a *ist* n-ter Potenzrest $(\bmod m) :\Leftrightarrow\ a \equiv r^n(m)\ \Leftrightarrow\ x^n \equiv a(m)$ lösbar

a quadratischer Rest $:\Leftrightarrow\quad a \equiv r^2 \bmod m$ $\qquad a \in Q_m$

(quadratischer Nichtrest) $a \notin Q_m$

Legendre-Symbol *(Legendresches Restsymbol)*

$$\left(\frac{kp}{p}\right) := 0 \qquad \left(\frac{a}{p}\right) := \begin{cases} 1 & a \in Q_p \\ -1 & a \notin Q_p \end{cases} \qquad (a,p)=1,\ p \text{ prim}$$

(Eulersches Kriterium) $\Rightarrow a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$

Jacobi-Symbol $\qquad (a,p_i)=1,\ p_i \geq 3$ prim

$$m = \prod_i p_i \qquad \left(\frac{a}{m}\right) := \prod_i \left(\frac{a}{p_i}\right) \qquad \textit{(Homomorphismus)}$$

es gilt: $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right),\ \left(\frac{r^2}{m}\right) = 1,\ \left(\frac{a+km}{m}\right) = \left(\frac{a}{m}\right)$

Gruppe der (primen) quadratischen Reste

$\{\overline{a} \mid a \equiv r^2\} =: Q_m^* < (\mathbb{Z}_m^*, \cdot)$ $\qquad$ Nichtreste $N_m^* := \mathbb{Z}_m^* \setminus Q_m^*$

$(\ \mathbb{Z}_p^*\ )$ $\qquad [\mathbb{Z}_p^*{:}Q_p^*] = 2,\ N_p^* = rQ_p^*$ $\qquad (\ a^2 = (-a)^2\ )$

Quadratisches Reziprozitätsgesetz *Gauß 1796 (Euler, Legendre)*

$$p, q \geq 3 \qquad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ *erster* Ergänzungssätze *zweiter* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \Leftarrow p \vee q \equiv 1(4) \qquad p \equiv q \equiv 3(4) \ \Rightarrow \quad \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

$$\left(\frac{-1}{p}\right) = 1 \quad \Leftarrow p \equiv 1(4) \qquad p \equiv 3(4) \ \Rightarrow \quad \left(\frac{-1}{p}\right) = -1$$

$$\left(\frac{2}{p}\right) = 1 \quad \Leftarrow p \equiv \pm 1(8) \qquad p \equiv \pm 3(8) \ \Rightarrow \quad \left(\frac{2}{p}\right) = -1$$

Primzahlsatz von Dirichlet *(1837)* $\qquad (\ (a,b)=1\ )$

Es gibt unendlich viele Primzahlen der Form $an+b$

Spezialfall $4k \pm 1$ $\qquad (p_i \equiv -1 \bmod 4)$ $\qquad$ *bilde* $4p_1p_2\cdots p_n - 1$

(analog zu Euklid) $\qquad (p_i \equiv 1 \bmod 4)$ $\qquad$ *bilde* $(2p_1p_2\cdots p_n)^2 + 1$

Solche Erkenntnisse, wo die Aussage eines Satzes völlig unerwartet ist und ohne Zusammenhang mit der Fragestellung selbst erscheint, haben immer wieder die Bewunderung der Mathematiker erregt.
Reinhold Remmert, Peter Ullrich, *Elementare Zahlentheorie* 1986

---

vollständiges Restsystem (p prim) $\overline{0}, \overline{\pm 1}, \overline{\pm 2}, \cdots, \overline{\pm \frac{p-1}{2}}$

$\overline{r} \mapsto \overline{ar}$, $(a,p) = 1$ Permutation von $\mathbb{Z}_p^*$ $\overline{-r} \mapsto -\overline{ar}$

$$\{\overline{1}, \overline{2}, \cdots, \overline{\tfrac{p-1}{2}}\} \to \{\varepsilon_1 \overline{1}, \varepsilon_2 \overline{2}, \cdots, \varepsilon_{\frac{p-1}{2}} \overline{\tfrac{p-1}{2}}\} \qquad \varepsilon_i = \pm 1$$

also $$\overline{a} \cdot \overline{2a} \cdots \overline{\tfrac{p-1}{2} a} = (\varepsilon_1 \overline{1}) \cdot (\varepsilon_2 \overline{2}) \cdots (\varepsilon_{\frac{p-1}{2}} \overline{\tfrac{p-1}{2}})$$ *oder*

($\varepsilon(a) :=$ Zahl der $\varepsilon_i(a)$ mit $\varepsilon_i(a) = -1$)

$$a^{\frac{p-1}{2}} (\tfrac{p-1}{2})! \equiv (-1)^{\varepsilon(a)} (\tfrac{p-1}{2})! \bmod p \ \Rightarrow$$

Lemma von Gauß $a^{\frac{p-1}{2}} \equiv (-1)^{\varepsilon(a)} \bmod p$

Eulersches Kriterium $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ $\Rightarrow$ **2. Ergänzungssatz**

denn: $\varepsilon_r(2) = -1 \ \Leftrightarrow \ (p-1)/4 < r \leq (p-1)/2$ ■

Quadratisches Reziprozitätsgesetz (Gauß 1796)

$p, q \geq 3$ prim $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

(Beweisskizze) *(nach Frobenius-Zeller 1872, Eisenstein 1844)*

$\varepsilon_r(a) = -1 \ \Leftrightarrow$ $(\exists k) \ -\frac{p-1}{2} \leq ar - kp \leq -1$ $\Rightarrow \ k < a\frac{r}{p} + \frac{1}{2}$

$0 < r \leq \frac{p-1}{2}$ $\Rightarrow \ 1 \leq k < \frac{a+1}{2}$

(bzgl. p) $\varepsilon_r(q) = -1 \ \Leftrightarrow \ (\exists s) \ s \leq \frac{q-1}{2}$ $-\frac{p-1}{2} \leq qr - sp \leq -1$

(bzgl. q) $\varepsilon_s(p) = -1 \ \Leftrightarrow \ (\exists r) \ r \leq \frac{p-1}{2}$ $-\frac{q-1}{2} \leq ps - rq \leq -1$

(„Rechteck") $1 \leq r \leq \frac{p-1}{2} \wedge 1 \leq s \leq \frac{q-1}{2}$ $\Leftrightarrow: (r,s) \in R$

$\varepsilon_r(q) = -1 \vee \varepsilon_s(p) = -1 \ \Leftrightarrow$

(„Diagonale") $-\frac{p-1}{2} \leq qr - sp \leq \frac{q-1}{2}$ $\Leftrightarrow: (r,s) \in D$

(Gaußsches Lemma) $\Rightarrow$ $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\varepsilon(q)+\varepsilon(p)}$

also zu zeigen: $\varepsilon(q) + \varepsilon(p) \equiv \frac{p-1}{2}\frac{q-1}{2} \bmod 2$ $\Leftrightarrow$ $|R \setminus D|$ *gerade*

$R \setminus D$ ist symmetrisch: *bezüglich* $((p+1)/4, (q+1)/4)$

(Paarbildung) $(r,s) \ \leftrightarrow \ (\frac{p-1}{2} + 1 - r, \frac{q-1}{2} + 1 - s)$ ■

Das Protokoll *(Verfahrensvorschrift)* Manuel Blum 1982

(1) **A** *wählt „Münze“*: nennt n

$p \equiv q \equiv 3 \bmod 4$ prim *(groß!)*, $n = pq$

(2) nennt y **B** *„wirft Münze“*

$y \equiv a^2 \bmod n$ $((a, n) = 1)$

(3) **A** *rät: „Kopf“ oder „Adler“*

sagt $+1$ *oder* -1

(4) Losentscheid: $\left(\frac{a}{n}\right) = \pm 1$ (Jacobi-Symbol)

Kontrolle: *(effizient durchführbar!)*

durch **B**: durch **A**:

$a^2 \equiv y \bmod n$? $n = pq, p \equiv q \equiv 3 \bmod 4$ prim?

Bemerkung: *(Protokoll ist sicher)*

A kann lösen: **B** kennt:

$x^2 \equiv y \bmod p$ (2 Lösungen)

$x^2 \equiv y \bmod q$ (2 Lösungen)

$\Rightarrow x^2 \equiv y \bmod n$ (4 Lösungen)

$\pm a$ und $\pm \varepsilon a$ $\pm a$

mit: $(\frac{\pm a}{n}) = -(\frac{\pm \varepsilon a}{n})$ $(\frac{a}{n}) = (\frac{-a}{n})$

Anwendung:

n-malige Anwendung: n zufällige Bits (0,1) $\rightarrow$ Zufallszahl $0 \leq 2^n - 1$

(a) Wurzeln: $x^2 \equiv 1 \bmod pq \Leftrightarrow x^2 \equiv 1 \bmod p \wedge x^2 \equiv 1 \bmod q$

$\Rightarrow x \equiv \pm 1 \bmod p \wedge x \equiv \pm 1 \bmod q$

4 Lösungen: $1, -1, \varepsilon, -\varepsilon \bmod pq$ $\varepsilon = p^{q-1} - q^{p-1}$

(b) Jacobi-Symbol: *wegen* $p \equiv q \equiv 3 \bmod 4$ *ist*

$(\frac{-1}{p}) = (\frac{-1}{q}) = -1 \Rightarrow$ $(\frac{-1}{n}) = (\frac{-1}{pq}) = (\frac{-1}{p})(\frac{-1}{q}) = (-1) \cdot (-1) = 1$

sowie $(\frac{\varepsilon}{p}) = (\frac{1}{p}) = 1$ *und* $(\frac{\varepsilon}{q}) = (\frac{-1}{q}) = -1 \Rightarrow$

$(\frac{\varepsilon}{n}) = (\frac{\varepsilon}{pq}) = (\frac{\varepsilon}{p})(\frac{\varepsilon}{q}) = 1 \cdot (-1) = -1$

(c) $a^2 \equiv (\varepsilon a)^2 \bmod pq \Rightarrow (a - \varepsilon a)(a + \varepsilon a) \equiv 0 \bmod pq$

$\Leftrightarrow$ $pq/(a - \varepsilon a)(a + \varepsilon a)$ *also:* $(a + \varepsilon a, n)$ *ist* p oder q

d.h. Wurzelziehen ist ebenso schwer wie Faktorisieren von n!