Wiederholung:

Satz 5.7 (Das Quadratische Reziprozitätsgesetz):

Seien $p, q \in \mathbb{P} \setminus \{2\}$. Dann gilt

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{falls } p, q \equiv 3 \bmod 4 \\ \left(\frac{p}{q}\right) & \text{sonst} \end{cases}$$

äquivalent: $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$

Satz 5.8 (1. Ergänzungssatz zum QRG):

$$\left(\frac{-1}{p}\right) = \begin{cases} -1 & \text{wenn } p \equiv 3 \bmod 4 \\ 1 & \text{wenn } p \equiv 1 \bmod 4 \end{cases}$$

äquivalent: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Satz 5.9 (2. Ergänzungssatz zum QRG):

$$\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{wenn } p \equiv 3, 5 \bmod 8 \\ 1 & \text{wenn } p \equiv 1, -1 \bmod 8 \end{cases}$$

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

Beweis des QRG und Ergänzungssätze

1. Satz 5.8 folgt aus dem Eulerschen Kriterium.

2. Für $1 \leq i \leq \frac{p-1}{2}$, sei $a_i = \varepsilon_i h_i + e_i p$

$(\varepsilon_i = \pm 1,\ h_i \in H,\ e_i \in \mathbb{Z})$

Behauptung: $\varepsilon_i = (-1)^{\left\lfloor \frac{2a_i}{p} \right\rfloor}$

Denn sei $\varepsilon_i = 1$

Dann ist $\frac{2a_i}{p} = \frac{2h_i}{p} + 2e_i$

$\Rightarrow \left\lfloor \frac{2a_i}{p} \right\rfloor = 2e_i$

$\Rightarrow (-1)^{\left\lfloor \frac{2a_i}{p} \right\rfloor} = (-1)^{2e_i} = 1.$

Andererseits, sei $\varepsilon_i = -1$

Dann ist $\frac{2a_i}{p} = \frac{-2h_i}{p} + 2e_i$

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

$\Rightarrow \left\lfloor \frac{2a_i}{p} \right\rfloor = 2e_i - 1$

$\Rightarrow (-1)^{\left\lfloor \frac{2a_i}{p} \right\rfloor} = (-1)^{2e_i - 1} = -1.$

In beiden Fällen ist $\varepsilon_i = (-1)^{\left\lfloor \frac{2a_i}{p} \right\rfloor}$.

3. Aus Lemma 5.6 und Schritt 2 folgt

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i = \prod_{i=1}^{\frac{p-1}{2}} (-1)^{\left\lfloor \frac{2ai}{p} \right\rfloor}$$

$$= (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ai}{p} \right\rfloor}$$

4. Behauptung: Für a ungerade gilt $\left(\frac{2a}{p}\right) = (-1)^{\left(\frac{p^2-1}{8} + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor\right)}$

Denn $\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\,\frac{a+p}{2}}{p}\right)$

$$= \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right)$$

$$= \left(\frac{\frac{a+p}{2}}{p}\right)$$

$$= (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{(a+p)i}{2} \right\rfloor} \qquad \text{(Schritt 3)}$$

und $\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{(a+p)i}{p} \right\rfloor = \sum_{i=1}^{\frac{p-1}{2}} i + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor$

$$= \frac{1}{2}\,\frac{p-1}{2}\left(\frac{p-1}{2}+1\right) + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor$$

$$= \frac{p^2-1}{8} + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor$$

$$\Rightarrow \left(\frac{2a}{p}\right) = (-1)^{\left(\frac{p^2-1}{8} + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor\right)}$$

5. Aus Schritt 4 folgt insbesondere, mit $a=1$, dass

$$\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8} + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{i}{p} \right\rfloor\right)}$$

$$= (-1)^{\frac{p^2-1}{8}}$$

Wenn $p = 8k \pm 1$, dann ist $\frac{p^2-1}{8} = \frac{64k^2 \pm 16k}{8}$

$= 8k^2 \pm 2k$ ist gerade

$\Rightarrow \left(\frac{2}{p}\right) = 1$

Wenn $p = 8k \pm 3$, dann ist $\frac{p^2-1}{8} = \frac{64k^2 \pm 48k + 9 - 1}{8}$

$= 8k^2 \pm 6k + 1$ ist ungerade

$\Rightarrow \left(\frac{2}{p}\right) = -1.$

Daraus folgt Satz 5.9.

6. Es gilt $\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right)$ (L. 5.4 (ii))

$= (-1)^{\frac{p^2-1}{8}} \left(\frac{a}{p}\right)$ (Schritt 5)

und $\left(\frac{2a}{p}\right) = (-1)^{\frac{p^2-1}{8}} (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor}$ (Schritt 4)

$\Rightarrow \left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor}$

7. Für $p=q$ ist Satz 5.7 klar $\left(\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=0\right)$

Seien $p,q \in \mathbb{P}\setminus\{2\}$ verschieden

und $p_1 := \frac{p-1}{2}$

$q_1 := \frac{q-1}{2}$

Behauptung: $\sum_{i=1}^{p_1} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{j=1}^{q_1} \left\lfloor \frac{pj}{q} \right\rfloor = p_1 q_1$

Denn sei $s_1 := \left|\{(i,j) : 1 \le i \le p_1,\ 1 \le j \le q_1,\ qi > pj\}\right|$

$s_2 := \left|\{(i,j) : 1 \le i \le p_1,\ 1 \le j \le q_1,\ qi < pj\}\right|$

Da $qi \neq pj$ immer gilt (für $0<i<p$, $0<j<q$), ist

$s_1 + s_2 = \left|\{(i,j) : 1 \le i \le p_1,\ 1 \le j \le q_1\}\right|$

$= p_1 q_1$

Ausserdem gilt $qi > pj \iff j < \frac{qi}{p} \iff j \le \left\lfloor \frac{qi}{p} \right\rfloor$

$\Rightarrow s_1 = \sum_{i=1}^{p_1} \left|\{j : qi < pj\}\right|$

$= \sum_{i=1}^{p_1} \left\lfloor \frac{qi}{p} \right\rfloor$

und analog ist $s_2 = \sum_{j=1}^{q_1} \left\lfloor \frac{pj}{q} \right\rfloor$

also ist $\sum_{i=1}^{p_1} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{j=1}^{q_1} \left\lfloor \frac{pj}{q} \right\rfloor = s_1 + s_2 = p_1 q_1$

8. $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{i=1}^{p_1} \lfloor \frac{q_i}{p} \rfloor} (-1)^{\sum_{j=1}^{q_1} \lfloor \frac{p_j}{q} \rfloor}$ (Schritt 6)

$= (-1)^{p_1 \cdot q_1}$

$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Wenn $p = 4k+1$, dann ist $\frac{p-1}{2} = 2k$ gerade

also ist $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1^{\frac{q-1}{2}} = 1$

Wenn $q = 4k+1$ ist ähnlich $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$.

Wenn $p = 4k+1$

$q = 4l-1$ dann ist $\frac{p-1}{2}\frac{q-1}{2} = (2k-1)(2l-1)$ ungerade

$\Rightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$

Daraus folgt Satz 5.7.

□

Anwendungen des QRG

Lemma 5.10: Sei $a \in \mathbb{Z}$, $n = 4a^2 + 1$ und $p \in \mathbb{P}$ ein Primteiler von n.

Dann ist $p \equiv 1 \bmod 4$

Beweis: n ist ungerade, also $p \neq 2$

Und $(2a)^2 \equiv -1 \bmod n$

$\Rightarrow (2a)^2 \equiv -1 \bmod p$

$\Rightarrow \left(\frac{-1}{p}\right) = 1$

$\Rightarrow p \equiv 1 \bmod 4$ (1. Ergänzungssatz) □

Satz 5.11: Es gibt unendlich viele Primzahlen p sodass $p \equiv 1 \bmod 4$.

5, 13, 17, 29, 37, 41, ...

Beweis: Angenommen es gäbe nur endlich viele $q_1, \dots, q_k$

Sei $P := \prod_{i=1}^{k} q_i$ und $n := 4P^2 + 1$

Dann gilt $q_i \nmid n$ und $n > 1$.

Aber n hat nur Primteiler $p \equiv 1 \bmod 4$ (L 5.10)

also nur aus $q_1, \dots, q_k$ ↯ □

Bemerkung: Es gibt auch unendlich viele Primzahlen $p \equiv 3 \bmod 4$.

Der Beweis ist sogar einfacher und dabei braucht man das QRG nicht.

Aufgabe.

Wir sehen zwei Anwendungen auf Quadratsummen

Satz 5.12 (Lagrange): Sei $p \in \mathbb{P} \setminus \{2\}$

$\exists\, x, y \in \mathbb{N}$ sodass $x^2 + y^2 = p \iff p \equiv 1 \bmod 4$

$5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$ sind alle als Summe zweier Quadratzahlen darstellbar.

Aber $3, 7, 11, 19, \ldots$ nicht

Die eine Richtung ($\Rightarrow$) ist einfach

Für die Rückrichtung brauchen wir

Satz 5.13 (Satz von Thue):

Seien $p \in \mathbb{P}$, $e, f \in \mathbb{N}$ mit $e, f \geq 2$, $ef > p$ und $r \in \mathbb{Z}$

Dann existieren $x, y \in \mathbb{N}$ mit $0 \leq x < e$
$1 \leq y < f$
und $(p, y) = 1$

sodass

$$r \equiv \pm x \cdot y^{-1} \bmod p$$

Beweis: Wenn $e \geq p$, wähle $y = 1$ und $x \equiv r \bmod p$ mit $0 \leq x \leq p-1$

Wenn $p \mid r$, wähle $x = 0$, $y = 1$

Wenn $p \nmid r$ und $f \geq p$, wähle $x = 1$ und $y \equiv r^{-1} \bmod p$ mit $1 \leq y \leq p-1$

Wir können also annehmen, dass $e, f < p$.

Betrachte $yr - x$ für $x = 1, \dots, e$
$y = 1, \dots, f$

Es gibt $ef > p$ solche Zahlen, also sind mindestens zwei davon kongruent mod p.

$$y_1 r - x_1 \equiv y_2 r - x_2 \mod p$$

und $y_1 \neq y_2$ oder $x_1 \neq x_2$.

Wäre $y_1 \equiv y_2 \mod p$, dann wäre $y_1 = y_2$ $(f \leq p)$

$$\Rightarrow x_1 - x_2 \equiv r(y_1 - y_2) \equiv 0 \mod p$$

$$\Rightarrow x_1 - x_2 = 0 \qquad (e \leq p)$$

$$\Rightarrow x_1 = x_2 \quad \lightning$$

Also ist $y_1 - y_2 \not\equiv 0 \mod p$

$$\Rightarrow r \equiv (x_1 - x_2)(y_1 - y_2)^{-1} \mod p$$

$$\equiv \pm |x_1 - x_2| (|y_1 - y_2|)^{-1} \mod p$$

und $0 \leq |x_1 - x_2| < e$

$1 \leq |y_1 - y_2| < f$

□