$h(\alpha)$ Quadrat in $(\mathbb{Z}/p)^\times \xRightarrow{(\beta^2)^{\frac{p-1}{2}} = \beta^{p-1} = 1} h(\alpha)^{\frac{p-1}{2}} = 1 \Longrightarrow h(\alpha^{\frac{p-1}{2}}) = 1,$

$\Rightarrow \alpha^{\frac{p-1}{2}} \in G^{(1)} \Rightarrow \alpha^{\frac{p-1}{2}\cdot p^{\nu-1}} = 1 \Rightarrow \alpha^{\frac{\varphi(p^\nu)}{2}} = 1$

$\xRightarrow[\mathrm{ord}(G) = \varphi(p^\nu)]{G \text{ zyklisch}}$ α Quadrat in G. (vgl. §4, F6).

$\sigma, \tau \in G$

$\sigma^2 = \tau^2 \Leftrightarrow (\sigma\tau^{-1})^2 = 1 \Leftrightarrow \sigma\tau^{-1}$ in der Untergruppe H_2 der Ordnung 2 der zykl. Gruppe G

$\Leftrightarrow \sigma = \rho\tau,\ \rho \in H_2$. Ist also $\alpha \in G$ ein Quadrat, so gilt

$$\#\{\sigma \mid \sigma^2 = \alpha\} = 2.$$

2) $p = 2$: für $\nu = 1$ und $\nu = 2$ Bel. klar: $(\mathbb{Z}/2)^\times = \{\bar 1\}$,
$(\mathbb{Z}/4)^\times = \{\bar 1, -\bar 1\}$ Quadrate: $\{\bar 1\}$

Sei $\nu \geq 3$.

$$G = (\mathbb{Z}/2^\nu)^\times \xrightarrow{h} (\mathbb{Z}/8)^\times$$

$\rho^2 = 1$ für alle $\rho \in (\mathbb{Z}/8)^\times$

α Quadrat in $G \Rightarrow h(\alpha)$ Quadrat in $(\mathbb{Z}/8)^\times \Rightarrow h(\alpha) = 1$
$(\Rightarrow a \equiv 1 \bmod 8)$

Umgekehrt: Sei $a \equiv 1 \bmod 2^3$ ⌜insb. $a \equiv 1 \bmod 4$, d.h. $\alpha \in G^{(2)}$

⇙ §4, Lemma 2

$$a^{2^{\nu-3}} \equiv 1 \bmod 2^\nu,\ \alpha^{2^{\nu-3}} = 1. \qquad 2^{\nu-3} = \frac{2^{\nu-2}}{2}$$

Aber $G^{(2)}$ zyklisch von der Ordnung $2^{\nu-2}$. Also α Quadrat in $G^{(2)} \subseteq G$.

Wieder: $\#\{\sigma \in G \mid \sigma^2 = \alpha\} = \#\{\rho \in G \mid \rho^2 = 1\} \overset{!}{=} 4$,
denn $G = \langle -\bar 1\rangle \times \langle \bar 5\rangle \simeq \mathbb{Z}/2 \times \mathbb{Z}/2^{\nu-2}$. □

Damit Reduktion auf Fall $m = \boxed{p \text{ Primzahl} \neq 2}$:

$$(*) \qquad X^2 \equiv a \bmod p \quad , \qquad (a,p) = 1$$

Def. (Legendresymbol) $\qquad p$ Primzahl $\neq 2$.

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } (*) \text{ lösbar} \\ -1 & \text{falls } (*) \text{ nicht lösbar.} \end{cases}$$

Definiert für jedes $a \in \mathbb{Z}$ mit $(a,p) = 1$.

$S = \{1, 2, \dots, p-1\}$ primes Restsystem mod p
⌜Vertr.system von $(\mathbb{Z}/p)^\times$⌟

Vor: $p \neq 2$, d.h. $p-1$ gerade

$\frac{p-1}{2} + 1 = \frac{p+1}{2}$

$$H := \{1, 2, \dots, \tfrac{p-1}{2}\} \qquad S = H \,\dot\cup\, \underbrace{\{\overset{\substack{-\frac{p-1}{2} \\ \equiv}}{\tfrac{p+1}{2}}, \dots, \overset{\substack{-2 \\ \equiv}}{p-2}, \overset{\substack{-1 \\ \equiv}}{p-1}\}}_{=:H' \text{ oberes Halbsystem}}$$

unteres Halbsystem

Ist a quadr. Rest mod p, so gibt es genau ein $b \in H$ mit

$$b^2 \equiv a \bmod p$$

Bew. klar (ÜA); beachte: $b^2 \equiv c^2 \bmod p \overset{\mathbb{Z}/p \text{ Körper}}{\Longrightarrow} b \equiv \pm c \bmod p$
($\Rightarrow b = c$, falls $b, c \in H$)

Also:

F3: Es gibt genau $\frac{p-1}{2}$ quadr. Reste mod p und ebensoviele quadr. Nichtreste mod p. $\qquad (p \neq 2)$

Sei a quadr. Rest mod p. $\qquad a \equiv b^2 \bmod p$, $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p$

Also

$$(1) \qquad a^{\frac{p-1}{2}} \equiv 1 \bmod p \quad \text{für jeden quadr. Rest mod } p.$$

$f(X) = X^{\frac{p-1}{2}} - 1$ als Polynom über $F := \mathbb{Z}/p\mathbb{Z}$.

$F^{\times 2} := \{\alpha^2 \mid \alpha \in F^\times\}$

f hat die $\frac{p-1}{2}$ Elemente von $F^{\times 2}$ als Nullstellen. Mehr Nullstellen kann f in F nicht haben. Also:

a quadr. Nichtrest mod p $\Longrightarrow$ $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$

wegen $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \mod p$, folgt:

(2) $a^{\frac{p-1}{2}} \equiv -1 \mod p$ für jeden quadr. Nichtrest mod p.

<u>F4:</u> Für jedes a (teilerfremd zu $p \neq 2$) gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

(<u>Eulersches Kriterium</u>).

<u>Bem'n:</u> 1) F3 und F4 folgen auch sofort aus der Existenz einer Primitivwurzel mod p. ($G = (\mathbb{Z}/p\mathbb{Z})^\times$ ist <u>zyklisch</u> von der Ordnung $p-1$)

2) Aus $\left(\frac{a}{p}\right) \equiv \varepsilon \mod p$ mit $\varepsilon \in \{1,-1\}$ folgt $\left(\frac{a}{p}\right) = \varepsilon$.

Denn $1 \equiv -1 \mod p$ unmöglich für $p \neq 2$.

3) F4 für $a = -1$: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p \overset{2)}{\Longrightarrow}$

$$(*) \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{für } p \equiv 1 \mod 4 \\ -1 & \text{für } p \equiv 3 \mod 4 \end{cases}$$

"1. Ergänzungssatz"

also erneut F8 in §3 bewiesen.

<u>F5:</u> (i) Das Legendresymbol $\left(\frac{a}{p}\right)$ hängt von a nur modulo p ab.

(ii) $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$$ für alle a, b (prim zu p)

<u>Bew.</u> (i) klar nach Def.

(ii) ⌜eigentlich 4 Aussagen, von denen (nur) die letzte, nämlich "quadr. Nichtrest × quadr. Nichtrest = quadr. Rest", nichttrivial ist⌟

$$\left(\frac{ab}{p}\right) \overset{\text{Euler}}{\equiv} (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p\,, \overset{\text{Bem. 2)}}{\Longrightarrow} \text{Beh.}$$

<u>Bem'n:</u> 1) Das Legendresymbol vermittelt Abb.

$$\chi:\ (\mathbb{Z}/p)^\times \longrightarrow \{1,-1\}\,,\quad \chi(a \bmod p) = \left(\frac{a}{p}\right)$$

Diese ist ein Homomorphismus von Gruppen.

"$\chi(a \bmod p)$ gibt quadratischen Charakter von a mod p an"

Allgemein: Jedes Homomorphismus einer endlichen (abelschen) Gruppe G in $\mathbb{C}^\times$ heißt ein Charakter von G.

2) $a = \pm q_1 q_2 \cdots q_s$, q_i Primzahlen $\neq p$.

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_s}{p}\right)$$

Zur Beantwortung von Problem 2 ist wegen F2 nur zu fragen:

Für welche <u>Primzahlen</u> $p \neq 2$ ist die gegebene Zahl a quadratischer Rest mod p ?

Wegen F5 genügt es dann weiter, für a folgende Fälle zu betrachten:

1. $a = -1$. Schon erledigt, durch "1. Ergänzungssatz"
2. $a = 2$. Wird erledigt durch "2. Ergänzungssatz"
3. a ist eine <u>ungerade Primzahl</u> q. Lösung durch "Quadratisches Reziprozitätsgesetz".

<u>Fortan $p \neq 2$.</u>

Wir betrachten das (untere) Halbsystem $H = \{1, 2, \dots, \frac{p-1}{2}\}$. Wir wissen:

Zu jedem $b \in \mathbb{Z}$ mit $(b,p) = 1$ gibt es <u>genau ein</u> $x \in H$ mit

$$b \equiv x \bmod p \quad \text{oder} \quad b \equiv -x \bmod p$$

Es ist also

$$b \equiv \varepsilon(b)\, x \bmod p \text{ mit eind. } x \in H \text{ und eind. } \varepsilon(b) \in \{1,-1\}$$

Für festes $a \in \mathbb{Z}$ mit $(a,p) = 1$ und bel. $x \in H$ ist also

(1) $\quad ax \equiv \varepsilon(ax)\, x_a \bmod p$ mit eind. $x_a \in H$.

Für $x, y \in H$ gilt

(2) $\quad x \neq y \Rightarrow x_a \neq y_a$

(denn sonst $x \equiv \pm y \bmod p$, $\overset{x,y \in H}{\Longrightarrow}$ $x = y$ W!)

F6 (Gaußsches Lemma):

$$\left(\frac{a}{p}\right) = \prod_{x\in H} \varepsilon(ax)$$

Bew.

$$a^{\frac{p-1}{2}} \prod_{x\in H} x = \prod_{x\in H}(ax) \overset{(1)}{\equiv} \prod_{x\in H}\varepsilon(ax)\cdot\prod_{x\in H} x_a \overset{(2)}{=} \prod_{x\in H}\varepsilon(ax)\cdot\prod_{x\in H} x \mod p,$$

$$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv \prod_{x\in H}\varepsilon(ax) \mod p, \quad \overset{\text{Euler}}{\Longrightarrow} \quad \text{Beh.} \qquad \square$$

Anw. auf $a=2$: Für $x\in H$ gilt

$$\varepsilon(2x) \overset{\text{nach Def}}{=} \begin{cases} +1 & \text{für } 2x \le \frac{p-1}{2}\text{, d.h. } x \le \frac{p-1}{4} \\ -1 & \text{für } \frac{p-1}{4} < x \le \frac{p-1}{2} \end{cases} \Bigg)$$

$$\overset{F6}{\Longrightarrow} \quad \left(\frac{2}{p}\right) = (-1)^{\nu(p)} \quad \text{mit } \nu(p) = \#\left\{x\in\mathbb{Z} \;\middle|\; \tfrac{p-1}{4} < x \le \tfrac{p-1}{2}\right\}$$

Es ist $p = 4k+1$ oder $p = 4k-1$ mit $k\in\mathbb{N}$

$k < x \le 2k$ $\qquad$ $k - \frac{1}{2} < x \le 2k-1$

$x = k+1, \dots, k+k$ $\qquad$ $x = k, \dots, k+k-1$,

also in beiden Fällen $\nu(p) = k$, und somit

$$\left(\frac{2}{p}\right) = (-1)^k = \begin{cases} +1 & \text{für } k \text{ gerade} \\ -1 & \text{für } k \text{ ungerade} \end{cases}$$

$\Rightarrow$

Euler **F7 („2. Ergänzungssatz“):**

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{für } p \equiv \pm 1 \mod 8 \\ -1 & \text{für } p \equiv \pm 5 \mod 8 \end{cases}$$

Satz 1 (Quadratisches Reziprozitätsgesetz) Euler, Legendre, Gauß

Für ungerade Primzahlen $p \neq q$ gilt

(R) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Das bedeutet:

1) Ist eine der beiden Primzahlen p, q kongruent 1 mod 4, so gilt

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

d.h. q quadr. Rest mod p genau dann, wenn p quadr. Rest mod q.

2) Sind beide Primzahlen p und q kongruent 3 mod 4, so gilt

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right),$$

d.h. q quadr. Rest mod p genau dann, wenn p quadr. Nichtrest mod q.

schon bewiesen

Zusatz: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ 1. Ergänzungssatz $p \neq 2$

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ 2. Ergänzungssatz

Das bedeutet:

$$-1 \text{ quadr. Rest mod } p \iff p \equiv 1 \bmod 4$$
$$2 \text{ quadr. Rest mod } p \iff p \equiv \pm 1 \bmod 8$$

⌈ $p = j + 8k \quad j \in \{1, 3, -3, -1\} \qquad p^2 \equiv j^2 \bmod 16, \implies$

$$\frac{p^2-1}{8} \equiv \frac{j^2-1}{8} \bmod 2 \qquad \frac{j^2-1}{8} = \begin{cases} 0 & \text{für } j = 1, -1 \\ 1 & \text{für } j = 3, -3 \end{cases}$$ ⌋

Beispiele:

a) $\left(\frac{6}{59}\right) = \left(\frac{2}{59}\right)\left(\frac{3}{59}\right) = -\left(\frac{3}{59}\right) = -\left(-\left(\frac{59}{3}\right)\right) = \left(\frac{59}{3}\right) = \left(\frac{2}{3}\right) = -1$

$59 \equiv 3 \bmod 8$

6 also kein quadr. Rest mod 59.