(i): $n = m^2 n_0$, n_0 quadratfrei [„n_0 quadratfreier Kern von n"]
(d.h. $p \mid n_0 \Rightarrow w_p(n_0) = 1$)

$\Leftarrow$: $n_0 = p_1 p_2 \cdots p_r$ mit $p_i \equiv 1 \bmod 4$ bis auf ggfls $p_1 = 2$ (falls n_0 gerade)

Nach Satz 3: $p_i = N(\pi_i)$, also

$$n_0 = N(\pi_1) N(\pi_2) \cdots N(\pi_r) = N(\underbrace{\pi_1 \cdots \pi_r}_{=: \alpha = c+di})$$

$$n_0 = c^2 + d^2 \quad , \quad n = m^2(c^2+d^2) = a^2 + b^2$$

$\Rightarrow$: $n = a^2 + b^2$ $\quad d := (a,b)$, $\tilde{a} := \frac{a}{d}$, $\tilde{b} := \frac{b}{d}$ $\quad (d \neq 0!)$

$$n = d^2(\tilde{a}^2 + \tilde{b}^2) = d^2 \tilde{m}^2 n_0 \;, \Rightarrow$$
$$\tilde{m}^2 n_0 = \tilde{a}^2 + \tilde{b}^2 \quad , \quad (\tilde{a}, \tilde{b}) = 1 .$$

Nach (ii) gehen in $\tilde{m}^2 n_0$ nur $p \equiv 1 \bmod 4$ oder $p = 2$ auf; folglich gehen auch in n_0 nur solche p auf.

Für jedes $p \equiv 3 \bmod 4$ ist also $w_p(n) = 2 w_p(m) + w_p(n_0) = 2 w_p(m)$ gerade.

(iii): Für beliebiges $n \in \mathbb{N}$ definiere

$$R(n) = \#\{(a,b) \in \mathbb{Z}^2 \mid n = a^2+b^2, (a,b) = 1\} \quad *)$$
$$= \#\{\alpha \in \mathbb{Z}[i] \mid n = N(\alpha), p \nmid \alpha \text{ für jedes } p\} = \#M_n$$

z.B.

(3) $R(1) = 4$, $R(2) = 4$

---

*) $r(n) := \#\{(a,b) \in \mathbb{Z}^2 \mid n = a^2+b^2\}$ [„ohne Bedingung $(a,b) = 1$"]
genaue Bestimmung der Fkt. $r(n)$ in §8.

Für n sei jetzt die Bedingung (2) erfüllt (und s sei die Zahl der Primteiler $\neq 2$ von n)

9.2.2. (4) $\quad R(n) = 2^{s+2} \qquad \forall\, n \in \mathbb{N}$

(Denn für $n>2$, d.h. $s \geq 1$ gilt: Ist $\alpha = a+bi \in M_n$, so sind die Elt'e $\pm a \pm bi$, $\pm ai \pm b$ acht verschiedene Elemente von M_n; beachte $a \neq b$ und $a,b \neq 0$. Somit $\frac{R(n)}{8} = 2^{s-1}$.)

Bew. von (4) durch Induktion nach s. Für $s=0$ richtig! [wegen (3)]

Sei $p \mid n$, $p \neq 2$.

Wegen (2): $\quad p = \pi\bar{\pi}$, $\quad \bar{\pi} \neq \pi$ $\quad$ (π fest gewählt)

$\alpha \in M_n$. $\quad p \mid n \Rightarrow N(\alpha) = \alpha\bar{\alpha}$, $\quad \Rightarrow \pi \mid \alpha$ oder $\pi \mid \bar{\alpha}$

$\pi \mid \alpha$ oder $\bar{\pi} \mid \alpha$

d.h. $\frac{\alpha}{\pi}$ oder $\frac{\alpha}{\bar{\pi}}$ in $\mathbb{Z}[i]$

$N\left(\frac{\alpha}{\pi}\right) = \frac{N(\alpha)}{N(\pi)} = \frac{n}{p}$, $N\left(\frac{\alpha}{\bar{\pi}}\right) = \frac{n}{p}$, also

$\frac{\alpha}{\pi} \in M_{n/p}$ oder $\frac{\alpha}{\bar{\pi}} \in M_{n/p}$

Es folgt $M_n = \pi M_{n/p} \,\dot\cup\, \bar{\pi} M_{n/p}$ disjunkt *) ....

Somit $\quad \# M_n = 2 \# M_{n/p}$, d.h. $R(n) = 2 \cdot 2^{(s-1)+2} = 2^{s+2}$.

(↑ Ind. Vorauss.)

---

*) sonst $\pi \mid \alpha$ und $\bar{\pi} \mid \alpha$, $\Rightarrow \pi\bar{\pi} \mid \alpha \overset{p=\pi\bar{\pi}}{\Rightarrow} p \mid \alpha$,

Widerspruch zu $\alpha \in M_n$

Korollar: Es sei n eine ungerade nat. Zahl > 1. Besitzt n im wesentlichen nur eine einzige Darstellung als Summe von 2 Quadraten und ist diese Darstellung primitiv, so ist n eine Primzahl. (Umkehrung von Korollar zu Satz 3).

Bew. Nach Satz 4 hat n nur einen einzigen Primteiler p, d.h. $n = p^k$, und es ist $p \equiv 1 \bmod 4$.

Wäre $k \geq 2$, so hätte man $n = p^2 p^{k-2} \overset{\text{Satz 4}}{=} p^2(a^2+b^2) = (pa)^2 + (pb)^2$ im

Widerspruch zur Vor.

Bem. $45 = 6^2 + 3^2$ die einzige Darstellung als Summe von 2 Quadraten; doch diese ist nicht primitiv.

Im übrigen die Vor. ungerade wesentlich: Für $n = 10$ ist $10 = 3^2 + 1^2$ die i.w. einzige Darstellung als Summe von 2 Quadraten und diese ist auch primitiv. Doch 10 ist keine Primzahl

§6 Quadratische Reste

Vorbemerkungen: $m \in \mathbb{N}$, $m > 1$. Untersuche Kongruenz der Gestalt

„alles über ℤ"

(1) $aX^2 + bX + c \equiv 0 \bmod m$, $a \neq 0$

$\Leftrightarrow 4a^2X^2 + 4abX + 4ac \equiv 0 \bmod 4am$ $\Leftrightarrow$

(2) $(2aX + b)^2 \equiv b^2 - 4ac \bmod 4am$

$D := b^2 - 4ac$ Diskriminante

$\Leftrightarrow$

(3) $\begin{cases} Y^2 \equiv D \bmod 4am \\ Y \equiv b \bmod 2a \end{cases}$ $\qquad y = b + 2ax$

Bem. 1) Für $(a,m) = 1$: (1) äquiv. zu $X^2 + \frac{b}{a}X + \frac{c}{a} \equiv 0 \bmod m$

2) Für m, a ungerade : (1) äquiv. zu $\left(aX + \frac{b}{2}\right)^2 - \left(\left(\frac{b}{2}\right)^2 - ac\right) \equiv 0 \bmod am$

F1: Die Kongruenz

(4) $X^2 \equiv D \bmod m$ $\qquad (D,m) = d = d_1^2 d_0$, d_0 quadratfrei

ist genau dann lösbar, wenn $\left(\frac{m}{d}, d_0\right) = 1$ und

(5) $X^2 \equiv d_0 \frac{D}{d} \bmod \frac{m}{d}$

lösbar ist. Hier sind $d_0 \frac{D}{d}$ und $\frac{m}{d}$ teilerfremd! (Denn $\frac{m}{d}$ prim zu $\frac{D}{d}$ und wegen $\left(\frac{m}{d}, d_0\right) = 1$ auch zu d_0.)

Bew. „$\Rightarrow$": $x^2 \equiv D \bmod m$; $d_1^2 \mid D$, $d_1^2 \mid m$, $\Rightarrow d_1^2 \mid x^2$, $\Rightarrow d_1 \mid x$,

$\Rightarrow$

(6) $\left(\frac{x}{d_1}\right)^2 \equiv d_0 \frac{D}{d} \bmod d_0 \frac{m}{d}$, $\Rightarrow$ $\frac{x}{d_1} \in \mathbb{Z}$ Lösung von (5).

$(6) \Rightarrow d_0 \mid \left(\frac{x}{d_1}\right)^2$, $\overset{d_0 \text{ quadratfrei}}{\Longrightarrow}$ $d_0 \mid \frac{x}{d_1}$, $\overset{(6)}{\Rightarrow}$

$\left(\frac{x}{d_1 d_0}\right)^2 d_0 \equiv \frac{D}{d} \bmod \frac{m}{d}$, $\Rightarrow \left(d_0, \frac{m}{d}\right) = 1$

[denn $\left(\frac{D}{d}, \frac{m}{d}\right) = 1$]

„$\Leftarrow$": Sei y Lsg. von (5) und $\left(\frac{m}{d}, d_0\right) = 1$

$y^2 \equiv d_0 \frac{D}{d} \bmod \frac{m}{d}$ $\overset{\left(\frac{m}{d}, d_0\right) = 1}{\Longrightarrow}$ $\left(\frac{y}{d_0}\right)^2 d_0 \equiv \frac{D}{d} \bmod \frac{m}{d}$,

$\Rightarrow d d_0 \left(\frac{y}{d_0}\right)^2 \equiv D \bmod m$, $\overset{d = d_0 d_1^2}{\Longrightarrow}$ $(y d_1)^2 \equiv D \bmod m$,

$\Rightarrow$ (4) lösbar. □

Damit alles reduziert auf eine Kongruenz der Gestalt

(*) $\quad X^2 \equiv a \bmod m$ mit $\boxed{(a, m) = 1}$

dabei wird stets $(a,m)=1$ vorausgesetzt!

Abkürzungen: QR, NQR

Ist (*) lösbar, d.h. ex. ein $b \in \mathbb{Z}$ mit $b^2 \equiv a \bmod m$, so heißt a ein quadratischer Rest mod m, andernfalls heißt a ein quadr. Nichtrest mod m. abus de langage!

[besser wäre: Nichtquadratrest]

Probleme: 1) Sei m gegeben. Man verschaffe sich eine Übersicht über die sämtlichen quadr. Reste mod m.

2) Sei a gegeben. Für welche (zu a teilerfremden) nat. Zahlen $m > 1$ ist a quadr. Rest mod m?

Problem 2) ist schwieriger und tiefer. Beantwortung durch das Quadratische Reziprozitätsgesetz.

Zu Problem 1):

F2: a ist quadr. Rest mod m genau dann, wenn:

1) a quadr. Rest mod p für jeden ungeraden Primteiler p von m

2) $a \equiv 1 \bmod 4$, falls $4 \mid m$, $8 \nmid m$
   $a \equiv 1 \bmod 8$, falls $8 \mid m$

Ist a quadr. Rest mod m, so hat (*) genau 2^{s+t} Lsg'en mod m; dabei s = Anzahl der ungeraden Primteiler von m und

$t = 2$ für $w_2(m) \geq 3$
$t = 1$ für $w_2(m) = 2$
$t = 0$ für $w_2(m) \leq 1$.

Bew. $f(X) = X^2 - a$, $m = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$ PFZ

$f(X) \equiv 0 \bmod m$ lösbar $\Leftrightarrow$ $f(X) \equiv 0 \bmod p_i^{\nu_i}$ lösbar für jedes i

Genauer $\quad N_f(m) = \prod_{i=1}^{r} N_f(p_i^{\nu_i})$ (vgl. §3)

F2 folgt nun aus folgendem

Lemma: p Primzahl, $\nu \in \mathbb{N}$. Dann für jedes zu p prime $a \in \mathbb{Z}$:

1) Für $p \neq 2$: $X^2 \equiv a \bmod p^\nu$ lösbar $\Leftrightarrow$ $X^2 \equiv a \bmod p$ lösbar.

2) Für $p = 2$: $X^2 \equiv a \bmod 2^\nu$ lösbar $\Leftrightarrow$
   - für $\nu = 1$: keine Bedingung
   - für $\nu = 2$: $a \equiv 1 \bmod 4$
   - für $\nu \geq 3$: $a \equiv 1 \bmod 8$

Falls lösbar, dann

$$N_f(p^\nu) = 2 \text{ für } p \neq 2, \quad N_f(2^\nu) = 2^t$$

Bew. $G = (\mathbb{Z}/p^\nu)^\times$

1) $p \neq 2$: $\quad G = (\mathbb{Z}/p^\nu)^\times \xrightarrow{h} (\mathbb{Z}/p)^\times$, $\operatorname{Ker} h = G^{(1)}$

$\alpha \in G$ Quadrat in $G \Rightarrow h(\alpha)$ Quadrat in $(\mathbb{Z}/p)^\times$. Umgekehrt: