}$
$\quad\uparrow$
$\quad\mathbb{Z}$

$\alpha = \sum q_i w_i + \sum r_i w_i$, $\overset{M \text{ Gruppe}}{\Rightarrow}$ $w' := \sum r_i w_i \in M$.
$\quad\cap\qquad\qquad\cap$
$\quad M \qquad M$ (da Gruppe)

Ist $w' = 0$, fertig. Ann. $w' \neq 0$. Wegen der Orthogonalität der $w_1, \dots, w_4$

$\langle w', w' \rangle = (r_1^2 + r_2^2 + r_3^2 + r_4^2)\langle w, w \rangle < \langle w, w \rangle$, es sei denn

$r_i = \frac{1}{2}$ für alle i. Dann $w' = \frac{1}{2}(w_1 + \dots + w_4) \in M$,

1. Koord. von w' in $\mathbb{Z}$ $\Longrightarrow$ gg. ③

(7) $a + b + c + d \equiv 0 \bmod 2$

o.E. a ungerade (denn nicht alle $a, b, c, d \equiv 0 \bmod 2$, sonst $\frac{w}{2} \in M$ [1] und $\langle w, w \rangle$ nicht minimal)

o.E. b ungerade (denn b, c, d nicht alle $\equiv 0 \bmod 2$ wegen (7)). Es folgt

$a \equiv b \bmod 2$, und dann auch $c \equiv d \bmod 2$. $\Rightarrow$

$\tilde{w} := \left(\frac{a-b}{2}, \frac{a+b}{2}, \frac{c-d}{2}, \frac{c+d}{2}\right) \in \mathbb{Z}^4$, sogar $\tilde{w} \in M$ [2]

Aber $\langle \tilde{w}, \tilde{w} \rangle = \frac{a^2 + b^2 + c^2 + d^2}{2} < \langle w, w \rangle$ W!.

---

1) beachte: $a/2, b/2, c/2, d/2$ stellen auch (2'), da 2 Einheit mod n (n ungerade)

2) Nach ⑤ ist $w_4 + w_2 = \begin{pmatrix} a-b \\ a+b \\ c-d \\ c+d \end{pmatrix} \in M$, $\Rightarrow \frac{1}{2}\begin{pmatrix} a-b \\ a+b \\ c-d \\ c+d \end{pmatrix} \in M$.

⑥ Sei nun S Übergangsmatrix von $(\omega_1,\dots,\omega_4)$ zu $(\beta_1,\dots\beta_4)$.
beides $\mathbb{Z}$-Basen von M.

$\Rightarrow \quad S \in M_4(\mathbb{Z})$, $S^{-1} \in M_4(\mathbb{Z})$, $\Rightarrow$

(8) $\quad \det(S) = \pm 1$

Nach Def. von S gilt

(9) $\quad B = AS$

[denn $ASe_i = A\sum_j s_{ji} e_j = \sum_j s_{ji} A e_j = \sum_j s_{ji}\omega_j = \beta_i = Be_i$]

Doch aus (9) folgt

$$\det(B) = \det(A)\,\det(S)$$
$$\overset{(4)}{\parallel} \qquad \overset{(5)}{\parallel} \qquad \parallel$$
$$n^2 = \pm(a^2+b^2+c^2+d^2)^2(\pm 1) \ ,$$

also $\quad n = a^2+b^2+c^2+d^2 \qquad$ q. e. d.

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

x $\quad 7 = 2^2+1^2+1^2+1^2$
$\quad 8 = 2^2+2^2$
$\quad 9 = 3^2$
$\quad 10 = 3^2+1^2 = 2^2+2^2+1^2+1^2$
$\quad 11 = 3^2+1^2+1^2$
$\quad 12 = 2^2+2^2+2^2$
$\quad 13 = 3^2+2^2$
o $\quad 14 = 3^2+2^2+1^2$
x $\quad 15 = 3^2+2^2+1^2+1^2$
$\quad \vdots$
x $\quad 29 = 3^2+3^2+2^2+1^2$
$\quad \vdots$
x $\quad 28 = 5^2+1^2+1^2+1^2 = 4^2+2^2+2^2+2^2 = 3^2+3^2+3^2+1^2$
$\quad \vdots$
x $\quad 31 = 5^2+2^2+1^2+1^2$